Wireless Physical-layer Security Using Precoding and an Active Eavesdropper

Pedro Ivo da Cruz, Ricardo Suyama and Murilo Bellezoni Loiola

Abstract— **The wireless physical layer security can assist traditional encryption mechanisms by generating the keys, for instance. However, some techniques allow hiding information directly in the physical layer, such as performing precoding at the legitimate user using information about the channel, such as the received signal strength or the phase response. Most works on this kind of precoding also considers a passive eavesdropper. This work considers an active eavesdropper and proposes the use of a precoder based on the full channel impulse response. The results show the effectiveness of the proposed technique to secure the information transmission.**

Keywords— **wireless physical-layer security, channel estimation, precoding, blind equalization**

I. Introduction

Wireless networks have become an essential part of everyday life, interconnecting an increasing number of devices - such as smartphones, tablets and mobile computers. In addition to that, a variety of new services is being provided through such networks: for example, a large amount of people now utilizes these devices to access personal data and bank accounts. However, even though these services provide access to sensible data, wireless networks are still very vulnerable, mainly due to the nature of its transmission medium, to attacks such as eavesdropping [1].

Although it is a very important issue today, the security over communications channels is not new topic. In 1949, Shannon published one of the first works on this topic [2]. In this work, he proposed a way of transmitting a coded version of the message in a way that the eavesdropper could not detect the original message, even though it can obtain the error-free version of the coded message. The coded message is obtained by the sum in the binary field between the bits from the original message and a key, which the eavesdropper does not have the knowledge. Also, Shannon obtained the maximum achievable rate region in which the message can be transmitted in a secure way.

In 1975, Wyner extended Shannon's work, defining what he called the *wiretap channel* [3]. In this work, Wyner considered that the eavesdropper obtains a degraded version on the transmitted message, defining the equivocal rate: the rate at which the eavesdropper can not obtain the correct message. Furthermore, he derived the mathematical region of the equivocal rate, also proposing a code to maximize it.

Most of the security techniques in use nowadays relies on encryption techniques that requires a shared key. Algorithms like the Data Encryption Standard (DES) [4], needs that the legitimate nodes have the knowledge of the key and, therefore, it needs to be generated at one node and then transmitted through a secure channel. However, this channel is not always feasible, and therefore, asymmetric encryption algorithms, such as the RSA [5] are the most used. In this algorithm, private and public keys are generated at one node. The private key is used to decrypt the message, while the public key has the ability to encrypt it only, and not decrypt it. Then, the public key is shared to the network, and the nodes that need to send information use the public key to encrypt their messages, and only the node with the private key will be able to decrypt them.

However, these algorithms rely on the assumption that the keys are long enough and that it is computationally inefficient to find the private keys, which is not necessarily true. They also require a high computational power to generate the keys [1], which may be unfeasible to some type of networks, such as sensor networks, where the devices have limited processing capabilities.

Instead of using the secure channel or asymmetric encryption techniques, the physical layer security methods can be employed here to generate the secret keys and support the upper layer security algorithms, making it more difficult for eavesdroppers to obtain the exchanged information. There are basically two categories of physical layer security techniques: the ones that support upper layer encryption algorithms by generating encryption keys, and the ones that operate only at the physical layer level.

In order to use the channel as a mechanism to provide security, it must meet some requirements: reciprocity and spatial decorrelation. The reciprocity means that the channel from a node A to node B is the same from node B to node A if they are transmitting at the same frequency. The spatial decorrelation means that if a node changes its position in space, the channel changes significantly. This is important to guarantee that an eavesdropper in a different position will not have the same channel than the legitimate nodes.

The first work suggesting the wireless channel as a random source mechanism to generate the keys at the legitimate nodes was presented in [6]. In this work were proposed some methods to provide security at physical layer, and one of them made use of a signal containing some carriers at different frequencies that are exchanged between two legitimate users. As the channel is considered reciprocal, both nodes obtain the same set of phase differences between the original signal and the received

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 work was partially supported by CAPES and by FAPESP (2013/25977-7).

signal. This set of phase differences is then used to generate an encryption key through a block code scheme. This proposition is evaluated through computer simulations in [7].

There are also works that use other information related to the communication channel, as the received signal strength (RSS), to generate the encryption keys [8]. The work in [9] makes a comparison between the RSS and the methods based on the channel phase information.

The work in [10] proposes a scheme without using an upper-layer encryption mechanism. The technique consists in sending a set of carriers with different frequencies and phases from one legitimate node to another, which then obtains the channel phase response. This node precodes the confidential message using the channel phase information. When the signal containing the compensated message is received at the first legitimate node, the phase effects will be already mitigated due to the channel reciprocity. As the eavesdropper channel is different, it will not be able to decode the message.

Most of the works using the channel as a mechanism to keep information secure, uses only the RSS or the channel phase response to generate the keys or precode the message. In this work it is intended to use the full channel impulse response (CIR), adopting a precoding mechanism, also considering the assumptions of reciprocal channel and spatial decorrelation.

Furthermore, the majority of the works consider a passive eavesdropper, i.e, it will not apply any method or algorithm to try to overpass the security schemes, trying to detect the confidential message directly from the received signal considering its channel as authentic.

In this work it is considered a scheme that uses the full CIR to perform precoding at the legitimate transmitter, and additionally, that the eavesdropper will try to detect the confidential message using blind equalization.

This paper is organized as follows. Section II presents the protocol and the signals involved in the security model proposed in this work. The channel estimation, precoding and blind equalization techniques used to implement the model are presented in section III, while the simulations and the obtained results are shown in section IV. Finally, conclusions are made at section V.

II. Security Model

The model used in this work is based on the traditional eavesdropping scheme shown in figure 1. In this scheme, Alice wants to send confidential information to Bob in the presence of an eavesdropper, called Eve. The channel h is assumed to be reciprocal, i.e, the channel from Alice to Bob has the same CIR as the one from Bob to Alice.

To perform the secure transmission, Bob will send a training sequence of N binary phase-shift keying (BPSK) symbols $\mathbf{x} = [x_0 \; x_1 \; \cdots x_{N-1}]^{\mathrm{T}}$ to Alice. The received signal obtained by Alice can be written as:

$$\mathbf{y}_A = \mathbf{X}\mathbf{h} + \mathbf{w}_A, \tag{1}$$

where $\mathbf{X}$ is a convolution matrix containing the training sequence $\mathbf{x}$, $\mathbf{h} = [h_0 \; h_1 \cdots h_{L-1}]$ is a vector containing the taps of the channel h of length L, and $\mathbf{w}_A$ is the vector containing the samples of additive white Gaussian noise (AWGN) with zero means and variance σ_w^2 received by Alice.

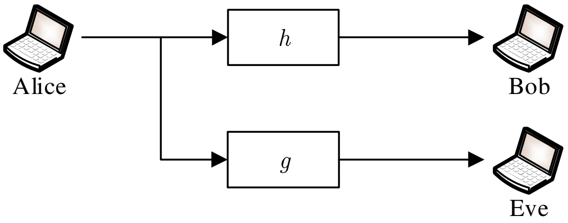

Fig. 1. Eavesdropping scheme over fading channels.

Alice, then, estimates $\mathbf{h}$ to perform precoding at the confidential message by obtaining an filter $w(n)$ from the estimated channel $\hat{h}(n)$, as will be shown in section III-B. Considering the confidential message being $m(n)$, the precoded signal is given by the convolution $m(n) * w(n)$. Letting $\mathbf{X}_p$ be the convolution matrix containing the samples from the precoded confidential message, and $\mathbf{w}_B$ the received AWGN ($\mathcal{N}(0, \sigma_w^2)$), the received signal at Bob is given by:

$$\mathbf{y}_B = \mathbf{X}_p\mathbf{h} + \mathbf{w}_B. \tag{2}$$

The signal received by Eve can be written as:

$$\mathbf{y}_E = \mathbf{X}_p\mathbf{g} + \mathbf{w}_E, \tag{3}$$

where $\mathbf{g}$ is the vector containing the taps of the channel between Alice and Eve, and $\mathbf{w}_E$ is AWGN ($\mathcal{N}(0, \sigma_w^2)$) received by Eve.

In this work, the channels are considered to have complex Gaussian distribution with L independent taps, each with zero mean and variance σ^2.

In summary, the steps followed by Alice and Bob in this technique is shown in figure 2. First, Bob send a training sequence to Alice. Second, Alice estimates the channel and performs precoding at the confidential message. Last, Alice broadcasts the precoded message, that will be received by Bob and Eve.

The security of this scheme is based on the assumption that $\mathbf{g}$ is different from $\mathbf{h}$ due to the spatial decorrelation, and therefore, Eve will not be able to recover the confidential message sent by Alice without trying to discover $\mathbf{h}$ or applying some other technique. In this work, it is considered that Eve applies blind equalization to recover the message.

III. Channel Estimation, Precoding and Blind Equalization

In general terms, in order to implement the scheme presented in the previous section, it is necessary to estimate the channel impulse response, hence obtaining $\hat{\mathbf{h}}$. Then, the precorder filter, $\mathbf{w}$, can be estimated based on different approaches, such as the ZF and MMSE equalizer, such that Bob receives a distortionless version of the information. At Eve side, since the channel is not the same, a blind equalization algorithm can be applied in order to unveil the message transmitted to Bob. The techniques used in this work are discussed in the following.

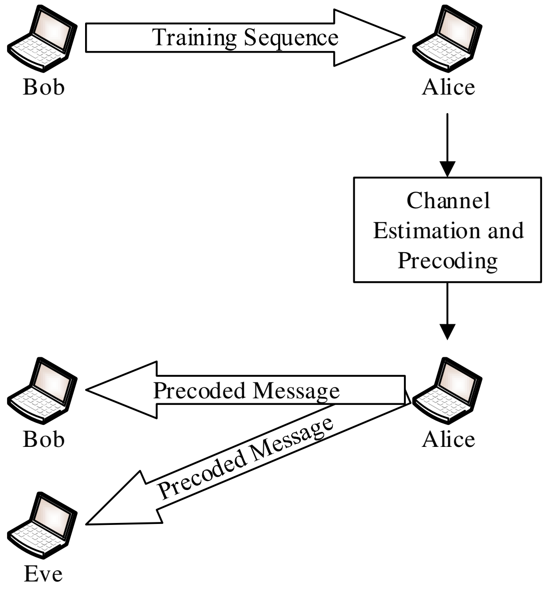

Fig. 2. Steps followed by Alice and Bob to secure the message.

A. Channel Estimation

This work considers two main supervised channel estimation techniques that can be found in the literature: the least squares (LS) and the Linear Minimum Mean Squared Error (LMMSE) estimators.

For the LS estimator, the channel estimate at Alice side is given by [11]:

$$\hat{\mathbf{h}} = (\mathbf{X}^{\mathrm{H}}\mathbf{X})^{-1}\mathbf{X}^{\mathrm{H}}\mathbf{y}_A. \tag{4}$$

On the other hand, the LMMSE estimator is obtained by considering the channel and noise covariance matrices ($\mathbf{R}_{\mathbf{hh}}$ and $\mathbf{R}_{\mathbf{ww}}$, respectively) known by Alice, and then computed as [11]:

$$\hat{\mathbf{h}} = \mathbf{R}_{\mathbf{hh}}\mathbf{X}^{\mathrm{H}}(\mathbf{X}\mathbf{R}_{\mathbf{hh}}\mathbf{X}^{\mathrm{H}} + \mathbf{R}_{\mathbf{ww}})^{-1}\mathbf{y}_A, \tag{5}$$

where $\mathbf{R}_{\mathbf{hh}} = \mathrm{E}\left[\mathbf{h}\mathbf{h}^{\mathrm{H}}\right] = \sigma^2\mathbf{I}$ and $\mathbf{R}_{\mathbf{ww}} = \mathrm{E}\left[\mathbf{w}\mathbf{w}^{\mathrm{H}}\right] = \sigma_w^2\mathbf{I}$.

B. Precoding

Precoding is a technique that weights the information stream in order to compensate for the channel effects before transmission, allowing the receiver to be as simples as a detector, such as a matched filter. To perform the precoding at Alice, it is necessary to obtain the precoding filter $\mathbf{w}$ from $\hat{\mathbf{h}}$ in order to avoid equalization at Bob. This procedure is called channel inversion. There are two main criteria to perform channel inversion: the zero-forcing (ZF) and the Minimum Means Squared Error (MMSE).

The precoder filter weights through the ZF criterion can be obtained through [12]:

$$\mathbf{w}_{ZF} = \mathbf{d}(\mathbf{H}^{\mathrm{H}}\mathbf{H})^{-1}\mathbf{H}, \tag{6}$$

where $\mathbf{d}$ is a column vector containing zeros and a 1 (one) at the center of the vector, and $\mathbf{H}$ is a convolution matrix containing the taps from channel h.

Using the MMSE criterion, the precoder filter weights is given by [13]:

$$\mathbf{w}_{MMSE} = \mathbf{d}\mathbf{H}^{\mathrm{H}}(\mathbf{H}\mathbf{H}^{\mathrm{H}} + \sigma_w^2\mathbf{I})^{-1}. \tag{7}$$

C. Blind Equalization

For equalization at Eve, it is used the constant modulus algorithm (CMA), an adaptive equalizer [14]. Considering $\mathbf{f} = [f_0\ f_1 \cdots f_{M-1}]$ to be the equalizer tap-weight vector of length M at the iteration n, the equalizer output can be written as:

$$\mathbf{y}(n) = \mathbf{f}^{\mathrm{H}}(n)\mathbf{u}(n), \tag{8}$$

where $\mathbf{u}(n) = [y_E(n)\ y_E(n-1) \cdots y_E(n-M+1)]^{\mathrm{T}}$ is the tap-input vector. The CMA error is then given by:

$$e(n) = |\mathbf{y}|^2 - 1, \tag{9}$$

and the tap-weight adaptation equation is given by:

$$\mathbf{f}(n+1) = \mathbf{f}(n) + \mu\mathbf{u}^*(n)\mathbf{y}(n)e(n). \tag{10}$$

Hence, Eve will apply this algorithm in order to recover the message precoded by Alice, and distorted by $\mathbf{g}$, even though $\mathbf{g}$ is different than $\mathbf{h}$, which is supposed to provide the security of this scheme.

IV. Simulations and Results

The security mechanism is evaluated by computer simulations in term bit error rate (BER) for different signal-to-noise ratios (SNR). A BPSK modulation is used for transmission, so the relationship E_b/N_0 is equal to the SNR. For each E_b/N_0 value, were performed 10^3 channel realizations, each of which with 10^3 transmitted symbols. Thus, a total of 10^7 bits were transmitted to compute the BER for each E_b/N_0 value.

In each realization, the channels have their taps generated randomly. The taps are independent, with complex Gaussian distribution with zero mean and unit variance. Thus, the magnitude of the channels will follow a Rayleigh distribution and the phases will follow an uniform distribution between 0 and 2π. In this work, it was considered both channels, $\mathbf{h}$ and $\mathbf{g}$ channel with 3 taps, and the precoder with 15 taps. The training sequence used contains 100 BPSK symbols for all cases. The precoder filters in this work have 15 taps, and the CMA equalizer has 45 taps, and adaptation step of $\mu = 0.0001$.

Figure 3 shows the BER obtained in Bob and Eve when Alice uses ZF or MMSE precoding with the LS channel estimator. In this case, Eve is a passive node. It can be seen that, while for Bob the BER reduces when E_b/N_0 increases, for Eve it keeps at 0.5. This means that Eve is not able to decode the message. In this figure, both curves for Eve are overlapped.

The same behavior can be observed in figure 4, when an LMMSE channel estimator is applied. Again, as expected, Eve is not able to recover the confidential message, once its BER remains at 0.5. Again, both curves for Eve are overlapped. In both figures 3 and 4 is possible to see that the MMSE precoder has a BER performance worse than the ZF precoder for Bob. This happens because the MMSE expression considers the noise variance σ_w^2 in its expression, given by (7), but the signal being precoded does not have any noise on it. Thus, the use of

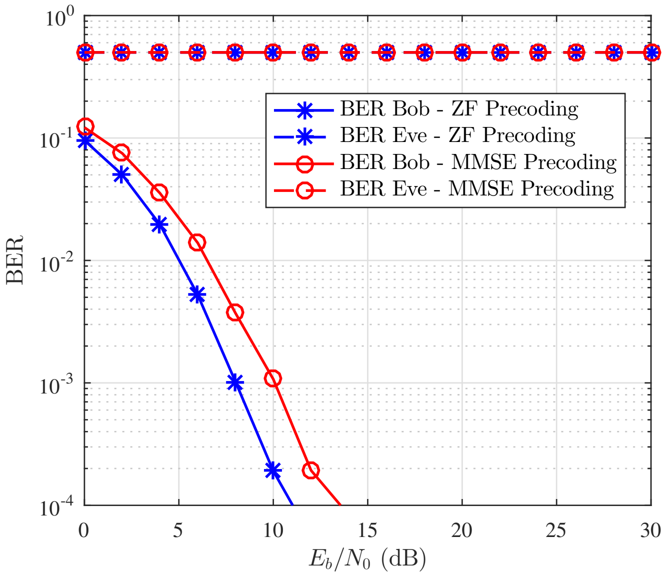

Fig. 3. BER for LS Channel Estimator comparing ZF and MMSE Precoding.

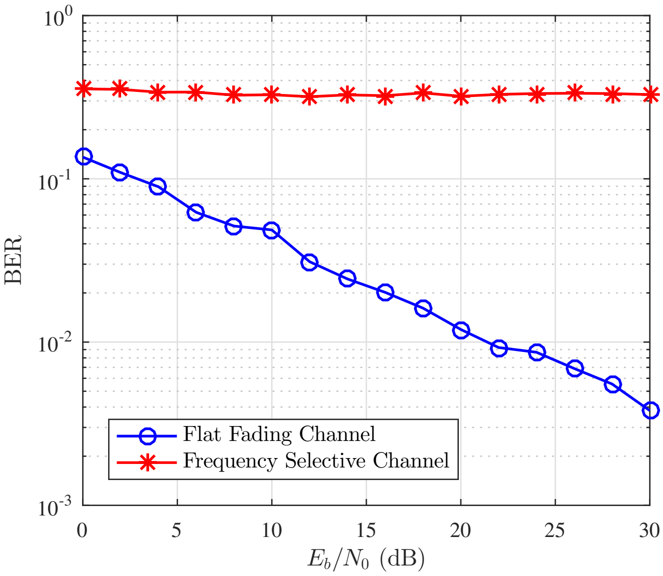

Fig. 5. BER at Eve using CMA equalizer for different channel lengths.

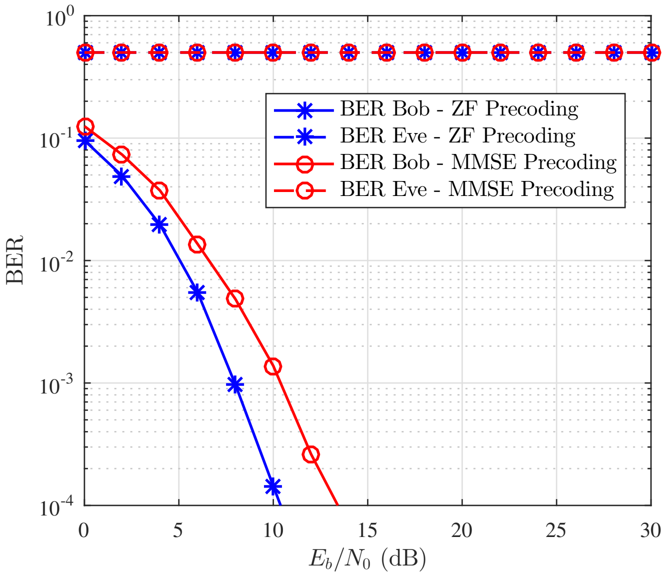

Fig. 4. BER for LMMSE Channel Estimator comparing ZF and MMSE Precoding.

MMSE precoder impairs the detection at Bob, and, as shown, does not bring any benefit to the security scheme, once the ZF brings the same BER performance at Eve.

The BER obtained when applying the CMA at Eve is shown in figure 5, considering the cases when $\mathbf{h}$ and $\mathbf{g}$ are flat fading channel, and frequency selective with 3 taps. It can be seen that, for a flat fading channels, the CMA helps EVE to to reduce the BER to a level of 4×10^{-3} for 30 dB, a level that might allow Eve to decode the message. However, for the 3 tap frequency selective channels, the BER keeps its value in 0.3, even with the increase in E_b/N_0. In practice, at this BER level, is impossible to decode any message. This happens because the CMA needs more time to converge when the channel is frequency selective and, therefore, it is necessary to increase the complexity of the receiver.

In this scenario, it was used a CMA with 45 coefficients. This number was chosen because the precoder filters have 15 taps. Therefore, the CMA needs to have a sufficient number of weights that allows it to mitigate the effects caused by the filter resulted from the convolution between the channel and the precoder filter. This also increases the complexity necessary to allows Eve to decode the message. Furthermore, Eve might not know the channel length, which makes important to choose a high value for the CMA equalizer length.

V. Conclusions

This paper proposes a wireless physical layer security scheme using the full CIR and precoding, while most works in literature focus on the RSS information and the channel phase information to achieve confidentiality.

Furthermore, this work also considers an active eavesdropper in the sense that it will try to apply some signal processing technique in order to try to recover the confidential message.

It is shown that, for a passive eavesdropper, the mechanism proposed here works well, providing a good BER at Bob (the legitimate node) and a very high BER at Eve (the eavesdropper). The system was evaluated for different combinations of LS and LMMSE channel estimators, and for ZF and MMSE precoders.

Finally, in order to recover the message, Eve uses the CMA equalizer. It was shown that, for a flat fading channel, Eve was able to reduce the BER level to a value that might allows it to recover the confidential message. However, for a frequency selective channel with 3 taps, it was show that the BER keeps at a high level, making it impossible for Eve to recover the message without any additional technique.

References

[1] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, “Physical layer security in wireless networks: a tutorial,” *IEEE Wireless Communications*, vol. 18, Apr. 2011.

[2] C. Shannon, “Communication theory of secrecy system,” *Bell System Technical Journal*, vol. 28, 1949.

[3] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, Oct. 1975.

[4] *Data Encryption Standard*, Federal Information Processing Standards Publication 46 Std., 1977.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, Feb. 1978.

[6] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, 1995.

[7] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, Oct. 1996.

[8] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM conference on Computer and communications security - CCS '07*. ACM Press, 2007.

[9] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, Aug. 2011.

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

[11] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.

[12] R. Ziemer and R. Peterson, *Introduction to digital communication*. Macmillan Pub. Co., 1992.

[13] B. Sklar, *Digital communications: fundamentals and applications*. Prentice-Hall PTR, 2001.

[14] P. Diniz, *Adaptive Filtering: Algorithms and Practical Implementation*. Springer US, 2012.