Physical Layer Authentication: A CSI-Based Approach with Information Reconciliation

Atsu Kokuvi Angélo PASSAH[1 2]   Arsenia CHORTI[2 4]   Rodrigo C. DE LAMARE[1 3]

[1]Department of Electrical Engineering (DEE), CETUC, PUC-Rio, Brazil

[2]ETIS Laboratory UMR 8051, ENSEA, CY Cergy Paris University, CNRS, France

[3] School of Physics, Engineering and Technology, York University, United Kingdom

[4]Barkhausen Institut gGmbH, Germany

Résumé – Ce travail étudie l'authentification au niveau de la couche physique (PLA) pour les futurs réseaux de communication sans fil. Les méthodes cryptographiques traditionnelles pourraient devenir impraticables en raison de leurs exigences en matière de calcul. PLA peut offrir une solution rentable pour les réseaux Internet des objets à faible coût. Nous proposons une technique de PLA utilisant la réconciliation d'informations basée sur des codes correcteurs d'erreurs, à la fois dans une configuration mono-utilisateur à entrées multiples et sortie unique (SIMO) et dans des configurations multi-utilisateurs SIMO. À la suite de la réconciliation, un test d'hypothèse est appliqué pour déterminer si un appareil est authentifié. Les résultats de simulation montrent que notre méthode de PLA proposée avec réconciliation surpasse largement les techniques existantes.

Abstract – This work studies physical layer authentication (PLA) for future wireless communication networks. Traditional cryptographic methods may become impractical due to their computational demands. PLA can offers a cost-efficient solution for low-end Internet of Things networks. We propose a PLA technique using information reconciliation based on error-correcting codes, in both single-user single-input multiple-output (SIMO) setup and multi-user SIMO configurations. Following reconciliation, hypothesis testing is applied to determine whether a device is authenticated. Simulation results demonstrate that our proposed PLA method with reconciliation significantly outperforms existing techniques.

1 Introduction

The advent of next-generation wireless systems characterized by large-scale and heterogeneous Internet of Things (IoT) networks introduces a lot of security challenges. In this context, conventional cryptographic schemes based on public key encryption for node authentication can impose significant computational burdens, potentially leading to performance degradation and increased latency [1]. To address these limitations, physical layer security (PLS) mechanisms, in particular PLA is expected to be a promising solution to be integrated into future wireless networks [2].

Various channel-based physical-layer authentication (PLA) schemes have been explored. The work in [4] introduced an authentication method leveraging the channel impulse response (CIR) and incorporating additional multipath delay characteristics of the wireless channel into the authentication process. A two-dimensional quantization technique was employed. In contrast, the authors in [5] proposed two CIR-based PLA schemes without quantization to avoid quantization errors that could degrade the authentication performance. Unlike both approaches, the study in [6] introduced a key-based PLA framework that uses the channel phase response for authentication.

The results presented in this work are related to those reported in [7] and [8]. These referenced works address the challenge of physical layer authentication based on channel state information (CSI). The proposed method uses information reconciliation based on Slepian-Wolf coding with polar codes to reconcile discrepancies between successive CSI.

The rest of this paper is organized as follows. Section 2 presents the system model. In Section 3, the proposed approach is described in detail, while performance analyses are carried out in Section 4. Simulation results are presented in Section 5 and the paper is concluded in Section 6.

2 System Model

We consider a multi-user wireless communication network. The network comprises Alice (the user of interest), Bob (the base station), and U additional legitimate users who act as interfering users during transmissions. Within this setup, Bob aims to authenticate Alice in the presence of both these interfering users and an adversary, Mallory. Mallory is modeled as a naive active attacker who attempts to impersonate Alice. The goal is to develop a channel state information (CSI)-based authentication scheme capable of reliably distinguishing Alice from Mallory, even in the presence of interference. All users, including Alice, Mallory, and the interfering nodes, are assumed to be equipped with a single antenna, while Bob is equipped with N_b antennas.

To ensure sufficient spatial separation among users, we assume a rich scattering environment and that the distance between any pair of users exceeds half a wavelength. Under these conditions, the channel characteristics between different transmitter-receiver pairs can be considered spatially uncorrelated [9].

The authentication process consists of two main phases: the enrollment phase and the authentication phase. During

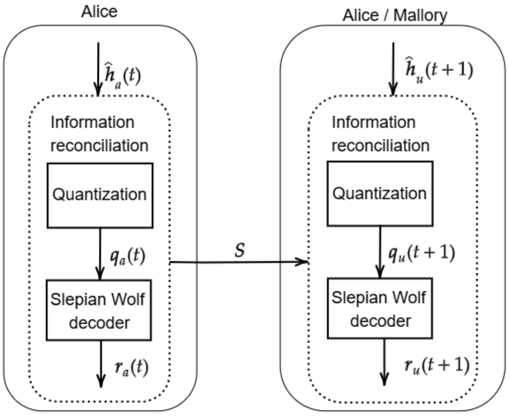

Figure 1 – Proposed PLA scheme, $u \in \{a, m\}$

the enrollment phase, Bob estimates Alice's channel state information (CSI), denoted as $\mathbf{h}_a(t) \in \mathbb{C}^{1\times N_b}$, in time slot t. This offline step enables Bob to store $\mathbf{h}_a(t)$ as a reference to verify Alice's identity in the next step. In the subsequent authentication phase, in the time slot $t+\ell$, Bob obtains a new CSI measurement $\mathbf{h}_u(t+\ell) \in \mathbb{C}^{1\times N_b}$, where $u \in \{a, m\}$ corresponds to Alice or Mallory. In this online phase, Bob must determine whether the estimated CSI originates from Alice or Mallory by comparing it to the reference obtained during enrollment.

We consider a scenario in which the CSI varies slowly over time. In this context, the channel between the same transmitter-receiver pair can be modeled as a first-order Gauss-Markov process in Eq. 1 [5].

$$\mathbf{h}_a(t+\ell) = \beta \mathbf{h}_a(t+\ell-1) + \sqrt{1-\beta^2}\mathbf{n}_a, \tag{1}$$

where β is the channel correlation coefficient and $\mathbf{n}_a$ is a measurement noise, $n_{ai} \sim \mathcal{CN}\left(0, \sigma_h^2\right)$, $i = 1, \ldots, N_b$. $\mathbf{n}_a$ is statistically independent of $\mathbf{h}_a$.

3 Proposed Authentication Scheme

To address the inconsistencies in CSI measurements observed across different time slots, we introduce the reconciliation scheme based on the Slepian-Wolf decoding principle [10]. This method aims to reconcile the channel measurements during the enrollment phase to the ones during the authentication phase as in Fig. 1. During each phase, the CSI is quantized, and the resulting vectors at time slots t and $t+\ell$ are interpreted as dithered codewords input to the reconciliation decoder (Fig. 1). The decoder produces a reconciled vector for each time instance.

3.1 PLA phases

First during the enrollment phase, Bob records the CSI of Alice as a reference to be used during the next phase

$$\hat{\mathbf{h}}_a(t) = \mathbf{h}_a(t) + \mathbf{z}(t), \tag{2}$$

where $\mathbf{z}(t) \in \mathbb{C}^{1\times N_b}$ is a zero mean complex Gaussian noise so that $z_i(t) \sim \mathcal{CN}\left(0, \sigma_z^2\right)$, $i = 1, \ldots, N_b$. M samples of $\hat{\mathbf{h}}_a(t)$ are concatenated and by considering the real and imaginary parts, we get the vector $\mathbf{x}_a(t) \in \mathbb{R}^{1\times N}$ where $N = 2MN_b$. $\mathbf{x}_a(t)$ is then quantized as $\mathbf{q}_a(t)$.

Then during the authentication phase (online phase), Bob records new CSI measurements of an unkown user. Without loss of generality, we assume $\ell = 1$. When the user is Alice,

$$\hat{\mathbf{h}}_a(t+1) = \mathbf{h}_a(t+1) + \sum_{i=1}^{U} \alpha_i^a \mathbf{h}_i^a(t+1) + \mathbf{z}_a(t+1), \tag{3}$$

whereas the new channel measurements of Mallory are described by

$$\hat{\mathbf{h}}_m(t+1) = \mathbf{h}_m(t+1) + \sum_{i=1}^{U} \alpha_i^m \mathbf{h}_i^m(t+1) + \mathbf{z}_m(t+1). \tag{4}$$

$\mathbf{z}_a(t+1)$ and $\mathbf{z}_m(t+1)$ are Gaussian noise vectors, $\mathbf{h}_i^a(t+1)$ and $\mathbf{h}_i^m(t+1)$ are interfering terms with interference weights α_i^a and α_i^m respectively. Similarly to the previous phase, M samples of the channel measurements are concatenated in a vector $\mathbf{x}_u(t) \in \mathbb{R}^{1\times N}$, $u \in \{a, m\}$, and quantized as $\mathbf{q}_u(t+1)$.

For the quantization, we employ Lloyd-Max quantizer, a powerful tool for designing optimal quantizers. Then Gray code is used to convert the optimal quantized levels into bits.

3.2 Reconciliation

$\mathbf{q}_a(t)$ and $\mathbf{q}_u(t+1) \in 0, 1^{1\times nN}$ are input to the reconciliation decoder, which maps them to output vectors $\mathbf{r}_a(t)$ and $\mathbf{r}_u(t+1)$ Fig. 1, respectively, where nN denotes the code length. Our reconciliation scheme is based on the Slepian-Wolf decoding principle, as described in [11]. Specifically, $\mathbf{q}_a(t+1)$ is decoded using side information $\mathbf{S}$. It is generated during the enrollment phase based on the quantized vector $\mathbf{q}_a(t)$ and the underlying code design. This mechanism leverages the correlation between CSI observations in the enrollment and authentication phases. By exploiting this correlation, the decoder is able to differentiate between Alice and Mallory. In this framework, $\mathbf{q}_a(t)$ and $\mathbf{q}_a(t+1)$ are treated as dithered versions of the same underlying codeword, allowing the scheme to correct measurement errors. Polar codes [11], a class of capacity-achieving error-correcting codes, are employed for the reconciliation process in this work.

To improve the performance of polar codes in the finite blocklength regime, the quantized vector $\mathbf{q}_u(t+1)$ is decoded using cyclic redundancy check (CRC)-aided successive cancellation list (SCL) decoding [10], with a list size denoted by L_s. In this decoding process, Bob simultaneously tracks L_s decoding paths and selects the most probable codeword that satisfies the CRC condition among the candidates. The syndrome is generated using the quantized vector $\mathbf{q}_a(t)$ obtained during the enrollment phase and the reliability sequence employed for the code construction. For this purpose, the reliability sequence for the polar code construction is derived using the recursive formulation associated with a binary erasure channel (BEC), as defined in [12].

To distinguish between Alice and Mallory, two hypotheses are defined: H_0, corresponding to the legitimate case where the transmission originates from Alice, and H_1, representing the spoofing scenario in which Mallory attempts to impersonate Alice.

$$\begin{cases} H_0 : \ \eta = \mathcal{H}_d\left(\mathbf{r}_a(t), \mathbf{r}_a(t+1)\right) \leq \eta_{th} \\ H_1 : \ \eta = \mathcal{H}_d\left(\mathbf{r}_a(t), \mathbf{r}_m(t+1)\right) > \eta_{th} \end{cases} \tag{5}$$

As bitwise comparison between $\mathbf{r}_a(t)$ and $\mathbf{r}_u(t+1)$, $u \in \{a, m\}$, is considered. $\mathcal{H}_d(\cdot)$ is then the Hamming distance between $\mathbf{r}_a(t)$ and $\mathbf{r}_u(t+1)$ as (6) [7].

$$\eta = \mathcal{H}_d((\mathbf{r}_a(t), \mathbf{r}_u(t+1)) = \sum_{j=1}^{K} |r_{a,j}(t) - r_{u,j}(t+1)| \tag{6}$$

4 Analysis

The probability of false alarm and of detection are considered. The probability distributions of η are given in Propositions 1 and 2 under H_0 and H_1, respectively.

Proposition 1

Under H_0, η follows a binomial distribution of parameters K and p_0, i.e. $\eta \sim \mathbb{B}(K, p_0)$.

$$P(\eta = k|H_0) = \binom{K}{k} p_0^k (1-p_0)^{K-k}, \tag{7}$$

where p_0 is the bit error probability.

Proposition 2

Under H_1, η follows a binomial distribution of parameters K and p_1, i.e. $\eta \sim \mathbb{B}(K, p_1)$.

$$P(\eta = k|H_1) = \binom{K}{k} p_1^k (1-p_1)^{K-k}, \tag{8}$$

where p_1 is the bit error probability.

Given the PDFs of η, the closed-form expressions of P_{FA} and P_D are respectively given by

$$P_{FA} = \sum_{k=\eta_{th}+1}^{K} \binom{K}{k} p_0^k (1-p_0)^{K-k} \tag{9}$$

and

$$P_D = \sum_{k=\eta_{th}+1}^{K} \binom{K}{k} p_1^k (1-p_1)^{K-k}. \tag{10}$$

5 Numerical Results

This section presents the simulation results of the comparison between our proposed method and the prior ones proposed in [4], [5] and [6]. We investigate the ROC curve which is P_D vs P_{FA} and the impact of the SNR on the probability of detection. Unless otherwise specified, the simulation parameters are: $N_b = 32$, $\beta = 0.9$, $\sigma_h^2 = 1$, $M = 16$, $N = 1024$, the code rate is 0.01, $\alpha_i^a = \alpha_i^m = 0.01$, $\forall\, i$ and $P_{FA} = 10^{-3}$.

5.1 Single user SIMO

In this case of single user SIMO communication channel, there are no interfering users ($U = 0$), the system contains Alice, Mallory and Bob (base station). Also, only 1-bit quantizer is considered.

Fig. 2 illustrates the receiver operating characteristic (ROC) curve for an SNR of $5\ dB$. As expected, P_D increases with P_{FA}. The proposed reconciliation-based method outperforms previous approaches, achieving a P_D very close to 1, even at very low false alarm probabilities. Fig. 3 shows P_D as a function of the code rate for a $SNR = 15\ dB$. We observe that the detection probability is almost equal to 1 for code rates less than 0.2.

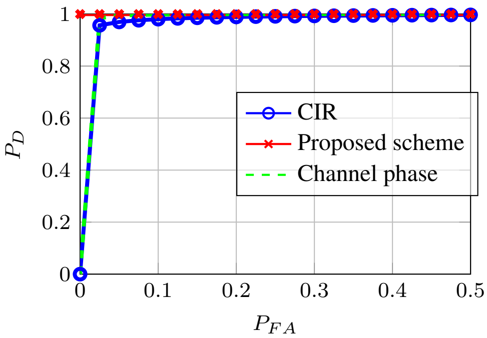

Figure 2 – ROC curve: $SNR = 5dB$

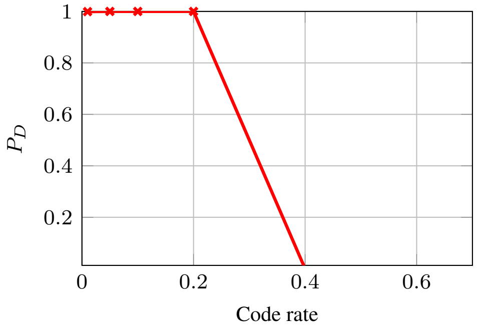

Figure 3 – P_D vs code rate: $SNR = 15dB$

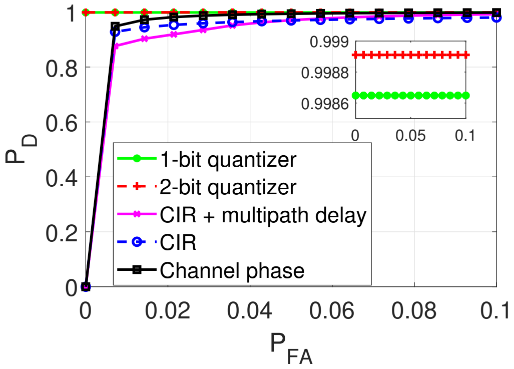

Figure 4 – ROC curve: $SNR = 5\ dB$

5.2 Multiuser SIMO

In this case of multiuser SIMO communication channel where the interfering users are included ($U = 5$), we also present the results of the proposed method for different code-lengths, $nN = 1024$ and $nN = 2048$, which correspond to 1-bit ($n = 1$) and 2-bit ($n = 2$) quantizers, respectively.

Fig. 4 shows the ROC curve. The proposed method demonstrates excellent performance, achieving a probability of detection (P_D) very close to 1 even for very low false alarm probabilities ($P_{FA} < 0.1$). As depicted in the figure, we get more than 99.80% increase in detection probability. Moreover, it outperforms previously reported schemes.

In Fig. 5, the impact of the signal-to-noise ratio (SNR) on the detection probability (P_D) is presented. As the SNR

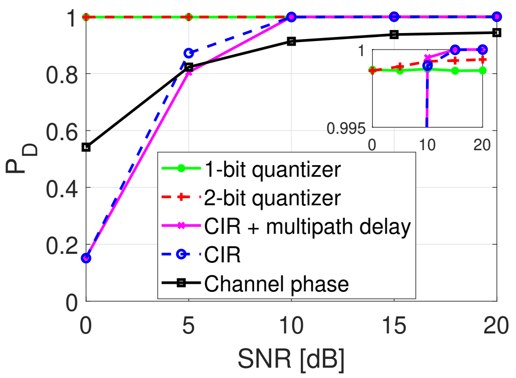

Figure 5 – P_D vs SNR: $P_{FA} = 10^{-3}$

Table 1 – Detection probabilities for different $\alpha^a = \alpha^m$

$\alpha^a = \alpha^m$	1-bit	2-bit	in [4]	in [5]	in [6]
0	0.99	0.99	0.99	0.99	0.99
0.01	0.99	0.99	0.99	0.99	0.91
0.8	0.99	0.99	0.90	0.22	0.43
1.6	0	0	0.90	0.01	0.07

increases, P_D improves accordingly. The proposed scheme demonstrates excellent performance, achieving a detection probability exceeding 99.86%. In contrast, the performance of existing methods significantly deteriorates at low SNR values, highlighting the robustness of our approach under challenging conditions.

Table 1 presents the behaviour of P_D for different values of the interference weights $\alpha^a = \alpha^m$ under a $SNR = 10\ dB$. We found that, for the given system parameters, the maximum interference weight that achieves almost perfect reconciliation is equal to 0.8 for the proposed scheme. The techniques reported in [5] and [6] perform poorly from $\alpha^a = \alpha^m = 0.8$, that is, the detection probabilities are respectively equal to 0.22 and 0.43 for $\alpha^a = \alpha^m = 0.8$. The work in [4] has a good performance for weights above 0.8 because of the high correlation in the multipath delays.

All the previous presented results are shown for 1-bit and 2-bit quantizers. The 2-bit quantizer performs better than the 1-bit one as there is more bits that increase the code length. This also shows the impact of the code length on the performance.

6 Conclusion

In this work, we investigated the problem of physical layer authentication (PLA) based on information reconciliation. Specifically, we employed error-correcting codes to reconcile discrepancies between channel measurements and to distinguish between legitimate and spoofed transmissions. We considered a single-user SIMO communication scenario and a multi-user SIMO system with interfering users. Simulations confirm the effectiveness of the proposed reconciliation-based authentication scheme.

Acknowledgment

A. K. A. Passah has been supported by the project SRV ENSEA. A. Chorti has been partially supported by the EC through the Horizon Europe/JU SNS project ROBUST-6G GA no. 101139068, the IPAL project CONNECTING, the ANR-PEPR 5G Future Networks project and the CYU INEX-PHEBE project. R. C. de Lamare has been supported by PUC-Rio, CNPq, FAPERJ and FAPESP.

References

[1] Shakiba-Herfeh, M., Chorti, A., Vincent Poor, H. (2021). *Physical Layer Security: Authentication, Integrity, and Confidentiality.* In: Le, K.N. (eds) Physical Layer Security. Springer, Cham.

[2] Bloch, M., and Barros, J. (2011). *Physical-Layer Security: From Information Theory to Security Engineering.* Cambridge: Cambridge University Press.

[3] F. J. Liu, X. Wang and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," 2013 *IEEE International Conference on Communications (ICC)*, Budapest, Hungary, 2013, pp. 4724-4728.

[4] J. Liu and X. Wang, "Physical Layer Authentication Enhancement Using Two-Dimensional Channel Quantization," in *IEEE Transactions on Wireless Communications,* vol. 15, no. 6, pp. 4171-4182, June 2016.

[5] N. Xie, J. Chen and L. Huang, "Physical-Layer Authentication Using Multiple Channel-Based Features," in *IEEE Transactions on Information Forensics and Security,* vol. 16, pp. 2356-2366, 2021.

[6] X. Lu, J. Lei, Y. Shi and W. Li, "Physical-Layer Authentication Based on Channel Phase Responses for Multi-Carriers Transmission," in *IEEE Transactions on Information Forensics and Security,* vol. 18, pp. 1734-1748, 2023.

[7] A. K. Angélo Passah, R. C. De Lamare and A. Chorti, "Physical Layer Authentication Using Information Reconciliation," *2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, Singapore, Singapore, 2024.

[8] A. Kokuvi Angélo Passah, A. Chorti and R. C. de Lamare, "Enhanced Multiuser CSI-Based Physical Layer Authentication Based on Information Reconciliation," in *IEEE Wireless Communications Letters,* vol. 14, no. 2, pp. 544-548, Feb. 2025.

[9] Jakes William C., "Microwave Mobile Communications," *IEEE,* 1994.

[10] M. Shakiba-Herfeh and A. Chorti, "Comparison of Short Blocklength Slepian-Wolf Coding for Key Reconciliation," *2021 IEEE Statistical Signal Processing Workshop (SSP),* Rio de Janeiro, 2021, pp. 111-115.

[11] E. Arikan, "Source polarization," *2010 IEEE International Symposium on Information Theory,* Austin, TX, USA, 2010, pp. 899-903.

[12] E. Arikan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," in *IEEE Transactions on Information Theory,* vol. 55, no. 7, pp. 3051-3073, July 2009.