Enhanced Multiuser CSI-Based Physical Layer Authentication Based on Information Reconciliation

Atsu Kokuvi Angélo Passah, Arsenia Chorti, *Senior Member, IEEE,*
and Rodrigo C. de Lamare, *Senior Member, IEEE*

Abstract—**This letter presents a physical layer authentication (PLA) technique using information reconciliation in multiuser communication systems. A cost-effective solution for low-end Internet of Things networks can be provided by PLA. In this letter, we develop an information reconciliation scheme using Polar codes along with a quantization strategy that employs an arbitrary number of bits to enhance the performance of PLA. We employ the principle of Slepian-Wolf coding to reconcile channel measurements spread in time. Numerical results show that our approach works very well and outperforms competing approaches, achieving more than 99.80% increase in detection probability for false alarm probabilities close to 0.**

Index Terms—**Physical layer authentication, physical layer security, information reconciliation, multiuser systems, multiple-antenna systems.**

I. INTRODUCTION

THE ADVENT of novel wireless systems such as large-scale, heterogeneous, Internet of Things (IoT) networks [1], introduces numerous security concerns. In this context, standard cryptographic schemes using public key encryption for node authentication may be broken by quantum computers while post-quantum alternatives may be inappropriate for simple devices due to their computational complexity, or significant delays in low-latency systems [2], [3]. Therefore, physical-layer security alternatives are of great interest [4], [5], [6]. In particular, physical-layer authentication (PLA) protocols are expected to play a crucial role by providing alternative low-complexity and low-latency quantum-resistant solutions. CSI-based PLA is a two-step procedure, including an enrollment (off-line) phase and an authentication (on-line) phase. Typically, higher layer

authentication protocols are assumed to be used during the enrollment phase, during which a CSI (or a RF fingerprint) baseline observation is recorded for a node of interest. In the authentication phase, hypothesis testing is subsequently used to verify the consistency of the recorded observation against a new measurement of the CSI.

Recently, several channel-based PLA schemes have been investigated. The study in [7] developed an authentication scheme using the channel impulse response (CIR) and incorporated extra multipath delay characteristics of the wireless channel into the authentication framework. Furthermore, this study employed a two-dimensional quantization method to reduce the impact of random variations in amplitudes and delays. Differently from [7], the authors in [8] proposed two PLA schemes based on CIR without employing a quantization algorithm. The approach in [8] eliminates the quantization errors that can negatively affect the authentication performance. Unlike the other works, [9] proposed a key-based PLA by exploiting the channel phase response to perform the authentication. In [10], preliminary results of a PLA scheme using information reconciliation with a one-bit quantization scheme have been reported for a single-user communication network in the presence of a naive active attacker.

In this letter, we present an information reconciliation scheme based on polar codes along with a quantization strategy that employs an arbitrary number of bits in order to enhance the performance of channel state information (CSI) based PLA in multiuser systems. In particular, we employ the principle of Slepian-Wolf coding reconciliation to reconcile channel measurements spread in time. An analysis of the proposed reconciliation scheme is carried out in terms of probabilities of detection and false alarm. To the best of our knowledge, apart from our preliminary results in [10] for a single-user system and a scheme with 1-bit quantization, it is the first time reconciliation is being considered in PLA, despite the use of similar concepts in the form of fuzzy extractors in physical unclonable functions and biometrics based authentication schemes.

The rest of this letter is organized as follows. Section II presents the system model and explains the authentication phases. In Section III, the proposed approach is described in detail, while performance analyses are carried out in Section IV by deriving closed-form expressions of the probabilities of false alarm and detection. Simulation results are presented in Section V and this letter is concluded in Section VI.

II. SYSTEM MODEL

A multiuser wireless communication network is considered Fig. 1. The network includes legitimate nodes, referred to

Fig. 1.   Multiuser system with interference.

Fig. 2.   Proposed PLA scheme, $u \in \{a, m\}$.

as Alice, Bob (base station) and U legitimate users that act as interfering users during the transmission. In this network, Bob wants to authenticate the user of interest Alice in the presence of the other legitimate users and an adversary Mallory that is a naive active attacker that attempts to impersonate Alice without the use of any precoder or other pre-processing technique [11]. The objective is to design a scheme based on CSI to distinguish Alice from Mallory in the presence of interfering users. Each user is equipped with a single antenna and Bob is equipped with N_b antennas.

To achieve a good separation between different users, we assume that the communication occurs in a rich scattering environment and the distance among users exceeds half of a wavelength. Thus, channel attributes between different transmitter-receiver pairs are spatially uncorrelated [12], [13]. We are testing the proposed algorithm on real datasets and preliminary results look promising but are left as future work.

The authentication comprises two phases, an enrollment phase and an authentication phase. First, in the enrollment phase, Bob estimates Alice's CSI $\mathbf{h}_a(t) \in \mathbb{C}^{1 \times N_b}$ in time slot t. This offline step allows Bob to use $\mathbf{h}_a(t)$ as a point of reference during the authentication phase to determine if the user is indeed Alice or not. Next, during the authentication phase in a subsequent time slot $t + \ell$, Bob takes new CSI measurements of $\mathbf{h}_u(t + \ell) \in \mathbb{C}^{1 \times N_b}$, $u \in \{a, m\}$, that may either come from Alice or Mallory, a and m denote, respectively, Alice and Mallory. In this online phase, Bob needs to make an authentication decision based on the CSI obtained in the enrollment phase. We consider a scenario where the CSI changes slowly over time. The channel between the same transmitter-receiver pair can then be well described by a first order Gauss-Markov process [8]. The channel between Alice and Bob in time slot $t + \ell$ can therefore be expressed as

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

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

III. PROPOSED AUTHENTICATION SCHEME

We present a reconciliation scheme to mitigate the impact of disparities in the CSI observed in different time slots. We use the principle of Slepian-Wolf decoding [14] to reconcile discrepancies in the CSI measurements over time, as depicted in the system model illustrated in Fig. 2. We propose this channel-based PLA scheme that employs quantization with an arbitrary number of bits for multiuser systems. Each phase involves quantizing the CSI, with the output vectors at time
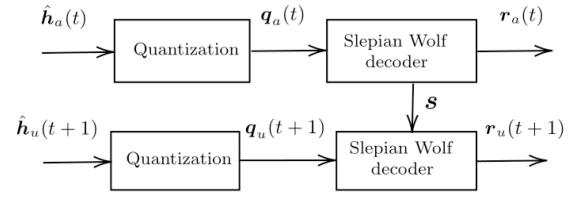
t and $t + \ell$ treated as dithered codewords at the input of the reconciliation decoder (Fig. 2). The reconciliation decoder outputs one reconciled vector at each time instance. Note that to this end, the helper data $\mathbf{S}$ (e.g., in the form of a syndrome) generated in the first phase is used by Bob in the authentication phase to reconcile the newly obtained CSI at time $t + \ell$ to the previous one at time t. Then, a hypothesis testing is performed to identify the legitimate user versus the impersonator.

A. PLA Phases

The PLA phases are structured as follows.

1) Enrollment Phase: In this offline phase, Bob measures the CSI of Alice as a reference for the authentication:

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

where $\mathbf{z}(t) \in \mathbb{C}^{1 \times N_b}$ is a zero mean complex Gaussian noise so that $z_i(t) \sim \mathcal{CN}(0, \sigma_z^2)$, $i = 1, \ldots, N_b$. 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 $\mathbf{q}_a(t)$.

2) Authentication Phase: Without loss of generality, we assume $\ell = 1$. In this online phase at time $t + 1$, new channel measurements associated with Alice are given by

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

such that $\mathbf{h}_a(t+1) = \beta \mathbf{h}_a(t) + \sqrt{1 - \beta^2} \mathbf{n}_a$, whereas the new channel measurements of Mallory are described by

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

where $\mathbf{z}_a(t + 1)$ 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. The weights account for the fact that in the channel estimation, different users might use different pilot sequences that can be quasi-orthogonal [15]. 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 $\mathbf{q}_u(t + 1)$.

3) Quantization: We use the Lloyd-Max quantizer that is a powerful tool for designing optimal quantizers. As 99.7% of the probability density of a Gaussian distribution (μ, σ^2) lies within $\mu - 3\sigma$ and $\mu + 3\sigma$, the design steps are described by
- n-bit quantizer $\implies L = 2^n$ quantized levels
- Divide the range $R = (\mu + 3\sigma) - (\mu - 3\sigma) = 6\sigma$ in L equal intervals
- Calculate each quantizer levels as midpoint of the corresponding interval

- Optimize the quantizer levels using the Lloyd-Max algorithm and then store them in the dictionary $\mathcal{D}$
- Then the squared error distortion is considered to quantize each sample according to

$$\hat{x}_i = \arg\min_{d \in \mathcal{D}}(x_i - d)^2, \qquad (5)$$

  where x_i is the sample to be quantized and $\hat{x}_i$ is the output.
- Codebook: mapping of $\hat{x}_i$ into bits using Gray code. Each Gray code corresponds to a quantized level in $\mathcal{D}$

B. Reconciliation

1) Reconciliation: The quantized vectors $\mathbf{q}_a(t)$ and $\mathbf{q_u}(t+1) \in \{0,1\}^{1 \times nN}$, fed into the input of the reconciliation, are mapped to the decoder outputs $\mathbf{r}_a(t)$ and $\mathbf{r}_u(t+1)$, where nN is the codelength. The principle of our reconciliation scheme is based a decoding process using the principle of Slepian-Wolf decoding as in [16], where $\mathbf{q}_a(t+1)$ is decoded using the side information (helper data) $\mathbf{S}$ derived from the code design and the quantized vector $\mathbf{q}_a(t)$ from the enrollment phase at time t. This approach ensures that the correlation between the CSI in both phases, is properly exploited. As a result, it is possible to distinguish Alice from Mallory. Specifically, when attempting to decode Mallory's CSI using the side information, the lack of correlation between their channels prevents Mallory's CSI from producing similar outputs. $\mathbf{q}_a(t)$ and $\mathbf{q}_a(t+1)$ are therefore considered as dithered versions of the same codeword. The aim here is to correct measurements errors in order to separate Alice from Mallory, i.e., although reconciliation will be successful for Alice, it will not be successful for Malory. Polar codes [16] are the family of error-correction codes examined in this letter for reconciliation. Thus, the scheme needs to be designed in such a way that the reconciliation gives (i) in the normal case, i.e., $\mathbf{q}_a(t)$ and $\mathbf{q}_a(t+1)$, identical or very close outputs, and (ii) in the spoofing case, i.e., $\mathbf{q}_a(t)$ and $\mathbf{q}_m(t+1)$, very different outputs. This also depends on the correlation coefficient and the noise variance.

2) Polar Codes: To enhance the performance of the polar code in finite blocklengths, $\mathbf{q}_u(t+1)$ is decoded using cyclic redundancy check (CRC) successive cancellation list decoding [14], [17] where the list size is denoted by L_s. During the decoding, Bob actually tracks L_s decoding paths simultaneous, where the decoder picks the most likely codeword which satisfies the CRC condition among the L_s paths. Therefore, Bob uses the side information $\mathbf{S}$ that contains the syndrome (frozen bits) and the CRC bits. The CRC assists the decoder in choosing the right decoding path from a list of possibilities. This syndrome is generated using the quantized vector $\mathbf{q}_a(t)$ and the reliability sequence used for the polar code construction. For the construction of the polar code, we use the recursive relation of the reliability sequence of a binary erasure channel (BEC), defined in [18].

3) Performance Metrics: Hypothesis testing is used to differentiate Alice from Mallory. Two hypothesis H_0 and H_1 corresponding respectively to the normal case (Alice) and the spoofing one (Mallory), are defined as follows:

$$\begin{cases} H_0 : \eta = \mathcal{H}_d(\mathbf{r}_a(t), \mathbf{r}_a(t+1)) \le \eta_{th} \\ H_1 : \eta = \mathcal{H}_d(\mathbf{r}_a(t), \mathbf{r}_m(t+1)) > \eta_{th} \end{cases} \qquad (6)$$

Algorithm 1 Multi-User Physical Layer Authentication

1: **Enrollment Phase:**
2: Initialization: N_b, β, U, α_i^a, α_i^m, $\forall\ i = 1, \dots U$, M, σ_z
3: Measure $\hat{\mathbf{h}}_a(t)$ and calculate $\mathbf{x}_a(t)$
4: Quantize $\mathbf{x}_a(t)$ to get $\mathbf{q}_a(t)$
5: Get $\mathbf{r}_a(t)$ (information bits) and frozen bits from $\mathbf{q}_a(t)$
6: **Authentication Phase:**
7: Measure $\hat{\mathbf{h}}_u(t+1)$ and calculate $\mathbf{x}_u(t+1)$, $u \in \{a, m\}$
8: Quantize $\mathbf{x}_u(t+1)$ to get $\mathbf{q}_u(t+1)$
9: Decode $\mathbf{q}_u(t+1)$ to get $\mathbf{r}_u(t+1)$
10: **Authentication Decision:**
11: Calculate $\eta = \mathcal{H}_d(\mathbf{r}_a(t), \mathbf{r}_u(t+1))$.
12: **if** $\eta \le \eta_{th}$ **then**
13:      Authenticate as Alice (Hypothesis H_0 is true)
14: **else**
15:      Identify as Mallory (Hypothesis H_1 is true)
16: **end if**

As in [10], a bitwise comparison between $\mathbf{r}_a(t)$ and $\mathbf{r}_u(t+1)$, $u \in \{a, m\}$, is a suitable choice for η. $\mathcal{H}_d(\cdot)$ is then the Hamming distance between $\mathbf{r}_a(t)$ and $\mathbf{r}_u(t+1)$ as (7).

$$\eta = \mathcal{H}_d(\mathbf{r}_a(t), \mathbf{r}_u(t+1)) = \sum_{j=1}^{K} \left| r_{a,j}(t) - r_{u,j}(t+1) \right| \quad (7)$$

The main steps of the proposed PLA scheme are summarized in Algorithm 1.

4) Algorithm Complexity: The time complexity of the enrollment phase is given by $O(N) + O(L) + O(L_s nN \log(nN))$. The time complexity of the authentication phase and the decision using hypothesis testing are respectively given by $O(UN) + O(L) + O(L_s nN \log(nN))$ and $O(K)$. L_s is the list size and K is the length of the reconciled vectors. The space complexity is the amount of memory required to perform the authentication process taking into account all steps of the scheme is given by $O(U) + O(L) + O(L_s nN)$.

IV. ANALYSIS

In this letter, the performance metrics are the probabilities of false alarm and of detection given respectively by $\mathrm{P_{FA}} = \mathrm{Pr}(\eta > \eta_{th} \mid H_0)$ and $\mathrm{P_D} = \mathrm{Pr}(\eta > \eta_{th} \mid H_1)$. Given the probability distribution of η, we can represent the receiver operating characteristic (ROC) curve. Based on the definition of η, 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., $\eta \sim \mathbb{B}(K, p_0)$.

$$P(\eta = k|H_0) = \binom{K}{k} p_0^k (1 - p_0)^{K-k}, \qquad (8)$$

where p_0 is the bit error probability during the decoding.

Proposition 2: Under H_1, η follows a binomial distribution of parameters K and p_1, i.e., $\eta \sim \mathbb{B}(K, p_1)$.

$$P(\eta = k|H_1) = \binom{K}{k} p_1^k (1 - p_1)^{K-k}, \qquad (9)$$

where p_1 is the bit error probability during the decoding.

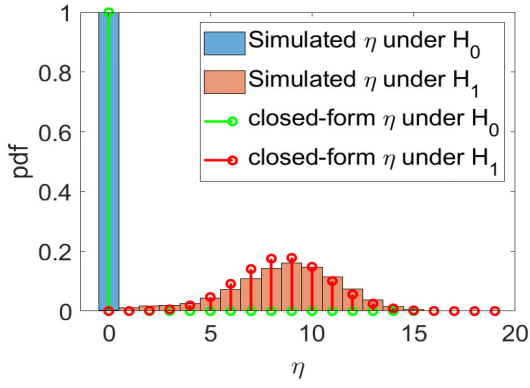See proofs of Proposition 1 and 2 in [10].

Fig. 3. Simulated vs closed-from expression: code rate $= 0.01$, $SNR = 10$ dB, $p_0 \approx 0$ and $p_1 \approx 0.4539$.

We compare the simulated probability distributions of η with the closed-form ones in the case of a 2-bit quantizer in Fig. 3. The closed-form expression almost matches the simulated result under both hypotheses. As can be seen, the reconciliation collapses the CSI observations of Alice to a single point probability mass function. As a result, the distance between the probability density function (PDF) of Alice's and Mallory's observations increases. Thus, despite the loss of precision due to the use of quantization, an enhancement of the PLA accuracy is achieved, as confirmed in the numerical results section.

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

$$P_{FA} = \sum_{k=\eta_{th}+1}^{K} \binom{K}{k} p_0^k (1-p_0)^{K-k} \tag{10}$$

and

$$P_D = \sum_{k=\eta_{th}+1}^{K} \binom{K}{k} p_1^k (1-p_1)^{K-k}. \tag{11}$$

V. NUMERICAL RESULTS

We compare here the proposed method with the prior ones proposed in [7], [8], and [9]. We first investigate the ROC curve which is P_D vs P_{FA} and the impact of the SNR on the probability of detection. Then, we provide the analysis of the other simulation setup parameters such as the correlation coefficient β, the interference weights α_i^a and α_i^m and the code rate. We also present the results of the proposed method for different codelengths, $nN = 1024$ and $nN = 2048$, which correspond to 1-bit ($n = 1$) and 2-bit ($n = 2$) quantizers, respectively.

Unless otherwise specified, the simulation parameters in this letter are considered as follow. The number of antennas at Bob $N_b = 32$, $\beta = 0.9$, $\sigma_h^2 = 1$, $M = 16$, $N = 1024$, the code rate is 0.01, $\alpha_i^a = \alpha_i^m = 0.01$, $\forall$ i and $P_{FA} = 10^{-3}$. This very small value of P_{FA} is chosen in order to match real-world communication systems in which low or very low false alarm probabilities are needed. The signal-to-noise ratio is defined as $SNR = \frac{\mathbb{E}[\mathbf{h}_a \mathbf{h}_a^H]}{N_b \sigma_z^2}$.

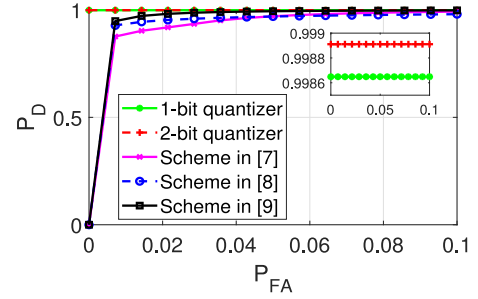Fig. 4 presents the ROC curve for a SNR of 5 dB. Our proposed method performs very well with a probability of

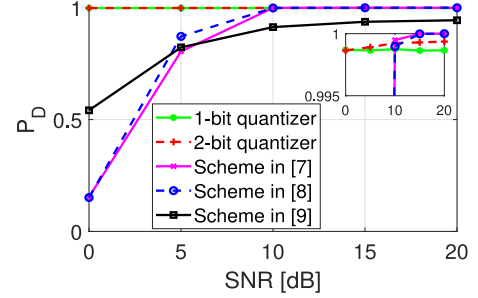
Fig. 4. ROC curve: $SNR = 5$ dB.
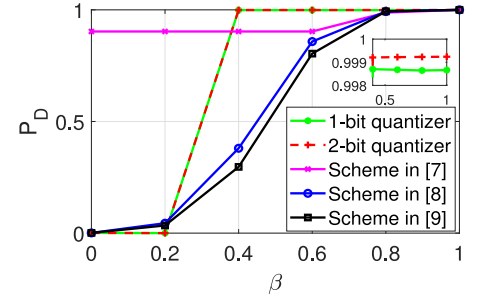

Fig. 5. P_D vs SNR: $P_{FA} = 10^{-3}$.

Fig. 6. P_D vs β: $SNR = 10$ dB, $P_{FA} = 10^{-3}$.

detection very close to 1 for very small probabilities of false alarm less that 0.1. It also performs better than the prior schemes. As shown in this figure, we get more than 99.80% increase in the detection probability even for false alarm probabilities very close to 0.

In Fig. 5, the impact of the SNR on the detection probability is studied. As the SNR increases, P_D increases as subsequent CSI measurements are more correlated due to decreased noise. The proposed scheme performs very well with a P_D greater than 99.86%. However the performance of the prior methods is poor for low SNRs less than 10 dB.

Fig. 6 shows the detection probability as a function of β. We have a P_D very close to 1 for $0.4 \leq \beta \leq 1$. We therefore have a very well performance even for poor scenarios of medium correlation coefficients. Thus, our proposed scheme performs better than the previous ones. We observe that the scheme in [7] is performing always good even for β less than 0.4. Actually, [7] proposed a two dimensional authentication scheme where the channel impulse response and the multipath delay are considered. This performance is due to the high correlations in the multipath delay dimension.
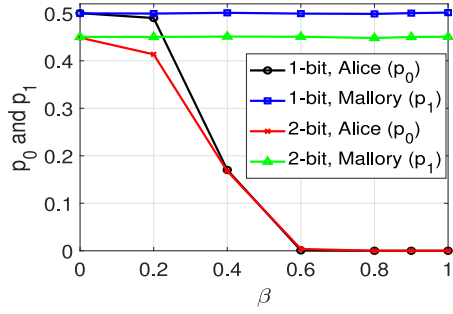
Fig. 7.   Error probabilities vs β: $SNR = 5$ dB.

TABLE I
DETECTION PROBABILITIES FOR DIFFERENT $\alpha^a = \alpha^m$

$\alpha^a = \alpha^m$	1-bit	2-bit	in [7]	in [8]	in [9]
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
2	0	0	0.90	0.005	0.04

TABLE II
DETECTION PROBABILITIES UNDER DIFFERENT CODE RATES

Code rate	0.01	0.1	0.2	0.3	0.4
1-bit	0.998	0	0	0	0
2-bit	0.999	0	0	0	0

Table I presents the behaviour of P_D for different values of $\alpha^a = \alpha^m$ 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 [8] and [9] 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 [7] has a good performance for weights above 1.6 because of the high correlation in the delays as mentioned before.

Error probabilities p_0 and p_1 mentioned in Section IV are evaluated in Fig. 7 for a false alarm of 10^{-3}. For both 1-bit and 2-bit quantizers, the normal case (H_0) is performing better than the spoofing case (H_1). This can be explained by the correlation between the channel measurements in the normal case.

An analysis of the code rate of the proposed scheme is shown in Table II for a SNR of 10 dB. We can see that the performance is almost perfect for a code rate of 0.01 and poor for values greater than 0.01. It can be improved for code rates greater than 0.01 by increasing the code length or designing an improved coding scheme.

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.

VI. CONCLUSION

In this letter, the problem of CSI-based PLA using information reconciliation has been investigated. An information reconciliation scheme using Polar codes along with a quantization strategy that employs an arbitrary number of bits has been developed for a multiuser communication scenario. CSI measurements from a legitimate user spread in time are reconciled using reconciliation decoders implemented using Polar codes. Simulation results have shown that our approach performs excellently well in the presence of multiple users and outperforms state-of-the art schemes.

REFERENCES

[1] Z. Lin, M. Lin, T. de Cola, J.-B. Wang, W.-P. Zhu, and J. Cheng, "Supporting IoT with rate-splitting multiple access in satellite and aerial-integrated networks," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11123–11134, Jul. 2021.

[2] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, *Physical Layer Security: Authentication, Integrity, and Confidentiality.*, K. N. Le, Ed. Cham, Switzerland: Springer, 2021.

[3] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6G security," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 375–388, 2023.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[5] X. Lu and R. C. de Lamare, "Opportunistic relaying and jamming based on secrecy-rate maximization for multiuser buffer-aided relay systems," in *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15269–15283, Dec. 2020.

[6] Y. Shi, X. Lu, K. An, Y. Li, and G. Zheng, "Efficient index-modulation-based FHSS: A unified anti-jamming perspective," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 3458–3472, Jul. 2023.

[7] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.

[8] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2356–2366, 2021.

[9] X. Lu, J. Lei, Y. Shi, and W. Li, "Physical-layer authentication based on channel phase responses for multi-carriers transmission," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1734–1748, 2023.

[10] A. K. A. Passah, R. C. de Lamare, and A. Chorti, "Physical layer authentication using information reconciliation," in *Proc. IEEE 99th Veh. Technol. Conf. (VTC-Spring)*, Singapore, 2024, pp. 1–5.

[11] T. M. Pham, L. Senigagliesi, M. Baldi, G. P. Fettweis, and A. Chorti, "Machine learning-based robust physical layer authentication using angle of arrival estimation," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Kuala Lampur, Malaysia, Dec. 2023, pp. 13–18.

[12] W. C. Jakes, *Microwave Mobile Communications*. New York, NY, USA: Wiley-IEEE Press, 1994.

[13] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[14] M. Shakiba-Herfeh and A. Chorti, "comparison of short block-length Slepian-Wolf coding for key reconciliation," in *Proc. IEEE Stat. Signal Process. Workshop (SSP)*, Rio de Janeiro, Brazil, 2021, pp. 111–115.

[15] H. N. Qureshi, I. H. Naqvi, and M. Uppal, "Massive MIMO with quasi orthogonal pilots: A flexible solution for TDD systems," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Toronto, ON, Canada, 2017, pp. 1–6.

[16] E. Arikan, "Source polarization," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, 2010, pp. 899–903.

[17] I. Tal and A. Vardy, "List decoding of polar codes," in *Proc. IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, 2011, pp. 1–5.

[18] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.