IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 23, 2022, accepted June 13, 2022, date of publication June 17, 2022, date of current version June 24, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3184038

Channel Impulse Response Multilevel Quantization for Power Line Communications

JAVIER HERNANDEZ FERNANDEZ[1,2], AYMEN OMRI[2], AND ROBERTO DI PIETRO[1], (Senior Member, IEEE)

[1]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar
[2]Iberdrola Innovation Middle East, Doha, Qatar

Corresponding author: Javier Hernandez Fernandez (jfernandez@hbku.edu.qa)

This work was supported by the Qatar National Library (QNL)—a part of Qatar Foundation (QF).

ABSTRACT Physical layer security (PLS) has become a popular topic in the research community as a complement to traditional security schemes. Particularly, by taking advantage of the channel's symmetry, a robust ecosystem of security applications has developed in wireless communications. However, in power line communications (PLC), the general lack of channel symmetry has limited and hampered the development of physical layer techniques. In this paper, we address the cited constraint, by deriving a symmetric virtual channel impulse response (CIR) from the corresponding asymmetric PLC channel state information (CSI). In view of this, we propose a low-complexity and, to the best of our knowledge, the first CIR multilevel quantization algorithm that can be used in various PLC applications. While we contextualize our solution within the PLS domain, it has a wide applicability. Specifically, we start by analyzing the PLC channel path delays reciprocity, its relationship with topology changes, and its independence from all other power line characteristics. Then, the quality and viability of the proposed scheme are quantified, by comparing the bit mismatch rate (BMR) with its one-level quantization counterpart. The simulation results, under different topologies, confirm the performance of the proposed approach that can reduce the BMR by at least three orders of magnitude with respect to the one-level quantization, for noise levels below 90 dBuV. Finally, we conclude the paper by showing a few applications of the proposed solution and highlighting some future research directions.

INDEX TERMS Channel impulse response (CIR), power line communications (PLC), quantization, reconciliation, smart grid, security.

I. INTRODUCTION

Smart grids require contributions from several disciplines that, when coupled with their unique requirements in terms of reliability and performance, complicate an already intricate scenario The electric network spreads out, covering vast and diverse areas ranging from highly populated cities to remote rural locations [1]. Except for primary substations, the rest of the infrastructure has limited physical security and constitutes a vulnerable access point [2]. In distribution transformer stations, regardless of the type, access to the equipment that operates the grid is usually only protected by a simple lock on a cabinet. Other network components, such as overhead lines and smart meters, are easily accessible, becoming an easy target for malicious users who can tamper with them. In-home or in-building wiring is susceptible to the same above introduced problem, sporting numerous accessible lines and unsupervised outlets.

The number of installed PLC devices has grown exponentially in the past years [3]–[5]. In addition to the traditional uses of PLC in home area networks and building automation, new applications, particularly those related to power utilities' distribution networks, have extensively leveraged this technology for their smart grid deployments [6]. In the European Union alone, 99+ million electrical smart meters were already installed in 2018, and the number is set to reach 220+ millions by 2024 [3], [4]. Many of those deployments use PLC as the primary communication technology [7], [8].

Current PLC technologies are classified based on the used frequency band: broadband PLC (BB-PLC), using the frequency range from 1.8 MHz to 250 MHz, and narrowband PLC (NB-PLC), operating from 3 kHz to 500 kHz [9]. Some

The associate editor coordinating the review of this manuscript and approving it for publication was Cristian Zambelli.

of the most recent and used PLC standards include PRIME, G3-PLC, G.hnem for NB-PLC, and G.hn or HomePlug AV2 for BB-PLC [10]. Regardless of the final application, all the cited protocols share two distinct techniques:

1) Orthogonal frequency division multiplexing (OFDM) is used as an efficient multiplexing technique. The use of OFDM is not unique to PLC as OFDM-based standards can be found in many wired (DSL) and wireless (WiMAX, 4G) communication protocols [11]–[13], including the 5G mobile standard [14]. Its wide adoption can be explained by its capacity to achieve high data rates, spectral efficiency, and robustness to interference [11].
2) The security of communications is based on the same mechanisms, public key infrastructure (PKI) and the symmetric key-based advanced encryption standard (AES) block cipher [9].

OFDM has been recommended as a powerful solution to reduce the negative frequency selective channel effects on both PLC and wireless mediums [11]–[13]. However, the broadcasting nature of the signal propagation makes both media prone to eavesdropping and opens to identity-based attacks, even with the deployment of traditional cryptograpic security techniques [15], [16]. In this context, physical layer security (PLS) has been proposed and deployed as an efficient security technique that ensures perfect secrecy data transmission between legitimate network nodes, giving malicious nodes no information. It aims at exploiting the randomness inherent in the channel physical properties, such as the channel state information (CSI) and the received signal strength (RSS) to provide an additional level of protection and high secrecy rate at the physical layer of both PLC and wireless communications [17]–[19]. Secrecy rate/capacity defines the secure transmission rate between legitimate nodes without leakage of information to an eavesdropper. Mathematically speaking, the secrecy rate can be expressed as follows:

$$SR = EC_L - EC_E, \tag{1}$$

where, EC_L and EC_E represent the ergodic capacities of the legitimate and eavesdropper channels, respectively [20], [21]. According to Shannon theorem, the general ergodic capacity expression is given by:

$$EC = \log_2(1 + SNR), \tag{2}$$

where, SNR represents the signal to noise ratio of the corresponding channel.

A. CONTRIBUTIONS

In this paper, we propose a novel CIR-based multilevel quantization scheme for PLC.

More specifically, we first provide a detailed characterization of the PLC channel model for path delays, followed by a comprehensive explanation of the algorithm. Among other possible benefits, the proposed method reduces the bit mismatch rate (BMR) in the information reconciliation stage, facilitating the adoption of physical layer techniques on PLC devices. We analyze our solution via an extensive simulation campaign run on a specific PLS problem, showing the quality and viability of the proposal. Finally, further research directions are highlighted in the conclusion.

B. PAPER ORGANIZATION

This paper is organized as follows. Section II reviews the existing related work on PLS in PLC. Section III details the channel model to confirm the symmetry in path delays. Section IV describes the proposed multilevel quantization scheme and the associated reconciliation stage. Numerical results drawn from several simulated scenarios are discussed in Section V. Finally, Section VI concludes this work.

II. RELATED WORK

Physical layer-based techniques have been presented as promising solutions for various communication problems. In wireless communications, for instance, challenges such as synchronization, security, interference management, or cognitive radio have found creative solutions in physical layer techniques [14], [22]–[25]. As previously stated, we have been focusing on PLS as a case study of our contribution. Accordingly, the following sub-section discusses relevant PLS research works in the literature.

Compared to PLS-based wireless communications, where many schemes and survey studies are available [26]–[32], PLS research attempts in PLC are rare and have been mainly focusing on power line channel characteristics analysis [17], [33], and certain related PLS approaches [17], [18], [34]–[38].

The authors in [17], [33], have analyzed the PLC characteristics in terms of reciprocity and symmetry to verify whether physical layer key generation can be efficiently implemented. In the PLC multi-path channel characterization has been presented and detailed. In view of this, a multi-path channel delay detection technique has been introduced to provide an accurate physical layer identification for the considered PLC links.

A recent work [17] has proposed two key-generation techniques, the first one is based on the channel path delays, and the second one uses the estimated transmission matrix. In [18], a PLS key generation technique has been proposed for PLC systems. It consists of a transfer characteristic amplitude quantization in log domain and a mapping to bit patterns with Gray coding. A key-generation scheme based on the shared patterns of noise observed in electrical circuits has been presented in [34]. By exploiting spatiotemporal randomness, devices can establish initial trust based on their unique contextual information. A similar concept, based, however, on the fast Fourier transform (FFT) analysis of the voltage rather than the amplitudes of the harmonics, has been proposed in [35]. The authors of [36] have showed that with dedicated coupling and by adapting to the characteristic impedance, the transfer functions of an in-home PLC can show symmetries

useful for key-generation purposes. Building on previous work, another study [37] has explored the randomization of the channel by terminating open paths (electrical sockets) with random loads. In [38], the authors have introduced a PLS solution for in-band full-duplex (IBFD) PLC systems with multiple inputs and outputs (MIMO). IBFD enables PLC receivers to jam the operational frequency spectrum while receiving the intended data packets. Several studies [39]–[43] have investigated the secrecy rate of PLC fading channels and concluded that it is lower than the one offered by wireless networks, mainly due to the keyhole effect produced by the branching of the electrical wiring topology.

In the remaining of this section, we report some works from the literature that dealt with relevant aspects of security and PLC. The authors of [44] have taken advantage of the communication latency between smart meters and the data concentrator in PLC to adapt the timed efficient stream loss-tolerant authentication (TESLA) scheme to PLC. A user authentication protocol for PLC-based internet applications, using second channel and location data, has been proposed in [45]. The authors of [46] and [47] have proposed an application-layer key-generation process and an identity-based cryptography system to deal with bandwidth limitations of PLC. In [48], a full-duplex PLC security method based on the power ratio between signal and introduced artificial noise has been described, assuming the wiretapper can perform optimal detection. Several studies have investigated and leveraged the benefits of a hybrid PLC and radio frequency (RF) solution for physical security purposes [49], [50]. A scheme to prevent availability attacks and communication impairments due to impulsive noise has been presented in [51]. The method combines the information dispersal algorithm (IDA) and the channel's physical characteristics to achieve a low overhead solution valid for PLC and PLC/RF hybrid systems. Availability in PLC channels has been studied in [52], where the probability of successful communications is calculated based on attenuation parameters and noise levels. To capture the variations between the different days (weekdays/weekends) and periods (night/day), noise measurements were taken continuously for an entire week in a total of 16 locations. The recorded data has been used in [53] to propose two channel-selection schemes to improve network coverage. Long-term trends of noise have been statistically analyzed for stationarity, autocorrelation, and independence in [54]. Finally, authors of [55] have proposed a machine learning-based IDS system that uses the CSI as input to detect intrusions.

For a holistic view of cybersecurity in PLC, we refer the reader to [9].

III. PLC CHANNEL MODEL

This section investigates the correlation between the PLC environment/topology and the channel parameters to confirm the PLC channel symmetry dependency on path delays. The investigation is based on the two main PLC channel modeling techniques, deterministic and empirical, which are used in the literature for low voltage power distribution grids [56]–[59]. Prior to presenting these two models, we will discuss the reciprocity features of PLC channels.

A. PLC CHANNEL RECIPROCITY

The CSI and the RSSs at the transmitters and their receivers are highly correlated in wireless communications [29], [60], whereas PLC differs considerably due to the impedance imbalance. Furthermore, while wireless devices are set to operate at 50 Ohms by default, traditional PLC transmitters and receivers are configured to enhance the transferred voltage, resulting in a lack of reciprocity [17]. In terms of the path delay, however, the CIR is positively linked for both communication systems [17], [29], without a significant correlation to impedance.

B. DETERMINISTIC MODELING APPROACH

This approach is based on the transmission line (TL) theory, which requires to obtain the two-port network-based ABCD matrix that describes the relationship between input and output voltages and currents [57], [58]. This relationship can be presented as follows:

$$H = \begin{bmatrix} V_1 \\ I_1 \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} V_2 \\ I_2 \end{bmatrix}, \tag{3}$$

where V_1, I_1, V_2 and I_2 are input (voltage and current) and the output (voltage and current) is given by $A = D = \cosh(\gamma l)$, $B = Z_C \sinh(\gamma l)$, $C = \sinh(\gamma l)/Z_C$, where l is the length of the considered conductor, and γ represents the propagation constant, which is expressed as follows [57], [58]:

$$\gamma = \sqrt{(R + j\omega L)(G + j\omega C)}, \tag{4}$$

where, R, L, C and G are the PL parameters, and ω is the angular frequency.

Accordingly, the TL theory based transfer function is given by

$$H = 20 \log_{10} \left(\frac{Z_L}{A\, Z_L + B + C\, Z_L\, Z_S + D\, Z_S} \right), \tag{5}$$

where, Z_S and Z_L represent the source and load impedance.

The deterministic modeling approach requires extensive knowledge of the installed transmission lines and power network parameters, hence sporting a high degree of complexity and limited viability.

C. EMPIRICAL MODELING APPROACH

The empirical modeling approach is a time-domain based modeling proposed by Zimmerman in [59]. It is a statistical modeling based on the multipath nature of the power line channel—this latter one arising from the presence of several branches and impedance mismatches that cause multiple reflections. According to this model, the PLC CIR is expressed as follows [56], [59]:

$$h(t) = \sum_{i=0}^{N-1} k_i\, \delta(t - \tau_i), \tag{6}$$

where, N is the number of the significant (non-negligible) paths, and k_i and τ_i denote the attenuation coefficient and the delay of the i-th path, respectively. This channel model can be implemented using an N-tap finite impulse response (FIR) filter. The first delay τ_0 indicates the 'natural' propagation delay of the main or direct path and k_0 is the corresponding attenuation. All following taps of the filter are associated with echoes.

In the remainder of this section, we describe the corresponding CFR to confirm that the multipath delays (τ_i), do not pivot on the power line characteristics, while depending exclusively on the power line (PL) network topology existing between a given transmitter and receiver.

Accordingly, the corresponding CFR of this model is given by evaluating the Fourier transform of (6), as follows:

$$H(f) = \sum_{i=1}^{N} k_i \ \exp\left(-j2\pi f \tau_i\right), \tag{7}$$

where, f is the carrier frequency.

Under real-world conditions, the coefficients k_i depend on the cable length and frequency. Evaluating a measurement database of numerous different power line channels has led to the following expression ([56], [59]) for the attenuation coefficients of echoes:

$$k_i = g_i \ \exp\left(-\alpha(f)\, l_i\right), \tag{8}$$

where, $\alpha(f)$ denotes the frequency-dependent attenuation coefficient, l_i presents the respective cable length (length of path index i), and g_i denotes certain weight factors, which include details of the network topology. In fact, g_i can be considered the product of reflection and transmission coefficients in the course of the path with index i. Summing up the effects of multipath propagation as well as frequency- and length-dependent attenuation, we obtain the complete transfer function:

$$H(f) = \sum_{i=0}^{N-1} g_i \ \exp\left(-\alpha(f)\, l_i\right) \ \exp\left(-j2\pi f \tau_i\right). \tag{9}$$

By examining and evaluating the attenuation factor $\alpha(f)$ for various types of power lines in detail, we obtain [59]

$$\alpha(f) = \frac{R'}{2Z_0} = a_0 + a_1 f^{a_2}, \tag{10}$$

where, R' is the resistance per length, Z_0 is the characteristic impedance of the power line, a_0, a_1, and a_2 are PL propagation parameters that depend on the impedance and the PL characteristics [56], [59]. Consequently, the empirical modeling-based expression of the PLC CFR is given by:

$$H(f) = \sum_{i=0}^{N-1} g_i \ \exp\left(- \left[a_0 + a_1 f^{a_2} + j \ \frac{2\pi f}{v_p} \right] l_i \right), \tag{11}$$

where, $v_p = \frac{l_i}{\tau_i}$.

From the above expression, it is worth noting that the PL impedances and characteristics affect the path gain k_i exclusively, and that the path delays depend only on the path lengths related to the PL topology only.

This empirical modeling approach has been verified in numerous applications, exhibiting good agreement with corresponding measurements [56]. In practice, it turns out that this model is not a good choice for providing exact agreement with certain individual links. At the same time, it delivers a quite accurate description of the overall system on a statistical basis.

IV. DESCRIPTION OF THE PROPOSED MULTILEVEL QUANTIZATION SCHEME

This section details the steps of our multilevel quantization scheme, from the channel probing to the reconciliation process that will mitigate mismatches produced by channel estimation errors.

To show the viability of the proposed solution, we have performed a simulation of a given CFR based on (11) and a power delay profile presented in [56]. Without loss of generality, the used simulation parameters are: sampling time $T_S = 0.05\ \mu$s, FFT number $N_{FFT} = 128$, $a_0 = 0$, $a_1 = 7.8 \times 10^{-10}\ \mathrm{m}^{-1}$, $a_2 = 0.5$ [56], $v_p = 0.6 \times 3\ 10^8\ \mathrm{m\ s}^{-1}$, maximum key length $K_{len} = 64$, and $L1 = 0.2$. These parameters are used to generate the CFR ($A \rightarrow B$) and ($B \rightarrow A$) links. To create certain channel asymmetries, a slight adjustment to the g_i coefficients has been made for the link ($B \rightarrow A$), by adding random numbers to the different coefficients g_i following a normal distribution with a mean of 0 and variance of 0.001.

A. CHANNEL PROBING

Channel probing consists of estimating the CIRs of the links between the two communicating nodes. This estimation can be done by performing two processes sequentially. First, the CFR is estimated using predefined pilots and interpolation methods or similar estimation techniques. The CFR is then converted into the CIR by using the inverse discrete Fourier transform (IDFT).

B. QUANTIZATION

As discussed in previous sections, the PLC channel is asymmetric, except for the reciprocity shown by channel path delays. Therefore, employing a direct multilevel quantization on the CIR will not generate symmetric keys at both sides, since the amplitudes of the peaks will differ. The cited limitation has prevented—so far—the use of multilevel quantization techniques and the advantages associated with them. In this work, we have tackled the cited constraint by converting the asymmetric CIR to a symmetric virtual CIR. Subsequently, we perform a multilevel quantization, using our proposed Algorithm 1. The outcome generates a unique key shared between the two communicating devices. The key generation process takes a set of five parameters as input:

- The estimated CIR, *CIRe*.
- The key length, k_{Len}.

- One level quantization threshold $L1$, that is a parameter based on the average floor noise level—to avoid detecting false CIR peak.
- The multilevel quantization thresholds, $L-$ and $L+$, initialized to $+1$ and -1, respectively; and,
- The multilevel quantization step α.

In detail, the proposed multilevel quantization Algorithm 1 consists of three main steps:

1) The first step is a simple single-level quantization of the estimated CIR, needed to generate an initial key $k0$ of length k_{Len}.
2) In the second step, the virtual CIR (VCIR) is generated, by dividing the vector $k0$ into $Part1$ and $Part2$. These two parts are then provided as input to Table 1, iterating through each position to obtain a final key, our VCIR, composed by half of the elements of the initial key $k0$.
3) The VCIR quantization is carried out in the third and final step. The algorithm scans the *VCIR* sequence to detect which samples n cross or equal the thresholds $L-$ and $L+$. This step is repeated, with an adjustment in the upper and lower levels, until the generated key length equals $k_{Len}/2$ or $L- = L+$. During this process, each peak detection is added to a position vector, and its level used to generate a key by converting it to the corresponding one or zero.

TABLE 1. The virtual CIR generation table for $n \in \{1, 2, \ldots, k_{Len}/2\}$.

Part1(n)	Part2(n)	$VCIR(n)$
1	1	1
1	0	-1
0	1	-0.5 if $VCIR(n-1) \leq 0$
		$+0.5$ if $VCIR(n-1) > 0$
0	0	0

Fig. 1 is a walk-though example for the above-mentioned three steps. To ease exposition, we chose a short key of 32 bits and four quantization levels.

Algorithm 1 Multilevel Quantization Algorithm

Inputs: Key Length: k_{Len}.
CIR Estimates: $CIRe$.
One level Quantization Threshold: $L1$.
Multilevel Quantization Thresholds:
$L- = -1$ and $L+ = +1$.
Multilevel Quantization Step: α.
$m = 1$.
Step 1: $CIRe$ **Magnitude One level Quantization**:
for n **from** 1 **to** k_{Len} **do**
  if ($|CIRe(n)| \leq L1$) **then**
    $k0(n) = 1$
  else
    $k0(n) = 0$
  end if
end for
Step 2: Virtual CIR (VCIR) Generation:
$Part1 = k0(1 : k_{Len}/2)$
$Part2 = k0(k_{Len}/2 + 1 : k_{Len})$
Generating the *VCIR*, according to Table 1.
Step 3: VCIR Multilevel Quantization
while ($m < k_{Len}/2$) and ($L+ \neq L-$) **do**
  for n **from** 1 **to** $k_{Len}/2$ **do**
    if ($VCIR(n) \geq L+$) **then**
      $key(m) = 1$
      $Pos(m) = n$
      $m = m + 1$
    end if
    if ($VCIR(n) \leq L-$) **then**
      $key(m) = 0$
      $Pos(m) = n$
      $m = m + 1$
    end if
  end for
  $L+ = (L+) - \alpha$
  $L- = (L-) + \alpha$
end while

C. RECONCILIATION

After generating the keys and the corresponding position vectors for both links, $(A \rightarrow B)$ and $(B \rightarrow A)$, reconciliation methods can be used to guarantee that the two keys key_{A-B} and key_{B-A} are the same. In this case, we have applied a reconciliation technique used in wireless communication and presented in [61]. In this method, node A sends the position vector Pos_{B-A} to B. Subsequently, B compares this vector with the one that it has locally computed to find the agreement bits and generate an updated position vector that will be sent back to A. A and B then locally updated the key based on the position vector, eventually generating a shared key.

To better explain the exposed peak position-based technique, we generated a simple scenario covering the three possible cases that could occur during the reconciliation. A PLC simulator was built to generate the CIRs, and calculate the corresponding VCIRs for different topologies and network parameters. Details about the simulator are presented in the subsequent section, including the numerical results and discussion. The scenario, based on the VCIR presented in Fig. 2, outputs the following initial keys and position vectors for the links $(A \rightarrow B)$ and $(B \rightarrow A)$:

Key_{A-B}
$= [01100101010010110000001001101000000000$
$00010010]$

Pos_{A-B}
$= [12\ 21\ 24\ 26\ 30\ 33\ 35\ 36\ 38\ 39\ 42\ 44\ 45\ 46\ 47$
$48\ 50\ 51\ 53\ 54\ 55\ 56\ 57\ 58\ 59\ 60\ 62\ 63\ 1\ \ 3$
$4\ \ 6\ 7\ 8\ 9\ 11\ 13\ 15\ 16\ 18\ 19\ 22\ 27\ 29\ 37\ 41]$

Key_{B-A}
$= [01100101011010110000001001101000000000000010]$

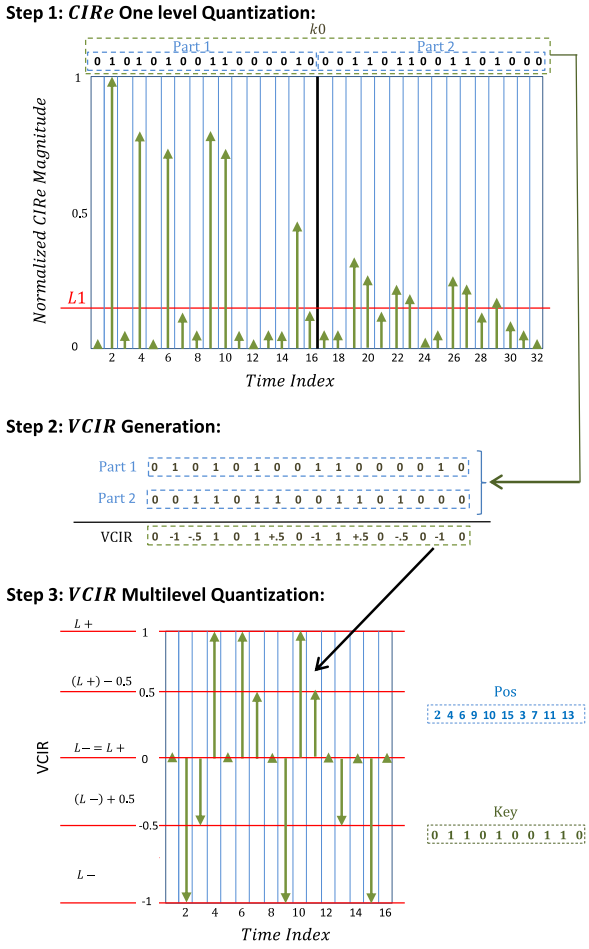


FIGURE 1. Output examples of Algorithm 1 Steps, with $k_{Len} = 32$, $L1 = 0.2$, $\alpha = 0.5$.

$$Pos_{B-A} = [12\ 21\ 24\ 26\ 30\ 33\ 35\ 36\ 38\ 39\ 42\ 44\ 45\ 46\ 47\ 48\ 50\ 51\ 53\ 54\ 55\ 56\ 57\ 58\ 59\ 60\ 62\ 63\ 1\ 3\ 4\ 6\ 7\ 8\ 9\ 11\ 13\ 15\ 16\ 19\ 27\ 29\ 37\ 41]$$

As shown in the above vectors, some peaks are not present on both sides—for example, peaks 18 and 22 (in red). The latter ones should be discarded when generating the final key. Accordingly, the updated keys after the position vectors have been shared are as follows:

$$Key_{A-B} = [01100101010010110000001001101000000000000010]$$
$$Key_{B-A} = [01100101011010110000001001101000000000000010]$$

Even with this signaling procedure, A and B could detect two peaks at the same position with different levels. For instance, the detected peak at position 42 (reported in blue), would result in a bit mismatch of the two keys. For these cases, some techniques, such as the one in [61] can be used,

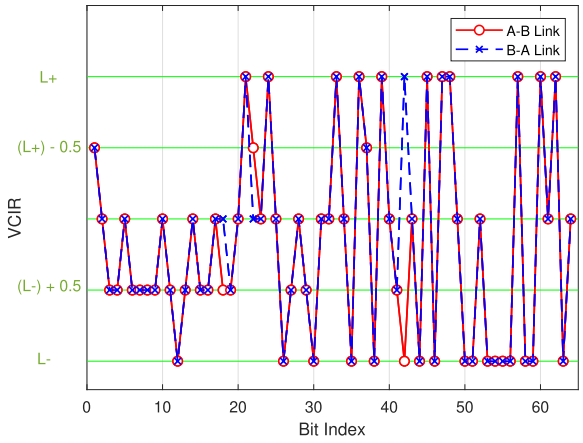


FIGURE 2. Virtual channel impulse response variations.

where A should generate a random number R, encrypt it with its new key, and send a message to B. Then, B should decrypt the received message, perform an arithmetic addition of one, and encrypt the result. The new key is then sent back to A. Finally, A will try to decrypt the received message. If the result is equal to $R + 1$, then A will send a key agreement acknowledgment to B. Otherwise, the key is discarded, and the key generation process is restarted.

V. NUMERICAL RESULTS AND DISCUSSION

This section analyzes the uniqueness and reciprocity of the outcome generated by our proposed quantization scheme under different simulated scenarios. Lastly, the benefits derived from being able to perform a reconciliation mechanism are presented.

A. SIMULATION SETUP

To evaluate the proposed scheme performance, we have developed a simulator that consists of the following main functions:

1) TOPOLOGY SIMULATION

Building a unique statistical model that would represent all possible topology configurations is a complex endeavor out of the scope of this paper. Therefore, we focus on three topologies, covering the most common medium and low voltage scenarios: bus, tree, and star topology. The star topology is intended to analyze direct and clean connections without discontinuities. The bus and tree topologies characterize the typical distribution networks, where secondary lines connecting end nodes are attached to the main cable.

For each topology simulation, we have been considering the transmission distances, discontinuities, branches, number of nodes, and cable joins that affect the channel path delays. In addition, the channel path delays can be altered during the channel estimation phase when trying to distinguish between signal and noise.

Our simulator is based on the PLC time-domain model introduced in [56] to generate the corresponding path delays and gains. As any signal will bounce and fork at any discontinuity, terminal node, or branch, a virtually infinite number of secondary paths are generated for every communication. Therefore, this function will yield a number of arriving paths between two given endpoints for each topology to account for this phenomenon.

To further explain this function, one can consider an example of a simple T scenario, with end nodes A, B, D, and C as the middle node connecting all the nodes. We denoted L_{XY} as the general distance between two given nodes X and Y, α, as the propagation attenuation coefficient per PL length unit, ρ_X as the reflection attenuation coefficient at node X, and δ_X as the discontinuity attenuation coefficient at node X. By considering the different attenuations above, the length of the first path ($A \rightarrow C \rightarrow B$) is equal to

$$l_1 = L_{AC} + L_{CB} = L_{AB}, \tag{12}$$

and, the corresponding path gain is

$$g_1 = (1 - \alpha L_{AC})\,(1 - \alpha L_{CB})\,(1 - \delta_C). \tag{13}$$

For the second path ($A \rightarrow C \rightarrow D \rightarrow C \rightarrow B$), the path length and the gain are given, respectively, by

$$l_2 = L_{AC} + 2\,L_{CD} + L_{CB}, \tag{14}$$

and,

$$g_2 = (1 - \alpha L_{AC})(1 - \alpha L_{CD})^2 (1 - \alpha L_{CB})(1 - \rho_D)(1 - \delta_C)^2 \tag{15}$$

During a predefined channel probing period, all the arriving paths are evaluated, by computing the path delays and gains. Then, the corresponding perfect CFRs are generated. Based on that, the different CFRs are estimated using the least-squares estimation method, where the channel estimation error is inversely proportional to the corresponding link's instantaneous complex noise value. Finally, the estimated CIRs of the different links are evaluated, by converting the CFR estimates to the time domain.

It is worth mentioning that, as the sampling rate is directly related to the multipath detection accuracy, the sampling frequency should be adapted to the topology to avoid saturation. Dense topologies with many paths, discontinuities, short distances, or low attenuation factors, will be more prone to capture paths for each sampling time.

2) VCIR GENERATION

The VCIR generation function uses the output of the topology simulation function to evaluate the two ways that VCIRs are generated between every two endpoints following the instructions detailed in Steps 2 and 3 of Algorithm 1.

3) RECONCILIATION

This function takes the position vector and key as an input and performs the reconciliation process as detailed in subsection IV-C.

4) BIT MISMATCH RATE (BMR) Evaluation

In this work, the BMR is defined as the ratio of the number of bits that do not match between the uplink and downlink IDs of a given communication link to the ID length. This metric has been used to evaluate the reciprocity of the proposed scheme, when compared to that of the single-level quantization scheme.

5) CORRELATION CALCULATION

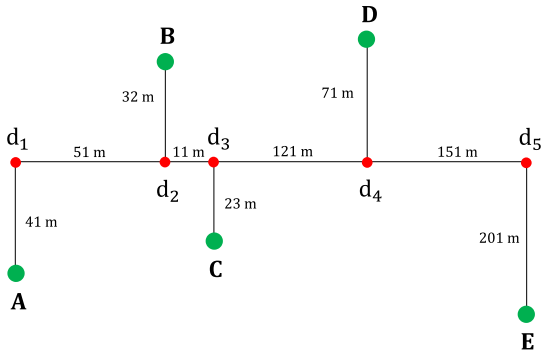
In this step, the correlation coefficients between the generated ID of a given link an all other links are computed. This metric is used to evaluate the independence between the different link IDs, which presents a crucial condition for different PLS applications, such as key generation and link identification.

6) SECRECY OUTAGE PROBABILITY (SOP)

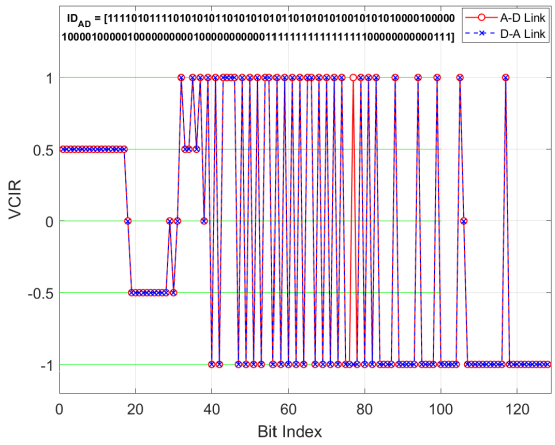
This metric investigates the SOP of the topologies presented in Figs. 3, 4, and 5. For each topology, and without loss of generality, an adversary model can be created by selecting two given nodes to be the legitimate transmitter and receiver, and any of the other nodes to be an eavesdropper. By using the SOP metric, the security level of the legitimate communication can be measured. Indeed, the SOP of a given communication link is defined as the probability of having a secrecy capacity that is less than a predefined target secrecy rate. The secrecy capacity is the difference between the instantaneous ergodic capacities of the legitimate channel (EC_L) and that of the eavesdropper channel (EC_I). Accordingly, the SOP is the probability of the event when ($EC_L - EC_I$) is less than a predefined target secrecy rate, denoted by SR_{Th}. By using the output of the proposed CIR multilevel quantization-based scheme as a transmission key, and once the legitimate nodes agree on it, the secrecy rate increases significantly. Specifically, when the eavesdropper is unable to detect the same key, which is the case when the keys at the endpoints are decorrelated. In other words, the SOP converges to zero, when the correlation between the legitimate and eavesdropper keys goes to zero.

Under imperfect channel conditions, the CIR observations are estimated but not error-free. Channel probing is subject to Gaussian and impulsive noises that will affect the reciprocity of the outcome of the quantization scheme by adding or removing some impulses. Simulations have been computed to account for this phenomenon, adding different noise levels and accounting for different instantaneous complex noise values at the nodes. The script has been designed to iterate for a given number of iterations, N_{max}, for each given noise power value, recording the resulting BMR and correlation coefficients. The values were then averaged for each noise power level, to generate the presented simulation results.

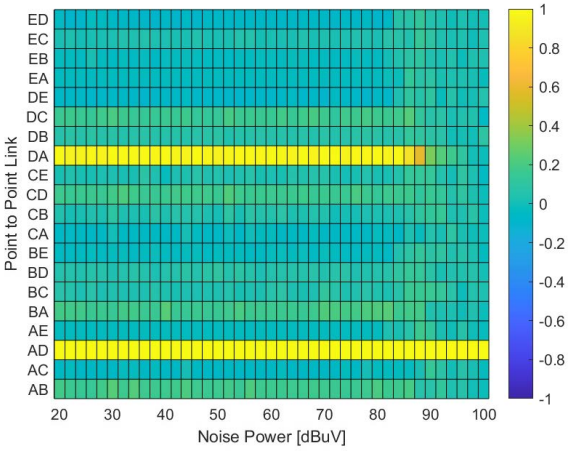
Accordingly, and without loss of generality, the used simulation parameters were set as follows: $N_{max} = 10^6$, the average noise power ranged from 20 dBuV to 100 dBuV in steps of 2 dBuV [54], the sampling time was equal to $T_s = 0.05$ us, and the quantization level set to $L1 = 0.02$. The



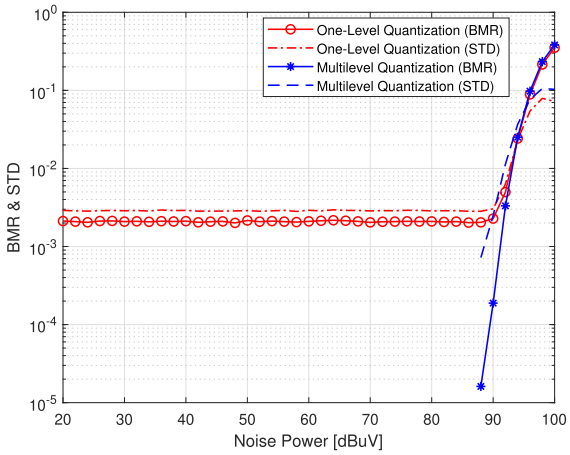
(a) Bus topology scenario



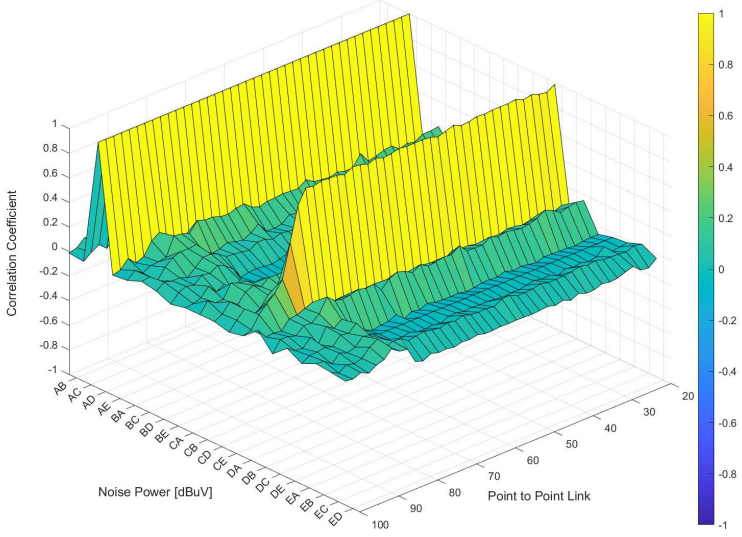
(b) The VCIR of $(A \leftrightarrow D)$ links and its generated ID/Key



(c) The correlation coefficients between the $(A \rightarrow D)$ link ID and the different link IDs

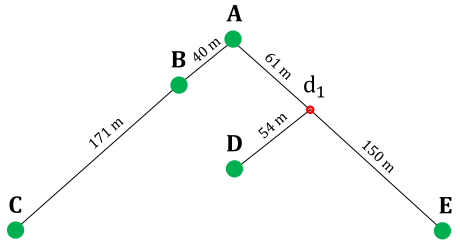


(d) BMR result after applying reconciliation techniques on $(A \leftrightarrow D)$ when compared with single-level quantization

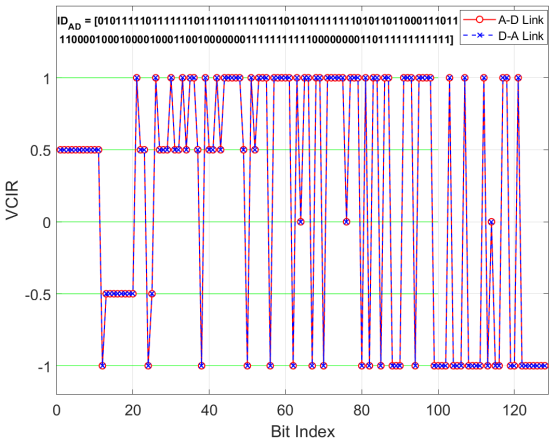


(e) 3D Projection of the correlation coefficients matrix in (c)

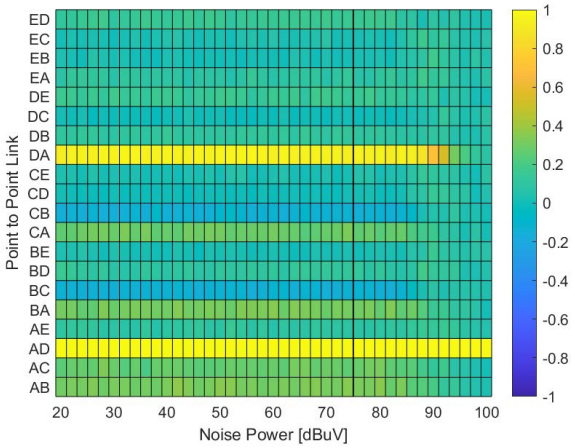
FIGURE 3. **Bus topology scenario simulation results.**



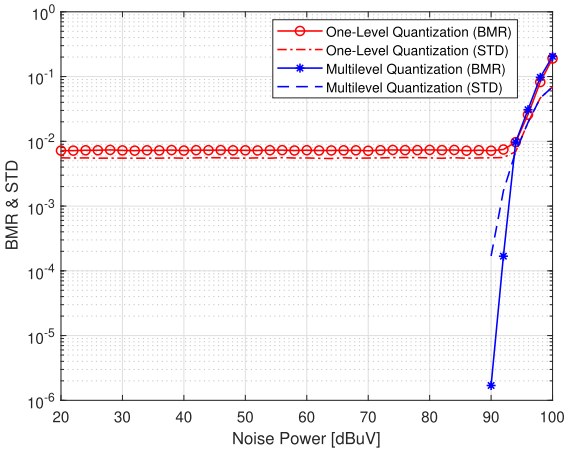
(a) A tree topology scenario



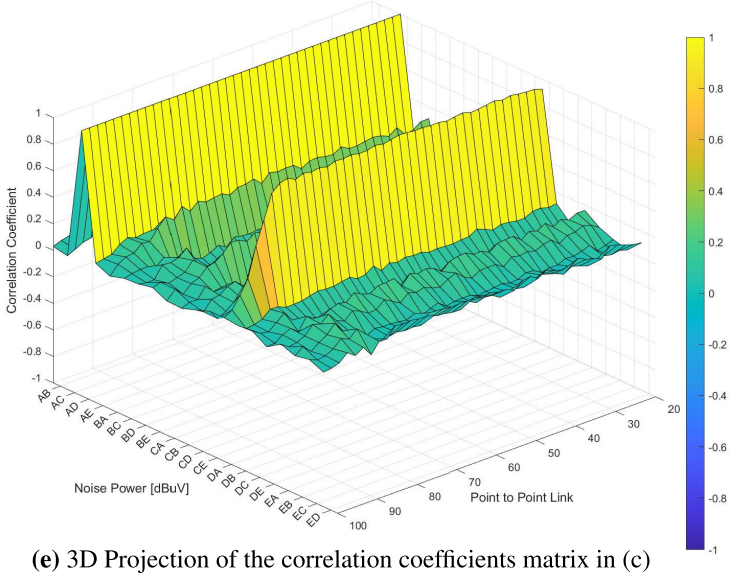
(b) The VCIR of $(A \leftrightarrow D)$ links and its generated ID/Key



(c) The correlation coefficients between the $(A \rightarrow D)$ link ID and the different link IDs

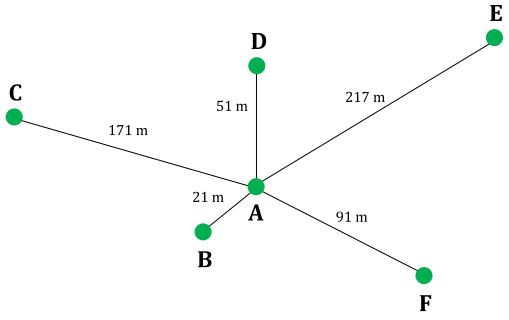


(d) BMR result after applying reconciliation techniques on $(A \leftrightarrow D)$ when compared with single-level quantization

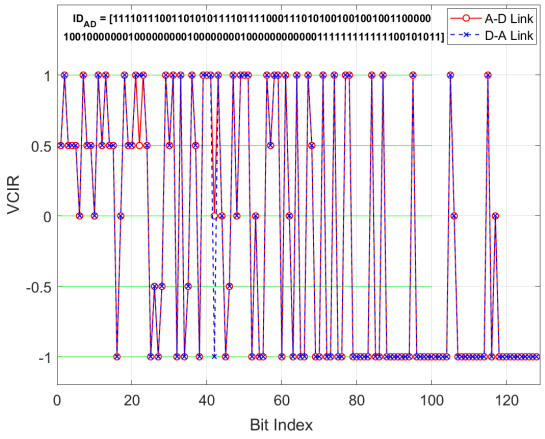


(e) 3D Projection of the correlation coefficients matrix in (c)

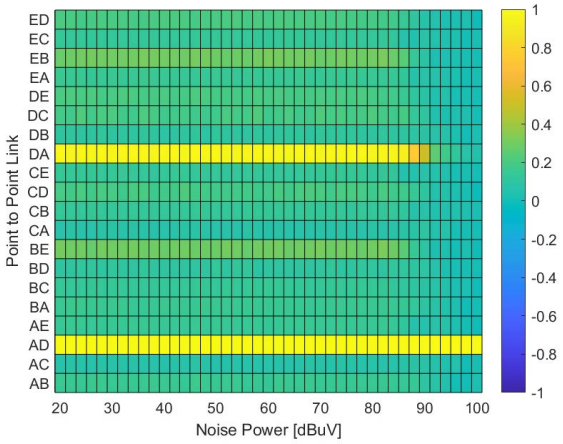
FIGURE 4. **Tree topology scenario simulation results.**



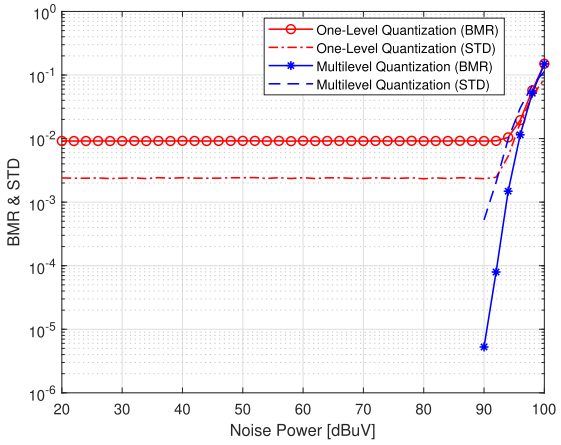
(a) A Star topology scenario



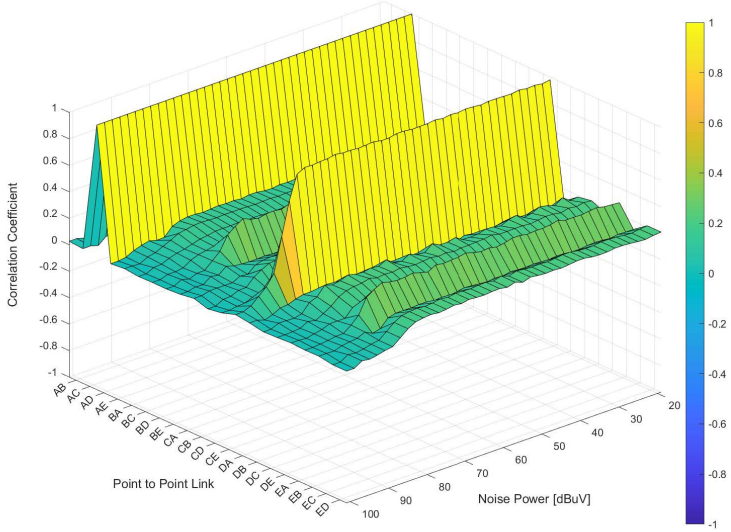
(b) The VCIR of $(A \leftrightarrow D)$ links and its generated ID/Key



(c) The correlation coefficients between the $(A \rightarrow D)$ link ID and the different links IDs



(d) BMR result after applying reconciliation techniques on $(A \leftrightarrow D)$ when compared with single-level quantization



(e) 3D Projection of the correlation coefficients matrix in (c)

FIGURE 5. **Star topology scenario simulation results.**

used PL propagation attenuation was $\alpha = -30$ dB/m, with a reflection attenuation of $\rho = -20$ dB and a discontinuity attenuation $\delta = -10$ dB. The transmit power was set to be 126 dBuV, the maximum ID key length was equal to 128, and the channel probing period was equal to $2 \times 128 \times T_s$, in order to cover the detection period of the two CIR parts.

B. SIMULATION RESULTS AND DISCUSSION

To evaluate the uniqueness of the keys, we computed the correlation coefficients between all links under different topologies and noise levels. Figs. 3, 4, and 5 show the simulation results, which are structured as follows:

a) The considered topology is presented. Communicating devices are represented in green and discontinuities in the cable, d_i, in red.
b) The VCIR multilevel quantization of the links ($A \leftrightarrow D$) is graphed, and the final generated key for the ($A \rightarrow D$) link after the reconciliation procedure.
c) The correlation coefficients between the ($A \rightarrow D$) link and all other possible links for the selected range of possible noise levels.
d) The BMR of the ($A \leftrightarrow D$) links is presented.
e) The corresponding three-dimensional (3D) graphical projection of the correlation matrix

As shown in the introduced figures, the reciprocity between the ($A \leftrightarrow D$) links shows a clear positive correlation for all cases. The star topology registers a higher correlation between the ($A \rightarrow D$) link and the other links, while the bus topology shows correlations below 0.2 for most links. The results for the star topology are justified taking into consideration the direct connections, shorter distances, and lack of discontinuities of the start topology, revealing a general spatial correlation between all links.

We simulated two alternative star-topology scenarios to test the above-introduced hypothesis, one duplicating the distances between all nodes while keeping all the other parameters unchanged to maintain the topology proportionality, and a second one adding a discontinuity between A and D at 21 m from A (replicating the A to B link).

The results for the first scenario, shown in Fig. 6, provide evidence that the correlation matrix is similar to the one of the initial topology, confirming the importance of the topology and keyhole effect in the correlation of impulses in PLC. In fact, the overall correlation increase with the rest of the links can be attributed to a combination of factors. Larger distances involve fewer paths detected and an increase in the first impulse arrival time for all nodes, reducing, in both cases, the entropy of the CIR, and hence an increase of the correlation between the links can be observed.

The 2D correlation coefficients display between the $A \rightarrow D$ link ID and the different link IDs for the second star-topology scenario is presented in Fig. 7. A comparable result to that of the first scenario is observed, similar to the correlation coefficients for the initial star-topology, with an increase of the correlation between $A \rightarrow D$ link ID and that of $A \rightarrow B$ and $B \rightarrow A$ link IDs. This can be explained by the fact that adding a discontinuity between A and D, exactly at the same distance from A to B, creates a similar set of multiple paths between the links $A \rightarrow B$ (or $B \rightarrow A$) and $A \rightarrow D$, and hence increases the correlation coefficients between these two link IDs.

The tree topology of Fig. 4 shows another example of the keyhole or pinhole effect. Links ($A \leftrightarrow D$), ($A \leftrightarrow B$) and ($A \leftrightarrow C$) share a common root node, and signals are therefore forced to pass through the same junction showing relatively high correlations. This characteristic effect of multipath propagation in PLC, provides no diversity gain due to reflections and becomes more evident in tree structures. As expected, and for all cases, the correlation coefficients between the different links decrease with increasing noise power levels. This phenomenon occurs due to the direct relationship between the CIR observations during the channel probing and the

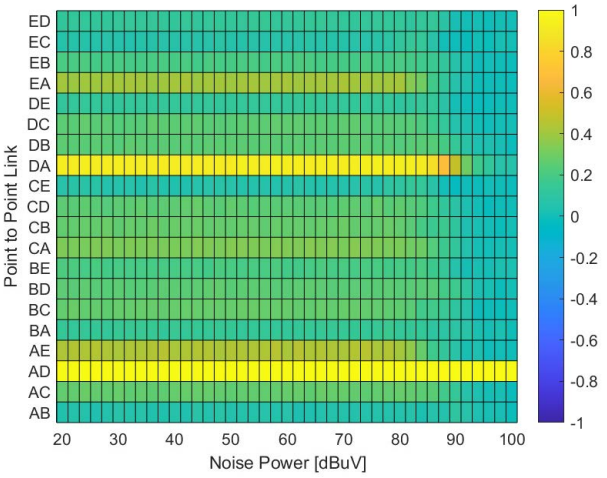


FIGURE 6. The correlation coefficients between the ($A \rightarrow D$) link ID and the different link IDs of topology 5 (a) with modified distances (x2).

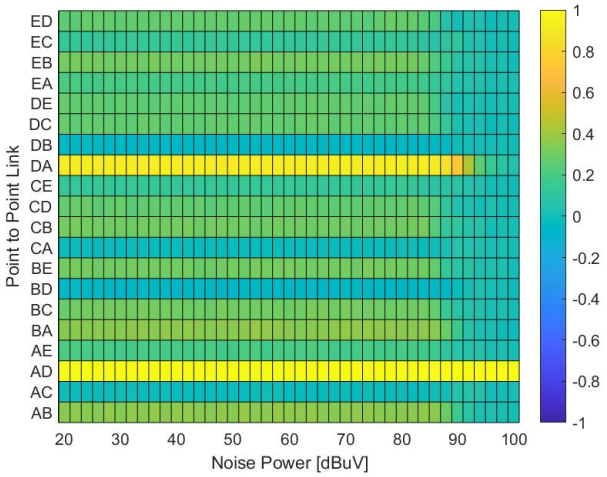


FIGURE 7. The 2D correlation coefficients display between the ($A \rightarrow D$) link ID and the different link IDs of topology 5 (a) with the addition of a discontinuity between A and D at 21 m from A.

noise: if the noise power increases, the CIR estimation error increases. Hence, the VCIR accuracy decreases, resulting in a noisy key that reflects the uncorrelated noise variation and not the PLC CIR. In general, and independently from any topological consideration, channel estimation errors become prevalent over high noises, with a consequent disruption of the communication channel. The simulations show that this threshold is situated at approximately 90 dBuV, for all cases. The bus topology presents a slighter lower tolerance due to the higher distances (attenuation) between the *A* and *D* nodes.

The BMR comparison between both quantization schemes shows considerable differences. While the minimum BMR for the one-level quantization exhibits values above 10^{-3}, with constant performance below 90 dBuV, the proposed scheme obtains null values for the same noise power range. The difference can be attributed to the reduction of bit mismatches performed in the reconciliation phase conducted for the multilevel quantization but not available for its one-level counterpart. Another side effect of not being able to apply a reconciliation method can be seen by the fact that the BMR of the one-level quantization converges to a minimum value that cannot be reduced even with decreasing levels of noise. The reported results for noise values above 90 dBuV are similar for both quantization schemes, indicating that the impact of the channel estimation error due to high noise levels affects them equally.

According to the presented results of the BMR and the correlation coefficients for the different topologies, we can infer that using the output of the proposed scheme can significantly enhance the legitimate communication security in terms of SOP. In particular, by considering the two legitimate nodes *A* and *D*, the simulation results have shown very low correlations of its generated key with the other links that can be used by eavesdroppers. Consequently, the secrecy rate can be easily increased, and hence a decrease of the SOP can be observed.

From what has been discussed so far, several research paths stem from the outcome of this work, in particular from the significant impact of the topology on the CIR. In detail, modeling the effect of different network topologies, distances, and discontinuities, seems the most challenging avenue, as well as studying the influence on the density of items in the system. Other research topics, such as security amplification techniques, especially tailored for the PLC scenario, would help improve the keys' entropy, making this type of approach a solution of choice for cryptographic applications.

VI. CONCLUSION

In this paper we propose, to the best of our knowledge, the first CIR multilevel quantization algorithm for PLC. Our solution tackles the communication impairments and the general lack of symmetry of the power line channel that has hindered the adoption of physical layer techniques for this medium. The introduced method has broad applicability and, in this paper, we have chosen to present an application for the PLS domain. In particular, our approach significantly reduces the error mismatch rate with respect to the existing single-level quantization method. The proposed solution enables the use of information reconciliation techniques that help reduce the effects of channel estimation errors and noise. These findings are supported by an extensive simulation campaign examining several characteristic topologies and testing them under different working conditions. The experimental results show the quality and viability of the proposed approach. In detail, for noise power levels lower than 90 dBuV, the proposed multilevel quantization algorithm can induce a reduction of at least three orders of magnitude of the BMR, when compared to the single-level quantization. The tests also confirmed that the adoption of such a scheme could enable the deployment, among others, of novel physical layer techniques for PLC. Finally, we have highlighted further research directions.

ACKNOWLEDGMENT

The findings reported in this article are under the sole responsibility of the co-authors.

REFERENCES

[1] X.-Y. Wang and X. Gao, "The typical designs of PLC network in MV distribution network," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2012, pp. 19–23.

[2] S. Hussain, J. H. Fernandez, A. K. Al-Ali, and A. Shikfa, "Vulnerabilities and countermeasures in electrical substations," *Int. J. Crit. Infrastruct. Protection*, vol. 33, Jun. 2021, Art. no. 100406.

[3] C. Alaton and F. Tounquet, "Benchmarking smart metering deployment in EU," Eur. Commission, Brussels, Belgium, Tech. Rep., 2020.

[4] F. Tounquet *et al.*, "Supporting country fiches accompanying the report benchmarking smart metering deployment in the EU-28," Eur. Commission, Brussels, Belgium, Tech. Rep., 2020.

[5] PRIME Alliance. *PRIME Alliance Interoperable Standard for Advance Meter Management and Smart Grid*. Accessed: May 16, 2020. [Online]. Available: https://www.prime-alliance.org

[6] I. Stoyanov, T. Iliev, G. Mihaylov, E. Ivanova, and P. Kogias, "Smart grid communication protocols in intelligent service for household energy use," in *Cybernetics Approaches in Intelligent Systems*. Cham, Switzerland: Springer, 2018, pp. 380–389.

[7] S. Erlinghagen, B. Lichtensteiger, and J. Markard, "Smart meter communication standards in Europe—A comparison," *Renew. Sustain. Energy Rev.*, vol. 43, pp. 1249–1262, Mar. 2015.

[8] N. Uribe-Pérez, L. Hernández, D. D. la Vega, and I. Angulo, "State of the art and trends review of smart metering in electricity grids," *Appl. Sci.*, vol. 6, no. 3, p. 68, 2016.

[9] J. P. A. Yaacoub, J. H. Fernandez, H. N. Noura, and A. Chehab, "Security of power line communication systems: Issues, limitations and existing solutions," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100331.

[10] L. T. Lars Torsten Berger, A. Schwager, and J. Escudero-Garzás, "Power line communications for smart grid applications," *J. Electr. Comput. Eng.*, vol. 2013, p. 3, Jan. 2013.

[11] A. Omri, *Channel Estimation for LTE MIMO-OFDM Systems: Estimation Techniques of Mobile Radio Channel selective in Time and in Frequency*. Sunnyvale, CA, USA: LAP Lambert Academic Publishing, 2012.

[12] *Specification for PoweRline Intelligent Metering Evolution, R1.4*, PRIME Alliance TWG, Des Moines, IA, USA, Oct. 2014.

[13] *Unified High-Speed Wire-Line Based Home Networking Transceivers—Data Link Layer Specification*, document ITU-T, Recommendation ITU-T G.9961, Apr. 2014.

[14] A. Omri, M. Shaqfeh, A. Ali, and H. Alnuweiri, "Synchronization procedure in 5G NR systems," *IEEE Access*, vol. 7, pp. 41286–41295, 2019.

[15] S. J. Golstein, F. Rottenberg, F. Horlin, P. D. Doncker, and J. Sarrazin, "Physical layer security in an OFDM time reversal SISO communication with imperfect channel state information," *IEEE Access*, vol. 10, pp. 26778–26794, 2022.

[16] H. Chamkhia, A. Erbad, A. K. Al-Ali, A. Mohamed, A. Refaey, and M. Guizani, "3-D stochastic geometry-based modeling and performance analysis of efficient security enhancement scheme for IoT systems," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6663–6677, May 2022.

[17] F. Passerini and A. M. Tonello, "Secure PHY layer key generation in the asymmetric power line communication channel," *Electronics*, vol. 9, no. 4, p. 605, Apr. 2020.

[18] W. Henkel, H. Y. Kim, A. M. Turjman, and M. Bode, "A simple physical-layer key generation scheme for power-line transmission," in *Proc. IEEE Int. Symp. Power Line Commun. its Appl. (ISPLC)*, Oct. 2021, pp. 13–18.

[19] A. Omri and M. O. Hasna, "Average secrecy outage rate and average secrecy outage duration of wireless communication systems with diversity over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3822–3833, Jun. 2018.

[20] A. Omri and M. O. Hasna, "Physical layer security analysis of UAV based communication networks," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–6.

[21] J. H. Fernandez, L. Lacasa, A. Omri, A. Sanz, and M. E. Koborsi, "Ergodic capacity analysis of OFDM-based NB-PLC systems," in *Proc. 24th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2022, pp. 399–405.

[22] W. Henkel and M. Namachanja, "A simple physical-layer key generation for frequency-division duplexing (FDD)," in *Proc. 15th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2021, pp. 1–6.

[23] A. Omri, M. O. Hasna, and K. B. Letaief, "Inter-relay interference management schemes for wireless multi-user Decode-and-Forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 2072–2081, Apr. 2015.

[24] N. K. Ibrahim, A. Sali, H. A. Karim, A. F. Ramli, N. S. Ibrahim, and D. Grace, "Multiple description coding for enhancing outage and video performance over relay-assisted cognitive radio networks," *IEEE Access*, vol. 10, pp. 11750–11762, 2022.

[25] A. Ivanov, V. Stoynov, D. Mihaylova, and V. Poulkov, "Energy detectors performance evaluation for interweave cognitive radio network scenario in 5G," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1032, no. 1, Jan. 2021, Art. no. 012010.

[26] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[27] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[28] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.

[29] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[30] H. N. Noura, R. Melki, A. Chehab, and J. H. Fernandez, "Efficient and secure message authentication algorithm at the physical layer," *Wireless Netw.*, pp. 1–15, Jun. 2020. [Online]. Available: https://link.springer.com/article/10.1007/s11276-020-02371-7

[31] R. Melki, H. N. Hassan, J. H. Fernandez, and A. Chehab, "Message authentication algorithm for OFDM communication systems," *Telecommun. Syst.*, vol. 76, no. 3, pp. 403–422, 2020.

[32] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.

[33] M. De Piante and A. M. Tonello, "Characteristics of the PLC channel: Reciprocity, symmetry and port decoupling for impedance matching," in *Proc. Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2016, pp. 93–97.

[34] K. Lee, N. Klingensmith, S. Banerjee, and Y. Kim, "VoltKey: Continuous secret key generation based on power line noise for zero-involvement pairing and authentication," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 3, no. 3, pp. 1–26, Sep. 2019.

[35] F. Yang, M. A. Islam, and S. Ren, "PowerKey: Generating secret keys from power line electromagnetic interferences," in *Proc. Int. Conf. Netw. Syst. Secur.*, Cham, Switzerland: Springer, 2020, pp. 354–370.

[36] W. Henkel, O. A. Graur, N. S. Islam, U. Pagel, N. Manak, and O. Can, "Reciprocity for physical layer security with wireless FDD and in wireline communications," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.

[37] W. Henkel, A. M. Turjman, H. Kim, and H. K. H. Qanadilo, "Common randomness for physical-layer key generation in power-line transmission," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[38] G. Prasad, O. Taghizadeh, L. Lampe, and R. Mathar, "Securing MIMO power line communications with full-duplex jamming receivers," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, Apr. 2019, pp. 1–6.

[39] C. Cano, A. Pittolo, D. Malone, L. Lampe, A. M. Tonello, and A. G. Dabak, "State of the art in power line communications: From the applications to the medium," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 7, pp. 1935–1952, Jul. 2016.

[40] Y. Zhuang and L. Lampe, "Physical layer security in MIMO power line communication networks," in *Proc. 18th IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2014, pp. 272–277.

[41] A. Pittolo and A. M. Tonello, "Physical layer security in PLC networks: Achievable secrecy rate and channel effects," in *Proc. IEEE 17th Int. Symp. Power Line Commun. Appl.*, Mar. 2013, pp. 273–278.

[42] A. Pittolo and A. Tonello, "Physical layer security in power line communication networks: An emerging scenario, other than wireless," *IET Commun.*, vol. 8, no. 8, pp. 1239–1247, May 2014.

[43] Â. Camponogara, H. V. Poor, and M. V. Ribeiro, "Physical layer security of in-home PLC systems: Analysis based on a measurement campaign," *IEEE Syst. J.*, vol. 15, no. 1, pp. 617–628, Mar. 2021.

[44] B. Sigweni, M. Mangwala, and J. Chuma, "Modified timed efficient stream loss-tolerant authentication to secure power line communication," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 9, no. 4, p. 2281, Aug. 2019.

[45] A. T. Sherman, D. Phatak, B. Sonawane, and V. G. Relan, "Location authentication through power line communication: Design, protocol, and analysis of a new out-of-band strategy," in *Proc. ISPLC*, Mar. 2010, pp. 279–284.

[46] J. Heo, C. S. Hong, M. S. Choi, S. H. Ju, and Y. H. Lim, "Identity-based mutual device authentication schemes for PLC system," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Apr. 2008, pp. 47–51.

[47] J. Heo, C. S. Hong, S. H. Ju, Y. H. Lim, B. S. Lee, and D. H. Hyun, "A security mechanism for automation control in PLC-based networks," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2007, pp. 466–470.

[48] S. Liu, M. Ma, Y. Li, Y. Chen, and B. Jiao, "An absolute secure wire-line communication method against wiretapper," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 536–539, Mar. 2017.

[49] A. Camponogara, H. V. Poor, and M. V. Ribeiro, "The complete and incomplete low-bit-rate hybrid PLC/wireless channel models: Physical layer security analyses," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2760–2769, Apr. 2019.

[50] A. El Shafie, M. F. Marzban, R. Chabaan, and N. Al-Dhahir, "An artificial-noise-aided secure scheme for hybrid parallel PLC/wireless OFDM systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[51] H. N. Noura, R. Melki, A. Chehab, and J. H. Fernandez, "Efficient and robust data availability solution for hybrid PLC/RF systems," *Comput. Netw.*, vol. 185, Feb. 2021, Art. no. 107675.

[52] M. R. Fliss, J. H. Fernandez, A. Omri, and G. Oligeri, "NB-PLC successful transmission probability analysis," in *Proc. 2nd Int. Conf. Smart Grid Renew. Energy (SGRE)*, Nov. 2019, pp. 1–6.

[53] A. Omri, J. H. Fernandez, A. Sanz, and M. R. Fliss, "PLC channel selection schemes for OFDM-based NB-PLC systems," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, May 2020, pp. 1–6.

[54] S. Raponi, J. H. Fernandez, A. Omri, and G. Oligeri, "Long-term noise characterization of narrowband power line communications," *IEEE Trans. Power Del.*, vol. 37, no. 1, pp. 365–373, Feb. 2022.

[55] G. Prasad, Y. Huo, L. Lampe, and V. C. M. Leung, "Machine learning based physical-layer intrusion detection and location for the smart grid," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–6.

[56] A. M. Tonello, L. Lampe, and T. Swart, *Power Line Communications: Principles, Standards and Applications From Multimedia to Smart Grid*. Hoboken, NJ, USA: Wiley, 2016.

[57] B. Masood, W. Nazar, and R. Masood, "Channel modeling of low voltage NB-PLC network using statistical and deterministic channel modeling approaches," in *Proc. 7th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Oct. 2018, pp. 693–696.

[58] G. Chu, J. Li, and W. Liu, "Narrow band power line channel characteristics for low voltage access network in China," in *Proc. 17th IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2013, pp. 297–302.

[59] M. Zimmermann and K. Dostert, "Analysis and modeling of impulsive noise in broad-band powerline communications," *IEEE Trans. Electromagn. Compat.*, vol. 44, no. 1, pp. 249–258, Feb. 2002.

[60] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Netw.*, vol. 21, no. 6, pp. 1835–1846, Mar. 2015.
[61] S. T. B. Hamida, J.-B. Pierrot, and C. Castelluccia, "An adaptive quantization algorithm for secret key generation using radio channel measurements," in *Proc. 3rd Int. Conf. New Technol., Mobility Secur.*, Dec. 2009, pp. 1–5.

JAVIER HERNANDEZ FERNANDEZ received the B.Sc. degree in computer science from the University of Ottawa, Canada, the master's degree in energy management from the University of Zaragoza, and the master's degree in project management from the University San Pablo CEU/IEP, Spain. He is currently managing research and technical consulting projects as part of the Innovation Team, Iberdrola, working in the smart grid, renewables, and energy efficiency domains. He specializes in the area of technology innovation and brings over 25 years of practical experience in overseeing the design and delivery of Research and Development initiatives on behalf of multi-national companies in the field of IT, telecom, and utilities. In addition to.

AYMEN OMRI received the engineering degree in telecommunications from The Tunisian Aviation Academy EABA, in 2007, and the M.Res. and Ph.D. degrees in information and communications technology (ICT) from the Engineering National School of Tunis (ENIT)/Tunis El Manar University, in 2009 and 2012, respectively. From 2012 to 2017, he was a Postdoctoral Researcher at the Electrical Engineering (EE) Department, Qatar University. From 2018 to 2019, he was a Postdoctoral Researcher at the Department of Electrical and Computer Engineering, Texas A&M University, Qatar. He is currently a Research Scientist with Iberdrola Innovation Middle East, Qatar Science and Technology Park. His research interests include modeling, design and performance analysis of communication systems, 5-G NR Systems, device to device communication systems, wireless/wired emulation and experimentation platforms, and power line communication (PLC) systems.

ROBERTO DI PIETRO (Senior Member, IEEE) is a ACM Distinguished Scientist, a Full Professor of cybersecurity, HBKU-CSE. He was in the capacity of the Global Head Security Research, Nokia Bell Laboratories, and an Associate Professor (with tenure) of computer science at University of Padova, Italy. He has been working in the security field for 25+ years, leading both technology-oriented and research-focused teams in the private sector, government, and academia (MoD, United Nations HQ, EUROJUST, IAEA, WIPO). His main research interests include AI driven cybersecurity, security and privacy for distributed systems (e.g. Blockchain technology, Cloud, IoT, OSNs), virtualization security, applied cryptography, and data science. He involved in M&A of start-up—and having founded one (exited)—he has been producing 250+ scientific papers and 15 patents over the cited topics, has coauthored three books, and edited one. From 2011 to 2012, he was awarded the Chair of Excellence from University Carlos III, Madrid. In 2020 he received the Jean-Claude Laprie Award for having significantly influenced the theory and practice of Dependable Computing. He is consistently ranked among the 2% world-top scientists since this ranking existed.