Electrical Power and Energy Systems 145 (2023) 108634

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Power grid surveillance: Topology change detection system using power line communications

Javier Hernandez Fernandez [a,b], Aymen Omri [b,*], Roberto Di Pietro [a]

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

ARTICLE INFO

Keywords:
Channel impulse response
Physical layer
Power line communications
Smart grid
Topology change detection
Security
Surveillance

ABSTRACT

This paper proposes an efficient channel impulse response (CIR)-based technique to detect topology changes in the power grid. The features of the proposed approach include the following aspects: (i) it is a software-only solution, not requiring any intervention on the current smart grid architecture; (ii) topology changes can be detected via a simple distributed algorithm that requires only local communications; and, (iii) both memory and computational footprints of the proposed solution are minimal. The above-mentioned features make this contribution notably appealing for the resource-constrained smart grid domain. Furthermore, the paper provides a detailed discussion of the introduced technique, accompanied by an implementation reflecting a realistic use case, and presents an extensive simulation campaign to show the quality and viability of the proposed approach. A unique feature of our solution is that it performs well even when the communication channel is affected by a high noise level. For instance, with noise levels below 100 dBμV (the typical PLC noise power range), the proposed solution showed a $\approx 100\%$ detection rate.

To the best of our knowledge, our solution is the first one proposing a fully CIR-based, distributed, deterministic algorithm for intrusion detection and localization. We believe that the performance and advantages of the proposed technique pave the way for further smart grid applications and solutions.

1. Introduction

The smart grid is the integration of smart technologies into power grids to optimize overall performance, including generation, transmission, distribution, and end-user applications. Power line communication (PLC) is currently one of the most popular telecommunication technologies for smart grids. The deployment of PLC-based smart grids enables two-way communications between the utility assets in a cost-efficient manner as it allows for the reuse of existing network infrastructure. PLC technology is mature, cost-effective, and has a wide range of applications such as advanced metering infrastructure (AMI), topology estimations [1], grid management [2,3], and energy loss detection [4,5], to cite a few.

Because of their geographical dispersion and ongoing transformation owing to automation and digitization, the cited critical infrastructures are naturally vulnerable to attacks [6]. The smart grid provides opportunities to improve the efficiency of power distribution, but it also introduces new vulnerabilities that could be exploited by an adversary. In particular, the security of PLC-based smart grids, a long-standing concern for both the industry and the research community, has been studied extensively in recent years [7]. As a result, PLC security-based techniques are becoming a popular method to protect smart grids against malicious cyber–physical attacks, fraud, or unintentional misbehavior [8,9].

Utility companies place a high value on topology-related services since they simultaneously cater to both operational and security needs. Topology could change due a number of events: some are legitimate, such as network extension works performed by linemen or line switching, while others are illicit, such as illegal connections (non-technical losses) or the addition of malicious equipment. PLC topology solutions work by constructing a network map that describes the physical layout of the network and the relationships between devices. This map may be used to monitor the removal or addition of devices to the network, detect anomalies, and identify malicious intrusions, while also optimizing the dispatch of crews to solve the issues. Topology solutions automatically ensure that the network map is accurate and up-to-date by checking changes in connectivity. They also eliminate the need for manual mapping of the network, significantly reducing both time and cost requirements as well as efforts related to configuration and PLC topology change detection. Moreover, automated topology solutions

[*] Corresponding author.
E-mail addresses: j.hernandezf@iberdrola.com (J. Hernandez Fernandez), aomri@iberdrola.com (A. Omri), rdipietro@hbku.edu.qa (R. Di Pietro).

https://doi.org/10.1016/j.ijepes.2022.108634
Received 26 January 2022; Received in revised form 15 August 2022; Accepted 13 September 2022
Available online 29 September 2022

are more reliable than manual methods when security-related applications are concerned because they reduce human error. Topology-based security is an example of the ability of PLC to support smart grid applications, which require the local enforcement of policies, such as restrictions on data or access to distribution devices.

In addition to enhanced security and the direct operational benefits, topology-based solutions can enable condition monitoring routines that, coupled with maintenance programs, have proven to have considerable technical and economic benefits in maintaining other grid assets such as transformers [10,11]. The possibility of reducing maintenance costs, increasing network reliability, performing robust network mapping, and providing real-time security features make these applications an ideal complement to PLC-based smart grids.

Contributions

The main contributions of the paper can be summarized as follows:

- We first detail some background information, revising state-of-the-art solutions on topology change detection, and presenting a thorough characterization of PLC signals and channel modeling.
- Then, we present and detail the proposed topology change detection approach. In particular, a distributed and fully channel impulse response (CIR)-based algorithm has been introduced to efficiently detect and identify topology changes in an electrical grid.
- Furthermore, we report on the performed extensive simulation campaign aiming to evaluate and investigate the introduced approach's performance.

Overall, our proposed approach is inspired by real use-cases, rooted in sound theory, and supported by an extensive simulation campaign, which confirms the quality and viability of the proposed solution.

Paper organization

The rest of the paper is organized as follows. Section 2 presents related work. The characteristics of PLC signals, and the PLC system and channel models are detailed in Sections 3 and 4, respectively. Section 5 describes the proposed power line (PL) identification scheme and the topology change detection system under imperfect channel state information (CSI). In Section 6, we present and discuss simulations results. Finally, conclusions are drawn in Section 7.

2. Related work

While PLC topologies are diverse in terms of elements, protocols, communication media, and methods, they have common features that provide the PLC-based smart grid with unique functionalities. The most distinctive advantage over other communication technologies is the ability to use the signals as a way to obtain real-time information on the power grid. A myriad of smart grid applications have been built, taking advantage of the inherent information obtained from the PLC telecommunication signals such as finding faults in the grid [12–14] or detecting losses [4,5]. Among all possible applications, electricity distribution companies place a high value on topology-related services since they address operational and security demands. PLC-based topology recognition is a research area of interest, with many techniques available to leverage the unique features of PLC for this specific task.

The available PLC monitoring strategies are classified as either frequency domain-based or time domain-based. The Time domain-based techniques examine PLC packets over time to reveal selected characteristics, while the frequency-domain based approaches analyze the PLC signal spectrum. The following subsections provide an overview of related work to PLC-based topology recognition, first introducing frequency domain-based methods and subsequently time domain-based methods.

2.1. *Frequency domain-based PLC topology solutions*

The first category of PLC topology recognition methods uses signal frequency information as the basis for identification. Frequency domain-based methods are typically divided into two categories: spectral analysis and autocorrelation. Spectral analysis considers the power spectrum of a signal to identify patterns and it is commonly used along with the CSI or frequency domain reflectometry (FDR). The latter can be subdivided into single-point [15,16] and multi-point FDR solutions, which are presented in combination with time domain-based solutions [17–20]. Autocorrelation measures the correlation of PLC signals over time. PLC signal characterization is then performed by grouping frequencies into clusters or classes. The authors of [21] propose the use of time-series to predict the CSI of channels avoiding the need for reference measurements or the comprehensive training associated with machine learning approaches. In [22], the relationship between the CFR and the powerline features is used to monitor the power quality.

2.2. *Time domain-based PLC topology solutions*

PLC communication signals can be used to achieve topology recognition by tracking PLC packet generation and propagation through the network. Analysis of PLC packets relies on extracting PLC waveforms at different points in the network to estimate the PLC signal propagation time. These values are then compared with known lengths to determine whether the PLC packets have followed the expected path. PLC packet recognition can be achieved by applying a threshold to the estimated signal propagation time. There are two main families of time domain-based PLC topology recognition methods: the time of arrival (ToA) and the time difference of arrival (TDoA). ToA estimation approximates the time taken for a PLC packet to reach the PLC receiver from each PLC transmitter based on its known location and the speed of light. TDoA estimation is used for PLC packet detection; that is, it measures the time difference between detections at two PLC receivers located some distance apart along a PLC branch. PLC signal processing is required to extract the packets, usually using either bandpass filtering or time/frequency transformations. PLC signal processing is subsequently used to compute the packet timing or packet size measurements. ToA is commonly used in topology estimation solutions [23–26], especially for inferring distances [27].

Some works have combined both domains to offer comprehensive solutions [17–20]. Others have avoided the PLC signals and employed electrical network parameters, such as the admittance [28] or smart meter data [29,30], to infer or identify changes in the topology. Solutions utilizing neural networks and machine learning algorithms in combination with PLC channel state data are now being developed for cable diagnosis and security applications with promising results [31–33]. A study worth mentioning is that of [34], focusing on the communication topologies that PLC modems create rather than the cable topology itself.

Our solution employs the path delay of the CIR to provide a distributed and deterministic algorithm that can identify and locate changes in the power grid network. In the usage of the CIR and path delays, there are some similarities with [35], a cable diagnosis solution, [31,36], a key generation method. In [16], two single point reflectometry methods for topology inferring are proposed; one based on time-domain peak location and a second based on signal propagation and transmission line theory. Our proposal shares the technique with the former but, in contrast, it addresses the problem from a distributed and multipoint perspective. The authors of [16] discuss the implicit resolution problem of time domain-based peak-detection approaches due to the limitation of the signal bandwidth and present the parametric or super-resolution methods as an alternative to overcome this limitation. The recent evolution of PLC technology and protocols, especially in BB-PLC, can offer sampling rates of up to 200 MHz [37], which significantly reduces the previously mentioned

Table 1
PLC signal propagation and topology change rate by voltage level and technology.

Voltage Level/PLC Type	Topology Change Rate	Max. signal propagation range	Signal propagation limit	Crosstalk
MV (BB-PLC)	Infrequent	<800 m for underground cables <2 km for overhead cables [46,47]	Limited to MV line segment, BB-PLC does not traverse transformers [48]	Crosstalk could occur due to cable proximity [30,49]
LV (BB-PLC)	Infrequent	≈200 m [50,51]	Limited to LV line segment: • BB-PLC does not traverse MV/LV transformers [48] • Customers fuse box provides high signal losses [51–54]	Crosstalk could occur due to cable proximity [30,49]
LV (NB-PLC)	Infrequent	<2 km [50,55]	Not limited to LV line segment: • Crosstalk between close transformers, as the signal is able to bypass transformers [56] • Customers fuse box provides low attenuation, negligible for high nominal current breakers [53]	Crosstalk could occur due to cable [30,49] or transformer proximity [57]
LV In-home (BB-PLC)	Frequent	<300 m [58] ≈90% outlets covered [51]	Limited to households, fuse box provides high signal loss [51,53,54]	Common, interferences between households are usually avoided by coupling after the fuse box [51]

resolution constraint for time-domain solutions. The work presented in [31] also employs CIR for security applications, by proposing a machine-learning-based PLC intrusion detection system. Besides not involving machine learning techniques, our proposal differs from the above as it is based purely on CIR, whereas [31], employs the channel frequency response (CFR) for detection while relying on the CIR for the location. To the best of our knowledge, our solution is the only one proposing a fully CIR-based, distributed, deterministic algorithm for intrusion detection and localization.

3. Characteristics of PLC signals

PLC is divided into three categories based on the utilized frequency band: ultra narrow-band (UNB)-PLC, narrow-band (NB)-PLC, and broad-band (BB)-PLC [38]. BB-PLC spans over the MHz frequency band and can offer a higher data rate than its NB counterpart at the expense of lowered ranges and increased consumption [39]. In addition, due to its high frequencies, the BB-PLC system suffers from increased attenuation, noise, and multipath effects. NB-PLC, operating in the kHz band, overcomes the high attenuation of high frequencies and is, therefore, able to communicate over longer distances. This has allowed NB-PLC protocols to prevail in current smart grid deployments, especially for smart metering applications, relegating BB-PLC to in-home and energy efficiency applications [40,41].

In this section, we present the main characteristics of PLC signals. In particular, for each voltage level/PLC type, we detail the signal propagation range, limits, and rate of topology changes, which are essential for the application, operation, and design of PLC systems.

High voltage (HV) lines have traditionally relied on PLC functioning at low frequencies to transmit teleprotection signals or to detect anomalies, such as sags or faults [12,42,43]. When compared with medium voltage (MV) and low voltage (LV) lines, despite providing lower attenuation and direct communications, HV PLC experiences higher noise levels and considerably more expensive coupling units [44]. The overall cost of HV PLC and the installation of fiber optic links along with HV cables have relegated HV PLC in transmission lines to a secondary role [45]. On the contrary, the complexity and capillarity of MV and LV distribution power lines provide an advantage for PLC, given the opportunity to reuse the infrastructure itself, and also because it is possible to leverage the signals to monitor the grid status [20].

The remainder of this section provides a framework for the broad topics of MV and LV PLC applications, topology, and signal propagation. Table 1 provides a summary of the section findings.

3.1. Physical properties

One of the primary advantages of PLC, when connected to the electrical grid, is its ability to communicate information about the power grid itself. Exploiting the physical properties of the transmission medium has proven to be an effective approach, particularly in wireless networks, where CSI provides fine-grained data to support different physical layer mechanisms. However, due to the inherent differences between wireless and power line media, most of the methods adopted in the wireless domain cannot be directly incorporated into power line media. The main distinction between wireless and PLC arises from the fact that wireless communications can rely on reciprocal channel characteristics, node mobility, and a changing environment [59,60]. On the contrary, in power line transmission there is no mobility of the communicating nodes, a more stable environment exists, and one cannot leverage CSI reciprocity—with the exception of channel path delays. Appendix A in [36] showed that the time domain response between two PLC modems is not perfectly symmetric but wide-sense symmetric. In particular, the time response of a pair of channels between two points/ports is not necessarily symmetric.

Notably, when a signal travels from port 1 to port 2 and back, the channel's multipath response features peaks in identical positions on both paths. However, the heights of the peaks vary, rendering a channel multipath response that is not perfectly symmetrical and limiting perfect symmetry to only the position of the impulses. In terms of spatial decorrelation, uncorrelated multipath fading occurs between devices more than half a wavelength apart in wireless communications [59]. In PLC, the keyhole effect, as well as its influence on diversity gain, causes crosstalk, resulting in channel response correlation [36,61–63].

3.2. Common applications of PLC

The deployment of MV lines can vary significantly within regions; however, independently from the network topology, MV PLC applications usually adopt a point-to-point architecture interconnecting transformer substations with BB-PLC [48,64]. The latency, reliability, and bandwidth provided by these dedicated broadband links provide an ideal backbone communication system for monitoring and control systems [65,66].

LV involves two distinguishable segments: the distribution network, managed by the power utility, and the in-building or in-home segment. In either case, the predominant topology is a radial network that expands into branching lines from the transformer station to the final customer. The use of both NB-PLC and BB-PLC is common in both

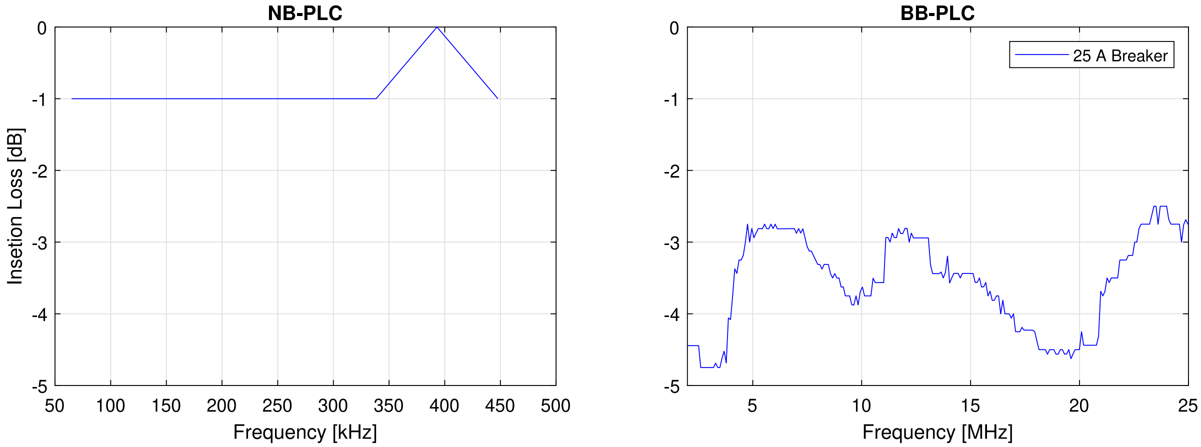

Fig. 1. Insertion loss of a 25 A breaker in NB-PLC and BB-PLC.

sections, covering a wide range of smart grid applications, such as metering, access networks, electric vehicles, or grid control [20,67,68]. Depending on the local regulations, the boundary between the in-home and distribution networks usually lies in the electrical meter or the protection/fuse box on the customer's premises. Multimedia, VoIP, and other home automation applications tend to require higher bandwidths and are, therefore, more likely to adopt BB-PLC solutions [69,70].

3.3. Frequency of topology changes in power lines

The switching, control, protection, and isolation of power lines are broad topics beyond the scope of this paper. However, when it comes to changes in the topology of utility-managed distribution networks, the rate of change is relatively infrequent. In addition to maintenance and extension works on the grid, non-malicious events that can trigger topology changes can be broadly classified as faults due to operational management of the network's power flow [71,72]. Both cases are infrequent and are known by the system operator. LV lines in the in-home segment are more prone to topological changes, as an average household or building would regularly see appliances being connected and disconnected from the network.

3.4. PLC signal propagation distances

Both path loss and noise inversely affect the signal propagation; higher frequencies experience higher attenuation but are usually less affected by power line noise [73]. Due to the sheer number of factors affecting the range of PLC, the solution of choice to obtain a representative value for PLC coverage involves resorting to real measurements.

Results of empirical testing for BB-PLC in MV lines have been presented in [46], yielding average distances for underground cables as follows: 800 m for a 2 to 7 MHz band, 400 m for the 8 to 18 MHz range, and under 2 km for overhead lines. The authors of [47] complemented the previous work by studying the performance and throughput of the BB-PLC IEEE 1901 in a laboratory environment, obtaining similar results. Regarding LV lines, [50] reported distances up to 2 km for NB-PLC. The authors of [55] reviewed the distances and data rates reached in over 15 countries, while [74] compared the transmission probability in low and high attenuation situations and [75] simulated the effect of using different frequency bands to provide efficient network coverage in the 42 to 471 kHz band. LV BB-PLC has lower communication distances than NB-PLC, usually ranging in the hundreds of meters [50]. Measurement campaigns performed for BB-PLC have shown a coverage probability of above 90% for the range from 150 to 200 m for frequencies below 8.4 MHz in distribution grids and over 90% for in-home outlets [51]. Recent studies based on the G.hn protocol have shown direct connections of over 300 m [58].

3.5. PLC signal limits

In PLC, signals are restricted to the transmission medium and therefore bound to the LV network between customers and transformers or between the transformers stations (MV) being interconnected. The signals can bypass the physical cables, either by crosstalk leaks due to cable proximity [30,49] or jumping the transformer station into the next voltage level. Traversing MV/LV transformers has proven to be unfeasible for BB-PLC, even with bypass couplers, due to asymmetries in the transfer functions between the LV-MV and MV-LV paths [48]. NB-PLC has proved able to bypass the transformers but at the expense of causing a high signal loss [56]. NB-PLC deployments have dealt with these cases by installing auxiliary PLC nodes to repeat the signals in those secondary substations with two or more transformers where complete isolation cannot be guaranteed [57].

Another impairment for signal propagation is the attenuation produced by the LV lines electrical protection and distribution equipment, such as street cabinets and customers' fuse boxes. The higher attenuation of these devices in BB-PLC produces a significant signal loss that, combined with the higher noises levels usually experienced in households, can filter the signal entirely, isolating the in-home network from the power utility segment or other neighboring networks [51,52,54]. To avoid these shortcomings, BPL repeaters are usually installed in street cabinets to relay the transmitted signals and ensure a longer reach [67]. The attenuation produced by breakers in NB-PLC is generally negligible for high nominal current breakers, and below 3 dB for low nominal breakers [53].

Fig. 1 shows the insertion loss of a standard residential 25 A residual current circuit breaker (Schneider Acti 9 iID), as measured in our laboratory. The NB-PLC measurements were performed using the Microchip evaluation kit for the PL360 modem [76] segmenting the FCC band into eight sub-bands from 42 kHz to 472 kHz, following the version 1.4 of PRIME standard [75,77]. The BB-PLC measurements covered the 2 to 30 MHz band using the UVAX G.hn modem COM-GPL module [78].

4. PLC system and channel models

In this section, we present and detail the considered PLC system and channel models.

4.1. PLC system models

In this work, without loss of generality, we consider two PLC topology models. The first one is a simple two-node topology, commonly used in the literature, aimed at presenting the main concepts of this contribution. The second one is a more general multi-node topology that is considered to evaluate the proposed PLC topology change detection approach.

Table 2
Power delay profile for the two-node topology model.

Path	Path Index	l_i	g_i
$N_1 \rightarrow N_2$	$i = 0$	L_{N1N2}	$(1-\alpha L_{N1N2})$
$N_1 \rightarrow N_2 \rightarrow N_1 \rightarrow N_2$	$i = 1$	$3L_{N1N2}$	$(1-\alpha L_{N1N2})^3\ (1-\rho_{N_1})\ (1-\rho_{N_2})$
$N_1 \rightarrow N_2 \rightarrow i(N_2 \rightarrow N_1 \rightarrow N_2)$	i	$(2i+1)L_{N1N2}$	$(1-\alpha L_{N1N2})^{2i+1}\ (1-\rho_{N_1})^i\ (1-\rho_{N_2})^i$

Table 3
Power delay profile of the ($N = 10$) first arrived paths for the two-node topology model with an added connection.

Path	Path Index	l_i	g_i
$N_1 \rightarrow X \rightarrow N_2$	$i = 0$	L_{N1N2}	$(1-\alpha L_{N1X})\ (1-\alpha L_{XN2})\ (1-\delta_X)$
$N_1 \rightarrow X \rightarrow N_1 \rightarrow X \rightarrow N_2$	$i = 1$	$3L_{N1X} + L_{XN2}$	$(1-\alpha L_{N1X})^3 (1-\alpha L_{XN2})\ (1-\rho_{N_1})\ (1-\rho_X)\ (1-\delta_X)$
$N_1 \rightarrow X \rightarrow Y \rightarrow X \rightarrow N_2$	$i = 2$	$L_{N1X} + 2L_{XY} + L_{XN2}$	$(1-\alpha L_{N1X})\ (1-\alpha L_{XY})^2 (1-\alpha L_{XN2})\ (1-\rho_Y)\ (1-\delta_X)^2$
$N_1 \rightarrow X \rightarrow N_1 \rightarrow X \rightarrow N_1 \rightarrow X \rightarrow N_2$	$i = 3$	$5L_{N1X} + L_{XN2}$	$(1-\alpha L_{N1X})^5\ (1-\alpha L_{XN2})(1-\rho_{N_1})^2 (1-\rho_X)^2\ \ (1-\delta_X)$
$N_1 \rightarrow X \rightarrow Y \rightarrow X \rightarrow N_1 \rightarrow X \rightarrow N_2$	$i = 4$	$3L_{N1X} + 2L_{XY} + L_{XN2}$	$(1-\alpha L_{N1X})^3\ (1-\alpha L_{XY})^2 (1-\alpha L_{XN2})(1-\rho_{N_1})(1-\rho_Y)\ \ (1-\delta_X)^3$
$N_1 \rightarrow X \rightarrow N_1 \rightarrow X \rightarrow Y \rightarrow X \rightarrow N_2$	$i = 5$	$3L_{N1X} + 2L_{XY} + L_{XN2}$	$(1-\alpha L_{N1X})^3\ (1-\alpha L_{XY})^2 (1-\alpha L_{XN2})(1-\rho_{N_1})(1-\rho_X)\ (1-\rho_Y)\ (1-\delta_X)^2$
$N_1 \rightarrow X \rightarrow N_2 \rightarrow X \rightarrow N_2$	$i = 6$	$L_{N1X} + 3L_{XN2}$	$(1-\alpha L_{N1X})\ (1-\alpha L_{XN2})^3 (1-\rho_{N_2})\ (1-\rho_X)\ (1-\delta_X)$
$N_1 \rightarrow X \rightarrow Y \rightarrow X \rightarrow Y \rightarrow X \rightarrow N_2$	$i = 7$	$L_{N1X} + 4L_{XY} + L_{XN2}$	$(1-\alpha L_{N1X})\ (1-\alpha L_{XY})^4 (1-\alpha L_{XN2})\ (1-\rho_X)\ (1-\rho_Y)^2\ \ (1-\delta_X)^2$
$N_1 \rightarrow X \rightarrow N_1 \rightarrow X \rightarrow N_2 \rightarrow X \rightarrow N_2$	$i = 8$	$3L_{N1X} + 3L_{XN2}$	$(1-\alpha L_{N1X})^3\ (1-\alpha L_{XN2})^3 (1-\rho_{N_1})\ (1-\rho_{N_2})\ (1-\rho_X)^2\ \ (1-\delta_X)$
$N_1 \rightarrow X \rightarrow N_2 \rightarrow X \rightarrow N_1 \rightarrow X \rightarrow N_2$	$i = 9$	$3L_{N1X} + 3L_{XN2}$	$(1-\alpha L_{N1X})^3\ (1-\alpha L_{XN2})^3 (1-\rho_{N_1})\ (1-\rho_{N_2})\ (1-\delta_X)^3$

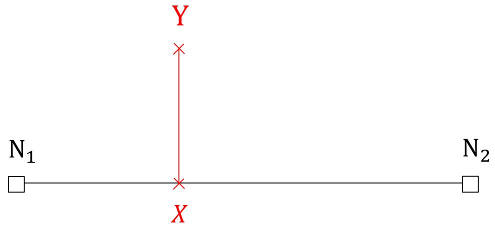

Fig. 2. Two-node topology model.

4.1.1. Two-node topology model

Fig. 2 presents the considered standard point-to-point model. It consists of a direct connection between two nodes N_1 and N_2, and a middle branch at a given point X with a termination point Y.

4.1.2. Multi-node topology model

The considered multi-node topology design includes several nodes that are connected to a main backbone/power line at various discontinuity points. In addition, two unknown connections are added at different locations X_1 and X_2, during the simulations. Without loss of generality, we present in Fig. 3, an example of a multi-node topology model with 14 nodes and 25 discontinuity points. We will show that our proposal will be able to detect such unknown connections in a distributed, efficient manner, leveraging just local communications.

4.2. PLC multipath channel model

The PLC time-domain model introduced in [79] is used to generate the corresponding path delays and gains for each of the considered models/scenarios.

Let us begin by investigating the first baseline situation depicted in Fig. 2, without the connection $(X-Y)$. For this configuration, the signal takes a first direct path $(N_1 \rightarrow N_2)$, and a nearly unlimited number of secondary paths as a result of the signal bouncing i times between N_1 and N_2. That is, for the first, direct path, when $i = 0$, we have the path $(N_1 \rightarrow N_2)$. Then, for the second path (first bounce, $i = 1$), we have $(N_1 \rightarrow N_2 \rightarrow N_1 \rightarrow N_2)$, and so on. Table 2 lists the path lengths l_i and weights g_i of each possible reflection.

Let L_{XY} denotes the general distance between two given nodes X and Y, α denotes the propagation attenuation coefficient per power line length unit, ρ_X denotes the reflection attenuation coefficient at node X, and δ_X denotes the discontinuity attenuation coefficient at node X. By considering the different aforementioned attenuation, the lengths l_i and weights g_i of the path $N_1 - N_2 -\ i(N_2 - N_1 - N_2)$, for the baseline scenario are given by:

$$l_i = L_{N_1 N_2}(1 + 2i) \tag{1}$$

and,

$$g_i = (1 - \alpha L_{N_1 N_2})^{2i+1} (1 - \rho_{N_1})^i (1 - \rho_{N_2})^i \tag{2}$$

respectively.

By adding the connection $(X - Y)$ and, as we mentioned before, due to the multiple reflections, there is a virtually infinite number of secondary paths arriving at N_2. Table 3 lists the corresponding first ten significant path lengths l_i and weights g_i for the two-node topology scenario, with the added connection. Assuming that the signal will be significantly attenuated after N reflections and/or discontinuity crossings, only the significant path with a gain equal to or larger than a given threshold will be considered.

Accordingly, we developed a script to exhaustively identify the significant paths and the corresponding delays and gains between any two nodes of the considered multi-node topology (Fig. 3).

Table 4 provides a list of the symbols employed in this paper.

5. Description of the topology change detection approach

The proposed approach for detecting topology changes is primarily based on the power line identification (PL ID) between two given nodes in the topology under consideration. The generation of the PL ID for the link between two nodes N_i and N_j^i is presented in Algorithm 1.

The inputs for the algorithm are system parameters—-namely, the PL ID length (in bits), the time resolution, the quantization threshold, the number of observations, and the different received signals—-which can be preset for the PLC system in use. Using these parameters, and as detailed in Algorithm 1, the first step consists of channel probing to estimate the different N_{Obs} CIRs from the received signals: $y_{N_i,N_j^i}(n)$, $n \in \{1,..N_{Obs}\}$. The second step subsequently minimizes the channel estimation error, by evaluating the average of the estimated CIRs, according to Eq. (3). Finally, the CIR quantization is performed to generate the PL ID ID_{N_i,N_j^i} for the link $N_i - N_j^i$. This generated PL ID represents the main parameter used to identify changes in the topology under consideration. For instance, let us assume that a new connected branch (X-Y) exists, as presented in Fig. 2. In this case, the proposed technique can easily detect the connection as follows. First, the node N_2 generates a PL ID $ID^{(0)}_{N_1,N_2}$ for the $N_1 - N_2$ link using Algorithm 1. After the elapsing of a predefined detection period, N_2 should repeat the same steps to generate a new PL ID, $ID^{(1)}_{N_1,N_2}$. At this point, if the

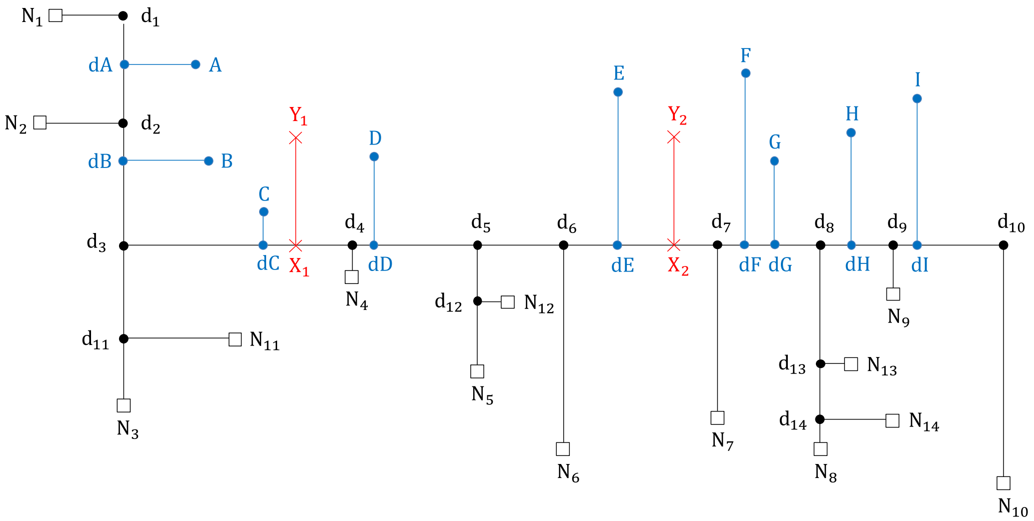

Fig. 3. An instance of a multi-node topology model.

Table 4
Table of notations.

Notation	Definition
ID_{Len}	PL ID length
T_s	Sampling time
Q_{th}	Quantization threshold
N_{Obs}	Number of observations
N_i	Node index i
L_{XY}	The distance between nodes X and Y
$h_{X,Y}$	The CIR of the link between nodes X and Y
$\hat{h}_{X,Y}$	The estimated CIR of the link between nodes X and Y
L_{min}	The minimum distance between two successive nodes
d_{max}	The maximum distance between two successive nodes
d_{min}	The minimum distance between a node and a topology change's location
α	The propagation attenuation coefficient
ρ_x	The reflection attenuation coefficient at node X
δ_x	The discontinuity attenuation coefficient at node X
l_i	ith path length
g_i	ith path gain
$ID^{(0)}_{N_X,N_Y}$	Original PL ID between nodes N_x and N_Y
$ID^{(1)}_{N_X,N_Y}$	Updated PL ID between nodes N_x and N_Y
P_{FND}	The false negative detection probability
P_{FPD}	The false positive detection probability
P_{SDP}	The successful detection probability
P_{TC}	The probability of a topology change

Algorithm 1 N_i-N_j^i Link PL identification scheme

```
Inputs: PL ID Length: $ID_{Len}$
        Sampling Time: $T_s$
        Quantization Threshold: $Q_{th}$
        Number of Observations: $N_{Obs}$
        Received Signals: $y_{N_i,N_j^i}(n)$, $n \in \{1,..N_{Obs}\}$

Step 1: Channel Probing:
        Estimation of the different $N_{Obs}$ CIRs: $\hat{h}_{N_i,N_j^i}(n)$

Step 2: Minimizing the Channel Estimation Error:

        $$\tilde{h}_{N_i,N_j^i} = \frac{\sum_{n=1}^{N_{Obs}} \hat{h}_{N_i,N_j^i}(n)}{N_{Obs}} \qquad (3)$$
Step 3: CIR quantization to generate the $N_i - N_j^i$ link
        PL ID: $ID_{N_i,N_j^i}$
```

bit mismatch rate (BMR) between $ID^{(1)}_{N_1,N_2}$ and $ID^{(0)}_{N_1,N_2}$ is larger than a given threshold, a detected topology change is declared; otherwise, no such declaration occurs.

By taking into account a more generic topology, as illustrated in Fig. 3, we present the various processes required for the multi-node topology change detection system in Algorithm 2, which involves seven main steps.

- **Step 1:** This step consists of initial signaling between each node N_i and the remaining nodes in the considered topology. In particular, by using the received signals from the various nodes, N_i should be able to evaluate the different corresponding received signal strength indicators (RSSIs). While node access control is outside the scope of this contribution, we assume that all legitimate nodes are registered in the network. Unregistered or unknown nodes cannot communicate with the registered nodes in this topology.
- **Step 2:** In this step, each node N_i should generate a list of N_j^i nodes with a significant RSSI, where, $j \in \{1,\dots,L_i\}$ and N_j^i denotes the jth node in N_i's list of length L_i. Regarding the nodes that cannot be connected to N_i or that have a very low RSSI, the corresponding PL ID cannot be generated or is not sufficiently accurate to be considered in the proposed algorithm—since a very low RSSI results in a high channel estimation error and hence, the generation of an inaccurate PL ID.
- **Step 3:** Each node N_i generates a list of PL IDs $ID^{(0)}_{N_i,N_j^i}$, $j \in \{1,\dots,L_i\}$, using Algorithm 1 and the outputs of **Steps 1** and **2.**
- **Step 4:** After the detection period has elapsed, this step involves repeating **Steps 1** to **3** to generate a new list of PL IDs: $ID^{(1)}_{N_i,N_j^i}$, by considering the same nodes identified in **Step 2.**
- **Step 5:** Each node N_i selects the node $N_{j^*}^i$, with the highest PL ID variation as presented in Algorithm 2. More specifically, each node N_i should evaluate the different PL ID variations (V_j) of the links $N_i - N_j^i$, $j \in \{1,\dots,L_i\}$. The variation V_j is defined as the ratio of the number of mismatching bits between $ID^{(0)}_{N_i,N_j^i}$ and $ID^{(1)}_{N_i,N_j^i}$ to the total number of $ID^{(0)}_{N_i,N_j^i}$ bits that are 1s. Subsequently, N_i should select the node with the highest variation V_j.

Algorithm 2 Topology Change Detection Approach

```
Inputs: PL ID Length: $ID_{Len}$
        Sampling Time: $T_s$
        Quantization Threshold: $Q_{th}$
        Number of Observations: $N_{Obs}$
        Detection Period
Step 1: Initial signaling between each node $N_i$ and the different
        other nodes.
Step 2: Each node $N_i$ should generate a list of
        $N_j^i$, $j \in \{1, .., L_i\}$, nodes with significant RSSIs.
Step 3: Each node $N_i$ generates a list of PL IDs:
        $ID^{(0)}_{N_i,N_j^i}$, $j \in \{1, .., L_i\}$, using Algorithm 1.
Step 4: Waiting for a detection period, then redo Steps 1 to 3.
        to get a new list of PL IDs: $ID^{(1)}_{N_i,N_j^i}$.
Step 5: For each node $N_i$, select the node $N_{j*}^i$, with the highest
        PL ID variation:
        • for $j$ from 1 to $L_i$ do
            $$V_j = \frac{\sum_{m=1}^{ID_{Len}} \left| ID^{(1)}_{N_i,N_j^i}(m) - ID^{(0)}_{N_i,N_j^i}(m) \right|}{\sum_{m=1}^{ID_{Len}} ID^{(0)}_{N_i,N_j^i}(m)}.   (4)$$
          end for
        • Select the node $N_{j*}^i$ with the highest PL ID variation.

Step 6: Each node $N_i$, with $N_{j*}^i \neq \emptyset$, sends its token to $N_{j*}^i$.

Step 7: If there is a token exchange between two given nodes,
        a topology change will be detected on the corresponding
        link.
```

- **Step 6:** In this step, each node N_i, with $N_{j*}^i \neq \emptyset$, sends its token to node N_{j*}^i.
- **Step 7:** If a token exchange occurs between two given nodes, a topology change will be detected on the corresponding link, and detection messages will be sent; otherwise, no topology change will be detected.

6. Performance analysis and numerical results

In this section, we first describe the performance analysis metrics in detail, and subsequently report and discuss the analysis and numerical results of the suggested approach when applied to the two studied system models.

The simulations were conducted in MatLab version R2020a, run on a 64-bit Windows 10 operating system.

6.1. Performance analysis metrics

To assess the advantages of the proposed approach, the following performance analysis metrics were used, presented along with their definitions:

- The false negative detection probability (FNDP): denoted by P_{FND}, is defined as the probability that the proposed method is unable to detect a topology change.
- The false positive detection probability (FPDP): denoted by P_{FPD}, is defined as the probability that the proposed method detects a non existent topology change.
- The successful detection probability (SDP): denoted by P_{SD}, is defined as the probability that the proposed method correctly detects a topology change and, more specifically, it detects a topology change and identifies the link where the relevant change is located. P_{SD} can be expressed as follows:

$$P_{SD} = P_{TC}(1 - P_{FND}) + (1 - P_{TC})(1 - P_{FPD}), \quad (5)$$

where P_{TC} is the probability of a topology change.

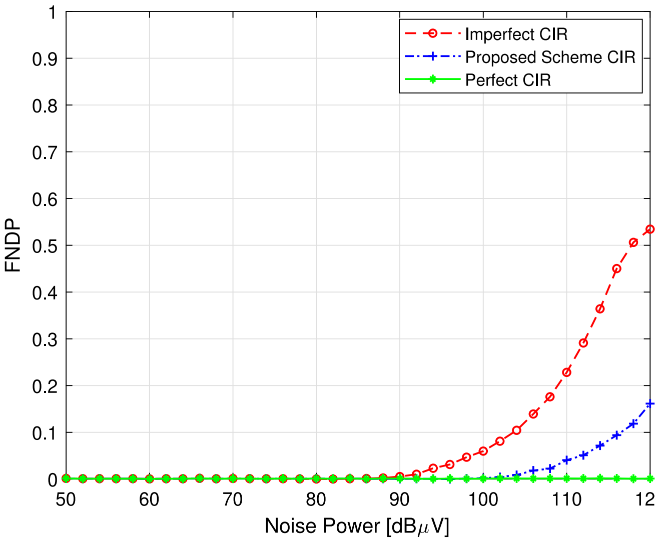

Fig. 4. FNDP vs. noise power for a two-node topology, with $P_{TC} = 0.5$.

6.2. Performance analysis in a two-node topology model

Without loss of generality, the used simulation parameters were set as follows: the distance between the two nodes were a random variable with possible values of $d_{N_1N_2} \in [L_{min}, L_{max}]$, $d_{N_1X} \in [d_{min}, d_{N_1N_2} - d_{min}]$, $d_{XY} \in [L_{min}, L_{max}]$, $L_{min} = 50$ m, $L_{max} = 200$ m, $d_{min} = 10$ m, $\alpha = -30$ dB/m, $\rho_X = -20$ dB, $\delta_X = -10$ dB, the sampling time = 0.005 μs, the PL ID length = 512 bits, $N_{Obs} = 20$, and the number of iterations = 10^4. It is important to point out that the channel estimation error depends mostly on the used transmit power and the noise level. Accordingly, to provide accurate and realistic results, the performed simulations used a transmit power of 126 dBμV, which is within the range used by several PLC systems and standards [80,81]. In addition, we have considered a noise power range from 50 dBμV to 120 dBμV, which is based on real field measurements in different PLC systems and environments [73,79,82].

Fig. 4 presents the FNDP versus the noise power for a two-node topology, with $P_{TC} = 0.5$. It shows that the FNDP increases with increasing noise power values for the proposed scheme with imperfect knowledge of the CIR and using the suggested CIR estimation approach. This is expected because increasing the noise power increases the channel estimation error; hence, the FNDP increases. In addition, the suggested CIR estimation approach showed a favorable performance, comparable to assuming a perfect knowledge of the CIR, due to the error-minimizing method used within the proposed scheme.

Fig. 5 shows the FPDP against the noise power for a two-node topology, with $P_{TC} = 0.5$. It shows that low noise power levels have a negligible effect on the FPDP, resulting in null values for the latter. By increasing the noise power levels, the FPDP increases until it reaches a maximum. This is because increasing the noise level decreases the accuracy of the CIRs and the relevant PL IDs—hence, an increase in the FPDP can be observed. Then, when the noise levels increase significantly (e.g. above 90 and above 105), both the CIR estimation error and that of the corresponding PL ID increase, resulting in a high likelihood of resemblance between the reference PL ID, $ID^{(0)}_{N_1,N_2}$, and the updated one, $ID^{(1)}_{N_1,N_2}$, leading to a reduction in the FPDP.

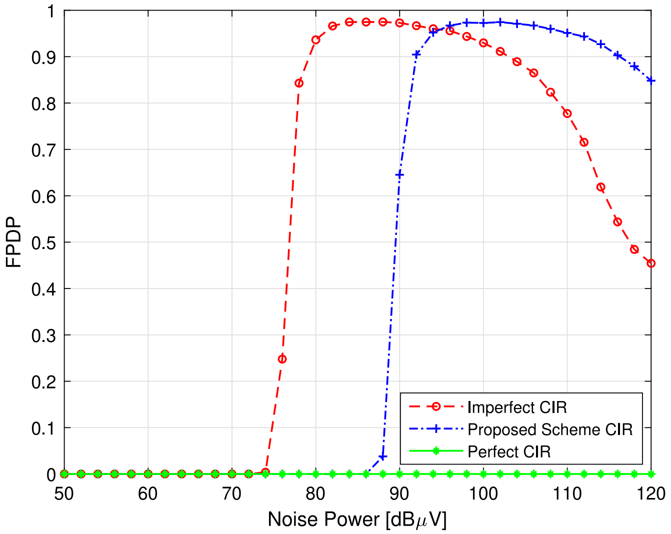

Fig. 5. FPDP vs. noise power for a two-node topology, with $P_{TC} = 0.5$.

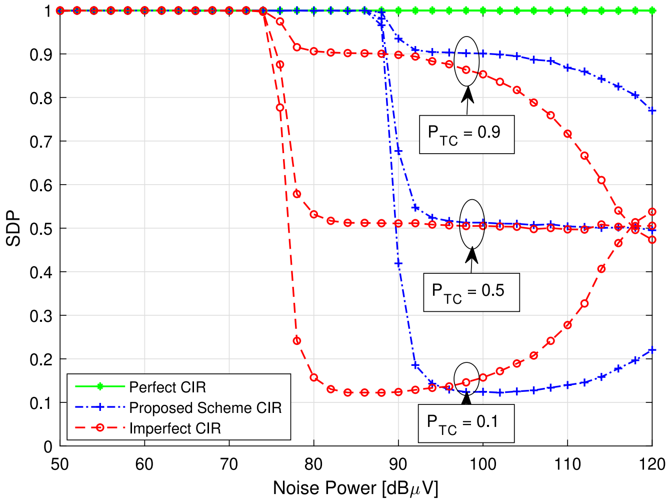

Fig. 6. SDP vs. noise power for a two-node topology, with $P_{TC} = 0.1,\ 0.5$ and 0.9.

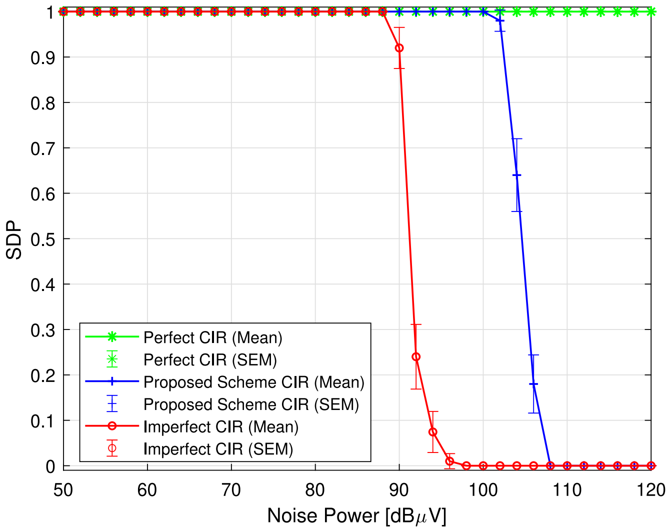

Fig. 7. Mean and standard error of the mean (SEM) of SDP vs. noise power for a multi-node topology, with two unknown connections.

Fig. 6 presents the SDP variations versus the noise power for a two-node topology, with $P_{TC} = 0.1,\ 0.5,$ and 0.9. For a low noise power ($\leq$ 72 dBμV), the SDP is always equal to 1. Notably, as seen in Figs. 4 and 5, the FNDP and FPDP are both null at low noise levels. As a result, the SDP is equal to 1, according to the formula in (5). Then, as the noise power increases, the FNDP increases and the FPDP proportionally decreases, resulting in the SDP converging to P_{TC} according to the expression in (5). The SDP then drops to 0.5 when the noise power is high, as expected. This is because the influence of the noise on the PL IDs accuracy is rather large in this case, resulting in identical values of the FPDP and FNDP (i.e., 0.5); therefore the SDP converges to 0.5, according to (5). By further increasing the noise power (> 120 dBμV), the SDP converges to $1 - P_{TC}$. Notably, for a very high noise level, the FPDP tends to 0 and the FNDP to 1; hence, according to expression (5), the SDP tends to $1 - P_{TC}$. However, this latter case is uncommon in practice, as noise levels are often less than or equal to 100 dBμV [73,82].

6.3. Performance analysis in a multi-node topology model

Without loss of generality, we have been considering a multi-node topology model with 14 nodes and 25 discontinuity points, as illustrated in Fig. 3, where the simulation parameters were set as follows: the distances between each set of two adjacent points (nodes, discontinuities, or terminals) as random variables with possible values from $L_{min} = 10$ m to $L_{max} = 50$ m, $\alpha = -30$ dB/m, $\rho_X = -20$ dB, $\delta_X = -10$ dB, the sampling time = 0.005 μs, the transmit power = 126 dBμV, the noise power range 50 – 120 dBμV, the PL ID length = 512 bits, $N_{Obs} = 20$, and the number of iterations = 10^3. In addition, we assumed that the considered multi-node topology always had two unknown connections at X_1, X_2. In order to assure the detection of both endpoints, we set $P_{TC} = 1$.

Fig. 7 presents the SDP versus the noise power for a multi-node topology. For low and medium noise power ($\leq$ 89 dBμV for an imperfect CIR and $\leq$ 100 dBμV for the proposed scheme CIR), the SDP equals 1. Notably, the FNDP is negligible at low and medium noise levels, and hence the SDP is equal to 1 since $P_{TC} = 1$. Then, by increasing the noise level, the FNDP increases significantly, and hence the SDP converges to zero, as expected. The results confirm the efficiency of the proposed PL ID variation detection technique that can be used to identify topology changes in practical PLC environments, where the noise levels are lower than 100 dBμV [73,79]. In addition to the SDP, Fig. 7 presents also the SDP standard error of the mean (SEM) for the different considered schemes. The SEM measures the extent to which the sample mean differs from the true population mean. As seen in Fig. 7, the SEM values are very low, compared to the SDP ones, which confirms the advantage of the proposed scheme.

6.4. Applicability

As mentioned in this paper, and particularly in Section 3, some of the main concepts and underlying factors needed to evaluate the applicability of the proposed solution, and in general most signal-based PLC techniques, are:

- Topology changes in the power grids, except in the in-home environment are generally infrequent.
- PLC signals cover most electrical grid topologies, especially when using multi-hop transmission techniques.
- Communication impairments encountered by the signals as they traverse MV/LV lines and in-home/LV distribution grids are generally enough to provide isolation between these segments.
- The detection resolution is proportional to the used sampling frequency, and therefore by decreasing the sampling frequency, the detection resolution value increases. As a consequence, to obtain a low detection resolution, a high sampling frequency is needed; making the proposed solution better suited for BB-PLC implementations.

- The range of application, the maximum length (D_{max}) of the link between two adjacent/successive nodes, is evidently bound to the detection of at least the first path of a link between two given nodes.

A critical issue for the application of the proposed solution is the maximum length (D_{max}) of the link between two adjacent/successive nodes. In detail, it is worth mentioning that generating the PL ID of a link between two given adjacent nodes depends on the specific system and environmental parameters, such as the PL ID length, the sampling time, the link length, and the signal attenuation factors. Notably, the maximum sensing period during the channel probing step between two given nodes is equal to the product of the PL ID length and the sampling time, that is, $ID_{Len} \times T_S$. Theoretically, to detect at least the first path of a link between two given nodes, the maximum corresponding length should be equal to or less than $D_{max} = ID_{Len} \times T_S \times 0.6 \times C$ [79]. Hence, generating the PL ID is possible only if the corresponding link is equal to/or less than D_{max}; otherwise, no path can be detected, and hence no PL ID can be generated and used for the proposed detection approach. For instance, for a sampling time of 0.005 μs and a PL ID length of 512 bits, the applicability range is $D_{max} = 460.8$ m—a range that satisfies all the possible applications discussed in this paper.

7. Conclusion

In this paper, a PLC topology change detection and identification technique, only leveraging CIR, has been proposed. We have first introduced and detailed an efficient CIR-based PL ID generation method that significantly improves the PLC channel multipath detection ability. Building on this detection accuracy, a topology change detection algorithm that is able to identify changes in the network's physical topology has been presented and detailed. The experimental results confirm the quality and viability of the proposed approach, showing an excellent successful topology change detection accuracy, even for high PLC noise levels. For instance, when noise levels are less than 100 dBμV, the proposed solution is able to offer a $\approx$ 100% detection rate. To the best of our knowledge, this is the first CIR-only based solution for topology detection, and we believe that the introduced technique, other than being a contribution on its own, also paves the way for further research and applications in the field.

CRediT authorship contribution statement

Javier Hernandez Fernandez: Conceptualization, Methodology, Software, Writing – original draft. **Aymen Omri:** Investigation, Data curation, Formal analysis, Validation, Writing – review editing. **Roberto Di Pietro:** Conceptualization, Methodology, Supervision, Validation, Writing – review editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

This publication is supported by Iberdrola S.A. as part of its innovation department research studies. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of Iberdrola Group.

References

[1] Lisowski M, Masnicki R, Mindykowski J. PLC-enabled low voltage distribution network topology monitoring. IEEE Trans Smart Grid 2019;10(6):6436–48.

[2] Uribe-Pérez N, Hernández L, Gómez R, Soria S, de la Vega D, Angulo I, Arzuaga T, et al. Smart management of a distributed generation microgrid through plc PRIME technology. In: 2015 International symposium on smart electric distribution systems and technologies. IEEE; 2015, p. 374–9.

[3] Caprolu M, Hernandez Fernandez J, Alassi A, Di Pietro R. Increasing renewable generation feed-in capacity leveraging smart meters. In: 2020 IEEE Green energy and smart systems conference. 2020, p. 1–7. http://dx.doi.org/10.1109/IGESSC50231.2020.9285082.

[4] Christopher AV, Swaminathan G, Subramanian M, Thangaraj P. Distribution line monitoring system for the detection of power theft using power line communication. In: 2014 IEEE Conference on energy conversion. 2014, p. 55–60. http://dx.doi.org/10.1109/CENCON.2014.6967476.

[5] Cho M, Huang H, Chen C, Thom HT, Wang P, Chang W, et al. The implementation and applications of low voltage distribution line theft supervisory system. In: 2016 3rd International conference on green technology and sustainable development. 2016, p. 178–84. http://dx.doi.org/10.1109/GTSD.2016.50.

[6] Hussain S, Hernandez Fernandez J, Al-Ali AK, Shikfa A. Vulnerabilities and countermeasures in electrical substations. Int J Crit Infrastruct Prot 2021;33:100406. http://dx.doi.org/10.1016/j.ijcip.2020.100406, URL https://www.sciencedirect.com/science/article/pii/S1874548220300706.

[7] Yaacoub JPA, Hernandez Fernandez J, Noura HN, Chehab A. Security of power line communication systems: Issues, limitations and existing solutions. Comp Sci Rev 2021;39:100331. http://dx.doi.org/10.1016/j.cosrev.2020.100331, URL http://www.sciencedirect.com/science/article/pii/S1574013720304317.

[8] Noura HN, Melki R, Chehab A, Hernandez Fernandez J. Efficient and robust data availability solution for hybrid PLC/RF systems. Comput Netw 2020;107–675. http://dx.doi.org/10.1016/j.comnet.2020.107675, URL http://www.sciencedirect.com/science/article/pii/S138912862031286X.

[9] Melki R, Noura HN, Hernandez Fernandez J, Chehab A. Message authentication algorithm for OFDM communication systems. Telecommun Syst 2020;1–20.

[10] Arshad M, Islam SM. A novel fuzzy logic technique for power transformer asset management. In: Conference Record of the 2006 IEEE Industry applications conference forty-first IAS annual meeting, vol. 1. 2006, p. 276–86.

[11] Hernandez Fernandez J, Wang B, Massoud A, Talib S, Shhaab M, et al. On ambient temperature of transformer substations in desert climates. In: 2021 IEEE Power energy society innovative smart grid technologies conference. 2021, p. 1–4. http://dx.doi.org/10.1109/ISGT49243.2021.9372154.

[12] Moreno JA, Quintanilla R. Smartgrid applications using narrow band power line carrier in underground power distribution systems. PLC fault locator. In: CIRED 2009 - 20th International conference and exhibition on electricity distribution - Part 1. 2009, p. 1–4. http://dx.doi.org/10.1049/cp.2009.0662.

[13] Zhao X, Qi Y, Li G. Research and implementation of PLC for multiport traveling wave fault location in the medium voltage distribution network. In: 2011 4th International conference on electric utility deregulation and restructuring and power technologies. 2011, p. 614–7. http://dx.doi.org/10.1109/DRPT.2011.5993966.

[14] Passerini F, Tonello AM. Smart grid monitoring using power line modems: Anomaly detection and localization. IEEE Trans Smart Grid 2019;10(6):6178–86. http://dx.doi.org/10.1109/TSG.2019.2899264.

[15] Ahmed MO, Lampe L. Power line network topology inference using frequency domain reflectometry. In: 2012 IEEE International conference on communications. 2012, p. 3419–23. http://dx.doi.org/10.1109/ICC.2012.6363874.

[16] Ahmed MO, Lampe L. Parametric and nonparametric methods for power line network topology inference. In: 2012 IEEE International symposium on power line communications and its applications. 2012, p. 274–9. http://dx.doi.org/10.1109/ISPLC.2012.6201319.

[17] Passerini F, Tonello AM. Smart grid monitoring using power line modems: Effect of anomalies on signal propagation. IEEE Access 2019;7:27302–12. http://dx.doi.org/10.1109/ACCESS.2019.2901861.

[18] Zhang C, Zhu X, Huang Y, Liu G. High-resolution and low-complexity dynamic topology estimation for plc networks assisted by impulsive noise source detection. IET Commun 2016;10(4):443–51.

[19] Ahmed MO, Lampe L. Power line communications for low-voltage power grid tomography. IEEE Trans Commun 2013;61(12):5163–75. http://dx.doi.org/10.1109/TCOMM.2013.111613.130238.

[20] Lampe L, Ahmed MO. Power grid topology inference using power line communications. In: 2013 IEEE International conference on smart grid communications (SmartGridComm). 2013, p. 336–41. http://dx.doi.org/10.1109/SmartGridComm.2013.6687980.

[21] Huo Y, Prasad G, Lampe L, Leung VCM. Power line communication based smart grid asset monitoring using time series forecasting. 2021, Online https://arxiv.org/abs/2110.10219/. [Accessed 28 December 2021].

[22] Yang F, Ding W, Song J. Non-intrusive power line quality monitoring based on power line communications. In: 2013 IEEE 17th International symposium on power line communications and its applications. 2013, p. 191–6. http://dx.doi.org/10.1109/ISPLC.2013.6525848.

[23] Smail MK, Pichon L, Olivas M, Auzanneau F, Lambert M. Recent progress in EMC and reliability for automotive applications. In: VXV International symposium on theoretical engineering. 2009, p. 1–5.

[24] Smail MK, Pichon L, Olivas M, Auzanneau F, Lambert M. Detection of defects in wiring networks using time domain reflectometry. IEEE Trans Magn 2010;46(8):2998–3001. http://dx.doi.org/10.1109/TMAG.2010.2043720.

[25] Erseghe T, Tomasin S, Vigato A. Topology estimation for smart micro grids via powerline communications. IEEE Trans Signal Process 2013;61(13):3368–77. http://dx.doi.org/10.1109/TSP.2013.2259826.

[26] Aouichak I, Khalil K, Elfeki I, Le Bunetel J, Raingeaud Y. Topology identification method for unknown indoor PLC home networks. In: 2017 International symposium on electromagnetic compatibility - EMC EUROPE. 2017, p. 1–4. http://dx.doi.org/10.1109/EMCEurope.2017.8094680.

[27] Erseghe T, Lorenzon F, Tomasin S, Costabeber A, Tenti P. Distance measurement over PLC for dynamic grid mapping of smart micro grids. In: 2011 IEEE International conference on smart grid communications (SmartGridComm). 2011, p. 487–92. http://dx.doi.org/10.1109/SmartGridComm.2011.6102371.

[28] Passerini F, Tonello AM. On the exploitation of admittance measurements for wired network topology derivation. IEEE Trans Instrum Meas 2017;66(3):374–82. http://dx.doi.org/10.1109/TIM.2016.2636478.

[29] Peppanen J, Grijalva S, Reno MJ, Broderick RJ. Distribution system low-voltage circuit topology estimation using smart metering data. In: 2016 IEEE/PES Transmission and distribution conference and exposition (T D). 2016, p. 1–5. http://dx.doi.org/10.1109/TDC.2016.7519985.

[30] Lisowski M, Masnicki R, Mindykowski J. PLC-enabled low voltage distribution network topology monitoring. IEEE Trans Smart Grid 2019;10(6):6436–48.

[31] Prasad G, Huo Y, Lampe L, Leung VCM. Machine learning based physical-layer intrusion detection and location for the smart grid. In: 2019 IEEE International conference on communications, control, and computing technologies for smart grids (SmartGridComm). 2019, p. 1–6. http://dx.doi.org/10.1109/SmartGridComm.2019.8909779.

[32] Huo Y, Prasad G, Lampe L, Leung VCM. Cable health monitoring in distribution networks using power line communications. In: 2018 IEEE International conference on communications, control, and computing technologies for smart grids (SmartGridComm). 2018, p. 1–6. http://dx.doi.org/10.1109/SmartGridComm.2018.8587458.

[33] Huo Y, Prasad G, Lampe L, Leung VCM. Advanced smart grid monitoring: Intelligent cable diagnostics using neural networks. In: 2020 IEEE International symposium on power line communications and its applications. 2020, p. 1–6. http://dx.doi.org/10.1109/ISPLC48789.2020.9115403.

[34] Hartmann T, Fouquet F, Klein J, Le Traon Y, Pelov A, Toutain L, et al. Generating realistic smart grid communication topologies based on real-data. In: 2014 IEEE International conference on smart grid communications (SmartGridComm). 2014, p. 428–33. http://dx.doi.org/10.1109/SmartGridComm.2014.7007684.

[35] Huo Y, Prasad G, Atanackovic L, Lampe L, Leung VCM. Cable diagnostics with power line modems for smart grid monitoring. IEEE Access 2019;7:60206–20. http://dx.doi.org/10.1109/ACCESS.2019.2914580.

[36] Passerini F, Tonello AM. Secure PHY layer key generation in the asymmetric power line communication channel. Electronics 2020;9(4):605.

[37] Yonge L, Abad J, Afkhamie K, Guerrieri L, Katar S, Lioe H, et al. An overview of the HomePlug AV2 technology. J. Electr. Comput. Eng. 2013;2013. http://dx.doi.org/10.1155/2013/892628.

[38] Galli S, Scaglione A, Wang Z. For the grid and through the grid: The role of power line communications in the smart grid. Proc IEEE 2011;99(6):998–1027.

[39] Mathur A, Bhatnagar MR, Panigrahi BK. PLC performance analysis over Rayleigh fading channel under nakagami-m additive noise. IEEE Commun Lett 2014;18(12):2101–4.

[40] Alaton C, Tounquet F. Benchmarking smart metering deployment in EU. European Commision; 2020, http://dx.doi.org/10.2833/492070, URL https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1403084595595{&}uri=COM:2014:356:FIN.

[41] Uribe-Pérez N, Hernández L, la Vega DD, Angulo I. State of the art and trends review of smart metering in electricity grids. Appl Sci 2016;6(3):68.

[42] de Villiers W, Cloete JH, Wedepohl LM, Burger A. Real-time sag monitoring system for high-voltage overhead transmission lines based on power-line carrier signal behavior. IEEE Trans Power Deliv 2008;23(1):389–95. http://dx.doi.org/10.1109/TPWRD.2007.905550.

[43] Adami JF, Silveira PM, Martinez MLB, Perez RC, Dallbello AC. New approach to improve high-voltage transmission line reliability. IEEE Trans Power Deliv 2009;24(3):1515–20. http://dx.doi.org/10.1109/TPWRD.2009.2013669.

[44] Berger LT, Schwager A, Pagani P, Schneider DM. MIMO power line communications. IEEE Commun Surv Tutor 2015;17(1):106–24.

[45] L. T. Berger LT, Schwager A, Escudero-Garzás J. Power line communications for smart grid applications. J. Electr. Comput. Eng. 2013;2013.

[46] Della Giustina D, Andersson L, Casirati C, Zanini S, Cremaschini L. Testing the broadband power line communication for the distribution grid management in a real operational environment. In: International symposium on power electronics power electronics, electrical drives, automation and motion. 2012, p. 785–9. http://dx.doi.org/10.1109/SPEEDAM.2012.6264631.

[47] Mlynek P, Silhavy P, Slacik J, Musil P, Blažek P. Broadband PLC on medium voltage - performance measurements. In: 2019 11th International congress on ultra modern telecommunications and control systems and workshops. 2019, p. 1–5. http://dx.doi.org/10.1109/ICUMT48472.2019.8970818.

[48] Ikpehai A, Adebisi B, Rabie KM. Broadband PLC for clustered advanced metering infrastructure (AMI) architecture. 9, (7):Multidisciplinary Digital Publishing Institute; 2016, p. 569,

[49] Corchado JA, Cortés JA, Cañete FJ, Arregui A, Díez L. Analysis of the spatial correlation of indoor MIMO PLC channels. IEEE Commun Lett 2017;21(1):40–3. http://dx.doi.org/10.1109/LCOMM.2016.2616341.

[50] S. Erlinghagen BL, Markard J. Smart meter communication standards in Europe-a comparison. Renew Sustain Energy Rev 2015;43:1249–62.

[51] Liu W, Widmer H, Raffin P. Broadband PLC access systems and field deployment in European power line networks. IEEE Commun Mag 2003;41(5):114–8. http://dx.doi.org/10.1109/MCOM.2003.1200110.

[52] Sendin A, Llano A, Arzuaga A, Berganza I. Field techniques to overcome aggressive noise situations in PLC networks. In: 2011 IEEE International symposium on power line communications and its applications. 2011, p. 113–7. http://dx.doi.org/10.1109/ISPLC.2011.5764374.

[53] Nizigiyimana R, Lebunetel J, Raingeaud Y, Achouri A, Ravier P, Lamarque G. Characterization and modeling breakers effect on power line communications. In: 18th IEEE International symposium on power line communications and its applications. 2014, p. 36–41. http://dx.doi.org/10.1109/ISPLC.2014.6812340.

[54] HomeGrid Forum. PLC Neighboring Networks Interference, URL https://homegridforum.org/wp-content/uploads/2018/09/4oMq.pdf.

[55] Sharma K, Saini LM. Power-line communications for smart grid: Progress, challenges, opportunities and status. Renew Sustain Energy Rev 2017;67:704–51. http://dx.doi.org/10.1016/j.rser.2016.09.019, URL http://www.sciencedirect.com/science/article/pii/S1364032116305111.

[56] Kikkert CJ. MV to LV transformer PLC bypass coupling networks for a low cost smart grid rollout. In: 2011 IEEE PES Innovative smart grid technologies. 2011, p. 1–6. http://dx.doi.org/10.1109/ISGT-Asia.2011.6167075.

[57] Sendin A, Peña I, Angueira P. Strategies for power line communications smart metering network deployment. Energies 2014;7(4):2377–420.

[58] Mlynek P, Misurec J, Silhavy P, Fujdiak R, Slacik J, Hasirci Z. Simulation of achievable data rates of broadband power line communication for smart metering. Appl Sci 2019;9(8):1527.

[59] Zhang J, Duong TQ, Marshall A, Woods R. Key generation from wireless channels: A review. IEEE Access 2016;4:614–26.

[60] Wang T, Liu Y, Athanasios A. Survey on channel reciprocity based key establishment techniques for wireless systems. Wirel Netw 2015;21(6):1835–46.

[61] Pittolo A, Tonello AM. Physical layer security in PLC networks: Achievable secrecy rate and channel effects. In: 2013 IEEE 17th International symposium on power line communications and its applications. 2013, p. 273–8.

[62] Pittolo A, Tonello AM. Physical layer security in power line communication networks: an emerging scenario, other than wireless. IET Commun 2014;8(8):1239–47.

[63] Cano C, Pittolo A, Malone D, Lampe L, Tonello AM, Dabak AG. State of the art in power line communications: From the applications to the medium. IEEE J Sel Areas Commun 2016;34(7):1935–52.

[64] Wang X, Gao X. The typical designs of PLC network in MV distribution network. In: 2012 IEEE International symposium on power line communications and its applications. 2012, p. 19–23. http://dx.doi.org/10.1109/ISPLC.2012.6201332.

[65] Slacik J, Mlynek P, Fujdiak R, Musil P, Voznak M, Orgon M, et al. Capabilities and visions of broadband power-line in smart grids applications. In: 2019 20th International scientific conference on electric power engineering. 2019, p. 1–5. http://dx.doi.org/10.1109/EPE.2019.8777935.

[66] Solaz M, Simon J, Sendin A, Andersson L, Maurer M. High availability solution for medium voltage BPL communication networks. In: 18th IEEE International symposium on power line communications and its applications. 2014, p. 162–7. http://dx.doi.org/10.1109/ISPLC.2014.6812375.

[67] Hallak G, Frauenrath T, Mengi A. Security concepts based on IEEE 802.1x for g.hn broadband PLC access networks. In: 2020 IEEE International symposium on power line communications and its applications. 2020, p. 1–6. http://dx.doi.org/10.1109/ISPLC48789.2020.9115402.

[68] Galli S, Scaglione A, Wang Z. Power line communications and the smart grid. In: 2010 First IEEE international conference on smart grid communications. 2010, p. 303–8. http://dx.doi.org/10.1109/SMARTGRID.2010.5622060.

[69] Schwager A, Stadelmeier L, Zumkeller M. Potential of broadband power line home networking. In: Second IEEE Consumer communications and networking conference, 2005. CCNC. 2005. 2005, p. 359–63. http://dx.doi.org/10.1109/CCNC.2005.1405197.

[70] Papaioannou A, Pavlidou F. Evaluation of power line communication equipment in home networks. IEEE Syst J 2009;3(3):288–94. http://dx.doi.org/10.1109/JSYST.2009.2023202.

[71] Deka D, Talukdar S, Chertkov M, Salapaka MV. Graphical models in meshed distribution grids: Topology estimation, change detection limitations. IEEE Trans Smart Grid 2020;11(5):4299–310.

[72] Guanghua T, Xingang W, Gang W. Topology analysis based on concentrated meter reading for low voltage district. In: 2016 3rd International conference on information science and control engineering. 2016, p. 1454–6.

[73] Raponi S, Fernandez JH, Omri A, Oligeri G. Long-term noise characterization of narrowband power line communications. IEEE Trans Power Deliv 2022;37(1):365–73. http://dx.doi.org/10.1109/TPWRD.2021.3060174.

[74] Fliss MR, Hernandez Fernandez J, Omri A, Oligeri G. NB-PLC successful transmission probability analysis. In: 2019 2nd International conference on smart grid and renewable energy. 2019, p. 1–6. http://dx.doi.org/10.1109/SGRE46976.2019.9020694.

[75] Omri A, Hernandez Fernandez J, Sanz A, Fliss MR. PLC channel selection schemes for OFDM-based NB-PLC systems. In: 2020 IEEE International symposium on power line communications and its applications. 2020, p. 1–6. http://dx.doi.org/10.1109/ISPLC48789.2020.9115404.

[76] Microchip Technology Inc. PL360-EK host controller. 2019, PL360.

[77] PRIME Alliance TWG. Specification for PoweRline intelligent metering evolution, R1.4. 2014.

[78] UVAX Concepts sl. Match+ COM-GPL module. 2021, Match+.

[79] L. Lampe AMT, Swart T. Power line communications: principles, standards and applications from multimedia to smart grid. John Wiley & Sons; 2016.

[80] ITU-T. Recommendation ITU-t g.9904; narrowband orthogonal frequency division multiplexing power line communication transceivers for PRIME networks. 2013.

[81] ITU-T. Unified high speed wireline based home networking transceivers - power spectral density specification. 2011.

[82] Takmaz E. Impedance, attenuation and noise measurements for power line communication. In: 2016 4th International istanbul smart grid congress and fair. 2016, p. 1–4.