Chapter 13: Internet of Things on Power Line Communications: an Experimental Performance Analysis

Luca DAVOLI[1,§], Luca VELTRI[2], Gianluigi FERRARI[3], Umberto AMADEI[4]

Abstract The giant information exchange enabled by the Internet of Things (IoT) paradigm, i.e., by a "network of networks" of smart and connected devices, will likely exploit electrical lines as a ready-to-use infrastructure. Power Line Communications (PLC) have received a significant attention in the last decade, as electrical lines are not used as simple energy supply media, but as information carriers. Among the different aspects of PLC-based architectures, an interesting and important analysis have to be reserved to security aspects that should be adopted in similar infrastructures, having that they are crucial to deliver trustworthy and reliable systems and, hence, to support users relying on available services, especially in case in which they should be inherently secure at the physical level (e.g., against unauthorized signal removal/interruption and eavesdropping, since they are difficult and dangerous). Motivated by the relevant impact of PLC on IoT, in this chapter we investigate experimentally the performance of IoT systems on PLC in indoor environments, considering a vendor-provided application tool and a self-developed Java library. The experimental tests are carried out on both cold and hot electrical lines, evaluating both fixed-size and variable-length power lines. Our results show that IoT-oriented PLC can reach a throughput of 8 kbps on a 300 m cold line and of 6 kbps on a 300 m hot line. Further experimental efforts will be oriented to performance analyses in presence of the adoption of security measures.

Keywords IoT, PLC, Performance, Experimental Analysis, Smart Grid.

[§]Corresponding Author

[1]Department of Engineering and Architecture, University of Parma, Parco Area delle Scienze, 181/A, 43124, Parma, Italy (IT), luca.davoli@unipr.it

[2]Department of Engineering and Architecture, University of Parma, Parco Area delle Scienze, 181/A, 43124, Parma, Italy (IT), luca.veltri@unipr.it

[3]Department of Engineering and Architecture, University of Parma, Parco Area delle Scienze, 181/A, 43124, Parma, Italy (IT), gianluigi.ferrari@unipr.it

[4]Tesmec Automation srl, Via Emilia Ovest, 61 – Frazione Rimale, 43036, Fidenza, Italy (IT), umberto.amadei@tesmec.com

13.1. Introduction

Power Line Communications (PLC) are mainly related to the use of existing electrical cables to transport data and have been investigated for a long time. Power utilities based their business on this technology for a long time to send or receive (limited amounts of) data on the existing power grid. Although PLC is mostly limited by the type of propagation medium, it can rely on existing wiring in the distribution network. This opens new opportunities and new forms of interactions among people and things in many application areas (e.g., smart metering services and energy consumption reporting, traversing the power line wires to reach data concentrators), making the PLC medium an enabler for sensing, automation, and control in large systems spread over relatively wide areas (e.g., smart city and smart grid scenarios) [1]. On top of PLC, one can adopt also enabling technologies that can improve smart automation processes, such as Internet of Things (IoT). For instance, the adoption of the PLC technology in industrial scenarios (e.g., remote control in automation and manufacturing companies) paves the way to the concepts of Industrial IoT [2] and Industry 4.0 [3]. Several applications are enabled by the following key feature of PLC technology: its ability to recover from network changes (in terms of repair/improvement, physical removal, and transfer function) mitigating the fallout on the signal transmission.

In this chapter, an experimental analysis on the joint adoption of PLC and IoT paradigms is presented, considering a state-of-the-art PLC modem transferring data according to the G3-PLC protocol [4]. In particular, on-field experimental performance evaluations in indoor environments are provided, considering two options. The former is based on the adoption of an application developed by the vendor of the chosen PLC modems. The latter is based on the adoption of a self-developed software (Java-based) library that allows to interact with the chosen PLC modems and to transmit data (obtained by on-board sensors equipping the used IoT devices) through the electrical line. The experimental tests rely on the transmission of packets with sizes compatible with IoT scenarios, on both cold and hot electrical lines, in order to estimate the throughput in different electrical conditions, and adopting different physical modulations (proposed by Internet standardization entities). The obtained results show that the highest achievable throughput is 6 kbps and 8 kbps with hot and cold lines, respectively. Our results show that Eight Phase-Shift Keying (8PSK) is the modulation format that allows to obtain the best performance.

The rest of this chapter is organized as follows. In Section 13.2, an overview of related works, in conjunction with the integration between IoT and PLC paradigms, are presented. In Section 13.3, an overview on security mechanisms in IoT and PLC are presented. In Section 13.4, an experimental performance analysis on electrical lines is investigated, considering meaningful realistic communication scenarios. Finally, in Section 13.5 we draw our conclusions.

13.2 Overview and Related Works

The IoT can be defined as a "network of networks" of physical devices connected in an Internet-like structure, thus enabling them to collect, exchange and process data. This gigantic information exchange enables new opportunities and new forms of interactions among things and people. In particular, in the last years the services over the IoT have evolved due to the needs identified by the new interactions (e.g., People-to-People, People-to-Machine and Machine-to-Machine (M2M) interactions). Therefore, a crucial enabler for IoT is represented by the availability of scalable and efficient mechanisms that minimize the need for external human intervention for configuration and maintenance of deployed objects [5], also exploiting the pervasive and ubiquitous computing concepts [6]. In this way, the IoT paradigm allows to join real and virtual worlds, especially when combined with other technologies, such as mobile and sensing technologies, and home networking applications (e.g., smart metering) [7]. The joint adoption of IoT and PLC concepts allows to rely on IoT protocols (e.g., Constrained Application Protocol (CoAP) [8], HyperText Transfer Protocol (HTTP), Constrained Session Initiation Protocol (CoSIP) [9,10]) over power lines. This has relevant implications on smart infrastructure management [11].

13.2.1 PLC Specifications and Regulations

Over the past several years, there have been intense research activities on modelling power line channels. Due to a significant interest in adopting the low-frequency bands for communication in PLC scenarios (from 20 kHz to 500 kHz), various standardization institutes have defined several PLC bands to regulate the frequency utilization, as illustrated in Fig. 13.1. Furthermore, the European Standard EN50065, proposed by the Comité Européen de Normalisation Électrotechnique (CENELEC) [12], has divided the low frequency power line spectrum, between 3 kHz and 148.5 kHz, into four different frequency bands, referred to as, respectively:

- "CENELEC A" frequency band: 3 kHz $\leq f \leq$ 95 kHz;
- "CENELEC B" frequency band: 95 kHz $< f \leq$ 125 kHz;
- "CENELEC C" frequency band: 125 kHz $< f \leq$ 140 kHz;
- "CENELEC D" frequency band: 140 kHz $< f \leq$ 148.5 kHz.

In Japan, the regulatory entity named Association of Radio Industries and Businesses (ARIB) [13] has defined an available PLC transmission band between 10 kHz and 450 kHz. In the United States, the whole spectrum between 10 kHz and 490 kHz has been allocated to one wideband channel by the regulatory entity named Federal Communications Commission (FCC) [14]. In China, the spectrum between 3 kHz and 500 kHz has been defined as single transmission band for PLC

applications, with the portion of the spectrum between 3 kHz and 90 kHz which is specifically reserved by the regulatory entity named China Electric Power Research Institute (EPRI) [15].

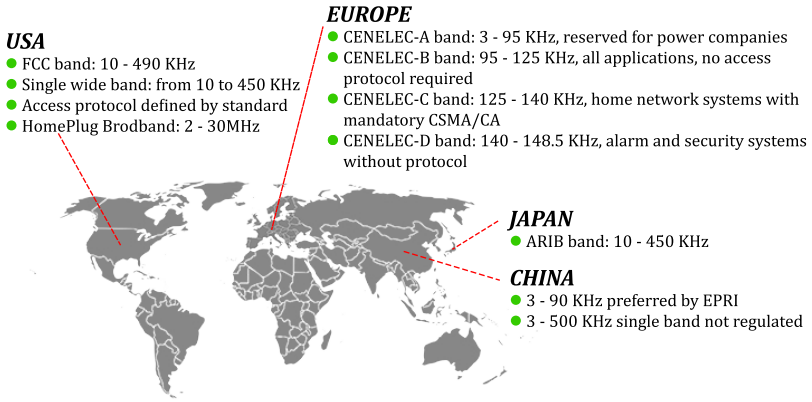

Fig. 13.1. PLC bands.

Following these band allocations, different physical layer protocols have been recently defined, to support data transmission in the low frequency bands, and further adopted by different PLC modems vendors (e.g., Texas Instruments (TI) [16], Maxim Integrated [17], STMicroelectronics [18]). We now summarize the main protocols to date, as shown in Table 13.1.

- PoweRline Intelligent Metering Evolution (PRIME) specification [19]: intended for PLC-based modems operating in the frequency range between 42 kHz and 88 kHz using Orthogonal Frequency-Division Multiplexing (OFDM).
- HomePlug specification [20]: operating at frequencies up to 400 kHz.
- G3-PLC specification: intended for PLC-based modems operating in a sub-frequency range of the “CENELEC A” band, from 35 kHz to 91 kHz.
- G.hnem specification [21]: drafted by the International Telecommunication Unit (ITU) and selecting G3-PLC and PRIME specification as two annexes to its main body.
- IEEE P1901.2 specification [22]: defined by the Institute of Electrical and Electronics Engineers (IEEE) and adopting G3-PLC and PRIME specifications as two profiles for PLC communication.
- PLCLite protocol [23]: proprietary protocol available on TI-based PLC modems and operating in the frequency range between 42 kHz and 88 kHz using OFDM.
- FlexOFDM protocol [24]: TI proprietary protocol intended for PLC-based modems using OFDM scheme and combining the strengths of PRIME and G3-PLC with variable bandwidth capabilities, adaptive tone mask capabilities, advanced modulation schemes, and the ability to work with an application-specific stack to provide high performance.

Table 13.1. Main PLC protocols.

PLC protocol	*Technology*	*Band Occupied*
PRIME	OFDM	42 – 88 kHz
HomePlug	OFDM	2 – 30 MHz
G3-PLC	OFDM	35 – 91 kHz
G.hnem	OFDM	2 – 25 MHz
IEEE P1901.2	OFDM	> 2 MHz
PLCLite	OFDM	42 – 88 kHz

13.2.2 Related Works

In the last years, the PLC paradigm has been investigated in terms of its applicability to modern communication scenarios. An overview on the role of communication and networking technologies in the transformation of existing electric power systems into smart grid is proposed in [25] where, after discussing on the key drivers for the development of smart grids (including reliability, timeliness, and data management services), a data-centric perspective for enhancing communications in this field is then adopted.

In [26], the enabling technologies for smart grids and a possible roadmap for their profitable evolution are discussed, motivated by the fact that quest for sustainable energy models is an important research driver for smart grids. Furthermore, an analysis on how current standard solutions (carried out by Internet standardization partners such the Internet Engineering Task Force (IETF) [27], the European Telecommunication Standards Institute (ETSI) [28] and the World Wide Web Consortium (W3C) [29]) can be engineered into a system, that fulfills the needs of the smart grid vision, leads the authors of [26] to the suggestion of using small and resource-constrained devices (namely, IoT), with pervasive computing capabilities, as key components to implement an energy control system.

Another comprehensive overview on PLC in the context of smart grid is proposed in [30], where network control problems inherent to smart grids are discussed. The PLC channel is modelled as a fading channel and, relying on this approach, control and traffic models are investigated in order to achieve a better understanding of the communications requirements needed in the PLC field [31].

Investigating the available protocols for PLC, in [32] an overview on the physical layer of two different PLC protocols is presented, trying to address the requests of emerging standards on Narrowband PLC (NB-PLC) [33,34]. The proposed theoretical analysis, aimed at selecting the best PLC protocol, is supported by simulation results. The application of NB-PLC in smart grids is also investigated in [35], comparing the benefits and drawbacks of PLC technology with respect to other communication solutions in energy distribution networks. NB-PLC is

shown to be suited for Medium-Voltage (MV) networks, due to their vast and complex geographical extension [36]. In [35], an analysis of the impact of channel and topological characteristics of MV distribution networks on the design and implementation of the PLC infrastructure is also presented. Another overview of PLC for smart grids is presented in [37,38], where current protocols for PLC scenarios are investigated to derive design guidelines for future standards.

A computational tool, able to simulate PLC systems for access applications in a smart grid scenario, is proposed in [39]. This tool is an event-based network simulator implemented in C++ language using OMNeT++ simulator [40], and can be used to off-line test a PLC network before a real deployment. However, this tool allows to adopt only a single signal modulation and cannot be used in a real scenario. An extensive overview on PLC technologies and their integrability with IoT is presented in [41]. The authors conclude that there is no need for additional wires to power devices (e.g., in buildings with an already available data concentrator, there is no need of smart meters), thus motivating the following choices: (i) adoption, by most electrical utilities, of the PLC paradigm for their smart grid projects, and (ii) adoption, by most cities, of ubiquitous computing and PLC for their smart street lighting projects.

An example of application of IoT in smart grids is represented by the Power Internet of Things (PIoT) concept [42,43]. Through wired or wireless communication network and smart information processing in power grid system, PIoT can achieve reliable information transmission, and it can be widely applied in every aspect of smart grid (e.g., electricity production, transmission, distribution and consumption). Moreover, PIoT [44] architecture is intended to directly monitor High-Voltage transmission lines (that are weather-sensitive and can paralyze large area power supply systems) through two main components: one component is installed along with the transmission wires to monitor the status of the conductors, while the other component is installed on the transmission towers to monitor the environment and the states of the towers.

13.3 Security Mechanisms in PLC

As previously highlighted, one of the natural roles of the PLC is to provide communication between equipments connected to the power line, thus supporting a communication network in different scenarios and, especially, in residential areas, paving the way to smart homes scenarios. Another role of the PLC is to provide a way for smart monitoring and managing the electrical grid itself (i.e., in a smart grid scenario). This connecting to the Internet new PLC-based applications that, in turn, will take advantage of all the possibilities made by IoT- and Web of Things (WoT)-enabled scenarios [45,46]. This allows to create a set of innovative services on top of PLC, in turn representing a potential added-value for customers.

However, new services' acceptance by end-users depends on several factors, among which trustworthiness plays a key role [47].

Smart grid-oriented networks can be thus classified based on the extent of monitored area, as well as on the technologies that should be adopted to manage the communications among the nodes in the networks [48].

- Home Area Network (HAN): proper of the consumer domain and consisting of electronics appliances which communicate (statistical) data to central collectors through different communication technologies, such as Bluetooth, IEEE 802.15.4 [49], IEEE 802.11 [50], IEEE 802.3 [51], and PLC. In turn, these central collectors must send their collected data to the central gateway, placed in the electricity grid, for control, monitoring, fault detection and billing purposes.
- Neighborhood Area Network (NAN): covers the task of communicating the information received by peripheral collectors to a higher-level aggregator infrastructure that, in turn, oversees managing and analyzing this information. Moreover, each NAN can few hundreds of devices deployed in HANs, in turn connected together through several NANs.
- Wide Area Network (WAN): groups various NANs, typically cover thousands of square miles, and collecting data from these peripheral networks for analysis and monitoring purposes.

Beyond the specific network, the concept of trust has been a research topic in several disciplines, with the main challenge of introducing features and properties that can support trust in the behaviour of a system, as well as providing support in case of breakdowns and maintaining a certain Quality of Service (QoS). Unfortunately, it is well-known that PLC security aspects have been addressed only in a limited way, due to its wired nature. However, security aspects will be crucial to deliver trustworthy and reliable systems and, hence, to support users relying on reliable services. Moreover, PLC has unique attributes in terms of security applications, being inherently secure at the physical level (e.g., unauthorized signal removal/interruption and eavesdropping are difficult and dangerous).

Based on these concepts, innovative applications that may take advantage of PLC technology could be the following:

- remote monitoring of security nodes;
- connection and control of active and passive alarm switches in building automation scenarios;
- access control monitoring;
- audio and video surveillance;
- authentication and authorization of individual access for site control.

The primary advantage of using PLC in the above scenarios lies in low cost of installation and simplicity, coupled with the security brought by communication on electrical distribution cables. However, when a PLC network is connected to

other networks (through routers), various network vulnerabilities emerge. An attacker can thus exploit these vulnerabilities and attack the owner of the system, as well as the end-users of the system itself. Particularly, this can happen when the system is connected to larger networks, such as those represented by the union of different IoT-oriented networks into a global Internet-like "network of networks." This means that new concerns on the trust in the system behaviour emerge, such as those related to integrity, privacy, and security [52]. It should be noted that is almost impossible to detect malicious behaviours by simply testing individual components of the system. Therefore, a continuous monitoring activity on the overall infrastructure (e.g., the electrical grid) is essential and fundamental against malicious intruders [53].

Thus, it is possible to classify the following security issues that can affect a communication system based on their effect:

- *threat*: is exemplary of any potential occurrence, malicious or not, that can have an undesirable effect on resources associated with an electronic system;
- *vulnerability*: an unfortunate feature that makes a threat potentially occur;
- *attack*: corresponds to an action taken by a malicious intruder and exploiting few vulnerabilities to make an existing threat to occur on a target infrastructure.

Threats to a network system take specifically into account the distributed aspects of data transmission and routing. In general, as well as with specific reference to a PLC network, it is possible to identify the following types of threats that may affect a system.

- Network security threats, which are typically due to the distributed nature of the PLC networks.
- Integrity threats, involving any unauthorized change to information stored on a system or in transit between communication systems.
- Disclosure threats, involving the dissemination of information to an individual by whom that information should not be known in any form.
- Denial of Service (DoS) threats, arising whenever access to some resources is intentionally blocked because of malicious actions taken by another user, as well as because of a multitude of simultaneous malicious actions (e.g., bombing hacks), defined as Distributed DoS (DDoS) threat.

As could be easily imagined, the definition, deployment and maintenance of trustworthy systems include different intermediate steps, such as: (i) vulnerability analysis and assessment of the system; (ii) definition of the system perimeter that should be protected; (iii) development and evaluation of threat models related to the system to be protected; and (iv) deep analysis to take appropriate security measures at an appropriate risk level. Selection of appropriate technologies (cryptography, key management, etc.) allows to protect a PLC network against unintended disclosure, integrity, DoS, and network threats [54]. Other crucial factors for the implementation of trustworthy systems are mechanisms supporting accountability (e.g., Authentication/Authorization/Accounting (AAA) [55]) and lia-

bility [56]. Issues of ownership and responsibilities, together with mechanisms of authentication and non-repudiation, are fundamental in large-scale scenarios like those represented by PLC scenarios.

For small-scale scenarios, in the last years different symmetric key-based security mechanisms have been defined and implemented, due to their simplicity in providing security. Unfortunately, in large-scale infrastructures, such as those proper of the PLC paradigm, this choice suffers of different issues, and it is advisable to adopt public/private key-based distribution and device authentication schemes (such as Identity-based Cryptography (IBC) [57]), in order to use public key-based security schemes in these scenarios. In the case of Identity-based Security (IBS), by eliminating the needs of public key certificates, these schemes can reduce the complexity of deploying and managing authentication credentials.

From a security viewpoint, PLC communication systems are similar to short-range radio communication systems, such as Bluetooth, Wi-Fi and Ultra-Wide Band (UWB) [58,59]. However, there are the following differences that make security enforcement in PLC scenarios interesting, as follows.

- Several devices, which the PLC aims at connecting together (e.g., PCs, routers, alarm systems, etc.), may not present a graphical interface: security should thus be inherently and internally analyzed and supported.
- While short-range radio-provided devices are inherently range-limited, PLC networks may become unmanageable and may require to be partitioned into logical subnetworks (which correspond to physical subnetworks). This could be the case of an entire building, in which all devices can assemble themselves into a single network.
- The physical layer provided by different PLC modulation schemes may provide, even if already integrated, a certain amount of security even in the absence of cryptography. This is obtained by basically acting in two different modes: (i) broadcast mode, in which, in case of simultaneous transmission of two stations, the low transmission bitrate is likely to be detected; and (ii) normal mode, in which a higher bitrate is used, but requiring a selective adaptation of tone maps (bit loading choices per carrier) for each communication direction over each link.

There exist several examples of security methods for PLC defined in technical specifications. In the HomePlug specification, different secure modes have been defined, namely: secure mode, insecure mode, user-confirm mode, lock-down mode, all adopting Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) [60] or 1024-bits Rivest–Shamir–Adleman (RSA) algorithm [61] for data encryption/decryption. In Open PLC European Research Alliance (OPERA) [62,63], Diffie-Hellman algorithm [64] has been chosen as secret key agreement, and Data Encryption Standard (DES) algorithm [65] as encryption method, together with the definition of a RADIUS server-based authentication system. The National Institute of Standards and Technology (NIST) [66] presented standards,

strategy and requirements for smart grid cybersecurity in 2010. The USA established the security requirements for the Advanced Metering Infrastructure (AMI) in December 2008. The European Union (EU) promoted the security in smart grid in different projects, such as "SmartGrids: European Technology Platform" [67] and "OPEN meter" [68]. The International Electrotechnical Commission (IEC) [69] presented a smart grid-oriented framework in 2010, including on overview of existing standards and future requirements, and recommendations for evolution.

As previously detailed, most of the above security specifications use symmetric key-based authentication and encryption systems, which result to be simple if used in small-scale scenarios, but, unfortunately, suffer of various limitations in large-scale scenarios. Because of this drawback, most applications may use public key-based techniques and an underlying Public Key Infrastructure (PKI) in case of large-scale networks. Public key-based schemes properly work using asymmetric key pairs $\{K_U, K_P\}$, of which one of the keys of the pair, namely the public key K_U, is made publicly available, while the other key, namely the private K_P, is kept private. In this way, since K_U is publicly shared, there is no need of secure key exchange algorithms; instead, there is a need for an infrastructure to distribute K_U in a secured way, and this may be done through a PKI, in which the Certification Authority (CA) is the core component, since it oversees managing the status of the issued certificates to each end device in its administrative domain. Due to their characteristics, public key-based schemes are used by several security protocols to support the establishment of the session keys, required to provide confidentiality and integrity, as well as for initiating sessions among the parties involved in the traffic exchange. It follows that the key point for these public key-based techniques is their ability to provide end-to-end security between two unknown parties, which stay unaware of the context in which they have to interact.

A possible public key-based approach, as mentioned above, is represented by the IBC, in which the public key K_U, proper of each network entity, could be predetermined by information that uniquely identifies it (e.g., its MAC address, IP address, Data Universal Numbering System (D-U-N-S) identifier [70], etc.), thus reducing the complexity of managing and deploying authentication credentials. Unlike CA-based approach, in which a binding between the device's identity and its public/private keys pair is needed, in IBS-oriented systems this binding is useless, since one derive the keys directly from the identity itself. More in detail, each entity participating in a network (e.g., connected to a PLC network) sends its identity to a trusted third-party component, denoted as Key Generation Center (KGC), to obtain its proper private key K_P, in turn calculated using the private key of the KGC, denoted as $K_{P,KGC}$, and the identity of the device, namely ID_D. It follows that the KGC oversees escrow keys, knowing all the private keys.

With respect to traditional public/private keys-oriented mechanisms, is possible to highlight the following features on IBS.

- Efficiency: using information that uniquely identify a device, IBS can provide security also to network components that do not allow user, as well as to devices whose security should be provided with a high-power consumption.
- Forward security: being based on the adoption of the Diffie-Hellman key exchange algorithm, IBS allows to keep the forward security among the network nodes and inside the overall architecture.
- Managing overhead: householders and electrical power companies can reduce management overheads implementing security solutions that decrease the amount of operations that should be done on the overall infrastructure.
- Computation overhead: since network devices are often equipped with constrained CPUs, not always capable of public-key cryptography, the capability to decrease the computational operations needed to assure security features in a communication system is an added value.

A reference application in large-scale scenario like the one represented by PLC is smart metering, since PLC communications do not require a separate communication line, can rely on the existing electrical grid infrastructure, and allow users to easily connect measuring devices to the PLC network by plugging the power cable into an electrical outlet [71]. As obvious, data recorded from each connected device should be protected against possible tampering attempts from attackers sniffing the traffic on the electrical grid, that may adopt different attack techniques. In this context, it is possible to adopt some of the previously highlighted security techniques, as well as to define newer mechanisms that may contemplate: (i) key generation and provisioning to devices without exposure, (ii) devices initialization, in order to authenticate them in the network, and key sharing between devices before exchanging data, (iii) secure transmission of collected data, and (iv) key revocation management to handle discarded devices from the network, thus preventing points of failure and reducing DoS attacks' risks against central collector points [72].

In these contexts, an intruder may attack a PLC-based system in different ways, the weakest of which are eavesdropping-based and Man-In-The-Middle (MITM) attacks between network nodes; in these scenarios, the attackers can collect only encrypted data readings. Following this approach, it is possible to classify the attacks, based on their strengthness, as follows.

- Ciphertext Only Attack, in which the attacker tries to deduce the decryption key or the plaintext by eavesdropping the ciphertext.
- Known Plaintext Attack, in which the intruder collects different pairs of plaintext/corresponding ciphertext, obtaining them by reading the output of the device and then eavesdropping the encrypted value.
- Chosen Plaintext Attack, in which the attacker can choose a pair of plaintext/corresponding ciphertext among a set of pairs.

- Chosen Ciphertext Attack, in which an attacker tries to gather information of plaintexts by obtaining the decryptions of chosen ciphertexts, thus attempting to recover the secret key used for decrypting the message.

Upon definition of the above attacks types, it is possible to classify the scopes of an attacker as follows: (i) to forge the encrypted traffic in an authenticated manner; (ii) to estimate the data reading that is encrypted and then transferred through the electrical line; (iii) to determine the symmetric secret key, or the asymmetric private key, of a network device; and (iv) to overload the sink gateway by using massive attacks, such as DoS or DDoS.

Finally, as stated before, as the wireless communication scenarios, also the PLC ones are intrinsically broadcast, and it is important to offer adequate data transmission rates, as well as to grant security, especially in multi-users contexts, in which the confidentiality of transactions and communications is a primary requirement [73,74]. Although cryptographic mechanisms have been defined, as highlighted before, there can be essentially two ways to strengthen and provide secrecy in a communication system: (i) at the physical layer, adopting a technique denoted as physical layer security or information-theoretic security, and (ii) at the high layers, using a mechanism known as complexity-based security.

- Information-theoretic security, which is considered unbreakable from a point of view of cryptanalysis-based attacks even if the adversary had unlimited computing power, since the adversary simply does not have enough information to break the encryption. This security mechanisms may be adopted in secret sharing schemes, in private information retrieval with multiple sources, and in scenarios in which symmetric encryption is required.
- Complexity-based security, which is the most adopted approach, since it includes all cryptographic methods and techniques (such as DES or RSA algorithms). Unlike the information-theoretic approach, the complexity-based one assumes the adversary to have constraints and limitations on available resources and computational power; a complete decryption of the ciphertext is practically unfeasible for the adversary in a reasonable time.

As previously detailed, the security issues in the field of PLC-based communications are related to: (i) confidentiality, dealing with secrecy of data communication; (ii) authentication, necessary to prevent fake messages from malicious sensor nodes, thus ensuring data authenticity; (iii) availability, in terms of consistency of services in the presence of attacks integrity, corresponding to the ability of receiving data or messages in an unaffected form at the destination; (iv) authorization, preventing unauthorized access of data to the secured system; and (v) replication avoidance, unavoidable to ensure that attackers do not put in place replay attacks, again sending old data trying to hinder the security of the system [75][76].

Recalling the different kinds of attacks previously detailed, it is possible to further classify the attacks based on several characteristics [77], as follow. Based on the access level of the adversary, attacks could be classified as follows.

- Active attacks, performed by an intruder through modification and theft of data, through the completion of some operation to hamper the availability, confidentiality, and integrity of data. Examples of active attacks may be false data injection, packet modification, node capturing, resource exhaustion, wormhole, spoofing, jamming, DoS, and sink hole.
- Passive attacks, performed by an adversary mainly through an observation of network activities, with the aim of impeding the confidentiality of the network. Examples of passive attacks may include traffic analysis, information capture, and decryption of vulnerable data.

Based on the location of the adversary, attacks may be classified as follows.

- Internal attacks, in which the adversary launches its attack from inside the range of the communication network. These types of attacks require a higher skills level, and may include examples such as physical tampering of node, and revelation of confidential information.
- External attacks, in which the intruder acts outside the range of the targeted communication network, including both physical and virtual networks. These are the most common attacks cases, with examples such as resource exhaustion, network jamming, DoS, and DDoS.

Based on the network layer at which the tampering is performed, attacks may be classified as follows.

- DoS attacks, in which a network congestion is exploited, together with possible restricted memory and constrained processing capacity, to make network resources unavailable and inaccessible. More in detail, DoS-oriented threats can be further described as follows.
  - Node capture/Physical devastation, in which physical damages on the device's case, as well as hardware and software alteration, can be performed to mutate the availability of the device itself.
  - Flooding of network resources, in which an attacker can exploit scarce resources making them unavailable for other devices.
  - Network configurations alteration, trying to falsify the characteristics of the network, to make the network unapproachable for genuine devices (e.g., network jamming, physical attacks, ambience camouflaging).
- Selective forwarding attacks, perpetrated at network layer, in which a forged node acts like an actual node, diverting traffic packets to a wrong path but selectively dropping some of them, so that it becomes difficult to identify the intrusion.
- Misdirection attacks, in which information traversing the network is routed toward fake paths, thus adversely affecting the reachability of the different devices participating in the network.

- Sinkhole attacks, operated at data link layer attack, in which an attacker joins the network contacting a genuine node, with the intent of introducing in the communication network, in the future, a fake node. In this way, when a counterfeit node attracts the network traffic, the attack is executed, leaving the fake node the ability to perform various malfunctions (e.g., dropping selective packets, dropping all packets, and altering data).
- Sybil attacks, in which a counterfeit node takes multiple identities to perform an attack, thus targeting the genuine collaboration that normally steers among network nodes and disturbing the routing and the traffic forwarding itself among trusted parties.
- Wormhole attacks, operated as a data link layer threat, in which a forged node registers all the information and forward them to wrong path. A well-known wormhole attack is Stuxnet [78,79], provided with an impressive toolkit for replicating itself while remaining undetected into the forged system. It is able to travel through different pathways (via removable media, as well as through shared network resources), thus exploiting several zero-days vulnerabilities (two of which escalate privileges to the administrator level), which, by definition, would not be defended. Finally, it uses two valid digital certificates to install a rootkit (a program which can boot up with complete control over a machine), after which a communication with particular Command-and-Control (C&C) servers is established.

In Fig. 13.2 a brief panoramic on the previously detailed attacks id depicted.

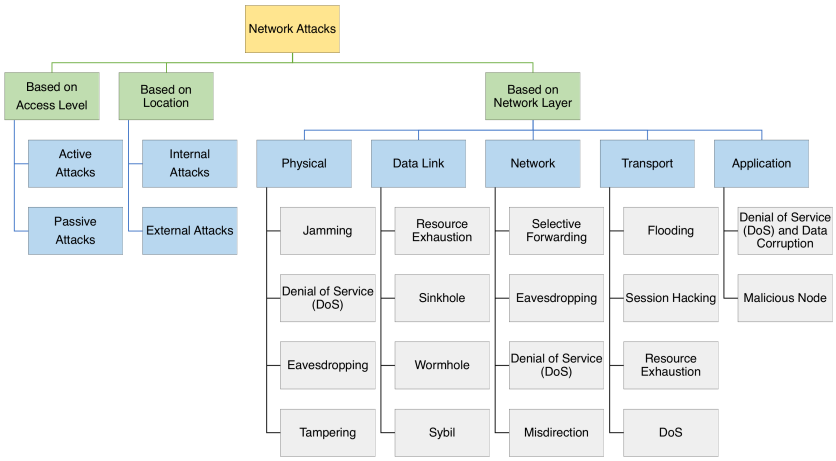

Fig. 13.2. Security attacks in function of different characteristics.

In Table 13.2, some countermeasures concerning different network layers, for a selection of possible intrusions, are shown.

Table 13.2. Security attacks and possible countermeasures, at different network layers.

Network Layer	*Security Attack*	*Countermeasures*
Application	Malicious node, DoS, DDoS, Data corruption	Malicious node detection and isolation
Transport	DoS, DDoS, Session hacking, Resource exhaustion, Flooding	Encryption, Intrusion detection
Network	Misdirection, DoS, DDoS, Eavesdropping, Selective forwarding	Topology control, Key management, Secured Routing
Data Link	Resource exhaustion, Sinkhole, Wormhole, Sybil	Link layer cryptography
Physical	Node capture, Jamming, DoS, DDoS	Spread spectrum technology

13.4 Experimental Evaluation

In order to investigate the joint integration of the PLC paradigm in an IoT scenario and to evaluate the performance of the overall communication architecture, an experimental evaluation has been carried out on a residential electrical line, in order to verify the capabilities to exchange data collected from different IoT devices (through their on-board sensors, e.g., temperature, humidity, brightness, and proximity sensors). In particular, the "CENELEC A" mask has been selected, in its 36 sub-carriers version (with adjacent sub-carrier separation $\Delta f = 1.5625$ KHz), since the other masks did not work properly on the electrical line, as verified by further experimental tests.

Among many PLC modems produced by different vendors, a PLC kit able to support both PRIME and G3-PLC protocols and provided by TI has been selected, namely the TMDSPLCKIT-V3 kit [80]. This modem allows to use different modulations (ROBO [81], a TI-provided modulation which provides repetition code; Binary Phase-Shift Keying (BPSK); Quadrature Phase-Shift Keying (QPSK); 8PSK) and can operate in a double transmission mode (*Stream*/*NO Stream*). Assuming a transmitter module (TX) and a receiver one (RX), the transmission modes work as follows:

- if the *Stream* mode is deactivated (*NO Stream* mode), the RX module has to send back an acknowledgment (ACK) message to the TX module for every received packet (slow transmission);
- if the *Stream* option is activated, the RX module has not to send back any ACK message to the TX module (fast transmission).

The experimental evaluation has been carried out by adopting the G3-PLC transmission protocol, due to its features and manageability in the chosen TI PLC modem, and has been mainly split into two phases. The former experimentation involves the adoption of an application developed by the vendor of the chosen PLC modems. The latter is based on the adoption of a self-developed software library that allows to interact with the chosen PLC modems and to transmit data (obtained by on-board sensors equipping the IoT devices) through the power line.

13.4.1 Evaluation using PLC modems as "Black Boxes"

In order to test the functionalities of the chosen PLC modem and of its APIs, an external Java-based library, denoted as *jPLC* and with which it is possible to interact with PLC modules, has been developed. This library is based, for its serial communication features, on the jSSC library [82] and needs to adhere to the TI-defined request/response "HostMessage" protocol, by which it is possible to initialize a G3-PLC-based network and to communicate over the power line. The configuration of a PLC modem is carried out through the following steps:

- system initialization (e.g., check for existing configurations, current configuration loading, system reboot);
- network configuration, required to make the modem part of an IP power line-based network (network parameters configuration, Base Node (BN) discovery, PLC module attachment to the BN);
- data transmission, in which the user transmits a "DATA TRANSFER" command to the PLC modem, which replies with a confirmation message and starts sending the message, properly encoded, on the power line.

Among other features, the *jPLC* library includes some APIs for managing the PLC modules in two distinct ways, denoted as "Point-to-Point" (P2P) and "Service Node" (SN) configurations, as follows.

- "Point-to-Point" (P2P) mode: the PLC module registers itself with the power line and waits for an input from the user; in the meantime, the PLC module can receive, in an asynchronous way, messages from another PLC module.
- "Service Node" (SN) mode: the PLC module registers itself on the power line network, waiting for a joining acknowledgment from a running BN. Once it has completed this joining step, it belongs to G3-PLC network and is addressable with an IPv6 address released by the BN, that, in this way, acts also as a Dynamic Host Configuration Protocol (DHCP) server.

Considering the P2P configuration, we have tested scenarios with two TI PLC modules, on both cold and hot lines, managing them with the *jPLC* library. In these tests, a transmitter module sends a HostMessage-based packet to a second PLC module which receives it and, then, replies to the TX with another HostMessage-based packet. The choice of experimentally performing several tests on both cold

and hot electrical lines is due to the fact that, in the case of a cold electrical line, the power line is disconnected and isolated from a real electrified line, keeping the operators protected from dangers of electric discharges and having the possibility to verify the performance and functionalities of a PLC modem in a "safe" and not disturbed scenario; in case of a hot electrical line, the power line is connected to a real and existing electrified line, with the advantage of being immersed in a real scenario, but with the main disadvantage of being sensitive to noises on the line, even more in case of highly disturbed power lines.

Regarding the SN configuration, an experimental scenario composed by a single SN (corresponding to a PLC modem) and a BN (whose features are provided by the TI Data Concentrator TMDSDC3359 [83] device) is considered. In order to prevent any damages to the BN module, the SN scenario has been deployed on a cold line. With this configuration, we experimented a successful communication, in which the BN initializes the G3-PLC network and the SN correctly joins the G3-PLC network, becoming an active member of the system. Another experimental scenario, composed of a TI Data Concentrator TMDSDC3359 as BN and with two PLC modules as SNs, has been successfully investigated. The obtained results show that, by using our *jPLC* library, one can identify both the SNs via their IPv6 addresses (assigned by the BN) and let them exchange HostMessage-based packets.

In Table 13.3, the results of several experimental tests among different offices of the School of Engineering and Architecture of the University of Parma, based on SN configuration, are reported. The performance metrics of interest in each test are: the measured distances between PLC endpoints and the transmission success.

Table 13.3. Performance results of experimental tests, using PLC modems as "black boxes" in SN configurations, among different offices.

Config.	*Line*	*Description*	*Transmission success*	*Reference*
SN	COLD	Zero distance between the PLC modems.	✓	Fig. 13.3, line (1)
SN	HOT	Same building, with 5 m between each line entry points.	✓	Fig. 13.3, line (2)
SN	HOT	Same building, on two different floors and with 15 m between each entry points.	✓	Fig. 13.3, line (3)

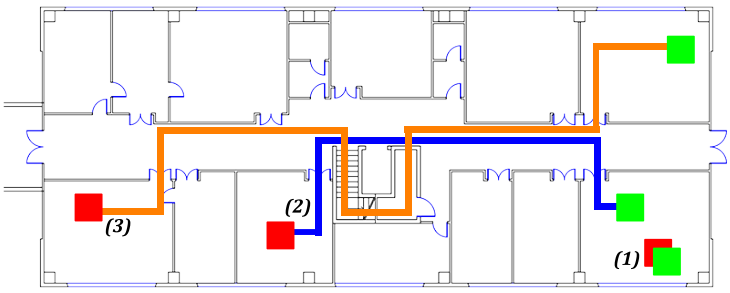

Fig. 13.3. Map of a scientific building of the School of Engineering and Architecture of the University of Parma.

In Table 13.4, the results of several experimental tests between the different scientific buildings of the School of Engineering and Architecture of the University of Parma, based on SN configuration, are reported. The performance metrics of interest in each test are: the measured distances between PLC endpoints and the transmission success.

Table 13.4. Performance results of experimental tests, using PLC modems as "black boxes" in SN configurations, between different buildings.

Config.	*Line*	*Description*	*Transmission success*	*Reference*
SN	HOT	Corridor between 2 buildings, with 50 m length.	✗	Fig. 13.4, line (4)
SN	HOT	Corridor between 2 buildings, with 25 m length.	✗	Fig. 13.4, line (5)

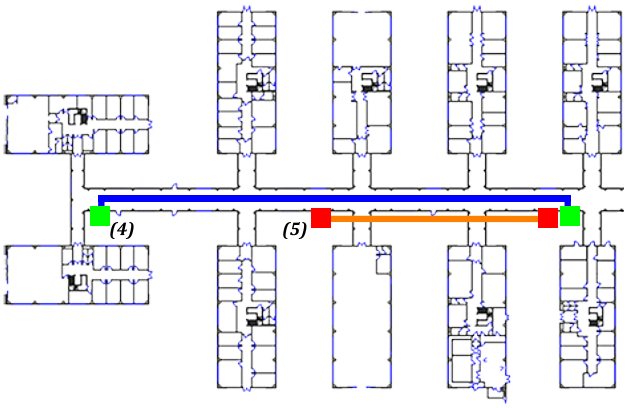

Fig. 13.4. Map of the corridor between the different scientific buildings of the School of Engineering and Architecture of the University of Parma.

In Table 13.5, the results of several experimental tests between different classes of the learning buildings of the School of Engineering and Architecture of the University of Parma, based on SN configuration, are reported. The performance metrics of interest in each test are: the measured distances between PLC endpoints and the transmission success.

Table 13.5. Performance results of experimental tests, using PLC modems as "black boxes" in SN configurations, among different classes.

Config.	*Line*	*Description*	*Transmission success*	*Reference*
SN	HOT	Same building.	✓	Fig. 13.5, line (6)
SN	HOT	Same building, with 10 m length.	✓	Fig. 13.5, line (7)
SN	HOT	Same building, with 40 m length.	✗	Fig. 13.5, line (8)
SN	HOT	Same building, with 15 m length.	✓	Fig. 13.5, line (9)
SN	HOT	Same building, with 20 m length.	✗	Fig. 13.5, line (10)
SN	HOT	Corridor between 2 classrooms at 50 m length.	✗	Fig. 13.5, line (11)

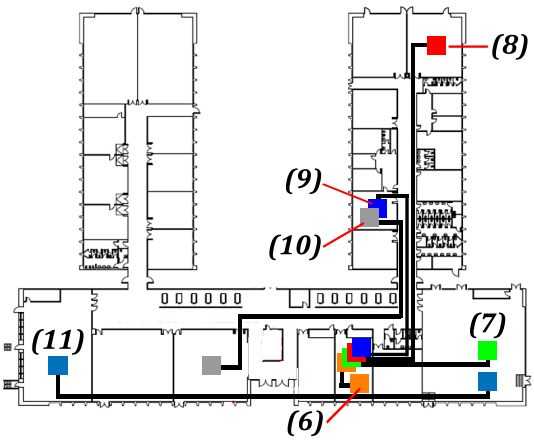

Fig. 13.5. Map of the learning buildings of the School of Engineering and Architecture of the University of Parma.

As expected, the main causes of communication failures (namely, electrical line noises and misconfigurations) are unpredictable and out of direct control.

13.4.2 Experimental Evaluation on a Supervised Electrical Line

Another experimental evaluation has been carried out by transferring an 88 Kbyte file between two PLC modems. Since each PLC transmission packet (at physical layer) has to be 256-bytes long, the transmission of an 88 Kbyte packet requires transmitting 351 PLC packets. In this case, the evaluation has been carried out, through a proper application provided by TI, on a residential hot electrical line. Different physical layer settings have been considered to test the communication on a hot line (a power strip connected and powered by the electrical residential line).

In particular, the considered configurations are the following:

- "CENELEC A 36"
- "CENELEC A 25" (use of the "CENELEC A" mask with 25 subcarriers)
- "CENELEC B"
- "CENELEC BC" (associated with a broader frequency range given by the union of "CENELEC B" and "CENELEC C" frequency bands)
- "CENELEC BCD" (obtained by the union of the "CENELEC B/C/D" masks).

The performance results, associated with the test on a hot line and the "CENELEC B" configuration, are shown in Table 13.6.

Table 13.6. Performance results (dimension: [bps]) on hot line, using default parameters, adopting different modulations, and "CENELEC B" mask.

CENELEC Mask		"B"
Packet Length		256 bytes
Modulation	*Stream*	TMR OFF
ROBO	OFF	729
	ON	902
BPSK	OFF	2984
	ON	4200
QPSK	OFF	4013
	ON	5574
8PSK	OFF	2501
	ON	5846

The performance results, associated with the test on a hot line and the "CENELEC BC" configuration, are shown in Table 13.7.

Table 13.7. Performance results (dimension: [bps]) on hot line, using default parameters, adopting different modulations, and "CENELEC BC" mask.

CENELEC Mask	"BC"	
Packet Length	256 bytes	
Modulation	*Stream*	TMR OFF
ROBO	OFF	1358
	ON	1691
BPSK	OFF	3928
	ON	5846
QPSK	OFF	✗
	ON	✗
8PSK	OFF	✗
	ON	✗

The performance results, associated with the test on a hot line and the "CENELEC BCD" configuration, are shown in Table 13.8.

Table 13.8. Performance results (dimension: [bps]) on hot line, using default parameters, adopting different modulations, and "CENELEC BCD" mask.

CENELEC Mask	"BCD"	
Packet Length	256 bytes	
Modulation	*Stream*	TMR OFF
ROBO	OFF	1617
	ON	2115
BPSK	OFF	✗
	ON	✗
QPSK	OFF	✗
	ON	✗
8PSK	OFF	✗
	ON	✗

The performance results, associated with the test on a hot line and the "CENELEC A 25" configuration, are shown in Table 13.9.

Table 13.9. Performance results (dimension: [bps]) on hot line, using default parameters, adopting different modulations, and "CENELEC A 25" masks.

CENELEC Mask		"A 25"
Packet Length		256 bytes
Modulation	*Stream*	TMR OFF
ROBO	OFF	1335
	ON	1648
BPSK	OFF	3772
	ON	5600
QPSK	OFF	4669
	ON	7374
8PSK	OFF	5148
	ON	8247

The performance results, associated with the test on a hot line and the "CENELEC A 36" configuration, and using traffic packets with 256-bytes length, are shown in Table 13.10.

Table 13.10. Performance results (dimension: [bps]) on hot line, using default parameters, adopting different modulations, and "CENELEC A 36" mask, and using traffic packets with a length of 256 bytes.

CENELEC Mask		"A 36"	
Packet Length		256 bytes	
Modulation	*Stream*	TMR ON	TMR OFF
ROBO	OFF	3389	1975
	ON	4976	2775
BPSK	OFF	3518	4568
	ON	5168	7074
QPSK	OFF	3883	5586
	ON	5487	8959
8PSK	OFF	4240	5985
	ON	5971	9807

The performance results, associated with the test on a hot line and the "CENELEC A 36" configuration, and using traffic packets with 1024-bytes length, are shown in Table 13.11.

Table 13.11. Performance results (dimension: [bps]) on hot line, using default parameters, adopting different modulations, and "CENELEC A 36" mask, and using traffic packets with a length of 1024 bytes.

CENELEC Mask		"A 36"	
Packet Length		1024 bytes	
Modulation	*Stream*	TMR ON	TMR OFF
ROBO	OFF	4501	2634
	ON	6076	3760
BPSK	OFF	4894	6661
	ON	6369	8769
QPSK	OFF	5166	8142
	ON	6789	11212
8PSK	OFF	5906	8766
	ON	7089	12344

Considering the values obtained with the inclusion of "CENELEC B" mask, it can be observed that the majority of the configurations with "CENELEC BC" and "CENELEC BCD" do not provide any data transmission. Moreover, the throughput obtained with the "CENELEC B" mask, for each configuration, is lower than the corresponding one obtained with the "CENELEC A 25" and "CENELEC A 36" masks. This is likely due, on one end, to a reduced frequency bandwidth and, on the other end, to the incompatibility between the available modulations and masks different from "CENELEC A." Although the best performance has been obtained with the "CENELEC A 36" mask, a further experimental test has been carried out considering the same settings assumed in the previous tests, except for the activation of the Tone Mask Request (TMR) option (a TI-provided setting that allows to tune the tone mask of OFDM for each currently selected frequency range). The obtained results are shown in Table 13.10.

Comparing the results obtained with activated TMR (column 1) with those with deactivated TMR (column 2), it is possible to observe that the activation of the TMR option only increases the transmission throughput when the ROBO modulation is adopted (improving it by almost 70%). At the opposite, in all other cases the throughput decreases, on the average, by approximately 35%.

Considering the "CENELEC A 36" mask (which guaranteed the highest throughput), we performed another test by increasing the PLC packet size from 256 bytes to 1024 bytes. The transmission of an 88 Kbyte file thus requires 88 PLC packets. The obtained results, with activation and deactivation of the TMR option, are reported in Table 13.11. Comparing the results with activated TMR with those obtained with deactivated TMR (more generally, with the results highlighted in Table 13.6-13.10), it can be concluded that the highest throughput (around 12 kbps) is achieved transferring a file in *Stream* mode, using the "CENELEC A 36" mask with 8PSK modulation and disabling the TMR option.

As can be observed, in general these results are in line with the expectations by the theory, in which it is expected that QPSK outperforms BPSK and, in turn, that 8PSK outperforms QPSK modulation.

13.4.3 Experiments on a Residential Electrical Line

We now focus on an experimental campaign carried out on a hot electrical line between two offices of the School of Engineering and Architecture of the University of Parma. Following the guidelines suggested by the results obtained in Subsection 13.4.2, the experimental tests have been carried out using the "CENELEC A 36" mask and transferring, between the two PLC modules, an 88 Kbyte file with 351 256-bytes PLC transmission packets (at physical layer). The results obtained with this physical layer setting, activating and deactivating the TMR option, are shown in Table 13.12.

Table 13.12. Performance (dimension: [bps]) on real hot line, transferring packets with 256-bytes length and using "CENELEC A 36" mask, and enabling and disabling the TMR option.

CENELEC Mask		"A 36"	
Packet Length		256 bytes	
Modulation	*Stream*	TMR ON	TMR OFF
ROBO	OFF	1972	1149
	ON	2723	1530
BPSK	OFF	2139	✗
	ON	2915	✗
QPSK	OFF	2466	✗
	ON	3219	✗
8PSK	OFF	2844	✗
	ON	3415	✗

The performance results on a real hot line, using the "CENELEC A 36" configuration, and using traffic packets with 1024-bytes length, are shown in Table 13.13.

Table 13.13. Performance (dimension: [bps]) on real hot line, transferring packets with 1024-bytes length and using "CENELEC A 36" mask, and enabling and disabling the TMR option.

CENELEC Mask		"A 36"	
Packet Length		1024 bytes	
Modulation	*Stream*	TMR ON	TMR OFF
ROBO	OFF	2549	2384
	ON	2990	3191
BPSK	OFF	2585	✗
	ON	3020	✗
QPSK	OFF	2878	✗
	ON	3430	✗
8PSK	OFF	3317	✗
	ON	3971	✗

The performance results on a real hot line, using the "CENELEC A 25" configuration, and using traffic packets with 1024-bytes length, are shown in Table 13.14.

Table 13.14. Performance (dimension: [bps]) on real hot line, transferring packets with 1024-bytes length and using "CENELEC A 25" mask, and enabling and disabling the TMR option.

CENELEC Mask		"A 25"	
Packet Length		1024 bytes	
Modulation	*Stream*	TMR ON	TMR OFF
ROBO	OFF	✗	✗
	ON	1175	1377
BPSK	OFF	✗	✗
	ON	1388	✗
QPSK	OFF	✗	✗
	ON	1655	✗
8PSK	OFF	✗	✗
	ON	1942	✗

Analyzing the results in Table 13.12-13.14, one can observe that the activation of the TMR option allows the communication through a real electrical line (between two different offices of our department) with all the tested modulations, with an average throughput on the order of 3.0 kbps when the *Stream* mode is enabled.

The performance results obtained increasing the PLC packet size from 256 bytes to 1024 bytes (an 88 Kbyte file requires 88 PLC packets), activating and de-

activating the TMR option, are shown in Table 13.13. Comparing the results with 256-bytes long PLC packets with those with 1024-bytes long PLC packets, it is possible to observe that, in the latter case:

- the reliability and the link quality remain the same, having that the ROBO modulation is the only enabling modulation working in both *Stream*/*NO Stream* modes;
- the adoption of a higher packet size improves links performance, showing that in a certain way the packet size's increase improves the communication performance, thus allowing the communication with all available modulations, with highest throughput (3.9 kbps) in the case of 8PSK modulation.

Also in this case, the results adhere to those expected by the theory. Furthermore, comparing these results with those in Table 13.6-13.11, it is possible to observe that: (i) with "CENELEC A 36" mask, activated TMR option, and 256-bytes packets, the performance results in Table 13.10 (column 1) are higher (almost 70%) than those in Table 13.12 (column 1); (ii) with "CENELEC A 36" mask, deactivated TMR option, and 256-bytes packet, the only operational modulation in Table 13.12 (column 2) is ROBO, while in Table 13.10 (column 2) all modulations allow data transmission; this could be due to the noises on the electrical line between the different offices identified as source and destination of the test; (iii) with "CENELEC A 36" mask, activated TMR option, and 1024-bytes packets, the performance results in Table 13.13 (column 1) are lower (almost half) than those in Table 13.11 (column 1); and (iv) with "CENELEC A 36" mask, deactivated TMR option, and 1024-bytes packet, the only operational modulation in Table 13.13 (column 2) is ROBO, while in Table 13.11 (column 2) all modulations allow data transmission, and this can be due to the noises on the electrical line.

Further experimental tests have been carried out maintaining the "CENELEC A" band and changing the mask from "CENELEC A 36" to "CENELEC A 25," thus activating and deactivating the TMR option. The corresponding results are reported in Table 13.14. Adopting the "CENELEC A 25" mask and disabling the TMR option, most of the modulations do not allow communication on the hot electrical line. The only operational configuration is the one with the ROBO modulation: however, in this case as well, the performance degrades with respect to that guaranteed by "CENELEC A 36." It can be observed that the activation of the TMR option increases the number of operational modulations (especially when the *Stream* mode is enabled), always respecting those expected by theory, in which 8PSK outperforms QPSK that, in turn, outperforms BPSK. Furthermore, by comparing the results in Table 13.12-13.14 with those in Table 13.6-13.11 (both with TMR option disabled), it can be observed that on a real hot line, the only operational modulation is ROBO, while in Table 13.6-13.11 all modulations allow data transmission.

Other transmission tests on hot power lines have led to the following results.

1. Adoption of the "CENELEC B/C/D" masks, using the same configurations of previous tests on supervised electrical line (Subsection 13.4.2): no data trans-

mission on these bands was successfully carried out, regardless of the used modulation.

2. Adoption of different masks in TX and in RX, looking for combinations which would allow the communication on the electrical line: with the “CENELEC A 36” mask in TX and the “CENELEC A 25” mask in RX, no configuration worked; with the “CENELEC A 25” mask in TX and the “CENELEC A 36” mask in RX, no communication was allowed as well.

13.4.4 Experiments on Electrical Lines with Different Lengths

We preliminary recall that it is not possible to control the exact extension and the loads on a real (walled) electrical line, as the one between different departments of the School of Engineering and Architecture of the University of Parma. Therefore, we also assembled a handmade 300 m electrical line, composed by 6 coils of 50 m-long electrical cables, as shown in Fig. 13.6.

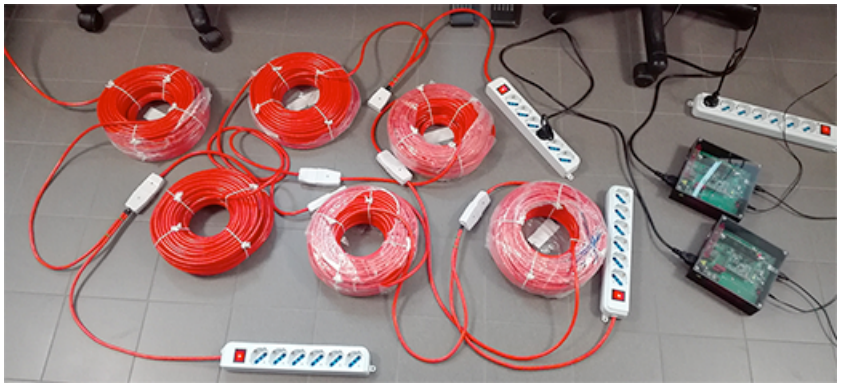

Fig. 13.6. Real deployment of an electrical line composed by different pieces of electrical cable.

Adopting the “CENELEC A 36” mask, tests were carried out with activated TMR option and using a PLC packet size equal to 1024 bytes. According to this setting, the transmission of an 88 Kbyte file requires 88 PLC packets on the electrical line.

13.4.4.1 Tests on cold electrical line

As in the test on a close-set electrical line described in Subsection 13.4.2, in this case experimental tests were carried out increasing progressively the length of the cold electrical line from 50 m to 300 m, with a 50 m step, as shown in Fig. 13.7.

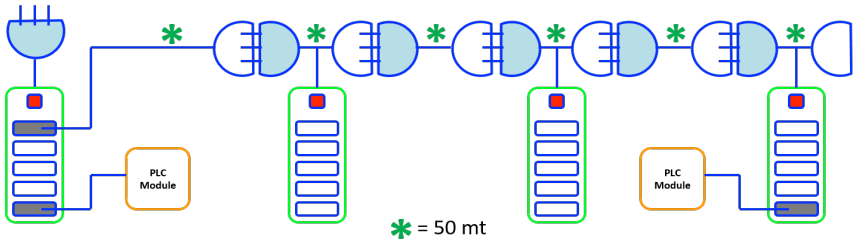

Fig. 13.7. Deployment of an electrical line composed by different segments of electrical cable.

In Table 13.15, the obtained results, considering various modulations available in adopted tool, on a cold cable, with length from 50 m to 100 m, transferring 1024-bytes packets and using "CENELEC A 36" mask, are shown.

Table 13.15. Transmission data rate (dimension: [bps]) on a cold cable, with length from 50 m to 100 m, transferring 1024-bytes packets and using "CENELEC A 36" mask.

Modulation	*Stream*	50 m cable	100 m cable
ROBO	OFF	5276	5201
	ON	7752	7560
BPSK	OFF	5589	5510
	ON	8054	7882
QPSK	OFF	6076	5859
	ON	8477	8383
8PSK	OFF	6375	6272
	ON	8769	8567

In Table 13.16, the obtained results, considering various modulations available in adopted tool, on a cold cable, with length from 150 m to 200 m, transferring 1024-bytes packets and using "CENELEC A 36" mask, are shown.

Table 13.16. Transmission data rate (dimension: [bps]) on a cold cable, with length from 150 m to 200 m, transferring 1024 -bytes packets and using “CENELEC A 36” mask.

Modulation	*Stream*	150 m cable	200 m cable
ROBO	OFF	4836	4710
	ON	7405	7260
BPSK	OFF	5444	5342
	ON	7704	7587
QPSK	OFF	5760	5669
	ON	8210	8094
8PSK	OFF	6080	5990
	ON	8416	8277

In Table 13.17, the obtained results, considering various modulations available in adopted tool, on a cold cable, with length from 250 m to 300 m, transferring 1024-bytes packets and using “CENELEC A 36” mask, are shown.

Table 13.17. Transmission data rate (dimension: [bps]) on a cold cable, with length from 250 m to 300 m, transferring 1024-bytes packets and using “CENELEC A 36” mask.

Modulation	*Stream*	250 m cable	300 m cable
ROBO	OFF	4513	4421
	ON	7005	6835
BPSK	OFF	5277	5145
	ON	7337	7055
QPSK	OFF	5595	5452
	ON	7815	7662
8PSK	OFF	5859	5759
	ON	8116	8093

In Fig. 13.8, the corresponding throughput is shown. It is possible to observe that, on a cold electrical line, the best performance is achieved transmitting the packets (e.g., data collected by IoT devices) with the *Stream* option enabled and 8PSK modulation. As expected, the obtained results on a cold electrical line are in line with those provided by the theory, in which BPSK modulation is outperformed by QPSK that, in turn, is outperformed by 8PSK modulation.

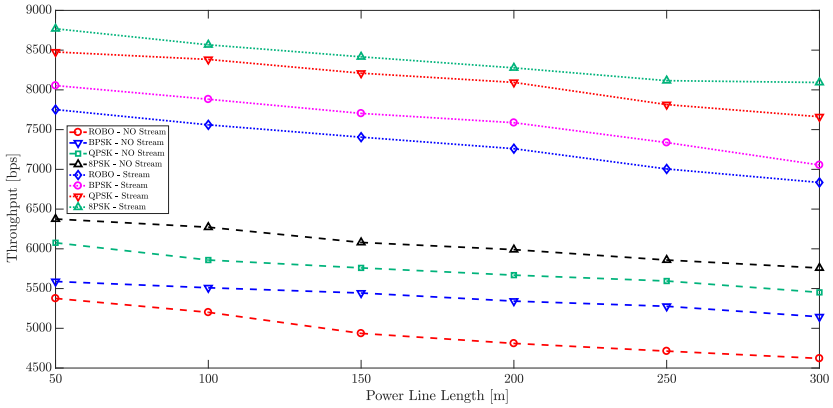

Fig. 13.8. Performance (dimension: [bps]) obtained on a cold electrical cable, transferring 1024-bytes packets and using "CENELEC A 36" mask.

13.4.4.2 Tests on a hot electrical line

The previously described handmade 300 m electrical line has thus been connected to a real hot line, attaching the electrical cables on two distinct wall outlets, at approximately 6 m, as shown in Fig. 13.9.

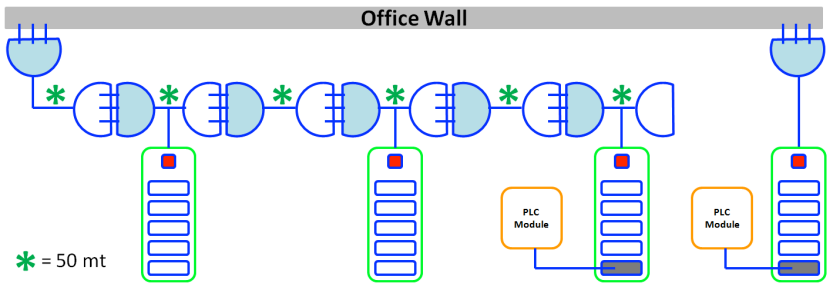

Fig. 13.9. Deployment of an electrical line composed by different pieces of cable, attached into two different wall outlets.

Experimental tests similar to those described in Subsection 13.4.4.1 were performed, increasing the length of the out-of-wall line from 50 m to 300 m, with a 50 m step. The performance results, in terms of transmission data rate (dimension: [bps]), are listed in Table 13.18-13.20 and shown in Fig. 13.10.

In Table 13.18, the obtained results, considering various modulations available in adopted tool, on a hot cable, with length from 50 m to 100 m, transferring 1024-bytes packets and using "CENELEC A 36" mask, are shown.

Table 13.18. Transmission data rate (dimension: [bps]) on a hot cable, with length from 50 m to 100 m, transferring 1024-bytes packets and using “CENELEC A 36” mask.

Modulation	Stream	50 m cable	100 m cable
ROBO	OFF	4600	4501
	ON	6067	5976
BPSK	OFF	4612	4562
	ON	6177	6075
QPSK	OFF	4879	4649
	ON	6446	6371
8PSK	OFF	5120	4800
	ON	6899	6788

In Table 13.19, the obtained results, considering various modulations available in adopted tool, on a hot cable, with length from 150 m to 200 m, transferring 1024-bytes packets and using “CENELEC A 36” mask, are shown.

Table 13.19. Transmission data rate (dimension: [bps]) on a hot cable, with length from 150 m to 200 m, transferring 1024-bytes packets and using “CENELEC A 36” mask.

Modulation	Stream	150 m cable	200 m cable
ROBO	OFF	4494	4306
	ON	5847	5778
BPSK	OFF	4510	4401
	ON	5990	5931
QPSK	OFF	4610	4504
	ON	6286	6204
8PSK	OFF	4711	4613
	ON	6686	6493

In Table 13.20, the obtained results, considering various modulations available in adopted tool, on a hot cable, with length from 250 m to 300 m, transferring 1024-bytes packets and using “CENELEC A 36” mask, are shown.

Table 13.20. Transmission data rate (dimension: [bps]) on a hot cable, with length from 250 m to 300 m, transferring 1024-bytes packets and using "CENELEC A 36" mask.

Modulation	Stream	250 m cable	300 m cable
ROBO	OFF	4295	4101
	ON	5691	5577
BPSK	OFF	4322	4208
	ON	5816	5689
QPSK	OFF	4410	4368
	ON	6121	5804
8PSK	OFF	4592	4409
	ON	6264	6087

As in Fig. 13.10, in this case as well it can be observed that, on a hot electrical line, the best performance is achieved by enabling the *Stream* option and selecting the 8PSK modulation scheme. As expected, the obtained results on a cold electrical line are in line with those provided by the theory, in which 8PSK modulation outperforms QPSK that, in turn, outperforms BPSK modulation.

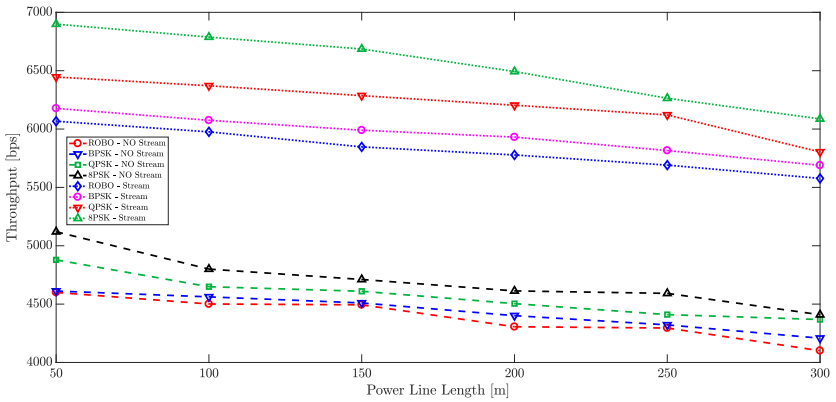

Fig. 13.10. Performance (dimension: [bps]) obtained on a hot electrical cable, transferring 1024-bytes packets and using "CENELEC A 36" mask.

Moreover, comparing the results in Fig. 13.8 (cold electrical lines) with those in Fig. 13.10 (hot electrical lines), it can be concluded that there is an obvious performance degradation, due to the unpredictable noises in a real (hot) electrical line. However, even in the latter case, the transmission rate remains acceptable (namely, 6 kbps) for relevant IoT scenarios (e.g., distributed monitoring). This motivates a joint IoT/PLC approach, as the one proposed in this chapter, not only for monitoring scenarios, but also for applications in which an already available electrical grid may provide benefits in place of having the need of new technology deployments, such as extra urban scenarios in which a power grid is present,

whereas wireless-oriented infrastructures require new deployments with high efforts and costs.

13.5 Conclusion

In this chapter, a feasibility study on the joint adoption of PLC and IoT paradigms in heterogeneous scenarios has been carried out, highlighting that the power line medium guarantees acceptable transmission data rates for IoT devices by adopting standard communication protocols (e.g., CoAP, CoSIP, HTTP). In order to validate a PLC/IoT communication strategy, an extensive experimental evaluation has been carried out using a vendor (Texas Instruments)-provided tool and a self-developed Java library, adopting the G3-PLC specification as PLC communication protocol standard. Experimental performance tests have been carried out on both cold and hot electrical lines with variable lengths. The obtained results highlight some interesting aspects: (i) the little importance of the chosen modulation when working with the "CENELEC A" mask, against the importance of choosing the correct modulation when working with the other masks; (ii) the advisable choice in transferring 1-Kbyte PLC packets, instead of 256-bytes packets, comparing the results in Table 13.6-13.11 with those in Table 13.12-13.14; (iii) an average throughput on the order of 8 kbps on cold lines (as shown in Table 13.15-13.17), and an average throughput on the order of 6 kbps on hot lines (as shown in Table 13.18-13.20), both obtained using the "CENELEC A 36" mask, activated *Stream* mode, 8PSK modulation, and 1024-bytes packets, which can support the adoption of the PLC paradigm for transferring data collected by IoT devices.

Acknowledgments The authors would like to thank Xiaolin Lu, Wonsoo Kim, Ariton Xhafa, and Andrew Soukup (Texas Instruments Research Center, Dallas, TX, USA) for the fundamental support and useful discussions.

References

[1] V.C. Gungor *et al*., "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529-539, Sep. 2011. DOI 10.1109/TII.2011.2166794

[2] S. Jeschke *et al*., "Industrial Internet of Things and Cyber Manufacturing Systems," *Industrial Internet of Things: Cybermanufacturing Systems*, Springer International Publishing, Cham, pp. 3-19, Oct. 2016. DOI 10.1007/978-3-319-42559-7_1

[3] M. Hermann *et al*., "Design Principles for Industries 4.0 Scenarios," *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 3928-3937, Jan. 2016. DOI 10.1109/HICSS.2016.488
[4] G3-PLC Alliance. URL https://goo.gl/EZA7r8 (accessed January 18, 2018)
[5] S. Cirani *et al*., "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 508-521, Sep. 2014. DOI 10.1109/JIOT.2014.2358296
[6] L. Belli *et al*., "A Scalable Big Stream Cloud Architecture for the Internet of Things," *International Journal of Systems and Service-Oriented Engineering*, vol. 5, no. 4, pp. 26-53, Oct. 2015. DOI 10.4018/IJSSOE.2015100102
[7] K. De Craemer and G. Deconinck, "Analysis of State-of-the-art Smart Metering Communication Standards," *Proceedings of the 5th young researchers symposium*. URL https://goo.gl/4SkCwa (accessed January 19, 2017)
[8] Z. Shelby *et al*., "The Constrained Application Protocol (CoAP)," *RFC 7252,* Internet Engineering Task Force (IETF), URL https://goo.gl/pJ2Ngg (accessed January 18, 2018)
[9] S. Cirani *et al*., "CoSIP: A Constrained Session Initiation Protocol for the Internet of Things," *Advances in Service-Oriented and Cloud Computing. ESOCC 2013. Communications in Computer and Information Science*, vol. 393, pp. 13-24, Sep. 2013. DOI 10.1007/978-3-642-45364-9_2
[10] S. Cirani *et al*., "Performance Evaluation of a SIP-based Constrained Peer-to-Peer Overlay," *2014 International Conference on High Performance Computing Simulation (HPCS), Bologna,* pp. 432-435, Jul. 2014. DOI 10.1109/HPCSim.2014.6903717
[11] L. Belli *et al*., "Design and Deployment of an IoT Application-Oriented Testbed," *IEEE Computer*, vol. 48, no. 9, pp. 32-40, Sep. 2015. DOI 10.1109/MC.2015.253
[12] European Committee for Electrotechnical Standardization (CENELEC). URL https://goo.gl/Vcymfn (accessed January 18, 2018)
[13] Association of Radio Industries and Businesses (ARIB). URL https://goo.gl/UK9yof (accessed January 18, 2018).
[14] Federal Communications Commission (FCC). URL https://goo.gl/1yjIfA (accessed January 19, 2018)
[15] China Electric Power Research Institute (EPRI). URL https://goo.gl/uiWZ3H (accessed January 18, 2018)
[16] Texas Instruments: Power Line Communications. URL https://goo.gl/RjJsAu (accessed January 18, 2018)
[17] Maxim Integrated: Powerline Communications. URL https://goo.gl/Y4kooA (accessed January 18, 2018)
[18] STMicroelectronics: Power Line Transceivers. URL https://goo.gl/ekuivi (accessed January 18, 2018)
[19] PRIME Alliance. URL https://goo.gl/tii1mN (accessed January 18, 2018)
[20] HomePlug Alliance. URL https://goo.gl/EU7Inj (accessed January 18, 2018)

[21] V. Oksman and J. Zhang, "G.HNEM: the new ITU-T standard on narrowband PLC technology," *IEEE Communications Magazine*, vol. 49, no. 12, pp. 36-44, Dec. 2011. DOI 10.1109/MCOM.2011.6094004

[22] IEEE P1901.2 Standard. URL https://goo.gl/rM84pD (accessed January 18, 2018)

[23] Texas Instruments: TI PLC Development Kit Design Guide. URL https://goo.gl/g9hnvF (accessed January 18, 2018)

[24] Texas Instruments: Developing a Flexible PLC Implementation for Worldwide Deployment. URL https://goo.gl/MHiqtZ (accessed January 18, 2018)

[25] E. Ancillotti *et al*., "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," *Computer Communications*, vol. 36, no. 17-18, pp. 1665-1697, Nov. 2013. DOI 10.1016/j.comcom.2013.09.004

[26] N. Bui *et al*., "The Internet of Energy: a Web-enabled Smart Grid System," *IEEE Network*, vol. 26, no. 4, pp. 39-45, Jul. 2012. DOI 10.1109/MNET.2012.6246751

[27] Internet Engineering Task Force (IETF). URL https://goo.gl/saehq (accessed January 19, 2018)

[28] European Telecommunications Standards Institute (ETSI). URL https://goo.gl/kLoUa (accessed January 18, 2018)

[29] World Wide Web Consortium (W3C). URL https://goo.gl/qgIivU (accessed January 18, 2018)

[30] S. Galli *et al*., "For the Grid and Through the Grid: The Role of Power Line Communications in the Smart Grid," *Proceedings of the IEEE*, vol. 99, no. 6, pp. 998-1027, Jun. 2011. DOI 10.1109/JPROC.2011.2109670

[31] S. Salsano *et al*., "PMSR – Poor Man's Segment Routing, a minimalistic approach to Segment Routing and a Traffic Engineering use case," *2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*, pp. 598-604, 2016. DOI 10.1109/NOMS.2016.7502864

[32] M. Hoch, "Comparison of PLC G3 and PRIME," *2011 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, pp. 165-169, 2011. DOI 10.1109/ISPLC.2011.5764384

[33] H.C. Ferreira *et al*., "Power Line Communications: Theory and Applications for Narrowband and Broadband Communications over Power Lines," 2010. DOI 10.1002/9780470661291

[34] B. Masood and S. Baig, "Standardization and deployment scenario of next generation NB-PLC technologies," *Renewable and Sustainable Energy Reviews*, vol. 65, pp. 1033-1047, 2016. DOI 10.1016/j.rser.2016.07.060

[35] T.A. Papadopoulos *et al*., "Application of Narrowband Power-Line Communication in Medium-Voltage Smart Distribution Grids," *IEEE Transactions on Power Delivery*, vol. 28, no. 2, pp. 981-988, Apr. 2013. DOI 10.1109/TPWRD.2012.2230344

[36] M. Sayed and N. Al-Dhahir, “Narrowband-PLC/Wireless Diversity for Smart Grid Communications,” *2014 IEEE Global Communications Conference*, pp. 2966-2971, 2014. DOI 10.1109/GLOCOM.2014.7037259

[37] K. Razazian and J. Yazdani, “CENELEC and Powerline Communication Specification in realization of Smart Grid Technology,” *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, pp. 1-7, 2011. DOI 10.1109/ISGTEurope.2011.6162685

[38] B. Adebisi *et al*., “Narrowband PLC Channel Modelling For Smart Grid Applications,” *2014 9th International Symposium on Communication Systems, Networks Digital Sign (CSNDSP)*, pp. 67-72, 2014. DOI 10.1109/CSNDSP.2014.6923800

[39] H. Kellerbauer and H. Hirsch, “Simulation of Powerline Communication with OMNeT++ and INET-Framework,” *2011 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, pp. 213-217, 2011. DOI 10.1109/ISPLC.2011.5764395

[40] Discrete Event Simulator: OMNeT++. URL https://goo.gl/mGlZC9 (accessed January 18, 2018)

[41] D.P.F. Miller and H. Vakilzadian, “Ubiquitous Networks: Power Line Communication and Internet of Things in Smart Home Environments,” *IEEE International Conference on Electro/Information Technology*, pp. 596-601, 2014. DOI 10.1109/EIT.2014.6871832

[42] Q. Ou *et al*., “Application of Internet of Things in Smart Grid Power Transmission,” *2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC)*, pp. 96-100, 2012. DOI 10.1109/MUSIC.2012.24

[43] X. Chen *et al*., “Application of Internet of Things in Power-Line Monitoring,” *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 423-426, 2012. DOI 10.1109/CyberC.2012.77

[44] Y. Zhen *et al*., “Study of Architecture of Power Internet of Things,” *IET International Conference on Communication Technology and Application (ICCTA 2011)*, pp. 718-722, 2011. DOI 10.1049/cp.2011.0762

[45] A. Hosseinpour *et al*., “Security and Feasibility of Power Line Communication System,” *Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 244-251, 2015. DOI 10.1007/978-3-319-23276-8_22

[46] L. Davoli *et al*., “Integration of Wi-Fi mobile nodes in a Web of Things Testbed,” *ICT Express, Special Issue on ICT Convergence in the Internet of Things (IoT)*, vol. 2, no. 3, pp. 96–99, 2016. DOI 10.1016/j.icte.2016.07.001

[47] R. Gustavsson, “Security Issues and Power Line Communication,” *International Symposium on Power Line Communications and Its Applications (ISPLC)*, pp. 311-318, 2011. URL https://goo.gl/tb8asB (accessed January 18, 2018)

[48] L. Chhaya *et al*., "Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control," Electronics, vol. 6, no. 1, 2017. DOI 10.3390/electronics6010005

[49] C. Montenegro *et al*., "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," *RFC 4944*, The Internet Engineering Task Force, 2007. URL https://goo.gl/KyJC8b (accessed January 18, 2018)

[50] Official IEEE 802.11 Working Group (WG) Project Timelines. URL https://goo.gl/jCghRD (accessed January 18, 2018)

[51] Pahlavan K, Krishnamurthy P (2009) IEEE 802.3 Ethernet. In: Networking Fundamentals: Wide, Local and Personal Area Communications, pp. 656, DOI 10.1002/9780470779422.ch8

[52] L. Belli *et al*., "An Open-Source Cloud Architecture for Big Stream IoT Applications," *Interoperability and Open-Source Solutions for the Internet of Things*, pp. 73–88, 2015. DOI 10.1007/978-3-319-16546-2_7

[53] L. Davoli *et al*., "An anonymization protocol for the Internet of Things," *2017 International Symposium on Wireless Communication Systems (ISWCS)*, pp. 459-464, 2017. DOI 10.1109/ISWCS.2017.8108159

[54] L. Davoli *et al*., "THORIN: an Efficient Module for Federated Access and Threat Mitigation in Big Stream Cloud Architectures," *IEEE Cloud Computing*, vol. PP, no. 99, pp. 1-1. DOI 10.1109/MCC.2017.455155318

[55] C. De Laat *et al*., "Generic AAA Architecture," *RFC 2903*, The Internet Engineering Task Force, 2000. URL https://goo.gl/tp8pwT (accessed January 18, 2018)

[56] L. Belli *et al*., "Applying Security to a Big Stream Cloud Architecture for the Internet of Things," *International Journal of Distributed Systems and Technologies*, vol. 7, no. 1, pp. 37-58, 2016. DOI 10.4018/IJDST.2016010103

[57] J. Heo *et al*., "Identity-based mutual device authentication schemes for PLC system," *2008 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, pp. 47-51, Apr. 2008. DOI 10.1109/ISPLC.2008.4510397

[58] J.S. Lee *et al*., "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," *IECON 2007 - 33rd Annual Conference of the IEEE Industrial Electronics Society*, pp. 46–51, Nov. 2007. DOI 10.1109/IECON.2007.4460126

[59] L. Davoli *et al*., "From Micro to Macro IoT: Challenges and Solutions in the Integration of IEEE 802.15.4/802.11 and Sub-GHz Technologies," *IEEE Internet of Things Journal*, vol. PP, no. 1, pp. 1–1, Sep. 2017. DOI 10.1109/JIOT.2017.2747900

[60] S. Frankel *et al*., "The AES-CBC Cipher Algorithm and Its Use with IPsec," *RFC 3602*, The Internet Engineering Task Force, 2003. URL https://goo.gl/qKx9b (accessed January 19, 2018)

[61] K. Moriarty *et al*., "PKCS #1: RSA Cryptography Specifications Version 2.2," *RFC 8017*, The Internet Engineering Task Force, 2016. URL https://goo.gl/DWnq9f (accessed January 18, 2018)

[62] F.J.S. Miravalles, “Opera 2: standardization of broadband PLC,” *2007 IEEE International Symposium on Power Line Communications and Its Applications*, pp. 11-11, 2007. DOI 10.1109/ISPLC.2007.371062

[63] G. Corral *et al*., “Security in OPERA Specification Based PLC Systems,” *2010 Sixth Advanced International Conference on Telecommunications*, pp. 474-478, 2010. DOI 10.1109/AICT.2010.26

[64] E. Rescorla, “Diffie-Hellman Key Agreement Method,” *RFC 2631*, The Internet Engineering Task Force, 1999. URL https://goo.gl/gPPtGo (accessed January 18, 2018)

[65] S. Kelly, “Security Implications of Using the Data Encryption Standard (DES),” *RFC 4772*, The Internet Engineering Task Force, 2006. URL https://goo.gl/B1DzFc (accessed January 18, 2018)

[66] National Institute of Standards and Technology (NIST). URL https://goo.gl/3x4xXg (accessed January 18, 2018)

[67] European Commission (EC) - SMARTGRIDS-ETPS, 2017. URL https://goo.gl/PavpBe (accessed January 18, 2018)

[68] European Commission (EC) - OPEN METER, 2017. URL https://goo.gl/w5DVrw (accessed January 18, 2018)

[69] International Electrotechnical Commission (IEC). URL https://goo.gl/TxX9x (accessed January 19, 2018)

[70] Dun and Bradstreet - What is a Dun and Bradstreet D-U-N-S Number?, 2017. URL https://goo.gl/9NKd50 (accessed January 19, 2018)

[71] N. Pavlidou et at., “Power line communications: state of the art and future trends,” *IEEE Communications Magazine*, vol. 41, no. 4, pp. 34-40, Apr. 2003. DOI 10.1109/MCOM.2003.1193972

[72] S. Kim *et al*., “A Secure Smart-Metering Protocol Over Power-Line Communication,” *IEEE Transactions on Power Delivery*, vol. 26, no. 4, pp. 2370-2379, Jul. 2011. DOI 10.1109/TPWRD.2011.2158671

[73] A. Pittolo and A.M. Tonello, “Physical Layer Security in Power Line Communication Networks,” *Physical and Data-Link Security Techniques for Future Communication Systems*, pp. 125-144, 2016. DOI 10.1007/978-3-319-23609-4_8

[74] A. Pittolo and A.M. Tonello, “Physical Layer Security in Power Line Communication Networks: An Emerging Scenario, Other Than Wireless,” *IET Communications*, vol. 8, no. 8, pp. 1239-1247, May 2014. DOI 10.1049/iet-com.2013.0472

[75] M. Esmalifalak *et al*., “Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study,” *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, 2013. DOI 10.1109/TSG.2012.2224391

[76] S. Dudek, “HomePlugAV PLC: practical attacks and backdooring,” 2014. URL https://goo.gl/FgTBQJ (accessed January 19, 2018)

[77] W. Ahn *et al*., “Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs,” *International Journal of Distributed Sensor Networks*, vol. 11, no. 9, 2015. DOI 10.1155/2015/836258

[78] J.R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies*, vol. 22, no. 3, pp. 365-404, 2013. DOI 10.1080/09636412.2013.816122
[79] J. Loeb, “Researchers warn of biggest cyber threat to power grids since Stuxnet,” 2017. URL https://goo.gl/FyVhz2 (accessed January 18, 2018)
[80] Texas Instruments - TMDSPLCKIT-V3 - C2000 Power Line Modem Developer’s Kit, 2017. URL https://goo.gl/9J8H4u (accessed January 18, 2018)
[81] Texas Instruments - Developing robust power line communications (PLC) with G3, 2017. URL https://goo.gl/EkygT1 (accessed January 18, 2018)
[82] A. Sokolov, “Java Simple Serial Connector (JSSC),” 2017. URL https://goo.gl/uATJqS (accessed January 18, 2018)
[83] Texas Instruments - TMDSDC3359 - Data Concentrator Evaluation Module, 2017. URL https://goo.gl/skCeRp (accessed January 18, 2018)