Hindawi
Security and Communication Networks
Volume 2017, Article ID 7369684, 18 pages
https://doi.org/10.1155/2017/7369684

Research Article

Cybersecurity Vulnerability Analysis of the PLC PRIME Standard

Miguel Seijo Simó, Gregorio López López, and José Ignacio Moreno Novella

Universidad Carlos III de Madrid, Madrid, Spain

Correspondence should be addressed to Miguel Seijo Simó; mseijo@it.uc3m.es

Received 20 February 2017; Accepted 18 May 2017; Published 5 July 2017

Academic Editor: Sherali Zeadally

Security in critical infrastructures such as the power grid is of vital importance. The Smart Grid puts power grid classical security approach on the ropes, since it introduces cyberphysical systems where devices, communications, and information systems must be protected. PoweRline Intelligent Metering Evolution (PRIME) is a Narrowband Power-Line Communications (NB-PLC) protocol widely used in the last mile of Advanced Metering Infrastructure (AMI) deployments, playing a key role in the Smart Grid. Therefore, this work aims to unveil the cybersecurity vulnerabilities present in PRIME standard, proposing solutions and validating and discussing the results obtained.

1. Introduction

The Smart Grid represents a revolution especially at distribution and customer levels, bringing monitoring and control capabilities, traditionally available up to the primary substations, down to the secondary substations and beyond. As a result, the number of devices to be monitored and controlled increases dramatically. Therefore, deploying accurate and robust Advanced Metering Infrastructures (AMIs) is a critical step towards making Smart Grids fully operational.

In the scope of Smart Grids, AMIs are systems installed by the Distribution System Operators (DSOs) in the power grid which are used for measuring, collecting, and analyzing the energy consumed and/or generated by the clients. In order to do so, they communicate with metering devices (i.e., smart meters) to retrieve the consumption/generation data. The elements involved in the AMI include the metering devices, communication protocols, consumer energy displays and controllers, customer systems, Meter Data Management (MDM) software, and supplier business systems. AMIs are being widely established worldwide, especially in Europe, where the investment forecast goes up to 45 B€ for the deployment of 200 M smart meters before 2020 [1]. Only in Spain, all the metering infrastructure will be replaced with smart meters by 2018, which means a deployment of approximately 30 M meters [2].

Information and Communications Technologies (ICTs) play a key role in AMI, which brings many advantages but also challenges for DSOs, being specially relevant the ones related to security and privacy. Attacks to critical infrastructures such as the power grid are specially dangerous, meaning a major impact on health, security, and economic welfare of the citizens or on the effective operation of the countries where this attacks are performed [3]. These attacks are especially attractive from an economic point of view (e.g., manipulating billing data), to obtain data that may reveal sensitive information or with terrorist purposes (e.g., to cause blackouts). Despite the novelty of these technologies, there are already examples illustrating the interest on attacking AMI infrastructures, such as the Malta incident [4], where more than a thousand smart meters were compromised between 2011 and 2012, incurring a power theft worth 30 M€.

Therefore, government authorities and competent bodies are taking measures to protect AMI deployments from cyberattacks. Thus, the European recommendation on Smart Grid systems deployment emphasises security and privacy aspects [5]. In the same way, in USA, cybersecurity also represents a major issue in this topic, in which different regulations from

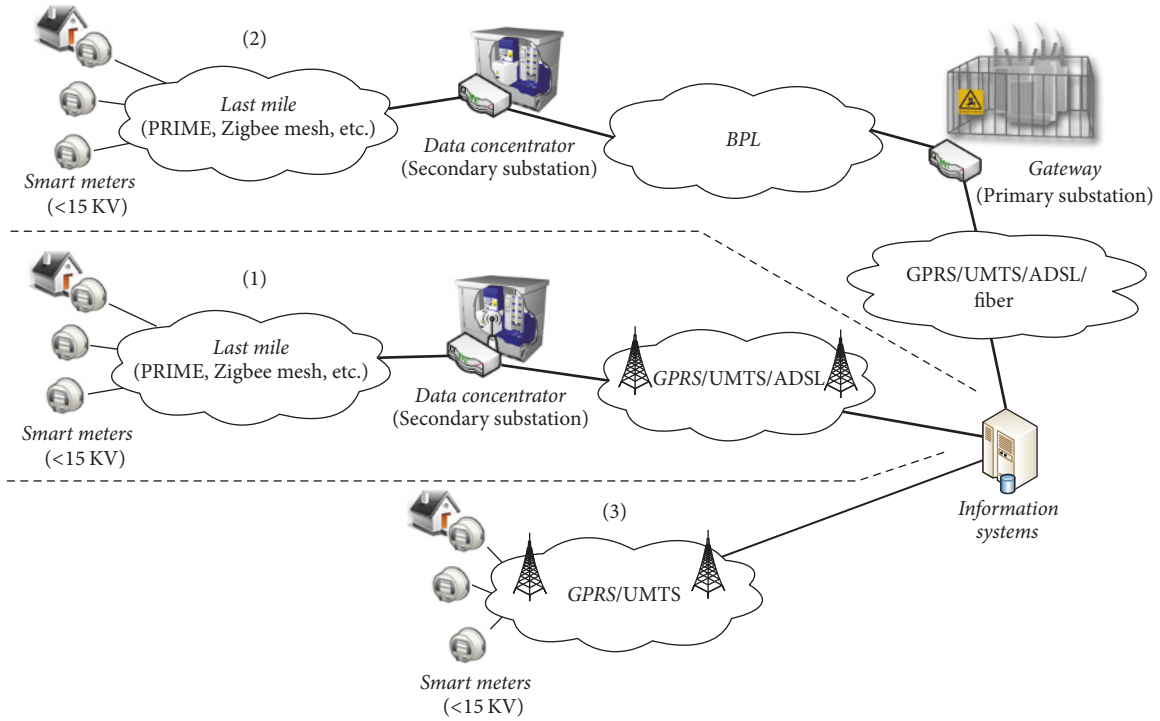


Figure 1: ICTs architecture in AMI.

National Institute of Standards and Technology (NIST) and North American Electric Reliability Corporation (NERC) exist (NIST IR-7628 [6], CIP-002 to CIP-009).

In order to comply with these security and privacy aspects, DSOs have to take security measures in all their infrastructure, being the last mile one of the most challenging parts due to the vast number of devices and the novelty of many of the technologies involved.

There are many different communication technologies present in the aforementioned last mile (e.g., Zigbee, Narrowband Power-Line Communications (NB-PLC), RF, and GSM) [7, 8]. However, using the low voltage infrastructure as communications medium brings many benefits to DSOs [9], thus making NB-PLC technologies a specially attractive solution in the last mile of current AMI deployments [10, 11]. PoweRline Intelligent Metering Evolution (PRIME) stands out as very promising NB-PLC technology. It was initially developed by PRIME Alliance, led by world-class DSOs such as Iberdrola or Gas Natural Fenosa and later accepted as standard by ITU-T [12]. Currently, there are 13 million PRIME-compliant smart meters deployed, and the latest version of the protocol aims to expand worldwide.

In this paper, the problem of security and privacy in the last mile of AMIs is addressed, focusing on infrastructures featuring PRIME NB-PLC technology.

The remainder of the paper is structured as follows. Section 2 sets the background on AMI, focusing on PRIME and giving an insight on the description of the protocol and its security features. Section 3 presents the vulnerabilities found in PRIME physical and data link layers, describing possible attacks and solutions. Section 4 validates the aforementioned vulnerabilities. Section 5 sets discussion and recommendations on security and privacy on PRIME networks. Section 6 draws the conclusions of the work.

2. Background

2.1. Overview of AMI Architectures and Communications Technologies. AMIs integrate smart meters, communication networks, and management systems, allowing duplex communication between the DSO and the final customers. This allows supporting several applications, including (1) improving supply quality control; (2) control of distributed generation scenarios based on renewable energies; (3) billing enhancements; (4) demand response; (5) antifraud techniques; (6) house automation applications [8]. Smart meter networks have heterogeneous nature due to the different density and distribution of its nodes depending on the scenario; big differences between rural and urban scenarios exist. Therefore, in addition to the main systems comprising the AMI, smart meters, communication networks, and management systems, it is necessary to include data concentrators in those scenarios with a vast number of nodes.

Figure 1 shows three different possible configurations for a communications network in an AMI environment. (1) and (2) typically correspond to highly populated networks, where the smart meters form a subnet with the data concentrator, normally placed in the secondary substations (medium voltage (MV) to low voltage (LV)). In the first case, the Concentrator has direct connection with the management system, while, in the second case, different technologies are used to connect

Table 1: Main PRIME features for v1.3.6 and v1.4 [20].

Layer	Feature	PRIME V1.3.6	PRIME V1.4
PHY	Frequency band	CENELEC band (3–95 kHz)	FCC vand (10–490 kHz)
	Data rate	Up to 130 kbps	Up to 1028.8 kbps
	Robust mode	No	Repetition coder
MAC	Network formation	Beacon discovery, automatic promotion	Beacon discovery (longer), automatic promotion
	Keep-alive monitoring	Yes	Yes (with link quality info)

these concentrators with the management system gateway. (3) is typically used in scenarios with a smaller number of nodes which are geographically dispersed, all of them being directly connected to the management system.

As it can be observed in Figure 1, the architecture is tree-shaped (except for the smart meters, which can form a mesh network), where every branch represents a different subnet, thus making possible the combination of different communication technologies in the same scenario. In the so-called last mile, covering from the smart meters to the secondary substation, the most deployed technologies are those not requiring deployment of new communication channels and featuring self-configuration network mechanisms and low cost (e.g., Zigbee mesh or NB-PLC). On the other hand, the main requirements for communication technologies between the substations and the management systems are robustness, long range, and higher bit rates, fiber, xDSL, cellular technologies, or Broadband PowerLine (BPL) communications being the most deployed technologies.

In AMI scenarios, both the communication architectures and technologies depend on many different factors, such as the characteristics of the infrastructure, regulations to be applied, or the applications to be supported. This generates broad differences in the different deployments worldwide. In Europe, for example, AMI deployments are oriented to provide consumption/generation measurements to the client aiming energy savings as well as providing remote control and measurements to the DSO, as stated in the European recommendation 2012/148/UE [5]. This recommendation also addresses cybersecurity and privacy in smart meter systems, focusing on privacy issues. In USA, however, the applications supported by AMI deployments are extended with new features, such as blackout, fraud, and nontechnical losses detection, quality assurance, prepaid interfaces, demand response (DR), and home automation applications. Regarding cybersecurity recommendations, NIST directives address security and privacy as well, focusing on security issues [6].

In order to ensure security and privacy in AMI deployments, every part of the architecture must be protected. However, the communications between the substations and the management systems are more centralized and mostly based on IP [9], making it easier to adapt existing security and privacy solutions. On the other hand, the last mile features a vast number of embedded terminal devices and a variety of network technologies that represent a broad research field in terms of cybersecurity and are more difficult to be physically protected.

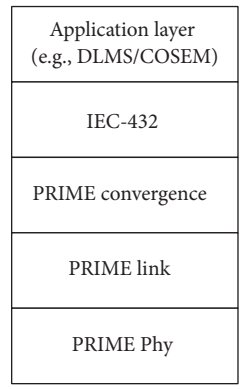


Figure 2: Protocol stack in AMI scenarios based on PRIME.

Among the different last-mile communication technologies, we can find cellular, wireless mesh (e.g., Zigbee or RF-Mesh), and NB-PLC. Cellular is the most expensive solution, but its performance and reliability make it an option where other solutions cannot be deployed. Wireless mesh technologies are mature, reliable, and more suitable for low density areas such as rural areas and villages. NB-PLC is cheap, fairly reliable, and suitable for dense areas such as cities. While RF-Mesh and Zigbee are widely used in the United States [8], NB-PLC technologies are winning momentum worldwide, especially in Europe [13].

Among the different NB-PLC standards, G3, Meters and More, and PRIME are largely deployed in Europe [13], where PRIME started its worldwide expansion in the new version of the standard, by not only supporting European CENELEC-A band, but also expanding to FCC and ARIB regulated bands for USA and Japan, respectively [14].

This work focuses on the vulnerability analysis of the physical and link layers of the protocol stack present in AMI scenarios based on PRIME NB-PLC networks, which is represented in Figure 2.

2.2. PRIME Description. PRIME is a NB-PLC technology developed by the PRIME Alliance, although version 1.3.6 of the physical (PHY), media access control (MAC), and convergence layers of PRIME has been also accepted as standard by the ITU-T [12]. Version 1.4 was released at the end of 2014, including additional features, although this section focuses on version 1.3 as it is the version present in most of the equipment deployed in the field. Table 1 summarizes the main differences between the aforementioned versions of the protocol.

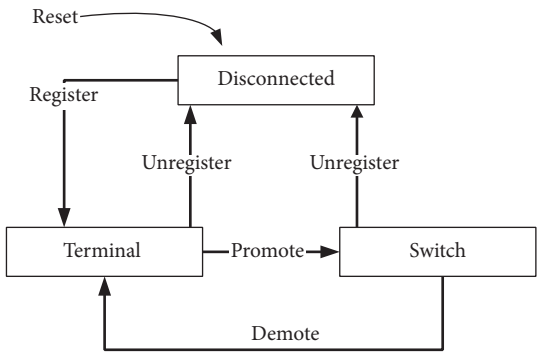


Figure 3: Different states that a PRIME SN can reach [20].

At PHY level, PRIME operates in the 41–89 KHz band (CENELEC-A band) [15] using Orthogonal Frequency Division Multiplexing (OFDM) modulation. The carriers use Differential Phase Shift Keying (DPSK), allowing raw data rates of up to 130 Kbps.

At MAC level, two kinds of nodes are defined: Base Node and Service Node. The Base Node, often referred to as Concentrator, coordinates the PRIME network, only being allowed a single Base Node per network. Service Nodes are generally smart meters but, when needed, they may promote to switches, combining then both roles. Switches are communications repeaters whose main goal is to increase signal range in the cable via relying, thus mitigating the effects of attenuation and noise. Figure 3 shows the different states and transitions of a Service Node.

In terms of logical addressing, a PRIME node counts with several addresses, which are used depending on the communication context. The main identifiers of a PRIME node are as follows:

(i) *EUI-48*. Extended Unique Identifier is the 48-bit long MAC address issued by the manufacturer. Additionally, since each network has only one Base Node, the Base Node's EUI-48 is used to identify the whole network. This address is known as the Subnetwork Address (SNA).

(ii) *SID*. Switch Identifier is used to identify a specific Switch within a network. It is dynamically assigned by the Base Node when a Service Node is promoted to Switch. The Base Node has Switch Identifier (SID) 0 by default.

(iii) *LNID*. Local Node Identifier is used to identify a specific node within a network. It is also assigned by the Base Node upon registration.

(iv) *LCID*. Local Connection Identifier is used to identify a connection between a pair of nodes.

Figure 4(a) illustrates the aforementioned identifiers and their lengths. A more complete description can be found in [14].

Media access control in PRIME includes a Shared Contention Period (SCP) and a Contention-Free Period (CFP). Current implementations only include the SCP, which is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). However, the benefits of using the CFP in new Smart Grid scenarios are under research [16].

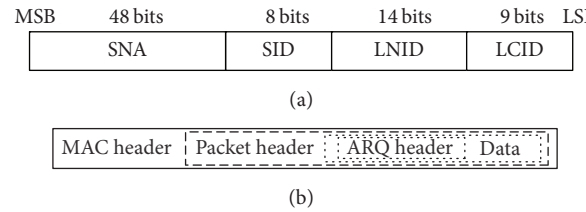


Figure 4: (a) PRIME addresses. (b) Generic MAC frame. Dashed lines represent the optional fields [20].

PRIME MAC frames can include different fragments of information depending on the kind of message to be sent. Figure 4(b) shows the encapsulation of the different fragments, where the first part of a MAC frame is known as MAC Header, which determines if the frame is a Beacon PDU, a Promotion Needed PDU, or a Generic packet. These frame types have the following functions:

(i) *Beacon PDU*. It is only sent by the Base Node or a Switch Node; it is used to publish their address so Service Nodes can register through them and to broadcast information related to the network synchronization.

(ii) *Promotion Needed PDU*. It is a mechanism used by the Service Nodes without connectivity (i.e., those which do not receive any Beacon PDU) to alert nearby nodes of this situation. Whenever a Service Node in Terminal state receives a Promotion Needed PDU (PNPDU), it should send a request to the Base Node for a Switch promotion. When the Service Node in Terminal state sends a Promotion Request message triggered by a received PNPDU, it includes the Promotion Needed Address (PNA), so the Base Node does not promote 2 different Terminal Nodes to give connectivity to the same Disconnected Node. The promotion can be authorized only by the Base Node, although the standard does not specify any promotion criteria to decide which node should be promoted.

(iii) *Generic MAC PDU*. It is sent by all the nodes in a PRIME network; Generic MAC frames can be either Control or Data packets, where Control packets manage the network and Data packets transmit information.

Figure 5 represents these frame types and shows the hierarchy relationship between frames and packets for data and control messages as well as the fields used to decode them.

As it has already been mentioned, version 1.4 introduced some changes both in the PHY and in the MAC layers [14]. One of the more interesting additions regarding the PHY layer is the extension to FCC and ARIB bands, allowing an increase of transmission speed of up to 1028.8 kbps. Nevertheless, the most significant impact regarding this band

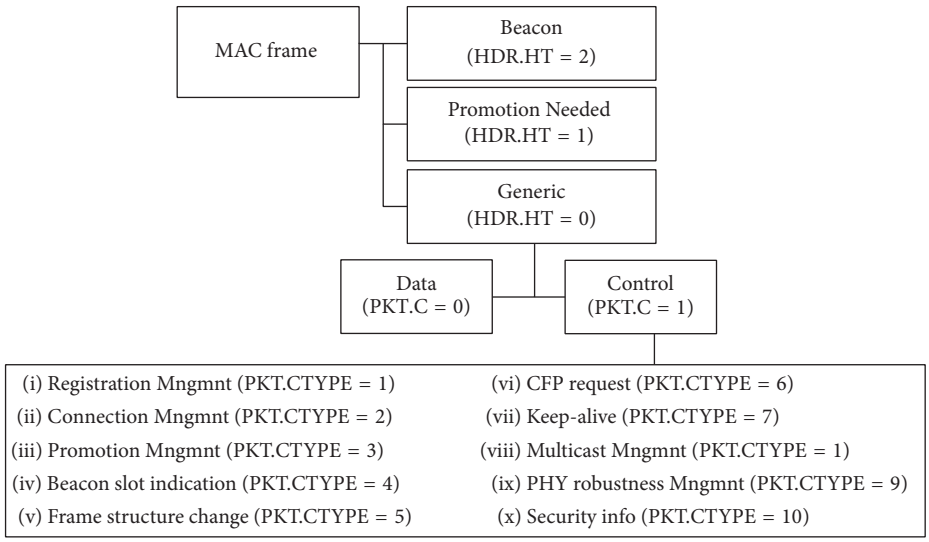


Figure 5: MAC type of messages encapsulation scheme. Field values corresponding to each type are detailed on each box [20].

expansion is the utilization of PRIME technology in US and Asia-Pacific markets.

The new specification also defines some changes regarding the MAC layer, such as the inclusion of link quality information inside the packet header. This allows obtaining link quality information in any section of the network, simplifying the diagnosis of connectivity problems.

As it could be expected, version 1.4 of the standard also details compatibility mechanisms with version 1.3.6.

At application layer, DLMS/COSEM is commonly used over PRIME, where COSEM (IEC 62056-61/62) is an energy metering profile of DLMS (IEC 62056-53) application protocol [17, 18]. DLMS/COSEM defines data models for common energy-related parameters together with a communication protocol designed to transport this kind of information. Moreover, DLMS/COSEM also provides some security mechanisms targeted to access control, event registry, and message ciphering [19].

2.3. Security in PRIME. Privacy, authentication, and data integrity in PRIME are provided in the MAC layer. There are 2 different Security Profiles which are negotiated between the Base Node and the Service Nodes. All packets must use the negotiated Security Profile except REG, SEC, BPDU, and PNPDU messages.

Security Profile 0 does not use encryption nor provide privacy authentication or data integrity, which are only provided in Security Profile 1, based on the encryption of the data and its associated Cyclic Redundancy Check (CRC). The encryption algorithm used is Advanced Encryption Standard (AES) with 128-bit secret key and Electronic Codebook (ECB) block-ciphering.

2.3.1. Security Profile Negotiation. The Security Profile is negotiated during the device registration. The REG_REQ message sent by the Service Node contains a supported Security Profile in the REG.SPC field. If the Base Node accepts the registration with the proposed Security Profile, it will send REG_RSP with the same REG.SPC value. The Base Node can also downgrade the Security Profile by setting REG.SPC to 0 or reject the connection if the proposed Security Profile is not sufficient.

2.3.2. Key Hierarchy

Initial Working Key (WK0). It is used in a disconnected Service Node to decrypt some fields of the REG_RSP message.

$WK0 = AES_{enc}(USK, 0)$.

Working Key (WK). It is used to encrypt all the unicast data between the Base Node and the Service Node. It is different for each Service Node.

$WK = AES_{enc}(USK, SEC.RAN)$, where SEC.RAN is the random sequence received in the SEC.RAN field.

Subnetwork Working Key (SWK). It is used for broadcast/multicast data or direct connections not involving the Base Node. It is never transmitted over the physical channel but computed from other keys.

$SWK = AES_{enc}(SNK, SEC.SNK)$, where SEC.SNK is the random sequence received in SEC.SNK

WK and SWK are updated each *MACRandSeqChgTime* seconds.

Master Keys (MK1, MK2). Base keys are administered by the Base Node and used to derive other keys. PRIME standard does not specify how these keys are administered.

Device Secret Key (DKS). It is unique to each Service Node and hard-coded in the device during production.

$DSK = AES_{enc}(MK1, UI)$, where UI is the EUI-48 of the device.

Key Diversifier (KDIV). It is also unique to each Service Node, but not constant for the entire life of the node. How this key

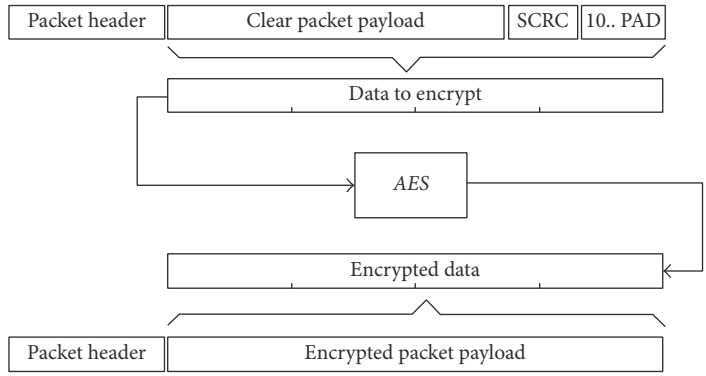


Figure 6: Security Profile 1 encryption algorithm [12].

is provisioned to the Service Node is not in the scope of the standard.

KDIV = AES_{enc}(MK2, UI), where UI is the EUI-48 of the device.

Unique Secret Key (USK). It is used to derive WK0 and WK.

USK = AES_{enc}(DSK, KDIV).

2.3.3. Encryption. Secure CRC (SCRC) is calculated for every packet encrypted in Security Profile 1. It is calculated over the unencrypted packet payload as the remainder of the division (Modulo 2) by the generator polynomial $g(x) = x^8 + x^2 + x + 1$ of the polynomial x_8 multiplied by the unencrypted packet payload.

Each 128-bit block is encrypted using AES with a valid working key, as shown in Figure 6.

3. Finding Vulnerabilities in PRIME Networks

When searching for vulnerabilities in communication systems, it is important to have a clear view of the protocol stack. This paper presents an analysis of vulnerabilities in the PRIME physical and data link layers.

The physical layer deals with the bit-level transmission between different devices and the interfaces connecting to the physical medium, the physical layer jamming being the only attack related to these functions. The rest of the attacks presented in this paper are related to the link layer. In this layer, PRIME deals with the channel access method, the logical topology (including addressing, switching, and registration of the nodes), packet aggregation, security, and error control methods, among others.

Note that this research is based on PRIME v1.3 given that it is the version of the standard that is present in most of the devices nowadays.

3.1. Physical Layer Jamming. At the physical layer, the most common kind of attack is the jamming attack. Jamming attack consists in deliberately blocking or interfering communications by transmitting signals that decrease the signal-to-noise ratio, disrupting the communications, and causing Denial of Service (DoS). This attack is more common in wireless communications, as the channel is more accessible to the attacker, but it can be applied to any kind of communication systems, such as power cables in PowerLine Communications (PLC).

Jamming can be divided into three different groups: noise jamming, interference jamming, and correlated jamming. Noise jamming is the simplest of all the jamming attacks, as it consists in injecting noise (normally Gaussian) in the channel. It can cover all the bandwidth (Barrage Jamming) or just a part of it (Partial Band Jamming). Interference jamming uses colored signals which are not synchronized to target signal [23].

As it has been explained in Section 2, PRIME uses OFDM with Phase Shift Keying (PSK) modulation and optional Forward Error Correction (FEC), which makes it more robust against noise and reduces the effectiveness of noise and interference jamming attacks.

In order to perform a noise or interference jamming attack against PRIME networks, we must take into account the fact that the signal band covers from 42 to 89 kHz (CELENEC A band). The UNE-EN 50065-1:2012 norm dictates the maximum output levels of the signal [15], but more accurate information about the maximum output levels of the device can be found in the manufacturer datasheet (e.g., [24], where Figure 34. 3 shows maximum output values of 100 dBuV). Figure 7 shows the Bit Error Rate (BER) for the different signal-to-noise ratio (SNR) values. For the most robust modulation (Binary Phase Shift Keying (BPSK) with FEC on), forcing the SNR to fall under 2 dB causes high BER which may disrupt the communications in the affected nodes.

The last type of jamming attacks is the correlated jamming, which is capable of causing damage to OFDM transmissions using minimal power. These attacks are more sophisticated and require detailed synchronization and knowledge of the target signal. In this case, the use of OFDM makes the signal more vulnerable to timing and frequency synchronization attacks as well as equalization attacks [25].

Jamming attacks are trivial, yet effective only in a physically limited range, being able to affect only nodes located nearby. Due to the dynamic logical topology of PRIME networks, the network can recover even if several Service Nodes or switches are affected by the attack. However,

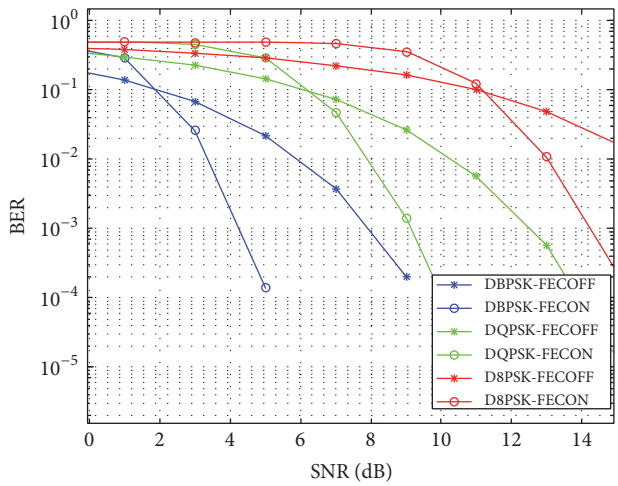


Figure 7: BER versus SNR for the different modulations present in PRIME [21].

disrupting the communications with the Base Node will take down the whole network.

In order to avoid this kind of attacks, the infrastructure must be physically protected. While it is highly recommended to physically protect the Base Node, the Achilles' heel in this kind of attacks, protecting the Service Nodes, represents a major challenge to the DSOs, as they are located right before the clients' power sockets. Installing signal filters between every Service Node and the client is an expensive solution, often used in specific cases to mitigate noise or interference problems, but not as a general protection against jamming or other kind of attacks.

3.2. CSMA/CA Jamming. The channel access method can be attacked by jamming CSMA/CA in the SCP of the MAC frame. It is important to note that the CSMA/CA algorithm presented in the PRIME specification corresponds to the basic access mode, as there is no RTS/CTS mechanism. As it has already been mentioned in Section 2, the MAC frame in PRIME also includes a CFP, but it is not currently implemented by the manufacturers, being its use under research [16]. To perform this attack, the attacker only needs to sense the channel and cause a small collision to corrupt a whole packet, thus using less energy than the victim. Even if the attacker uses the channel when it is idle, it will cause nodes attempting to transmit to back off, and, after *macSCPMaxTxAttempts* attempts, the packet transmission will fail.

The goal of this attack is to cause DoS in all the devices located in the attacker's range by blocking their communications.

There are studies such as the one presented in [26]; analyzing the effects of this kind of attack for CSMA/CA and [27] presents a solution to detect them. Although there are also studies presenting solutions trying to detect and avoid CSMA/CA greedy behaviors [28], the measures proposed against jamming attacks are also applicable and recommended to protect the network.

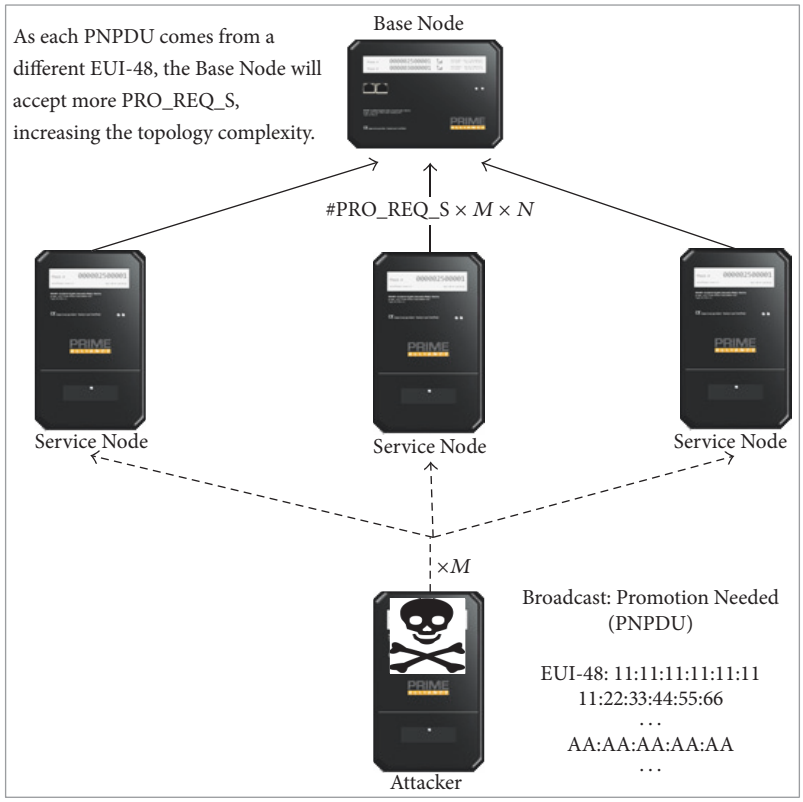
3.3. Promotion Needed Flooding. PNPDU, as explained in Section 2.2, is a mechanism that allows Service Nodes to announce that they do not have good connectivity with the Base Node (i.e., do not receive Beacons from the Base Node) so the Service Nodes nearby that receive PNPDUs send a Promotion Request to ask for promotion and act as a repeater for the nodes with connectivity problems. This mechanism can be abused by spoofing PNPDUs from different EUI-48 addresses, causing the following effects: (1) amplification of the traffic due to the Promotion Request sent by each Service Node that received the PNPDU and (2) increasing the number of switches, and thus the complexity of the logical topology, as the Base Node will accept some of the Promotion Requests sent by the Service Nodes near the attacker. The Promotion Requests triggered by the PNPDU in the Service Nodes near the attacker include the Promotion Needed Address to help the Base Node to evaluate the requests and promote a Service Node to Switch only if necessary. By spoofing different EUI-48 addresses, the Base Node is tricked into thinking that there are many different nodes without connectivity, enabling more and more switches. This attack is depicted in Figure 8.

PRIME specifications recommend Service Nodes to limit the number of PNPDUs received in a time interval to avoid flooding the network. However, this would affect also legitimate nodes with connectivity problems.

The goal of this attack is not to completely block the communications but to hinder them, causing delays and errors in its operation.

PNPDUs are not encrypted in any of the security profiles, making every network vulnerable to this attack. There is no way to avoid the first effect described (traffic amplification) apart from following the recommendations on the limit of PNPDUs received in a time interval. However, it is possible to avoid the effect on the number of Service Nodes promoted to Switch by supporting the following features in the firmware of the Base Node: whitelisting the promotion needed addresses and ignoring the Promotion Requests coming from nodes that are already registered.

3.4. Node Registration Overflow. The registration of the nodes also presents a potential vulnerability. The standard defines that the Service Nodes register in the Base Node using its EUI-48 (MAC address) as identifier, obtaining a Node Identifier (NID) that is unique for that network. Even if the NID is a 22-bit long identifier, it is composed by the SID (8 bits) and the Local Node Identifier (LNID) (14 bits), the LNID being unique for the nodes directly connected to a Switch. Thus, the number of unique identifiers in a real network gets reduced to a maximum of 16384 nodes per Switch. The attacker can specify in the registration request the SID he requests to connect through, which simplifies the attack, given that the number of switches is restrained in real networks. If a malicious node spoofs registration requests with pseudo-random EUI-48 identifiers, it can overflow the LNIDs available for the SIDs of the most critical switches in the topology.



N: Number of Service Nodes
M: Packets sent by attacker

Figure 8: Promotion Needed Flooding attack.

The specification dictates that when assigning a LNID, the Base Node shall not reuse a LNID released by an unregister process until after $(macMaxCtlReTx + 1) * macCtlReTxTimer$ seconds (where macMaxCtlReTx is the maximum number of times a MAC entity will try to retransmit an unacknowledged MAC packet, and macCtlReTxTimer is the number of seconds for which a MAC entity waits for acknowledgement of receipt of the MAC packet from its peer entity), to ensure that all retransmit packets have left the subnetwork. Similarly, the Base Node shall not reuse a LNID freed by the keep-alive process until *Tkeep_alive* seconds have passed, using the last known acknowledged *Tkeep_alive* value, or if larger, the last unacknowledged *Tkeep_alive*, for the Service Node using the LNID. This means that, in a network under this attack, a legitimate node that loses connectivity or unregisters will not have an available LNID under the attacked SIDs for, at least, the timeout specified in the standard. There is no directive in the specification regarding the behavior when all the LNIDs are assigned for a certain SID. Depending on the implementation in the Base Node, it can start unregistering older nodes, stop accepting registration of new nodes, or even cause a memory overflow.

The goal of this attack is to cause DoS in some or all the nodes in the network by overflowing the LNID table in the Base Node.

PRIME specification keeps registration messages unencrypted in all the security profiles, but, as the attack requires the registration to be completed, the attacker needs to comply with the security level of the network. For this reason, the most effective countermeasure against this kind of attacks is the use of Security Profile 1 presented in PRIME.

When Security Profile 0 is used or in cases where the attacker is able to connect to the encrypted network and due to the potential effects of the attack, it is recommended to ensure that the firmware in the Base Node is prepared to minimize the effects of node registration overflow. It is also possible to detect this kind of attack using a Network Intrusion Detection System (NIDS) near the Base Node, given that this attack is very noisy from the point of view of the generated traffic.

The nature of PRIME networks is physically static and logically dynamic. This makes EUI-48 registration whitelisting a good countermeasure against node registration overflow attacks, as new nodes are rarely added to the network, at the expense of impairing the protocol autoconfiguration capabilities.

Manufacturers are encouraged to implement registration algorithms in the Base Node that avoid memory overflows. As the number of legitimate devices is normally much lower than the number of spoofed ones when the network

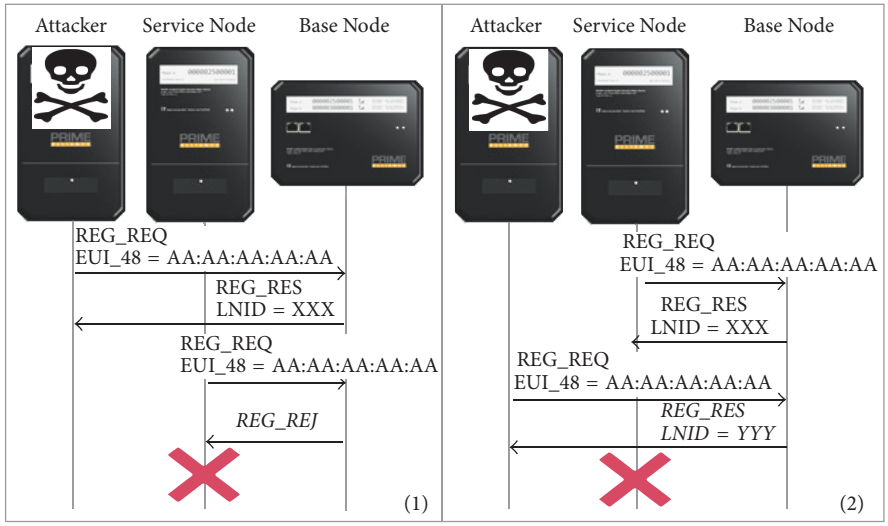


Figure 9: Node registration spoofing attack for behaviors (1) and (2).

is under this kind of attack, the impact can be reduced if, after the exhaustion of all the available LNIDs, the Base Node assigns them randomly. This way, if there are no free LNIDs available and a new node tries to connect (being it legitimate or not), the probability of getting a LNID used by an spoofed node will be much higher compared to a case where the LNIDs are assigned using a Round Robin policy, thus limiting the impact of the attack.

3.5. Node Registration Spoofing. Another potential vulnerability present in the registration process is the lack of specification on how to handle a registration request of an EUI-48 that is already registered. There are two possible behaviors to be considered in the Base Node: (1) the Base Node rejects the registration requests until the Service Node is unregistered, either explicitly or by timeout; (2) the Base Node acknowledges the registration request with a registration response assigning a new NID, as old NIDs cannot be reused until the appropriate timeout has passed. The first behavior can be abused by an attacker by spoofing the EUI-48 of a Service Node (victim) and sending a registration request before the victim registers (or right after it temporary unregisters due to communication problems), blocking the registration for this legitimate Service Node. The second behavior can be abused by an attacker just by sending a registration request with the spoofed EUI-48. The attacker can request registration through a different SID to make sure the victim never gets to see the response. All further messages from the Base Node will be addressed to the new NID, leaving the victim out of the network. These attacks are pictured in Figure 9, in order to obtain EUI-48 identifiers of the victims; the attacker can perform network sniffing and obtain the EUI-48 from the registration requests (which are never encrypted). It is also possible to extract this information from the meter itself, as shown in Figure 20.

The goal of this attack is to cause DoS in an specific Service Node by registering a rogue node in the name of the victim.

This attack requires the attacker to comply with the security level specified by the Base Node, as the registration has to be completed for the attack to be successful. For this reason, the main protection against this kind of attacks is to encrypt the communications using Security Profile 1. In networks with no encryption or where the keys are known by the attacker, there is no mechanism that allows telling which registration attempts are legitimate and which are not to avoid this kind of attacks. Nevertheless, it is possible to analyze the traffic in the Base Node and using NIDS mechanisms detects unusual behaviors caused by registration spoofing, such as multiple registration attempts with different SIDs.

3.6. LSID Overflow. The relay system present in PRIME, which ensures scalability and enables communications with nodes without direct connectivity with the Base Node, also presents potential vulnerabilities. This mechanism can be abused if an attacker creates many rogue Service Nodes and requests their promotion to Switch. Local Switch Identifier (LSID) is a 8-bit value, so there can be up to 256 switches in the whole network. The Base Node can, depending on the implementation, either stop granting new Promotion Requests or demote the oldest switches. In order to get the Promotion Requests to be accepted by the Base Node, the PNAs must be different so the Base Node is tricked into accepting new switches. This makes the attack very noisy, thus easily detectable using a NIDS near the Base Node.

The goal of LSID overflow is to avoid the creation of new switches or replace the old ones with bogus switches, by causing an overflow of the LSIDs. This implies connectivity problems in those nodes depending on the switches affected by the attack.

In order to perform this attack, the attacker has to be able to register in the network, meaning it should comply with the

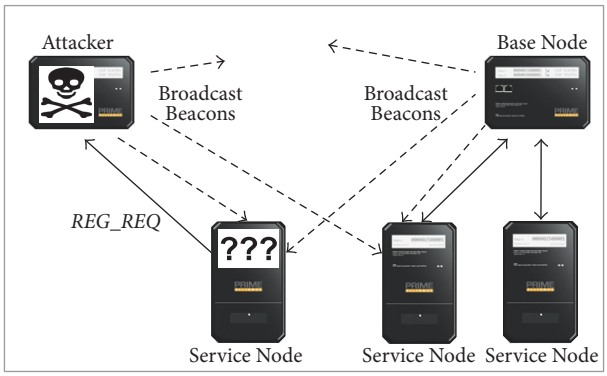


Figure 10: Base node spoofing attack.

security level imposed by the Base Node. This makes Security Profile 1 the best option to protect the network against this kind of attacks.

Registration whitelisting can help with LSID overflow attacks, as it blocks the creation of random rogue nodes in the network and limits the attacker to spoof existing nodes. Similar to the case of node registration overflow, if the Base Node assigns random SIDs after the exhaustion of the available ones, the impact of the attack can be reduced. This way, when there are no available LSIDs and a new node tries to promote to Switch (being it legitimate or not), the probability of getting a SID used by an spoofed Switch will be much higher compared to the case where the LSIDs are assigned using a Round Robin policy, thus limiting the impact of the attack.

3.7. Base Node Spoofing. According to the standard, there can be only one Base Node in the network. If an attacker physically connects to the network another node acting as a Base Node, some of the Service Nodes will hear its Beacon messages and request connection to the rogue Base Node, thus losing connectivity with the legitimate network. This attack is depicted in Figure 10.

The goal of this attack is to perform a DoS against some of the Service Nodes present in the network. The victims cannot be chosen, although the attack can be coarsely targeted by placing the rogue Base Node physically near the target nodes.

The standard specifies that the Service Node indicates the supported security profiles, but the Base Node is the one accepting the Security Profile or downgrading it to Security Profile 0. That means a rogue Base Node can perform a downgrade in the communications and hijack a Service Node even if it supports Security Profile 1. If the upper layers are not encrypted or the security profile can be downgraded by the Base Node, then the rogue Base Node can operate as a legitimate Base Node requesting consumption reports, or even power shutdown. In order to avoid this attack, NIDS systems can be used to detect Beacons from rogue Base Nodes, being necessary to install several sensors covering the traffic in all the physical network. Since this is a suboptimal solution, it is recommended that Base Node authentication mechanisms are implemented in the PRIME standard.

3.8. Sniffing. In PRIME networks with Security Profile 0 enabled, it is possible to plug a sniffer and see the traffic in plain text. While plugging a sniffer in the bottom part of the topology tree may reveal only the data sent between the Base Node and the Service Nodes nearby, locating it near the Base Node will allow obtaining all the traffic in the network. If the traffic in the upper layers is unencrypted, the attacker will be able to see all the information transmitted including the consumption reports and other private information. By analyzing the connection requests, it is also possible to identify the NID corresponding to each EUI-48 address, which can be physically identified in the smart meter, as shown in Figure 20.

Therefore, this attack allows getting access to the information sent through the network (e.g., consumption data), violating the privacy of the communications.

This attack is completely stealthy, as it does not require to send any packet to the network. Encryption at PRIME or application layers will preserve the secrecy in the communications. However, PRIME security profiles lack of Perfect Forward Secrecy, meaning that compromise of the keys compromises recorded past information. There have already been successful attempts on compromising the keys in the Service Nodes, as documented in [29].

3.9. Demotion/Unregistration/Disconnection Spoofing. The mechanism present in PRIME for demotion of the switches, unregistration, and disconnection is very similar and suffers from the same vulnerability. The above-mentioned actions can be initiated either by the Base Node (REG_UNR_B/PRO_DEM_B/CON_CLS_B message for unregistration, demotion, and disconnection, resp.) or by the Service Node (REG_UNR_S/PRO_DEM_S/CON_CLS_S), where the message initiating the process is the request and the one answering is the acknowledgement.

If an attacker locates a target (a LNID/SID/LCID to unregister/demote/disconnect) by sniffing the network, it can spoof a request from the Base Node (REG_UNR_B/PRO_DEM_B/CON_CLS_B) and send it to the target. The target Service Node will acknowledge the request with REG_UNR_S/PRO_DEM_S/CON_CLS_S and send it to the Base Node. As the Base Node has not really sent the request in the first place, it will understand the acknowledgement as a request, sending REG_UNR_B/PRO_DEM_B/CON_CLS_B to acknowledge, which will be discarded by the Service Node as the process was already completed. Therefore, an action was acknowledged and executed by both the Base Node and Service Node when the request was not coming from any of them. This process is illustrated in Figure 11.

The goal of this attack is to unregister, demote, or disconnect a Service Node, which may cause DoS in the Service Node in the case of an unregistration, in all the Nodes that are connected through the Switch in the case of a demotion or unregistration of a Switch or in a connection in the case of a disconnection. It is important to note that the impact of the attack is different depending on the kind

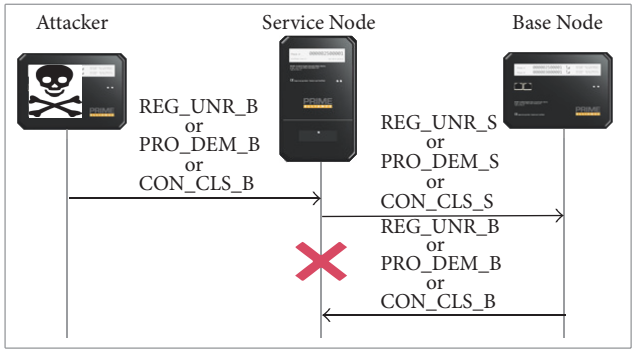


Figure 11: Demotion/unregistration/disconnection attack.

of attack, the demotion attack being the most aggressive and the disconnection attack the least aggressive one.

The only way to avoid these attacks is to use Security Profile 1, which enables encryption. In unencrypted networks, however, it is possible to detect these attacks using a NIDS located near the Base Node, throwing an alert when the unregistration/demotion/disconnection message that acts as an acknowledgement is answered from the other party.

3.10. Security CRC. Integrity checking in the Security Profile 1 is provided by a SCRC that is calculated over the unencrypted packet payload and encrypted before transmission. Therefore, the receiver has to check the CRC in the packet header, then decrypts the payload, and finally checks the SCRC before consuming a packet.

This means an attacker can create a packet containing a bogus payload without knowing the encryption key by creating a valid header with a valid CRC and replaying it again and again spending very low computational resources and yet the receiver will have to check the CRC, decrypt, and check SCRC every time causing resource exhaustion on its side. Longer packet sizes imply more expensive CRC and SCRC computations and more 128-bit blocks to be decrypted.

The impact of this attack in the network performance depends on the target. If the target of the attack is any regular Service Node, such a Service Node (and so the associate client) may lose connectivity or stop working. However, if the target is the Base Node, this attack may cause a DoS to all the network if the attacker achieves getting the Base Node busy enough.

There is no mechanism that can completely avoid this kind of attacks, as whitelists and other mechanisms can be trespassed simply by observing the traffic of the network and performing NID spoofing. Nevertheless, PRIME modem chipsets include AES cryptographic modules and compute the CRCs before passing the message to the main processor [24], resulting in a much lower impact on the overall performance.

3.11. Traffic Replay. A classic attack in communication networks is the traffic replay. It consists in eavesdropping the channel until there are some packets that are potentially interesting for the attacker; then the attacker saves those packets and replay them into the channel later to repeat the actions previously performed. Assuming that the upper layers do not have any antireplay mechanism, it is possible to perform traffic replay in networks with Security Profile 0 just by capturing any relevant packets and changing the Local Connection Identifier (LCID) to a valid one (establishing a connection may be necessary). In this mode, it is possible to replay traffic originally addressed to a Service Node in another different Service Node just by changing the LNID, SID, and LCID. If Security Profile 1 is enabled, it is possible to use cryptoanalysis to locate the packets we want to capture (e.g., report requests will be those packets coming from the Base Node just before a Service Node starts sending a big amount of data) and, as the header is not encrypted nor covered by the integrity protection mechanism of the Security Profile 1, it is possible to change the LCID or any other header field as desired. One important restriction in this mode is that the WK are different for each device and session, making it possible to replay traffic obtained only from the same device in the period of time where the node is still registered and using the same WK. It is worthwhile to mention that any change in the packet requires computing the CRC again.

Enabling Security Profile 1 drastically reduces the attack surface regarding replay attacks. However it would be possible to reduce it even more if the integrity protection (SCRC) would cover the packet header as well.

4. Validation

In order to complete the vulnerability analysis covering the physical and link layers of the protocol stack present in PRIME NB-PLC networks, it is necessary to validate the attacks described in Section 3. In the present section, the tools and infrastructures involved in the validation process are described, and the validation results are explained.

4.1. Validation Tools and Infrastructures

4.1.1. Cyberphysical Infrastructures. The cyberphysical infrastructures available for this work are as follows: (1) a small metering panel located in the laboratory of the research group and (2) part of the research infrastructure available in the Grid Integration Laboratory (LINTER) of Unión Fenosa Distribución [30].

The smart metering panel installed in the laboratory includes the following: a PRIME Base Node, 4 PRIME smart meters (Service Nodes), and a traffic sniffer, which were used to perform basic tests in a controlled environment.

In addition to the smart metering panel, the collaboration with one of the major DSOs in Spain (Unión Fenosa Distribución) as part of the Spanish Research Project OSIRIS [31] included different tests and measurements in LINTER, their Smart Grid laboratory. This laboratory is equipped with 2 transformation centers, distributed generation capabilities, different Base Nodes, and more than a hundred Smart Meters from different manufacturers, as well as different tools such as a signal generator, oscilloscope, or attenuators.

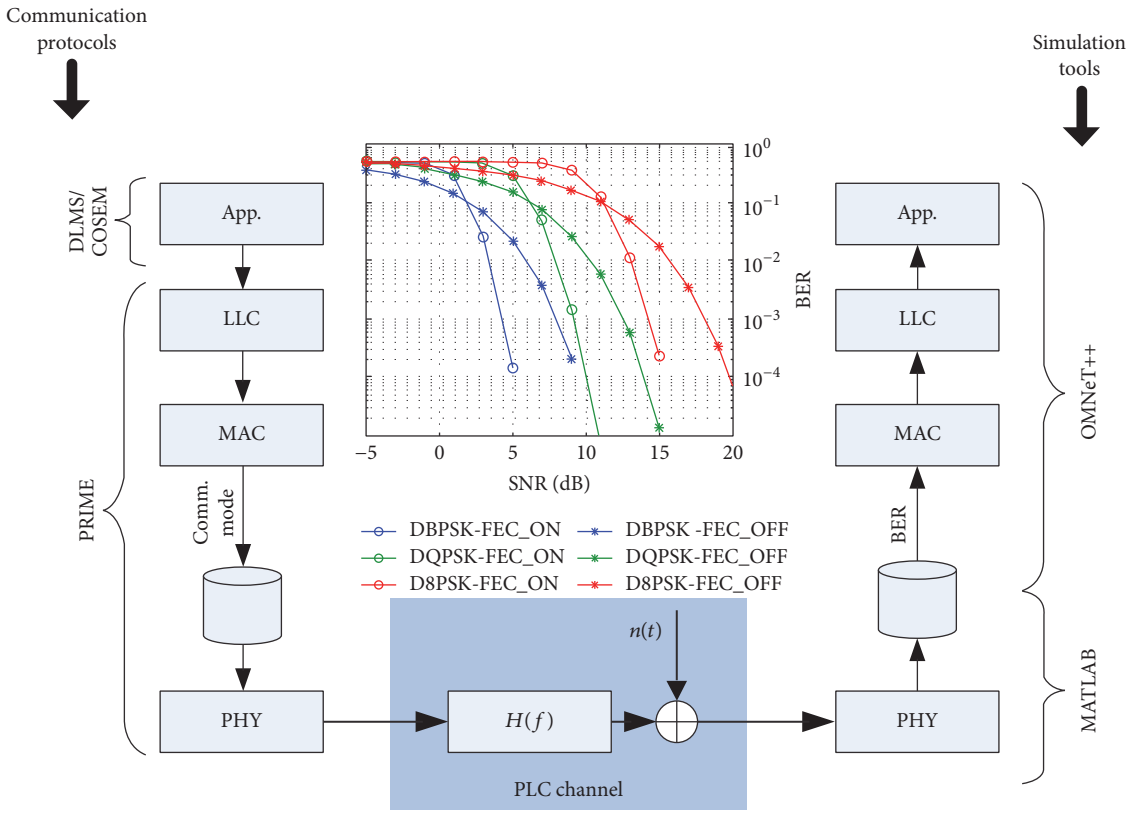


Figure 12: Architecture of the PRIME network simulator [22].

4.1.2. PRIME Network Simulator. A PRIME network simulation tool was used to validate some of the attacks described in this work. It is based on the simulator developed in [22], which combines MATLAB and OMNeT++ to model the effects of the PHY and upper layers (MAC and Logical Link Control (LLC)) of the PRIME protocol. Application layer is modeled as a payload. Figure 12 shows the architecture of the simulator.

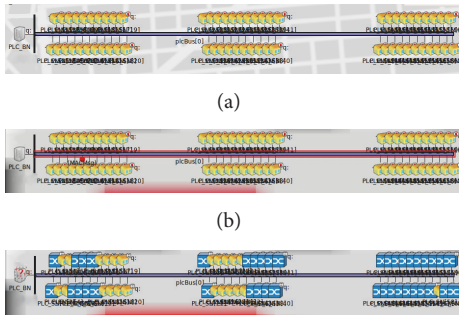
The interaction between MATLAB and OMNeT++ is performed in the PHY layer as follows: knowing the transmission power and the base noise level when a node sends a message to another one, the received power is calculated based on a matrix containing the attenuation between each pair of nodes. With the received power and the base noise level, the SNR is obtained in OMNeT++. Knowing the SNR and the constellation, the BER can be obtained using SNR versus BER tables previously calculated in MATLAB (see Figure 7). OMNeT++ uses the BER value to decide if the message received contains errors (and must be discarded) or was received correctly (and can be processed by the upper layers).

The functionality of the original simulator has been extended to allow assessing the performance of given network topologies and configurations under different noise conditions [32]. In addition, for the validation of part of the identified vulnerabilities, the behavior of a malicious node has been implemented to allow simulating different attacks and evaluating its effects in the network performance The results are validated comparing the results from an scenario under attack with the same scenario in normal conditions.

For all the tests, the simulated scenario was the one represented in Figure 13(a), including a Base Node and 63 smart meters (Service Nodes) distributed along a power line, where one of the Service Nodes represents an attacker performing one of the different analyzed attacks. Each test consists in running the simulated scenario, while the Base Node requests consumption reports sequentially to each one of the Service Nodes. A total number of 4 parallel and independent simulations were ran for 10000 seconds each in order to get a significant number of output values. The most relevant output value is the *TTRi*, an indicator of the time needed to read a smart meter which measures the time between the request of a report from the Base Node (usually a report containing the electricity consumption of a household) and the response from the smart meter.

4.1.3. Synthetic Traces. Some of the attacks could not be validated in cyberphysical infrastructures due to the lack of technical resources to perform some of the tests. The validation using a network simulator was not possible either as, for some specific attacks, the expected results are highly dependent on the implementation of the devices. For this reason, a forensic NIDS was developed to validate the use of this kind of solution to detect the aforementioned cyberattacks against PRIME networks.

The NIDS was tested using synthetic traces that were created from real traffic traces obtained in the field. These



(a)

(b)

(c)

Figure 13: Simulated scenario under (a) no attack; (b) jamming CSMA/CA; (c) PN Flooding.

```
13:32:07.9,156638108,380,PRO,UP,000,OK,2d,1c59,2,11,OK,PRO_REQ_S RQ: 03 TIME:
13:32:08.0,156638188,80,PRO,UP,000,OK,20,1e25,2,11,OK,PRO_REQ_S RQ: 01 TIME:
13:32:08.6,156638789,601,ALV,DW,000,OK,03,1df2,2,3,OK,ALV_B Count: (rx 2|tx 3
13:32:08.7,156638928,139,PRO,UP,000,OK,20,1e5b,2,11,OK,PRO_REQ_S RQ: 06 TIME:
13:32:08.8,156638988,60,PRO,UP,000,OK,00,1cc1,2,11,OK,PRO_REQ_S RQ: 04 TIME:
13:32:08.8,156639048,60,REG,UP,000,OK,17,1d0c,2,8,OK,REG_UNR_S TIME: 00 EUI48
13:32:08.8,156639049,10,REG,DW,000,OK,17,1d0c,2,8,OK,REG_UNR_B TIME: 00 EUI48
13:32:08.8,156639050,60,REG,UP,000,OK,17,1d0c,2,8,OK,REG_UNR_S TIME: 00 EUI48
13:32:08.0,156639180,122,ALV,DW,000,OK,03,1eff,2,3,OK,ALV_B Count: (rx 1|tx 6
13:32:09.0,156639218,38,PRO,UP,000,OK,00,1c70,2,11,OK,PRO_REQ_S RQ: 02 TIME:
```

Figure 14: Fragment of a PRIME traffic trace under an unregistration attack.

traces were altered to add the packets involved in each specific attack. Figure 14 shows a fragment of one of these traces.

The NIDS developed is an extension of our previous proof-of-concept forensic web application developed under the scope of the Project OSIRIS. It allows importing network traces directly in the format given by the data concentrator, imports them in a common format into a database, and analyzes patterns that may imply an attack, alerting the attack or attacks detected and the most relevant metrics for each one of them. Figure 15 shows the output of the web application.

4.2. Validation Results

4.2.1. Physical Layer Jamming. Jamming attack was validated in the scope of noise testing in the Project OSIRIS. The tests were carried out in the LINTER where, using a waveform generator and a signal coupler, previously recorded noise signals were replayed in the laboratory environment. The jamming signal under study in this work can be found in Figure 16 and is associated with the charging process of an electric vehicle. The scenario included a Base Node and 76 smart meters (Service Nodes).

The tests consisted in recording the traffic trace in normal conditions for 10 minutes, then injecting the noise signal for 10 minutes, and finally switching off the noise signal to record a recovery period of 10 minutes. After that, the traffic traces were analyzed to extract the number of disconnection messages as a metric of network stability. The physical location of the disconnected nodes was also analyzed.

The results were the following: 132 disconnection messages in the 10-minute period prior to the noise injection, 242 disconnection messages during the 10-minute period when the noise was injected, and 431 disconnection messages during the 10-minute after the noise injection. These results show that although in the first minutes of the attack most of

Figure 15: Output of the forensic NIDS system.

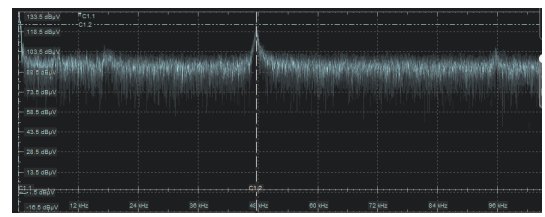


Figure 16: Jamming signal replayed in the laboratory.

the smart meters were losing connectivity, they were able to reconnect for small periods of time before losing connectivity again. The high number of disconnection messages in the 10 minutes after the noise injection is related to 2 facts: (1) the disconnection messages are triggered after a keep-alive timeout expires; (2) the network becomes very unstable after the attack. It was also observed that the most affected nodes were the ones physically closest to the noise injection socket as it was expected.

4.2.2. CSMA/CA Jamming. CSMA/CA jamming attack was validated with the PRIME network simulator, where a smart meter (Service Node) was modified to perform a CSMA/CA jamming attack. This modification consists in changing the CSMA/CA implementation of the node to send a packet every time the node detects that the channel is busy, causing a collision. Figure 13(b) illustrates the scenario when a collision is happening.

The results are shown in Table 2. As we can see in the table, introducing a CSMA/CA attack hinders the communications, allowing obtaining very few results (22 and 3) compared with the simulations in normal conditions (1398 successful readings). In the tests performed, the attack is effective independently of the position of the attacker as the transmission power was high enough to propagate through the whole transmission line. The mean of the time needed to obtain the reading is a bit larger under attack conditions, and the standard deviation is much larger in the case with the attacker at the beginning of the line, due to the fact that the attack destabilizes the network. The standard deviation in the case of an attacker at the end of the line is not representative, as only 3 results were obtained.

4.2.3. Promotion Needed Flooding. Promotion Needed Flooding was validated with the PRIME network simulator, where a smart meter (Service Node) was modified to never connect to the Base Node and continuously send PNPDU messages instead. Figure 13(c) illustrates the scenario during the simulation, showing a significant increase on the number

Table 2: CSMA/CA jamming results.

	No attack	Attacker at the beginning of the line	Attacker at the end of the line
Number of of *TTRi* results	1398	22	3
TTRi mean	12.52	18.03	13.55
TTRi standard deviation	1.32	7.94	0.29

Table 3: Promotion Needed Flooding results.

	No attack	Promotion Needed Flooding attack
Number of *TTRi results*	1398	119
TTRi mean	12.52	13.55
TTRi standard deviation	1.32	3.61

of switches (up to 40 switches according to the simulations), as expected in this kind of attack.

The results are shown in Table 3. The column # of *TTRi* results represents the number of successful readings from the smart meters. As we can see in the table, introducing a Promotion Needed Flooding attack has a severe impact on the communications, as the network gets congested by the PNPDU messages and the Promotion Request Messages which are triggered result in too many smart meters being promoted to Switch, which overcomplicates the logical topology of the network. Although only a few smart meters are able to send their reports, the mean and standard deviation of the time needed to obtain the reading are not significantly larger under attack conditions.

4.2.4. Node Registration Overflow. Node registration overflow attack is highly dependent on the implementation of the manufacturers, so the validation was focused on validating the use of a NIDS to detect this kind of attack. The NIDS module was implemented to search in the traces for the number of different LNIDs in defined time slots. The developed tool allows changing both the threshold of the number of different LNIDs and the length of the subintervals can be changed. The tests were performed for a threshold of 10000 new LNIDs in slots of 600 seconds, meaning that an attack will be detected if there are more than 10000 different LNIDs in less than 600 seconds.

The system was validated with synthetic traces simulating a scenario under attack and several real traces in scenarios that were not under attack.

4.2.5. Node Registration Spoofing. This attack was validated in the smart metering panel installed in the laboratory of the research group. The node registration spoofing attack was performed by changing the timeout in the Base Node to the highest value so it will never unregister a node. This means that if one smart meter connects to the network and then is physically switched off and on again, it will register again sending the same packet an attacker would send, thus emulating the effect of a registration spoofing attack.

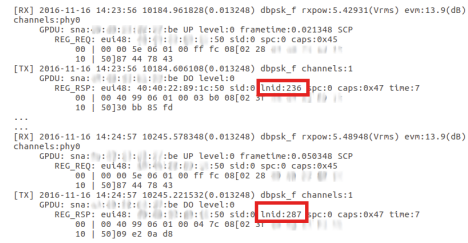


Figure 17: Traffic traces during a node registration spoofing attack.

Figure 17 illustrates the effects of the attack. A first registration request is sent and the Base Node registers the node with LNID 236. Then a second registration request is sent and the Base Node registers the node with LNID 287. This confirms that the Base Node manufacturer implemented the second behavior from the ones described in Section 3 for the present vulnerability. If an attacker spoofs this second registration request, the Base Node will change its LNID, so the victim will stop receiving packets and the attacker will hijack the communications. If the attacker and the victim are nearby, the victim may receive the unsolicited registration response, and update its LNID, but such a behavior is not specified in the standard so it is dependent on the implementation. If the attacker and the victim are far away and connected through different switches, then the victim will not see any anomalous packet and will just stop receiving packets addressed to it.

4.2.6. LSID Overflow. LSID overflow attack is also highly dependent on the implementation of the manufacturers, so the validation was focused as well on validating the use of a NIDS to detect this kind of attack. The NIDS module in this case was implemented similarly to the LNID overflow module to search in the traces for the number of different SIDs in defined time slots. Same as in the LNID case, both the threshold of the number of different SIDs and the length of the subintervals can be changed. The tests were performed for threshold of 200 new SIDs in slots of 3600 seconds, meaning that an attack will be detected if there are more than 200 different SIDs in less than 3600 seconds.

As in the LNID case, the system was validated with synthetic traces emulating a scenario under attack and several real traces in scenarios that were not under attack. The system was able to identify the attack with no false positives or negatives, as the thresholds were high. Lowering the thresholds would allow early detection of these attacks, with the disadvantage of rising the probability of false positives.

Figure 15 shows the output of the developed NIDS in the event of a LSID overflow attack, including the number of LSIDs detected for a better diagnosis of the attack.

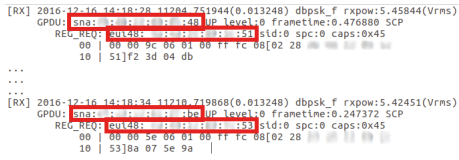


Figure 18: Traffic traces during a Base Node spoofing attack.

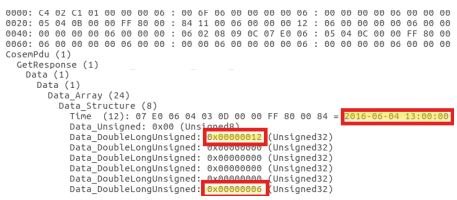


Figure 19: A report sent from a smart meter can be read by an attacker.

4.2.7. Base Node Spoofing. The Base Node spoofing attack was tested in the smart metering panel, where the sniffer has the functionality to emulate a Base Node. Plugging this emulated Base Node to the original network and capturing the traffic traces allows validating whether the emulated Base Node is able to hijack the smart meters, disappearing from the original Base Node, or not.

An example of how a smart meter connects to the malicious Base Node is shown in Figure 18, where, in the first packet, we can see the smart meter with MAC address ending in :51 requesting connection to the Base Node with MAC address ending in :48. In the second packet, less than 10 seconds later, another smart meter in the same panel with MAC address ending in :53 requests connection to the malicious Base Node with MAC address ending in :be. It was observed that the effects of the attack are not immediate. The smart meters should disconnect from the legitimate Base Node and then they will connect to the Base Node that offers the best connectivity, so this attack is more effective when executed together with an attack that causes smart meters to disconnect (e.g., jamming attacks).

4.2.8. Sniffing. The sniffing attack was validated in the smart metering panel with Security Profile 0 (no encryption) configured. The validation for this kind of attack consists in enabling the sniffer while a consumption report is under request. The response can be interpreted from the hexadecimal trace as shown in Figure 19, where the date and the consumption data are obtained from the trace.

4.2.9. Demotion/Unregistration/Disconnection Spoofing. For the demotion/unregistration/disconnection attack, the validation was focused on validating the use of an NIDS for attack detection. The NIDS module was implemented to search in the traces for *REG_UNR_S* → *REG_UNR_B* → *REG_UNR_S* patterns in defined time slots. Same with demotion and disconnection packets.

The system was validated with synthetic traces simulating a scenario under attack and several real traces in scenarios that were not under attack. Tests were performed with time slots of 20 seconds where the system was able to identify the attack, but there were false positives in some of the real scenarios. This happens when a smart meter sends REG_UNR_S twice and the response from the Base Node arrives in between. For this reason, it is important to perform further checking for the alerts.

4.2.10. Security CRC and Traffic Replay. Security CRC and traffic replay attacks will not be validated as they require a traffic injection tool that was not available in the validation infrastructures presented at the beginning of this section.

5. Discussion

After unveiling and validating the vulnerabilities present in PRIME standard, this section evaluates the results and discusses their impact and solutions from a practical point of view, taking into consideration different factors present in real deployments. Table 4 summarizes the vulnerabilities analyzed in this work, describing its impact and enumerating the possible solutions. The discussion will be focused on security and privacy. Recommendations and good practices addressed to the DSOs will wrap up this section.

5.1. Security. According to Table 4, the main security issue in PRIME is the possibility of performing DoS attacks. This kind of attack implies an impact to the DSO, as it has to analyze the situation and send technicians to diagnose and solve the problem or even confront the clients' complains, which can be translated in expenses of time and money. Besides, other Smart Grid applications such as DR and distributed generation (DG) are very sensitive to real-time information and to DoS attacks. The countermeasures against this kind of attacks are defined in their description and can be summarized into the following: (1) encrypting communications in order to avoid traffic injection and (2) using NIDS to detect the attacks.

Other vulnerabilities as Security CRC are not exploitable in practice, as most of the devices implement encryption hardware (e.g., see Figure 3 in [24]). Taking control of a device via traffic replay could be possible, but the probability of success in this kind of attacks can be neglected when using Security Profile 1 or any security measures in the upper layers.

DSOs are aware of these potential issues and, to the best of the authors' knowledge, they are starting to deploy security measures in field by enabling the security options available in the upper layers (i.e., DLMS/COSEM) but not in PRIME. This protects the network against sniffing and replay attacks but leaves the network unprotected against most of the DoS attacks described in this work. Most commercial Base Nodes include whitelisting capabilities, but that does not solve most of the security issues present in PRIME networks. Another solution proposed in this work is using filters that isolate the power distribution lines from the domestic infrastructure. However, this represents an expensive solution which is currently being deployed just in few premises located in very noisy environments, but not as a security measure, leaving the

Table 4: Summary of vulnerabilities, impact, and solutions.

Vulnerability	Impact	Solutions
Physical layer jamming	Severe DoS in a part of the network	Install filters that block the signal from the smart meter to the household.
CSMA/CA jamming	Severe DoS in a part of the network	Install filters that block the signal from the smart meter to the household.
Promotion Needed Flooding	Saturates the traffic Complicates the logical topology Can result in DoS	Limit PNPDU bursts Base node implementing whitelisting Not accepting promotions triggered by PNPDUs from registered nodes NIDS near the base node
Node registration overflow	Can cause DoS in some nodes	Use of encryption (Security Profile 1) Base node implementing whitelisting Base node implementing random LNID assignation after overflow
Node registration spoofing	Targeted DoS	Use of encryption (Security Profile 1)
LSID overflow	Can cause DoS in several nodes	Use of encryption (Security Profile 1) Base node implementing random LSID assignation after overflow NIDS near the base node
Base Node spoofing	Can cause DoS in several nodes Privacy issues	NIDS distributed along the network
Sniffing	Privacy issues	Use of encryption (Security Profile 1)
Demotion/unregistration/disconnection spoofing	Targeted DoS (disconnection/unregistration) Can cause DoS in several nodes (demotion)	Use of encryption (Security Profile 1) NIDS near the base node
Security CRC	May cause DoS	Use of encryption hardware
Traffic replay	Privacy issues Take control of the smart meters	Use of encryption (Security Profile 1) drastically increases the difficulty of this attack

door open for attackers to connect to a PRIME network from any power socket inside the houses.

5.2. Privacy. The main privacy issues in PRIME deployments are sniffing attacks in unencrypted networks. As mentioned before, this is starting to get solved by the DSOs with the use of encryption in the upper layers. Using encryption (i.e., Security Profile 1) in PRIME is the best solution against attacks, but not a perfect solution for privacy, as it does not feature Forward Perfect Secrecy. This means that all the communications can be recorded and, when the keys are broken, all can be decrypted. PRIME standard does not specify how the derived keys are calculated and set in the devices, where manufacturers usually hard-code them in the firmware. As normal firmware updates are performed using the same firmware image for all the devices, researchers demonstrated that the same key is stored in every smart meter, being possible to extract this key by looking into the firmware [29]. There are other privacy issues which are not PRIME vulnerabilities but still can be exploited against privacy. One of these issues is present in the smart meters as shown in Figure 20. If an attacker has physical access to the smart meter its trivial to obtain its EUI-48 unique address through the smart meter's display, which can be used

Figure 20: The EUI-48 address is shown in the smart meter. The address is shown in two parts, where the latter is censored for privacy reasons.

by an attacker to map the EUI-48 to their temporary NID. Therefore the attacker is able to identify users in sniffing attacks or target them in DoS attacks.

5.3. Recommendations. In order to protect PRIME networks against security and privacy threats, the authors highly recommend DSOs to make use of Security Profile 1 in their deployments, which enables encryption and prevents the

attacker from snooping or injecting the malicious packets needed to perform most of the attacks, as it is mentioned in their description.

It is also recommended the development and use of NIDS solutions adapted to this kind of scenarios in the Base Node, normally located in secondary substations. Early detection of attacks where this solution was proposed is allowed by this technique; thus their impact could be reduced.

To solve the key exchange problem present in the PRIME standard, it is necessary that the PRIME Alliance makes an effort to include key exchange methods in the standard. There is research on key management in wireless networks where efficient key distribution and management mechanisms are discussed [33]. These mechanisms can be easily adapted to the case of PLC networks such as PRIME.

6. Conclusion

This paper provides an insight on the vulnerabilities detected in the PLC PRIME standard and presents a set of recommendations to increase the security and privacy in this kind of networks, which are being broadly deployed in Europe and starting its expansion all around the globe.

To be precise, the paper introduces the problem of cybersecurity in the Smart Grid, focusing on AMI and describing the PRIME standard, and emphasising its security features. Then, the detected vulnerabilities are explained in detail, giving a further insight on their impact and solutions. The vulnerabilities are validated, explaining the procedures, tools, and infrastructures involved. The paper ends discussing the current deployment scene in terms of security and privacy and giving recommendations to the main actors involved in PRIME networks.

The analysis carried out in this work is crucial to improve the security of PRIME specifications by the PRIME Alliance, the implementation by the manufacturers, and the deployment by the DSOs. A set of recommendations is given to these entities so that the security and privacy risks could be minimized.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The research leading to these results has been partly funded by the Spanish Ministry of Economy and Competitiveness through Project OSIRIS (RTC-2014-1556-3) and by the Network of Excellence REDYD2050 (ENE2015-70032-REDT). The authors would like to acknowledge the entire OSIRIS Consortium and REDYD2050 members. The authors would also like to thank Professor Dr. Javier Matanza (ICAI School of Engineering) for his valuable support with the PRIME network simulator.

References

[1] European Commission, "Com/2014/356/final: benchmarking smart metering deployment in the eu-27 with a focus on electricity," 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2014:0356:FIN.

[2] Ministerio de industria and energía y turism, "Orden iet/290/2012," 2012, http://www.boe.es/boe/dias/2012/02/21/pdfs/BOE-A-2012-2538.pdf.

[3] European Commission, *Communication from the commission to the council and the european parliament—critical infrastructure protection in the fight against terrorism*, 2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:EN:NOT.

[4] SmartGridNews, *Malta's smart meters scandal*, 2014, http://www.smartgridnews.com/story/maltas-smart-meter-scandal-41-millio n-worth-electricity-stolen/2014-02-18.

[5] European Commission, *2012/148/eu: commission recommendation of 9 march 2012 on preparations for the roll-out of smart metering systems*, 2012, http://eur-lex.europa.eu/legal-content/EN/ALL/.

[6] NIST, "Guidelines for smart grid cyber security," 2014, http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[7] N. Andreadou, M. Guardiola, and G. Fulli, "Telecommunication technologies for smart grid projects with focus on smart metering applications," *Energies*, vol. 9, no. 5, p. 375, 2016.

[8] N. Uribe-Pérez, L. Hernández, D. de la Vega, and I. Angulo, "State of the art and trends review of smart metering in electricity grids," *Applied Sciences*, vol. 6, no. 3, pp. 1–24, 2016.

[9] G. López, J. I. Moreno, H. Amarís, and F. Salazar, "Paving the road toward smart grids through large-scale advanced metering infrastructures," *Electric Power Systems Research*, vol. 120, pp. 194–205, 2015.

[10] S. Galli, A. Scaglione, and Z. Wang, "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, 2011.

[11] C. Cano, A. Pittolo, D. Malone, L. Lampe, A. M. Tonello, and A. G. Dabak, "State of the art in power line communications: from the applications to the medium," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 7, pp. 1935–1952, 2016.

[12] "Recommendation itu-t g.9904. narrowband orthogonal frequency division multiplexing power line communication transceivers for prime networks," Tech. Rep. ITU-T, 2012, http://www.itu.int/rec/T-REC-G.9904-201210-I/en.

[13] A. Haidine, A. Tabone, and J. Muller, "Deployment of power line communication by European utilities in advanced metering infrastructure," in *Proceedings of the 17th IEEE International Symposium on Power Line Communications and Its Applications (ISPLC '13)*, pp. 126–130, IEEE, Johannesburg, South Africa, March 2013.

[14] "Specification for PowerLine Intelligent Metering Evolution v1.4," Tech. Rep. PRIME Alliance, 2014, http://www.prime-alliance.org/wp-content/uploads/2014/10/PRIME-Spec_v1.4-20141031.pdf.

[15] CENELEC, "Signalling on Low-Voltage Electrical Installations in the Frequency Range 3 kHz to 148,5 kHz—Part 1: General Requirements, Frequency Bands and Electromagnetic Disturbances," Tech. Rep. en 50065-1, European Committee for Electrotechnical Standardization, April 2011, http://standards.globalspec.com/std/1379982/cenelec-en-50065-1.

[16] A. Sendin, I. Urrutia, M. Garai, T. Arzuaga, and N. Uribe, "Narrowband PLC for LV smart grid services, beyond smart

metering," in *Proceedings of the 18th IEEE International Symposium on Power Line Communications and its Applications (ISPLC '14)*, pp. 168–172, IEEE, Glasgow, UK, March-April 2014.

[17] Excerpt from Compation Specification for Energy Metering - Architecture and Protocols, DLMS User Association,.

[18] Excerpt from COSEM - Identification System and Interface Classes, DLMS User Association,.

[19] DLMS/COSEM over PLC security of meter data exchange over open networks, DLMS User Association,.

[20] M. Seijo, G. Lopez, J. I. Moreno et al., "Let there be light: Dissecting how PRIME networks work based on actual traffic traces," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm '15)*, pp. 472–477, November 2015.

[21] J. Matanza, S. Alexandres, and C. Rodríguez-Morcillo, "Advanced metering infrastructure performance using European low-voltage power line communication networks," *IET Communications*, vol. 8, no. 7, pp. 1041–1047, 2014.

[22] N. Hadjsaïd and J. Sabonnadière, *Smart Grids*, John Wiley & Sons, Inc., Hoboken, NJ, USA, 2013.

[23] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[24] S. T. Microelectronics, "St7590 prime compliant power line networking soc design guide," Tech. Rep., http://www.st.com/resource/en/application_note/dm00107740.pdf.

[25] C. Shahriar, M. La Pan, M. Lichtman et al., "PHY-layer resiliency in OFDM communications: a tutorial," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 292–314, 2015.

[26] J. Konorski, "A game-theoretic study of CSMA/CA under a backoff attack," *IEEE/ACM Transactions on Networking*, vol. 14, no. 6, pp. 1167–1178, 2006.

[27] A. L. Toledo and X. Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 347–358, 2008.

[28] L. Mokdad, Y. Hammal, J. Ben-Othman, and A. Abdelli, "Formal modeling and analysis of greedy behaviors in IEEE 802.11 protocols," in *Proceedings of the IEEE International Conference on Communications (ICC '15)*, pp. 3579–3584, June 2015.

[29] J. Vazquez Vidal and A. Garcia Ilera, "Lights off! the darkness of the smart meters," *BlackHat*, 2014.

[30] LINTER, "Grid Integration Laboratory," https://www.unionfenosadistribucion.com/en/smart+grids/research+and+development/1297137260045/find+out+about+our+laboratory.html.

[31] OSIRIS, "Optimización de la Supervisión de la Red de DIStribución," http://www.proyecto-osiris.com/.

[32] M. Seijo, G. López, J. Matanza, and J. I. Moreno, "Planning and performance challenges in power line communications networks for smart grids," *International Journal of Distributed Sensor Networks*, vol. 2016, Article ID 8924081, 2016.

[33] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2314–2341, 2007.