Cyber security vulnerabilities of smart metering based on LPWAN wireless communication technologies

Carine Zaraket, Panagiotis Papageorgas, Michel Aillerie, Konstantinos Agavanakis, Chafic Salame

Cyber Security Vulnerabilities of Smart Metering Based on LPWAN Wireless Communication Technologies

Carine Zaraket[1,a)], Panagiotis Papageorgas[2,b)], Michel Aillerie[1,c)], Kyriakos Agavanakis[2,d)] and Chafic Salame[3, e)]

[1] Université de Lorraine, CentraleSupélec, LMOPS, F-57070 Metz, France
[2]Department of Electrical and Electronics Engineering, University of West Attica, P. Ralli & Thivon 250, 12244, Athens, Greece
[3]Lebanese University – Faculty of sciences-90656 Jdeidet, Lebanon

[a)] Corresponding author: carine.zaraket@hotmail.com
[b)] ppapag@uniwa.gr
[c)] aillerie5@univ-lorraine.fr
[d)] k.agavanakis@uniwa.gr
[e)] salame@ul.edu.lb

Abstract. Smart Metering allows utilities to get a remote and instant reading of the electronic meters used for Electricity power consumption and water utilization. Despite all the advantages presented by the smart metering system, there are always some challenges to be faced, such as security and communication. Cyber-attacks not only may threaten the consumer's privacy but they can even lead to a compromised system with direct implications on people's safety and society activities. On the other hand, nodes Geo-location may also impose problems, when they are geographically dispersed and hard to reach from the usual cluster. The provisioning of such a large number of smart meters directly affects the operational cost expenditures. The same is true when there is not currently an appropriate communication infrastructure. Wireless technology offers an easier, faster, and cost-effective approach. To discuss and answer the above challenges, Low Power Wide area networks (LPWAN) technologies are considered, with special focus on Long Range/Low Power Wide Area Network (LoRa/LoRaWAN) technology which facilitates long-range wireless, as they seem promising to anticipate for many of the recognized problems. Accordingly, for building such a reliable LPWAN-based smart metering infrastructure, applicability, feasibility, and cybersecurity vulnerabilities have to be examined using the existing literature.

Keywords: IoT, LPWAN, Energy Smart Metering Solution, Zigbee, Z-wave, 6LoWPAN, Sigfox, LoRa, LoRaWAN, NB-IoT, Cyber-Security**.**

INTRODUCTION

With the growth of electricity demand by modern societies and the degradation of fuel resources, the integration of distributed renewables energy resources to compensate these needs becomes a must. To integrate these resources governments have focused on converting the conventional electricity grids to be smarter and more efficient. Smart Grid (SG) is an enhancement of existing grids that utilizes ICT (Information and Communication Technologies) to improve the efficiency, sustainability, and reliability of power grids. SG as a cyber-physical system overlays the traditional grid with an IoT (Internet of Things) network that consists of Smart Meters (SM) to contribute to the management, control, and monitoring of consumption parameters in near real-time. Building a smart grid is based on introducing a chain of technologies that include Smart sensors, IT systems, Smart meters, and communication networks [1]. For example, smart metering, which is a basic function in smart grids, permits the provider to have an overview of the user power consumption in real-time and to modulate the amount of generated power to satisfy the user's energy needs without any unnecessary waste. Since smart metering is based on embedded systems and communication technologies it is in the risk of cyber-attacks, despite all its advantages. Smart meters are distributed everywhere. Both the smart meter and the transmission medium are physically exposed to hackers. Therefore, the data collected by meters are exposed and could be sniffed, intercepted, altered or the meter itself could be compromised, with a wide variety of negative side effect to the whole network infrastructure. Hence, to protect the privacy and the integrity of these readings it is important to highlight the crucial role of security and to consider it from the very early of the SG design and throughout the whole lifecycle of the system implementation and evolution.

Moreover, while the majority of meters are installed in clustered areas, there are still some nodes hard to reach placed far away from any available cluster. Although these nodes are not many in quantity, studies show that 1% of these nodes can account for 50% of the entire network operational cost. Therefore, up to 50% of the unnecessary cost can be saved by the integration of Low Power Wide area networks (LPWAN) wireless communication technology for solving this 1% problem. Also, recent studies have mentioned that over the past several years, LPWANs have received a lot of hype in the IoT sector because of their suitability for many IoT applications for sensing and actuation. With the adoption of LPWAN technologies for smart metering, it is expected that the number of SM connected will reach 153.3 million out of 1.2 billion smart meters in total, that will be installed over the next ten years—a small but growing share of 12.7%—according to a new study published [2]. So it is obvious that LPWAN is reserving its place in the smart metering systems in the upcoming years with the freedom and flexibility that wireless communication technologies provide.

This paper focuses on defining a detailed approach of the Advanced Metering Infrastructure (AMI) system. It examines the communication requirements and discusses the communication architecture of the AMI by studying the speciation and security vulnerabilities of different used short-range wireless technologies and LPWAN which their integration will affect the smart metering infrastructure. The organization of the article is as follows: the first section gives an overview of a smart metering system, the second section defines what are the different existing communication networks (focusing on wireless technologies) that are used in the last mile of a smart metering infrastructure and their security basics, section three presents and compares the different security vulnerabilities of the wireless communication technologies based on the existing literature, while section five lists the suggested security improvements released for AMI and finally the article conclusions and recommendations.

I. SMART METERING SYSTEM

A Smart Grid is the new generation of the conventional electricity infrastructure that is going to be a solution to improve the electrical energy system not only by integrating Renewable Energy Resources (RES), but also the Distributed Generation (DG) and Distributed Storage (DS). Smart Grid targets to solve different existing problems in power delivery, answer the climate changes, improve energy efficiency, and open a new direction in electricity markets (like Peer-to-Peer P2P energy trading). A direct implication of the Smart Grid is to have an electric model that is capable to manage different generation and storage devices in an efficient and decentralized way by deploying an Advanced Metering Infrastructure.

Advanced Metering Infrastructure AMI

The latest infrastructure investments focus on the metering part, with the Automated Meter Reading (AMR) as the first trial, which provides utilities with basic remote information about the energy consumption records of each consumer-user [3]. But the AMR system was limited only to a remote reading and cannot provide utilities with any new additional information or data due to the support of a one-way communication system. This limitation pushed utilities to move towards Advanced Metering Infrastructure (AMI) and Smart Metering. With AMI, utilities can establish bidirectional communication with the meter, to evaluate the grid status and to remotely connect, disconnect, and even to configure the electricity service [4]. The latest Smart Metering Systems allow utilities to manage and control the gird based on an improved architecture that cooperates with smart sensors and distributed control technology [5]. Moreover, AMI provides consumers with the ability to access their data through Internet applications to control and manage their power usage, pay bills, and to sell their excess of generated electricity from renewables. With AMI, renewable energy sources at the consumer's premises can be integrated into the smart grid [6]. Figure 1 shows the evolution from AMR to AMI with lists of stakeholders and benefactors for each step [7].

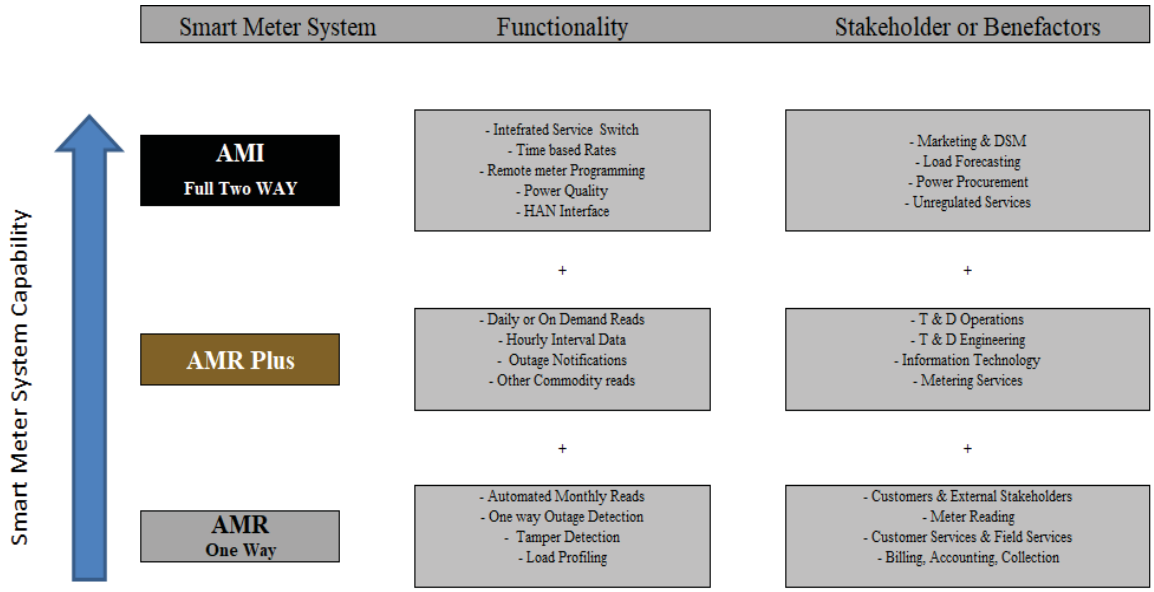

FIGURE 1. Evolution of Smart Metering.

Smart Meter

The Smart Meter (SM) is the main component of AMI. SM provides an accurate and remote measurement reading and it communicates with smart home appliances to manage their power consumption efficiently. These functionalities are realized through two-way communication and advanced sensors [9]. A SM has two main communication functions, one to send the data to the utility and receive commands from the Grid operator, and the second is to exchange data with the Home Energy Management System (HEMS) [10]. Also, some SMs are equipped with a web application that helps consumers to control their energy usage and to be aware of their consumption [11]. In general, the main SM characteristics are summarized by energy metering, communication with other intelligent devices like sensors, and time-based pricing. In addition to the previously mentioned characteristics come the security features that include security data encryption and energy theft detection [11].

Mainly, a SM is composed of four parts:

- Analog Frond End signal conditioning metering subsystem,
- Communication interfaces,
- Micro Controller Unit (MCU),
- Power system.

The AnalogFrond End signal conditioning metering subsystem integrates the electronics for signal conditioning (amplification, antialiasing filtering, offset compensation) for the voltage and current analog signals before digitization. The Microcontroller Unit (MCU) contains Analog to Digital Converter (ADC) and Digital to Analog Converter (DAC). MCU's main role is to control inputs and outputs, to keep track of time stamp operation, to preprocess the metering data (digital filtering, harmonics calculations, statistics, encryption, and decryption of measurements) and to store data in RAM, ROM, EEPROM, or Flash memories. Also the meter activities logs are saved by the MCU [12]. The communication interfaces are either wired or wireless allows the meter to communicate with the grid and the end user's Home Area Network (HAN). The power subsystem is used to power the electronic components of the smart meter through a switched-mode power supply that converts the mains line alternating current AC to direct current DC. When there is no power from the mains line a backup system based on a battery AC/DC is activated automatically. This battery is used only in case of a mains line power failure. The American National

Standards Institute (ANSI) and the International Electro-Technical Commission (IEC) are the two organizations for smart meter standards in the USA and Europe. For example, the IEC 62052 Electricity metering equipment defines the General requirements, tests, and test conditions, the IEC 62052-11 with Part 11 defines the Metering equipment, the IEC 62052-31 with Part 31defines the Product safety requirements and tests, the IEC 62053-22 with Part 22 defines the Static meters for reactive energy (classes 0.2 S and 0.5 S)), and the IEC 62056 Electricity metering defines the Data exchange for meter reading, tariff, and load control, etc.

FIGURE 2. Shows examples of ANSI and IEC smart meters [13][14].

Communication Networks

The communication technologies used in SMs are either the wired like a power line carrier (PLC) or the wireless one using radio frequency (RF) transceivers following a plethora of networking technologies like mobile telephony while recently LPWAN technologies are taking an important part of this sector. Each of these technologies has its advantages and disadvantages in an application, for example using wireless communication technologies can be straightforward for hard to reach geographically isolated areas where the infrastructure cost is low in comparison with the wired technologies. However, with the wired technologies the interference problems do not exist and the electrical wiring for energy transfer can be utilized for communication. In a Smart Metering System the data transmission through power-line communication, wireless communications, cellular technologies or the Internet must be guaranteed in terms of time, quality, and security. The communication technologies should cover the security requirements such as:

- Security
- Bandwidth needed,
- Geographical coverage based on the environment (internal/ external)
- Power quality with the minimum number of repetitions [15].

Therefore, utility selects the best technology based on technology availability, reliability, operational cost, business needs, and cybersecurity considerations. In the following sections, we will present only the wireless communications technologies that are used in Smart Metering with their security specifications and vulnerabilities, since the majority of devices that are used and implemented nowadays in the HAN and NAN are wireless communicating nodes.

Data Concentrator

The data concentrator's main role is to gather data generated from the SMs in the NAN. Also, concerning the SMs management, the embedded system integrated into modern Data Concentrator Units (DCU) provides a new enhancement that is manifested by including an advanced low-voltage (LV) supervisor and Power Line Communication (PLC) controller with network monitoring functions.

Data Management System

The Data Management System (DMS) receives and stores the data sent by SMs to be processed. In the DMS there are integrated the appropriate subsystems for validating, processing, and editing of the metering data providing the

appropriate information interchange between the different parts of the Smart Metering system [16]. With the evolution of the smart metering system and its capabilities in terms of compilers and storage, the DMS became an advanced system with the ability to make decisions and real-time system management. The smart metering generated data are very useful assets for utilities. These data give utilities the chance to go further and work in proactive mode instead of reactive mode. Utilities use the metering data to make a vast scope of forecasts and predictive analysis that cover user's consumption predictions, energy availability, and Smart grid stability (power failures).

II. LAST-MILE COMMUNICATION TECHNOLOGIES

To achieve the two ways of communication the AMI architecture uses different communication networks, each one having its requirements and considerations which were discussed in the previous study and illustrated in (Figure3) [17]: Home Area Network (HAN) for energy management at the consumer end, Neighborhood Area Network (NAN) is the last mile for providing the AMI and Wide Area Network (WAN) for providing the communication between all pieces of the SG including control center, renewable energy sources, transmission, and distribution. The HAN is connected to the WAN via NAN. The NAN is formed of SM and the Data collected will be transmitted to the DCU (Data Concentrator Unit). A high transmission data rate is required at the WAN level therefore, different wireless communications technologies than the ones used at the HAN/NAN level, are used e.g. WiMAX, 3G/LTE, and micro-wave [18]. In the rest of this section, the widely used wireless communication technologies adopted by HAN and NAN are presented.

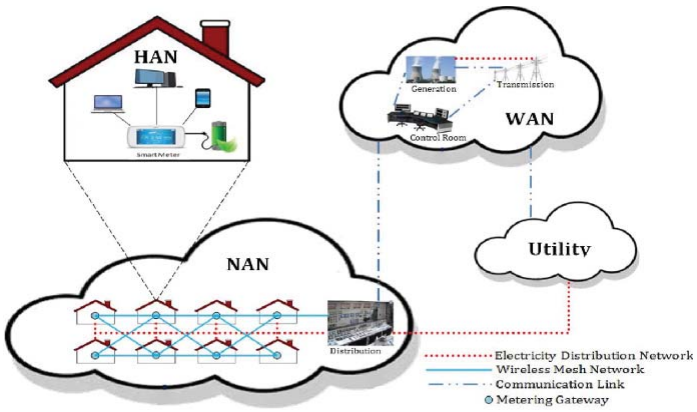

FIGURE 3. Smart Grid Network.

HAN Wireless Communication Network

Home Area Network consists of different appliances such as microwaves, washing machines and Smart TVs. The communication between these appliances and the Smart Meter is ensured by different existing wireless technologies and protocols such as ZigBee, Z-wave, Wifi, Bluetooth, 6LoWPAN, wireless M-Bus, and LoRa recently. The data exchanged via wireless communication between the SM and home appliances consist of power consumption information and network monitoring. Therefore secure Machine to Machine (M2M) communication protocols are needed [19]. The wireless technologies that will be discussed in the HAN area are ZigBee, Wi-Fi, 6LoWPAN, Z-Wave, Wireless M-Bus, and LoRaWAN. For Zigbee and wifi, different standards which define the first two Layers Physical (PHY) and Medium Access Control (MAC), have been developed by IEEE. For 6LoWPAN it was introduced by IETF (Internet Engineering Taskforce) however for Z-wave it is an appropriate solution.

ZigBee: Zigbee standard is built on top of IEEE 802.15.4 standards which are the basis of different wireless technologies, define the first two layers according to the TCP/IP model [20] : the PHY physical layer and the MAC media access layer. Zigbee adds additional layers to cover the network and application capabilities. The Physical layer represents the packet's physical transmission using specific modulation Direct Sequence Spread Spectrum (DSSS) and demodulation (Radio transmission). The data rate depends on the used band. The 2.4GHz band gives a data rate of 250Kbps per channel, whereas the 915MHz band achieves a rate of about 40Kbps per channel and for the 868MHz

band this drops to 20Kbps. With a point to point topology Zigbee coverage can reach up to 10-75m and 30m for indoor however with a mesh topology the covered distance is not limited. For the MAC layer, it is used to avoid any collision during frame transmission. Zigbee is based on a wireless mesh network "self-healing network" which means that it is tolerant against Link failures and affords network stability and high scalability. It is composed of three main components, i.e. the coordinator, which is responsible for some fundamental functionalities e.g. security management, the definition of frequency in use, session initiation (permits for nodes to join the network), the Router, that is responsible for packets routing between nodes, and finally the End devices, for sending and receiving communication packets with the actual payload. Zigbee Alliance has developed different standards for different domains like ZigBee Smart Energy, ZigBee Healthcare, and many others. Zigbee is a highly efficient and cost-effective solution [21].

Zigbee Security Basics: 8 security levels are defined by Zigbee. The lower four are unencrypted and no authentication neither integrity are checked the upper four are encrypted and contain Message Integrity Codes (MIC) where the MIC length can be 16, 32, 64, and 128 bits [22]. For encryption, Zigbee uses the AES algorithm in counter mode and for the authentication, the same algorithm is used but in block cipher chaining CBC mode. This combination is named AES-CCM and it is considered secure. While for the integrity and the replay protection Zigbee uses a message integrity code and a frame counter [23]. Two keys types are used by Zigbee: network keys and link keys. The network key is known by the entire group of devices that belong to the network, it is used for securing the exchanged messages at the network layer and it is exchanged via key-transport or transmitted by trust center, for the link keys are used for end to end encryption at the application layer and all devices get this key either via Key-transport or pre-installed (by factory fabrication for example). On the other hand, some developed key negotiation protocols are used by some application profiles for key exchange. Eventually, the security between devices is guaranteed by a secure initialization and installation mechanism of these keys [24]. The verification of the link key is done by using the Hashed Message Authentication Code (HMAC), where the hash function is a Matyas-Meyer-Oseas construction with AES-128 as block cipher [24]. Zigbee devices firmware updates happen wirelessly or Over the Air (OTA).

Z-Wave: Z-Wave, which is a proprietary standard, is usually implemented in the HAN area for business and residential remote application control. Z-wave protocol stack consists of the four lower layers of the OSI models: physical, data link, network, and transport. The PHY physical layer is where data are transmitted. In Europe Z-wave uses the 868MHz band however in the US it uses the ISM band 908MHz. It is a low data rate protocol originally specified at 9.6Kbps and later extended to reach the rate of 40Kbps [39]. Z-wave also operates on the 2.4GHz band with a data rate of up to 200Kbps [20]. Usually, Z-Wave coverage can reach 30m for indoor applications and up to 100m for the outdoor ones; however once a mesh network is employed the coverage is unlimited. The network layer represents the routing capabilities where messages are routed between nodes and it contains a unique ID for the controller and a unique ID for each new device before joining the network. Usually, a Z-wave network is composed of a controller and a slave. Controllers to define the network topology and the slave for sensors monitoring. The data link is the security layer where the encryption takes place and the MAC address is stored, whereas the MAC layer is used to avoid any collision during frame transmission. Transport layer main functions are error detection and retransmission acknowledgment. On the top of the protocol layers, comes the Application layer. Z-wave technology supports IP, it is a low bandwidth control medium.

Z-wave Security Basics: In 2016 Z-wave alliance declared Security 2 (S2) update, which is required for all certified devices since April 2017. The security measures for providing the confidentiality, authentication, data integrity, and replay attack are deployed by Z-wave at a distinct Security Layer within it is security Command Classes. For robust security Z-wave has adopted a declaration of Security (2) which is classified into three subclasses: S2 Access Control, S2 Authenticated, and S2 Unauthenticated. AES-128 is the common encryption algorithm that is used by these tree classes. For the key exchanges, the Elliptic Curve Diffie Hellman (ECDH) which is considered secure enough, is adopted by S2 with a 256 bits public key. The 256 bits of key length is recommended by the German Federal Office for Information Security (BSI) [25]. For avoiding low-security classes form impacting high-security classes S2 has to define for each subclass its network which means that S2 Access Control and S2 Authenticated are separated from S2 Unauthenticated.AES-128 in CCM mode is used for encryption and authentication however AES-128-CMAC is used for integrity [26]. For all the legacy devices that cannot support S2, Security 0 (S0) for lightweight is there to provide them with security features. With S0 the network key like Zigbee is shared by all devices in the network.

6LoWPAN IPv6 over the Low-Power Wireless Personal Area Network: 6LoWPAN is a combination of IEEE 802.15.4 standard and Ipv6 to realize the IP enabled low power networks (for example for sensors and controllers).This combination between IPv6 and low power wireless networks is discussed by RFC4944 it specifies its format and functionalities. This combination is based on adding an adaptive layer between the link layer and the network layer.

This allows the IPv6 transmission over IEEE 802.15.4. Devices that are based on IEEE 802.15.4 transmit on a short-range with a small packet size of about 127 bytes and a data rate that varies between 250Kbps for 2.45GHz and 20Kbps for 868MHz. An analysis of home automation networks that adopt 6LoWPAN with IPv6 was discussed in [27]. They have simulated home appliances by using a web interface and they have discussed the utility and the challenges of combining IPv6 and 6LoWPAN. Another case study discussing the application of Ipv6 and 6LoPWAN. It emphasized on managing the device memory. Nowadays, and to integrate the IP functionality, vendors are always trying to implement 6LoPWAN protocols, for example, the Zigbee Alliance has developed Zigbee IP which supports 6LoPWAN. 6LoPWAN network topology is a mesh network that offers scalability and high availability. Since IP is supported by the majority of the latest technologies, 6LoPWAN is considered to be high interoperable technology.

6LoWPAN Security Basics:

6LoWPAN vulnerability surface is the combination of WSN wireless sensor network vulnerabilities and IPv6 vulnerabilities. To secure the communication via 6LoWPAN the RFC4919 has defined the security requirements in terms of confidentiality, authentication, integrity freshness, and availability. By using Cryptography, authentication, integrity, and confidentiality are ensured. As mentioned before since 6LoWPAN is the combination of IPv6 and WSN, it is normal to use the cryptographic mechanism used by both of them. AES is used by WSN to secure the Link layer however IPv6 is based on IPsec to secure end-to-end the network layer. With WSN it was judged that using the public key technic it is heavy to be used, but lately, new studies have shown that the combination of RSA and ECC works successfully [28][29]. For the key exchange, the IPsec key exchange that is based on network key exchange is not feasible and cannot be adopted due to its heavy signaling messages and the 802.15.4 small packet size. The WSN adopts different technics for key distribution like a pool of keys, pre-distribute key, and public-key cryptography.

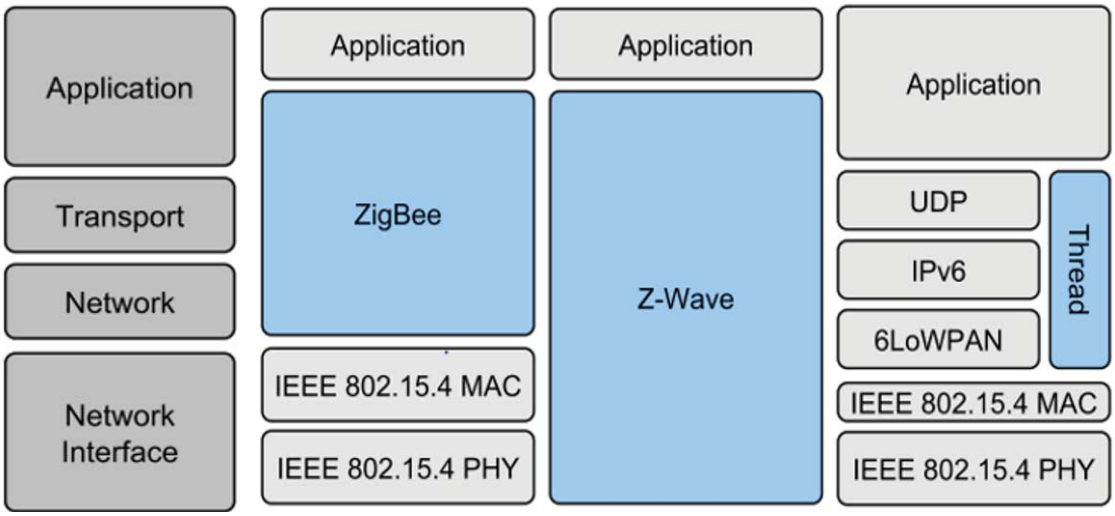

FIGURE 4. Protocols stack referring to the TCP/IP Model

LoRaWAN: Recently Semtech's LoRa/LoRaWAN has developed a new platform to address the indoor challenges faced by the above mentioned technologies. In addition to the IoT application extension to the home boundaries and into the garden, with LoRa solution all IoT devices can be connected directly to the same platform where the range of old systems falls short. With LoRa there is no need for a mesh network and the implementation of repeaters due to the long-distance coverage. In the following section, the LoRa will be more detailed and discussed in terms of physical specs and security features [30].

NAN Wireless Communication Network

The NAN area is composed of hundreds of smart meters creating a star, tree, or a mesh network, which covers a few urban homes or buildings. Different HANs can be connected to the same NAN and transmits for each home the energy consumption to the local data center through the NAN via the smart meter [31]. The measurement data are important

and critical since they are used to manage the energy on demand generation and they are also used from the billing system. The NAN data rate is up to 2Kbps, different technologies can be used for data transmissions like PLC which is a wired technology and WiFi, Wireless M-bus, LPWAN (NB-IoT, LoRaWAN, and Sigfox) and recently MIOTY which are all wireless technologies. In the remaining section, we will focus only on wireless technologies.

Wireless M-Bus: compared to other existing protocols Wireless M-bus is relatively simple, therefore it was vastly deployed in Europe. The star network is adopted with sub GHz frequencies that offer long-range with a software stack of minimal size. The three Industrial Scientific and Medical (ISM) frequency bands used are at 868MHz, 433 MHz, and 169MHz. Each European country has defined its requirement, for example in France they have used the 169MHz frequency band combined with 4GFSK modulation. Compared to the TCP/IP model Wireless M-Bus differs slightly. It consists of 3 main layers the Physical, data link, the Network, and the Application one[32].

LPWAN: usually used for long-range coverage where other technologies failed and for low power consumption solutions. It offers a data rate from 250bps up to 50Kbps per channel [33].

LoRa/LoRaWAN: LoRa wireless communication technology is patented form Semtech, and uses a chirped spread spectrum modulation for layer one or the physical layer for LoRaWAN. The chirped spread spectrum modulation decreases the interference impact on data transmission providing increased reliability. LoRa MAC developed by LoRa Alliance forms the data link and network layer. The adaptive rate is one of LoRa features, and it can be modified accordingly with the chosen bandwidth. The transmission energy is defined with the selection of optimum spreading factor. The LoRa transceivers that must be integrated with the smart meter are not expensive compared to other technologies. LoRaWAN uses the ISM frequency bands with a data rate that varies from 0.3kbps to 50kbps and transmits data within 5kms range in the urban region and 20kms in a rural area with a payload size of 243 bytes. In Europe, the adopted frequency band is between 863MHz and 870MHz. LoRaWAN end devices operate in three different operation modes, namely A, B, and C, with each mode providing different uplink and downlink capabilities and energy needs accordingly [34]. Class A nodes listen to incoming messages directly after the upload of some data and after that, they go back to sleep mode (batteries saving mode), for Class B nodes the gateway sends a beacon messages to the end device that is used to synchronize time windows for listening and finally Class C devices are always in listening mode. LoRa networks are typically following a star topology where the gateway is just a delay between the end node and the central server. The end node communicates with the gateway via LoRaWAN and the gateway communicates with the backend via the IP standard.

LoRaWAN Security Basics: The AES encryption is adopted by LoRaWAN on two levels of security the network level and the application level. The LoRaWAN provisioning process is based on the unique device ID and two keys. The first one is the network session key, which is used to secure the communication between the device and the shared network server, and the second one is the application session that is used to secure the data between the end node and the application server (application payload encryption). These Keys are exchanged via two ways: ABP which stands for Activation By Personalization where the keys are stored into the device and locked since the production deployment or via OTAA which stands for Over the Air Activation is based on a handshake process using a unique device key. With OTAA both keys were obtained from the same application key which has to be recognized by the network operator. However the specification 1.1 raises a new AES-128 network key, this key has to be recognized by the network operator and it is used for obtaining the network key and managing the devices joining procedure while the application key is kept protected and in private. With LoRaWAN the end device ID protection is based on the device ID which is unchangeable for ABP devices and changeable for OTAA device. The CMAC algorithm with AES-128 encryption combined is used to generate a 4 byte MIC that ensures data integrity. This MIC is derived from the network key and the MAC payload. To avoid any replay attack LoRAWAN relies on the counter field which is encrypted and integrated in every message. For data confidentiality AES-128 encryption is adopted in CTR mode, application payload encryption is based on the application session key. LoRaWAN end nodes supports two ways of communication and also support a multicast firmware upgrade over the air (OTA).

Sigfox: Also implementation of the narrowband technology, can be deployed for long-range applications. It uses the BPSK (binary phase-shift keying) modulation in the uplink and Gaussian Frequency-Shift Keying (GFSK) in the downlink, it offers a data rate up to 100bps and transmits data up to 10kms in an urban area and up to 40kms in the rural region [35]. Sigfox endpoints are inexpensive but the base station that controls and manages the network is more complicated than the corresponding element in LoRaWAN. Sigfox protocol stack consists of: the physical layer PHY where Sigfox uses also ISM frequency Band which is 915MHz in the US and 868MHz in Europe. The MAC layer is responsible of the assembly and disassembly of data. The frame layer is used for the generation of the radio frame an
d

finally the application layer which depends on the user requirements. Sigfox is a cloud-based model where the data is transmitted from the end device to the backend server via the gateway; it doesn't support the IP networking and like LoRaWAN it is fit for applications that don't require big and frequent data transmission.

Sigfox Security Basics: generally based on symmetric cryptography, however not all security features are afforded by default. Sigfox provisioning process is based on three main identities the network key, the device ID, and the Porting Authorization Code (PAC). These credentials are transported in different ways either they are already stored in the device since the production or via Secure Element (SE) providers in addition to the possibility of using a Central Registration Authority (CRA). The network key's main role is to encrypt the communication and it is only recognized by the CRA the SE and the device maker. The device ID is a unique identifier for the end node and it is not encrypted or protected. The PAC can be used only for one time and it is used during the registration process to confirm the ownership of an end device by a specific group of devices. After any registration, the PAC is regenerated and transported to the group owner where it must be well protected and remained confidential to avoid any breaches [36]. Sigfox defines two additional keys one is used for the authentication which is the same as the network but the network key is for the registration however the authentication one is for the cryptography, the second one for the encryption it is functionality is to encrypt the traffic exchanged between the end node and the core network, it is generated by combining the AES-128 to the network key. Sigfox data integrity is by cyclic redundancy check (CRC) field [37]. With Sigfox the data exchanged between the end node and the gateway are not encrypted by default however in 2017 Sigfox came out with a new service to secure this exchange of data. This service is based on using AES-128 with the encryption key. For the end to end security, it should be ensured by the application developers. To avoid any replay attack Sigfox relies on the counter field which is encrypted and integrated into every message. This field length is about 12 bit. In addition to the counter field, sigfox relies also on two timestamps the first one is added to every single message received by the Gateway and the second one is added by the network server once a message is received [38].

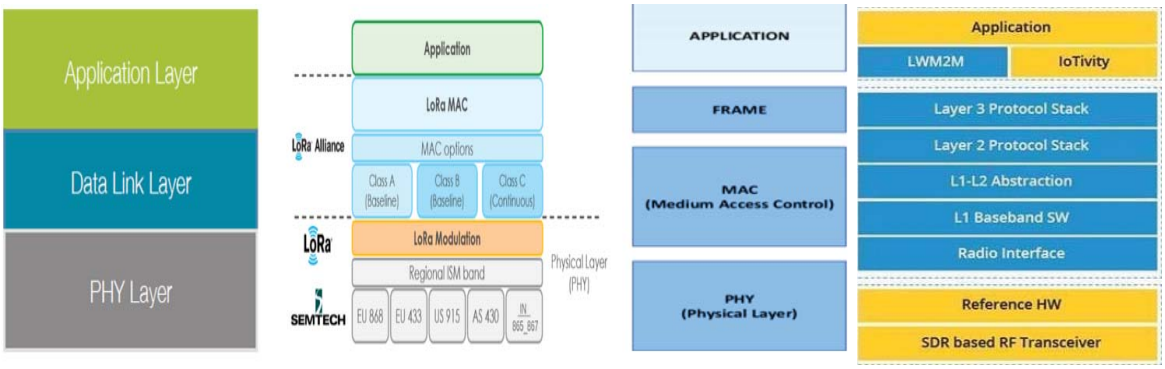

FIGURE 5. Wireless M-bus, LoRaWAN, Sigfox,and NB-IoT Protocols Stack.

Narrowband-Internet of Things (NB-IoT): is a standard developed by third-generation partnership project (3GPP), that uses cellular telecommunication band to connect a vast range of nodes**.** It is used for M2M and IoT applications that required an extended range of transmission with a low cost and low power for long battery life. It coexists in long term evolution (LTE) or Global System for Mobile (GSM) under licensed frequency. The LTE functionality is deducted by NB-IoT to its minimum and enhanced I way to fit the IoT application requirements. The frequency bandwidth used by NB-IoT is 200 kHz, which is one of GSM and LTE transmission resource bands.
NB-IoT operates in 3 modes:

- In-band operation mode which based on using the LTE resources,
- Guard band operation which based on using the LTE's guard band unutilized resources,
- Standalone operation mode which based on using the GSM frequencies

However, 3GPP advises the use of the In-band operation mode. Since NB-IoT protocol is based on LTE it uses the LTE protocol stack (the physical and the upper layers). The QPSK modulation, Frequency Division Multiple Access (FDMA) used by NB-IoT for the uplink, and Orthogonal FDMA (OFDMA) for the downlink. The data rate can reach up to 200Kbps in downlink and up to 20Kbps in the uplink, with a payload size of 1600 bytes for each transmitted or received packet and it sends data over 1km in an urban area and up to10kms in a rural area. NB-IoT can support up to

50K devices per cell and this number can be extended by using multiple carriers. With 3GPP release 15 new improvements were introduced, like the multicast services that be used by NB-IoT for end-nodes firmware update[42].

NB-IoT core network is composed of the evolved packet system (EPS), and two enhancements for the cellular internet of things (CIoT): the User Plane CIoT EPS, and the Control Plane CIoT EPS. The two planes select the optimal path in both directions (uplink and downlink) for control and user packets. The process of NB-IoT users accessing a cell is similar to the LTE procedure. The evolved UMTS Terrestrial Radio Access Network (E-UTRAN) which consists of eNBs, controls the RF communication between the User Equipment (UE) and the Mobile Management Entity (MME) at the control plane and the transmitted data between UE and Packet Data Network Gateway (PGW) through Serving Gateway (SGW) at the user plane. The non-IP data will be delivered to the application server via the Service Capability Exposure Function (SCEF) through the control plane. However, at the user plane, both IP and non-IP data can be sent over radio bearers to the application server through the SGW and PGW[43].
In the uplink and download link, both planes select the optimal path for control and user packets. The NB-IoT network access is like accessing the LTE network. In conclusion, the E-UTRAN architecture and the backbone can be used for NB-IoT.
NB-IoT Security Basics: The security mechanisms adopted by NB-IoT are similar to the LTE system, from which it was developed. Entity provisioning process: Authentication in NB-IoT is based on the UE first affirming a unique identity so that the network can then check that the UE's credentials match that identity. There is a hypothesis, thus, that the identifier is unique and always assigned to a specific UE, otherwise, any authentication of that identity is denied. For confidentiality and data integrity NB-IoT uses four algorithms: the NULL which means no security mechanism used, the SNOW3G based 128-bit stream cipher, the AES based 128-bit block cipher in CTR mode, and the ZUC (Zu Chongzhi) based128-bitstream cipher.
For data, confidentiality is controlled in NB-IoT by the non-access stratum (NAS) commands. As well, the previous three cipher algorithm built on symmetric cryptography is adopted. Against the replay attack, NB-IoT uses the Key hierarchy for protecting and encoding of the NAS signaling exchanged messages between the UE and the MME. For firmware updates, the OTA is supported by NB-IoT only in IP mode. NB-IoT core network is IP based, the network traffic can be monitored using a firewall. The network can be monitored in real-time by mobile network inner mechanisms[37].
MIOTY: Developed by Fraunhofer-IIS, it is a novel telegram-splitting ultra-narrowband (TS-UNB) technology. It offers a reliable and energy-efficient solution for every application system. It is possible to have a variety of transmissions simultaneously with only one unit receiver without interference. Due to its little self-interference generated, the system can support up to a million simultaneous transmitters [44]. The transmission range is up to 15Km in a flat area and 5Km in an urban area. The channel encoding scheme used by MIOTY increases its range by a factor of 10 over the 868MHz wireless standard [45]. MIOTY is better than the current cellular and non-cellular existing LPWAN technologies because it's more robust and resistant to interference from other systems. MIOTY provides network security based on an integrated AES-128 peripheral.

III. Smart Meters and AMI CYBERSECURITY

Smart Meter is the first point that is responsible for gathering the energy consumption data for the power grid. As mentioned before the smart meter consists of two network communication interfaces and a serial port for access and maintenance. As the internal serial links are not protected any physical access to the smart meter can expose the whole system to some security vulnerabilities. The security leak of the built-in Microcontroller, the radio interfaces, and the firmware updates exposes consumer privacy and introduces cyber-physical vulnerabilities.

Advanced Metering Infrastructure (AMI) is currently quickly implemented across the power grid and is allowing the introduction of technology to the smart grid. With its fast, huge, and vast deployment AMI security has become a scope of attention with the following main directions:

- Data collection
    - Data availability which means that the network is always up and alive.
    - Data confidentiality is necessary to maintain data privacy and to save the data from being exposed to unauthorized parties, it can be guaranteed by using techniques for data encryption. Data freshness is required to make sure that data is new and recent, it is guaranteed by adopting counter and timestamp techniques.

- Network management and provisioning
    - Authentication is used to verify if any entity has the right and privilege to access, participate and join any network and finally non-repudiation which is a way to be sure that the sender has no way to deny of having sent a message and the same for the receiver, this security requirement is essential to avoid replay and data injection attacks and it is guaranteed by using public-key encryption with a digital signature.
    - Authorization: this guarantees that just certified devices are allowed to get access or use or control the system and breach whatever is permitted.
    - Non-repudiation: This states that just authorized devices can receive data and do not subsequently deny receiving it. Some devices can't state the data reception if they didn't. Therefore, no false alarm of exchanged data is considered, i.e. any end of the system cannot deny any measure or action taken by the AMI.
    - Initial provisioning and secure firmware update. Whether performed on the air (OTA) or with a physical connection.
    - Accountability is used to verify every action taken by the system. it is similar to the Non-repudiation
- Reporting
    - Monitor and Analysis give AMI system the ability to examine itself and try self-healing. AMI systems have to be capable of achieving automated control in cases of any internal or external trouble and transmitting these records for further examination, processing, and analysis.
- Furthermore, contemporary AMIs are meant to support Smart Grid processes built on top of it (e.g. DR scenarios with active involvement of consumers, aggregators, ESCOs, etc. , Demand Side Management scenarios will be supported providing real-time analytics and modeling of the microgrid operation, etc), in near real-time, including energy demand, storage and supply (even including self-production when applicable), which raises the bar even higher in terms of speed, and security for the optimization of the microgrid energy generation.

These mentioned requirements are mandatory and essential to guarantee data security. Therefore defining the attack surface is mandatory to secure the smart grid and AMI. The following will define the surface attack of AMI and specifically wireless technology[46].

Communication Network and Technologies

Usually, the communication network is used to connect the AMI different components (for example to connect the SM to the Data concentrator). Besides it comes that AMI information network links the HAN (the consumer side by using Zigbee, Z-wave, or other wireless technologies) to the NAN. These communication networks are geographically spread along with the smart grid. These networks consist of hundreds of thousands of devices including smart meters and data collectors that are forecasted to have a long life and they are implemented widely. By deploying this huge number of long devices, and taking into consideration the cost impact, means that hardware replacement is not that easy and any future firmware upgrade will be difficult. These constraints will lead to an increasing with time AMI system intrusion vulnerability in case of compromising even a single smart meter.

By adding the extensive use of wireless protocols by AMI, the cyber-attacks risks increase and so too the system vulnerability. Although these protocols have been used for a long time ago and that are widely adopted they are still the main target for attacking the Smart Grid infrastructure. Usually, they are based on AES for data encryption. Some of these protocols experience weak encryption and vulnerable key exchange processes which can threaten the data integrity and compromise the system. In the following paragraphs, we will discuss the security vulnerabilities of each one of the previously mentioned wireless communication technology.

Zigbee Security Vulnerabilities

Physical attacks: these attacks are targeting critical and sensitive information that is stored in devices. This information is used to launch diverse attacks against the Zigbee network.

- Unsafe Key Storage: Zigbee security is based on the assumption of secure Key storage. Usually, the network key is preconfigured within the coordinator however for the link key it is preconfigured for routers and end devices. Any unsafe storage of one of the networks, links, and master keys would make easy the extraction of the key which will compromise the whole network.

- RF interference: while Zigbee adopts some reliable techniques to protect the network from interference, but they are slow to be executed and not completed, which allows the attacker to take control of the frequency channel that the network is running.

- Network Spoofing: Zigbee allows the link key reuse for network rejoining. Therefore an attacker can copy an end device's credentials and rejoin the network with a different device. As a result, the trust center passes the network key encrypted and the old link key to the cloned device, which will allow the attacker to get access to the entire network.

Cyber Attacks:

- Unsafe Key Transportation: A new node that is going to join the Zigbee network gets its network key over the air. In case the key is sent in plaintext an attacker can get the key by eavesdropping and will compromise the network since this key is shared between all network devices.

- Unencrypted Security Headers: Usually the auxiliary frames are used to ensure replay protection. However, when an attacker generates a false security header without knowing the key behind creating the MIC, even though attacks against data integrity fail, the receiver will spend a notable amount of energy to process these false messages which will lead to battery exhaustion. This what we call a ghost-in-wireless attack.

Other Attacks:

- Replay attack: Even that Zigbee instructions and specifications have adopted mechanisms to stop the replay attack, but 802.15.4 has restricted replay security techniques, that cannot be enhanced even with an encrypted message. Therefore an attacker can replay an earlier message without changing the content (since Zigbee restricts the packet modification) until key rotation. Different attacks come with the replay attack, like DDOS where a suspicious user in the network receives packets and replays these packets to disrupt and interfere with the total network functionality.

- Man in the middle attack: for packet acknowledgment, Zigbee instructions do not ensure integrity and confidentiality security. By consequence, a non-validated attacker can spoof the acknowledgment packets and make the sender think that the packet is well received by the right receiver. In other words, if the sender doesn’t receive an ACK packet he will retransmit the same packet, if the network is compromised and the ACK is unauthenticated, the attacker can intervene and send a false ACK to the sender. Then the sender will transmit all the remaining packets to the attacker.

- Information theft: like any other wireless protocols Zigbee is at risk of statistical attacks that exploit weaknesses in a targeted algorithm. These types of attacks compromise end-user privacy, which allows an attacker to gather and collect critical information. [47]

Z-wave Vulnerabilities

Pairing vulnerabilities: To protect the traffic Z-wave uses a shared network key. This key is transmitted between the controller and the end device during the pairing process. These Keys are used to secure the communications and to stop hackers from compromising joined devices. The former Z-wave S0 paring mechanism is too weak and vulnerable where the network key was shared between nodes by using a key of zeroes which is easy to be sniffed by a hacker within the RF coverage and once the network key is obtained the attacker can have access to control the Z-wave network. Hence Z-Wave has improved and fix this pairing process by Z-Wave S2. But unfortunately, recent studies

have shown that even it is not easy to hack Z-Wave S2 but it can be downgraded back to S0, canceling all security enhancement. The downgrade attack requires physical closeness to the device while the pairing mechanism [48].

6LoPWAN Vulnerabilities

IPV6 network and WSN combined form 6LoPWAN, hence its security vulnerabilities come from both networks. Also there some vulnerabilities that point to the adaptation layer.

Physical attacks:

- Jamming: this attack tends to perturb the network operation and this is achieved by transmitting high energy signals. To stop such types of attacks spread spectrum techniques are used.
- Radio Interference: where the attacker generates a big amount of interferences discontinuously or constantly.
- Tampering: when an attacker gets access to the end device, he can extract some critical information such as cryptographic keys. Such types of attacks can be avoided by node tamper-proofing or by self-destruction when anyone accesses physically the device, nodes erase their memory which will prevent any information leakage.

Outside/ Inside Attack when an attacker is out of the network and get illegitimate access to listen or initiate DoS attack by jamming or power depletion. Usually to protect against such types of attacks, to avoid strangers from getting access to the network, systems deploy cryptography mechanisms. But these techniques are not effective to protect against internal compromised devices. An insider device can be compromised in several ways for example any physical attack can guarantee the attacker the opportunity to retrieve the cryptography key or to change the device firmware. Usually, this type of attack points to spoil a network operation. These attacks are too dangerous since they can be simply launched and harm network operation, for example, a Sybil attack which is a link-layer attack. One Sybil attack type concerns the data aggregation where a compromised node acts differently, while a second type is based on the packet forging technique, and it leads to some other attacks like misdirection, exhaustion, and unfairness. In addition to some attacks that are related to the IPV6 network, where the neighbor discovery and address autoconfiguration mechanisms are adopted. These mechanisms are exposed to some threats, like an attacker can get into these processes and spoof the neighbor solicitation/ advertisement [49].

Adaptation layer threats: this layer functionality is implemented on the edge router between the two networks IPV6 and WSN. Usually, this edge router is very well secured and protected but the packet fragmentation and reassembly still subject to some threats. Some of these threats are tiny fragmentation, frag router attack, such attacks will lead to significant node damage (like buffer overflow due to packet re-sequence).

LoRaWAN Vulnerabilities

Physical attacks: network devices can be used by attackers to launch the below attacks.

- Taking out Security Variable: LoRaWAN instructions insist on securing of the relevant key material against reuse. But if an attacker gets direct physical access to the device, the opportunity the changing the firmware or thieving / reusing the key material becomes easy. Therefore devices should be secured against any firmware alteration that can guide to key material reuse or thieve.
- In LoRaWAN session keys derived from the root keys which usually are produced during fabrication. Hence, breaking of a root key will only compromise the stored data within this device. This information can be accessed only by destroying or stealing an end device.
- Unsecure Key storage: if Keys are stored in ordinary text files within the end device and the security storage requirements are not fulfilled then plaintext Key Capture attack is a significant danger that will risk the confidentiality, integrity, and availability of the network.
- RF Jamming Attack: using cheap hardware makes the RF jamming possible. RF jamming can cause DoS (Denial-of-Service) which is simple to be detected. However, the selective RF jamming attacks are more difficult to be catch and so damaging for wireless protocols since it is not easy to avoid.

Cyber Attacks:

Eavesdropping attack: here the attacker relays on weaknesses that reside at the gateway level to receive packets and conclude some information about the transmitted data and the adopted key material. However, without obtaining the key material an attacker cannot decode the packet content.

Other Attacks:

Man in the middle MIM attack: there 2 attacks under MIM the first one is a bit-flipping attack in which the attacker modifies the message content while this message is transmitted between the network server and the application server. The second attack is frame payload attack this attack is due to the handover-roaming as the unprotected FRMPayload messages are first transported from the serving-NS to the homing-NS, and from there to the AS.

Replay attack: to access the network an end device has to retrieve the key materials that should be well protected. One way an attacker can get access to these credentials either by taking over a device or by changing the firmware in a way to make possible the reuse of the key materials. End devices are information sources and cannot reach the data at the server. Hence, any compromised device cannot leak data from the network, it can only inject fake information to the application server. A compromised device can be used to launch a replay attack. All packets that are transmitted by the remaining devices can be caught and replayed subsequently. In general, this attack detected by the use of the nonce values, but this will lead to available resources occupation and reduce the Gateway availability from serving the non-malicious devices.

Self-Replay Attack: The OTAA is invented to improve LoRaWAN security. However, by itself, it becomes a subject of attacks. Using the above mentioned selective RF Jamming an attacker can compromise LoRaWAN joining process. However, a professional attacker can selectively jam the signals that are generated during the OTAA process. In this case, the Join-request with DevNonce that is sent by an authorized end device is successfully detected. Applying the selective-jamming methods Join-accept message sent by the network server to the end device is jammed. The end device wait to receive the Join-accept after a certain time if it doesn't receive this message it will resend again the same Join-request with DevNonce to join the network, the sever from its side will send again the Join-accept since everything is legitimate and the joining process is not completed yet. This exchange of data will continue until the end device messages quota is exhausted since with OTAA the exchange of messages is restricted and under quota. To succeed an attacker should get the packets sent by the network server before it reaches the end device [49].

Sigfox Vulnerabilities

Replay attack: the 12-bit Sequence Number (SN) is used to protect Sigfox from a replay attack. It is secured by Message Authentication Code (MAC) and sent in each uplink frame. The server will discard any packet with a SN lower than the latest received packet. MAC calculation is not public, but some of its inputs are AES in CMAC mode combined with the Network Authentication Key (NAK) and the SN. For downlink packets there are no public details about the SN size, therefore there is no enough details about the downlink messages security compared to the uplink messages. The 12-bit SN of the uplink packet allows 4096 unique messages, then the SN is reset back to 0. Since Sigfox NAK key (that is used for MAC calculation) is static through the node lifetime, replay attacks become a serious possible threat to Sigfox. Sigfox SN number resets approximately every 30 days based on the maximum number of uplinks packets that can be daily sent by Sigfox. In practice, the Sigfox end device can still send packets even beyond the limit, and these packets can be still received and accepted by the server, this leads to an early SN reset. Following the SN reset, the hacker can replay one of the earlier frames indefinitely, as the NAK key used for MAC calculation is static and unchangeable, which means that the MAC will ever be valid during the lifetime of the compromised node [50].

NB-IoT Vulnerabilities

Denial-of-Service (DoS) attacks: the invisible threats in NB-IoT nodes derive from their scale. There is a high potential for launching denial-of-service (DoS) attacks by exploiting a group of devices to send unexpected communication to specific victims. In addition to a service disruption on the victims' services side, such type of attacks has also an impact on the service provider network which cause a service deterioration due to a signaling load prohibiting the remaining uninfected devices from sending, receiving data, and responding to their control solicitations[51].

IV. COMPARISION BETWEEN TECHNOLOGIES

In the above sections, we have focused on defining the specification and the security vulnerabilities of different wireless communication technologies used by the SM which is a main component of the AMI network. These technologies are divided into two categories the short and long-range wireless communication technologies.

To expand the coverage limitation due to their physical short-range (less than 100m), wireless technologies (e.g. Zigbee and Z-wave) use mesh network topology. However, the major drawback is their high deployment cost to link the big number of nodes which geographically scattered in a large area.
Furthermore, since data is communicated via multi hops to the gateway, a big number of nodes are more loaded and congested than other which will impact their batteries life (i.e. excessive use of energy) and therefore the network lifetime will be affected. This restriction is solved by LPWAN (Sigfox, LoRaWAN, and NB-IoT) technologies, which are based on star network topology, where end nodes are directly connected to the gateway. Contrary to Mesh network, before sending data the end node doesn't listen to the radio channel which guarantees energy saving. And since gateways are always online, they assure instant access to connected nodes.
However, compared to LPWAN short-range technologies provide a higher data rate, where the data rate is between 250bps and 200Kbps for LPWAN and 250Kps for Zigbee.
Also not all LPWAN technologies are equal in terms of coverage, cost, data rate, latency, scalability, standardization, and power consumption. LPWAN technologies operate in both the licensed (e.g. NB-IoT) and unlicensed (e.g. MIOTY, LoRa, Sigfox, etc.) spectrum. NB-IoT, which has faster response time than sigfox, and LoRa, guarantee a better quality of service (QoS) since it based on time slotted an LTE synchronous protocols, while LoRa and Sigfox do not support any QoS. NB-IoT operates with a data rate of 200Kbps where the maximum data rate is about 50Kbps and 100bps, for LoRa and Sigfox respectively which much lower than NB-IoT. In an urban area, Sigfox can transmit data over 10kms where LoRa and NB-IoT transmit data respectively at 5kms and 1km. loRaWAN and Sigfox consume less energy than NB-IoT since they reduce their energy consumption in sleep mode, which will save device battery life. Hence, for an application like Smart City, Smart Building where low data rate, low-cost solution, long battery life, and no QoS are required LoRa/ Sigfox are best suitable technologies, however in applications, where high data rate, low latency, QoS, scalability, and standardization to ensure a secure, reliable, and interoperable network, are main concerns, NB-IoT is best to be deployed.

V. AMI SECURITY BEST PRACTICES

To protect the Smart Grid against any potential cyber-security threats, defense strategies and some good practices have to be adopted and integrated at the AMI level including wireless communication protocols and the architecture in use. Besides, the security of all participating components, which addresses the safety of each component including the SM, has to be performed and tested. It covers device conformity, functionality, and interoperability testing.

This section focuses on listing the most relevant attacks against AMI, their impact on the system, and the recommended published best practices. There are several best practices released for all aspects of Smart Meter, AMI, and communication networks/ technologies that can be concluded from the previous sections where we have mentioned their security gaps and vulnerabilities that can lead to a compromised system. Table 1 mainly focuses on Smart Meter devices, wireless communication technologies, and communication networks in general[52].

Table 1: Comparison for Smart Meter devices, wireless communication technologies, and communication networks

	Category	**Attacks**	**Impact On**	**Best PRACTICES**
		Illegitimate physical access	Access control	Restrict the Physical access of the network devices to only specific persons
	Physical security		Availability Integrity Confidentiality	Disable unused ports Use strong encryption

	Category	Attacks	Impact On	Best PRACTICES
Advanced Metering Infrastructure				Credential secure storage
	Physical security	Data theft	Access control	Restrict the Physical access of the network devices to only specific persons
		Intentional damage	Availability Integrity Confidentiality	Disable unused ports
		Firmware modification		Use strong encryption
		Smart Meter hijacking		Credential secure storage
		False Data Injection		
		Data theft		
	Wireless Networks		Integrity Access control Confidentiality Availability	Here are some measures to be taken into consideration to protect wireless networks: Use of mutual Authentication Hash function monitoring Devices secure communication. Use only approved communication channels Use of secure communication protocols MAC address filtering Access control List AES Encryption Security against masquerading parties Recently Blockchain is adopted as solution for a secure OTA firmware update

	Category	Attacks	Impact On	Best PRACTICES
	Wireless Networks Others	Man in the middle MITM Identity theft Session hijacking Data gathering OTA firmware modification Smart Meter hijacking	Integrity Access control Confidentiality Availability Integrity Authentication Access control Confidentiality Availability	Here are some measures to be taken into consideration to protect wireless networks: Use of mutual Authentication Hash function monitoring Devices secure communication. Use only approved communication channels Use of secure communication protocols MAC address filtering Access control List AES Encryption Security against masquerading parties Recently Blockchain is adopted as solution for a secure OTA firmware update Adopt metering security standard Adopt session control mechanism to detect any abnormal session Network to only authenticated devices: this by verifying the identity of each device before joining the network. This also provides data integrity Authentication and integrity checks: this is by verifying the

	Category	Attacks	Impact On	Best PRACTICES
				readings to make sure they were not modified and tampered Encryption of the meter data: this to protect the user privacy Non-repudiation: this is to verify the data origin and that the received data are not tampered
	Others	Data Theft	Integrity Authentication Access control Confidentiality Availability	Adopt metering security standard Adopt session control mechanism to detect any abnormal session Network to only authenticated devices: this by verifying the identity of each device before joining the network. This also provides data integrity Authentication and integrity checks: this is by verifying the readings to make sure they were not modified and tampered Encryption of the meter data: this to protect the user privacy Non-repudiation: this is to verify the data origin and that the received data are not tampered
		Malicious Code		
		Illegitimate access		
		Gateway Eavesdropping		

VI. RECOMMENDATIONS

Through the last decade, information systems passed through a significant transformation from proprietary, isolated systems to open architectures highly interconnected with other corporate networks and the Internet. Also, Critical

Infrastructures (CIs) become huge infrastructures with many points of access. However, CIs expanded, and communication protocols were designed having no security in mind. Physical IoT nodes attacks, especially in the case of interconnected nodes, compromise not only the node but also the network security and are more difficult to get identified. This exposes CIs to a variety of threats either physical or cyber.

As such, the evolution of power grid systems has led to an important improvement, which has brought benefits to the utilities, consumers, and the environment. The enrolment of Smart Meters, the introduction of wireless protocols, and the adoption of a bidirectional communication have raised the necessity for a safe communication to protect the data transmission. The AMI which is part of the smart metering network system is responsible for metering data transportation that includes the billing data and other information. The smart meter network is composed of a huge number of smart meters that are linked together through different wireless protocols to deliver the metering data to the control center.

All the SG structure heavily relies on the communication networks and the secured delivery and management of smart meters data. This dependency and the software-oriented management of the underlying network makes the SG vulnerable to a wide range of threats. These threats or possible attacks could cause many problems in the SG ranging from physical damages to blackouts. Also, attackers could gain access to electricity companies and customer's information. In the United States, CIA's reports have already revealed that hackers turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power[53].

The U.S. National Institute of Standards and Technology (NIST) has already produced a report that presents a cyber-security strategy and architecture. The document identifies a set of risks to the SG involving:

- **(i)** Vulnerabilities and exposure to attacks or unintentional errors;
- **(ii)** Novel vulnerabilities generated by the interconnection of different networks;
- **(iii)** Vulnerabilities and weaknesses caused by disruptions of the communications network and the introduction of malicious software;
- **(iv)** Increased numbers of entry points and paths available for potential adversaries to exploit;
- **(v)** Threats to data confidentiality and integrity caused by interconnected systems that can increase the amount of private information exposed;
- **(vi)** Vulnerabilities introduced by the use of new technologies or potentials to compromise the data integrity e.g., customer privacy breaches due to increases in the collected data.

The main problem is that as the SG exposes the electric infrastructure to a software guided framework managed by computer-based control systems – at the same time, these systems are increasingly connected to open networks, such as the Internet, exposing them to cyber risks.

Due to the heterogeneous communication architecture of SGs, a challenge is to design sophisticated and robust security mechanisms that can be easily deployed to protect the management of data and the communications among different layers of the SG infrastructure.

We not only need help to define models and mechanisms for threats identification but also to define plans for the (pro-) active response in the threats presence and the relevant recovery methodologies to avoid any negative consequences in the SG performance. Threats will be categorized according to specific security goals set for:

- **(i)** Electricity companies or grid operators,
- **(ii)** Customers and,
- **(iii)** Home/business environments.

Considering three overall tiers (i.e., layers): **(i)** the first tier is related to security management in the smart meters, **(ii)** the second tier is related to the security management in the concentrators' level and, **(iii)** the third tier is related to the security management at the operator's level. Concentrators aim to manage the data coming for a number of smart meters creating a set of 'islands' (i.e., a subset of interconnecting smart meters based on spatio-temporal characteristics). Different technologies will be adopted at each tier focusing on different threat categories. Provides a holistic framework for enhancing the resilience of the SG infrastructure. It is capable of handling both physical (electrical) and cyber threats which are rapidly detected so that remedial actions are effected. Offers a framework that is capable of responding to a dynamic environment like the SG and provides concrete solutions to face possible security leaks in the infrastructure maximizing its performance.

VII. CONCLUSIONS

AMI which is a crucial part of the SG faces various security threats. Countermeasures for SG attacks in terms of physical or cyber-attacks will focus on a sensor/actuator infrastructure (IoT devices), secured networking functionalities, and automatic – if possible – the neutralization of any attack on critical parts of the infrastructure. This paper gives a detailed approach of the AMI system different components and various threats sources. It examines the communication requirements for the AMI and discusses the communication architecture that is based on the HAN, NAN, and the WAN. Various communication technologies for AMI applications are discussed in terms of communication coverage, basics security measures, and privacy. Then a study addressing the security vulnerabilities, challenges, and attacks had to be done. The specifications of each protocol were very well defined in terms of coverage, frequency band in use, data rate, and protocol stack. The first security objectives to be met were by identifying the security mechanisms adopted by each protocol in term of the encryption algorithm, key exchange process, and authentication process, then potential attacks and security vulnerabilities of each protocol were outlined based on 3 categories the physical attacks, the cyber-attacks, and other remaining types of attacks. The second security objectives to be met were identified by listing the possible attacks targeting the AMI requirements, in terms of availability, integrity, control, and authentication, which directly impact the AMI system functionality.

ACKNOWLEDGEMENTS

The publication cost has been funded from the University of West Attica-Greece.

REFERENCES

[1] "No Title." https://www.smart-energy.com/regional-news/north-america/russia-attacked-the-us-power-grid-what-if-they-dont-stop/.

[2] "No Title." https://www.smart-energy.com/industry-sectors/smart-meters/just-153-3-million-lpwan-smart-meters-from-2019-2028/.

[3] 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," *Appl. Sci.*, vol. 6, no. 3, pp. 1–24, 2016, doi: 10.3390/app6030068.

[4] G. Barnicoat and M. Danson, "The ageing population and smart metering: A field study of householders' attitudes and behaviours towards energy use in Scotland," *Energy Res. Soc. Sci.*, vol. 9, pp. 107–115, 2015, doi: 10.1016/j.erss.2015.08.020.

[5] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, 2010, doi: 10.1109/MPE.2009.934876.

[6] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 5–20, 2013, doi: 10.1109/SURV.2012.021312.00034.

[7] "Smart Meters and Smart Meter Systems : A Metering Industry Perspective," no. March, 2011.

[8] O. S. O. and Omorogiuwa Eseosa, "Smart Grid and Energy Management in Nigeria Integrated Power System," *Int. J. Eng. Innov. Res.*, vol. 3, no. 6, pp. 732–736, 2014, doi: 10.13140/RG.2.1.3664.0242.

[9] M. R. Abid, A. Khallaayoun, H. Harroud, R. Lghoul, M. Boulmalf, and D. Benhaddou, "A wireless mesh architecture for the advanced metering infrastructure in residential smart grids," *IEEE Green Technol. Conf.*, pp. 338–344, 2013, doi: 10.1109/GreenTech.2013.58.

[10] F. Halim, S. Yussof, and M. E. Rusli, "Cyber Security Issues in Smart Meter and Their Solutions," *Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 3, pp. 99–109, 2018.

[11] P. W. Schultz, M. Estrada, J. Schmitt, R. Sokoloski, and N. Silva-Send, "Using in-home displays to provide smart meter feedback about household electricity consumption: A randomized control trial comparing kilowatts, cost, and social norms," *Energy*, vol. 90, pp. 351–358, 2015, doi: 10.1016/j.energy.2015.06.130.

[12] F. Molazem, "Security and Privacy of Smart Meters : A Survey," *Work. Pap.*, pp. 1–11, 2012, [Online]. Available: http://blogs.ubc.ca/computersecurity/files/2012/04/FMolazem_SurveyFaridMolazem.pdf.

[13] "No Title," [Online]. Available: https://www.networkedenergy.com/en/products/ANSI-smart-meter.

[14] "No Title," [Online]. Available: https://www.networkedenergy.com/en/products/iec-single-phase-meter.

[15] S. Shekara, S. Reddy, L. Wang, and V. Devabhaktuni, "Smart meters for power grid : Challenges , issues , advantages and status," *Renew. Sustain. Energy Rev.*, vol. 15, no. 6, pp. 2736–2742, 2011, doi: 10.1016/j.rser.2011.02.039.

[16] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on Advanced Metering

Infrastructure," *Int. J. Electr. Power Energy Syst.*, vol. 63, pp. 473–484, 2014, doi: 10.1016/j.ijepes.2014.06.025.
[17] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive Radio for Smart Grids : Survey of Architectures , Spectrum Sensing Mechanisms , and Networking Protocols," no. c, pp. 1–41, 2015, doi: 10.1109/COMST.2015.2481722.
[18] H. Hu, D. Kaleshi, A. Doufexi, and L. Li, "Performance analysis of IEEE 802.11af standard based neighbourhood area network for smart grid applications," *IEEE Veh. Technol. Conf.*, vol. 2015, pp. 0–4, 2015, doi: 10.1109/VTCSpring.2015.7146000.
[19] T. Chen, "Smart grids, smart cities need better networks," *IEEE Netw.*, vol. 24, no. 2, pp. 2–3, 2010, doi: 10.1109/MNET.2010.5430136.
[20] C. Gomez and J. Paradells, "Survey of home automation networks," *IEEE Commun. Mag.*, no. June, pp. 92–101, 2010, [Online]. Available: http://www.ann.ece.ufl.edu/courses/eel6935_11fal/papers/Survey of home automation networks.pdf.
[21] "No Title," [Online]. Available: file:///C:/Users/user/Downloads/f-secure-zigbee-overview.pdf.
[22] O. ZigBee, "ZigBee Smart Energy Standard ZIGBEE SMART ENERGY," pp. 1–628, 2014, [Online]. Available: http://www.zigbee.org/wp-content/uploads/2014/11/docs-07-5356-19-0zse-zigbee-smart-energy-profile-specification.pdf.
[23] S. Marksteiner, V. J. E. Jimenez, H. Valiant, and H. Zeiner, "An overview of wireless IoT protocol security in the smart home domain," *Jt. 13th CTTE 10th C. Conf. Internet Things - Bus. Model. Users, Networks*, vol. 2018-Janua, pp. 1–8, 2017, doi: 10.1109/CTTE.2017.8260940.
[24] Z. Alliance, "ZigBee Specificarion," *Stand. Oct*, 2015, [Online]. Available: http://ieeexplore.ieee.org/document/6264290/.
[25] "No Title," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=10.
[26] B. Fouladi and S. Ghanoun, "Security Evaluation of the Z-Wave Wireless Protocol," *Black hat*, p. 6, 2013.
[27] B. M. Dörge and T. Scheffler, "Using IPv6 and 6LoWPAN for home automation networks," *Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron.*, pp. 44–47, 2011, doi: 10.1109/ICCE-Berlin.2011.6031865.
[28] K. F. Tsang, W. C. Lee, K. L. Lam, H. Y. Tung, and K. Xuan, "An integrated ZigBee automation system: An energy saving solution," *Proc. 14th Int. Conf. Mechatronics Mach. Vis. Pract. M2VIP2007*, pp. 252–258, 2007, doi: 10.1109/MMVIP.2007.4430752.
[29] J. S. Lee, C. C. Chuang, and C. C. Shen, "Applications of short-range wireless technologies to industrial automation: A zigbee approach," *Proc. 2009 5th Adv. Int. Conf. Telecommun. AICT 2009*, pp. 15–20, 2009, doi: 10.1109/AICT.2009.9.
[30] "No Title," [Online]. Available: https://www.semtech.com/lora/lora-applications/smart-homes.
[31] I. L. L. P. Computing, B. E. The, N. Killer, I. Application, L. Most, and C. A. S. E. T. Of, "P - -p n," pp. 75–77, 2001.
[32] V. Mohan, "An introduction to wireless M-Bus," pp. 1–19, 2015.
[33] LinkLabs, "Low Power, Wide Area Networks networks (LPWANs)," vol. 19, no. 2, pp. 855–873, 2017.
[34] L. Germani, V. Mecarelli, G. Baruffa, L. Rugini, and F. Frescura, "An IoT architecture for continuous livestock monitoring using lora LPWAN," *Electron.*, vol. 8, no. 12, 2019, doi: 10.3390/electronics8121435.
[35] "No Title." http://www.link-labs.com/blog/sigfox-vs-lora.
[36] Sigfox, "Sigfox Technical Overview," vol. 1, no. May, p. 26, 2017, [Online]. Available: https://www.disk91.com/wp-content/uploads/2017/05/4967675830228422064.pdf.
[37] R. Fujdiak *et al.*, *Security in low-power wide-area networks: state-of-the-art and development toward the 5G*. INC, 2020.
[38] O. León, J. Hernández-Serrano, and M. Soriano, "Securing cognitive radio networks," *Int. J. Commun. Syst.*, vol. 23, no. 5, pp. 633–652, 2010, doi: 10.1002/dac.
[39] "No Title," [Online]. Available: https://medium.com/coinmonks/lpwan-lora-lorawan-and-the-internet-of-things-aed7d5975d5d.
[40] "No Title," [Online]. Available: https://www.iot-now.com/2019/12/13/100351-selecting-right-low-power-wide-area-network-lpwan-technology/.
[41] "No Title," [Online]. Available: https://www.ltts.com/solutions/nbon-narrow-band-iot.
[42] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of Cellular LPWAN Technologies for IoT Deployment :," pp. 197–202, 2018.
[43] R. S. Sinha, Y. Wei, and S. H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*,

vol. 3, no. 1, pp. 14–21, 2017, doi: 10.1016/j.icte.2017.03.004.
[44] "No Title." https://www.iis.fraunhofer.de/en/ff/lv/net/telemetrie.html.
[45] K. Nolan and M. Kelly, "IPv6 convergence for IoT cyber-physical systems," *Inf.*, vol. 9, no. 4, 2018, doi: 10.3390/info9040070.
[46] A. O. Otuoze, M. W. Mustafa, O. O. Mohammed, M. S. Saeed, N. T. Surajudeen-Bakinde, and S. Salisu, "Electricity theft detection by sources of threats for smart city planning," *IET Smart Cities*, vol. 1, no. 2, pp. 52–60, 2019, doi: 10.1049/iet-smc.2019.0045.
[47] "No Title." https://research.kudelskisecurity.com/2017/11/21/zigbee-security-basics-part-3/.
[48] "No Title." https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/.
[49] C. Hennebert and J. Dos Santos, "Security protocols and privacy issues into 6LoWPAN stack: A synthesis," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 384–398, 2014, doi: 10.1109/JIOT.2014.2359538.
[50] F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp, "Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT," *Glob. IoT Summit, GIoTS 2019 - Proc.*, 2019, doi: 10.1109/GIOTS.2019.8766430.
[51] "No Title," [Online]. Available: https://blog.radware.com/serviceprovider/2019/08/protecting-against-narrowband-iot-security-risks/.
[52] K. Mattioli, R ; Moulinos, *Communication Network Interdependencies in Smart Grid*. 2015.
[53] "No Title," [Online]. Available: http://www.cyberpunkreview.com/news-as-cyberpunk/the-cias-latest-claim-hackers-have-attacked-foreign-utilities/.