Cyber Security Issues for IoT based Smart Grid Infrastructure

Mariya Ouaissa¹, Mariyam Ouaissa¹

¹ENSAM, Moulay Ismail University, Meknes, Morocco

E-mail: mariya.ouaiissa@edu.umi.ac.ma

Abstract. We have been witnessing for several years the increasing networking of objects of all kinds that were not previously used to communicate. These newly connected objects together form the concept of Internet of Things (IoT). The energy sector is currently exploring the possibilities offered by the Internet of Things. However, for this sector, network intelligence is not a completely new phenomenon. The electrical networks already have information retrieval capacities for their monitoring and control, but these are still limited. The meeting of IoT and Smart Grids opens the way to data collection from all points of the network and in real time. Certain data previously collected in an aggregated manner over large geographic areas could now be collected on a local scale, near production or transmission points, and at a reasonable cost. It is also the massive accumulation of this data and its processing that is possible today. The smart grid is a network for the transport and distribution of electricity that is enhanced by capacities in terms of digital control, surveillance and telecommunications. It provides a two-way, real-time exchange of energy and information between the various players in the electricity chain, from the production site to commercial, industrial and residential users. The energy transition and the new smart grids raise many challenges in terms of industrial cybersecurity. Digital exchanges are intensifying (production, distribution and consumption are interconnected) and the use of connected objects (facilitating remote monitoring, observation and control of the entire value chain) increases the degree of vulnerability of information systems industrial. The cybersecurity of smart grids is today a decisive element in ensuring global security of our global energy systems. The purpose of this work is to present a comprehensive overview of challenges, threats and some solutions of security in IoT based smart grid. We focus in our study in network vulnerabilities, security requirements and cyber-attacks in smart grid in order to determine their impact in the network and give a guide on future research directions for cyber-security in smart grid applications.

1. Introduction
Currently the Internet knows a remarkable growth due to the development of connected objects. Internet is defined as a concept of communication of people anytime and anywhere, with the appearance of connected objects, the physical world can now communicate, whether for person-to-person, person-to-object or object-to-object relationships [1]. The Internet of Things (IoT) is defined as a global network of interconnected services and intelligent objects of all kinds designed to support humans in activities of daily living thanks to their detection, calculation and communication capabilities. Their ability to observe the physical world and provide information for decision making
will be an integral part of the architecture of the Internet of the future. These objects must integrate into a more global system than the digital world and adapt to it [2].

The IoT relies on the implementation of a multitude of new sensors, actuators and intelligent systems, which communicate with each other. The energy sector is currently exploring the possibilities offered by the internet of things [3]. Network intelligence is not a completely new phenomenon for this sector. The Smart Grid already have information retrieval capacities for their monitoring and control, but these are still limited.

Smart grids are electrical grids that adjust the flow of electricity between providers and consumers using information technology. These networks provide a balance of production, distribution and consumption by gathering information on the state of the network. Smart grids improve the balance between production and consumption, the efficiency and security of grids, promote the integration of renewable energy sources throughout the network and, thanks to better system management, generate energy savings and lower costs (for both production and consumption) [4].

The advent of the internet of things requires an increased need for cybersecurity. The increase in the number of points of interaction with the network potentially exposes smart grids to modern threats targeting information systems [5]. Various factors are directly implicated; the lack of consideration of safety during the design phases, the risk of obsolescence in the face of rapid technological developments, the absence of applicable and followed standards in terms of security and confidentiality, or the routing, storage and management of an exponential amount of data [6].

In this paper, we present the cyber security issues and challenges of the IoT based smart grid infrastructure. The next section describes the system network, features and standard of smart grid. In section 3 we discuss briefly the IoT concept and the link between IoT and smart grid. We present the security requirements of smart grid in section 4. We investigate security issues and challenges in the IoT based smart grid in section 5.

2. The Smart Grid Network

National and international energy saving needs make the modernization of electricity grids an absolute necessity. The smart grid constitutes a solution in term of management, metering, integration of renewable energies in the network. In this section, we start by briefly presenting the smart grid network and citing its advantages. Next, we will describe the most important standards in this field.

2.1. Smart Grid

For a long time, electricity was produced mainly from nonrenewable energy resources (nuclear, coal, natural gas, oil) centrally. These resources were becoming more and more expensive and scarce. Problems with the traditional power grid have accelerated the creation of a new concept called the smart grid, which is an electricity distribution network that uses information technologies to optimize the production, consumption and distribution of electricity [7]. It seeks to balance supply and demand for electrical energy by smoothing consumption peaks, which are costly and polluting. In practice, smart grids are presented as electrical networks to which a digital system of bidirectional communication between the supplier and the consumer has been added, an intelligent measurement system and a control system, the intelligent measurement system generally being an integral part (Figure1).

2.2. The Features of the Smart Grid Network

The features can be classified into four classes: operational efficiency, energy efficiency, customer satisfaction and environmental benefits [8].
2.2.1. **Operational Efficiency.** The smart grid increases the operational efficiency, first, it integrates the decentralized production of Distributed Energy Resources (DER). Each user can produce energy using energy resources renewable. There is an evolution from the model of one producer and several consumers to a model of several producers and several consumers. Then, it enables remote monitoring by using the Supervisory Control and Data Acquisition (SCADA) system and diagnostics by integrating sensors that are installed across the entire network. These sensors instantly indicate electrical flows and consumption levels. Still, it improves the reliability of public service power, operational performance and overall productivity.

2.2.2. **Energy Efficiency.** The smart grid helps reduce losses on the energy transmission and distribution network by optimizing electricity flows. It allows you to know the network status in real time, to anticipate incidents and to facilitate decision-making.

2.2.3. **Customer Satisfaction.** The smart grid offers several advantages to consumers. First, it reduces the duration and frequency of outages through remote maintenance with the Outage Management System (OMS). Then it improves the quality of the power supply with the voltage setting. Second, it allows consumers to reduce energy costs since they can decide when and how they want to use electricity. On the other hand, it helps empower the consumer to manage their energy consumption, to save money and overcome certain constraints in the power system, without compromising their lifestyle.

2.2.4. **Environmental Benefits.** The smart grid has several environmental benefits. First, it allows the integration of renewable energy resources. Then, it activates the wide adoption of electric vehicles. These vehicles reduce carbon emissions. Still, it ensures and enhances reliability and security of environment in order to resist to disruptions, attacks and natural disasters, anticipating and responding to system disruptions and strengthening security supply through capabilities of improved transfers.

2.3. **Security Standards for the Smart Grid**
Several standardization organizations have defined standards for the deployment of the smart grid network. The American organization National International Standard Technology (NIST) has defined an architecture for the smart grid. The European organization Institute of Electrical and Electronics Engineers (IEEE) defined the three layers of the network. He added the concept of centralized management of renewable energy [9].

![Figure 1. Smart Grid](image-url)
2.3.1. The Architecture Proposed by NIST. NIST proposed the basic architecture for smart grids. This architecture has seven domains namely: distribution, transmission, customer, markets, operations, bulk Generation, service provider as shown in Figure 2.

![Figure 2. NIST Smart Grid Architecture](image)

2.3.2. The Architecture Proposed by IEEE. In the architecture of NIST, each consumer can generate electricity using renewable resources. The surplus of produced energy is managed by the consumer himself, the management of the surplus of energy is decentralized. Given the complexity of the management task, the IEEE proposed an architecture based on that of NIST, but defined a new field called DER, which allows to manage the surplus of energy produced, the management surplus energy is centralized. In addition, IEEE has provided guidelines for understanding and defining the interoperability of smart grids. It defines three integrated architectural perspectives: the energy layer, the communication layer and the information layer (Figure 3).

![Figure 3. European Extension of the NIST Model](image)
3. IoT based Smart Grids

The internet of things is a major development in the field of Information Technology (IT) which increasingly dominates and reigns in the market for computer systems. IoT is the result of the development and combination of different technologies. It encompasses almost all areas of information technology today such as smart cities, Machine to Machine systems, connected vehicles, sensor networks, etc. IoT, also known as Web 3.0, represents an extension of the Internet to things and places in the physical world. Each physical object that can be a person, a computer, a smartphone, a car, a sensor, a smart house, is associated with a virtual entity, which behaves like an active entity in the system. The integration of IoT with a smart environment extends the capabilities of smart objects by enabling the user to monitor the environment from remote sites. IoT can be integrated with different smart environments and can generally be classified into the following areas: smart cities, smart homes, smart grid, smart buildings, smart transportation, smart health, and smart industry. Figure 4 illustrates the IoT-based smart environments [10].

Figure 4. IoT based Smart Environment

The Internet of Things (IoT) has recently emerged as enabling technology for the smart gird. Each device in the grid can be considered as an object. Utilizing the concept of IoT, each device can have a unique IP address that can upload its status and download control commands via the Internet. IoT allows devices on the smart grid infrastructure to be sensed and controlled remotely via a scalable communication network, which allows for easier integration between the physical world grid devices and computer based control systems thereby leading to improved efficiency and accuracy and enabling the grid to meet the energy needs of current and future generations (Figure 5) [11].
4. Security Requirements of IoT based Smart Grid

A certain number of security services are necessary to secure the exchanges of the objects based smart grid with the control center and to avoid attacks. The main challenges [12] of securing these exchanges can be summed up in the implementation of:

- An authentication service to prevent spoofing and fake message injection attacks. The injection of false disconnect commands, for example, can deprive electricity of an entire neighborhood or even sensitive public buildings such as hospitals, police stations, etc.

- An integrity service to avoid modification attacks. For example, the messages containing the measurements of energy consumed at the Home Area Network (HAN) level are of great importance in the smart grid network and their modification can have serious consequences on consumption costs.

- A privacy service to counter eavesdropping and invasion of privacy attacks. This service is of primary importance, since it will make the messages exchanged between the objects and the control center incomprehensible to any attacker. The use of the privacy service should meet the needs of applications in the smart grid network.

- Communications between the smart grid and the control center require the implementation of anti-replay mechanisms to avoid the replay of certain messages or orders such as; fault messages, consumption rate messages, invoice, and cut-off commands.

- Regarding the availability service, a malfunction of objects can have serious consequences, hence the need for the implementation of an availability service to avoid denial of service attacks. The same is true for the control center and the collector.
5. Cyber Security Challenges and Issues
Several equipment’s of smart grid network exchange a huge amount of data on a daily basis to optimize the production, consumption and distribution of energy [13]. Securing these data flows is essential. A single failure or attack could compromise the security of the entire power grid. In this section, we will describe in detail the attacks that can affect the intelligent network by classifying them [14].

5.1. Cyber Attacks on the Smart Grid Architecture
The deployment of information and communication technologies on power grids raises more concerns about the security of the power system and the protection of consumer data than with traditional power grids. We review some attacks that can be carried out on smart grids. We have chosen the classification of which makes it easier for us to identify smart grid attacks, since it is concerned with the various components of the smart grid network, namely:

- Devices
- Systems
- Networks

5.1.1. Attacks on Smart Grid Network Devices. The different devices of a smart grid network can be affected by several types of attack. In this part, we will present these attacks.

- Smart Meter

A malicious node can disrupt the functioning of smart meters by making several types of attacks:

✓ The jamming attack can be launched to prevent the Smart Meter from communicating with other nodes in the smart grid network.
✓ The wiretapping attack can be performed to detect sensitive information about the customer’s energy consumption. Similarly, this attack can lead to an attack on the privacy of consumers. In effect, the attacker can recover several private information. This information is critical since it can be exploited by thieves.
✓ Stealthy attacks: the attacker can inject false information about electricity prices, which can significantly increase consumers' bills.
✓ The application called Remote Connect Disconnect (RCD) can be used by attackers to perform a remote disconnection attack on the smart meter, thus depriving the customer of electricity. Still, attackers can use this application to connect a smart meter and take advantage of illegal power.
✓ Replay attack: the attacker can use the smart meters out of use by injecting incorrect data into the system, which can lead to incorrect energy prices or inaccurate predictions.
✓ Smart Meters are placed outside houses. An attacker can have physical access to at least one smart counter. It can launch a compromising attack via the Test Action Group (JTAG) interface to steal keys and other information.
✓ The energy requirements of certain devices are based on the energy consumption data supplied by the smart meter to plan their load according to demand and prices. An attacker can spoof the identity of a smart meter and send a false response to these devices in order to cause a great demand for energy, to increase the electricity bill or to cause the equipment to shut down.

- Phasor Measurements Units (PMU)

PMUs are placed on the transmission lines. They help create a snapshot of the state of the power grid (voltage measurement). They are able to collect measurements on electrical voltages and quantities and send them to the Phasor Data Concentrator (PDC). The PDC reads data from multiple PMUs and then merges it into a single message. This message will be communicated to the area of operations. PMUs transmit their measurements to the PDC hierarchically. Hierarchical architectures suffer from
drawbacks such as delay in messages. This drawback can be exploited by attackers. Package destinations of data to be sent is preconfigured. Manipulation of the destination lists of a (damaged) PMU by an attacker can cause attacks to spread to damage other PMUs. A malicious node can perform a spoofing attack on a PMU, modify PMU messages that contain energy measurement data, and can also read messages in transit between the PMU and the PDC. These attacks affect critical decision operations such as detection and the location of the event. For example, when an attacker re-plays an old PMU message that contains line failure information or energy loss measures, Grid systems can make a decision to cut power to an area. The availability of real-time PMU data is a critical issue; any inaccessibility of real-time data can affect the functionality of Wide Area Monitoring, Protection and Control (WAMPAC).

- **Plug-in Hybrid Electric Vehicle (PHEV)**

  Although a two-way communications infrastructure can bring many advantages for the smart grid, it can introduce new vulnerabilities. An attacker can manipulate the real-time pricing information that is communicated by the utility company for vehicles. The attacker can disrupt the transmission of electricity price information to the PHEV owner, resulting in the loss of the pricing information, which is, in fact, one of the possible attacks Denial of Service (DoS) on the smart grid. Likewise, it is possible for the attacker to manipulate pricing information by injecting incorrect price values in order to mislead owners of plug-in hybrid vehicles.

- **Remote Terminal Unit (RTU)**

  Remote Terminal Units are traditionally used to configure and troubleshoot devices in the remote intelligent network. This remote access functionality can give rise to attacks that allow malicious nodes to take control of devices. A denial of service attack on a smart grid device can saturate the computing power of the CPU, memory or bandwidth and will result in delay in real-time data exchange. As a result, control center operators do not have a complete picture of the state of the power grid, leading to incorrect decisions.

- **Sensors or Intelligent Electronic Devices (IEDs)**

  Switches are used to protect the power infrastructure in substations, when an IED detects an anomaly, it sends a message to open/close to the switches to balance the power load. If an attacker impersonates a surveillance IED, he could send false close/open messages to the switches and damage the protection system, resulting in potential loss of power to clients.

5.1.2. **Attacks on Smart Grid Systems.** In this part, we will study the security of some smart grid systems.

- **Control and Management Systems**

  Control and management systems (For example: Distribution Management System (DMS), Energy Management System (EMS), Supervisory Control and Data Acquisition (SCADA)) play a key role in the smart grid network. It is necessary to protect them from attack. A malicious node can carry out DoS attacks on control systems and make them unavailable.

- **Wide Area Monitoring, Protection and Control (WAMPAC)**

  The Wide Area Monitoring, Protection and Control system exchanges transmission data with other control systems to provide real-time monitoring and alarm functions and ensure efficient power transmission, production and aggregation in the electric grid. The WAMPAC system is also vulnerable
to DoS attacks while these services are provided in real time. Denial of service can affect the different layers of communication.

- Advanced Metering Infrastructure (AMI)

AMI is the communication infrastructure for smart meters. It is used to provide two-way communication between customers and suppliers. The communication channels used by AMI to communicate data between smart meters and utilities are also vulnerable to cyber attacks. Data transit through these channels can be intercepted. The Man In The Middle (MITM) attack can be launched. Energy consumption data can be changed before sending messages. Also, by listening to the wireless communication channel, an attacker could obtain the information exchanged between smart meters and the control center. Demand Response (DR) is an essential part of automatic load management and builds on the ability of the AMI communications infrastructure to send load reduction requests for smart meters and other devices, for dynamically manage the overall system load.

- Outage Management System (OMS)

Automated outage management requires smart meters to send out fault information. The utility uses the information to restore power in reduced time. A disruption of this application directly affects by delaying detection and the correction of faults. Crash management is resilient if the utility can still identify and recover from crashes within a limited time, where time is dependent on the specific requirements of the utilities. An attacker can spoof the identity of a smart meter and send a crash message, however he can modify the message sent to influence the resilience of the grid. On a larger scale, several attackers can impersonate several smart meters in the same geographic area and send almost identical messages to learn about a disaster. The control center can make the decision to cut the power in this geographic area.

5.1.3. Attacks on Smart Grid Networks. Smart grids are connected and controlled by communication networks. We have chosen to classify the attacks that can be carried out on networks, in two categories.

- Attacks used on the routing protocols
- Attacks used on the communication protocols

- Attacks on Routing Protocols

Among the routing protocols that can be used in NAN networks, we cite:

- Routing Protocol for Low-Power and Lossy Networks (RPL) defined in RFC6553 by the Internet Engineering Task Force (IETF). It has been designed to support the specific requirements of these networks. RPL is a proactive distance vector routing protocol that builds a Destination Oriented Directed Acyclic Graph (DODAG). The DODAG built allows each node to transmit the data it has collected to the DODAG root. Each node in the DODAG selects a parent according to a given routing metric and an objective function. The collected data is forwarded from child to parent to the root. RPL routing protocol for IoT can be affected by Selective Forwarding Attacks: malicious nodes try to stop packets in the network by refusing to forward or delete the messages that send them. crosses. With these attacks, it is possible to launch DoS attacks where malicious nodes selectively transmit some packages. This attack is mainly intended to disrupt the routing paths.

- The Energy Minimum Transmission Protocol (MTE) takes the basic Dynamic Source Routing (DSR) protocol and assigns a weight to each of the links which is a function of the energy required to transmit a packet on this route. Routing takes place along lighter routes, aggregating all the
links making up a path. The attacks of the wireless sensor network are applicable to the MTE routing protocol (DoS, ...).

- Attacks on Communication Protocols

The communication protocols used within a smart grid are also a major source of vulnerabilities. Certain protocols can be affected by attacks: DoS, listening, modifying.

- ZigBee: ZigBee has a major drawback, all passwords are stored in clear text in the storage space. If the attacker obtains physical access to the device, he can copy the memory of the device to the computer, and then he can find the key. ZigBee can be affected by DoS attacks.
- Protocol C37.118: is an IEEE standard for the use of synchrophasors in power systems. The C37.118 protocol does not encrypt the messages exchanged between the PDC and PMU. An attacker can perform a listening attack. Still, it is vulnerable to MITM attacks because it does not verify the source of the messages it receives from the PMU.
- DNP3: Distributed Network Protocol (DNP3) is a communication protocol widely used by public services of electricity. They used iperf (a network traffic generator) to occupy the communication channel, which reduces network availability. They showed that the packages Long DNP3 are more vulnerable to DoS attacks than short DNP3 packets. The DNP3 protocol is a documented protocol, it may be subject to reverse engineering.

5.2. Countermeasures against Cyber Attacks

To protect system from multiple attack vectors, we find that the countermeasures, which until now were almost exclusively software, are no longer sufficient and that a good knowledge of the hardware platform becomes more and more important for a better mastery of the security of a computer system. Thus, it is essential today to know not only the functioning of the programs, but also to ensure the good behavior of the entire processing chain, including lesser known hardware components, such as the chipset, inputs-outputs or peripherals. Many challenges are encountered to secure intelligent grid systems from many attacks and to achieve the security demands and objectives of the intelligent grid, since intelligent grid assets are distributed across large areas. The cyber defense solutions should protect all aspects of smart grid systems. The defense solution integrate multiple defense techniques including proactive real-time intrusion prevention/detection systems (IPS/IDS) using machine learning and artificial intelligence, network segmentation, controlled wireless propagation, authentication, authorization, certification [15]. The proposed solutions should comprise of scalable, resilient, and adaptive cyber security/defense techniques for smart grid operation without affecting any legitimate smart grid operations.

6. Conclusion

The smart grid is an energy distribution network that uses communication technologies to optimize the production, consumption and distribution of electricity. IoT is the next step towards a globally and pervasive connection to any communication and computation enabled objects. The smart grid is the biggest deployment of IoT technology, where smart devices are deployed along the energy path, all the way from the generation plant to the end-customer. In the literature, several researchers have looked into the security of the smart grid network and have identified a number of attacks that can be carried out, namely identity theft attacks by a smart meter, one of the essential components of the smart grid network. Similarly, the attacker can replay energy consumption messages that aim to disrupt the billing system of users. Some attacks can even deprive the customer of electricity. The integration of communications technologies into the electrical grid presents a source of vulnerability.

In this paper, we presented a comprehensive survey of the main security issues and challenges for the IoT based smart grid infrastructure. In this context the use of the IoT provide a better control and
monitoring of the power grid in smart grid network, so it is necessary to concentrate on the security challenges in order to develop to implementation and integration of the IoT devices in the smart grid.

References

[1] Atzori L, Iera A, and Morabito G, The Internet of Things: A survey, Computer Networks \textbf{54(15)}, 2787–2805, 2010.

[2] Yacchirema DC and Palau C, Smart IoT Gateway For Heterogeneous Devices Interoperability, \textit{IEEE Latin America Transactions} \textbf{14(8)}, 3900-3906, 2016.

[3] Ouaissa M, Ouaissa M, and Rhattoy A, An efficient and secure authentication and key agreement protocol of LTE mobile network for an IoT system, \textit{International Journal of Intelligent Engineering and Systems}, \textbf{12(4)}, 212-222, 2019.

[4] Fang X, Misra S, Xue G, ans Yang D, Smart grid—The new and improved power grid: A survey, \textit{IEEE communications surveys & tutorials}, \textbf{14(4)}, 944-980, 2011.

[5] El Mrabet Z, Kaabouch N, El Ghazi H, and El Ghazi H, Cyber-security in smart grid: Survey and challenges, \textit{Computers & Electrical Engineering}, \textbf{67}, 469-482, 2018.

[6] Kimani K, Oduol V, ans Langat K, Cyber security challenges for IoT-based smart grid networks, \textit{International Journal of Critical Infrastructure Protection}, \textbf{25}, 36-49, 2019.

[7] Chen SY, Song SF, Li LX, ans Shen J, Survey on smart grid technology, \textit{Power system technology}, \textbf{33(8)}, 1-7, 2009.

[8] Yan Y, Qian Y, Sharif H, ans Tipper D, A survey on smart grid communication infrastructures: Motivations, requirements and challenges, \textit{IEEE communications surveys & tutorials}, \textbf{15(1)}, 5-20, 2012.

[9] Gungor VC, Sahin D, Kocak T, Ergut S, Buccella C, Cecati C, and Hancke GP, Smart grid technologies: Communication technologies and standards, \textit{IEEE transactions on Industrial informatics}, \textbf{7(4)}, 529-539, 2011.

[10] Ahmed E, Yaqoob I, Gani A, Imran M, ans Guizani M, Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges, \textit{IEEE Wireless Communications}, \textbf{23(5)}, 10-16, 2016.

[11] Mugunthan SR and Vijayakumar T, Review on IoT based Smart Grid Architecture Implementations, \textit{Journal of Electrical Engineering and Automation (EEA)}, \textbf{1(1)}, 12-20, 2019.

[12] Rawat DB ans Bajracharya C, Cyber security for smart grid systems: Status, challenges and perspectives. In SoutheastCon, IEEE, 1-6, 2015.

[13] Bekara C, Security issues and challenges for the IoT-based smart grid. In FNC/MobiSPC, 532-537, 2014

[14] Gunduz MZ and Das R, Cyber-security on smart grid: Threats and potential solutions, \textit{Computer Networks}, \textbf{169}, 107094, 2020.

[15] Wang W and Lu Z, Cyber security in the smart grid: Survey and challenges, \textit{Computer networks}, \textbf{57(5)}, 1344-1371, 2013.