Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2019, 6(12):205-208**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

The Investigation of Information Security Risks and Solutions in Smart Grids

Mehmet ÇINAR

Tatvan Vocational School, Bitlis Eren University, Bitlis, Turkey
e-mail: engmcinar@gmail.com

Abstract Developments in electrical energy systems make the system increasingly intelligent; As it becomes smarter, it will bring the integration of information and communication technologies and infrastructures. This integration of energy systems with Information and Communication Technologies and infrastructure; it will make the network more vulnerable to cyber attacks and threats. At this stage, the issue of information security is of great importance. Information security; means securing the confidentiality, integrity and accessibility of the information. The main tools of information security: Protection of data integrity, rapid and high quality of access to information, prevention of unauthorized access, continuity of the business continuity and ensure the continuity of the system. According to internationally published reports, electricity networks are targeted at various cyber attacks on a daily basis. Threats and cyber attacks from malware are increasing day by day. Modern routing and control technologies, such as the protection of critical infrastructures and data communication links, are now among the fundamental tasks of the energy sector. With the development of smart grids, in addition to the physical network environment, there is a cyber world where millions of new generation smart devices with communication capability are created. The physical infrastructure of the conventional network and the provision of cyber security of smart grids that bring this new cyber world under one roof will be the most important future for the electric power sector. Cyber security should be considered as an integrated solution to evaluate organizational, economic, technological and regulatory perspectives. Communication standards in smart networks are divided into two types: wired and wireless; powerline communication (PLC) and cable line communication (fiber / optic) standards are used. In wireless communication; Zig-Bee, Z-wave, Wi-fi, WIMAX and cellular communication standards are used.

In this study, the above mentioned communication standards are explained in the smart grid; Network security, endpoint / endpoint user security, data security, application security, identity and access control are elaborated and how to protect the smart grid from a possible cyber attack or how to protect the network with the least loss.

Keywords Smart Grids, Information Security, Cyber Attack, Network Security

1. Introduction

If we look at the smart grid as a definition, it is an approach that must be added to smart grid and monitoring systems in order to ensure mutual electronic communication between the supplier and the consumer. In fact, it is not only the meter but the whole network from production to the end consumer can be monitored and controlled remotely. The development and transition of energy is continuing and in the future, customers are expected to take an active role in the management of energy. This change affects a wide range of operational processes, network control and monitoring systems, production facilities, communications and information exchange between companies and customers. Traditional business models are changing and with the introduction of new

technologies, isolated systems will be able to communicate with each other continuously using open standards. Thus, a large amount of sensitive information will be exchanged. These trends present many challenges in resource security, network stability and increasing network security. Threats and cyber attacks from malware are increasing. Modern routing and control technologies such as the protection of critical infrastructures and data communication connections are now among the core tasks of the Energy Sector.

2. Information Security

Information security means ensuring the confidentiality, integrity and accessibility of information. Storing information in an environment where continuous access to information is ensured is defined as the process of ensuring the integrity of the information from the sender to the recipient in a confidential manner (with the protection of privacy), without disturbance, alteration and being seized by others, and transmitting it safely. In this context, three basic concepts of information security are briefly stated as follows [1]:

Confidentiality: Access to private and confidential information only by authorized persons,

Integrity: Protection of corporate information from unauthorized changes or corruptions,

Accessibility: Accessibility of corporate information when needed,

Basic Objectives of Information Security (Cyber Security): [2]

a. Protection of data integrity
b. Maintaining access to information, speed and quality of access,
c. Prevention of unauthorized access, Protection of privacy and confidentiality,
d. Preventing cyber theft,
e. Ensuring business continuity and continuity of the system.

2.1. Types of Communication Used in Smart Grids:

In smart grids, the amount of data offered by each component in the system will increase exponentially. It is important to ensure that large amounts of data are transmitted in a safe, fast and accurate manner. In particular, the use of smart meters, which is one of the cornerstones of smart networks, involves high amounts of data transfer. While this data is sensitive, it is confidential and access to this data should be limited to specific personnel. It is equally important that the smart meter data contains all information about the energy consumption of the consumer and the state of the network without any manipulation or miscalculation. Some standardized communication networks, which are on the way to standardization in smart grids, should support the operation and distribution automation of the smart grid system even in case of power failure. However, the selected communication technologies should be cost effective; provide adequate data rate, security features, bandwidth and power quality [3]. Communication in smart networks can cover large or small geographic areas Communication infrastructures used for these networs:

1. Wireless communication
2. Wired communication infrastructures.

2.1.1. Wireless communication:

Wireless communication technologies use airborne signals and therefore do not require wiring, the locations of the endpoints are flexible, and wireless signals can reach areas where it is physically difficult to access. The most commonly used technologies in this group are as follows:

ZigBee: ZigBee is a short-range, low data rate, energy efficient wireless technology based on the IEEE 802.15.4 standard.

Z-wave: It is a short range, low data rate wireless RF network standard.

Wi-Fi: It is the short-range communication standard that is known to most people and has IEEE 802.11 standard.

WiMAX: Worldwide Worldwide Interoperability for Microwave Access (WiMAX) “approach for microwave access; IEEE 802.16 is a standard based communication system developed for broadband wireless access in terms of fixed and mobile point-to-point communication.

Cellular communication: This standard, which started with analog phones in 1980s, is the GSM GPRS communication standard in our daily lives with 2G, 3G, 4,5 G standards.
Cognitive radio: IEEE 802.22 standard CR-based, 802.22 standard communication infrastructure that allows unlicensed users to access TV bands not used by licensed users.

2.1.2. Wired communication technologies

It serves as fiber optic and communication cable. There is additional cost of cable pulling and operating. Power line communication: The first steps for automation of the power grid have been taken using power line communication PLC technology. PLC uses low and medium voltage power lines as data communication area. PLC was used by some electrical companies for load control and remote measurement. Since the power lines already reach the meter, they can simply be adapted to the intelligent meter system. The PLC is considered suitable for HAN, NAN and FAN since it does not involve an external wiring cost. PLC technology was first operated in narrowband and started to operate in broadband due to the needs of consumer applications [4].

2.2. Security analysis in smart grids

One of the most important issues in smart grid systems is communication systems. It is of great importance to have a reliable system in addition to an extensible, applicable communication network. In the event of a security vulnerability, the main threats include blocking communication and control systems, and sending and modifying production and consumption data. In order to avoid such situations, the designed system should be analyzed in detail, definitions and needs should be determined. In this way, needs will be identified and solutions will be more successful.

2.2.1. Problems with the consumer interface

Together with smart grids, new system components are expected to be deployed at the consumer layer. The first of these is the smart meters that will allow consumption data to flow to the distribution system center in real time. The second one is the use of inverters, etc., to transmit data on the energy generated by consumers through solar panels and wind turbines to the distribution system center. components are. After evaluating this table from the information security perspective, two risks can be expected:

- End users changing consumption data by intervening in meter data
- Loss of personal privacy of the consumer
- End users intervene with inverter data and modify production data.

When the first risk is taken into consideration, it is seen that data integrity should be ensured at the interface between smart meters and distribution system. This requirement, which can be provided by end-to-end cryptography, reveals the need to implement the crypto algorithm on the smart meter. In addition, the key management process, involving millions of smart meters, must be able to operate effectively. These requirements are difficult to meet, especially as the residential smart meters need to be under a certain price. In addition to end-to-end cryptography, it is stated that it is necessary to identify attacks by testing the “normality inin of data collected at the system center [5]. It is noted that additional R & D studies are required to meet these requirements [6].
By monitoring the consumption in a residential or commercial facility by means of smart meters, information about the activities carried out in these areas or habits of the living individuals can be produced [7]. This raises the violation of personal privacy rights and requires more serious access control than confidential information that must be protected in corporate information systems in accordance with the esi need to know ”principle. In order to meet this requirement, firstly, unnecessary data should not be collected, and secondly, access to the data collected in the system center should be managed in the most serious way.
It is noted that the security requirement regarding the integrity of the production data can be solved by end-to-end cryptography as in smart meters, and that the budget constraint on the component on which the crypto algorithm will be implemented will not be as challenging as the smart meter, but there is a need for R & D on “tamper-resistant structures.

3. Conclusion

Smart grid systems, simultaneous monitoring, management, information storage, electricity network security, rapid fault detection and self-repair, the importance of the communication system to be used in terms of functions is better understood. With the introduction of Smart Grid applications, which are highly dependent on information systems, information security threats to existing electricity transmission and distribution systems are expected to diversify and reach system centers from a wider attack surface. Therefore, for the success of smart grids, additional solutions in the dimension of information security must be produced. Some of the requirements are within the scope of interface standardization and can be realized through inter-institutional coordination and cooperation. For another part of the requirements, efficient and economic products need to be developed. The first product that comes to mind in this context is the smart meter. It is considered that distribution companies act in solidarity within the scope of determination of requirements related to smart meters, product standardization, procurement and testing, which will help in solution. It can be said that the studies carried out within the scope of both interface standardization and smart meter standardization under the leadership of an authorized public institution will contribute to the solution.

References

[1]. Wang, W., & Lu, Z. (2013). Cybersecurity in the Smart Grid: Survey and Challenges. *Computer Networks*, 57(5), 1344-1371.

[2]. Yan,Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys & Tutorials*,14(4), 998-10.

[3]. Gharavi, H., & Hu, B. (2013). 4-way handshaking protection for wireless mesh network security in smart grid, IEEE Global Communications Conference (GLOBECOM) Atlanta GA, 790-795.

[4]. Amarsingh, A.A., Latchman, H.A., & Yang, D. (2014). Narrowband power line communications: Enabling the smart grid. *IEEE Potentials*, 33(1), 16-21.

[5]. Cardenas A. A., Moreno R., "Cyber-Physical Systems Security for the Smart Grid", NISTIR 7916 Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop, 2012

[6]. NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References, 2010

[7]. NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, 2010