International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:15, No:4, 2021

Taxonomy of Threats and Vulnerabilities in Smart Grid Networks

Faisal Al Yahmadi, Muhammad R. Ahmed

***Abstract*—**Electric power is a fundamental necessity in the 21st century. Consequently, any break in electric power is probably going to affect the general activity. To make the power supply smooth and efficient, a smart grid network is introduced which uses communication technology. In any communication network, security is essential. It has been observed from several recent incidents that adversary causes an interruption to the operation of networks. In order to resolve the issues, it is vital to understand the threats and vulnerabilities associated with the smart grid networks. In this paper, we have investigated the threats and vulnerabilities in Smart Grid Networks (SGN) and the few solutions in the literature. Proposed solutions showed developments in electricity theft countermeasures, Denial of services attacks (DoS) and malicious injection attacks detection model, as well as malicious nodes detection using watchdog like techniques and other solutions.

***Keywords*—**Smart grid network, security, threats, vulnerabilities.

I. Introduction

SGN is an emerging technology that utilizes the developed infrastructure to overcome different upcoming challenges expected to be faced in the next decades. The challenges are modeled based on the power production through alternative energy sources, decentralized generation and the growing power demand expected with the use of electrical vehicles (EVs). SGN is a power network empowering a two-way stream of power and data with communication technology [1]. The network enables the detection, reaction and pro-action towards any changes in usage and other issues. The technology also enables recognition, response and support of acts to changes in usage and different issues. SGN has the capability of handling itself as well as enabling the consumer to become an active participant in the network. The behavior and the actions of all stockholders of the electricity are observed in SGN. In order to ensure an economically efficient and sustainable power system with low losses with quality of service, it is important to ensure the security of supply and safety of SGN. The benefits of SGN include:

- Reliable electrical supply,
- Generation of green energy and alternative energy,
- decentralized generation with multiple energy sources,
- Reduction of carbon emissions,
- Smart home appliances and smart meter, and
- Opening new doors for jobs.

Information and communications technologies (ICT) enabled SGN to monitor, operate and control the system with added features. The technology was implemented in the transmission phase in conventional grids. In SGN, the technology used is advanced. Therefore, extended to generation and distribution phases [2]. ICT has the ability for two-way communication which allows electricity providers and companies to use the current used infrastructure more efficiently. It will also allow the customer to participate and choose new power usage patterns.

A model of SGN proposed by the National Institute of Standards and Technology (NIST) of SGN architecture is shown in Fig. 1.

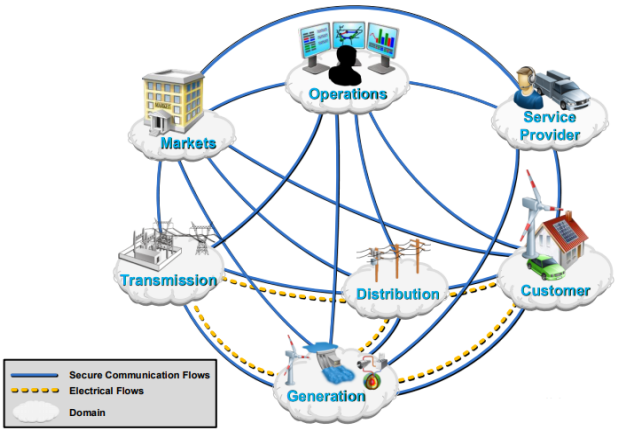

Fig. 1 NIST Smart grid architecture model (SGAM) [3]

The architecture has seven domains, which are generation, transmission, distribution, operations, service providers, markets and consumer. These domains use ICT to communicate and operate SGN efficiently. Fig. 1 also illustrates the electric flow between transmission, distribution, customer and generation, while communication flows across all seven domains. SGN uses many components in its system and network, all explained as follows:

1) SGN system components: SGN system components are smart appliances in households, smart meters, renewable sources and Electric Utility Operation Center. Service providers make use of these components to monitor and control electrical energy.
2) SGN network components: SGN uses different networks for its communication, which are Home Area Network (HAN) and Wide Area Network (WAN). A HAN used to connect smart appliances in the house with a smart meter to communicate with the network. A WAN used to

Faisal Al Yahmadi* and Muhammad R Ahmed are with the Marine Engineering Department, Military Technological College, Muscat, Sultanate of Oman (*corresponding author, phone: +968 22091204, e-mail: 1606002@mtc.edu.om, Muhammad.ahmed@mtc.edu.om).

communicate between a HAN and service provider and markets providing the required information.

SGN works based on communication technology. In any communication network security is the major concern. As a result, SGN security is one of the most important factors to be considered. Considering the SGN security concerns, in the paper we have worked on the security threats and vulnerabilities of SGN.

This paper is organized as follows. Section II gives an insight of general security. Section III explains the main SGN vulnerabilities. Sections IV and V consist of a brief explanation about SGN attackers and SGN types of attacks, respectively. Section VI addresses the vital challenges faced in SGN implementation. Section VII suggested the proposed solutions found in literature. Section VIII concludes this paper.

II. SGN Security Requirements

In the SGN, security has the utmost importance when it comes to sharing our data with multiple parties. Security is vital across all SGN and systems. Moreover, to explain the security requirements for all types of networks, the following requirements will be discussed [4].

- Confidentiality: or privacy, which means data can be only accessed by authorized parties.
- Authentication: means the ability of the service or host to validate users' identity.
- Integrity: data can only be modified by authorized parties.
- Availability: data are available to authorized parties when requested.
- Nonrepudiation: receiver must have the ability to identify the received message sender or source
- Data Freshness: the data received should be the current and new data.
- Secure management: in the network management levels the security should be dealt is an efficient way.

III. Vulnerabilities of SGN

Security is an essential need for SGN, especially cyber security. The SGN will digitalize the grid by implementing new technologies. The backbone of the SGN is the ICT which will be sending and receiving the data that need to be delivered safely and on time in order to properly operate grid functions. Different data will have different security levels and different functions. Digitalizing the grid with new technologies has made it more complex, thus exposing it to a wider range of attacks. Any attack that delays, manipulates or views data can affect thousands of households and consumers. The vital security concern of SGN network security is the connecting of private dwellings to the internet exposing consumer's privacy to many risks. There are many external/ physical and software/internal vulnerabilities in SGN [5]. Hence, if attacks happen in SGN that could compromise the privacy of the dwellings. Both external and internal vulnerabilities will be discussed below:

1) Physical/External vulnerabilities: which can be defined as the physical security related to electronic devices and equipment that operates the grid. Some of the vulnerabilities are as follows:

a. Vital power electronics located in unguarded areas,
b. Outdated power electronics made without security in mind,
c. Outdated power electronics might be fully or partially incompatible with new technologies.

2) Software vulnerabilities: which can be defined as the security related to designed systems and software systems that have been fabricated to operate grid functions and protect its security. Some of the vulnerabilities are as follows:

a. Customer information security,
b. Greater number of intelligent devices,
c. Implicit trust between traditional power devices,
d. Using Internet Protocol (IP) and commercial off-the- shelf hardware and software,
e. Modbus security selected.

IV. SGN Attackers

SGN attackers normally try several methods to attack the network. In order to discuss the attacks, we have to understand the source and motivation behind it. Several types of attackers exist [6]; it is easier to classify network attackers into two main groups depending on the attacks types which are external and internal attackers explained as follows:

1) External attackers: who execute attacks against SGN without having access to the grid's internal security. Some of the attackers who commit these attacks are [7]:

a. Non-Malicious attackers: who view the security and operation of the system as a puzzle to be cracked. Those attackers are normally driven by intellectual challenge and curiosity.
b. Terrorists: who view the smart grid as an attractive target as it affects millions of people making the terrorists draw more attention at a large scale.
c. Competitors: attacking each other for the sake of financial gain.

2) Internal attackers: who execute attacks while having access or knowledge to the network security [8]. These attacks can be harder to detect and have a higher success rate because of the valuable resources attached to the attacks. These attacks can be correlated with the following attackers [7]:

a. Consumers: driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power.
b. Employees: disgruntled on the utility/customers or ill-trained employees causing unintentional errors.

V. SGN Types of Attacks

The SGN is a large-scale network and usually across thousands of miles. The bigger the network, the higher chance it will encounter attacks. To insure both company and consumer security, all attacks must be studied before

happening to prevent anyone taking advantage of weak links in the systems and to put the right measures in place to encounter them. SGN attacks can be classified into external attacks and internal attacks, and will be discussed as follows.

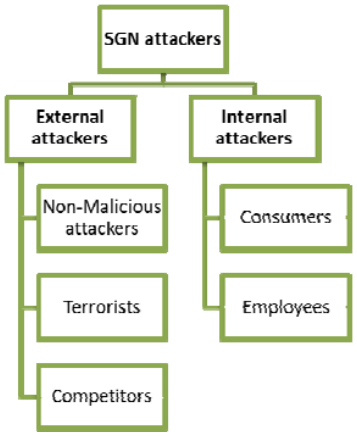

Fig. 2 Types of SGN attackers

External attacks can be defined as the attacks that are executed directly through the grid infrastructure or physical components rather than through the ICT of the grid. These attacks can cause destruction; in other words, it can be defined as physical attacks. On the other hand, internal attacks can be defined as attacks targeting network nodes or other components connected to the grid ICT, which leads to the abnormal or malicious behavior of the target causing distribution or malfunction to the network.

In SGN, there are several external and internal attacks found in the literature [9]. We have outlined a few attacks in Fig. 3.

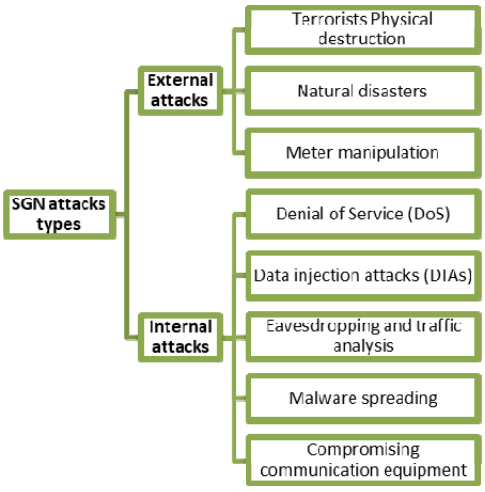

Fig. 3 Types of attacks on SGN

VI. Vital Challenges for Attack Detection

Attack detection can be a difficult task, because some attacks are not trying to alter the system operation and the reason might be to steal or view data. Considering these, preventive measures must be applied and checked regularly. In this process, researchers found some challenges when detecting malicious attacks, as listed below [7]:

- Old power electronics devices and equipment were designed in the early days without cyber security in mind. This causes the power electronics to serve as a weak point in the network security.
- Smart grid is a massive network that has digital components all across the nation and most of the devices are located out of companies' guarded facilities. These components can be reached and used as multiple entry points to access the network from anywhere.
- Smart grid implements different technologies together increasing the network complexity. The more complex the system is, the more exposure the network to a wider range of attacks. This will ultimately increase the need to regularly supervise the network for any up normal activity.
- Lack of expertise. Since SGN have not been around for a long time, engineers have to think ahead to prevent weak links in the security chain of the system. Implementing new technologies can have flaws and will need a regular risk assessment and development to perform in the best manner possible.
- Different standards. Different regions have their own standards and policies making it difficult to settle on one universal security architecture. Integration of systems and technologies can have various difficulties because of the different ways adopted to implement the new technologies. Different approaches taken to develop resilient security solutions consumed longer periods to develop robust solutions. As a result, the network is still vulnerable to many attacks. Moreover, having universal standards will speed the development process and will eliminate possible threats faster and more efficient.

VII. Suggested Solutions in Literature

The SGN introduces enhancements and improved capabilities to the conventional power network making it more complex and vulnerable to different types of attacks. Researchers over the years have developed many solutions related to SGN cyber security. However, some solutions were developed to protect SGN from certain types of attacks. Some of the suggested solutions discussed are as follows:

Abdulrahman et al. in [10] provided answers to three major questions pertaining to the performance of electricity theft detectors in the presence of data poisoning attacks, by proposing a sequential ensemble detector based on a deep auto-encoder with attention (AEA), gated recurrent units (GRUs), and feed forward neural networks. The proposed robust detector retains a stable detection performance that is deteriorated only by 1−3% in the presence of strong data poisoning attacks.

Lizong et al. in [11] proposed a time series anomaly detection model, which is based on the periodic extraction method of discrete Fourier transform, and determines the

sequence position of each element in the period by periodic overlapping mapping, thereby accurately describing the timing relationship between each network message. The experiments demonstrate that the model has the ability to detect cyber-attacks such as man-in-the-middle, malicious injection, and Dos in a highly periodic network.

Jing et al. [12] discussed defense mechanisms to either protect the system from attackers in advance or detect the existence of data injection attacks to improve smart grid security. Focusing on signal processing techniques, this article introduces an adaptive scheme on detection of injected bad data at the control center.

Watchdog like techniques were discussed in [13]-[15]. The main goal of the watchdog algorithm technique is to determine a malicious node by over-hearing the communication of the next hop from the network. These mechanisms can detect the packet dropping attack by allowing nodes to communicate with neighbor nodes by broadcasting data transmission. The communication allows neighbor nodes to detect dropped packets and report to the system.

Recently, game theory is used to investigate wireless sensor networks for the detection of attacker nodes [16]. Reddy and Ma did work on game theory in [16], [17], respectively. Reddy et al. proposed a zero-sum game which has the ability to detect malicious wireless sensor nodes in the forwarding and dispatching routes only [16]. In a zero-sum game, an algorithm is necessary to retain a convenient level of energy in the node. The presented game theory method in [17] is an improvement work. It has the advantages of being cost effective and improving the security of the network. It also decreases the cost instigated by monitoring or observing sensor nodes and extends the life span of each sensor node.

VIII. Conclusion

The conventional grid systems are transforming to the smart grid considering the new grid benefits and features. SGN utilizes the ICT to perform two-way interchange of electricity and the exchange of information. Communication networks are always susceptible to the security threats. Therefore, provisioning of security is an essential task for SGN. To do that, we need to understand the security threats and vulnerabilities posed to the SGN. In this paper, we have presented the threats and vulnerabilities in SGN. This will lead the researchers to develop the resilient security mechanisms by considering threats and vulnerabilities associated with SGN.

References

[1] J. B. Ekanayake, N. Jenkins, K. Liyanage, J. Wu, and A. Yokoyama, *Smart Grid: Technology and Applications*. John Wiley & Sons, 2012.

[2] F. Skopik and P. Smith, *Smart Grid Security: Innovative Solutions for a Modernized Grid*. Elsevier Science & Technology Books, 2015.

[3] C. Greer *et al.*, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," National Institute of Standards and Technology, NIST SP 1108r3, Oct. 2014. doi: 10.6028/NIST.SP.1108r3.

[4] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification," p. 7, 2013.

[5] ETV 2 NITTTRCHD, *Cyber Security in Smart Grid: Overview Session 1 Module 15 by Janorious Rabeela*. 2019.

[6] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011, doi: 10.1109/TSG.2011.2159999.

[7] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions," *SGCE*, pp. 1–6, 2012, doi: 10.12720/sgce.1.1.1-6.

[8] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of Security Threats in Information Systems," *Procedia Computer Science*, vol. 32, pp. 489–496, Jan. 2014, doi: 10.1016/j.procs.2014.05.452.

[9] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas, "Smart Grid Security: Threats, Challenges, and Solutions," *arXiv:1606.06992 (cs, math)*, Jun. 2016, Accessed: Mar. 06, 2021. (Online). Available: http://arxiv.org/abs/1606.06992.

[10] A. Takiddin, M. Ismail, U. Zafar, and E. Serpedin, "Robust Electricity Theft Detection Against Data Poisoning Attacks in Smart Grids," *IEEE Transactions on Smart Grid*, pp. 1–1, 2020, doi: 10.1109/TSG.2020.3047864.

[11] L. Zhang, X. Shen, F. Zhang, M. Ren, B. Ge, and B. Li, "Anomaly Detection for Power Grid Based on Time Series Model," in *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Aug. 2019, pp. 188–192, doi: 10.1109/CSE/EUC.2019.00044.

[12] J. Jiang and Y. Qian, "Defense Mechanisms against Data Injection Attacks in Smart Grid Networks," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 76–82, Oct. 2017, doi: 10.1109/MCOM.2017.1700180.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, New York, NY, USA, Aug. 2000, pp. 255–265, doi: 10.1145/345910.345955.

[14] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in DSR based ad-hoc networks," in *Proceedings IEEE 56th Vehicular Technology Conference*, Sep. 2002, vol. 4, pp. 2424–2429 vol.4, doi: 10.1109/VETECF.2002.1040656.

[15] S. Bansal and M. Baker, "Observation-based Cooperation Enforcement in Ad Hoc Networks," *arXiv:cs/0307012*, Jul. 2003, Accessed: Feb. 01, 2021. (Online). Available: http://arxiv.org/abs/cs/0307012.

[16] Y. B. Reddy, "A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks," in *2009 Third International Conference on Sensor Technologies and Applications*, Jun. 2009, pp. 462–468, doi: 10.1109/SENSORCOMM.2009.76.

[17] Yizhong Ma, Hui Cao, and Jun Ma, "The intrusion detection method based on game theory in wireless sensor network," in *2008 First IEEE International Conference on Ubi-Media Computing*, Jul. 2008, pp. 326–331, doi: 10.1109/UMEDIA.2008.4570911.