Dogo Rangsang Research Journal
ISSN : 2347-7180

UGC Care Group I Journal
Vol-09 Issue-01 No. 01 : 2022

Challenges of the Existing Security Measures Deployed in the Smart Grid Framework

Kummari.Shailaja
Assistant Professor of EEE
Balaji Institute of Technology & Science
e.Mail:-shailaja5607 @gmail.com

Gali.Sridhar
Assistant Professor of EEE
Balaji Institute of Technology & Science
e.Mail:sridhar08249@gmail.com

V .Chinmeyi Laxmi Prasanna
Assistant Professor of EEE
Balaji Institute of Technology & Science
e.Mail:-vasavimartha15@gmail.com

***Abstract*—Due to the rise of huge population in mankind and the large variety of upcoming utilization of power, the energy requirement has substantially increased. Smart Grid is a very important part of the Smart Cities initiative and is one of the crucial components in distribution and reconciliation of energy. Security of the smart grid infrastructure, which is an integral part of the smart grid framework, intended at transitioning the conventional power grid system into a robust, reliable, adaptable and intelligent energy utility, is an impending problem that needs to be arrested quickly. With the increasingly intensifying integration of smart devices in the smart grid infrastructure with other interconnected applications and the communication backbone is compelling both the energy users and the energy utilities to thoroughly look into the privacy and security issues of the smart grid. In this paper, we present challenges of the existing security mechanisms deployed in the smart grid framework and we tried to bring forward the unresolved problems that would highlight the security aspects of Smart Grid as a challenging area of research and development in the future.**

Keywords-smart grid; SCADA; ICS; Smart meter; AMI

I. INTRODUCTION

Security of the Operational Technology Devices, which are the important part of the smart grid venture, deliberated at transforming the conventional power grid system into a robust, reliable, adaptable and intelligent energy utility, is an impending problem that needs to be attended quickly. Again with the increased integration of operational technology devices with other ecosystem applications and the existing communication backbone is compelling both the customers and the energy utilities to thoroughly look into the privacy and security issues of the Smart Grid [1]. The definition of Smart Grid and current Indian Scenario has been discussed in Section 2. The security challenges in the key operational technologies like ICS, SCADA & AMI has been studied in detail and described in Section 3 of the paper [2], [3].

II. UNDERSTANDING THE SMART GRID

A conventional power grid including generation, transmission and distribution coupled with the telecommunication infrastructure and information technology is called a smart grid. The modernized grid is supplied with electronic gadgets that can be used for monitoring, management and command control. From monitoring point of view, the live operations of the smart grid helps the system operators to test and alleviate issues ofthe smart grid operations that might have caused an power outage or a collapse situation in the recent past. From the consumer‟s point of view, the live information‟s traversing through the smart grid allows the energy users to restrain their power consumption and maintenance cost. „Fig. 1‟ shows the schematic diagram of a Smart grid.

Smart Grid Architecture = Electricity Network + Telecommunication Infrastructure + Information Technology

Figure 1. Schematic diagram of a smart grid.

A. Smart Grid Benefits

- Improves the reliability and quality of power
- Capacity enhancement of the present conventional power grid
- Improves the difficulties of disturbance
- Self-healing responses and predictive maintenance can be achieved
- Control and monitoring of the composite system from a central smart grid control center
- Distributed energy sources are considered
- Embraces distribution and substation automation
- Provides facility as a service
- Enhance the possibility of grid security and safety
- Customers are given preferences
- Exploration of new equipment‟s, services and consumerization
- Energy storage options through electric vehicles and modern storages

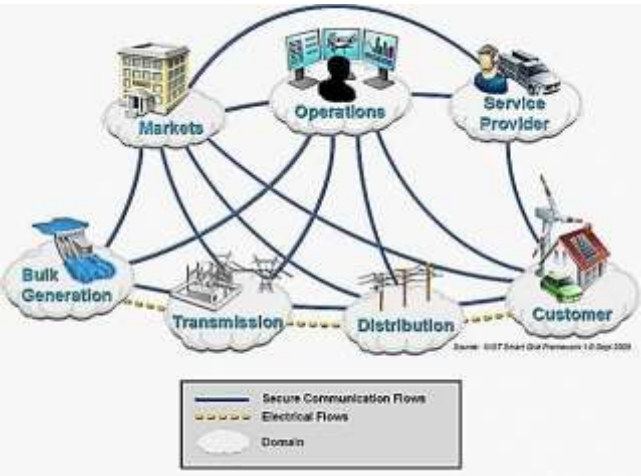

Figure 2. NIST framework of smart grid with 7 domains.

The above diagram in „Fig. 2‟ shows that the Distribution domain is connected to the countrywide or regional level Transmission Grid and provides power to the consumers through its own or other connected network. To manage the grid and the consumers of the Distribution domain, all the six domains users have to exchange data within themselves through a secure communication medium [4]. Nowadays the mission critical operation of energy utilities has becomemore complex. The IT and OT systems are being automated for effective management of the electrical grid and associated enterprise applications. The IT operations are carried out through a robust and secured data communicationnetwork at various locations including the IT for OT stations.IT and OT segregation as per the regulators or ministry is just next to impossible. In this scenario the availability of theOT systems can be maintained with an IT/OT convergence through a secured communication channel.

„Fig. 3‟ shows the schematic of various IT & OT systems deployed in Power Industry. The IT applications are riding on the IT bus and encompass the enterprise corporate network which is exposed to the Internet. Since the IT systems are exposed to the Internet they are more prone to the cyber-attacks and thus the OT systems are connected in asegregated manner. For the enterprise application integration, the information in form of data has to be traded between the IT & OT systems through an Enterprise Service Bus (ESB) or a complementary secured information flow method. The conventional electrical grid was designed to provide electrical energy from the generating stations through the transmission systems to the domestic and commercial consumers. The lower middle class took the full protection ofthe Government and used the pilferage technique of power theft as a luxury. As the power utilities are privatized, the energy theft was restrained with the modern electronic gadgets and growing communication technology.

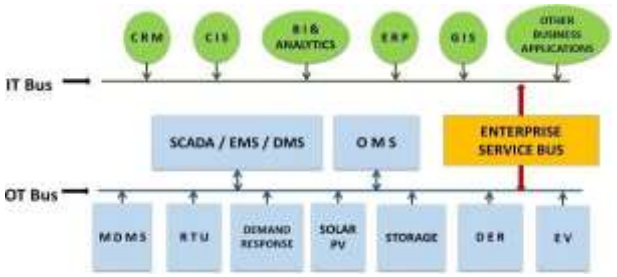

Figure 3. IT & OT operation under smart grid regime.

According to a study in Emerging Markets Smart Grid: Outlook, each year the world loses around 89.3 billion US$ [5], of which India recorded the highest loss followed by Brazil and Russia. In Indian perspective, record says that most theft occurs in Mumbai, Maharashtra, and house to the third largest slum in the world, Dharavi. So, the techniques of the pilferage used are very unpurified and incompetent, which can be easily opposed but due to the incompetency of the government and utility alike, criminals have been getting away with it. Deployment of smart meters might prove exceptionally influential, since they require more revolutionary stealing techniques. But this will provide a chance for the expert criminals to make sustainable and reproductive products that can be used for electricity theft. Hence, security against more advanced forms of energy theft like data tampering will become more sensitive.

The organization for Smart Grid standardization like IEEE, NIST, IEC, ETSI etc. are coming up with guidelines and standards. Maximum contributions are in the field of smart metering, advanced metering infrastructure, generation & transmission systems, distribution and substation automation, electric vehicles and distributed energy resources. The National Institute of Standards and Technology (NIST) collaborated with few forums and groups to provide a guideline for the Smart Grid framework. The European Telecommunications Standards Institute (ETSI) worked on the architecture for the smart grid to be proposed for the European Union. IEEE has developed the

IEEE 2030-2011 guide for Smart Grid interoperability that defines three levels of the Smart Grid architecture: power systems, communications technology, and information technology.

III. Security Challenges in the Smart Grid

A. *Vulnerabilities, Attacks & Type of Attackers in SCADA/ICS Systems*

Utilities having Smart Grids implemented meet the electricity demand by way of generating or purchasing power from the agencies having centralized/distributed generating stations and deliver to the customers through its transmission and distribution systems [6]. The electronic systems and upgraded communication technologies plays an important part in the monitoring and maintenance of the electrical power grid. The modern technologies assure energy utilities to control the supply and demand chain maintained at a sustainable cost. The most critical problem in smart grid operations is Information security. Three main objectives must be fulfilled in the smart grid system: 1) availability of uninterrupted power supply as per customer requirements 2) integrity of communicated information and 3) confidentiality of user‟s data. Operational Technology deployed in Smart Power Grid introduces flexibility and improved capabilities to the conventional power network. With the introduction of advanced ICTs and IEDs the power management has become simplified but the entire IT enabled grid has become vulnerable to different types of attacks. The said threats might give access to the criminals to attack the communication network and compromise the confidentiality and data integrity of the information affect the consumers with a blackout. The motivated and targeted attacks are still unknown by the firewalls and unifies threat monitoring devices as it could not read the behaviors‟ of the attackers [7], [8]. The next generation threat protection is still missing in the legacy control system of the energy utilities. The different attack variants in the SCADA/ICS Systems are given below in „Fig.4‟.

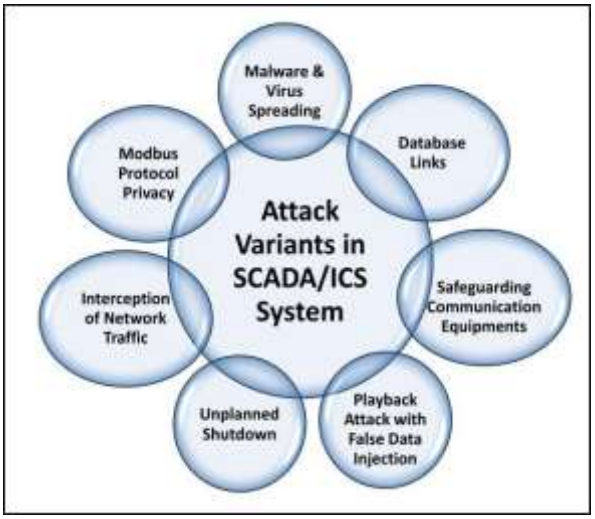

Figure 4. Attack variants in SCADA/ICS system.

Types of attackers:

- ✓ The attackers with intention to crack the system as an ethical hacker have no intention to bring down the system. Their motive is to gain reputation amongst the peers.
- ✓ The end customers in home may become revengeful and try hacking methods to physically shutdown their home meters.
- ✓ The cyber criminals are special types of attackers always try to jeopardize the meter management system through the public internet.
- ✓ Dissatisfied employees commits unintentional mistakes to affect the power systems and eventually becomes an attacker.
- ✓ The other power utilities due to stiff competition may try to bring other utility systems down to have financial profits.

The criminal which creates innovative attacks are mostly classified into three main categories: Component-wise, protocol-wise, and topology-wise. Component-wise attacks target the field components that include Field Remote Terminal Unit (FRTU) and Remote Terminal Unit (RTU) used for the Distribution Systems. Again the remote monitoring facility used for the monitoring, management and control of the FRTU and RTUs may endanger the power distribution system. False data injection and reverse engineering are the methods popularly used in the Protocol-wise attacks. The DOS and distributed DOS are mainly used in the Topology-wise attacks to cripple the communication channels of the system operators resulting into congestion of the data communication traffic in the power system.
The attack surface is as follows [9]:

a. Sending false broadcast messages to endpoint devices (Message spoofing),
b. Replaying authentic recorded messages back to the master control center (Baseline response replay),
c. Locking out a master and controlling one or more field devices (Direct slave control),
d. Sending trustworthy information to all possible addresses to collect equipment information (network scanning),
e. Scanning Modbus messages (Passive reconnaissance),
f. Delaying response messages intended for the masters (Response delay), and
g. Attacking a machine with the proper ports (Rouge interloper).

B. *Vulnerabilities / Attack Surfaces of AMI*

1) *AMI Architecture*

The Advanced metering infrastructure (AMI) is one of the major entities in the context of Smart grid. The concept of bi-directional communication could be achieved through the automated meter reading (AMR) and AMI. Since the public cloud is used for the AMR, there is a high chance of man in the middle attacks. The AMI on the other hand has a RF mesh network in which the smart meters communicates

with a data collector and the data collector in turn communicates with the meter data management system through the corporate communication network. „Fig. 5" below describes the architecture of AMI and their interface. The AMI interface includes Consumer Portal layer, Metering layer and the Communications layer. The distributed energy resources, Smart meters, Distribution management systems are all interconnected with each other through the communication interface.

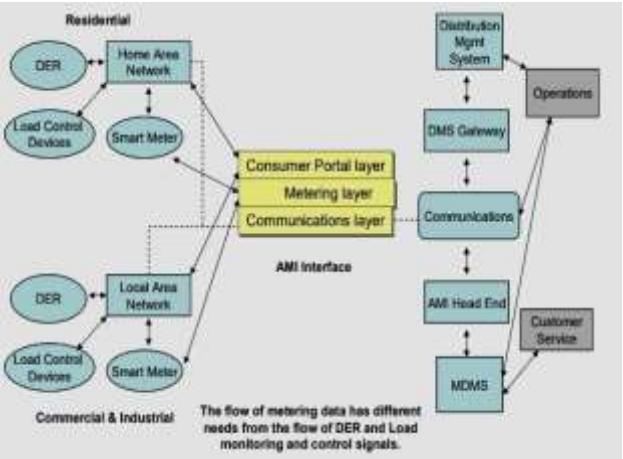

Figure 5. Architecture of advance metering infrastructure.

In the above mentioned figure, the consumption data is communicated from the customer premises to the power utility servers through communication layer. The energy usage can be monitored by the consumers through the smart meters at their home. The tariff pricing information is very sensitive and supplied by the service provider. The service provider triggers the load control devices to control the energy demands depending on the customer price preference.

2) Communication System

The two major communication systems predominant in the smart metering framework [10]:

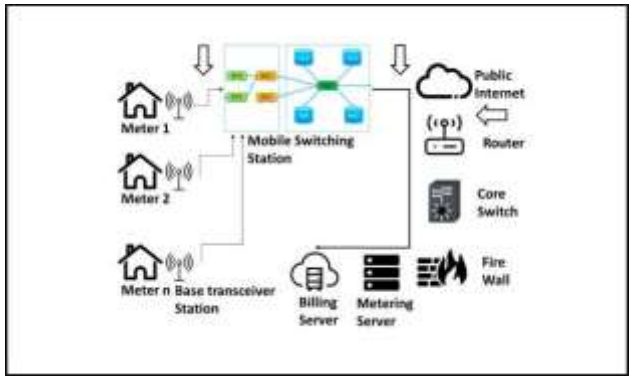

Figure 6. Vulnerability points of the smart meter communication using public internet.

a) Public Internet –In this system, the smart meters are having an in-built General Packet RadioService (GPRS) modem to communicate with a point of presence tower known as the Base Transceiver Station (BTS) of the service provider. The data from the smart meters are passed through the internet to the head end Energy Utilities network. Passed through a link load balancer and stateful packet filtering through a firewall, the data arrives at the core switch which performs port based access control and finally the data in form of customized files are sent to the billing server for customer billing. The effective areas of vulnerability are marked in „Fig. 6" with arrows.

b) RF mesh network- In this system a large network of interconnected smart meters, which serve as communicating nodes. This network is an adaptive and smart communication network in which the signal hops from one node to another until it reaches its head end servers of the energy utility. The nodes communicate through the access point and the data reaches the corporate network which traverses through a core switch and firewall and finally to the meter data management systems (MDMS) with the help of a trusted IPSec virtual private network (VPN) channel. From the MDMS the customized files are sent to the billing server where the consumer billing is done. The smart meters try to communicate using the access points or its neighborhood meters and in case of non- success there is an arrangement for mobile communication through the same access points to the GPRS cloud and finally through the public internet to the designated utility server. The effective areas of vulnerability are marked in „Fig. 7" with arrows.

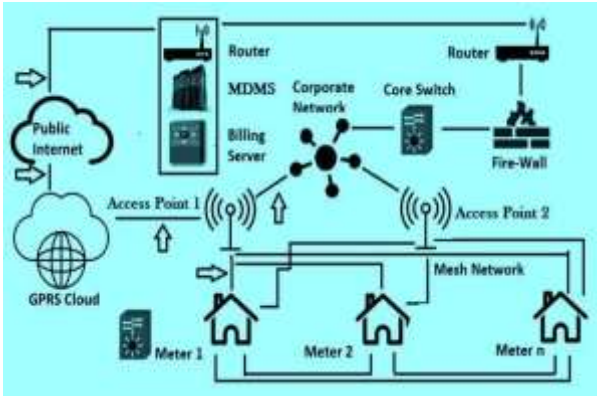

Figure 7. Vulnerabilities points of the smart meter communication using RF mesh network.

3) Tampering and Data Manipulation Techniques

We have classified tampering into two parts:

1. Physical Tampering – In this tampering scheme, the perpetrator tries to access the meter physically. In this method mostly the customer himself in their home tries to tamper the meters. Basically no

certified training is required to achieve this, so it is largely practiced among members of the lower middle class community [11], [12].

2. Data Hacking– This is a more advanced technique of data manipulation; this is associated with structured crime carried in a systematic way. The reasons here is to earn money from the operation of energy theft, disposing of hardware or software tools to settle the deals related to smart meters, or to create terrorism. Data can be tampered in a number of methods – alter the meter data in the servers, or system or in the public internet or service providers network by man in the middle attacks [13]-[15].

IV. CONCLUSION

The Smart Grid security is a necessity since the information flow is delicate and system operations are censorious and responsive (switching off the electricity, shutting down of smart meters etc.). The Smart Grid is arranged in many verticals and each vertical involves disparate devices and systems. Thus, it is very difficult to study the vulnerabilities and threats of the whole power distribution and generation network. In this paper, most of works are focused on identifying threats and attacks on domains and even on complex devices and systems. The smart meter is a critical instrument and is vulnerable to many types of attacks (physical tampering and data hacking). Industrial Control systems can be affected by DOS, Denial of service attacks that make systems slow and even unavailable. Man in the middle attacks on the AMI systems can lead to physical or data tampering which could cripple the functionality of the system and also may incur huge financial loss as if the meter data consumption unit is increased then the utility would be benefited and the consumer will suffer .Similarly if the consumption unit is reduced then the consumer would be benefited and the utility suffers. The detailed survey on the security of the smart grid framework brings out the gaps that have to be minimized if not eradicated through an end to end security mechanism from the field devices to the control center.

REFERENCES

[1] Rajiv K Bhatia, Varsha Bodade, "Smart grid security and Privacy: Challenges, Literature Survey and Issues," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 1, January 2014.

[2] Jing Liu and Yang Xia, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Communication Survey and Tutorials*, Vol. 14, No. 4. , 2012, Page**(s):** 981 – 997.

[3] Lindah Kotut, Luay A. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids ," *In Proceedings of the 2016 Cybersecurity Symposium (CYBERSEC)*, Coeur d'Alene, ID, USA, 18-20 April, 2016.

[4] The Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for Smart Grid Cyber security, NISTIR 7628 (2010) 1–597.

[5] Northeast Group, llc, "Emerging Markets Smart Grid-Outlook 2015", 2014. [Online].Available: http://www.northeast-Group.com/reports/Brochure Emerging%20Markets%20Smart%20Grid-Outlook%202015-Northeast%20Group.pdf.

[6] Fadi Aloul, A.R. Al-Ali, Rami Al-Dalky, Mamoun Al-Mardini, Wassim El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions," International Journal of Smart Grid and Clean Energy, vol. 1, no. 1, September, 2012.

[7] Feng Ye, Yi Qian, Rose Qingy Hu, "Smart Grid Communication Infrastructures: Big Data, Cloud Computing, and Security," Wiley-IEEE Press, 304 pages, August, 2018.

[8] Longfei Wei, Luis Puche Rondon, Amir Moghadasi, Arif I. Sarwat, "Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid" *In Proceedings of the 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Denver, CO, USA, 16-19 April 2018.

[9] Chen Peng, Hongtao Sun, Mingjin Yang, and Yu-Long Wang, "A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks," IEEE Transactions on Systems, Man and Cybernetics: Systems PP (99): 1-16, January 2019.

[10] Tanvi Mehra, Vasudev Dehalwar, Mohan Kolhe, "Data Communication Security of Advanced Metering Infrastructure in Smart Grid," 5th International Conference and Computational Intelligence and Communication Networks, Mathura, India, 27-29 Sept, 2013.

[11] Mathew Carpenter, Travis Goodspeed and Josh Wright, "Hacking AMI," InGuardians, Inc., 2008. [Online]. Available:https://rmccurdy.com/scripts/downloaded/Pen%20Test%20Perfect%20Storm/090202-SANS-SCADA-Hacking%20AMI.pdf.

[12] Stephen McLaughlin, Dmitry Podkuiko, and Patric McDaniel, "Energy theft in the Advanced Metering Infrastructure," Conference: Critical Information Infrastructures Security, 4th International Workshop, CRITIS 2009, Bonn, Germany, September 30 - October 2,2009.

[13] Pallab Ganguly, Sumit Poddar, Sourav Dutta, Mita Nasipuri, "Analysis of the Security Anomalies in the Smart Metering Infrastructure and its impact on Energy Profiling and Measurement," *In Proceedings of the 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*, Rome, Italy, Volume 1, April, 2016, pages 302-308.

[14] Muhammad Ismail, Mostafa Shahin, Mostafa F. Shaaban, Erchin Serpedin, Khalid Qaraqe, "Efficient Detection of Electricity Theft Cyber Attacks in AMI Networks," *In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC)*, Barcelona, Spain, 15-18 April 2018.

[15] Pallab Ganguly, Mita Nasipuri, Sourav Dutta, "A Novel Approach for Detecting and Mitigating the Energy Theft Issues in the Smart Metering Infrastructure," Technology and Economics of Smart Grids and Sustainable Energy,Springer,Volume 3, Issue 1, December, 2018.