A Review of Possibilities and Solutions of Cyber Attacks in Smart Grids

[1]Suman Avdhesh Yadav, [2]Shipra Ravi Kumar, [3]Smita Sharma, [4]Akanksha Singh
[1]Department of Information Technology, [2] Computer Science Engineering, [3, 4] Electronics and Communication Engineering
[1,2,3,4] Amity University, Greater Noida, India
[1]suman.avdheshyadav@gmail.com, [2]shipra.chaudhary85@gmail.com, [3]smitapandey86@gmail.com, [4]akankshasingh5614@gmail.com

Abstract **- The conventional power grid is now maturing to smart grid that incorporates a heterogeneous amalgam of operating measures like smart appliances, meters, renewable energy resources. Smart grid merges the conventional electrical power grid with ICT. Electric convenience can now realize three sets of amendments: framework upgrade, digital inclusion; the ethos of smart grid; and business process transformation, that make capital out of investments in smart technology. With this amalgam both the service providers and users get benefitted with numerous advantages like improved efficiency and availability, better control, benchmarking and managing user requirements. Smart grid technology also infers re-engineering of the conventional framework. A smart grid is a complex network which comes with many security issues and threats. This paper highlights the security issues associated with smart grid network. We enlighten the challenges faced and the drawbacks in existing security solutions.**

Keywords- Smart Grids; user privacy; cyber attacks.

I. INTRODUCTION

A smart grid includes a variety of operational and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficiency resources [1]. Smart grids make use of distributed systems to provide its services to its customers. These help in cutting down the cost of providing services in an authentic and systematic manner. Smart grid systems make use of data provided by the customers through a 2-way digital communication. According to the National Institute of Standards and Technology, smart grid systems provide the following benefits:

1) Improved power reliability and Quality
2) Minimize requirement of Back-up
3) Enhanced capacity and efficiency
4) Improving Resilience to Disruption and Being Self-Healing
5) Automated operation and maintenance
6) Reduced greenhouse gas emissions
7) Improved utilization of Renewable and Distributed Energy Sources
8) Reducing oil consumption
9) Enable adaptation to plug-in electric vehicles
10) Increasing consumer choice

978-1-5090-2084-3/16/$31.00 ©2016 IEEE

Security is the most dominant affair in smart grid systems. Now when we talk about security; it comes with three key goals:

1) Availability of service
2) Data Confidentiality
3) Integrity of Information shared.

The chief components of Smart Grid are elaborated below:

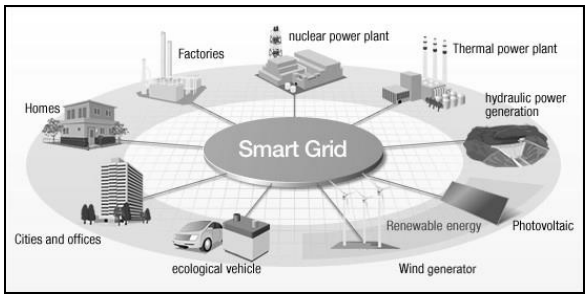

Fig. 1. Smart grid network

Fig. 1 demonstrates the smart grid framework. The power generation is commuted by different sources like wind, solar, nuclear etc. the generated power is then provided to users through different centers. There are five key factors to consider for the efficient operation of the smart grid: communications, smart metering, distributed energy resources, monitoring and controlling [2, 3]. Communication across the power line uses feeder section lines as a medium between consumers and utilities [4]. The distribution of energy resources allows for the moving away from centralized power stations to more widely available options as well the inclusion of alternative energy supplies [5, 6].

The paper is organized as follows. Section II enlightens the fundamental concepts of smart grids. Section III discuss about the core vulnerabilities to smart grid systems. Section IV explores the possible threats. Section V discusses the difficulties in implementing security measures. Section VI talks over the present and requires solutions, and Section VII condenses the paper.

II. BASIC CONCEPTS OF SMART GRIDS

Fig.2 illustrates the Smart Grid framework as suggested by NIST incorporating seven specific areas.

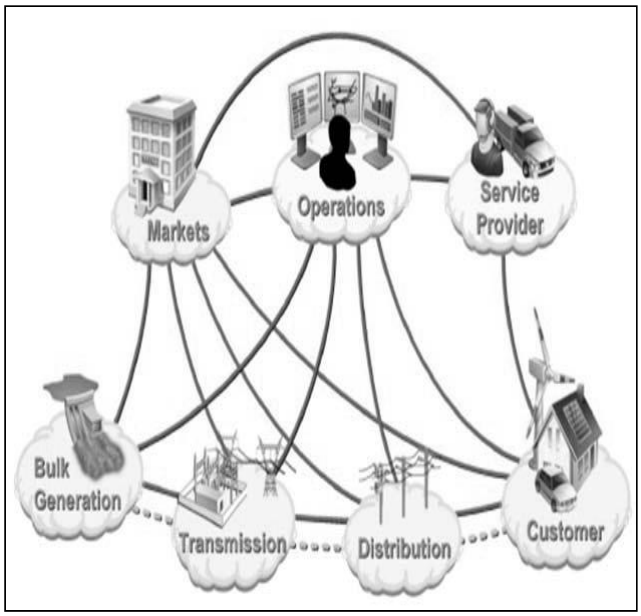

Fig. 2. Domains of a smart grid [NIST].

As mentioned previously, the smart grid allows for more efficient energy distribution than its predecessor, however, Refs. [7-12] demonstrates that, the smart grid is vulnerable to security threats at both the physical and logical layer. Theft, Sabotage and Vandalism are threats encountered in the Physical layer whereas data confidentiality is vulnerable at the logical layer.

The smart energy sector has suffered a wide spectrum of attacks over the last five years. Web-based applications and SCADA systems are vulnerable to entities coming between the data and the data-gathering system, such as the Stuxnet worm which hit Iranian power stations in 2010. It has been demonstrated in 2011, that the load on devices can be increased overflowing levels over the internet. The metering network can be compromised and deny consumer services, according to the work of Berthier, et al. in 2012.

Today's smart energy sector is especially designed to bear heavy power generation that serves its distant customers via a two-way transmission and distribution system. The upcoming Smart grids will incorporate huge small-scale generation units of renewable energy resources and other contrasting energy resources. Highly scalable and decentralized integrated communication, computing and power networks will be necessary to monitor these smart grids of the future [13].The main constituents of smart grid are Home Appliances, Renewable Energy resources, Smart Meter and Service Providers.

Home Appliances used in our home today are able to operate with smart meters connected in our Home Networks. This provides facilitating systematic consumption of electricity.

Renewable Energy Resources are used in providing locally generated power to home appliances.

Smart Meter is a device used to that account the power consumption periodically. Smart meters are embedded system constituting a microcontroller, analog/digital ports, timers, clock and serial communication facilities. These meters also activate alarms if any deviation from normal functionality is encountered.

Service Providers work with consumers to serve power on contractual basis. These Service providers collaborate via an authenticated certificate with smart meter to control internal equipments. These certificates are provided by getting registered with the electric authority and act as facilitator in communicating customers.

Smart grid work with two types of networks: Home Area Network (HAN); installed in our houses and Wide Area Network (WAN); that connects a wider range of devices. A home network establishes connection among all the smart devices installed in a house and connects them to the smart meter. Home networks passes messages using Zigbee, Ethernet, or Bluetooth; whereas a WAN establish connections between distant devices, smart meters and the service providers through WiMAX, LTE/3G/GSM, or optical fiber for establishing a communication. Fig. 3 illustrates the basic architecture of smart grid networks demonstrating the HANs, BANs and IANs.

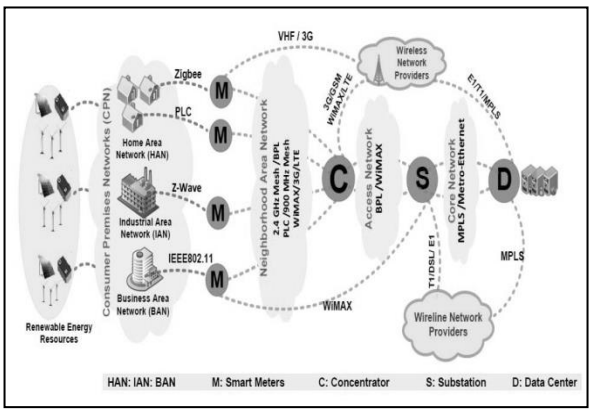

Fig. 3. Basic network architecture of Smart Grid

To make the network more efficient, flexible and reasonable; new features, intelligence and communication functionalities can be added to it [14] [15].

III. CORE VULNERABILITIES TO SMART GRID SYSTEMS

There is a vast range of vulnerabilities to smart grid as it has a vast infrastructure. There can be a reduction in demand as a result of lack of availability of services initiated by cyber attacks [16].

Smart grid network introduces enhancements and improved capabilities to the conventional power network making it more complex and vulnerable to different types of attacks. These vulnerabilities might allow attackers to access the network, break the confidentiality and integrity of the transmitted data, and make the service unavailable. As proposed in [17], the following vulnerabilities are the most serious in smart grids:

1) *User's Privacy*: The Smart meters have the access on customer's private information that can be used to obtain sensitive information like user's activities like the consumption time or idle time when devices are free or when there is no one at the user's location.

2) *Large number of access points*: Smart grid involves numerous devices that are used to control both power supply and network requirements. All these numerous devices give a broad access to attackers. Also, managing such a big number of devices is a complex task.

3) *Physical security*: Smart grid connect devices that are situated in remote locations, thus physical security of each and every device is again a major concern. These insecure locations need separate security mechanisms controlled by local bodies.

4) *Frequent Updating of network components:* The life of the IT components is limited in a grid. These need to be updated time to time and act as weak points and some time raise compatibility issues too.

5) *Wholehearted trust among conventional energy devices*: Communication between devices installed in a grid is vulnerable to spoofing; especially among cascaded devices. For instance, if the output of a device acts as input to another device, wrong data can lead to malfunctioning of entire network.

6) *Dissimilarity between Teams*: Different teams work in different locations in smart grid. The incompatibility and communication gaps between teams result in bad decisions and leaves loop holes in system security.

7) *Use of Internet Protocol (IP) and commercial off-the-shelf hardware and software*: IP gives a benefit of maintaining compatibility between devices. But, IP is vulnerable to several cyber attacks such as DoS, spoofing and many more.

8) *More stakeholders*: More and more stake holders are being added to the network each day. This has an adverse effect also. An authorized user can also attack the system and this too is tough to detect.

IV. POSSIBLE THREATS AND THEIR CATEGORIES

With a big number of malicious cyber attacks on the networks, identifying possible vulnerabilities is of great significance. Any attacker can utilize the vulnerabilities discussed in previous section with different intentions and can affect the network security. An attacker can be internal or external to the network.

The authors in [18] have categorized cyber attackers into following categories:

1) *Non-malicious attackers*; who take the security system as a puzzle and try to decode them with their intellectual concepts.
2) *Consumers;* mainly the unhappy customers driven by revenge and hatefulness for other consumers or the service provider.
3) *Terrorists;* who target smart grids and aim to cut down the service or retrieve crucial information.
4) *Internal Employees;* untrained employees or unhappy employees who have hatefulness for other consumers or the service providers.
5) *Rivals;* they attack each other for personal benefits or sometimes just to disrupt the resources of counterpart.

Few more categories of attacks are discussed in [19] including:

1) *Using Malware:* An intruder can use malwares to crash the smart meters or important resources. Malwares can also alter or delete sensitive information.

2) *Unauthorized Access:* Intruders can access the network through unauthorized access if the database is not using a security mechanism to check the authenticity of the logins. Unauthorized access can exploit the network resources and this is tough to detect if the login is not secure.

3) *Replay:* An attacker may send false messages or may retransmit same message multiple time to create an unauthorized effect. These false messages have adverse effect. These can engage the receiver unnecessarily or may overload receiver resulting in malfunctioning or slow down of the whole communication.

4) *DoS attacks:* This type of attack delays the response from servers and since smart grid uses IP, smart grid has the possibility of vulnerabilities inherent in the DoS attacks. Such attacks can also block the transmission of message packets over the network.

5) T*raffic analysis:* A cyber attack can take a form of simply analyzing the network traffic and the pattern in which data packets are routed. By such attack an attacker can gain crucial information like basic structure of Smart grid, amount of energy usage, price etc.

V. DIFFICULTIES IN IMPLEMENTING SECURITY MEASURES

Security measures designed to deal the cyber attacks are not much efficient when used in grid networks. The three core objectives of a security mechanism are CIA (confidentiality, integrity and availability), but the security mechanism used in Smart Grid has few more objectives. They focus on safety of employees and users, the devices connected to the network and the transmission lines. They also focus on reliability, availability.

Thus, the Smart Grids need continuous profiling, testing and comparison to maintain security and performing traffic analysis. Moreover, the grids need to construct a self-healing ability for designing an improved framework for handing attacks.

There is a major difference between securing an IT network and securing a smart grid. IT networks focus on securing data repositories and network using well defined protocols; whereas when we talk about securing energy grids, the control is in hand of service providers. The protocols used in smart grids are defined by the vendors. Also, the Quality of Service (QoS) metrics are different for IT networks and Smart grids. Smart grids maintain the availability in presence of individual component failures and updates; whereas IT networks need to reboot the complete system. This variation raises a requirement to establish new solutions to security of Smart Grids.

VI. CONCLUSION

Conventional energy systems are now maturing to Smart grids with improved network designs, improved reliability, and reduced costs with better efficiency. Implementing security measures against Cyber attacks in the Smart Grid is now-a –days attracting the researchers, industrialists and Government agencies. In this paper, we introduced the framework of Smart grids, identified the core vulnerabilities, discussed the possible threats to smart grids and analyzed the difficulties in implementing security measures.

Smart grids have perilous architecture, thus, identification of all possible vulnerabilities is must to reduce the chances and effects of attacks.

References

[1] *"Federal Energy Regulatory Commission Assessment of Demand Response & Advanced Metering" (PDF). United States Federal Energy Regulatory Commission.*

[2] Ye, Y., and Qian, Y. 2012. "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges." *IEEE Communications Surveys and Tutorials* 15 (1): 5-20.

[3] Knapp, E. D. 2011. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.* New York: Elsevier Inc.

[4] Ye, Y., and Qian, Y. 2012. "A Survey on Smart Grid: A Communication Infrastructures: Motivations, Requirements and Challenges." *IEEE Communications Surveys and Tutorials* 15 (1): 5-20.

[5] Richter, A. 2012. "Transitioning from the Traditional to the Smart Grid: Lessons Learned from Closed Loop Supply Chains." In *Proceedings of the 2012 International Conference on Smart Grid* Technology*, Economics and Policies,* 1-7.

[6] Pepermans, G. 2005. "Distributed Generation: Definition, Benefits and Issues." *Energy Policy* 33 (6): 787-98.

[7] Bari, A. 2014. "Challenges in the Smart Grid Applications: An Overview." *International Journal of Distributed Server Networks* 2014 (1): 1-11.

[8] Ericsson, G. 2010. "Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure." *IEEE Transactions on Power Delivery* 25 (3): 1501-7.

[9] Knapp, E. D., and Samani, R. 2013. *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure.* New York: Elsevier Inc.

[10] McLaughlin, S. 2009. "Energy Theft in the Advanced Metering Infrastructure." *IEEE Journal on Selected Issues in Communications* 6027 (15): 176-87.

[11] Molazem, F. 2012. "Security and Privacy of Smart Meters: A Survey." In *Overview of Computer Security,* British Columbia: University of British Columbia.

[12] Cleveland, F. 2008. "Cyber Security Issues for Advanced Metering Infrastructure." In *Proceedings of the Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century,* 1-5.

[13] Mohhammad Zahran, "Smart Grid Technology, Vision Management and Control" WSEAS TRANSACTIONS on SYSTEMS, Volume 12, Issue 1, January 2013.

[14] S. M. Amin, B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," IEEE Power and Energy Mag., vol.3, no.5, pp. 34-41, Sept.-Oct. 2005.

[15] Litos Strategic Communication "The Smart Grid: An Introduction ," 31 May 2009 [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/DOE SG Book Single Pages.pdf

[16] S. Clements, H. Kirkham, "Cyber-security considerations for the smart grid," in IEEE Power and Energy Society General Meeting 2010, pp. 1-5, 2010.

[17] Pearson I. Smart grid cyber security for Europe. *Energy Policy*, 2011; 39(9):5211-5218.

[18] Flick T and Morehouse J. *Securing the Smart Grid: Next Generation Power Grid Security*. Syngress, 2010.

[19] Wang X and Yi P. Security framework for wireless communications in smart distribution grid. *IEEE Transactions on Smart Grid*, 2011; 2(4):809-818.