A Survey on Cyber Security for Smart Grid Networks

Yuvaraj S. Patil
Ph.D. student, Electronics, Engineering,
Department of Technology, Shivaji University,
Kolhapur, Maharashtra, India
yuvaraj.pat@gmail.com

Dr. Mrs. Swati V. Sankpal
Associate Professor, Department of Electronics Engineering,
D Y Patil College of Engineering and Technology,
Kolhapur, Maharashtra, India
sankpal16@yahoo.com

Abstract—Smart grid is a electrical grid in which power generation units, transmission units, distribution units and electricity consumers are connected using advanced communication and information technologies. It is a new form of next generation power grid. Most of the countries across the globe are transforming their existing electrical grids to smart grid and hence smart grid technology is progressing worldwide. Smart grid provides a bi-directional flow of electricity and information from generation to transmission to distribution and hence more exposed to attacks. Many advanced communication technologies have been identified for smart grid usages. A secure communication infrastructure is a critical component of smart grid systems. Success of smart grids highly depends on secure communication network. Thus cyber security of smart grid networks is very important. In this paper, we summarize the cyber security threats, possible vulnerabilities and existing standards and solutions available for cyber security in smart grids networks based on the available reference material.

Keywords- *Smart Grid, Communication Networks, Advanced Metering Infrastructure, Cyber Security, Reliability, Vulnerabilities*

*****

I. INTRODUCTION

Smart grid refers to advanced electrical grid which uses advanced communication and information infrastructures and provides more secure and reliable electrical energy.

The aim of converting the existing electrical grids into smart grids is to provide secure, stable, reliable and high-quality electricity in an environmentally friendly way. This is achieved through the use of existing and advanced technologies, integration of natural energy sources, demand-response management, monitoring and control [2]. The demand for electric energy is growing day by day due to increasing population [3] and hence there is strong need of smart grids to make optimal utilization of available energy sources.

In smart grid networks, intelligent devices like smart meters are installed at consumer facilities and these devices are monitored, controlled and optimized from a centralized control center. Such an infrastructure offers great benefits like increased reliability, efficiency, transparency, reduced cost [4] [5]. Smart grids uses bi-directional communication networks for transmission of energy and information and hence provides real-time information and achieves balance of demand and supply of electrical energy [5].

As smart grids heavily uses intelligent devices and communication infrastructure, the success of smart grids depends on dependability on such devices and secure communication infrastructure. Smart grid systems could lead to unreliable operations, instability, damage to infrastructure and devices if proper cyber security mechanism are not used [6] [7]. Hence cyber security for smart grid systems is becoming more important. As the smart grid systems are becoming more and more complex due to heavy usage of communication networks and information technology, these systems are becoming more vulnerable to cyber-attacks and cyber security is becoming a major concern [3].

As part of cyber security preventive measures, it needs to prevent unauthorized usage and access to communication networks and information contained therein, prevent damages to devices and infrastructure to ensure reliability, availability, data integrity and confidentiality. It also needs to restore the information and communication systems in case of equipment failure due to malfunctioning, user errors, attacks and natural disasters.

Secure smart grid systems helps consumers to manage their electricity usage efficiently. Smart grid systems will have a strong positive impact on economy and efficient utilization of natural resources. Hence cyber security for smart grid systems is of much importance because of the essential nature of electricity in day to day life.

II. SMART GRID CONCEPT AND ITS BENEFITS

Smart grid uses advanced technologies and equipments to control and monitor its information and components. It uses bi-directional communication to transfer information and data across all its layers. Due to usage of advanced sensors, smart devices and powerful computing capabilities, it provides the real-time information. As the real time information is available at the centralized control centers, it helps to balance the demand of electricity with supply. Energy from the various renewable energy resources like water, wind, solar energy is used to meet the increased demand of electricity. At the same time, end users of electricity will have real time data of their electricity usage and billing information. It will help the end user to better manage their electricity consumption and usage.

A. Conceptual Model of a Smart Grid

Smart grid heavily uses communication and information infrastructure across all the layers. Hence communication and information infrastructure plays an important role in smart grids.

Figure 1 provides a conceptual general model of a smart grid system [6] [10] [24]. The diagram is a simplified version of a complex smart grid system. It consists of various domains like generation, transmission, distribution and end customers.

Each domain owns a specific responsibility within the Smart Grid system. Domains are connected and controlled from a centralized control station. Due to heavy communication infrastructure and interconnections, cyber security of smart grid is very critical and is treated with high importance within each domain of a smart grid.

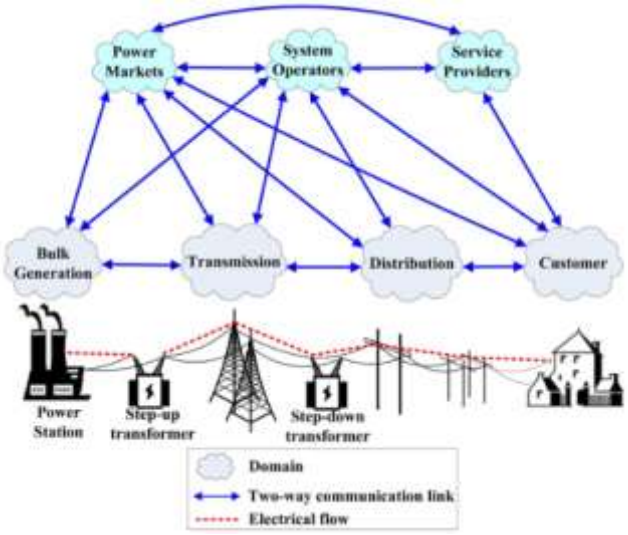

Figure 1. Smart grid conceptual model [10].

Smart grid replaces the existing equipment and devices with new advanced digital equipment and devices and deploys strategically across all the domains to increase reliability, efficiency and stability. Centralized control centers monitors and controls the smart grid domains and gets accurate, rea-time information of available energy and its usages. Hence it helps to maintain demand supply balance. Due to usage of advanced sensor, it can closely monitor and control generation units, transmission units, distribution units and end consumers. Due to usage of advanced computing applications and capabilities, it receives the real time information of electricity consumption. It analyzes the available information and performs decision-making and takes appropriate actions. It can get the customer electricity usage data from smart meters and get the pricing information from data centers and take a decision on billing rate based on electricity consumption patterns. When the demand of electricity increases, it supplies the energy from other available reusable resources and tries to maintain demand supply balance [9]. Hence it improves the smart grid reliability. As the smart grid domains are monitored and controlled from a centralized control station rather than operating independently, it provides more stability of the smart grid system. Secure communication infrastructure help to use the available electricity resources more effectively and efficiently and hence optimal usage of smart grid systems.

B. *Benefits of Smart Grid System*

Smart grid systems improves quality of service to end customers by minimizing electricity outage times. If the electricity supply needs to be interrupted due to some unavoidable circumstances, it tries to minimize the outage time. It provided advanced notifications with proper options to customers before service interruption so that customer can manage their electricity needs and optimize their electricity usage. It also helps to optimize the electricity usage during critical peak hours. It helps to avoid grid service quality degradation [5].

Most of the existing electricity generation plants emits lot of carbon di-oxide in the air and increases pollution. It creates critical impact on environment and human being [3]. As the demand of electricity is growing day by day, this concern is becoming more and more critical. Smart grid uses renewable energy resources like wind, solar, hydro energy and helps reducing environment pollution. Also it creates social awareness among its customers to reduce usage of electricity based on carbon fuel and promotes to use electricity based on natural renewable resources [5].

Smart grid technology provides lot of advantages like increased reliability, stability, efficiency, real time prices and less costs to end customers, help reducing environment pollutions. Due to increased benefits, most of the countries are migrating their existing grids to smart grid systems. Hence cyber security of smart systems needs to be handled with extreme care and attentions.

III. CYBER SECURITY REQUIREMENTS IN SMART GRIDS

It is a responsibility of each domain within smart grid system to deploy appropriate security measures to prevent malicious attacks or damage to the system resources.

As the smart grid domains are inter-connected using advanced communication infrastructure, it should also have high level of security mechanisms to meet the security requirements of the smart grid systems. Smart grid systems will become more reliable as more security measures gets added to smart grid systems. Hence higher degree of security mechanisms and security protocols needs to be deployed to smart grid networks to deal with increasing vulnerabilities and cyber threats. Due to heavy inter-networking within smart grid systems and due to usage of multiple appliances and smart devices from various manufacturers and suppliers, it becomes very challenging to deploy security mechanisms within smart grid systems. As the smart grid systems gets more and more interconnected, it is more exposed to cyber-attacks and vulnerabilities and hence cyber security of smart grid systems becomes very critical. Apart from preventing cyber-attacks, the cyber security mechanisms also need to deal with equipment malfunctioning and failures, human errors and natural disasters to preserve the infrastructure and information [7].

A. *Advanced Metering Infrastructure and Data Privacy*

Smart grid systems measures and monitors the ream time power consumption of the end consumer by using advanced metering infrastructure and smart meters. Smart details stores the electricity usage information of the consumer along with other necessary details. This information is transferred to centralized control stations using communication network. As the smart meter data is transferred over the communication networks and is critical, it must be protected to provide data privacy [7] [9] [28].

B. *Data Integrity*

Smart grid systems uses two-way communication networks to transmit electricity and information. Huge amount of information and data is transferred over the smart grid networks and the data is very important and critical as it contains sensitive information. Due to its critical nature, data integrity plays an important role in cyber security of smart grid systems. Unnecessary changes to data by unauthorized means must be prevented to achieve data integrity. If the data integrity

mechanisms are not powerful and defensive, then causes serious security and privacy issues and it may damage smart grid infrastructure and smart devices. Due to poor data integrity mechanisms, customer information, billing details, electricity usage can be compromised, the data may be heavily modified and it can cause serious security concerns. Hence data integrity is of much importance in smart grid systems [7] [11] [22].

C. *Authorization and Authentication*

Only authorized persons and systems with appropriate access permissions need to access various elements of smart grid systems. Authorization is a capability which distinguishes between authorized and unauthorized access. If authorization mechanisms are poor, it may causes serious safety concerns. Authentication is a capability which identifies the real identity of the use or system who is trying to access the system. Valid user account and access passwords are the most common methods used for authorization. Strong authorization and authentication policies needs to be deployed due to critical nature of smart grid systems [7] [24].

D. *Availability and Reliability*

Availability is a capability of the system which provides timely and reliable access to the use of information and data of the system. As the smart grid systems are of critical nature, it is very necessary to assure availability and reliability of smart grid systems. As the electricity is very important in day to day life and as most of the devices and activities are dependent on electricity, a small interruption in the electricity services may cause serious issues and major impacts both socially and financially. Hence reliability is one of the important factor while dealing with smart grid systems. All components of the system are important to the security design and reliability of the smart grid systems [6] [7] [21] [25] [29].

E. *Flexibility*

As smart grid systems are enhancing day by day and widely uses newly developed devices and software applications, security of smart grids systems cannot be planned and designed at initial stage and needs to be evolving over the time period. Smart grid systems needs be enough flexible to accommodate future technology enhancements. Hence complete cyber security in smart grid systems cannot be designed and implemented at one time and needs to be flexible and evolving over the time period. The existing security mechanisms needs to planed and designed in such a way that it will be enough flexible to accommodate future technology enhancements [24].

IV. Security threats and Challenges in Smart Grid

Vulnerability, threat detection and prevention is an essential part of a smart grid security planning phase. All the smart grid domains need to identify the different types of cyber and physical attacks they may undergo. They also need to determine the impact that such attacks could create to the system and take appropriate action to maintain system reliability, stability and safety [6] [18]. As a typical risk management process, it need to identify the threats; assess the risk and impact; take appropriate preventive action and monitor the system.

Types of cyber-attacks in smart grid systems are malware spreading, false data injection attack, load re-distribution attack in a power distribution systems, compromising communication network, anomalies in the power system control centers, attacks on smart meters, malicious modification of network data stored in a database [22] [26] [27].

Smart grid systems uses advanced information and communication technologies, adopts various standards and regulations. While designing and developing smart grid systems, cyber security aspect needs to be considered with much importance on the basis of available industry standards and regulations [7] [10]. Various devices and equipments from different manufacturers and suppliers are interconnected in smart grids using communication infrastructure. It is unsafe to assume that the devices and equipments used may have built-in security mechanisms. To protect smart grid systems across multiple domains, it needs to provide comprehensive, real time threat detection and solution.

It is not practical and feasible to establish a completely new network for smart grid systems and need to reuse the available communication infrastructures such as Internet. If a smart grid system is not equipped with appropriate security mechanisms, then it opens the grid to multiple attacks from various sources when connected to Internet [8]. Various levels of security mechanisms needs be built into the system to minimize the threats from various sources [29].

V. Standards and Current Solutions on Cyber Security for Smart Grids

This section lists the existing standards and solutions on cyber security for smart grid systems. There are various organizations working on the development of smart grid security standards. Some of the organizations are North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC-CIP), International Society of Automation (ISA), IEEE 1402, National Infrastructure Protection Plan (NIPP), and National Institute of Standards and Technology (NIST. While designing and developing smart grids, it is necessary to work with standards bodies, such as NIST and others, to ensure a highly secure, scalable, reliable smart grid systems, as these standards bodies will defines the security requirements of the smart grid systems [7] [22].

In [11], the authors have offered an efficient algorithm to find the attacks involving two smart meters. They have derived canonical forms and offered a solution for arbitrary unobservable attacks.

In [12], the authors have analyzed false data injection attacks. They have derived a module to demonstrate that unauthorized person can alter smart meter data by changing electricity usage reading. They have proposed a hybrid intrusion detection framework and grid sensor placement algorithm to detect malicious activities such as smart meter attacks. Grid sensors in this algorithm are considered fully trustworthy. The proposed design and algorithm is limited to a one player attack.

In [13], the authors have proposed an algorithm for anomaly detection. The simulated results have shown the effectiveness of the proposed method for anomaly detection. The proposed algorithm is intended to improve the cyber security of existing substation computer networks.

In [14], the authors have proposed an architecture for smart grid security assessment. The proposed architecture consists of

network data acquisition with advanced security functionalities, a security engine for online analysis of system security and a web based graphical user interface. The results shows that the proposed architecture is a very effective solution for performing run time security analysis of big electrical networks.

Authors have presented a very nice summary of various communication standards for smart grid networks in [15]. They have presented the details of latest communication technologies like 3G, GSM, GPRS, ZigBee, WiMAX with respect to smart grid usage and spectrum utilization. They also have presented a summary of various standards available for smart grid systems. For advanced metering infrastructure (AMI), standards like G3-PLC, MBus, PRIME, ANSI12.22/18/19 are proposed [25]. For home area networks (HAN), standards like Z-wave, U-SNAP and Homeplug are proposed. IEC62351 and IEC60870 are proposed for information system security and control center communication. IEC61969 and IEC61970 are proposed for transmission and distribution system energy management.

Authors of [16] have presented a new game theory model of interactions between centralized control station operator of a smart grid system and a cyber-attacker. This model is useful for estimating adverse interaction and subsequent analysis.

In [17], the authors have presented a security test bed to provide accurate cyber-physical environment for smart grid systems. The proposed PowerCyber test bed have capabilities like real time digital simulator (RTDS), WAN emulation and virtualization. The authors have simulated and evaluated various attack scenarios using the test bed to prove the effectiveness of the solution.

In [19], the authors have proposed a Markov games scalable solution for protecting smart grid infrastructure. The proposed solution is very useful for modeling the interactions between attacker and security defending mechanisms. They have proposed an algorithm which uses a threshold parameter to control solution accuracy and computation time.

In [20], the authors have introduced a framework for cyber-physical state estimation. The framework obtains measurements from various types of power system sensors at various time intervals to detect malicious activities within cyber-physical system. The authors have implemented and evaluated a working prototype using IEEE 24 bus bench marking system. The experimental results shows that proposed solution improves scalability of intrusion detection techniques.

In [21], the authors have presented a peer-to-peer communication protection system to improve reliability and security of smart grid systems. The results obtained from simulation shows that system is capable of detecting cyber-attacks and overcomes denial of service attacks.

Authors of [23] have implemented and tested a mechanism for anomaly detection using experimental test bed. The demonstration results shows that the system performs accurate anomaly detection. It also demonstrates that a domain knowledge can dramatically improve anomaly detection performance by adjusting threshold of sensitivity.

Based on the above summary, it is clear that the smart grid security solutions need to evolve further to address newer security challenges and to provide stable, safer and reliable operations of smart grid systems. It is important to note that the currently available security solutions and approaches are insufficient and needs to be replaced by new advanced techniques to ensure the security of complex and dynamic smart grid environment [22].

VI. CONCLUSION

In this paper, we reviewed and discussed the cyber security issues for smart grid communication networks and the existing standards and solutions. Smart grid communication network is a critical component and it needs to be designed and implemented properly to high reliability, stability and efficiency of smart grid systems.

There is no single device or mechanism that can provide all the necessary security measures required for cyber security of a smart grid system. An enterprise undertaking a smart grid project need to work closely with manufacturers, vendors and regulatory authorities to ensure that the chosen solution can evolve to meet the security requirements of a smart grid system. Building a secure smart grid system is a complex task which requires a collective efforts from all the entities involved. Cyber security is a growing concern and is very important and critical for a successful deployment of a smart grid system.

REFERENCES

[1] Enrique Santacana, Gary Rackliffe, Le Tang and Xiaoming Feng "Getting Smart - With a Clearer Vision of the Intelligent Grid, Control Emerfrom Chaos," IEEE power and energy magazine, pp. 41-48, Mar/Apr2010.

[2] S. Massoud Amin and Bruce F. Wollenberg, "Towards a Smart Grid, IEEE power and energy magazine, pp. 34-41, Sep/Oct. 2005.

[3] Thomas G. Garrity, "Getting Smart - Innovation and Trends for Future Electric Power System," IEEE power and energy magazine, pp. 38-45, Mar/Apr. 2008.

[4] Khosrow Moslehi and Ranjit Kumar, "A Reliability Perspective of Smart Grid," IEEE trans. Smart Grid, Vol. 1, no. 1, pp. 57-64, Jun. 2010.

[5] Ye Yan, Yi Qian, Hamid Sharif and David Tipper, "A Survey Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," IEEE Communications Surveys and Tutorials, Vol. no. 1, pp. 998-1010, First Quarter 2013.

[6] Goran N. Ericsson, "Cyber Security and Power System Communication - Essential parts of a Smart Grid Infrastructure," IEEE trans. Power Delivery, Vol. 25, no. 3, pp. 1501-1507, Jul. 2010.

[7] Ye Yan, Yi Qian, Hamid Sharif and David Tipper, "A Survey Cyber Security for Smart Grid Communications," IEEE Communications Surveys and Tutorials, Vol. 14, no. 4, pp. 998-1010, Fourth Quarter 2012.

[8] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in Smart Grid," IEEE Security and Privacy, Vol. 7, no. 4, pp. 75- 77, 2009.

[9] Jing Liu, Yang Xiao, Shuhui Li, Wei Liang and C. L. Philip Chen, "Cyber Security and Privacy Issues in Smart Grids," IEEE Communications Surveys and Tutorials, Vol. 14, no. 4, pp. 998-1010, Fourth Quarter 2012.

[10] Ruofei Ma, Hsiao Hwa Chen, Yu Ren Huang and Weixiao Meng "Smart Grid Communication: Its Challenges and Opportunities," IEEE trSmart Grid, Vol. 4, no. 1, pp. 36-46, Mar. 2013.

[11] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and Poolla "Smart Grid Data Integrity Attacks," IEEE trans. Smart Grid, 4, no. 3, pp. 1244-1253, Sep. 2013.

[12] C. H. Lo and N. Ansari, "CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid," IEEE tr. Emerging Topics in Computing, Vol. 1, no. 1, pp. 33-44, Jun. 2013.

[13] C. W. Ten and C. H. Lu, "Anomaly Detection for Cybersecurity of the Substations," IEEE trans. Smart Grid, Vol. 2, no. 4, pp. 865-873, Dec. 2011.

[14] Michele Di. Santo, Alfredo Vaccaro, Domenico Villacci and Eugenio Zimeo "A Distributed Architecture for Online Power Systems Security Analysis ," IEEE trans.on Industrial Electronics, Vol. 51, no. 6, pp. 12381248, Dec. 2004.

[15] V. C. Gungor, D. Sahin, T. Kocak, S, Ergut, C. Buccella, C. Cecati and G. H. Hancke "Smart Grid Technologies: Communication Technologies and Standards," IEEE trans.on Industrial Informatics, Vol. 7, no. 4, pp. 529-539, Nov. 2011.

[16] Scott Backhaus, Russell Bent, James Bono, Ritchie Lee, Brendan Tracey, David Wolpert, Dongping Xie, and Yildiray Yildiz "Cyber-Physical Security: A Game Theory Model of Humans Interacting Over Control Systems," IEEE trans.on Smart Grid, Vol. 4, no. 4, pp. 2320-2327, Dec. 2013.

[17] Adam Hahn, Aditya Ashok, Siddharth Sridhar and Manimaran Govindarasu "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," IEEE trans.on Smart Grid, Vol. 4, no. 2, pp. 847-855, Jun. 2013.

[18] Stan Pietrowicz and Tom Mazzone "The Growing Need for Cyber Security in Smart Grid Networks," Grid-Interop Forum, 2011.

[19] Chris Y. T. Ma, DavidK.Y.Yauand NageswaraS.V. Rao "Scalable Solutions of Markov Games for Smart-Grid Infrastructure protection," IEEE trans.on Smart Grid, Vol. 4, no. 1, pp. 47-55, Mar. 2013.

[20] Saman Zonouz, Katherine M. Rogers, Robin Berthier, Rakesh B. Bobba,William H. Sanders, and Thomas J. Overbye "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures," IEEE trans.on Smart Grid, Vol. 3, no. 4, pp. 1790-1799, Dec. 2012.

[21] Keith J. Ross, Kenneth Mark Hopkinson and Meir Pachter "Using a Distributed Agent-Based Communication Enabled Special Protection System to Enhance Smart Grid Security," IEEE trans.on Smart Grid, Vol. 4, no. 2, pp. 1216-1224, Jun. 2013.

[22] A. Anwar and A. Mahmood "Cyber Security of Smart Grid Infrastructure," CRC Press, Taylor and Francis Group, USA, Vol. 4, no. 2, pp. 449-472, Jan. 2014.

[23] Ondrej Linda, Milos Manic and Todd Vollmer "Improving CyberSecurity of Smart Grid Systems Via Anomaly Detection and Linguistic Domain Knowledge," 5th International Symposium on Resilient Control Systems, Aug. 2012.

[24] "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," The Smart Grid Interoperability Panel Cyber Security Working Group , Sep. 2010.

[25] Lee-Cheun Hau, Jer-Vui Lee, Yea-Dat Chuah and An-Chow Lai "Smart Grid The Present and Future of Smart Physical Protection: A Review, International Journal of Energy, Information and Communications," Vol.4, no. 4, pp. 43-54, Aug. 2013.

[26] Byron Flynn "Smart Grid Security," Cyber Security for Process Control Systems Summer School, Jun. 2008.

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

[28] S. Zeadally, A. Pathan, C. Alcaraz, and M. Badra "Towards Privacy Protection in Smart Grid ," In Wireless Personal Communications, pp. 1-28, Sep. 2012.

[29] Wenye Wang and Zhuo Lu "Cyber security in the Smart Grid: Survey and challenges," Computer Networks 57 , pp. 1344-1371, 2013.