Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2019, 6(8):146-152**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Cybersecurity in Smart Grid

Matthew N. O. Sadiku, Yogita P. Akhare, Sarhan M. Musa

Roy G. Perry College of Engineering, Prairie View A&M University
Email: sadiku@ieee.org; yakhare@student.pvamu.edu; smmusa @pvamu.edu

Abstract Electricity is the core element that connects and affects how we live and work. In the modern society, our security, health, and vitality depend on the uninterrupted supply of electricity to homes, businesses, and public spaces. The electric power system is the most capital-intensive infrastructure in North America. Cybersecurity is an emerging challenge for the smart power grid. Cybersecurity threats to the smart grid can be expected to challenge the industry for many decades. This paper provides a brief overview on cybersecurity of the smart power grid.

Keywords cybersecurity, smart grid

Introduction

Electricity is integral to modern life. It is vital to the commerce and daily functioning of individuals. The electric power grid consists of generating plants together with the transmission and distribution systems that bring power to end-use customers. The US power grid consists of over 200,000 miles of high-voltage transmission lines and hundreds of large transformer substations. The various components of the system are all vulnerable to failure due to natural, operational, or manmade events [1].

The ongoing modernization of the electric power grid is commonly referred to as the smart grid. Like any new technology, the smart grid introduces new concerns about security. The challenge lies in the fact that the smart grid as well other critical national infrastructure (consisting of 16 infrastructure sectors) were not built with security in mind. It is well known that electric power grids are a major target for foreign actors, with the possibility of seriously disrupting businesses and causing widespread public fear. Unfortunately, it is impossible to secure the whole grid from terrorist attacks.

The nation's security, economic prosperity, and the well-being of our citizens depend on reliable and secure energy infrastructure. The electric distribution systems have always been regulated by state and local governments. Congress gave the Federal Energy Regulatory Commission (FERC) authority to oversee the reliability of the electric power system. The NERC Critical Infrastructure Protection (CIP) standards were introduced to ensure the reliability of the nation's electric system. For every nation, government and private industry work together to protect critical infrastructure.

Smart Grid Architecture

The term "grid" is traditionally used for electricity generation, electricity transmission, electricity distribution, and electricity control. A "smart grid" is an enhancement of the traditional electric power grid. It is an electric network that can efficiently integrate the behavior and actions of all users connected to it. It is the modernization of the power delivery system. It is a transformation of the legacy unidirectional electric grid into automatic intelligent system of bidirectional exchange of electric power and information. A smart grid may be defined as any combination of enabling technologies, hardware, software, or practices that collectively make the delivery infrastructure (or the grid) more reliable, more versatile, more secure, more accommodating, more

resilient, and ultimately more useful to consumers [2]. A smart grid basically consists of overlaying the physical power system with the information system.

According to the National Institute of Standard and Technology (NIST), a smart grid consists of seven logical domains: bulk generation, transmission, distribution, customer, markets, service provider, and operations. A conceptual model of the smart grid is shown in Figure 1 [3]. From the technical point of view, the smart grid can be divided into three major systems [4]:

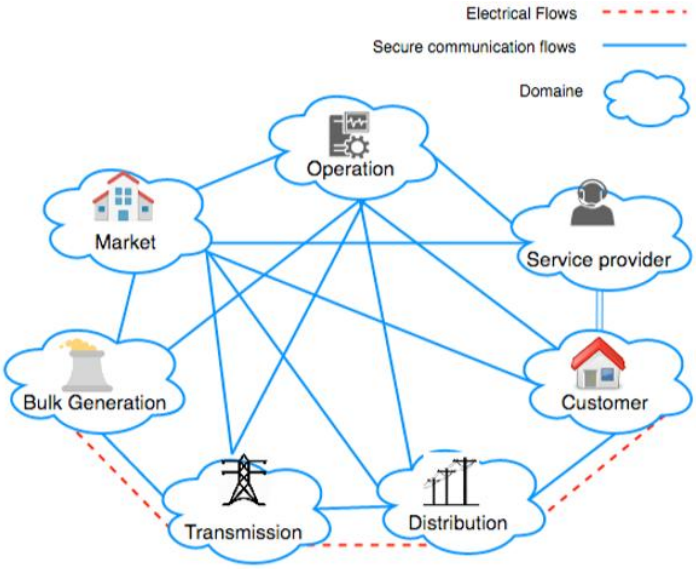

Figure 1: A conceptual model of the smart grid based on NIST [3]

- *Smart infrastructure system:* This is the energy, information, and communication infrastructure underlying the smart grid. This allows two-way flow of electricity and information. This implies that the users may put back electricity into the grid. The system enables multiple entities (such as intelligent devices, dedicated software, control center, etc.) to interact.
- *Smart management system:* This provides advanced management and control services. Efficient management is fundamental for efficient operation of smart grids. Management of smart grid includes the development and implementation of smart metering, real time pricing, efficient management of renewable energy sources, and management of transmission and distribution networks.
- *Smart protection system:* This provides advanced reliability analysis, fault protection, and security services. The existing infrastructure has become vulnerable to several security threats.

The smart grid is made possible by applying sensors, smart meters, and field automated devices to the electrical power grid. The grid can predict, adapt, and reconfigure itself reliably and efficiently. It will be able to handle uncertainties in schedules, power transfer across regions, managing and resolving unpredictable events, and meeting the demand for reliable supply [5]. Smart grid may also be regarded as a combination of several micro grids. Each micro grid operates autonomously within its system supervisory control and data acquisition (SCADA) system.

SCADA is a control system for smooth managing large-scale, automated industrial operations. When applied to electric power industry, it can help the industry to save time and money, reduce operational costs, and improve efficiency. It provides real-time monitoring and automation for smart power grid. SCADA is now used extensively in the electricity sector and integrated with external systems. It is the controlling system as well as the communication network in smart grid [6]. The Department of Energy (DOE) lists the following benefits of the smart grid technologies include [7]:

- More efficient transmission of electricity
- Quicker restoration of electricity after power disturbances
- Reduced operations and management costs for utilities, and ultimately lower power costs for consumers

- Reduced peak demand, which will also help lower electricity rates
- Increased integration of large-scale renewable energy systems
- Better integration of customer-owner power generation systems, including renewable energy systems
- Improved security

Some of those benefits are depicted in Figure 2 [8].

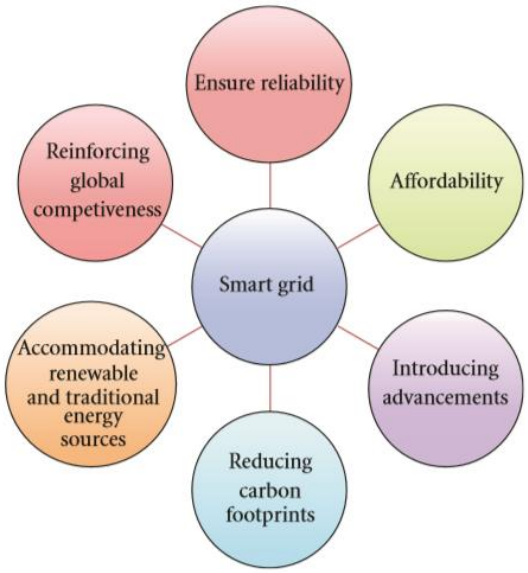

Figure 2: Some of those benefits of the smart grid [8]

Overview of Cybersecurity

Cybersecurity is the process of protecting computer networks from cyber attacks or unintended unauthorized access. Cybersecurity takes different forms including military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, and information systems. The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity.

Cyber-attacks are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). Cyber-attacks or threats include malware, phishing, denial-of-service attacks, social engineering attacks, and man-in-the-middle attack. Cybersecurity involves reducing the risk of cyber-attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available. A typical cyber-attack on a local area network is shown in Figure 3 [9].

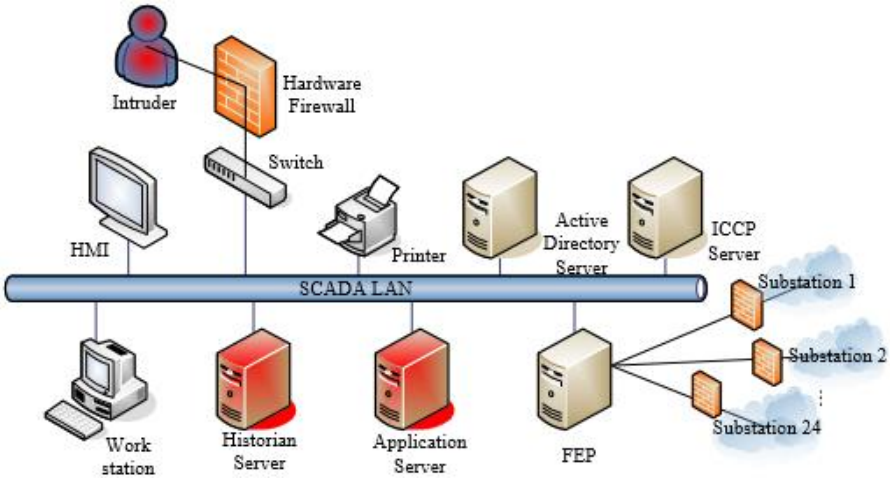

Figure 3: Cyber attack on a local area network [9]

Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the Department of Homeland Security (DHS). The DHS has a dedicated division responsible for risk management program and requirements for cybersecurity called the National Cyber Security Division. The Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical computer networks and networked infrastructure. The Computer Fraud and Abuse Act (CFAA) remains the most relevant applicable law expressing the U.S. proactive cybersecurity effort [10].

Cybersecurity of the power grid encompasses attack prevention, detection, mitigation, and resilience. Following are series of goals for good cybersecurity operations on smart grid [11]:

- Be able to operate in an environment where cyber-attacks occur.
- Reduce an attackers' access to our systems
- Seek proper treatment. Computer systems get exposed to germs, viruses, and other attacks
- Provide cyber defense in depth, so there are coordinated layers of protection
- Use continuous monitoring and compliance with cybersecurity best practices
- Develop systems so that cybersecurity is more like storms and hurricanes where we can track and predict consequences.

.

Attacks of Smart Grıd

The energy infrastructure or the power grid has become a major target with attacks from nation-states and cyber criminals. Hackers can manipulate SCADA systems to disrupt the flow of electricity, transmit erroneous messages to operators, or block vital information flow. The 2015 Ukraine cyberattack, and blackouts demonstrated that a power grid could be rendered inoperable. Hackers targeted portions of Ukraine's energy grid with a denial of service attack. They disrupted power by gaining access through SCADA software. That cyberattack in Ukraine could be a turning point in the security battle. Cyberattacks on electric power grids are becoming a common headline. Cyber threats to the smart grid can come from attacks directed via Internet of Things (IoT) devices. The threats have become so pervasive that every connected device needs to have a cybersecurity strategy.

Cyber-attacks and threats can come from direct attacks aimed at electric grid. Some recent foreign hackers targeting the US electric power include the following [12]:

- Cyber intrusions on the SCADA systems of the Bowman Dam in Rye, New York resulted in federal indictments against a group of hackers linked to Iran.
- Black out in US three cities in April 2017: A series of power outages in Los Angeles, San Francisco, and New York City left commuters stranded.
- Cyber intrusions in October 2017 attributed to North Korea.[5] were reported to have targeted electric company networks.
- In March 2018, the US Computer Emergency Readiness Team (US-CERT) issued an alert concerning cyber intrusions attributed Russian government hackers at critical energy and manufacturing infrastructure companies.

The National Cybersecurity and Communications Integration Center (NCCIC) is largely responsible for informing the utility industry of cyber and physical threats.

Improvıng Grıd Cybersecurıty

In the US, a lot of effort is being made by the power industry and the US government to protect the power grid from cyberattacks.

- *Power Industry:* Although the national security responsibilities are assigned to Department of Energy, an electric utility industry is mainly responsible for implementing cybersecurity measures. The industry takes this responsibility very seriously. It is advancing cybersecurity with several initiatives. In the US, utility companies are spending billions of dollars a year on grid cybersecurity.

- *US Government*: Cybersecurity has been a concern of the US government in recent years, budgeting billions for cybersecurity. Congressional interest on cybersecurity has been growing after it was reported that Iran has stepped up its cyberattacks against US critical infrastructure. In February 2016, President Obama presented his Cybersecurity National Action Plan to safeguard against malicious cyber activity. President Trump is not afraid to deploy cyber tools in a very aggressive manner. In 2017, he issued an executive order to protect critical infrastructure from cyberattacks, designating the Department of Homeland Security (DHS) as the lead agency in the action. Some states such as New Jersey, Texas, and Pennsylvania: have cybersecurity procedures and practices. The Idaho National Laboratory contains one of the United States' primary cybersecurity facilities that use the existing power grid for experiments.

The major objectives of smart grid security is to comply with policies while securing information using Confidentiality, Integrity and Availability, as known in Figure 4 [13].

Artificial Intelligence (AI) algorithm can be deployed to mitigate cybersecurity risks.

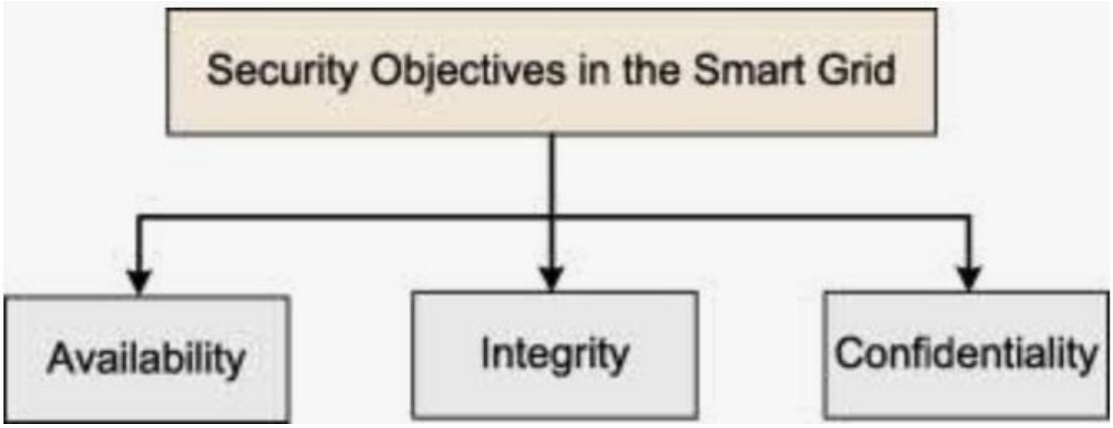

Figure 4: Securing information using Confidentiality, Integrity and Availability [13]

Benefits and Challenges

Two-way communication among generators, transmitters, and customers is the main feature of the smart grid. This feature offers solid benefits such as energy management, increased reliability and resilience, and integration of intermittent renewable energy generation and storage [14]. Smart grid can wisely meet the environmental requirements by facilitating the integration of green technologies.

One challenge utility industry faces is the cost of taking cybersecurity measures. Although public conversations have increased public awareness of the risks to the smart grid, the thinking of most people has not changed much. The human factor is the weakest link in cybersecurity since several cybersecurity breaches are caused by individuals.

Defending against cyber-attacks on SCADA systems is challenging due to the wide range of attack mechanisms, the decentralized nature of the control, deregulation, and the lack of coordination among various entities in the electric grid. The current evaluation techniques used in IT systems are inadequate for SCADA environments.

Reporting cybersecurity incidents should be standardized to allow for ease of comparison of reports. One prevention approach is to maintain up-to-date firmware on all security devices, but the burden this places on end users is unsustainable without some form of automation. Quantitative assessment and the impact analysis of the cyber-attacks and defense on the smart grid are needed in cybersecurity evaluation. Assessing cybersecurity risk is especially important for new manufacturers, vendors, and service providers.

Conclusıon

The energy sector (electricity, natural gas, and petroleum) is one of 16 critical infrastructure sectors designated by the Department of Homeland Security. Our modern society depends on critical infrastructure sectors, especially the energy sector. The US power grid has long been considered a logical target for a major

cyberattack. Cybersecurity is vital to protect critical infrastructure including the smart power grid. It will continue to be a major concern and focus area for the electric power sector.

Although cyberattacks by terrorist and criminals cannot be ruled out, carrying out a cyberattack that successfully disrupts power grid operations is very difficult. Cyber threats to power utilities will likely to grow in number. Attack resiliency should be the key attribute of the next generation electric grid. Utility industry needs to adopt cybersecurity best practices and invest in adequate cybersecurity preparedness. More information on cybersecurity for smart grid can be found in the books in [15-17].

References

[1]. P. W. Parfomak, "Physical security of the U.S. power grid: high-voltage transformer substations," *Current Politics and Economics*, vol. 19, no. 2, 2015.

[2]. F. P. Sioshansi (ed.), *Smart Grid: Integrating Renewable, Distributed, and Efficient Energy*. Oxford, UK: Academic Press, 2012, pp. xxix, xxx, 393.

[3]. Z. Elmrabet et al., "Cyber-security in smart grid: Survey and challenges," https://arxiv.org/ftp/arxiv/papers/1809/1809.02609.pdf

[4]. X. Fang et al, "Smart grid – The new and improved power grid: A survey," *IEEE Communications Survey and Tutorials*, vol. 14, no. 4, Fourth Quarter, 2012, pp. 944-980.

[5]. M.N.O. Sadiku, S.M. Musa, and S. R. Nelatury, "Smart grid – An introduction," *International Journal of Electrical Engineering & Technology*, vol. 7, no.1, Jan-Feb, 2016, pp. 45-49.

[6]. M. N. O. Sadiku, Y. Wang, S. Cui, S. M. Musa, "SCADA in power systems," *International Journal of Software & Hardware Research in Engineering*, vol. 6, no. 2, February 2018, pp. 23-27.

[7]. C. Anderson, "How cybersecurity regulation for the smart grid could upset the current balance of federal and state jurisdiction in electricity regulation," American *University National Security Law Brief*, vol. 8, no. 1, 2018.

[8]. S. Iyer, "Cyber security for smart grid, cryptography, and privacy," *International Journal of Digital Multimedia Broadcasting*, 2011.

[9]. Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," Doctoral *Dissertation*, University of Toledo, 2015.

[10]. M. N. O. Sadiku, S. Alam, S. M. Musa, C. M. Akujuobi," A Primer on Cybersecurity," International *Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[11]. C. W. Draffin, "Cybersecurity white paper," https://energy.mit.edu/wp-content/uploads/2016/12/CybersecurityWhitePaper_MITUtilityofFuture_-2016-12-05_Draffin.pdf

[12]. "Electric grid cybersecurity," September 2018, https://www.everycrsreport.com/reports/R45312.html

[13]. *W. Wang* and *Z. Lu*, "Cyber security in the smart grid: Survey and challenges," Computer Networks, vol. 57, no. 5, April 2013, pp. 1344-1371.

[14]. K. Maize," The dark side of the smart grid," May 2019, https://www.powermag.com/the-dark-side-of-the-smart-grid/

[15]. E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Waltham, MA: Elsevier, 2013.

[16]. I. E. Reid and, H. A. Stevens (eds.), Smart Meters and the Smart Grid: Privacy and Cybersecurity Considerations. Nova Science Pub., 2012.

[17]. P. Barker and R. F. Price (eds.), *Cybersecurity for the Electric Smart Grid: Elements and Considerations*. Nova, 2012.

Authors

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interests include computational electromagnetics and computer networks. He is a fellow of IEEE.

Yogita P. Akhare is a doctoral student at Prairie View A&M University, Prairie View, Texas. Her research interests include machine drives and nanotechnology.
Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Sprint and Boeing Welliver Fellow.