INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Cyber Security in Smart Grid

Praveen Kumar Mishra[1], Prabhakar Tiwari[2],
[1]PG Scholar, Electrical Engineering Department, Madan Mohan Malaviya University of technology Gorakhpur, Uttar Pradesh, India.
[2]Associate Professor, Electrical Engineering Department, Madan Mohan Malaviya University of technology Gorakhpur, Uttar Pradesh, India.
praveen.mishra590@gmail.com[1]

Abstract

The smart grid harnesses the power of information technology to provide energy intelligently using two-way communication and wisely meets environmental requirements by facilitating the integration of green technologies. The intelligent network is a system based on communication and information technology in the generation, delivery and consumption of energy. It uses the bi-directional flow of information to create an automated and widely distributed system that has new features such as real-time control, operational efficiency, network resilience and better integration of renewable technology that will reduce the carbon footprint. Any interruptions in power generation could disrupt the stability of the smart grid and could potentially have major socio-economic impacts. These survey documents provide various classifications of smart grid attacks, most of which are based on confidentiality, integrity or availability. We examine cyber security goals in the smart network and describe a new classification of cyber attacks based on a method used by hackers or penetration testers. This document provides an overview of the current state and future directions of cyber security of the intelligent network. The main contribution of this review is to provide a complete overview of resilience in power systems: definitions, frameworks, metrics and practices.

Keywords *;**cyber attacks, network security, confidentiality, security protocol***

1. Introduction

The smart grid is a system made up of distributed and heterogeneous components to provide electricity in an intelligent way and meet environmental requirements through the integration of renewable technologies. The National Institute of Standards and Technology (NIST) described the smart grid as integrating the electricity grid of the last century with the current development of the century in information and communication technologies (LCT)[1].

Smart Grid offers new functions for the collection, communication and exchange of data relating to energy consumption and these technologies in turn generate privacy problems. With the implementation of Smart Grid, the importance of information technology (IT) and telecommunication infrastructures has been increased to ensure the reliability and security of the electricity sector. Cyber security must address not only deliberate attacks launched by disgruntled employees, industrial espionage agents and terrorists, but also involuntary commitments to the information infrastructure due to user errors, equipment failures and natural disasters [2].

The Smart Grid can be defined as an update to the existing power grid infrastructure, which is becoming more sustainable, more economical,

more efficient and more reliable and contains information and communication technologies to enable mutual communication between all components. One of the possible approaches for improving the resilience in an energy system is the integration of microgrids in the energy system.[3] The electricity industry faces major challenges in integrating renewable energies into the existing network for the transmission of mass energy, namely protection, security of supply, fulfilment of base load requirements, etc. MG, which is integrated in intelligent sensors and managed by intelligent energy management systems (EMS), can medium to low voltage levels can be efficiently integrated into the existing distribution network in order to maintain efficient, reliable and economical operation. The documents in this area are rich in information from the Department of Energy, the International Standards Organization (ISO), and the NERC, the NIST, the Software Engineering Institute (SEI) and the SANS Institute. Some serve as a framework. At least one is a regulatory standard for processes and documentation (ISO 27001)[4].

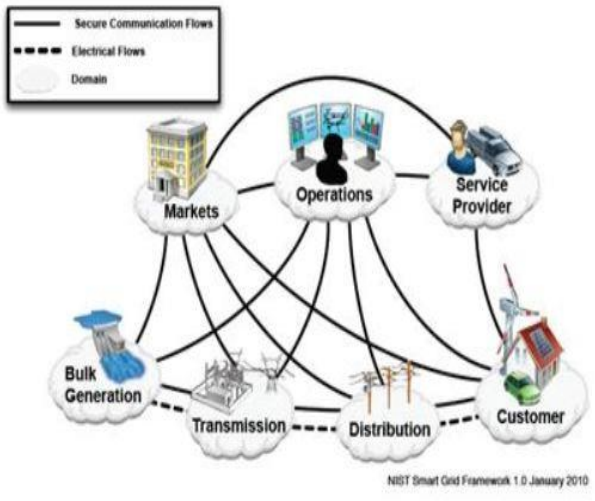

Figure 1: Information and electricity flow across a smart grid system (NISTIR 7628 Guidelines)

1.1 Smart grid's features

The main advantages envisaged by the smart grid are the increased network resilience and improved environmental performance. Resilience indicates the ability of a given entity to withstand unexpected events and to recover quickly thereafter. The concepts of smart grids have been around for many years, starting with measurement. Companies have long sought to reduce the cost of reading traditional meters, with humans reaching the meter and recording usage readings. The smart grid promises to provide flexibility and reliability, allowing additional energy expenditures, facilitating the integration of new resources into the grid and allowing corrective resources in the event of failures. "Cybersecurity and communication of power systems: essential parts of an intelligent grid infrastructure" warns: "The fact that SCADA / EMS [supervising and acquiring data / power management] systems are interconnected and integrated with external systems creates new possibilities and threats"[5] The purpose of a risk management program is to identify risks, understand their likelihood and impact on the company, and then implement security controls that mitigate risks. In addition to assessment and mitigation, a robust risk management program includes continuous assessment and assessment of cyber security risks and controls throughout the entire life cycle of smart grid component software "[6]. The smart grid harnesses the power of information technology to provide energy intelligently using bidirectional communication and wisely meets environmental requirements, facilitating the integration of green technology [7].

1.2 Security Requirements and Objectives

The smart grid is made up of a large number of interconnected devices. There are two types of data that are exchanged through the smart grid: information data and operational data. Perhaps information on energy bills, trends, registration, labelling, geographic location of historical reports, consumer information and emails. The operational data can be real-time current and voltage values, transformer tap-changers, and capacitor banks, current loads from the transformer power supplies, fault positions, relay status, and switch status [8]. Operational data requires a high level of security to protect smart grid systems from any vulnerabilities and attacks that could cause a power outage. The main objective of smart grids is that they are robust to continue operating or remain standing in the face of a disaster and withstand low probability, but high consequences. The second is the ingenuity that effectively manages a disaster as it develops, identifying options, prioritizing what should be to control and mitigate the damage. Fourth the adaptability to absorb new lessons from a catastrophe that introduces new tools and technologies to increase robustness, resourcefulness and recovery before the next crisis [9].

2. The Interconnected Smart Grid

A smart grid uses innovative products and services, along with smart technologies for monitoring, control, communication and self-regeneration [10]. A Smart Grid is an electric grid that can efficiently integrate the behaviour and actions of all users connected to it - generators, consumers and those who do both - in order to guarantee economically efficient and sustainable energy systems with low losses and high levels of quality and security of supply and security [8]. Since then, network cyber security has become one of the main points on the government and industrial agenda, with the recognition that the more interconnected the network becomes, the greater the attack surface. The level of communication is the backbone of the Smart Grid and is vulnerable to cyber attacks. In the past, concessionaires carried out communication operations on their networks [11].

2.1 New Approaches to Grid Security

Conventional approaches to network protection, involving hardware firewalls, encryption levels and multiple authentications, have dominated the response to security deficiencies. But there may be new and better ways to approach the topic. The biggest security threat today. Most innovations focus on attack research and management. India plans to implement a smart grid across the country by 2027 in three five-year phases [12]. As part of the National Smart Grid Mission (NSGM), India plans to invest more than INR 314 billion from 2012 to 2017, with 14 pilot projects dealing with various Smart Grid technologies. The implementation of Smart Grid in India is controlled by the India Smart Grid Forum (ISGF) and the India Smart Grid Task Force (ISGTF). With mechanisms for better integration of variable sources of renewable energy, such as wind and solar, the implementation of Smart Grid allows countries to increase the percentage of energy produced by these sources and, consequently, reduce their dependence on sources of energy. Conventional hydrocarbon and nuclear power [13].

3. Methods of cyber fortification of substations

a. Router level security: When data is transferred, a router reads the address information in the packet to determine the ultimate destination. The access control list (ACL) is a fundamental component of router administration. ACLs should be defined in routers between different communication interfaces in the substation automation network to enforce cyber security

Fig.2.security mechanism

.

b.Firewall level security: Some routers also act as firewalls and help in creating secure cells of network. A firewall enforces an access control policy between two networks. Transparent firewalls can be used to add security to a network. Firewalls can create alerts during attacks or failures by logging, administering, and auditing network access. Secure control functions include inspection, content inspection, access control, user control, protocol and services control, and data control for secure substation automation networking [14].

c.Gateway level security: Gateways must be used to achieve cyber security against a variety of cyber attacks when the substation network is connected to a wide area network (WAN) or remotely accessed. A gateway collects metering, status, event, and fault report data from IEDs and RTUs.It can be achieved by virtual private network (VPN) and encryption.

d.Virtual private network (VPN): A VPN is used to establish an encrypted, secure connection between two points across an insecure network. IP packets are encrypted and encapsulated prior to being sent. This is known as tunnelling.

4. Ongoing cyber challenges faced by the U.S.

Various entities such as NERC, NIST, FERC, DHS, and the DoE have made security of the electricity grid a primary focus. However, various gaps still exist and will require concentrated efforts: Four major issues need to be addressed for effective deployment of Smart Grids [15].

1. Security threats.

2. Privacy issues
3. High expenses
4. High tariffs.

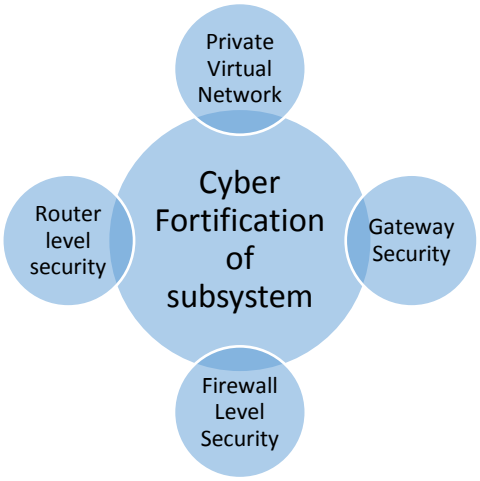

Fig 3. Methods of cyber fortification of substations

Fig.4 cyber security challenges faced by government

4.2 according to grid modernization initiative, modern grid should have –

1) Greater resilience to hazards of all types.
2) Improved reliability for everyday operations.
3) Enhanced security from an increasing and evolving number of threats.
4) Additional affordability to maintain our economic prosperity.
5) Superior flexibility to responds to the variability and uncertainty of conditions at one or more timescales, including a range of energy futures.
6) Increased sustainability through energy efficient and renewable resources[16].

Conclusions

A modern grid is vital to the country's existing and future security, economy and lifestyle will provide the foundation for essential services that people rely on every day. The smart grid technology markets in India are growing. The market segment is strongly encouraged by the federal government, which provides billions of resources for research and development. This integrated network will be more reliable to prevent or reduce energy shortages and provide people and businesses with access to the latest consumer technologies to manage their energy consumption. Researchers are now experimenting with smart grid technologies to overcome the deficiency of the traditional grid, which is based on one way, the utilities of the consumer system and is transformed into an interconnected national system, which allows for a massive transfer of electricity between regions in the India.

Results

Cyber security of the smart grid is a major challenge, but it is essential to the success of the smart grid applications. A high level of IT security can be achieved by combining the results of this research with a process that includes security as a key design parameter for a smart grid system, a process for maintaining security throughout the life of the system. Protecting our infrastructure, smart grid and IoT environments requires all the needs of industry participants to manage risk in components, subsystems and systems. The smart grid can be seen as a network that allows the two-way flow of data and power between its various elements. it is self-healing. It can distinguish, analyze, and respond to commotion. Smart grid technologies allow electricity grid operations to become more efficient, reducing the losses in the conventional grid. The quality of the supplied power is also higher and more consistent.

References

Journals

[1] Z. Mrabet, N. Kaabouch, H. Ghazi and H. Ghazi, "Cyber-security in smart grid: Survey and challenges", Computers & Electrical Engineering, vol. 67, pp. 469-482, 2018. Available: 10.1016/j.compeleceng.2018.01.015.

[2] NIST, Introduction to NISTTR 7628 Guidelines for Smart Grid Cyber Security. [Online]. Available: http://www.nist.gov/smartgrid/upload/ nistir-7628 _total.pdf

[3] G. Strbac, N. Hatziargyriou, J. P. Lopes, C. Moreira, A. Dimeas, and D. Papadaskalopoulos, "Microgrids: Enhancing the resilience of the European megagrid," IEEE Power Energy Mag. 13(3), 35–43 (2015).

[4] G. Huang, J. Wang, C. Chen, J. Qi, and C. Guo, "Integration of preventive and emergency responses for power grid resilience enhancement," IEEE Trans. Power Syst. 32(6), 4451–4463 (2017).

Book

[5] "Cybersecurity Smart Grid Systems Market $7.25 billion by 2020, Zpryme Reports," 2013,[Online].Available

Chapter in a Book

[6] Baumeister, T., 2010, "Literature Review on Smart Grid Cyber Security," Collaborative Software Development Laboratory, University of Hawai'i, [Online].Available:https://csdltechreports.googlecode.com/svn/trunk/techreports/2010/10-11/10-11.pdf.

Conference Proceedings

[7] S. Yao, P. Wang, and T. Zhao, "Transportable energy storage for more resilient distribution systems with multiple microgrids," IEEE Trans. Smart Grid 10(3), 3331–3341 (2019).

[8] R. Qiu and S. Jing, "Intrusion detection system using Online Sequence Extreme Learning Machine (OS-ELM) in advanced metering infrastructure of smart grid", PLOS ONE, vol. 13, no. 2, p. e0192216, 2018. Available: 10.1371/journal.pone.0192216.

[9] .K. Song, W.-W. Jung, J.-Y. Kim, S.-Y. Yun, J.-H. Choi, and S.-J. Ahn, "Operation schemes of smart distribution networks with distributed energy resources for loss reduction and service restoration," IEEE Trans. Smart Grid 4(1), 367–374 (2013).

[10] B. Chen, and J. Wang, "Decentralized energy management system for networked microgrids in grid-connected and islanded modes," IEEE Trans. Smart Grid 7(2), 1097–1105 (2016)

"Cybersecurity Smart Grid Systems Market $7.25 billion by 2020, Zpryme Reports," 2013, [Online]. Available: http://www.prurgent.com/2013-04-16/pressrelease293687.html

[11] "Cyber Security of the Smart Grids," 2012, Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids, [Online]. Available: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1761.

[12] Baumeister, T., 2010, "Literature Review on Smart Grid Cyber Security," Collaborative Software Development Laboratory, University of Hawai'i, [Online]. Available: https://csdltechreports.googlecode.com/svn/trunk/techreports/2010/10-11/10-11.pdf.

[13] Zhang Z, Gong S, Dimitrovski AD, Li H. Time synchronization attack in smart grid: impact and analysis. IEEE Trans Smart Grid 2013;4(March(1)):87–98.

[14] Wang W, Lu Z. Cyber security in the smart grid: survey and challenges. Comput Netw 2013;57(5):1344–71.

[15] Gungor , Sahin D, Kocak T, Ergut S, Buccella C, Cecati C, Hancke GP. A Survey on smart grid potential applications and communication requirements. IEEE Trans Ind Inf 2013; 9(1):28–42.

[16] O. Kosut, L. Jia, R.J. Thomas,, L. Tong, Malicious data attacks on smart grid state estimation: attack strategies and countermeasures, in: Proc. of the IEEE Conference on Smart Grid Communications, 2010