ISSN:2229-6107

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY

E-mail :
editor.ijpast@gmail.com
editor.ijpast@.in

www.ijpast.in

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107 www.ijpast.in

Vol 8,Issuse 2.May 2018

Smart Grid Security: Threats, Vulnerabilities and Solutions

B.HARI,v.Praveen ,V. RAMESH,JITTA SEYONI

Abstract

In the present moment, the conventional electrical power grid is transforming into the smart grid. The term "smart grid" refers to the combination of information and communication technologies with the existing electrical power system (ICT). Providers and users of electrical utilities benefit from this integration since it allows for better monitoring, control, and management of customer demand as well as increased efficiency and availability of the power system. A smart grid is a massive interconnected network of many different types of equipment and organisations. There are several potential threats and security flaws in a network of this magnitude. In this article, we discuss what's new in the world of smart grid safety. We emphasise the heterogeneity and interconnectedness of the smart grid network and talk about the risks that come with it. Then, we talk about the difficulties of safeguarding the smart grid network and why the standard security measures used for IT networks are insufficient. Finally, we provide an overview of the existing and required smart grid security solutions.

Keywords:

Advanced Metering Infrastructure, Information and Communication Technologies for a Secure Smart Grid

Introduction

Using transmission and distribution networks, smart grids bring energy produced at both centralised and decentralised power plants to consumers. Information and communication technologies are used for grid operation, control, and monitoring (ICT). These advancements in technology have made it possible for utilities to more easily regulate power use and provide steady, low-cost electricity to customers. The smart grid technology facilitates the most effective electric network operations in response to customer data sent and received through digital two-way communications between consumers and electric power firms. Given the potential harm and disruption to both individuals and businesses should the grid come under assault, security remains one of the most pressing concerns about smart grid technology.

The key security goals of the smart grid system are to provide the following: 1) reliable power supply at all times; 2) information integrity in all communications; and 3) user data privacy. Here is how the rest of the paper is structured. In Section 2, we get a quick primer on what smart grids are and why they're important. The most significant threats to the grid are discussed in Section 3. In Section 4,

ASSISTANT PROFESSOR[1,2,3], STUDENT [4]
Department of EEE
Arjun College Of Technology & Sciences
Approved by AICTE& Affiliated to JNTUH

SPONSORED BY BRILLIANT BELLS EDUCATIONAL SCOITEY

we discuss the different adversaries and the assaults they may launch. In Section 5, we discuss the key obstacles to addressing smart grid security via proposed solutions. There is a summary of the paper's findings in Section 7, and Section 6 describes the present and necessary security measures.

Background

As may be seen in Figure 1, the National Institute of Standards and Technology (NIST) developed a Smart Grid design with seven distinct sections. The grid may be broken down into two parts: the system and the network.

Fig. 1. Domains of a Smart Grid [NIST].

The Role of This System's Subsystem

Electrical home appliances, renewable energy sources, smart metres, electric utility control centres, and service providers are the main system components of a smart grid. It is anticipated that all electrical home appliances (both smart and legacy) may interact with smart metres across a Home Area Network (HAN), allowing for centralised control of energy usage for the whole household. Solar and wind power, which are examples of renewable energy resources, are increasingly being used to power homes and other residential facilities. The smart metre operates as an independent embedded system. Each smart metre is outfitted with a microcontroller that has a combination of non-volatile and volatile memory, analogue and digital I/O, timers, a real-time clock, and serial communication capabilities. Smart metres may remotely turn on or off a customer's electricity, as well as send out warnings if anything is amiss with the data being sent from the smart metre to the utility computer. Some smart metres have relays that may be interfaced directly with smart home equipment to regulate them; for example, turning OFF the air conditioner during peak hours. A further use for the smart metre is in demand side management. In order to control energy use, the Electric Utility Center communicates with smart metres. Over General Packet Radio Service (GPRS), it receives sub-hourly power use data and emergency/error warnings from smart metres and sends out instructions for adjusting consumption as needed. Electricity for specific devices is provided by contract between customers and service providers. The smart metre acts as a messenger between the service provider and the inside gadgets. Getting digital certificates for identities and public keys requires service providers to register with the electric utility. The certificates are then put to use in order to ensure encrypted user-to-user communication.

Connected Device

The smart grid uses two different kinds of networks to communicate: HAN and WAN (WAN). Through a HAN, all of the smart appliances in a house may communicate with the smart metre. The HAN is capable of talking to the outside world through Bluetooth, conventional Ethernet, and Zigbee. In contrast, a wide-area network (WAN) links together the electric utility, service providers, and smart metres. The WAN may use WiMAX, 3G/GSM/LTE, or fibre optics for data transmission. The smart metre relays data between the home's internal systems and the outside world. The electric company is in charge of the smart grid's power distribution, collecting data on the smart metres' sub-hourly power use, and alerting the metres when action is needed. Messages from HAN devices are picked up by the smart metre and sent to the relevant service provider. The fundamental structure is seen in Figure 2 [1]. It's important to keep in mind that HANs are mostly utilised in residences, whereas BANs and IANs are primarily used in commercial and industrial settings.

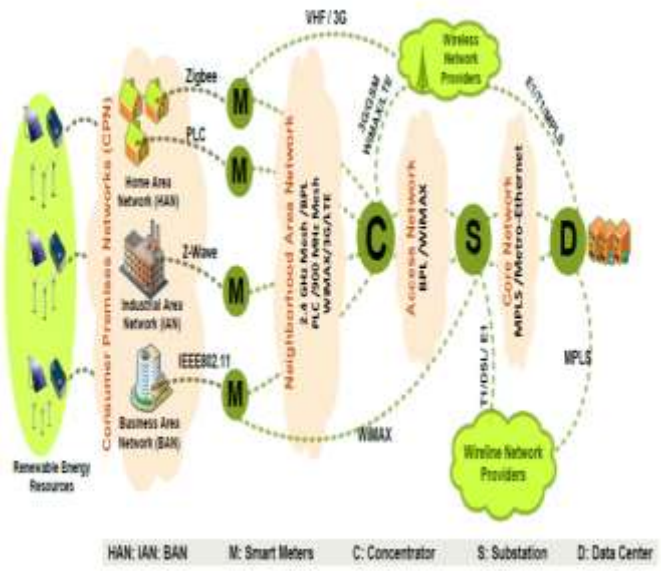

Fig. 2. Basic Network Architecture [1].

Vulnerabilities

The traditional electricity network is made more complicated and prone to many forms of assaults by the introduction of smart grid network's improvements and better capabilities. Intruders might potentially get access to the network, compromise the security of the sent data, and even cause the service to go down due to these flaws. According to [2-3], the following security flaws are the most concerning in smart grids: 1) Privacy for the customer: Smart metres gather vast quantities of information and transmit it to the utility company, the customer, and the service providers without any intervention from the user. Private information about consumers is included here, and it might be used to infer things like their whereabouts, the kind of gadgets they use, and when they leave the house. More sophisticated gadgets are used in a smart grid to control the flow of power and meet the needs of the network. These smart gadgets have the potential to serve as backdoors into the network. Furthermore, monitoring and managing the smart grid network is particularly challenging due to its vast size (100-1000 times greater than the internet). Thirdly, the smart grid network has numerous parts, the vast majority of which are located outside the boundaries of the utility's property, which means that physical security is a major concern. Because of this, there are more places out there that aren't properly secured, and criminals may easily get entry to them. Because power systems exist alongside the more shorter-lived IT systems, it is certain that ageing machinery will be in use for some time to come. This gear may not be compatible with the gadgets now used in the electrical grid, and it may also serve as potential weak spots in security. Trust between conventional power sources that is assumed: In control systems, data spoofing may occur during device-to-device communication, which can have dire consequences when the condition of one device impacts the operations of another. By communicating a bogus state, for instance, a device might cause unexpected behaviour in other devices. Sixth, the diversity of the teams itself may contribute to problems like ineffective and disorganised communication, which can result in a flood of poor choices and increased susceptibility. The use of Internet Protocol (IP) and commercially available hardware and software is a major benefit of smart grids since it ensures that all of the individual parts are compatible with one another. IP-based network assaults, such as IP spoofing, Tear Drop, Denial of Service, and others, may easily compromise IP-using devices. An increase in the number of parties involved increases the risk of insider assaults, which may have devastating consequences.

Causers and Varieties of Harmful Attacks

Each of the aforementioned flaws may be exploited by malicious actors with varying goals and degrees of technical knowledge, potentially resulting in widespread system compromise. There is no telling who may launch an attack; it might be script kids, skilled hackers, terrorists, workers, rivals, or consumers. The authors classify attackers as follows in [4]: 1) Attackers who aren't trying to do any harm but instead see the system's defences and functionality as a puzzle. Those assailants often seek for conflict and information out of a desire to learn. Two) Consumers who are so motivated by anger that they find methods to cut off electricity to their neighbours. 3) Terrorists, who see the smart grid as a tempting target because of the widespread impact it will have on public awareness of their cause. Fourthly, untrained workers or those who are dissatisfied with their utility or consumers might make mistakes. Five) Rival businesses battling each other for commercial benefit. There are many other types of assaults that these adversaries may launch, and they can be grouped into three broad groups [5-6]: component-level, protocol-level, and topology-level. The field components, such as the Remote Terminal Unit, are attacked one by one (RTU). Engineers often use RTUs for remote smart grid device configuration and troubleshooting. Attacks on this remote access function allow bad actors to take command of the gadgets and send them into bad situations like powering down. Attacks on a communication protocol use techniques like reverse engineering and forged data injections to compromise the protocol itself. Attacks that focus on the smart grid's architecture might disrupt service and force operators to make poor decisions because they lack the whole picture of the power system. In [7–10], other assaults, such as:

The propagation of malware: An adversary may programme malicious software and release it, infecting smart metres or a company's servers. Malware has the potential to completely alter the functionality of a device or system, including the transmission of private data.

Database connections for easy access:

Activity logs generated by control systems are stored in a database on the control system network and replicated to the business network. A well-trained attacker may exploit the control system network if the underlying database management systems are not correctly set up to prevent unauthorised access to the business network database.

Telecommunications system compromise:

Attackers may get access to sensitive information or cause direct harm by compromising communication devices like multiplexers.

Manipulating data via intentional misrepresentation (Replay Attack)

Incorrect metre readings, inflated costs, fabricated emergencies, and other forms of network disruption are all possible outcomes of an attacker sending packets with malicious data. The electrical markets are particularly susceptible to the monetary effects of false information.

Access to the Network:

Since the smart grid relies on IP protocol and the TCP/IP stack, it is vulnerable to denial-of-service (DoS) attacks and other flaws in the TCP/IP architecture. Denial-of-service (DoS) attacks aim to render smart grid resources unavailable by delaying, blocking, or corrupting information transmission.

Secret listening posts and traffic studies:

If an attacker is able to monitor network traffic, they may be able to steal confidential information. Future pricing information, the grid's control structure, and energy use are all examples of things that may be tracked.

Problems with the safety of Modbus:

SCADA is short for supervisory control and data acquisition, and it describes a group of computer systems and protocols used to keep tabs on and manage things like smart grid operations. The Modbus protocol is an integral part of the supervisory control and data acquisition (SCADA) system, which is responsible for sharing SCADA data to regulate manufacturing processes. Multiple attacks are possible because the Modbus protocol was not developed for highly secure environments, such as (a) sending fake broadcast messages to slave devices (Broadcast message spoofing), (b) playing back genuine recorded messages to the master (Baseline response replay), (c) locking out a master and controlling one or more field devices (Direct slave control), and (d) sending benign messages to all possible addresses to collect devices' information (Rouge interloper).

New security solutions face a number of challenges.

Typical IT network security measures are ineffective in grid environments [6]. When comparing the goals of security in IT networks versus automation (grid) networks, one can see that the former is concerned with ensuring the three security principles (confidentiality, integrity, and availability) while the latter is concerned with ensuring the protection of people, equipment, and power lines. Further, security in IT networks is accomplished by giving additional protection at the core of the network (where the data sits), but in automation networks, security is done at the network centre and edge, hence the two types of networks have distinct security architectures. IT networks adhere to a standard set of operating systems (OSs) and protocols, whereas automation networks use a wide variety of in-house or vendor-specific protocols and OSs. Last but not least, the Quality of Service (QoS) metrics for IT and automation networks are distinct in that the latter do not permit the rebooting of devices in the event of a failure or update, while the former do. With such a wide gap between IT and grid network security goals, it is clear that new security solutions tailored to the smart grid are required. A number of obstacles [5-6] stand in the way of the development of these security solutions, including: 1) the use of proprietary operating systems to control functionality rather than security; 2) an automation system network that was not designed with security in mind; 3) the need to integrate security with existing systems without compromising performance; 4) the need to monitor and control remote access to grid devices; and 5) the need for new protocols to be capable of incorporating f.

Alternate Methods

- After introducing the broad scope of the security issues and their implications, this part discusses the most recent security solutions [3, [11-14]:
- Robust authentication procedures should be used to confirm an individual's identity. Companies should adopt an implicit refuse policy where users are not automatically allowed network access.
- Embedded and general-purpose computer malware defence. Typically, the manufacturer's own software is the only one that can be used on an embedded device. Keying material for software validation must be stored in a secure location embedded in the device, and the producer is responsible for providing this. Any freshly downloaded programme may be verified by the system using a key before being executed. Although, general-purpose computers are made to run additional programmes. Host-based intrusion protection and up-to-date antivirus software are necessities for this system.

- The host-based defences should be supplemented by Network Intrusion Prevention System (IPS) and Network Intrusion Detection System (IDS) technologies to provide maximum security against both external and internal threats.
- At the very least once a year, you should conduct a vulnerability assessment to guarantee the safety of all components that come into contact with the boundary.
- User behaviour may sometimes create security holes in a system. Users of a network should be made aware of security risks associated with their actions by means of awareness campaigns.
- Communicating gadgets need to be aware of both the sender and receiver of their messages. Transport Layer Security (TLS), often known as Internet Protocol Security, is a protocol that facilitates this via the use of reciprocal authentication procedures (IPSec).
- Virtual Private Network (VPN) designs should be supported on devices to allow for encrypted data transfer.
- When exchanging data, gadgets need to use PKI [15] to ensure security. Nonetheless, there are limitations in cryptography and key management [16]: Communication in a smart grid system would occur through channels with varying bandwidths, and all devices, certificate authorities, and servers must be connected at all times, making it impossible for present devices to conduct sophisticated encryption and authentication mechanisms.
- Utilities should only mine the data transfer traffic for the information they really require.
- Engineers from both the control system and the information technology sector are needed to ensure the safety of the smart grid infrastructure.
- Since the smart grid will be around for far longer than any of the information technology systems it uses, any and all of those systems must be upgradable.
- The smart grid has to include security measures. Unless this problem is solved, device security will be dependent on the manufacturer, which might lead to a wide variety of vulnerabilities due to incompatibilities.
- Utilities should think about contracting with outside communication firms. Leaving all grid communication to the utilities rapidly becomes too much of a burden for the utilities to bear. Companies not directly involved in the movement of data might assist manage its communication and security.
- It is crucial that all parties involved in a smart grid system have a strong authentication procedure when exchanging information. The protocol has to be able to function in real-time while adhering to certain limitations, such as a small computing footprint, minimal communication overhead, and resistance to assaults, notably Denial-of-Service ones.

Conclusion

Smart grids are replacing traditional power networks because of their capacity to streamline operations, boost efficiency and dependability, and lower prices for consumers. Because of its scale and enhanced connectivity, the smart grid is more vulnerable to cyber assaults. The smart grid is a vital infrastructure that requires thorough investigation to determine all potential points of failure and enough countermeasures to bring the associated risks down to an acceptable level. In this article, we take stock of the state of smart grid network security, the forms of attack and the perpetrators, the difficulties in developing new security measures, and the available and necessary remedies.

References

[1] Ban Al-Omar, A. R. Al-Ali, Rana Ahmed, Taha Landolsi, "Role of Information and Communication Technologies in the Smart Grid", in Journal of Emerging Trends in Computing and Information Sciences, 3(5), 707-716, 2012.

[2] I. Pearson, "Smart grid cyber security for Europe", in Energy Policy, 39(9), 5211-5218, September 2011.

[3] S. Clements and H. Kirkham, "Cyber-Security Considerations for the Smart Grid", in Proc. of the IEEE Power and Energy Society General Meeting, 1-5, 2010.

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

[5] Dong Wei, Yan Lu, Mohsen Jafari, Paul M. Skare and Kenneth Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks", in IEEE Transactions on Smart Grid, 2(4), December 2011.

[6] Dong Wei, Yan Lu, Mohsen Jafari, Paul Skare and Kenneth Rohde, "An Integrated Security System of Protecting Smart Grid against Cyber Attacks", in Proc. of the IEEE PES Conference on Innovative Smart Grid Technologies, 2010.

[7] Xudong Wang and Ping Yi, "Security Framework for Wireless Communications in Smart Distribution Grid", in IEEE Transactions on Smart Grid, 2(4), December 2011.

[8] V. Aravinthan, V. Namboodiri, S. Sunku and W. Jewell, "Wireless AMI Application and Security for Controlled Home Area Networks", in Proc. of the IEEE Power and Energy Society General Meeting, July 2011.

[9] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickin- son,Heejo Lee, Adrian Perrig, and Bruno Sinopoli,

"Cyber-Physical Security of a Smart Grid Infrastructure", in Proc. of the IEEE, 100(1), 195-209, January 2012.

[10] Byron Flynn, "Smart Grid Security", in Cyber Security for Process Control Systems Summer School, June 2008.

[11] Xudong Wang and Ping Yi, "Security Framework for Wireless Communications in Smart Distribution Grid", in IEEE Transactions on Smart Grid, 2(4), December 2011.

[12] Zhuo Lu, Xiang Lu, Wenye Wang and Cliff Wang, "Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid", in Proc. of the Military Communications Conference, 1830-1835, 2010.

[13] Cisco White Paper. Available at: http://www.cisco.com/web/ strategy/docs/energy/white paper c11539161.pdf

[14] A. Metke and R. Ekl, "Security technology for smart grid networks", in IEEE Transactions on Smart Grid, 1(1), June 2010.

[15] Anthony R. Metke and Randy L. Ekl,"Security Technology for Smart Grid Networks", in IEEE Transactions on Smart Grid, 1(1), June 2010.

[16] S. Iyer, "Cyber Security for Smart Grid, Cryptography, and Privacy", in International Journal of Digital Multimedia Broadcasting, 2011. Article ID 372020, doi:10.1155/2011/372020