UGC JOURNAL NUMBER 44557

International Journal of Allied Practice, Research and Review
Website: www.ijaprr.com (ISSN 2350-1294)

A Review on Security in Smart Grids

Jeetu Sharma, Partha Pratim Bhattacharya and V K Jain
College of Engineering and Technology,
Mody University of Science & Technology,
Lakshmangarh, Sikar, Rajasthan, India

Abstract - The security of information in smart grids is of prime concern to prevent unauthorized access to the crucial information. The security threats are continuously increasing due to the usage of wireless communication standards in WSNs deployed in smart grids. The development of novel security mechanisms is required to establish strong security infrastructure from smart grids to smart homes and vice versa. The flow of information and power in smart grids is bidirectional which is controlled with the help of software and supporting hardware. The security of operating systems and algorithms is of prime importance too. This paper elaborates the threats, challenges and countermeasures to prevent the attacks of hackers.

Keywords - ***Smart grid, Security challenges, Wireless Sensor Network, Security solutions***

I. Introduction

The efficient distribution and utilization of power requires a novel sophisticated infrastructure constituted of efficient hardware and software. The deployment of Wireless Sensor Networks (WSNs) in the tradition electric grid upgraded it to a smart grid. The implementation of Information and Communications Technologies (ICT) has optimized the monitoring and control as well as increases the security threats to the critical information of smart grids. The unauthorized access to either the information generated by smart grids or by the consumers' premises can cause severe deterioration to the successful implementation of smart grid. This paper is an attempt to present major security threats, challenges and their solutions in a smart grid.

Section 2 presents literature survey, types of security attacks are elaborated in section 3, protocols to mitigate attacks are illustrated in section 4. Finally, conclusion is presented in section 5.

II. **Literature Survey**

The effective utilization and implementation of ICT improves the security in WSNs employed in smart grids [1]. The model and mechanisms are implemented in Europe to enhance the integrity of information [2]. It is very important to consider the cyber-security of smart grids [3]. The security of next generation power grid can be enhanced by the utilization of efficient security countermeasures [4]. The cyber-attacks against automation systems need to be prevented for the deployment of actuating networks [5]. There is a requirement to develop an integrating security system to mitigate cyber-attacks by developing a security framework to perform wireless communication [6, 7]. Advanced Metering Infrastructure (AMI) and Home Area Network (HAN) deployed in the consumers' premises require cyber-physical security to prevent any changes in the units consumed and variations in the state of control systems [8-10]. The designing and implementation of security mechanisms and technologies by determining the potential security threats in the form of cryptography to ensure privacy is very important [11-15]. The threats, vulnerabilities and security solutions are elaborated to optimize the security of information [16].

III. The Types of Vulnerabities

There is numerous security threats to the WSNs deployed in smart grids. Table 1 signifies distinct security threats [2, 3].

Table 1 Different type of vulnerabilities in smart grids

Vulnerabities	**Explanation**
Security of users privacy	The information collected by smart monitoring can be used to intrude the security of users may be in the form of cyber- attack or physical access.
Intelligent devices are employed	The intelligent devices can be used by a hacker to access the network of smart grids.
The physical security of assets	The installation of devices in very remote and insecure areas is a threat to its physical security.
The lifespan of the systems used	The use of outdated power systems with the latest communication systems increases the probability of security-attack by enabling unauthorized access to the outdated devices.
Propagation of wrong signal	The wrong signal generated by a device affects the performance of all the devices receiving that signal and changes their state.
Communication gap between different teams	The communication gap between different engineering teams may cause undesirable changes in the infrastructure as well as the communication architecture to increase the vulnerability.
The use of outdated hardware and software compatible with Internet Protocol (IP)	The outdated devices used are very prone to security attacks. Also, Internet Protocol (IP) is compatible with most of the wireless standards increasing the probability of unauthorized access.
Large number of stakeholders	The large number of stakeholders increases the competition and may result in internal attacks.

IV. **The Different Types of Security Attacks**

The different types of security attacks are important to elaborate. These are presented in Table 2.

Table 2 Different types of security attacks

Security-Attacks	**Explanation**
Infusion of Malware	The use of malware to malfunction the devices or servers to transmit sensitive information.
Intrusion through the links of database	The accessing of critical data bank of a control system to vary the controlling states causing severe damage to the physical and logical infrastructure.
Affecting equipments used for communication	The equipments used for communication can be blocked to disable the communication between the devices.
Generation of false information	The injection of wrong data and signals in the network to access the crucial devices to access critical information.
Availability of Network	The wireless standards and protocols employed in smart grids are widely used in internet making it vulnerable and accessible from any remote location.
Ability to analyze traffic and eavesdropping	The ability to access and analyze the data traffic may leads to know about the future pricing and energy usage.
Issue of Modbus security	Modbus protocol used in Supervisory Control And Data Acquisition (SCADA) is not ready to counter the security attacks. It is very easy to infiltrate this protocol to break its security.

V. Solutions to Prevent Security Attacks

The different types of solutions to prevent security attacks are presented in Table 3.

Table 3 Different solutions to prevent security attacks

Security-Solutions	Explanation
Authentication mechanisms	**The authenticated mechanism to access the network must be very strict.**
Malware Protection	**The implementation of systems able to prevent malware attacks should be installed.**
Intrusion prevention and detection systems	**Network Intrusion Prevention System (IPS) and Network Intrusion Detection System (IDS) technologies should be exploited to prevent external and internal attacks.**
Assessments of vulnerabilities	**The timely assessment of vulnerabilities should be performed to update the security systems.**
Educate users about security	**The knowledge of users to ensure the security of their accounts is necessary.**
Authentication Techniques	**The implementation of mutual authentication techniques using Transport Layer Security (TLS) or Internet Protocol Security (IPSec) enhances the security at various network layers.**
Virtual Private Network (VPN)	**The installed device should be compatible with Virtual Private Network (VPN).**
Key Infrastructure	**The device should use public and private key infrastructure to ensure the secure access.**
Selective data aggregation	**The devices should collect the data which is necessary to perform a particular operation and able to discard the unnecessary data.**
Security engineers	**The attainment of security should be a collaborative responsibility of control and information technology engineers.**
Upgraded IT systems	**The lifetime of IT systems is very less in comparison to the electrical systems. So, the IT systems should be upgraded time to time.**
Security in design	**Security should be embedded in the design of smart grid and should not be the responsibility of vendors.**
Third party	**The use of third party is also desirable to perform Communication and attain security.**

VI. Conclusions

In this research work numerous security vulnerabilities, attacks and solutions are presented. It is very important to establish secure wireless communication by determining the type of potential attacks. In future, the development of protocol to enhance the security will be considered.

VII. References

1. **Al-Omar B, Al-Ali AR, Ahmed R, et al. Role of information and communication technologies in the smart grid. Journal of Emerging Trends in Computing and Information Sciences, 2012; 3(5):707-716.**
2. **Pearson I. Smart grid cyber security for Europe. Energy Policy, 2011; 39(9):5211-5218.**
3. **Clements S and Kirkham H. Cyber-security considerations for the smart grid. In: Proc of the IEEE Power and Energy Society General Meeting, 2010:1-5.**
4. **Flick T and Morehouse J. Securing the Smart Grid: Next Generation Power Grid Security. Syngress, 2010.**
5. **Wei D, Lu Y, Jafari M, et al. protecting smart grid automation systems against cyber attacks. IEEE Trans on Smart Grid, 2011; 2(4):782-795.**
6. **Wei D, Lu Y, Jafari M, et al. An integrated security system of protecting smart grid against cyber attacks. In: Proc. of the IEEE PES Conference on Innovative Smart Grid Technologies, 2010:1-7.**
7. **Wang X and Yi P. Security framework for wireless communications in smart distribution grid. IEEE Transactions on Smart Grid, 2011; 2(4):809-818.**
8. **Aravinthan V, Namboodiri V, Sunku S and Jewell W. Wireless AMI application and security for controlled home area networks. In: Proc. of IEEE Power and Energy Society General Meeting, July 2011:1-8.**
9. **Y Mo, Kim T H-J, Brancik K, et al. Cyber-physical security of a smart grid infrastructure. Proc. of the IEEE, 2012; 100(1):195-209.**
10. **Flynn B. Smart Grid Security. Presented at: Cyber Security for Process Control Systems Summer School, June 2008.**
11. **Wang X and Yi P. Security framework for wireless communications in smart distribution grid. IEEE Transactions on Smart Grid, 2011; 2(4):809-818.**
12. **Lu Z, Lu X, Wang W and Wang C. Review and evaluation of security threats on the communication networks in the smartgrid. In: Proc. of the Military Communications Conference, 2010:1830-1835.**
13. **Cisco White Paper. [Online]. Available: http://www.cisco.com/web/strategy/docs/energy/white paper c11539161.pdf**
14. **Metke AR and Ekl RL. Security technology for smart grid networks. IEEE Transactions on Smart Grid, 2010; 1(1):99-107.**
15. **Iyer S. Cyber Security for Smart Grid, Cryptography, and Privacy. International Journal of Digital Multimedia Broadcasting, 2011; doi:10.1155/2011/372020.**
16. **Fadi Aloula, A. R. Al-Alia, Rami Al-Dalkya, et al. Smart Grid Security: Threats, Vulnerabilities and Solutions. International Journal of Smart Grid and Clean Energy, 2012; 1(1), 1-7.**