Survey on Security Aspects in Smart Grid: Performance and Parametric Analysis

V. V. Vineeth, S. Sophia and S. Jayanthy

Abstract Smart grid is a great new aspect of the power industry. It integrates various advanced technologies and information and communication capabilities to deal with problems found to occur with the existing electrical networks. Such integration facilitates and improves efficiency and accessibility of the electric power system with the additional features of regularly supervising, calculating, and administrating customer demands. This leads to the excessive deployment of smart meters in order to recognize the actual benefits. But, the deployment of smart meters brings up different concerns on the security of information among both consumers and service providers. This paper aims to focus on the major attacks on smart meter security which challenges the overall grid security.

Keywords Smart grid · Smart meter · Cyber attack · Physical attack · Security solutions

1 Introduction

The several improvements and better new capabilities of the smart grid environment make the grid architecture more complex and expose it to various kinds of attacks. Smart meters tend to be an important component of the grid by acting as a central gateway located on customer's site supporting two-way communication. Smart

V. V. Vineeth (✉)
Department of Electrical and Electronics, Sri Krishna College of Engineering & Technology, Coimbatore, India
e-mail: vineethvv@skcet.ac.in

S. Sophia
Department of Electronics and Communication, Sri Krishna College of Engineering & Technology, Coimbatore, India

S. Jayanthy
Department of Electronics and Communication, Sri Ramakrishna Engineering College, Coimbatore, India

H. S. Saini et al. (eds.), *Innovations in Electrical and Electronics Engineering*,
Lecture Notes in Electrical Engineering 626,
https://doi.org/10.1007/978-981-15-2256-7_55

meters gather a large amount of information and transfer to companies, service providers, and consumers. Collected data includes information about a private consumer which may be made use to deduce activities of consumer, devices used, and the times when home is vacant [1].

Smart meter security aspects include customer security, physical security, and implicit trust that exist among traditional power devices. Customer security issues arise when the private consumer information collected by a meter is prone to attack. The vulnerability to physical access and attacks of various distributed components comprises the physical security aspect [2]. The security aspect of communication among power devices includes the data spoofing attack which may affect the device-to-device communication which can affect more devices.

2 Smart Meter Overview

Smart meters are key components in the grid infrastructure, the idea being emanated due to the wide-scale deployment of smart grid environment. Smart meter systems are available in smart grid environment not just to stipulate instant meter information on supplies, including water, electricity, and gas to service providers, but it, in turn, use this information so as to make it available to end users who are the final users of electricity and some of them even include the measurement of worthiness of power and essential control features [3]. Smart meter devices can adapt the power generation as on demand and thus can enable the balancing of power production and its distribution in a smart grid environment. Such devices are actually the point of contact among the two components such as the electric utility and the end user. Smart meter acts as a point of managing being located at the end use premise and physically managing the same. Smart meters have the added characteristics including identification of power usage patterns and behaviors by tracking the usage of data, capability to disconnect an end user from smart grid, generating alerts for the service providers in case of any problem, and monitoring and controlling of smart home devices at peak times [4]. Deploying a large quantity of software aspects and techniques is involved in the integration of smart meters to smart grid concept. These techniques depend primarily on the aspects of the demanding situations. The National Institute of Standards and Technology developed smart grid infrastructure composed of seven domains as shown in Fig. 1. This design and also the implementation of the smart meters thus depend on the specific requirements of service providers and that of end users.

Different control devices and sensors are employed in a smart meter for the purpose of identifying the various devices and parameters so as to permit transmission of command signals and information. By active monitoring of performance and also the electricity usage features of smart grid load, smart meters can carry out a vital role in power grid in the future. Gathering of power consumption information from end users helps providers to analyze and manage power demands and the same can be made use of to notify the customers about efficient way so as to make use of their smart devices. It also helps service providers to detect stealing of

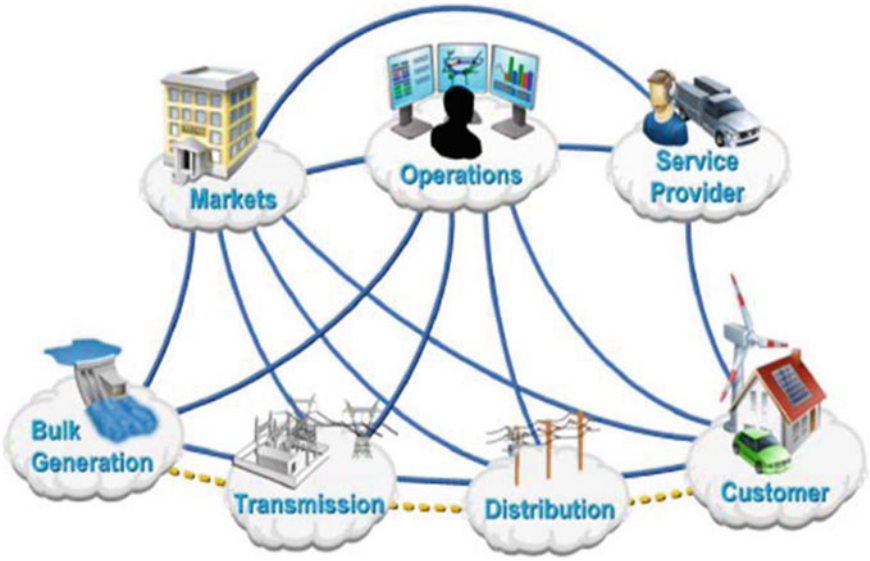

Fig. 1 Smart grid domains (NIST)

electric power and unauthorized access which in turn helps in improving the power distribution and power quality [5]. Since smart meters can identify profitable end users depending on overall energy consumption and power generation sources, service providers can provide such customers with advanced voluntary value-added services. These all require the collection of large amount of real-time data from end users.

Though there is an enormous list of various features and capabilities provided by a smart meter, its deployment raises many security and privacy concerns. It comes up with major concerns on overall security including data security(regarding end user privacy data), data integrity issues, availability, access control, to name a few. These security concerns are due to the reality that smart meters often act as the weakest link in grid environment [6]. That is, they can be easily attacked through other networks since they operate on wireless means for communications. These attacks launched on smart meters can in turn affect the overall security of the grid which can cause data corruption, mistakes in accounting, power blackouts, etc (Fig. 2).

3 Security Solution Challenges

The different problems and challenges concerned in the implementation, design, exploitation, and maintenance of smart meters are outlined in paper [7].

The deployment of smart meters in distributed systems is analyzed which incur huge cost, and it faces more difficulties with the increasing number of customers.

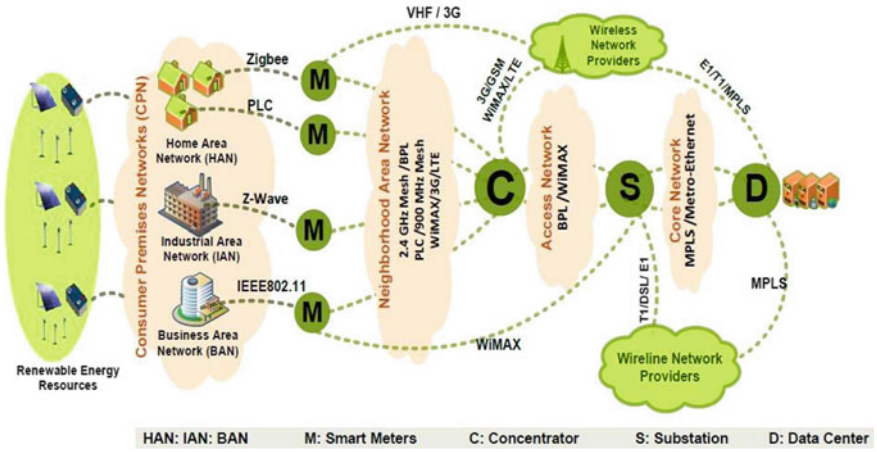

Fig. 2 Basic network architecture

The gathering and transmission of power consumption data raise privacy and security risks. Data can also disclose the location of customers, and the authentication of such information is vital [8, 9]. DNP3 and its enhanced versions can be used for communication network, but it cannot offer needed security [10]. Power consumption information being carried over cellular networks has security risks [11] which tend to other problems like poor protocols and authentication. This is added up by data concentrators. The paper identifies different design issues including technology aspects, physical aspects, cost of device, communication, and identification for all devices. The maintenance issues were classified as being of network failures, communication network, smart meter, and base server. Further, it investigates the challenges with data transfer as being the quantity of information to be transmitted, the access criteria and also the kind of modulation to be employed. Certain sections of people are also interested in collecting data from smart meter including illegal customers and attackers [12], and since the gateways can be compatible with other appliances, it brings up cyber security and also physical security risks [13]. The weaknesses of current smart metering systems are highlighted in paper [14]. It focuses on the methods used to secure transmission of data, including symmetric and asymmetric means. Both the approaches are found to have problems: communication security (where whole information will be lost) for symmetric and there are problems of the reduced speed of systems in case of asymmetric approach. It was outlined that weak security could be resulted by using symmetric algorithm at both parts of communication, whereas though some sort of security can be attained in asymmetric case, it is a lot of waste of time. The process of generation and management of keys for the algorithm is also a tedious process.

The possibilities that can be modeled on a smart meter system are discussed in paper [15]. Two types of derived attacks have been launched; assuming an attacker can have system-level access, and an abstract model has been designed to extract

and analyze the attacks. The first attack being launched is communication interface attack targeting on communication link. This is done by writing fake processes and using ports, which indeed resulted in fake consumption of data. The second attack is physical memory attack, which takes into consideration the fact that power consumption data will be written to flash memory in case of network unavailability. A script has been written to deactivate scripts and to overwrite data file with fake data. Power consumption could be modified by activating the script. The effect of these two attacks has been studied in the paper by considering the CPU and memory overhead involved, and it is found to have a great impact. This paper [16] focuses in detail on the security and privacy issues of smart meters. The potential attackers, their model of attacks and threats caused, are presented. Different types of attackers on smart meters are identified including eavesdroppers, marketing agencies, customers, novice attackers, and active attackers. Security attacks launched by these attackers include eavesdropping, denial of service, packet injection attacks, man-in-the-middle attack, remote connect/disconnect, malware injection attacks, and firmware manipulation. It is identified in the paper that the security and privacy issues are closely related. The consequences are also highlighted.

A collective analysis of the reading of smart meter among a clustered group of meters based on a detection model is done in paper [17]. The attacker is aimed at producing faulty readings by the compromised meters. The meters of neighborhood network are grouped into clusters, and they multicast their reading values. The compromised meters can either report fault readings to its peers in a cluster thus avoiding detection, or it can report it to both peers and central unit at the same time. The results of the attacks have been identified, and an effective peer-monitoring system is analyzed to be appropriate to find out the misbehaving of meters in a cluster. The possible attacks on smart grid infrastructure are identified in paper [18] focusing on smart meter perspective. Different types of attacks affecting the confidentiality, integrity, availability, and non-repudiation are identified and analyzed in detail. The physical attacks as well as their cyber counterparts are listed out, and it is identified that smart meters are the possible targets of attack in a grid environment.

4 Smart Grid Security Goals

Security of smart grid security can be examined as being a group of main goals such as availability, integrity, confidentiality, and also accountability.

- Availability: This goal makes sure that information be accessed on reliable and also in a timely fashion. Collection of the data, refinement, and the sharing of data is important and is to be maintained by security solutions.
- Integrity: Data should be highly accurate and reliable. It should be ensured that the data is accurate and should be free from manipulation in order to prevent harmful attacks and fraud.

- Confidentiality: Huge volumes of data generated by the grid should be collected, stored, and analyzed. It includes sensitive data regarding consumers and utilities. Care should be taken so as to avoid unauthorized access to sensitive information.
- Accountability: Since proper care is needed while disclosing sensitive information, the communications of the user with the systems are logged properly and are linked with specific users. That is, smart grid users are responsible for the activities they carry out. Logs should be such that it may not be manipulated, and integrity is to be maintained.

5 Proposed Solutions

1. Powerful authentication methods are required to verify the integrity. Explicit requests are needed to permit access to network, and all other accesses are denied implicitly.
2. Smart grid infrastructure may have embedded and also general-purpose systems. Both these should be secured from the malwares. Embedded systems generally run on software from manufacturer that must necessarily have a secure storage which should contain keys that can be used for the validation of the particular software. Key can be made use to validate any software that is newly downloaded. Third party generally provides general-purpose systems, and its security is assured by means of updated antivirus solutions which regularly get updated and also by way of intrusion prevention systems.
3. Host-based security measure should be supplemented with intrusion prevention and detection systems (IPS and IDS) so as to guard the system against inside and outside attacks.
4. At least once in a year, vulnerability evaluation should be done to ensure that the interfacing elements are secured.
5. Awareness programs are to be conducted so as to educate network users about the security aspects on using the network so as to avoid possible system threats.
6. Common authentication mechanisms like Internet Protocol Security (IPSec) and Transport Layer Security (TLS) should be employed by the source and destination systems in order to know each other.
7. For safe and secure communication, devices should enable virtual private network (VPN).
8. For reliable and secure communication, devices must use public key infrastructure (PKI) [7]. While using cryptography for security, certain constraints exist like the storage and processing power to execute authentication and encryption mechanisms [8]. This is of major concern in smart grid environment since communications involve various channels of various bandwidths to which all the devices, other entities, and servers will be connected all the time.

9. Data filtering should be done by the utilities in order to obtain the relevant data for their processing.
10. For achieving smart grid security, both control system engineers and software engineers for security must equally be involved.

6 Conclusion

The various attack strategies and its effects on smart metering systems have been identified in this paper. The detailed analysis on the attack regimes indicates a line open up for the future research to introduce secure and appropriate model for smart meter architecture so as to make it secure and can function by ensuring that the model is free from all the various kinds of attacks. The model should be such that it considers all the various categories of attacks including cyber and physical categories. This is of primary importance since the loopholes open up for launching attacks on a smart meter affect the overall functionality of smart grid infrastructure and may lead to the overall destruction of the grid.

References

1. J. Naruchitparames, M.H. Güne, C.Y. Evrenosoglu, Secure communications in the smart grid, in *Consumer Communications and Networking Conference (CCNC)*, pp. 1171–1175 (2011)
2. S.S.S.R. Depuru, L. Wang, V. Devabhaktuni, N. Gugi, Smart meters for power grid: challenges, issues, advantages and status, in *Power Systems Conference and Exposition (PSCE)*, pp. 1–7 (2011)
3. S. Jaarsma, R. van Gerwen, R. Wilhite, Smart metering. *Leonardo Energy* (2006)
4. Y. Tanaka, Y. Terashima, M. Kanda, Y. Ohba, A security architecture for communication between smart meters and han devices, in *IEEE Third International Conference on Smart Grid Communications*, pp. 460–464 (2012)
5. H. Li, R. Mao, L. Lai, R. Qiu, Compressed meter reading for delay-sensitive and secure load report in smart grid, in *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 114–119 (2010)
6. U. Greveler, P. Gloesekoetter, B. Justus, D. Loehr, Multimedia content identification through smart meter power usage profiles, in *Proceedings of the International Conference on Information and Knowledge Engineering IKE'12*, Jul 16–18, Las Vegas, Nevada, USA (2012)
7. S.S.S.R. Depuru, L. Wang, V. Devabhaktuni, N. Gudi, *Smart Meters for Power Grid—Challenges, Issues, Advantages and Status*, IEEE (2011)
8. C. Bennett, D. Highfill, Networking AMI smart meters, in *Proceedings of the IEEE Energy 2030 Conference*, Atlanta, GA, pp. 1–8 (2008)
9. D. Silva, *New 'Smart' Electrical Meters Raise Privacy Issues* (Online). Available: http://www.physorg.com/news176703307.html
10. T. Mander, H. Cheung, A. Hamlyn, W. Lin, Y. Cungang, R. Cheung, New network cyber-security architecture for smart distribution system operations, in *Proceedings of the*

IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy, Pittsburgh, PA, pp. 1–8 (2008)
11. F.M. Cleveland, Cyber security issues for advanced metering infrastructure, in *Proceedings of the IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy*, Pittsburgh, PA, pp. 1–5 (2008)
12. M.F. Foley, *The Dangers of Meter Data (Part 1)*, (Online). Available http://www.smartgridnews.com/artman/publish/industry/The_Dangers_of_Meter_Data_Part_1.html
13. G.N. Ericsson, Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Trans. Power Deliv. **25**, 1501–1507 (2010)
14. R. Rashedi, H. Feroze, Optimization of process security in smart meter reading, in *2013 Smart Grid Conference (SGC)*, December 17–18, Tehran, Iran (2013)
15. F.M. Tabrizi, K. Pattabiraman, *A Model for Security Analysis of Smart Meters*, IEEE (2012)
16. O. Ur-Rehman, N. Zivic, C. Ruland, *Security Issues in Smart Metering Systems* (2015)
17. Z.A. Baig, A. Al Amoudy, K. Salah, Detection of compromised smart meters in the advanced metering infrastructure, in *Proceedings of the 8th IEEE GCC Conference and Exhibition*, Muscat, Oman (2015)
18. R. Vigo, E. Yüksel, C.D.P.K. Ramli, Smart grid security a smart meter-centric perspective, in *20th Telecommunications Forum TELFOR* 2012, Serbia, Belgrade (2012)