Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Smart Grid Security and Privacy: Challenges, Literature Survey and Issues

Rajiv .K. Bhatia, Varsha Bodade
Dept. of Information Technology
Terna Engineering College
Nerul, Navi-Mumbai 400-706, India

Abstract: Security in smart grid is challenging. Smart Grid is recognized as two way communication technology. There are numerous communication, intelligent, monitoring and electrical elements employed in power grid that makes it smart. These elements regularly generates cum real timely talks the critical information like monitoring data, customer energy consumption, grid status, demand response etc among the smart grid devices. So, security attacks on such a system threatens the security of smart grid, results in severe consequences. So, this paper briefly discusses the important security and privacy challenges, issues and some likely solutions for protecting the smart grid.

Index Terms: AMI (Advanced Metering Infrastructure), SG(Smart grid), PKI(Public Key Infrastructure), Attacks, Vulnerabilities, Privacy, Security.

I. INTRODUCTION

The two way communication technology is called smart grid. It involves employment of communication cum information system with power infrastructure, enabling monitoring, inculcating demand response activities among energy producers and consumers which significantly increases effcient utilization of the power. The Smart Grid employs millions of devices forming networked together, and the crucial aspect is the security, integrity, privacy of these individual devices is important to ensure whole stability of the power infrastructure. There are many smart meters employed in smart grid forming AMI network. These meters generate critical information in bulk that must be prevented from attacks or manipulations. Thus study of cyber security attacks their possible counter measures should be done to ensure reliable operation. Each and every smart grid device who some how uses or intends to take benefit of smart grid must be authenticated, authorized using some strong, easy cum light weight authentication mechanism [3] which preserves their identities .In [1] attempt for authentication is done using digital certificate for each device with intelligence by multi agent system to ensure self healing, guarantee the reliable operation of smart grid. Numerous system employs PKI technology to secure the SG. In [2] authors propose that PKI is the likely solution to address the security hunger of smart grid and they propose several PKI models which can be adaptable but the bridged security model ensures the scalability, reliability, high availability and realtime operation. Also,in smart grid, there is vital employment of communication networks (specially wireless) puts a huge concern on security and privacy aspect of the system. Security attacks can result in severe blackout or outages making million homes powerless. Cyber security must tackle to deliberate attacks, such as eavesdroper, and terrorists, as well as inadvertent compromises of the information infrastructure because of human errors, equipment failures, and natural disasters. Vulnerabilities gives that an attacker to have the opportunity to penetrate into a smart grid system, gain access to control hardware and software, and manipulate load conditions of the grid to destabilize it.

II. SECURITY AND PRIVACY IN SMART GRID

Security is a challenging game of wits, pitting security attackers versus assets holders. Security in SG is of no exception to this paradigm. Cyber security is intended as one of the crucial challenges for SG[4], [5], [6]. Vulnerabilities usually allow an attacker to break a system, corrupts user privacy, aquire access to control software,
and modifies load conditions to destabilize the grid in unexpected ways [5]. Fig. 1 shows the classification of the function on security and privacy for SG. We must take a note that the advanced infrastructure employed in SG on one hand encourages us to exercise more powerful mechanisms to defend against cyber attacks and handle failures effciently, on the other side opens so many new vulnerabilities. Hence in the following, it is going to be discussed countless new security and privacy issues due to the deployment of many smart meters, sensors, and PMUs, together with some solutions.

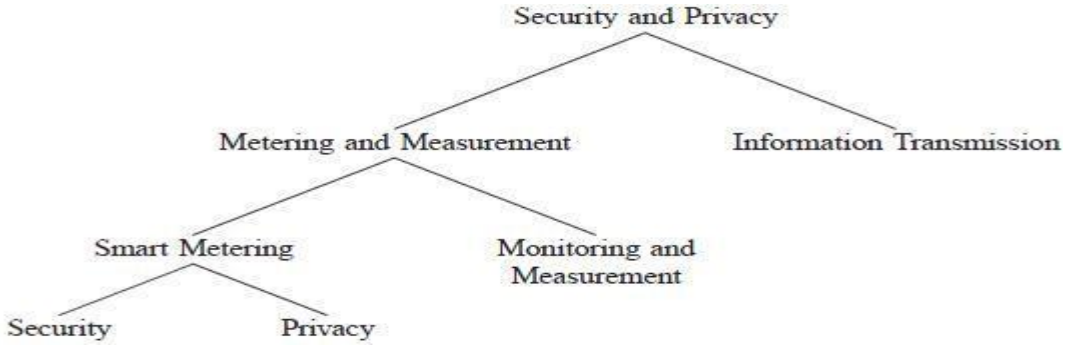

Fig. 1. Classification of the function on security and privacy for SG

A. Smart Metering, Monitoring and Measurement

1) Security in Smart Metering: The security issues arrives from the recently deployed smart meters in large quantity. Smart meters are very attractive point for malicious hackers, since vulnerabilities can effortlessly be monetized [7]. Hackers or attackers who compromises a smart meter can immediately alter their energy costs or change generated energy meter readings to make money. A common consumer cheating in traditional power grid is that customers turn a physical meter upside down inside the electrical socket so as to cause the internal usage encounters to run backward. Due to the usage of smart meter, such attack can even be done with remote PCs. Moreover, wide usage of smart meters may provide a potentially many number of opportunities for adversaries. For example, inserting false information could mislead the electric utility into making incorrect decisions about regiona or local usage and capacity. Let us consider a simple but effective Denial-of-Service (DoS) attack. An adversary establishes the demand request of a smart meter, and keeps requesting a large amount of electricity. Within the framework of SG, it can be possible that the utility disconnects all the appliances connected to the meter so that all the power services for this user are refused. Deployment of smart meters in large not only leads to a large number of opportunities for adversaries, but also opens up the door to the cyber attacks which could lead to broad effects and even severe disasters. Let us take an example given by Anderson and Fuloria [8]. An ideal attack on any target country is to corrupt its citizens electricity supply. till now, the only effective way to do that involves attacks on generation, transmission, and distribution electrical system, which are now increasingly well defended. However, the rise of smart meters changes this game. The scenario is that a country where there are millions of smart meters, controlled by a few of their central utility controller. The attacker can also compromise these controllers and can send the set of commands that will cause meters to interrupt the electric supply. Such attack could cause severe disastrous results. In order to improve the security of smart metering systems, researchers have found many possible attacks and proposed some solutions. Cleveland [9] illustrates the security requirements i.e (integrity, confidentiality, availability, and accountability) and other related threats to the main components of an advanced metering infrastructure (AMI) of SG. McLaughlin et al. [10] dissusses an adversarys means of defrauding the electrical grid by altering AMI systems, and validated the effectiveness of such attacks by doing penetration testing on commodity devices. They found that not only is theft still possible in AMI
systems, but that current AMI devices introduce a list of new vectors for achieving it. To protect the attacker from forging the reading ofsmart meter and guarantee the meter reading accuracy, Varodayan and Gao [11] gives a secure technique for power suppliers to echo the meter readings they receive from smart meters back to the customers so that particular users can verify the integrity of the smart meter. Furthermore, their process can also guarantee information-theoretic confidentiality, hence solving the confidentiality leak introduced by the redundant measurement. Berthier et al. [12] investigated the practical essentialities for monitoring and intrusion detection through a thorough analysis of the numerous threats targeting an AMI. They specified that specification-based detection technology has got the potential to meet the industrial requirements and constraints of an AMI. However, such technology puts a excessive development cost.

2) Privacy in Smart Metering: Smart meters in AMI also have unintended outcomes for customers privacy. NIST found out that the big benefit give by the SG, i.e. the ability to get richer data to and from consumer meters and other electric appliances, is also its Achilles heel from a privacy viewpoint [13],[6]. The more obvious privacy trouble is that the power usage information stored in the meter reacts as an information-rich side channel, and can be reused by interested groups to get personal data like consumer energy usage habits, behaviors, activities, likings, and even beliefs [14], [16],[7]. A little monitoring test on a private residence conducted in [16] reflected that personal information can be approximated with high accuracy, even with propotionaly unadvanced hardware scheme, and algorithms. To tackle with privacy propaganda of smart meters in AMI, some proposals have been proposed. Li et al. [15] gives a very distributed incremental data aggregation approach, in which data is aggregated at all smart meters. Homomorphic encryption is used to secure the data in transit. Hence, intermediate meters can not notice any intermediate or final outcome. Li et al. [17] proposed to compress the smart meter data and use random sequences in the compressed sensing to boost the privacy and integrity aspects of the meter readings to enhance the security. A privacy-preserving protocol forenergy billing and for performing general calculations on fine grained energy meter

readings is proposed by Rial and Danezis [18]. The Zero-knowledge proofs are utilized particularly to ensure that the fee is correct without disclosing any energy consumption data. Costas and Kalogridis [19] anonymizes smart metering data so that information obtained from it cannot be easily attached with an identified person thus effectively deals with privacy problem. Garcia and Jacobs [20] suggested that the current smart metering structure must be shuffled or altered in order to replace a unilateral trust assumption with a more multilateral architecture in which smart meters have a more trusted component and can possibly enjoy a proper level of autonomy. Kalogridis.

[13] protects smart metering data privacy by a load signature moderation system. Authors discussed a model in which the amount of utility energy required may hide the consumers demand, by properly configuring the power router to determine the power given or required by a battery. Such type of system allows users to control (upto a certain extent) their energy usage, security, and home energy privacy.

3) Security in Monitoring and Measurement: High deployment of monitoring and measurement devices (e.g. sensors, Meters and PMUs) could also gives rise to system vulnerabilities. The effective functioning of SG is widely dependent on the widely-deployed accurate measurement devices. Such measured information are typically transmitted to a control utility center, such as Supervisory Control and Data Acquisition (SCADA) Systems [21]. State estimators in the utility center estimate the power grid status by analysing the measurement data and power system models. Therefore, it is very vital to guarantee the integrity of the data in SG. A usual attack to corrupt data integrity is the stealth attack (also called false-data injection attack), which was first interpreted by Liu et al. in [22]. It disscussed that an attacker can change the state estimated data without triggering bad-data alarms in the control center. Xie et al. [23] reflected that with the knowings of the system configuration, such attacks will circumvent the false data measurement detections in the SCADA systems, and may give rise to profitable financial misconduct. So, In order to know that how difficult it is to do a successful false-data injection attack on a particular measurements, Sandberg. [24] expalins security indices to measure the less effort required to reach attack goals while refusing false data alarms in the power grid utility control center. Yuan. [25] successfully developed the abstraction of a special type of false data injection attacks load redistribution attacks, and analyzed their worst damage to power grid operation in different time move with different attacking resource limitations. To protect the system from such attacks, scientists have defined various approaches. Early we disscussed that the control center of power grid uses state estimators to estimate the power grid state. In [26], it is shown how one can fully protect a state estimator from such hidden attacks by encrypting a adequate number of measurement devices. Dan and Sandberg [27] expanded the research in [26],[24] and defined two algorithms to keep encrypted appliances in the system to maximize their utility's system security.

B. Information Transmission

It is widely famous that the communication technologies that we are utilizing are often not secure enough themselves and can easily be attacked. Hence most of the security and privacy issues which are there in the general communication networks (e.g. Internet and wireless networks) can also exist in SG Especially, we have to take more care of wireless communication technologies since wireless networks are expected to be the more vulnerable and functional deficit networks in SG. For example, wireless mesh networks (WMNs) are considered very reliable because they provide multi hop redundant communication paths, but WMNs are vulnerable to attacks by only intelligent adversaries. ZigBee is known widely as a low-cost, low-power, wireless networking technology, found on the IEEE 802.15.4 standard. However, there also exist vulnerabilities associated with IEEE 802.15.4 implementations [32].

Security attacks on information transmission in SG can be classified in three major types based on their motto [30].

1) Network Availability: Malicious attacks on intending network availability can be called as DoS attacks. They attempt to slow down, block, or even manipulate information transmission so as to make network resources unavailable to terminals that are in need to exchange information in SG. As shown out by NIST [28], the high priority is of designing the information transmission networks that should be robust to attacks which are targetting network availability, because the network unavailability may outcome in the loss of real-time monitoring of critical smart grid infrastructures and power system disasters.
2) Data Integrity: Data integrity attacks generally intend to deliberately manipulate or corrupt information shared within the SG, its elements and may be highly damaging in the SG
3) Privacy of Information: Information privacy attacks just intend to eavesdroping on communications in SG elements so as to acquire desired information,like consumer account number and their energy usage.Initially, the work was done by Li et al. [29], who investigated the fundamental limit, i.e, how much channel capacity is essential to promise the secured communications among SG elements, from the perspective of information theory, and found the situation of a single meter and or Gaussian noise communication channel with an eavesdropper.

Thus to improve the security and privacy of information transmission in SG, researchers have exhibited several solutions. Lu et al. [30] suggested that the strong authentication protocol design and intrusion detection mechnism as the countermeasures to tackle and protect the SG network against attacks targeting data integrity and information privacy . Further, Khurana et al. [31] proposed a bunch of designs and talked practices which can often ensure the correctness of standards for authentication in SG. Such design principles encompass names, unique encoding, explicit trust considerations, implementations of timestamps, protocol boundaries, deliverance of secrets, and clear-cut security parameters.

III. FUTURE SCOPE

In this section we have disscussed about security of SG to ensure reliable operation of it and mitigate the security attacks with perspection on privacy preservation.

A. Interoperability between cryptographic systems in SG elements:

Since there will be different cryptography requirements and security needs of each of various communication protocols and technologies used in SG, employing interoperability between cryptographic systems is not a easy task. Before employing cryptography, It is very essential for us to have a method of securely communicating the cryptographic keys between the SG elements. possible solutions can be is to design, as suggested in [4],[1], a public key infrastructure approach, which can use the layered based approach in communication models. A whole solution based on this these idea is needed.

B. Clash in between privacy preservation and information usage

balancing privacy preservation and information accessibility is not easy . Assume, for example,group of users. On one side, the large information about demand patterns such users are intending to disclose, the smart decisions a management system can take so as to optimize profits. However, more accesibility of information usually demands more privacy leaks, which can quickly reveals user profiles and behaviors. We advice that to issuing numerous privacy preservation levels similar to these in access control, each of which describes a tolerable amount of data leak. On each level, we can define the management objectives based on the information which can be used,. For example, single privacy policy within a group of users may allow full information exchange. Hence, suchgroup of users can increase their profits by employing their shared information. Other mechanisms accomplishing advanced encryption techniques like AES, Homomorphic may also be applicable.

C. effect of increased system complexity and spreaded communication paths:

The advanced infrastructure used in SG is a double-edged sword. On one side, it puts the foundation for the future advanced power grid that can serve better. On the another side, high complexity of system and spreaded communication networks can easily lead to an increment in vulnerability to cyber security attacks and system failures. A wholly implemented SG may contain of millions of nodes. This system large scale makes it hectic to expect how attacks may be made by an unpredictable and clever adversary, and which resultant failures could happen because of many dependent or independent factors [32]. One possible direction to overcome this challenge is to split the whole system into many individual sub-grids so that the system complexity can be declined easily. Therefore, the effect of system failures and attacks can be at a too limited level as much as possible. This is necessarily equal to the concept of microgrid. We should concern that autonomy does not mean that there is no connection among these sub-grids and utilities. The outcome of the existence of these links is that attacks cannot be wholly isolated. Hence a total solution needs to be considered for both autonomy and interconnectivity.

IV. CONCLUSION

The paper exhibited the major concerns to protect the smart power grid infrastructure from malicious attacks in connection to metering, transmission,measurement etc. We have shown the work for system reliability, failure prevention mechanism security cum privacy in SG. However, we should understand that the advanced infrastructure used in SG on one side motivates us to realize high powerful mechanisms to defend against security attacks and tackle failures, but on the another side, it opens too many new vulnerabilities. More extensive quality research and study on the smart protection system is needed.

REFERENCES

[1] V. Dehalwar, R. K. Baghel, M. Kolhe. Multi-Agent based Public Key Infrastructure for Smart Grid, The 7th International Conference on Computer Science & Education (ICCSE 2012) July, 2012. Melbourne, Australia.
[2] T. Baumeister, Adapting PKI for the Smart Grid, Cyber and Physical Security and Privacy (IEEE SmartGridComm),2011
[3] Xudong Wang,and Ping Yi, Security Framework for Wireless Communications in Smart Distribution Grid. IEEE Transactions On Smart Grid., vol. 2, no. 4, December 2011
[4] T. Baumeister. Literature review on smart grid cyber security, Technical Report, http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf. 2010.
[5] A. R. Metke and R. L. Ekl. Security technology for smart grid networks. IEEE Transactions on Smart Grid, 2010.
[6] National Institute of Standards and Technology. NIST framework and roadmap for smart grid interoperability standards, release 1.0, http://www.nist.gov/public affairs/releases/upload/smartgrid interoperability final.pdf. January 2010
[7] P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid. IEEE Security & Privacy, 2009.
[8] R. Anderson and S. Fuloria. Who controls the off switch? IEEE SmartGridComm10, pages 96102, 2010.
[9] F. M. Cleveland. Cyber security issues for advanced metering infrastructure (AMI). IEEE Power and Energy Society General Meeting: Conversion and Delivery of Electrical Energy in the 21st Century, pages 1-6, 2008
[10] S. McLaughlin, D. Podkuiko, and P. McDaniel. Energy theft in the advanced metering infrastructure. 4th Workshop on Critical Information Infrastructures Security, 2009.

[11] D. P. Varodayan and G. X. Gao. Redundant metering for integrity with information-theoretic confidentiality. IEEE SmartGridComm 2010, 345349, 2010.
[12] R. Berthier, W. H. Sanders, and H. Khurana. Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. IEEE SmartGridCommunication 2010, 350355, 2010.
[13] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda. Privacy for smart meters: Towards undetectable appliance load signatures. IEEE SmartGridComm2010, 2010.
[14] H. S. Cho, T. Yamazaki, and M. Hahn. Aero: Extraction of users activities from electric power consumption data. IEEE Transcations on Consumer Electronics, 2010
[15] F. Li, B. Luo, and P. Liu. Secure information aggregation for smart grids using homomorphic encryption. IEEE SmartGridComm2010. 2010
[16] M. A. Lisovich and S. B. Wicker. Privacy concerns in upcoming residential and commercial demand-response systems. the TRUST 2008 Spring Conference, 2008
[17] H. Li, R. Mao, L. Lai, and R. C. Qiu. Compressed meter reading for delay-sensitive and secure load report in smart grid. IEEE SmartGridComm2010, 2010.
[18] A. Rial and G. Danezis. Privacy-preserving smart metering, http:// research.microsoft.com/pubs/141726/main.pdf.
[19] C. Efthymiou and G. Kalogridis. Smart grid privacy via anonymization of smart metering data. IEEE SmartGridComm2010, 2010.
[20] F. D. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption, Techinical report. Radboud Universiteit Nijmegen, 2010.
[21] National Communications System. Technical Information Bulletin 04- 1, Supervisory control and data acquisition (SCADA) systems. 2004.
[22] Y. Liu, P. Ning, and M. Reiter. False data injection attacks against state estimation in electric power grids. ACM CCS, 2009.
[23] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. IEEE SmartGridComm, pages 226231, 2010.
[24] H. Sandberg, A. Teixeira, and K. H. Johansson. On security indices for state estimators in power networks. the First Workshop on Secure Control Systems, 2010.
[25] Y. Yuan, Z. Li, and K. Ren. Modeling load redistribution attacks in power systems. IEEE Transaction on Smart Grid, 382392, 2011.
[26] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye. Detecting false data injection attacks on DC state estimation. the First Workshop on Secure Control Systems2010, 2010.
[27] G. Dan and H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems. IEEE SmartGridComm2010, 2010.
[28] The Smart Grid Interoperability Panel - Cyber Security Working Group. Guidelines for Smart Grid cyber security: Vol. 1, Smart Grid cyber security strategy, architecture, and high-level requirements. NISTIR 7628.
[29] H. Li, L. Lai, and R. C. Qiu. Communication capacity requirement for reliable and secure state estimation in smart grid. IEEE SmartGrid- Comm2010, 2010.
[30] Z. Lu, X. Lu, W. Wang, and C. Wang. Review and evaluation of security threats on the communication networks in the smart grid. Military Communications Conference2010, 2010.
[31] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine. Design principles for power grid cyber-infrastructure authentication protocols .Hawaii International Conference on System Sciences, pages 1-9, 2010.
[32] Department of Energy, Office of Electricity Delivery and Energy Reliability. Study of security attributes of smart grid systems - current cyber security issues 2009, http://www.inl.gov/scada/publications/d/securing the smart grid current issues.pdf.

