IEEE Proceedings of the IEEE SoutheastCon 2015, April 9 - 12, 2015 - Fort Lauderdale, Florida

A Survey on Security Assessment of Metering Infrastructure in Smart Grid Systems

Arash Anzalchi, *Student Member, IEEE* and Arif Sarwat, *Member, IEEE*
Department of Electrical and Computer Engineering
Florida International University
Miami, USA

***Abstract*— Effective integration of renewable energy resources, energy management and better usage of the high voltage transmission system are major motivating forces for an improved electric grid regularly called the Smart Grid. Along with the soundless features of the Smart Grid, cyber security appears to be a serious issue because many electronic devices are connected via communication networks throughout critical power services, which has a direct impact on the reliability of such a common infrastructure. An assessment of cyber security topics in the Smart Grid is presented in this paper especially, security necessities of AMI, network vulnerabilities, attack countermeasures, secure communication protocols and architectures in the Smart Grid.**

Cyber-attacks against the power grid may aim to disrupt operations modifying or inserting messages. For example, malicious entities might change the set points at outstation devices, by pretending to be a master device at a control center, and cause instability in the grid. Satisfactory protection contains authenticating both the devices and control commands.

Keywords*— *Smart Grid, Advanced Metering Infrastructure (AMI), Cyber Security, cyber attack, Physical Attack

I. INTRODUCTION

COMPARED with traditional power systems, the Smart Grid is offered to fully integrate high-speed and two-way communication technologies [1] into many of power apparatus to create a dynamic and collaborating infrastructure with new energy management capabilities, such as advanced metering infrastructure (AMI) and demand response.

Though, such a dependency on information networking certainly exposes the Smart Grid to probable weaknesses associated with communications and networking systems. The objective of this paper is to provide a study of some potential cyber security threats, review existing security solutions, and summarize research experiments in the Smart Grid.

Unidentifiable attack in power system, which is a novel type of attack was discussed in [2]. In such an attack, the control center cannot get an assured state estimation, as there may be more than a few probable cases and the control center cannot just prefer one over the others. Additionally, reference [2] propose a three-step system that allows someone to find all possible circumstances under an unidentifiable attack, in which attack area was found in the beginning and later considerably lessen the search space when compared to the search space using directly the brute force search scheme.

An automated AMI configuration, authentication, identification and repair procedure that is applied with a tool called Smart Analyzer was introduced in [3]. Smart Analyzer describes various AMI system invariants and restrictions that are important for keeping safe AMI from some sorts of security threats. By means of these constraints and the AMI structure, a logic based formal model of AMI was created and then a Satisfiability Modulo Theory (SMT) solver was used to solve the constraint problem.

Sushmita Ruj and Amiya Nayak in [4] use homomorphic encryption technique to reach a modernized security structure for smart grids that could support data aggregation and access control. The customer data is sent to the substations where it is checked by Remote Terminal Units (RTU). Attribute-Based Encryption (ABE) was used as the suggested access control tool which gives selective access to customer data which is stored in databases and used by not the same smart grid users. Cryptographic keys distributed by several key distribution centers (KDC) and RTUs and users have attributes. RTUs sent data encoded under a set of attributes.

A combined intrusion detection solution to find malicious energy theft efforts in advanced metering infrastructures AMIDS is described in [5]. This solution uses various information sources to create an adequate amount of evidence about an attack which has just started before it makes an action as a malicious energy theft.

Integrated Authentication and Confidentiality (IAC) is proposed as a new protocol by Ye Yan et al. In [6] to provide well-organized, secure AMI communications in smart grid. An AMI, when using the IAC system, can offer trust services, data privacy, and integrity by mutual authentications at any time a new smart meter initiates and joins the smart grid AMI network. Data integrity and confidentiality are satisfied by message authentication and encryption services, using the corresponding keys created in mutual authentications.

Results of attacks to smart grid came in multiple forms is discussed in [7]. Amongst others, they consist of financial losses from not an optimal economic dispatch to load, robustness/resiliency losses by placing the grid at operating points that are at larger risk from contingencies, cascading failures made by poor operational points, differences in magnitude of load-generation and frequency abnormality and influences on market price. When the system operator answers back to compromised data by re-dispatching generation under

978-1-4673-7300-5/15/$31.00

normal or contingency protocols, data integrity attacks have consequences [7].

A survey on the confidentiality of information in the AMI involving nodes with mutually dependent security assets was done by Ziad Ismail et al. in [8]. In this survey, the defender can select one of several security modes accessible on each node.

II. ADVANCED METERING INFRASTRUCTURE (AMI)

Advanced Metering Infrastructure (AMI) is the essential module in a smart grid that exhibits a highly complex network formation. AMI consists of various cyber-physical components, which are connected through different communication media, protocols, and security measures. They use different data transfer methods and security policies [3]. The regular structure of an AMI network is presented in Fig. 1, which usually contains millions of smart meters, thousands of intelligent data collectors, and one or more headend systems as the main mechanisms. A meter creates a secure connection with a particular collector and reports energy consumption data periodically [3].

There are two data transfer methods, which can be used between the meter and collector, and between collector and headend: (i) push-driven mode in which a meter or a collector reports data periodically based on a pre-defined transfer plan, and (ii) pull-driven mode in which a meter or a collector sends data only when getting a request. In the real world, the push mode is used between the meter and collector, while the pull mode is used between collector and headend (Fig. 2) [3].

Recently there has been large numbers of nationwide AMI deployment effort, however, it has had quite a reverse outcome by fueling concerns about new ways to steal power, e.g., through remote smart meter. For example, a wide and organized energy theft attempt was reported to the FBI in 2009 that may have cost up 3 to 400 million dollars per annum to a utility behind an AMI utilization [5].

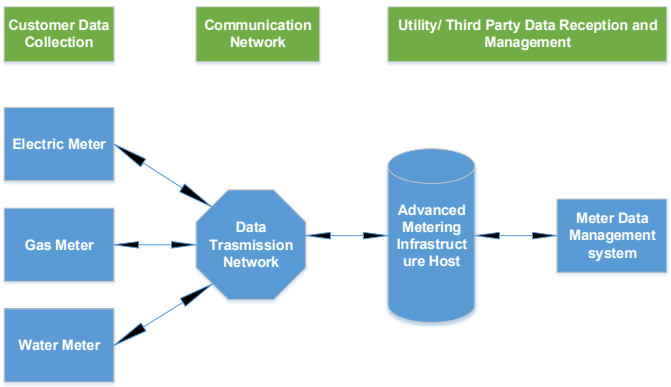

Fig 1. Typical AMI smart grid network

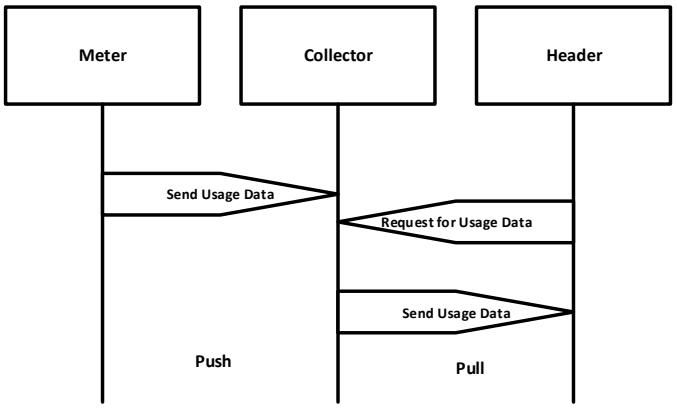

Fig. 2: Push and Pull modes in transferring data in Smart Grid

III. SECURITY CHALLENGES IN AMI:

When the number of smart meters proliferate, security issues related to the Smart Grid and AMI grow significantly from inside the system besides outside. If customers believe that their personal data is used against their determination, or they experience bad service or power quality because of outside manipulation of the system by unlicensed parties or hackers, then the execution of AMI is most likely resisted. Considering its influence, the security problem from three different aspects is discussed in this paper: maintaining the privacy of consumers' information, resilience of system against cyber or external attacks, and the power theft.

Unique security mechanisms are needed to ensure the integration, availability, and privacy of both meter reading data and management messages. In such security mechanisms, the cryptographic overhead, including digital certificates and signatures, is quite significant for an embedded device like a smart meter in smart grid AMI compared to normal personal computers in a regular enterprise network [6].

A. End users privacy

Smart meters also have unintentional consequences for customer privacy. Energy use information stored on the meter and distributed afterward performs as an information-rich side station, uncover end user habits and behaviors. History has revealed that where financial or political encouragements align, the approaches for mining behavioral data will progress fast to match the cravings of those who would exploit that information.

Utility companies aren't the only sources of possible privacy abuse. Real-time usage statistics from installing smart meters was received by the Google PowerMeter service. Customers who subscribed to the service receive a specially made web page that displays local usage. Although Google has not announced the final privacy policy for this facility yet, companies that were using this software had free access to this information for commercial purposes, such as marketing individual or aggregate usage data to third parties.

The customer has less control over the use of power information delivered to utility companies by Google PowerMeter service. Existing privacy laws in the US are in

general a mishmash of rules and guidelines. It is unclear how these or any laws apply to customer energy usage.

B. Security against external cyber or physical attacks:

Lots of security necessities in AMI are the same as those of regular IT networks; however, there are some distinctive security requirements that are represented below [9]:

- **Confidentiality:** Confidentiality can be translated as the privacy of customers' consumption configuration and information. To be more precise, unauthorized access to the data from other connected automated systems through gateways, physical theft of meter to access the stored data as well as customers access to other customers' information should be prohibited.
- **Integrity:** Hackers aim to check the unity of the organization, creating the authentication system believe they are authorized entities and issue instructions to execute their attacks.
- **Availability:** concerns differ based on the type of information communicated in the system. Sometimes it is important that the real values be collected in very short time intervals, e.g. every minute.
- **Accountability:** Since different components of an AMI system are usually manufactured by different companies and owned by various entities, i.e., Customers, service providers, etc., Accountability requirement is particularly a concern, Audit logs are the most accepted ways to ensure accountability; on the other hand, these audit logs are vulnerable themselves.

C. Power Theft:

If attackers could access the stored data of smart meter they would have ample control over the meter as the Time of Use rates, received or executed commands, event logs, consumption and time stamps, and the firmware dwell there [9].

Because AMI can use cryptography and authentication to communicate, hackers need to obtain encryption keys that are stored in the meter. If the authentication and encryption procedures or the integrity protocol of the meter and utility are not strong enough, attackers can use spoofing techniques to send their false request values or event log to the utility end. In the context of network security, a spoofing attack is a condition that one person or program effectively masquerades as another by faking data and thereby gaining an unlawful benefit. If the authentication process is faulty but an encrypted communication exists between meter and utility, then a node between meter and utility on the backhaul is needed by attacker to imitate meter for the utility and vice versa during the encoded communication to achieve cryptographic keys [9].

IV. COUNTERMEASURES:

A. Security of Protocols [10]:

It is important to know the threat environment in which the protocol is expected to operate and ensure that it is designed to be secure in such an environment. Some of the principles for security protocols are discussed below:

- **Explicit Names:** If the identity of a principle is essential to the meaning of a message, it is sensible to mention the principle's name clearly in the message.
- **Unique Encoding:** If an encrypting is used to for the meaning of a message, therefore it should be possible to tell which encoding is being used.
- **Use of Timestamps:** If timestamps are used by reference, then the difference between local clocks on various machines must be greatly less than the maximum age for a message to be thought valid.

B. Access control:

Access control is essential because there are sensitive information, which should be accessed only by designated group of people.

A new decentralized security framework for smart grids, integrating simultaneously privacy preserving aggregation and access control was used in [4]. Aggregation of data at gateway smart meters of Home Area Network (HAN), Building Area Network (BAN), and Neighborhood Area Network (NAN) is done using homomorphic encryption. Homomorphic encryption is a form of encryption which permits selected types of calculations to be executed on ciphertext and produce an encrypted outcome that, when decrypted, matches the result of processes performed on the plaintext [1]. Other encryption techniques like RSA, one of the first practicable public-key cryptosystems, encrypts a message with the public key of the receiver, such that the receiver can decrypt it using its secret key. The message is sent and received as is [4].

C. Confidentiality:

Integrated Authentication and Confidentiality (IAC) protocol uses mutual authentication between an isolated server situated in the local management office and a nearby smart meter as the authenticator to obtain correct cryptography keys for resulting secure data communications. Consequently, readings from smart meters and management messages from central SCADA and/or local management offices can exploit encryption and message authentication appliances custom-made for the security necessities and system restrictions [6].

In [8] the authors were able to derive the expected behavior of the attacker and the defender for two types of interactions between the players. Also sets of devices which after compromisation will be the most attractive for the attacker is presented. In a leader and follower game where the defender expects attacker's movements, it was resulting the minimum defense budget required and the ideal encryption rates on each device in the AMI in order to frustrate attacks.

V. CONCLUSION:

Cyber security in the Smart Grid is a new area of study that has attracted fast growing consideration in the government, industry and university. We presented a survey of security issues in the Smart Grid and consequences of using AMIs. Improved security for transferred information and delivered power is the most valuable advantage of AMI. Furthermore, AMI lets the users to control their consumption in a better pattern with higher power quality and stability.

REFERENCES

[1] Fang, Xi; Misra, Satyajayant; Xue, Guoliang; Yang, Dejun, "Smart Grid - The New and Improved Power Grid: A Survey," *Communications Surveys & Tutorials, IEEE* , vol.14, no.4, pp.944,980, Fourth Quarter 2012.

[2] Zhengrui Qin; Qun Li; Mooi-Choo Chuah, "Unidentifiable Attacks in Electric Power Systems," *Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on* , vol., no., pp.193,202, 17-19 April 2012.

[3] Rahman, M.A.; Al-Shaer, E.; Bera, P., "A Noninvasive Threat Analyzer for Advanced Metering Infrastructure in Smart Grid," *Smart Grid, IEEE Transactions on* , vol.4, no.1, pp.273,287, March 2013.

[4] Ruj, S.; Nayak, A., "A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids," *Smart Grid, IEEE Transactions on* , vol.4, no.1, pp.196,205, March 2013.

[5] McLaughlin, S.; Holbert, B.; Fawaz, A.; Berthier, R.; Zonouz, S., "A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures," *Selected Areas in Communications, IEEE Journal on* , vol.31, no.7, pp.1319,1330, July 2013.

[6] Ye Yan; Hu, R.Q.; Das, S.K.; Sharif, H.; Yi Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," *Network, IEEE* , vol.27, no.4, pp.64,71, July-August 2013.

[7] Giani A.; Bent R., "Addressing Smart Grid Cyber Security," *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, 2012.

[8] Ismail, Z.; Leneutre, J.; Bateman, D.; Lin Chen, "A Game Theoretical Analysis of Data Confidentiality Attacks on Smart-Grid AMI," *Selected Areas in Communications, IEEE Journal on* , vol.32, no.7, pp.1486,1499, July 2014.

[9] Ramyar Rashed Mohassel, Alan Fung, Farah Mohammadi, Kaamran Raahemifar, A survey on Advanced Metering Infrastructure, International Journal of Electrical Power & Energy Systems, Volume 63, December 2014, Pages 473-484, ISSN 0142-0615

[10] Khurana, H.; Bobba, R.; Yardley, T.; Agarwal, P.; Heine, E., "Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols," *System Sciences (HICSS), 2010 43rd Hawaii International Conference on* , vol., no., pp.1,10, 5-8 Jan. 2010.

[11] Wenye Wang, Zhuo Lu, Cyber security in the Smart Grid: Survey and challenges, Computer Networks, Volume 57, Issue 5, 7 April 2013, Pages 1344-1371, ISSN 1389-1286