Retraction

Retraction: Power Theft Recognition and data security in Smart Meter Reading of a Smart Grid (J. Phys.: Conf. Ser. 1916 012216)

Published 23 February 2022

This article (and all articles in the proceedings volume relating to the same conference) has been retracted by IOP Publishing following an extensive investigation in line with the COPE guidelines. This investigation has uncovered evidence of systematic manipulation of the publication process and considerable citation manipulation.

IOP Publishing respectfully requests that readers consider all work within this volume potentially unreliable, as the volume has not been through a credible peer review process.

IOP Publishing regrets that our usual quality checks did not identify these issues before publication, and have since put additional measures in place to try to prevent these issues from reoccurring. IOP Publishing wishes to credit anonymous whistleblowers and the Problematic Paper Screener [1] for bringing some of the above issues to our attention, prompting us to investigate further.

[1] Cabanac G, Labbé C and Magazinov A 2021 arXiv:2107.06751v1
Retraction published: 23 February 2022
Power Theft Recognition and data security in Smart Meter Reading of a Smart Grid

Vineeth V V¹, Ambrish V¹, Haricharan D V¹, Harshini V¹, Abilash C¹
¹Department of Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India.
vineethvv@skcet.ac.in

Abstract. Smart meter is an important component of smart grid environment has enormous features like precise measurement and possibility of two way communication among the entities involved in grid. Nevertheless, it has distinctive features like intricate structure, resource constriction and confidential sensitive data. These features make a meter structure more susceptible for attack and error. Power theft is identified as a major threat in meter infrastructure. Several literature has found to study this issue in detail because it poses a great threat to the overall grid architecture. This paper investigates the major thefts and threats in such an environment and identifies the essential safety prerequisites to be maintained by a smart meter. A risk model is identified using attack characteristics to figure out major risks. Different class of power theft detection mechanisms are analysed and reviewed to precisely define and understand the attack vulnerability in smart meters.

Keywords: Energy meter, Intrusion Detection, Power theft, Advanced metering infrastructure.

1. INTRODUCTION

In a grid infrastructure smart meter has a great task in dealing power and energy data associated with individual consumers of a grid. It facilitates bidirectional communication from home to grid and from grid to home. Common people can not only get data from meter but also can perform customized operations over it. This leads to the possibility of malicious attempts to tamper and change meter data. This leads to serious problems and one of the major problems in this regard is power theft attack. In this case, intruders or malicious attackers make use of meter data to steal energy power. Many theft cases are reported and thus to be considered seriously. Recognizing such stealing is difficult to the overall infrastructure of smart meter. This serious issue even affects the quick development of smart metering infrastructure. Lots of researches are in this area to effectively detect such attacks since they effectively aim at stealing power that is to be actually delivered to legitimate consumers.
Smart meters consist of a tree structure comprising of different networks in it. Networks by its nature are always susceptible for attacks mostly because of wireless nature. So an attack on meter can be carried out easily by the malicious users. Smart meter contains different data like power usage data, implementation data, personal data of end users, etc. In these types of data, attack is launched on power consumption data to steal power. Attackers can be either passive who just collect data without performing any modifications on it and the second category is active attackers who modifies the meter
data mainly for monetary benefits that is by way of stealing of power. Different categories of recognizing these types of attacks are done in this paper.

2. LITERATURE SURVEY

Many security problems are brought about by the changing connectivity and disconnection of several parts of metering infrastructure [1]. A secure authentication key could be propagated to have bidirectional communication links among various devices that aims at providing several security aspects in grid and meter. This key can use cryptographic functions and exchange of secure keys among entities that make use of good secure protocol standards. This helps in carrying out better security measures in authentication and also methods to use ideal shared key functionalities. The performance could be experimentally verified and compared with similar existing protocols. Smart meters are important active equipment in grid along with having numerous loop holes for attacks. Much number of vulnerabilities exists in the architecture. Petri net model can be used to analyze data flow between various equipments in meter [2]. Menace model could be used by considering different restrictions imposed on meter. Intrusion detection technique could be used for detecting any malicious activity in meter infrastructure. Data falsification can also be detected. Changing software of meter will not change this detection scheme.

Another development for smart meter security is a key supervision technique [3]. It is found to be high advance features. And this paper is significantly looking into managing key functions and ensuring security in smart meter. Comparison of general key supervision in ordinary meters and newly advanced metering infrastructure has also been analyzed in the paper.

3. RISK MODEL

A hierarchical arrangement is adopted as the risk model. This structure analyzes the possible ways by which an attacker can carry out the attack over meter data [4]. The attacker makes use of loop holes to enter the system and perform various malicious attempts to finally reach the actual target of attack. So it goes through children nodes to reach a root node which is its target [5]. The final target is power stealing. This target can be subdivided as tampering, modifying, etc. The attacker thus decompose target into sub targets and accomplish it one by one to get the final one. This risk model can effectively help to study the behavioural characteristics of an attacker who aims to steal power. This model can incorporate other sub structures if an attack is analyzed to have diversities in attack nature.

4. POWER THEFT PROCEDURES

The recognition of power stealing is difficult to identify compared to other attacks in smart grid. Mainly there are three kinds of recognition strategies, including, categorization based approach, monitoring state based approach and game theory based approach. In the categorization based approach, normal energy pattern is studied and then an abnormal usage of power is identified whenever such a case occurs [6]. This is based on the principle that there can be a significant difference in power usage pattern when an intruder tries to access and use power of legitimate consumers. In the second approach that is in monitoring state based approach the recognition is improved by considering the state of monitoring. This can be obtained using a wireless sensor network which is comparatively cheap. Logs for audit can be used here. RFID technology can also be used instead of wireless sensor network. But here there is extra cost for the installation of particular equipments. In the third approach, a model is constructed involving distributors and consumers along with attackers [7]. It will lead to identification of abnormal behaviour in a more stable way by way of intense calculations.
5. INSIGHT INTO UPCOMING THREATS

The recognition of attacker behaviour may need the storing of private confidential and sensitive data of end users [8]. Many of them do not take risk by revealing their real identities and sensitive data which makes the recognition difficult. Techniques for the security of physical equipments are also an issue. Cost involved in the data storage for analysis and recognition is yet another issue [9]. So these issues are to be properly dealt with in order to properly recognize attack scenarios in a smart meter.

6. CONCLUSION

A major problem regarding the implementation of smart grid is the attack scenarios associated with smart meters. The main problem identified is the stealing of power form such systems. Proper recognition of such attacks is very essential in order to come with effective solutions. Three recognition mechanisms are evaluated in the paper. Along with that, a proper insight into the challenges in this area is also identified. Once the problem of actual attack scenario is identified and eradicated, smart meters can be a promising and innovative mechanism for future generations.

Reference

[1] Abdullah Irfan, Syed Zuqadar Hassan, Rohan Ahmed, Irfan Ishaq, Amir Zahoor, Tasawar Murtaza, Muhammad Farhan Masood, Tariq Kamal, Muhammad Abbas Kha, ‘IoT Based Smart Meter’, Institute of Electrical and Electronics Engineers (IEEE), DOI:10.1109/ICIC48496.2019.8966684.
[2] Andreas Weigel, Christian Renner, Volker Turau, Holger Ernst, ‘Wireless sensor networks for smart metering’, Institute of Electrical and Electronics Engineers (IEEE), DOI:10.1109/ENERGYCON.2014.6850506.
[3] F. Abate, M. Carratu, C. Liguori, M. Ferro, V. Piciello, Smart meter for the IoT, Institute of Electrical and Electronics Engineers (IEEE), DOI: 10.1109/I2MTC.2018.8409838.
[4] S.G. Priyadharshini, C. Subramani, J. Preetha Roselyn, An IoT based smart metering development for energy management system, International Journal of Electrical and Computer Engineering (IJECE), 9(4), August 2019, pp. 3041–3050.
[5] H. Anandakumar and K. Umamaheswari, A bio-inspired swarm intelligence technique for social aware cognitive radio handovers, Computers & Electrical Engineering, vol. 71, pp. 925–937, Oct. 2018. doi:10.1016/j.compeleceng.2017.09.016
[6] R. Arulmurugan and H. Anandakumar, Early Detection of Lung Cancer Using Wavelet Feature Descriptor and Feed Forward Back Propagation Neural Networks Classifier, Lecture Notes in Computational Vision and Biomechanics, pp. 103–110, 2018. doi:10.1007/978-3-319-717678_9,
[7] Amrita Singh, Ravi Gupta, IoT based smart energy meter, International Journal of Advance Research and Development, 3(3).
[8] Andreas Weigel, Christian Renner, Volker Turau, Holger Ernst, Wireless sensor networks for smart metering, Research Gate Conference Paper, May 2014DOI:10.1109/ENERGYCON.2014.6850506.
[9] Sneha Chaudhari; Purvang Rathod; Ashfaque Shaikh; Darshan Vora; Jignesh Ahir, Smart energy meter using Arduino and GSM, Institute of Electrical and Electronics Engineers (IEEE), DOI: 10.1109/ICOEL.2017.8300772.