International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 24th Feb 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-02

Title: ABSI: A NEW APPROACH FOR METER INSPECTION IN SMART GRID

Volume 08, Issue 02, Pages: 143–147.

Paper Authors

MS.G.PRASHANTHI, Y.VENKATA GOPI KRISHNA

Vignan's Lara Institute of Technology & Science

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ABSI: A NEW APPROACH FOR METER INSPECTION IN SMART GRID

MS.G.PRASHANTHI[1], Y.VENKATA GOPI KRISHNA[2]
Assistant Professor[1], Department of M.C.A ,Vignan's Lara Institute of Technology & Science
M.C.A Student[2],Department of M.C.A ,Vignan's Lara Institute of Technology & Science

Abstract:
Electricity theft is a widespread problem that causes tremendous economical losses for all utility companies around the globe. As many countries struggle to update their antique power systems to emerging smart grids, more and more smart meters are deployed throughout the world. Compared with analog meters which can be tampered with by only physical attacks, smart meters can be manipulated by malicious users with both physical and cyber attacks for the purpose of stealing electricity. Thus, electricity theft will become even more serious in a smart grid than in a traditional power system if utility companies do not implement efficient solutions. The goal of this paper is to identify all malicious users in a neighborhood area in a smart grid within the shortest detection time. We propose an Adaptive Binary Splitting Inspection (ABSI) algorithm which adopts a group testing method to locate the malicious users. There are two considered inspection strategies in this paper: a scanning method in which users will be inspected individually, and a binary search method by which a specific number of users will be examined as a whole. During the inspection process of our proposed scheme, the inspection strategy as well as the number of users in the groups to be inspected is adaptively adjusted. Simulation results show that the proposed ABSI algorithm outperforms existing methods.

Introduction
Introduced to more and more countries, such as USA, Japan, and China [1, 2]. To make electrical grids "smart", a multitude of modern hardware and software techniques are integrated into power systems [3, 4]. For example, analog meters in traditional power systems are upgraded to digital smart meters, which have capabilities of computation, communication, and remote control [5–7]. Besides, a cyber layer is added to the metering system. Unfortunately, while these techniques bring us convenience and efficiency, they also enable malicious users to apply numerous new ways to steal electricity, where malicious users are referred as to the users stealing electricity.Compared to analog meters which can be tampered with by only physical attacks, such as directly tapping into power lines and bypassing energy meters, smart meters can also be manipulated with cyber attacks. It is reported that users with a moderate level of computer knowledge are able to hack into the digital chips of smart meters, with low-cost tools and software readily available on the Internet [8–10]. Another commonly used method to steal electricity is to bribe

employees in utility companies. These employees will then log into the electricity consumption database of their utility companies, and manipulate malicious users' readings to smaller numbers and even make them unregistered.

PURPOSE OF THE PROJECT

The purpose of cost saving, the authors in paper propose to install a limited number of inspectors for each neighborhood area network (NAN) where inspectors are actually enhanced smart meters with larger memory and stronger computation capability. Clearly, fewer inspectors inevitably suggest longer detection time of malicious users. With the goal of identifying all malicious users within the shortest detection time, a series of inspection methods based on logical binary trees are proposed in papers. Since we recently observe that the electricity theft detection issue has some common features with the group testing problem (which will be explained later), in this paper, we propose to apply a group testing method to electricity theft detection to locate malicious users. The proposed electricity theft detection method in this paper is called Adaptive Binary Splitting Inspection (ABSI) algorithm in which groups of users are tested together and the group size is changed dynamically during the testing process. There are two considered inspection strategies in this paper: a scanning method in which users will be inspected individually, and a binary search method by which a specific number of users will be examined as a whole. During the inspection process of our proposed scheme, the inspection strategy as well as the number of users in the groups to be inspected will be adaptively adjusted. The main contributions of this paper are highlighted as follows: First, we propose to apply a group testing method to electricity theft detection to locate malicious users in smart grid in which the inspection strategy as well as the number of users in the groups to be inspected is adaptively adjusted. Second, we provide the performance analysis of the ABSI algorithm, e.g., estimating the minimum upper bound of the number of malicious users and the maximum number of inspection steps (detection time). Third, simulations are conducted to evaluate the performance of the ABSI algorithm. Simulation results show that the proposed ABSI algorithm outperforms existing methods.

PROBLEMS EXISTING SYSTEM

A cyber layer is added to the metering system. Unfortunately, while these techniques bring us Convenience and efficiency, they also enable malicious users to apply numerous new ways to steal electricity, where malicious users are referred as to the users stealing electricity. Compared to analog meters which can be tampered with by only physical attacks, such as directly tapping into power lines and bypassing energy meters, smart meters can also be manipulated with cyber attacks. Almost all utility companies around the globe, especially those in many emerging market countries [11], suffer from electricity theft. Currently, according to a new study published by Northeast Group, LLC, the world loses $89:3 billion annually due to electricity theft, among which the top 50 emerging market countries lose $58:7 billion per year . The highest losses were in India

($16.2 billion), followed by Brazil ($10.5 billion) and Russia ($5.1 billion). It is said that 80% of worldwide electricity theft occurs in private dwellings and 20% on commercial and industrial premises. Provided that utility companies do not implement efficient solutions, electricity theft will become even more serious in smart grids than in traditional power systems.

Existing system:

A cyber layer is added to the metering system. Unfortunately, while these techniques bring us Convenience and efficiency, they also enable malicious users to apply numerous new ways to steal electricity, where malicious users are referred as to the users stealing electricity. Compared to analog meters which can be tampered with by only physical attacks, such as directly tapping into power lines and bypassing energy meters, smart meters can also be manipulated with cyber attacks. Almost all utility companies around the globe, especially those in many emerging market countries [11], suffer from electricity theft. Currently, according to a new study published by Northeast Group, LLC, the world loses $89:3 billion annually due to electricity theft, among which the top 50 emerging market countries lose $58:7 billion per year . The highest losses were in India ($16.2 billion), followed by Brazil ($10.5 billion) and Russia ($5.1 billion). It is said that 80% of worldwide electricity theft occurs in private dwellings and 20% on commercial and industrial premises. Provided that utility companies do not implement efficient solutions, electricity theft will become even more serious in smart grids than in traditional power systems.

Proposed system

The purpose of cost saving, the authors in paper propose to install a limited number of inspectors for each neighborhood area network (NAN) where inspectors are actually enhanced smart meters with larger memory and stronger computation capability. Clearly, fewer inspectors inevitably suggest longer detection time of malicious users. With the goal of identifying all malicious users within the shortest detection time, a series of inspection methods based on logical binary trees are proposed in papers. Since we recently observe that the electricity theft detection issue has some common features with the group testing problem (which will be explained later), in this paper, we propose to apply a group testing method to electricity theft detection to locate malicious users. The proposed electricity theft detection method in this paper is called Adaptive Binary Splitting Inspection (ABSI) algorithm in which groups of users are tested together and the group size is changed dynamically during the testing process. There are two considered inspection strategies in this paper: a scanning method in which users will be inspected individually, and a binary search method by which a specific number of users will be examined as a whole. During the inspection process of our proposed scheme, the inspection strategy as well as the number of users in the groups to be inspected will be adaptively adjusted. The main contributions of this paper are highlighted as follows: First, we propose to apply a group testing method to electricity

theft detection to locate malicious users in smart grid in which the inspection strategy as well as the number of users in the groups to be inspected is adaptively adjusted. Second, we provide the performance analysis of the ABSI algorithm, e.g., estimating the minimum upper bound of the number of malicious users and the maximum number of inspection steps (detection time). Third, simulations are conducted to evaluate the performance of the ABSI algorithm. Simulation results show that the proposed ABSI algorithm outperforms existing methods.

Modules:

1. **Adaptive Binary Splitting Inspection**
2. **The head inspector monitors all the users statically**
3. **The sub-inspectors can be effortlessly added into or removed from the inspector box**

Conclusion:

In this paper, we investigate the MMI problem whose goal is to identify all malicious users with the minimum number of inspection steps. We propose to apply the group testing method to address the MMI problem and we call our method the ABSI algorithm. During the inspection process, the ABSI algorithm adaptively adjusts the inspection strategies. Specifically, among the users which need to be further inspected, if one user out of an average number of at least two users is malicious, the binary search method will be applied; otherwise, the scanning method will be applied. Furthermore, based upon some assumptions, we demonstrate how to estimate the minimum upper bound of the number of malicious users in the NAN, which is the prerequisite for applying the ABSI algorithm. Moreover, we give out the maximum number of inspection steps of the ABSI algorithm. After obtaining the theoretical minimum number of inspection steps, we analyze how much improvement can be made over the ABSI algorithm. Simulation results show that the ABSI algorithm outperforms existing methods in some aspects. Specifically, the ABSI algorithms surpass the ATI algorithm in terms of the speed. Compared to the BCGI algorithm, the ABSI algorithm is a more general approach.

References

[1] I. Hosni and N. Hamdi, “Distributed cooperative spectrum sensing with wireless sensor network cluster architecture for smart grid communications,” International Journal of Sensor Networks, vol. 24, no. 2, pp. 118–124, 2017.

[2] M. Faisal and A. A. Cardenas, “Incomplete clustering of electricity consumption: an empirical analysis with industrial and residential datasets,” Cyber-Physical Systems, vol. 3, no. 1-4, pp. 42–65, 2017.

[3] S. Ma, Y. Yang, Y. Qian, H. Sharif, and M. Alahmad, “Energy harvesting for wireless sensor networks: applications and challenges in smart grid,” International Journal of Sensor Networks, vol. 21, no. 4, pp. 226–241, 2016.

[4] G. Xu, W. Yu, D. Griffith, N. Golmie, and P. Moulema, “Toward integrating distributed energy resources and storage devices in smart grid,” IEEE Internet of Things Journal, vol. 4, no. 1, pp. 192–204, Feb 2017.

[5] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," (Elsevier) Future Generation Computer Systems, vol. 28, no. 2, p. 391404, 2012.

[6] Z. Ling, K. Liu, Y. Xu, Y. Jin, and X. Fu, "An end-to-end view of iot security and privacy," in Proceedings of the 60th IEEE Global Communications Conference (Globecom), Singapore, December 4-8 2017.

[7] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: A case study of the smart plug system," IEEE Internet of Things Journal (IoT-J), 2017.

[8] B. Krebs. (2012) FBI: Smart meter hacks likely to spread. [Online]. Available: https://krebsonsecurity:com/2012/04/fbismart-meter-hacks-likely-to-spread/

[9] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 981 – 997, 2012.

[10] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," IEEE Transactions