Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Coded grouping-based inspection algorithms to detect malicious meters in neighborhood area smart grid

Xiaofang Xia[a,b,c], Yang Xiao[d,*], Wei Liang[a,b,*], Meng Zheng[a,b]

[a] Key Lab of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China
[b] Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China
[c] University of Chinese Academy of Sciences, Beijing 100049, China
[d] Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290, USA

ARTICLE INFO

Article history:
Received 28 September 2017
Revised 19 February 2018
Accepted 2 May 2018
Available online 11 May 2018

Keywords:
Smart grid
Malicious meter inspection
Theft of electricity
Grouping
Intrusion detection
Security

ABSTRACT

When modern hardware and software technologies are integrated into smart grid, numerous vulnerabilities are introduced at the same time. The vulnerabilities are now leveraged by malicious users for the purpose of electricity theft. Many approaches are proposed to identify malicious users. However, some of them have low detection rates; the others suffer from either low inspection speed or huge cost of deploying monitoring devices. In this paper, to accurately locate malicious users stealing electricity in a fast and economic way, we propose three novel inspection algorithms. First, Binary-Coded Grouping-based Inspection (BCGI) algorithm is proposed. Under some assumptions, it can locate malicious users with only one inspection step. Given n users, the BCGI algorithm requires $\Theta(\log_2(n))$ inspectors. Unfortunately, in some cases we do not have enough inspectors for the BCGI algorithm to work. To deal with these cases, we further propose two algorithms: M-ary Coded Grouping-based Inspection (MCGI) and Generalized BCGI (G-BCGI). In the MCGI algorithm, users' identification (ID) numbers are encoded into $(l+1)$-nary notations, where l is adaptively determined by the number of users and the number of available inspectors. It can locate malicious users within l inspection steps. In G-BCGI algorithm, users' IDs are encoded into binary notations, similar to the BCGI algorithm, and multiple rounds may be needed to locate malicious users. Experiment results show that the proposed algorithms can locate malicious users accurately and efficiently.

© 2018 Elsevier Ltd. All rights reserved.

1. Introduction

Compared to a traditional power system, a smart grid provides more reliable, economical, and environment-friendly energy management. Many countries are striving to establish their own smart grids (Faruqui et al., 2009). Nevertheless, each coin has two sides. Smart grid itself also has drawbacks (Wichmann, 2014). Many vulnerabilities are introduced when modern hardware and software technologies (e.g., advanced metering infrastructure and information and communication technologies) are integrated into smart grids (Liu et al., 2012). Among these vulnerabilities, the risk of security breaches garners the most attentions (Jow et al., 2017). Electricity theft is one special form of security breaches and has harassed the worldwide utility companies for a long time.

On the whole, electricity theft grows even more serious in smart grids. Apart from physical attacks such as directly

[*] Corresponding authors.
E-mail address: yangxiao@ieee.org (Y. Xiao).

https://doi.org/10.1016/j.cose.2018.05.004
0167-4048/© 2018 Elsevier Ltd. All rights reserved.

hooking from line and bypassing energy meters, malicious users can also launch various invisible cyber attacks to tamper with smart meters anytime and anywhere. The Federal Bureau of Investigation (FBI) warns that insiders and individuals with only a moderate level of computer knowledge are likely able to compromise meters with low-cost tools and software readily available on the Internet (Krebs, 2012).

Many negative and severe effects come with electricity theft. First, huge economic losses are brought to the utility companies, which are further spared to all the users. For example, the annual losses caused by electricity theft in UK amount to €500 million, putting extra €30 a year on individuals' bills (Arkell, 2014). Besides, it overloads the generation unit and drastically impinges on the power quality, resulting in users' electronics and appliances harmed and even damaged more easily. To top it all off, some malicious users (especially the ones adopting physical attacks) even lose their lives when trying to steal electricity.

Numerous approaches are proposed to detect electricity theft. In papers Jokar et al. (2016); Nagi et al. (2008, 2010); Nizar et al. (2008a,b); Pereira et al. (2013); Trevizan et al. (2015), various machine learning approaches, such as support vector machine and extreme learning machine, are applied to analyze users' load-profile information. The malicious users[1] are recognized as the ones who exhibit abnormal behaviors that are highly correlated with electricity theft. These approaches have a relatively low detection rate but a rather high false positive rate. In papers Bandim et al. (2003); Han and Xiao (2014, 2016a, 2016b, 2016c, 2017a, 2017b); Liu et al. (2014); McCary and Xiao (2017); Xia et al. (2015a, 2017, 2015b); Xiao et al. (2011, 2013a, 2013b), redundant monitoring devices (e.g., sensors and inspectors) are installed at the utility company side for detecting the malicious users. These approaches are able to identify the malicious users with absolute certainty. Nonetheless, the inspection speed or the cost issue becomes the major concern.

To address the above limitations, this paper first proposes a novel Binary-Coded Grouping-based Inspection (BCGI) algorithm. Under some assumptions, the BCGI algorithm is able to locate a malicious user by only one inspection step. It consists of two phases - a grouping phase and an inspecting phase. During the grouping phase, the users are grouped according to the binary notations of their identification numbers; and during the inspecting phase, the malicious users are identified in line with the inspectors' states. Given n users, the BCGI algorithm needs $\Theta(\log_2(n))$[2] inspectors. However, in some cases (e.g., when there are a lot of users in the smart grid, but very limited budget for installing inspectors), we do not have enough inspectors for the BCGI algorithm to work. To conquer the limitation of the BCGI algorithm, we propose two more algorithms: M-ary Coded Grouping-based Inspection (MCGI) and Generalized BCGI (G-BCGI). In the MCGI algorithm, users' IDs are encoded into $(l+1)$-nary notations, where l is adaptively determined by the total number of users and the number of available inspectors. For different inspection steps, users are regrouped based upon different digits (i.e., $0, 1, \ldots, l-1, l$) of the $(l+1)$-nary notations of users' ID numbers. The MCGI algorithm can locate a malicious user within l inspection steps. In the G-BCGI algorithm, users are allocated with unique ID numbers for different inspection steps. These ID numbers are then encoded into binary notations, according to which users are grouped. In essential, both the MCGI and G-BCGI algorithms are general forms of the BCGI algorithm. They can be used when we are short of inspectors for the BCGI algorithm to work. Theoretical analyses and experiment results show that the G-BCGI algorithm can locate malicious users more quickly than the MCGI algorithm. The contributions of this paper are highlighted as follows:

- First, we propose the BCGI algorithm, which can locate malicious users with only one inspection step under the assumption that there are $\Theta(\log_2(n))$ available inspectors, given n users;
- Next, to deal with the cases where we are short of inspectors for the BCGI algorithm to work, we propose the MCGI algorithm, which can locate malicious users within l inspection steps.
- Furthermore, we propose the G-BCGI algorithm, which is proved to be able to locate malicious users more quickly than the MCGI algorithm.
- In addition, theoretic analyses are provided on the performance of the BCGI, MCGI and G-BCGI algorithms;
- Finally, experiment results show that the proposed algorithms are efficient to locate the malicious users.

The rest of this paper is organized as follows. Section 2 reviews the related work. Section 3 defines the problem. We propose the BCGI algorithm in Section 4, and both the MCGI and G-BCGI algorithms in Section 5, with theoretical analyses and examples provided. In Section 6, experiment results are reported. The conclusion and the future work are presented in Section 7.

2. Related work

Smart Grid is one special kind of cyber-physical systems in which security becomes more complex since they normally involve both cyber and physical aspects (Chao Liu and Sarkar, 2017; Yucelen et al., 2016). In recent years, there are many published papers for detecting malicious meters. Among these works, the most popular ones are the various kinds of machine learning-based approaches (Jokar et al., 2016; Nagi et al., 2008, 2010; Nizar et al., 2008a, 2008b; Pereira et al., 2013; Trevizan et al., 2015), which usually involve training a classifier with a historical dataset and then applying it to find irregularities or deviations in the customer energy consumption profile. For instance, in paper Depuru et al. (2013) the simplified encoded data are classified into three classes to detect the malicious users, by applying both support vector machine and rule engine based algorithms. Similarly, the paper Nizar et al. (2008a) proposes an extreme learning machine-based approach to expose abnormal behaviors that are highly

[1] In this paper the terms "meter" and "user" are used interchangeably. Malicious users are referred to as the users stealing electricity by manipulating their own reported electricity consumptions to smaller values via cyber or physical attacks. If users do not steal electricity, they are called honest users.

[2] We write $f(n) = \Theta(g(n))$ if there exist constants $c, c' > 0$ such that, for large enough n, $cg(n) \leq f(n) \leq c'g(n)$.

Download English Version:

https://daneshyari.com/en/article/6883895

Download Persian Version:

https://daneshyari.com/article/6883895

Daneshyari.com