Computer Networks 000 (2016) 1–13

Contents lists available at ScienceDirect

Computer Networks

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

A novel detector to detect colluded non-technical loss frauds in smart grid

Wenlin Han[b], Yang Xiao[a,b,*]

[a] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[b] Department of Computer Science, the University of Alabama, Tuscaloosa, AL 35487-0290, USA

ARTICLE INFO

Article history:
Received 27 July 2016
Revised 11 September 2016
Accepted 18 October 2016
Available online xxx

Keywords:
Smart grid security
Smart meter
Non-technical loss
Colluded fraud
Malicious meter

ABSTRACT

A Non-Technical Loss (NTL) fraud occurs when a fraudster tampers with a smart meter so that the meter registers less electricity consumption than the actual consumed amount, and therefore the utility becomes the victim who suffers the corresponding economic loss. In the literature, many detection schemes have been proposed to detect NTL frauds. However, some NTL frauds are far more complicated than what the existing schemes expect. We recently discovered a new potential type of frauds, a variant of NTL frauds, called Colluded Non-Technical Loss (CNTL) frauds in the Smart Grid. In a CNTL fraud, multiple fraudsters can co-exist or collaborate to commit the fraud. Existing detection schemes cannot detect CNTL frauds since these methods do not consider the co-existing or collaborating fraudsters, and therefore cannot distinguish one from many fraudsters. In this paper, we propose a CNTL fraud detector to detect CNTL frauds. The proposed method can quickly detect a tampered meter based on recursive least squares. After identifying the tampered meter, the proposed scheme can detect different fraudsters using mathematical models. Our experiments show that our method is effective in detecting CNTL frauds.

1. Introduction

Smart Grid is the new generation of power grid with two-way electricity flows and two-way communication links [1,2]. The system losses in Smart Grid can be classified into two types [3]: technical loss and non-technical loss. Technical loss is the loss during the generation, transmission, distribution, and redistribution processes, and it is due to the loss of energy in power lines, transformers, and other devices. Generally, Non-Technical Loss (NTL) is referred as to the loss other than technical loss, including unpaid bills, electricity theft, inaccurate metering, etc. An NTL fraud occurs when a fraudster tampers with a smart meter so that the meter registers less electricity consumption than the actual consumed amount, and this causes non-technical loss to the utility [4,5].

Utility companies have experienced huge economic loss because of NTL frauds. NTL frauds cause yearly $89.3bn economic loss world-wide as reported by Northeast Group LLC [6]. Among the $89.3bn loss, $58.7bn loss is reported in the 50 emerging market countries, including India, China, etc. These 50 countries planned an investment of totally $168bn to make Smart Grid more reliable and to reduce NTL frauds. In the U.S., the annual loss due to NTL frauds is $6bn, and it is reported by law enforcement in Houston that probably 60%–70% of meters have been tampered with [7].

NTL frauds not only exist in Smart Grid, but also in the old power grid [8]. In the traditional power grid, people have a long history of using physical methods to steal electricity [3,9]. A typical method is to use an additional power line to bypass a meter. Smart Grid brings novel technologies to the power grid. However, when meters become electronic and smart, there are much more ways to commit an NTL fraud. Examples are given as follows: smart meters could be remotely controlled [10]; the communication between the meters and the utility could be intercepted; moreover, those physical methods can be still applied in Smart Grid.

Traditional NTL fraud detection methods attempt to identify a tampered meter or multiple tampered meters among meters [11,12]. However, an NTL fraud can be very sophisticated. In our recent studies, we discovered a new potential type of frauds, a variant of NTL frauds, called Colluded Non-Technical Loss (CNTL) frauds in the Smart Grid. In a CNTL fraud, more than one fraudster can co-exist or collaborate to commit the fraud. In other words, in a single tampered meter, there are multiple fraudsters. They may not realize the existence of other fraudsters, and we call them co-existing fraudsters. On the other hand, they may realize the existence of other fraudsters and collaborate to commit an NTL fraud, and then we call them collaborating fraudsters. We study the behaviors of

* Corresponding author.
E-mail addresses: whan2@crimson.ua.edu (W. Han), yangxiao@ieee.org (Y. Xiao).

http://dx.doi.org/10.1016/j.comnet.2016.10.011
1389-1286/

the co-existing and collaborating fraudsters and analyze the features of CNTL frauds. We classify CNTL frauds into four types: segmented CNTL frauds, fully overlapped CNTL frauds, partially overlapped CNTL frauds, and combined CNTL frauds.

To combat NTL frauds, many schemes have been proposed including intrusion detection based methods [13–16], industrial control based methods [17,18], physical methods [19–22], profiling based methods [23,24], statistical methods [25,26] and comparison based methods [3,11,27–30]. These schemes can detect NTL frauds and identify the tampered meters, but they cannot detect CNTL frauds since these methods do not consider the co-existing or collaborating fraudsters, and therefore cannot distinguish one from many fraudsters.

In this paper, a novel detector, called Colluded Non-Technical Loss Fraud Detection (CNFD), is proposed to address the CNTL fraud problem in Smart Grid. CNFD has two steps to detect CNTL frauds: (1) NTL fraud detection and (2) fraudster differentiation. In the NTL fraud detection step, CNFD quickly identifies the tampered meter within a group of meters. In the fraudster differentiation step, CNFD differentiates multiple fraudsters in the tampered meter. CNFD adapts Recursive Least Square (RLS) [31] to model fraudsters' behaviors using linear functions. Different fraudsters have different models to represent themselves. CNFD is lightweight and requires only a small amount of data. CNFD can even predict the behaviors of fraudsters which they may not realize by themselves. We have conducted various experiments to test the effectiveness and performance of CNFD. The experimental results show that CNFD can effectively detect four types of CNTL frauds and describe the behaviors of different fraudsters clearly.

The main contributions of this paper include:

- We recently discovered a potential type of frauds in Smart Gird, called the CNTL frauds;
- We study the features of different CNTL frauds and categorize them into four types;
- We propose a novel detector CNFD to detect CNTL frauds in Smart Grid;
- Our experiments show that CNFD is effective.

The rest of the paper is organized as follows. The problem definition, the CNTL attack model, and the four types of CNTL frauds are introduced in Section 2. In Section 3, we introduce the CNFD algorithm. In Section 4, experiments and experimental results are presented to show the effectiveness of CNFD. In Section 5, we introduce related works and conclude the paper in Section 6.

2. Colluded NTL fraud

In this section, we first define the problem that we are trying to solve, and then present the attack model of CNTL frauds. Furthermore, detailed analysis on the features of these frauds is then presented, and based on the analysis, we classify CNTL frauds into four types.

2.1. Problem definition

Alabama Power, a utility company headquartered in Birmingham, is responsible for providing electricity service for southern Alabama where Alabama is a state located in the southeast (SEC) region of USA. Consider a community with N households in total served by Alabama Power. As shown in Fig. 1, these households have smart meters installed outside their houses, and each household has one smart meter. Some households may have multiple meters, but there is always one meter that is responsible for recording the total energy consumption and providing data for the billing purpose. Alabama Power keeps records of the total amount of electricity supplied to this community. However, the total billed amount is always smaller than the supplied amount if there are some compromised meters.

Alabama Power checks technical problems during the transmission and distribution processes. Electricity losses of power lines and transformers are deducted from the total loss. But the amount of loss is still large. Alabama Power suspects that at least one meter was tampered with in this community, and one or more than one customer are fraudsters who stole electricity. The problem is how to identify the tampered meters and fraudsters.

In this paper, we only consider the case that the total billed amount is smaller than the consumed amount, i.e., it is an NTL fraud; we do not consider the case that the total billed amount is larger than the consumed amount, i.e., it is not an NTL fraud.

2.2. Attack model

There are two types of fraudsters in general: inside fraudsters (fraudsters inside the households) and outside fraudsters (fraudsters outside the households). Inside fraudsters have the ability to physically tamper with smart meters, such as slowing down the meters using magnets. They also have the ability to impersonate smart meters using simulation software or overwrite the firmware of the meters. Outside fraudsters have the ability to remotely control smart meters, intercept the communication between smart meters and head-end systems in the utility, and extract encryption keys or passwords from network traffic. If the fraudsters are from the outside, the owner of the tampered meter may not realize the fraud. In a single tampered meter, the outside fraudsters and the inside fraudsters may co-exist.

As shown in Fig. 1, some smart meters are normal, while some other smart meters are tampered with. In a tampered meter, there may be one or multiple fraudsters. Collaborating fraudsters are those fraudsters who cooperate with each other to tamper with a meter and are aware of the existence of other fraudsters. Co-existing fraudsters are those fraudsters in a single tampered meter who just co-exist and are not aware of the existence of other fraudsters. Typically, collaborating fraudsters are either from the outside or from the inside. It is not common for the inside fraudsters to collaborate with the outside fraudsters. But for co-existing fraudsters, inside fraudsters may co-exist with outside fraudsters.

2.3. Colluded NTL fraud

A CNTL fraud occurs when multiple fraudsters tamper with a meter so that the meter records less electricity than the consumed amount by the household, and the fraudsters gain illegal benefit by paying less money. After further analyzing these fraudsters, we find that they have different behaviors which they may not realize themselves. Moreover, the behaviors of how they collude the frauds can be different.

Sometimes, when a meter is tampered with by multiple fraudsters, these fraudsters may commit the malicious manipulation at different time segments. As shown in Fig. 2(a), we name this kind of CNTL frauds as segmented CNTL frauds. In a segmented CNTL fraud, fraudsters usually do not realize the existence of other fraudsters. Thus, these fraudsters are co-existing fraudsters, and are not collaborating fraudsters.

During most of the time, CNTL frauds are not segmented. Different fraudsters can manipulate the same meter at the same time, or at least part of the manipulation time overlaps. We call this kind of colluded NTL frauds as overlapped CNTL frauds. Overlapped CNTL frauds can be classified into partially overlapped CNTL frauds and fully overlapped CNTL frauds, as shown in Fig. 2(b) and (c), respectively. The difference between partially overlapped CNTL and fully overlapped CNTL is that there is one fraudster who overlaps all other fraudsters in a fully overlapped CNTL fraud. This feature

Please cite this article as: W. Han, Y. Xiao, A novel detector to detect colluded non-technical loss frauds in smart grid, Computer Networks (2016), http://dx.doi.org/10.1016/j.comnet.2016.10.011