This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

A Control Chart based Detector for Small-amount Electricity Theft (SET) Attack in Smart Grids

Xiaofang Xia, *Member, IEEE,* Jian Lin, Yang Xiao, *Fellow, IEEE,* Jiangtao Cui, *Member, IEEE*, Yanguo Peng, *Member, IEEE*, Yong Ma

***Abstract*—For achieving the goal of two-way communication and power flows, smart grids are integrated with much state-of-the-art hardware and software. However, these newly added components also introduce a lot of vulnerabilities into the power systems, which results in that malicious users can launch various cyber-physical attacks to steal electricity. Existing electricity theft detection techniques suffer from an implicit assumption that malicious users tamper with smart meter readings to values much less than their actual electricity consumptions. These are called Large-amount Electricity Theft (LET) attacks. Nevertheless, in the real world, some malicious users may be cautious enough to deliberately launch Small-amount Electricity Theft (SET) attacks where smart meter readings are manipulated to numbers slightly lower than actual values, mainly to escape detection. To address this limitation, we propose a detector able to deal with both LET and SET attacks effectively. This detector applies a cumulative sum (CUSUM) control chart and a Shewhart control chart together to analyze users' reported readings and measurements of a central observer meter. It consists of an electricity theft detection phase which aims to detect the existence of LET/SET attacks timely and a malicious user identification phase which aims to identify malicious users exactly. Extensive experiments are conducted to evaluate the proposed detector, and the results show that it has good performance in terms of several metrics.**

***Index Terms*—Internet of Things (IOTs), Electricity theft, smart grid, anomaly detection, malicious users identification, control charts.**

I. Introduction

With electricity demand increasing rapidly over decades, power systems which were built over one century ago are operating at an overload [1, 2]. Consequently, people around the world are experiencing exponentially increasing power outages [3]. To better satisfying users' power demands and simultaneously reducing carbon dioxide emissions, many countries like the USA, Japan, and China are making every effort to establish their own smart grids [4]. This new generation of power systems is promised to provide two-way communication and power flows between users and utility companies. For achieving this goal, many Internet of Things hardware (e.g., smart meters) and software (e.g., a cyber layer for metering systems) are integrated into smart grids. This introduces many potential vulnerabilities into the power systems [5]. By leveraging these vulnerabilities, malicious users can launch various cyber-physical attacks against electronic devices and communication networks in smart grids.

One main purpose of these malicious users is to steal electricity, mainly by launching cyberattacks (e.g., man-in-the-middle attacks) or physical attacks (e.g., bypassing meters) to tamper with meter readings into smaller numbers. Compared to physical attacks, cyber-attacks are usually more covert and flexible and can be launched almost anywhere and any time. Electricity theft has many negative effects. First, it incurs huge economical losses for worldwide utility companies, which amounts to $89.3 billion and $96 billion in 2014 and 2017, respectively [6, 7]. These economical losses are passed on to all the users, by charging all customers with higher tariffs for the electricity services. It is reported that each customer in the UK has to pay an extra €30 for electricity theft [8]. If electricity theft is pervasive in a region (e.g., India), many power quality problems such as brownouts and blackouts will appear more frequently, which can seriously harm users' electrical appliances.

Many countries issue-specific laws to punish users' electricity theft behaviors. For example, the Theft Act 1968 in the UK says that malicious users are liable to imprisonment for a term not exceeding five years [9]. As reported, from 2014 to 2016, in Northern Ireland, a total number of 354 people were convicted on charges for electricity theft, among which nearly 50 people were imprisoned [10]. However, due to factors such as poverty and illiteracy, electricity theft can still be found in almost every region throughout the world. For example, in some areas of Northern Ireland, as many as six out of every 10 meters are tampered [10]. The Energy and Minerals Regulatory Commission in Jordan says that 8,836 electricity thefts in total are documented during the first half of 2019 [11]. According to Netbeheer Nederland, the illegal cannabis farms discovered and closed down in the Netherlands in 2019 steal a total of around 60 million euros in electricity [12]. In March 2020, police in California also bust three illicit marijuana grow-ops which have stolen electricity which is worth approximately $120,000, $88,000, and $11,000, respectively [13].

To prevent users from stealing electricity, many detection techniques have been developed, which can be roughly classified into machine learning-based and measurement mismatch-based methods. The basic idea of the former category is to apply various machine learning methods such as support vector machine and artificial neural networks to analyze users' load profiles, aiming to find abnormal electricity consumption patterns that are highly related to electricity theft [14–17].

Xiaofang Xia, Jian Lin, Jiangtao Cui, and Yanguo Peng are with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China.

Yang Xiao is with the Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487-0290, USA.

Yong Ma is with the College of Computer Information Engineering, Jiangxi Normal University, Nanchang 330022, China.

The co-corresponding authors: Yang Xiao and Jiangtao Cui, emails: yangxiao@ieee.org, cuijt@xidian.edu.cn

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

In contrast, the measurement mismatch based detection techniques require to deploy some advanced sensors in distribution networks [18–23]. By comparing measurements from advanced sensors with summations of reported readings of users under investigation, the search zone of electricity theft can be gradually narrowed down until all malicious users are identified.

Existing detection techniques have a limitation in that they implicitly assume that malicious users' reported readings are much less than their actual electricity consumptions. These attacks are called Large-amount Electricity Theft (LET) attacks in this paper. Nevertheless, in the real world, some malicious users may deliberately tamper with meter readings to values just a little smaller than the actual values, which is called Small-amount Electricity Theft (SET) attacks, to escape detection. Since existing detection techniques do not consider SET attacks when they are originally designed, their performance undoubtedly degrades drastically or even is not effective under SET attacks. In this paper, to address the above limitation, we aim to develop a detector that can effectively detect both LET and SET attacks.

The cumulative sum (CUSUM) and the Shewhart control charts are two commonly used statistical tools for change detection. Both of them have a centerline as well as two control limits. The CUSUM control chart plots the cumulative sum of deviations between sample values and a target value of a process variable of interest in time order. If the cumulative sum of deviations exceeds one of the two control limits, the CUSUM control chart claims that this process variable is affected by some special causes of variation. Since the CUSUM control chart incorporates all the information contained in multiple consecutive samples, it can efficiently detect small changes in the process [24]. Thus, it is applied to detect the SET attacks. In contrast, the Shewhart control chart simply plots the sample values of the process variable of interest in time order. If the last sample value exceeds one of its control limits, it claims that this process variable is affected by some special causes of variation. Since the Shewhart control chart uses only information in one sample and ignores other information given by the entire sequence of samples, it is insensitive to detect small changes but can detect large changes in a process more quickly than the CUSUM control chart [24]. Thus, the Shewhart control chart is employed to detect LET attacks. To sum up, we in this paper propose an electricity theft detector in which the Shewhart and the CUSUM control charts are mainly used to detect LET attacks and SET attacks, respectively.

Following papers [22, 23], we assume that a central observer meter is installed in a community to measure the total amount of electricity supplied to all users. The proposed detector consists of an electricity theft detection phase and a malicious user identification phase. In both phases, the control charts' parameters need to be first estimated based upon historical readings of smart meters and measurements of the central observer meter. In the electricity theft detection phase, the goal is to detect the existence of electricity theft. In this phase, the Shewhart and the CUSUM control charts are applied to analyze the difference between the central observer meter's measurements and the summation of users' reported readings. If the Shewhart control chart detects reading anomalies, it indicates the existence of at least one malicious user launching LET attacks and/or several malicious users launching SET attacks. If the CUSUM control chart detects reading anomalies, it indicates the existence of at least one malicious user launching SET attacks. About the malicious user identification phase, it aims to locate malicious users exactly. In this phase, the above two control charts are combined to analyze every user's daily electricity consumption. On the whole, if the Shewhart/CUSUM control chart detects reading anomalies, the corresponding user is a malicious user launching LET/SET attacks. Contributions of this paper are highlighted as follows:

- To the best of our knowledge, it is the first work that considers SET attacks in electricity theft detection. For better understanding SET attacks, we conduct analyses regarding how malicious users launch SET attacks when a central observer meter is installed in a community;
- We propose an electricity theft detector in which the Shewhart and the CUSUM control charts are jointly used. The proposed detector not only can detect the existence of LET and SET attacks timely but also can locate malicious users exactly;
- We provide theoretical performance analysis for the proposed detector, mainly by modeling the detection process as a Markov chain;
- Extensive experiments are conducted to evaluate the proposed detector. Results show that it has good performance in terms of several metrics.

The remainder of this paper is organized as follows. In Section II, we introduce related works regarding electricity theft detection techniques and provide some preliminaries of the Shewhart and the CUSUM control charts. In Section III, we define the problem and analyze how SET attacks are conducted. In Section IV, we present how the detector works. In Section V, we provide algorithm analysis about the proposed detector. In Section VI, the experimental results are reported. We conclude this paper in Section VII.

II. Related works & Preliminaries

A. Related works on electricity theft detection

In this section, we review related works regarding electricity theft detection techniques. As aforementioned, these works can be roughly classified into machine learning-based and measurement mismatch-based detection techniques.

The machine learning-based detection techniques are essentially various classifiers whose inputs are features extracted from users' load profiles, prior records, and other information (such as geographical locations and tariff categories) [25] and outputs are a list of adversaries that are highly suspected to commit electricity theft [14–17]. For example, the authors in [15] integrate a decision tree and a support vector machine (SVM) to detect electricity theft. The decision tree outputs users' expected electricity consumptions, which are further used as an input of the SVM for reducing false-positive rates. The authors in [16] apply a deep and wide conventional neural network for electricity theft detection, where the wide component captures global knowledge of users' electricity consumption data, and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

the deep component accurately identifies the non-periodicity of electricity theft and the periodicity of normal electricity usages.

However, existing machine learning-based detection techniques suffer from the following two issues: (1) data imbalance, which means that among the collected samples, the number of abnormal samples of malicious users is significantly lower than those of benign samples of honest users [14]; (2) non-malicious factors, which mainly include normal moving in/out of residents, replacement of electrical appliances, and change of seasonality [14]. Due to the above two issues, existing machine learning-based detection techniques usually have a relatively low detection rate, but a relatively high false-positive rate [26].

About power-measurement-based methods, they usually require to install some advanced sensors in the distribution networks to monitor whether users are consuming their electricity abnormally [18–23]. For example, in [22, 23], the authors propose to install a central observer meter to register the total amount of electricity supplied to all users in a neighborhood area network. Relationships between users' actual electricity consumptions and reported readings are modeled by linear or non-linear functions, called users' behavior functions [22]. Since the central observer meter's measurements are approximately equal to the summation of users' actual electricity consumptions, the measurements are further related with users' reported readings via a linear or non-linear system of equations. By solving this system of equations, these detection techniques can find out how much users' reported readings deviate from their actual electricity consumptions.

Compared to machine learning-based detection techniques, measurement mismatch-based detection techniques usually have higher detection rates and lower false-positive rates, with a trade-off of higher deployment costs for installing advanced sensors. However, both of the above two categories of detection techniques implicitly assume that malicious users manipulate electricity consumption to values far less than the actual values. This implies that these detection techniques are initially designed to detect LET attacks and that their performance undoubtedly degrades a lot when used for detecting SET attacks.

To address this limitation, in this paper, we apply the CUSUM control chart, which can effectively detect small changes in a process to detect the SET attacks. Since the Shewhart control chart can detect large changes in a process more quickly than the CUSUM control chart, it is applied to detect LET attacks. Although the CUSUM or the Shewhart control charts have been applied in many fields such as freeway incident detection [27] and intrusion detection [28], to the best of our knowledge, they are first used in electricity theft detection. The above two control charts are used to analyze measurements from a central observer meter and readings reported from users' smart meters to detect electricity theft and locate malicious users.

B. Preliminaries of control charts

For better understanding, in this section, we introduce some preliminaries of the Shewhart and the CUSUM control charts,

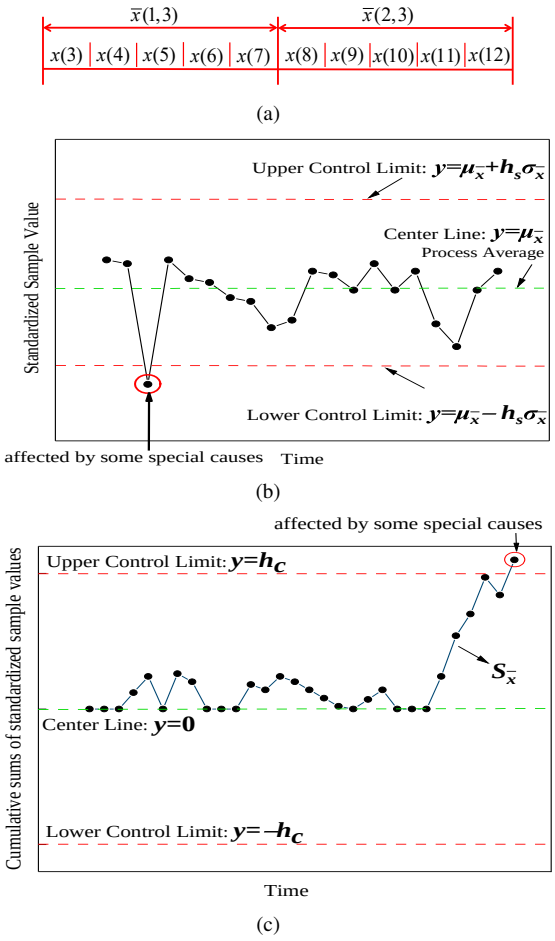


Fig. 1. An illustration of a Shewhart control chart and a CUSUM control chart: (a) samples of x are divided into subgroups of equal size; (b) a typical Shewhart control char; (c) a typical standardized CUSUM control chart.

which are two typical statistical tools to determine whether a process variable of interest, denoted by x, is affected by some special causes of variation or not. As shown in Fig. 1, both the Shewhart and the CUSUM control chart contain a centerline, an upper control limit, and a lower control limit, explained later.

We do not make any assumption regarding the distribution of the process variable x. Assume that samples of x are obtained periodically. Specifically, we use $x(j)$ to denote the sample of x at period j, with $j = 1, 2, 3, \cdots$. Let m_x denote the size of subgroups into which consecutive samples of x are divided. As shown in Fig. 1(a), we set $m_x = 5$. We denote by $\bar{x}$ the average of samples of x in one subgroup. According to the central limit theorem [29], provided that the process variable x follows a certain distribution with mean μ_x and variance σ_x^2 and that m_x is large enough, the sample average $\bar{x}$ approximately follows a normal distribution with mean $\mu_{\bar{x}} = \mu_x$ and $\sigma_{\bar{x}} = \frac{\sigma_x^2}{m_x}$. As pointed out in [24], in most cases, when m_x equals 4 or 5, it is sufficient to ensure reasonable robustness to the normal distribution assumption [30].

Assume that samples of x after the j-th period are divided into subgroups. For example, in Fig. 1(a), samples of x after the 3rd period, i.e., $x(3), x(4), \cdots, x(12)$, are divided into

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

two subgroups, with the first subgroup containing the first five samples (i.e., $x(3), x(4), \cdots, x(7)$) and the second subgroup containing the last five samples (i.e., $x(8), x(9), \cdots, x(12)$). Apparently, the k-th subgroup contains the following samples: $x(j+(k-1)m_x), x(j+(k-1)m_x+1), \cdots, x(j+km_x-1)$, whose average, denoted by $\bar{x}(k,j)$, is calculated as

$$\bar{x}(k,j) = \frac{1}{m_x} \sum_{t=j+(k-1)m_x}^{j+km_x-1} x(t). \quad (1)$$

For example, in Fig. 1(a), the averages of the first and the second subgroups of samples are $\bar{x}(1,3) = \frac{1}{5}\sum_{t=3}^{7} x(t)$ and $\bar{x}(2,3) = \frac{1}{5}\sum_{t=8}^{12} x(t)$, respectively. Note that values of $\bar{x}(k,j)$ are regarded as samples of $\bar{x}$.

Shewhart control chart: As shown in Fig. 1(b), in a Shewhart control chart, the samples of $\bar{x}$ are plotted in a time order. The center line, the upper control limit, and the lower control limit are the lines $y = \mu_{\bar{x}}$, $y = \mu_{\bar{x}} + h_s\sigma_{\bar{x}}$, and $y = \mu_{\bar{x}} - h_s\sigma_{\bar{x}}$ on a coordinate plane, respectively, where h_s is the distance of control limits from the center line, expressed in multiples of standard deviation of $\bar{x}$ (i.e., $\sigma_{\bar{x}}$) [24]. When the Shewhart control chart is used independently, it is customary to choose $h_s = 3$ [24]. If all samples of $\bar{x}$ fall between the line $y = \mu_{\bar{x}} + h_s\sigma_{\bar{x}}$ and the line $y = \mu_{\bar{x}} - h_s\sigma_{\bar{x}}$, the process variable x is unaffected by some special causes of variation. Otherwise, if one or more samples are plotted beyond one of the above two control limits, the process variable x is considered to be affected by some special causes of variation [24].

CUSUM control chart: Let $S_{\bar{x}}(k,j)$ denote cumulative sum of deviations between the first to the k-th samples of $\bar{x}$ after period j (i.e., $\bar{x}(1,j), \bar{x}(2,j), \ldots, \bar{x}(k,j)$) and the target value $\mu_{\bar{x}}$, expressed in units of $\sigma_{\bar{x}}$. If we need to detect positive changes (which mean that with time going by, values of sample averages $\bar{x}$ tend to increase), $S_{\bar{x}}(k,j)$ is calculated as

$$S_{\bar{x}}(k,j) = \max\left[0, \frac{\bar{x}(k,j) - \mu_{\bar{x}}}{\sigma_{\bar{x}}} - l + S_{\bar{x}}(k-1,j)\right], \quad (2)$$

where $\max[a,b]$ returns the maximum between numbers a and b. The constant l is called a reference value, which is often set to one half of the magnitude of the change to be detected in units of $\sigma_{\bar{x}}$ [24]. For example, if we set $l = 0.5$, then when the mean of the normal distribution followed by $\bar{x}$ changes from $\mu_{\bar{x}}$ to $\mu_{\bar{x}} + \sigma_{\bar{x}}$, the CUSUM control chart can detect it. On the other hand, if we need to detect negative changes (which mean that with time going by, the values of sample averages $\bar{x}$ have a tendency to decrease), we need to put a negative sign "$-$" before the standardized term $\frac{\bar{x}(k,j)-\mu_{\bar{x}}}{\sigma_{\bar{x}}}$ for calculating $S_{\bar{x}}(k,j)$.

In a standardized CUSUM control chart, the cumulative sum $S_{\bar{x}}(k,j)$ is plotted in a time order, as shown in Fig. 1(c). The center line, the upper control limit, and the lower control limit of the CUSUM control chart are the lines $y = 0$, $y = h_c$, and $y = -h_c$, respectively, where h_c is a user-defined decision interval. In applications, if the CUSUM control chart is used independently, we typically set $h_c = 5$ [24]. If $S_{\bar{x}}(k,j)$ exceeds h_c, then the process variable of interest x is affected by some special causes of variation; otherwise, x is not affected by any special causes of variation. If the starting value $S_{\bar{x}}(0,j)$ is set as zero, the CUSUM control chart is called a standard one. Otherwise, if $S_{\bar{x}}(0,j)$ is set as a non-zero value, the CUSUM control chart is called a fast initial response (FIR) one [24].

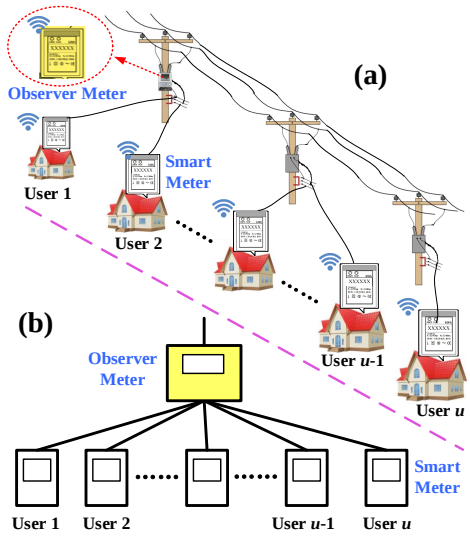


Fig. 2. A simplified architecture of smart grid in a community.

To conclude, the CUSUM control chart incorporates all the information contained in multiple consecutive samples of $\bar{x}$. Thus, it is sensitive to detect the occurrence of small changes in the process [24]. In contrast, the Shewhart control chart uses only information contained in the last sample of $\bar{x}$ and ignores other information given by the entire sequence of samples. Thus, it is relatively insensitive to detect small changes in the process [24]. Also, the Shewhart control chart has the advantage that it usually can detect large changes more quickly than the CUSUM control chart [24]. Hence, in applications, the CUSUM control chart is usually applied to detect small changes in the process, while the Shewhart control chart is usually applied to detect large changes in the process [24]. Finally, we summarize the main notations in this paper in Table I. Note that in real applications, for different scenarios, the process variable of interest (i.e., x) may be different. In those cases, the symbol x in the above notations (e.g., μ_x, σ_x, m_x) is replaced by that specific variable's notation. In this paper, we are mainly interested in the process variables w and y_i, the definitions of which can be seen in Table I.

III. Problem Statement

In Fig. 2, we depict a simplified architecture of the smart metering system in a community. As shown in the figure, a smart meter with two-way communication capability is installed at each user's premises. The smart meters periodically measure corresponding users' electricity consumptions. These readings are further reported to utility companies via a central observer meter which is installed at some places (e.g., on an electrical pole) in the community. The central observer meter is essentially a tamper-resistant and function-enhanced smart meter with stronger computation capability and larger

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

TABLE I
NOTATIONS

Notations	Descriptions
U	Let $U = \{1, 2, ..., u\}$ denote the set of all users in the community, with u being the total number of users.
$r(j)$, $\varepsilon(j)$	Let $r(j)$ and $\varepsilon(j)$ denote the central observer meter's electricity measurement and the measurement error, respectively, at period j. Then, the actual amount of electricity supplied to all the users in the community can be calculated as $r(j) + \varepsilon(j)$, with $j = 1, 2, 3, \cdots$.
$q(i,j)$, $q'(i,j)$	Let $q(i,j)$ and $q'(i,j)$ denote user i's measured and reported electricity consumptions at period j, respectively, with $i \in U, j = 1, 2, 3, \cdots$.
$e(i,j)$	Let $e(i,j)$ denote the measurement error of user i's smart meter at period j, with $i \in U, j = 1, 2, 3, \cdots$.
$f(i,j)$, $\tilde{f}(i,j)$	Let $f(i,j)$ denote the technical losses of electricity when it is transmitted from the central observer meter to user i's smart meter at period j, with $i \in U, j = 1, 2, 3, \cdots$. Let $\tilde{f}(i,j)$ denote our estimated value of $f(i,j)$.
$w, w(j)$	Let $w(j)$ denote the difference between the central observer meter's measurement and the summation of all users' reported readings and the estimate of technical losses at period j, i.e., $w(j) = r(j) - \sum_{i \in U} (q'(i,j) + \tilde{f}(i,j))$. $w(j)$ is regarded as the j-th sample of the random variable w, with $j = 1, 2, 3, \cdots$.
τ	Let τ (in hour) denote the length of a reporting period of smart meters, which is usually set as 0.25 hour in applications.
y_i, $y_i(k,j)$	Let $y_i(k,j)$ denote user i's total electricity consumption on the k-th day from period j. Since each smart meter generates $24/\tau$ electricity consumption readings every day, we technically have $y_i(k,j) = \sum_{t=j+(k-1)\frac{24}{\tau}}^{j+k\frac{24}{\tau}-1} q(i,t)$. Moreover, $y_i(k,j)$ is regarded as the k-th sample of the random variable y_i, with $k = 1, 2, 3, \cdots$. In the context, we drop the subscript i of y_i and $y_i(k,j)$ for notation simplicity, and write them as y and $y(k,j)$, respectively.
x, μ_x, σ_x, $x(j)$	Let x denote the process variable of interest, which is assumed to follow a certain distribution with a mean μ_x and a variance σ_x^2. We denote by $x(j)$ the sample of x at period j.
m_x, $\bar{x}(k,j)$, $\bar{x}$, $\mu_{\bar{x}}$;	Let m_x denote the size of subgroups into which samples of x are divided. Let $\bar{x}(k,j)$ denote the average of the k-th subgroup of samples of x from period j. $\bar{x}(k,j)$ is regarded as the k-th sample of the random variable $\bar{x}$, with $k = 1, 2, 3, \cdots$. Let $\mu_{\bar{x}}$ denote the mean of the distribution followed by $\bar{x}$.
$\tilde{x}(k,j)$, $S_{\bar{x}}(k,j)$	Let $\tilde{x}(k,j)$ denote the difference between the largest and the smallest samples of x in the k-th subgroup from period j. Let $S_{\bar{x}}(k,j)$ denote the cumulative sum of deviations between the first to the k-th samples of $\bar{x}$ after period j and the target value $\mu_{\bar{x}}$.

storage space [22]. It can measure the total amount of electricity supplied to all users in the community.

In practice, no matter how well designed the central observer meter and smart meters are, these devices have measurement errors, which are defined as the differences between measured quantities and their actual values. Let $r(j)$ and $\varepsilon(j)$ denote the central observer meter's electricity measurement and measurement error, respectively, at period j. Then, the actual amount of electricity supplied to all the users in the community can be calculated as $r(j) + \varepsilon(j)$. Assume that in the community there are u users which are denoted by $U = \{1, 2, \cdots, u\}$. Let $q(i,j)$ and $q'(i,j)$ denote user i's measured and reported electricity consumptions at period j, respectively, where $i \in U, j = 1, 2, 3, \cdots$. In the real world, most users honestly report their electricity consumptions. Then, for honest users, we have $q'(i,j) = q(i,j)$. However, some malicious users manipulate their readings to smaller values, trying to use electricity for fewer fees and even for free. For these malicious users, we have $q'(i,j) < q(i,j)$. Let $e(i,j)$ denote the measurement error of user i's smart meter at period j, where $i \in U, j = 1, 2, 3, \cdots$. Then, the actual amount of user i's electricity consumption at period j can be calculated as $q(i,j) + e(i,j)$. Let $f(i,j)$ denote the technical losses of electricity when it is transmitted from the central observer meter to user i's smart meter at period j. Based upon the energy conservation law, the total energy supplied to all users is equal to the summation of all users' actual electricity consumptions and their technical losses. Technically, we have

$$r(j) + \varepsilon(j) = \sum_{i \in U} (q(i,j) + e(i,j) + f(i,j)). \tag{3}$$

In practical applications, the technical loss $f(i,j)$ is usually estimated based upon some mathematical models [31]. Let $\tilde{f}(i,j)$ denote the estimated value of $f(i,j)$. Let $w(j)$ denote the difference between the central observer meter's measurement and the summation of all users' reported readings and estimated technical losses at period j. Technically, we have

$$w(j) = r(j) - \sum_{i \in U} (q'(i,j) + \tilde{f}(i,j)). \tag{4}$$

Combining Equations (3) and (4), we can derive

$$\begin{aligned} w(j) = &\sum_{i \in U} (q(i,j) - q'(i,j)) + \sum_{i \in U} e(i,j) - \varepsilon(j) \\ &+ \sum_{i \in U} \Big(f(i,j) - \tilde{f}(i,j) \Big), \end{aligned} \tag{5}$$

where the first, second, and third items are the reported error of the users, the sum of the measurement estimation error of the users, and the power-transmission-loss estimation error, respectively. Apparently, if there are malicious users in a community, we have

$$w(j) > \sum_{i \in U} e(i,j) - \varepsilon(j) + \sum_{i \in U} \Big(f(i,j) - \tilde{f}(i,j) \Big). \tag{6}$$

For easy implementation, in applications we usually set a threshold h_0 to help judge whether there are malicious users in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

the community. Specifically, we claim that there are malicious users in the community if the inequality

$$w(j) = r(j) - \sum_{i \in U} (q'(i,j) + \tilde{f}(i,j)) > h_0 \tag{7}$$

holds [18, 19]. We will later demonstrate how h_0 can be determined in practice.

In the existing literature such as papers [14, 18–23, 32, 33], it is assumed that malicious users' reported readings are much less than their actual electricity consumptions. Once these malicious users begin to steal electricity, the central observer meter [18–23] can detect the existence of reading anomalies. Attacks of this kind are referred to as Large-amount Electricity Theft (LET) attacks in this paper. However, in reality, some malicious users may have a sense of counter-reconnaissance and they will try to escape the detection when stealing electricity. For all the detection methods in the literature, detection thresholds are used to judge if users steal electricity or not. A malicious user can steal electricity successfully by only stealing an amount much smaller than the corresponding detection threshold.

In this paper, we consider the cases where some malicious users deliberately and carefully tamper with their electricity consumptions to values just a little smaller than actual readings. The differences between the central observer meter's measurements and the summation of smart meters' readings do not exceed the threshold h_0, i.e., the inequality (7) does not hold. Attacks of this type are referred to as the Small-amount Electricity Theft (SET) attacks in this paper.

We summarize our assumptions as follows:

- These readings of smart meters are reported to utility companies via a tamper-resistant and function-enhanced central observer meter which is installed at some places (e.g., on an electrical pole) in the community. It can measure the total amount of electricity supplied to all users in the community.
- We consider SET attacks with which malicious users deliberately and carefully tamper with their electricity consumptions to values just a little smaller than actual readings.
- Once malicious users begin electricity theft behaviors, they do not stop until they are caught by utility companies.
- Malicious users only tamper with their smart meters.

With the system model listed as the above equations along with the explanations as well as the above assumptions, we summarize our goals as follows:

- This paper addresses the limitation that the performance of existing electricity theft detection techniques degrades a lot under SET attacks.
- We aim to develop detection techniques that can effectively deal with both LET and SET attacks.

IV. The proposed detector

For a better understanding of the SET attacks, in this section, we first present a SET attack example. Then, we demonstrate the working strategy of the proposed detector, utilizing the Shewhart and the CUSUM control charts together to detect and locate malicious users launching LET or SET attacks. The proposed detector consists of an electricity theft detection phase which aims to detect the existence of LET or SET attacks as well as a malicious user identification phase which aims to identify malicious users launching LET or SET attacks exactly.

A. SET attack analysis

We first demonstrate how the threshold h_0 in inequality (7) can be determined in practice. From Equation (5), we can know that if all the users in the community are honest, we have $w(j) = \sum\limits_{i \in U} e(i,j) - \varepsilon(j) + \sum\limits_{i \in U} \left(f(i,j) - \tilde{f}(i,j) \right)$. Let us think of $w(j)$ as samples of a process variable w. Since measurement errors $e(i,j), \forall i \in U$ and $\varepsilon(j)$, and the difference between $f(i,j)$ and $\tilde{f}(i,j), \forall i \in U$ can be regarded as samples of independent random variables, based upon the central limit theorem [29], we can conclude that when all the users are honest, the process variable w approximately follows a normal distribution with a mean μ_w and a variance σ_w^2, i.e., $w \sim N(\mu_w, \sigma_w^2)$.

Assume that we have n_0 periods of historical readings of $r(j)$ and $q'(i,j)$ starting from period j_0 and that all the users in the community are honest from period j_0 to period $j_0 + n_0 - 1$. Based upon some mathematical models [31], the estimated technical loss $\tilde{f}(i,j)$ can be calculated. Thus, the sample values of w during the above n_0 periods can be derived according to Equation (4). Let $\hat{\mu}_w$ and $\hat{\sigma}_w$ denote the unbiased estimation of μ_w and σ_w, respectively. Then, based upon the statistical knowledge [34], $\hat{\mu}_w$ and $\hat{\sigma}_w^2$ can be calculated as the mean and the variance of samples of w, respectively. Technically, we have

$$\hat{\mu}_w = \frac{1}{n_0} \sum_{j=j_0}^{j_0+n_0-1} w(j), \tag{8}$$

and

$$\hat{\sigma}_w^2 = \frac{1}{n_0 - 1} \sum_{j=j_0}^{j_0+n_0-1} \left(w(j) - \hat{\mu}_w \right)^2. \tag{9}$$

The statistical knowledge in [34] also indicates that the random variable $\frac{\hat{\mu}_w - \mu_w}{\hat{\sigma}_w / \sqrt{n_0}}$ follows a Student's t-distribution with $n_0 - 1$ degrees of freedom. We can set the threshold h_0 as the upper $100(1-\alpha)\%$ confidence bound for the mean μ_0. Technically, we have

$$h_0 = \hat{\mu}_w + \frac{\hat{\sigma}_w}{\sqrt{n_0}} t_{\alpha, n_0 - 1}, \tag{10}$$

where t_{α, n_0-1} denotes the $100(1-\alpha)$-th percentage point of the Student's t distribution with $n_0 - 1$ degrees of freedom such that the probability $\Pr\{ \frac{\hat{\mu}_w - \mu_w}{\hat{\sigma}_w / \sqrt{n_0}} \geq t_{\alpha, n_0 - 1} \} = \alpha$. In applications, a typical value for α is 0.05.

For better understanding, we next illustrate the SET attacks with the example in Fig. 3, where we assume that if all users are honest, we have $w \sim N(\mu_w = 10, \sigma_w^2 = 1)$. Furthermore, we assume that based upon historical values of $r(j)$ and $q'(i,j)$ as well as calculated values $f(i,j), \forall i \in U, j_0 \leq j \leq j_0 + n_0 - 1$, we can obtain $\hat{\mu}_w = 9.8$ and $\frac{\hat{\sigma}_w}{\sqrt{n_0}} t_{0.05, n_0 - 1} = 3.2$. Thus, according to Equation (10), h_0 can be set as 13. For easy understanding, we now consider a simple case where there is only one malicious user in the community who constantly

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

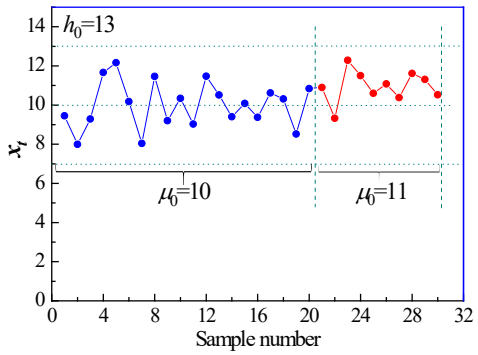


Fig. 3. An example for illustrating SET attacks.

steals 1 unit (e.g., kWh) of electricity every period. In this case, w will then follow a normal distribution with a mean $\mu_w + 1$ and variance σ_w^2, i.e., $w \sim N(\mu_w + 1 = 11, \sigma_w^2 = 1)$. According to statistical knowledge, we can derive the probability $\Pr(w(j) \leq 13)$ is about 97.5%. This implies that the central observer meter can detect this small reading abnormality with a probability of 2.5%, which is relatively low. To conclude, in applications, when malicious users launch SET attacks, they could try their best to make the probability that the inequality $w(j) \leq h_0$ holds as large as possible.

B. Phase I: Electricity theft detection

In this phase, we aim at detecting the existence of electricity theft, mainly by applying the Shewhart and the CUSUM control charts to monitor whether there are large and small changes in the sample values of w, respectively. This phase is further divided into a parameter estimation sub-phase and an anomaly detection sub-phase, as demonstrated in the following.

Parameter estimation: As aforementioned, with historical measurements of the central observer meter, users' historical reported readings and calculated technical losses, we can derive samples $w(j), \forall j = j_0, j_0+1, \cdots, j_0+n_0-1$. Also, we analyze that the process variable w approximately follows a normal distribution with a mean μ_w and a variance σ_w^2. This means that if we apply the Shewhart can the CUSUM control chart to monitor the changes in sample values of w, the normal distribution assumption is satisfied.

However, to make the detector more robust and more practical (which means that it works regardless of the distribution followed by w), we still divide the samples of w into subgroups, each containing m_w consecutive samples. In applications, we usually choose n_0 and m_w such that we have at least 20 such subgroups [24], i.e., $\lfloor \frac{n_0}{m_w} \rfloor \geq 20$. Let $\bar{w}$ denote the mean of samples of w in one subgroup. Then, according to the central limit theorem [34], $\bar{w}$ follows a normal distribution with a mean $\mu_{\bar{w}} = \mu_w$ and a variance $\sigma_{\bar{w}}^2 = \sigma_w^2/m_w$.

To let the Shewhart and the CUSUM control charts work properly, we need to know both $\mu_{\bar{w}}$ and $\sigma_{\bar{w}}$ in advance. Nevertheless, in practice, the true values of $\mu_{\bar{w}}$ and $\sigma_{\bar{w}}$ are usually unknown, and thus their estimate values are used instead. Next, we demonstrate how to get an unbiased estimation of $\mu_{\bar{w}}$ and $\sigma_{\bar{w}}$, denoted by $\hat{\mu}_{\bar{w}}$ and $\hat{\sigma}_{\bar{w}}$, respectively.

(1) We first explain how to derive $\hat{\mu}_{\bar{w}}$. Since $\mu_{\bar{w}} = \mu_w$ and $\hat{\mu}_w$ can be obtained by Equation (8), we have

$$\hat{\mu}_{\bar{w}} = \hat{\mu}_w = \frac{1}{n_0} \sum_{j=j_0}^{j_0+n_0-1} w(j).$$

(2) We then focus on how to derive $\hat{\sigma}_{\bar{w}}$. Since $\sigma_{\bar{w}}^2 = \sigma_w^2/m_w$, we have

$$\hat{\sigma}_{\bar{w}} = \frac{\hat{\sigma}_w}{\sqrt{m_w}}.$$

This implies that once $\hat{\sigma}_w$ is obtained, we can immediately derive $\hat{\sigma}_{\bar{w}}$. Although the unbiased estimation of the variance σ_w^2 (i.e., $\hat{\sigma}_w^2$) can be obtained by Equation (9) [34], the unbiased estimation of the standard deviation (i.e., $\hat{\sigma}_w$) cannot be obtained by simply performing the square root on the right side of Equation (9) [24]. In practice, $\hat{\sigma}_w$ is calculated as follows:

(a) Let $\tilde{w}$ denote the difference between the largest and the smallest values in one subgroup of samples of w. Let $\tilde{w}(k, j)$ denote the k-th sample of w after period j. As aforementioned, n_0 samples of w after period j_0 (i.e., $w(j), \forall j = j_0, j_0+1, \cdots, j_0+n_0-1$) are divided into subgroups, each containing m_w elements. Thus, we can obviously obtain $\tilde{w}(k, j_0), \forall k = 1, 2, \cdots \lfloor \frac{n_0}{m_w} \rfloor$.

(b) Let d_w denote the mean of the distribution followed by the ratio of $\tilde{w}$ to σ_w, i.e., $d_w = \mathrm{E}(\frac{\tilde{w}}{\sigma_w})$, where $\mathrm{E}(\cdot)$ denotes the mean operation. It is well studied that the value of d_w is a function of the subgroup size m_w [24]. The values of d_w for different subgroup sizes up to 10 are shown in Table II [24]. Obviously, once m_w is determined, the value of d_w is known. For example, if $m_w = 3$, we have $d_w = 1.693$. Thus, we have

$$\hat{\sigma}_w = \frac{E(\tilde{w})}{d_w} = \frac{1}{d_w} \frac{1}{\lfloor \frac{n_0}{m_w} \rfloor} \sum_{k=1}^{\lfloor \frac{n_0}{m_w} \rfloor} \tilde{w}(k, j_0). \tag{11}$$

Anomaly detection: Assume that we start the detection from period j_1, with $j_1 > j_0 + n_0 - 1$. Obviously, by Equation (4), the samples of w after period j_1 can be calculated. These samples of w are arranged into subgroups, each containing m_w elements. With elements in the k-th subgroup, the average $\bar{w}(k, j_1)$ is calculated by Equation (1). If there are malicious users in the community, sample values of w have a tendency to get larger, which further leads to the increase of sample values of $\bar{w}$.

We apply the Shewhart control chart to see whether there are moderate or large increases in the sample values of $\bar{w}$. Specifically, if

$$\frac{\bar{w}(k, j_1) - \hat{\mu}_{\bar{w}}}{\hat{\sigma}_{\bar{w}}} > h_s,$$

the detector signals the existence of reading anomalies in the community. On the whole, the following three cases are possible: (1) At least one malicious user is launching LET attacks; (2) At least one malicious user is launching LET attacks and at least one malicious user is launching SET attacks simultaneously; (3) Several malicious users are simultaneously launching SET attacks and the summation of their stolen electricity is large enough to be detected by the Shewhart control chart.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

TABLE II
VALUES OF CONSTANT d_w FOR OBTAINING UNBIASED STANDARD DEVIATION

m_w	2	3	4	5	6	7	8	9	10
d_w	1.128	1.693	2.059	2.326	2.534	2.704	2.847	2.970	3.078

At the same time, we also apply the CUSUM control chart to monitor the slight increase of sample values of $\bar{w}$, which usually implies the existence of malicious users launching SET attacks. Specifically, we calculate $S_{\bar{w}}(k, j_1)$ according to Equation (2). If $S_{\bar{w}}(k, j_1) > h_c$, there exists at least one malicious user launching SET attacks. In this case, the following two cases are possible: (1) there is only one malicious user to launch SET attacks; (2) there are several malicious users simultaneously launching SET attacks, but the stolen electricity is not large enough to be detected by the Shewhart control chart.

The above strategies are concluded in Algorithm 1, where the parameter estimation phase is summarized in lines 1 to 4, and the anomaly detection phase is summarized in lines 5 to 27. In Algorithm 1, the variable v is a counter indicating the number of rounds of inspection. In each round of inspection, the cumulative sum $S_{\bar{w}}(k, j_1)$ involves at most K_1 samples of $\bar{w}$. If within one round of inspection, neither the Shewhart nor the CUSUM control chart can detect the existence of reading anomalies, the detector concludes that all users are honest up to now, and sets out the next round of inspection for continuing the monitoring process. Before a new round of inspection process begins, the detector resets the value of $S_{\bar{w}}(k, j_1)$ to the initialized value $S_{\bar{w}}(0, j_1)$. Otherwise, if within one round of inspection, either the Shewhart or the CUSUM control chart detects reading anomalies, the proposed detector goes into *Phase II: malicious user identification*, which is detailed in the following.

Algorithm 1 Electricity theft detection

Require: $r_j, q'_{i,j}, f_{i,j}, i \in U, j = j_0, j_0+1, \cdots, j_0+n_0-1$
Ensure: signals indicating whether there are malicious users in U

1: Initialize $S_{\bar{w}}(0, j_1), l, h_s, h_c$;
2: Compute $w(j), j = j_0, j_0+1, \cdots, j_0+n_0-1$ by Equation (4), which are then sub-grouped by every m_w samples;
3: Compute $\hat{\mu}_w$ and $\hat{\sigma}_w$ according to Equations (8) and (11), respectively;
4: $\hat{\mu}_{\bar{w}} \leftarrow \hat{\mu}_w, \hat{\sigma}_{\bar{w}} \leftarrow \frac{\hat{\sigma}_w}{\sqrt{m_w}}$;
5: $k \leftarrow 1, v \leftarrow 0, flag \leftarrow 0$;
6: **while** $flag == 0$ **do**
7: $S_{\bar{w}}(k, j_1) \leftarrow S_{\bar{w}}(0, j_1), v \leftarrow v + 1$;
8: **while** $(v-1)K_1 < k \leq vK_1$ **do** ▷ Every K_1 samples of $\bar{w}$
9: Calculate $w(j), j = j_1+(k-1)m_w, \cdots, j_1+km_w-1$ by Equation (4); and then calculate the average $\bar{w}(k, j_1)$ according to Equation (1);
10: **if** $\frac{\bar{w}(k,j_1)-\hat{\mu}_{\bar{w}}}{\hat{\sigma}_{\bar{w}}} > h_s$ **then** ▷ Shewhart control chart
11: $flag \leftarrow 1$;▷ Indicate the existence of electricity theft
12: **else** ▷ CUSUM control chart
13: Calculate $S_{\bar{w}}(k, j_1)$ according to Equation (2);
14: **if** $S_{\bar{w}}(k, j_1) > h_c$ **then**
15: $flag \leftarrow 1$;
16: **end if**
17: **end if**
18: **if** $flag == 1$ **then**
19: **Break**;
20: **else**
21: $k \leftarrow k + 1$;
22: **end if**
23: **end while**
24: **if** $flag == 0$ **then**
25: All users are honest up to now and continue monitoring;
26: **end if**
27: **end while**
28: Perform Algorithm 2 to identify malicious users;

C. Phase II: Malicious user identification

After detecting the existence of reading anomalies in phase I, we are still unknown which users are malicious. Thus, in this phase, we aim to identify malicious users exactly, mainly by applying the Sheahart and the CUSUM control charts to monitor whether there are large and small changes in users' daily electricity consumptions, respectively. This phase is further divided into a parameter estimation sub-phase and a malicious user identification sub-phase, with details given below.

Parameter estimation: Let τ (hour) denote the length of a reporting period of smart meters, which is usually set as 0.25 hours (i.e., 15 minutes) in applications. Each smart meter can generate $24/\tau$ electricity consumption readings every day. Let $y_i(k, j)$ denote user i's total electricity consumption on the k-th day from period j. Technically, we have

$$y_i(k, j) = \sum_{t=j+(k-1)\frac{24}{\tau}}^{j+k\frac{24}{\tau}-1} q(i, t). \tag{12}$$

For notation simplicity, we in the following drop the subscript i of $y_i(k, j)$. Since all users' reported electricity consumptions need to be examined, this does not impact the following discussions. Let y denote one user's daily electricity consumption. Then, $y(k, j)$ can be regarded as the k-th sample of the process variable y after period j.

In this paper, we assume that the process variable y approximately follows a normal distribution. This is reasonable based upon the following facts: (1) In [35], the authors investigate a data set with 702 households and find that users' daily electricity consumptions approximately follow a normal distribution; (2) We explore the dataset in [36], which are measurements of electricity consumptions in one household with a one-minute sampling rate over almost four years. The results are shown in Fig. 4. As can be seen, this user's daily electricity consumption also approximately follow a normal distribution with a mean of 25.87 and a standard deviation of 10.36. In this way, the normal distribution assumption in the Shewhart and the CUSUM control chart is satisfied.

To make the detector more robust and more practical (which means that it works regardless of the distribution followed by

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

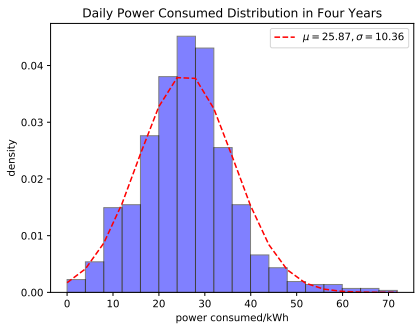


Fig. 4. The histogram are obtained based on the dataset in [36]. It shows that users' daily electricity consumptions follow normal distribution with a mean 25.87 and a standard deviation of 10.36.

the process variable y), users' daily electricity consumptions are arranged into subgroups, each containing m_y elements. Let $\bar{y}$ denote the mean of a user's daily electricity consumptions in one subgroup. Let $\bar{y}(k,j)$ denote the k-th sample of $\bar{y}$ after period j. Then, $\bar{y}(k,j)$ can be calculated by Equation (1). Let μ_y and σ_y denote the mean and the standard deviation of the distribution followed by the process variable y, respectively. Then, according to the central limit theorem [29], $\bar{y}$ follows a normal distribution with a mean $\mu_{\bar{y}} = \mu_y$ and a variance $\sigma_{\bar{y}}^2 = \frac{\sigma_y^2}{m_y}$.

Since $\mu_{\bar{y}}$ and $\sigma_{\bar{y}}$ are usually unknown, we next focus on how to obtain their unbiased estimation, denoted by $\hat{\mu}_{\bar{y}}$ and $\hat{\sigma}_{\bar{y}}$, respectively. Assume that for any given user, we have n_1 periods of historical electricity consumptions starting from period j_2 and that all users are honest during these periods. Then, for each user, we can obtain a total number of $\lfloor \frac{n_1\tau}{24} \rfloor$ daily electricity consumptions, i.e., $y\left(k,j_2\right), \forall k = 1,2,3,\cdots,\lfloor \frac{n_1\tau}{24} \rfloor$. Using these data, we can further calculate the subgroup mean $\bar{y}(k,j_2), \forall k = 1,2,3,\cdots,\lfloor \frac{n_1\tau}{24m_y} \rfloor$. Afterwards, $\hat{\mu}_{\bar{y}}$ can be calculated as the mean of sample values of $\bar{y}$ [34]. Technically, we have

$$\hat{\mu}_{\bar{y}} = \frac{1}{\lfloor \frac{n_1\tau}{24m_y} \rfloor} \sum_{k=1}^{\lfloor \frac{n_1\tau}{24m_y} \rfloor} \bar{y}(k,j_2), \forall i \in U.$$

We next focus on how to get $\hat{\sigma}_{\bar{y}}$. Let $\tilde{y}$ denote the difference between the largest and the smallest values in one subgroup of users' daily electricity consumption. Let $\tilde{y}\left(k,j\right)$ denote the k-th sample of $\tilde{y}$ after period j. Let d_y denote the mean of the distribution followed by the ratio of $\tilde{y}$ to σ_y, i.e., $d_y = \mathrm{E}(\frac{\tilde{y}}{\sigma_y})$. The relationship between d_y and m_y is the same as that between d_w and m_w. In other words, if $m_y = m_w$, we have $d_y = d_w$. Thus, similar to the estimation of $\hat{\sigma}_{\bar{w}}$ in Section IV-B, we can obtain

$$\hat{\sigma}_{\bar{y}} = \frac{\hat{\sigma}_y}{\sqrt{m_y}} = \frac{1}{\sqrt{m_y}} \frac{1}{d_y} \frac{1}{\left\lfloor \frac{n_1\tau}{24m_y} \right\rfloor} \sum_{k=1}^{\left\lfloor \frac{n_1\tau}{24m_y} \right\rfloor} \tilde{y}\left(k,j_2\right).$$

Malicious user identification: Assume that the identification process starts from period j_3, with $j_3 > j_1$. Then, from period j_3, every m_y days of users' reported electricity consumptions are arranged as a subgroup. Afterward, the subgroup means $\bar{y}(k,j_3), \forall k = 1,2,\cdots$ can be calculated. If some users commit electricity theft, their daily electricity consumptions y tend to get smaller, leading to the decrease of $\bar{y}$. Thus, we apply the Shewhart and the CUSUM control chart to monitor whether sample values of $\bar{y}$ have a tendency to decrease.

Specifically, we apply the Shewhart control chart to capture the moderate and large decrease of the sample values of $\bar{y}$. If

$$\frac{\bar{y}\left(k,j_3\right) - \hat{\mu}_{\bar{y}}}{\hat{\sigma}_{\bar{y}}} < -h_s,$$

the corresponding user is identified as a user launching LET attacks.

Besides, we apply the CUSUM control chart to judge whether there is a slight decrease in sample values of $\bar{y}$. Specifically, we calculate $S_{\bar{y}}\left(k,j_3\right)$ by Equation (2), with a negative sign "$-$" put before the standardized term. If $S_{\bar{y}}\left(k,j_3\right) > h_c$, the corresponding user is identified as a user launching SET attacks.

We conclude the above strategies in Algorithm 2, where M and H denote the set of malicious users and honest users, respectively. The parameter estimation sub-phase is summarized in lines $3 \sim 6$, and the malicious user identification sub-phase is summarized in lines $7 \sim 30$. In Algorithm 2, we set a user-defined parameter V (a positive integer) to limit the maximum number of rounds of inspections to be performed before determining whether a user is "malicious" or "honest". Within one round of inspection, at most K_2 sub-groups of users' daily electricity consumptions are involved to calculate the cumulative sum $S_{\bar{y}}\left(k,j_3\right)$. If both the Shewhart and the CUSUM control chart cannot detect reading anomalies within one round of inspection, the detector resets the cumulative sum $S_{\bar{y}}\left(k,j_3\right)$ to its initial value and automatically goes to the next round of inspection. If within V rounds of inspection, either the Shewhart or the CUSUM control chart detects reading anomalies, this user is identified as a malicious one; otherwise, this user is identified as an honest user.

V. Algorithm Analysis

In this section, we aim to analyze the efficiency of the proposed detector. Since the proposed detector consists of an electricity theft detection phase and a malicious user identification phase, this goal can be achieved by analyzing the efficiency of Algorithm 1 and Algorithm 2, respectively. More specifically, this goal can be achieved by answering the following two questions:

- Question 1: if malicious users set out to steal electricity, how long does it take (on average) for the proposed detector to signal the existence of reading anomalies?
- Question 2: if the proposed detector has detected the existence of malicious users, how long does it take (on average) for the proposed detector to identify whether a user is malicious or not?

Since Algorithm 1 and Algorithm 2 have similar working strategies, we can infer that analyses for answering these two questions are similar. Thus, in this section, we explain in detail the analysis for answering Question 1 but omit the analysis for answering Question 2.

Based upon the following facts: (1) smart meters have equal length of reporting periods; (2) one sample of w can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

Algorithm 2 Malicious user identification

Require: $q'(i,j), \forall i \in U, j = \{j_2, j_2+1, \cdots, j_2+n_1, \cdots, j_3, j_3+1, j_3+2, \cdots\}$ ▷ users' historical and newly reported readings
Ensure: M, H ▷ the set of malicious users and honest users, respectively

1: $M \leftarrow \emptyset, H \leftarrow \emptyset$;
2: Initialize $S_{\bar{y}}(0, j_3), l, h_s, h_c$;
3: **for** each user in the community **do** ▷ parameter estimation
4: Arrange every m_y days' electricity consumptions into one subgroup;
5: Calculate $\bar{y}(k, j_2)$ and $\tilde{y}(k, j_2), \forall k = 1, 2, 3, \cdots, \lfloor \frac{n_1 \tau}{24 m_y} \rfloor$; and then compute $\hat{\mu}_{\bar{y}}$ and $\hat{\sigma}_{\bar{y}}$;
6: $k \leftarrow 1, v \leftarrow 0, flag \leftarrow 0$;
7: **while** $v \leq V$ and $flag == 0$ **do**
8: $S_{\bar{y}}(k, j_3) \leftarrow S_{\bar{y}}(0, j_3), v \leftarrow v + 1$;
9: **while** $(v-1)K_2 < k \leq vK_2$ **do**
10: Calculate $\bar{y}(k, j_3)$ with the k-th subgroup of user i's daily reported electricity consumptions;
11: **if** $\frac{\bar{y}(k,j_3) - \hat{\mu}_{\bar{y}}}{\hat{\sigma}_{\bar{y}}} < -h_s$ **then** ▷ Shewhart control chart
12: $flag \leftarrow 1$;
13: **else** ▷ CUSUM control chart
14: Calculate $S_{\bar{y}}(k, j_3)$ by Equation (2), with a negative sign "−" put before the standardized term;
15: **if** $S_{\bar{y}}(k, j_3) > h_c$ **then**
16: $flag \leftarrow 1$;
17: **end if**
18: **end if**
19: **if** $flag == 1$ **then**
20: Put this user into set M;
21: **Break**;
22: **else**
23: $k \leftarrow k + 1$;
24: **end if**
25: **end while**
26: **end while**
27: **if** $flag == 0$ **then**
28: Put this user into set H;
29: **end if**
30: **end for**
31: **Return** M, H

be generated at a reporting period; (3) one sample of $\bar{w}$ is calculated based upon m_w consecutive samples of w, Question 1 can be transformed into the following question:

- Question 3: if malicious users set out to steal electricity, how many samples of $\bar{w}$ (on average) should be involved for the proposed detector to signal the existence of reading anomalies?

We address Question 3 mainly by modeling the inspection process from line 10 to line 17 in Algorithm 1 as a Markov chain, explained as follows.

For convenience, we let

$$z_k = \frac{\bar{w}(k, j_1) - \hat{\mu}_{\bar{w}}}{\hat{\sigma}_{\bar{w}}}.$$

(1) We first consider the case $z_k \leq h_s$ where the CUSUM control chart works.

According to Equation (2), given the value of the present cumulative sum $S_{\bar{w}}(k, j_1)$, the value of the future cumulative sum $S_{\bar{w}}(k+1, j_1)$ does not depend on the value of the past cumulative sum $S_{\bar{w}}(k-1, j_1), S_{\bar{w}}(k-2, j_1), S_{\bar{w}}(k-3, j_1), \cdots$. This implies that the inspection process of the CUSUM control chart satisfies the Markov property [37]. Thus, it is reasonable

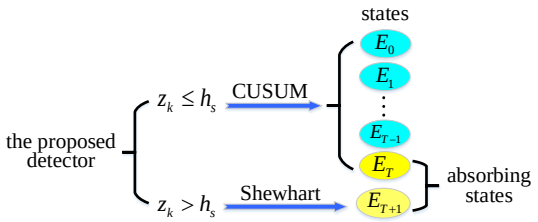


Fig. 5. Analyzing the inspection process from line 10 to line 17 in Algorithm 1 with a Markov chain model.

to model the above inspection process as a Markov chain with $T+1$ states labeled $E_0, E_1, \ldots, E_T$, where T is a positive integer and E_T is an absorbing state[1] [38].

The Markov chain modeling the inspection process of the CUSUM control chart is established as follows: (a) First, we divide the value range of the cumulative sum $S_{\bar{w}}(k, j_1)$, i.e., $[0, +\infty)$, into the following $T+1$ intervals: $\underbrace{\left[0, \frac{\theta}{2}\right]}_{\text{interval } 0}, \underbrace{\left(\frac{\theta}{2}, \frac{3\theta}{2}\right]}_{\text{interval } 1}, \ldots, \underbrace{\left(i\theta - \frac{\theta}{2}, i\theta + \frac{\theta}{2}\right]}_{\text{interval } i}, \ldots, \underbrace{\left(h_c - \theta, h_c\right]}_{\text{interval } T-1}, \underbrace{\left(h_c, +\infty\right)}_{\text{interval } T}$, where $\theta = \frac{2h_c}{2T-1}$ [38]. (b) Then, based upon the value of the cumulative sum $S_{\bar{w}}(k, j_1)$, we associate the inspection process of the CUSUM control chart to one state in $\{E_0, E_1, \ldots, E_T\}$. Specifically, if $S_{\bar{w}}(k, j_1) \in \left[0, \frac{\theta}{2}\right]$, we say that the inspection process is in state E_0. If $S_{\bar{w}}(k, j_1) \in \left(i\theta - \frac{\theta}{2}, i\theta + \frac{\theta}{2}\right]$, we say that the inspection process is in state $E_i, i = 1, 2, \cdots, T-1$. If $S_{\bar{w}}(k, j_1) > h_c$, we say that the inspection process is in state E_T. Once the Markov chain enters into the absorbing state E_T, the CUSUM control chart detects the existence of malicious users.

(2) For the case $z_k > h_s$, according to the lines $10 \sim 17$ Algorithm 1, the Shewhart control chart immediately detects the existence of malicious users. We regard this case as another absorbing state, denoted by E_{T+1}. By adding the absorbing state E_{T+1} to the Markov chain of the CUSUM control chart, we can model the whole inspection process applying the CUSUM and the Shewhart control charts together as a Markov chain with $T+2$ states $E_0, E_1, \ldots, E_T, E_{T+1}$. As summarized in Fig. 5, if $z_k \leq h_s$, the Markov chain changes among states $E_0, E_1, \ldots, E_T$; otherwise, it enters into the state E_{T+1}.

Let $p_{i,j}$ denote the probability for the Markov chain to transition from state E_i to state E_j, where $i = 0, 1, 2, \cdots T+1, j = 0, 1, 2, \cdots T+1$. Then, we have

$$\begin{aligned}
p_{i,0} &= \Pr(z_k \leq h_s) \Pr(E_i \to E_0) \\
&= \Pr(z_k \leq h_s) \Pr\left(z_k - l \leq -i\theta + \tfrac{\theta}{2}\right), \\
p_{i,j} &= \Pr(z_k \leq h_s) \Pr(E_i \to E_j) \\
&= \Pr(z_k \leq h_s) \Pr\left((j-i)\theta - \tfrac{\theta}{2} \leq z_k - l \leq (j-i)\theta + \tfrac{\theta}{2}\right), \\
p_{i,T} &= \Pr(z_k \leq h_s) \Pr(E_i \to E_T) \\
&= \Pr(z_k \leq h_s) \Pr\left((T-i)\theta - \tfrac{\theta}{2} \leq z_k - l\right), \\
p_{i,T+1} &= \Pr(E_i \to E_{T+1}) = \Pr(z_k > h_s) = 1 - \Pr(z_k \leq h_s),
\end{aligned} \tag{13}$$

[1]An absorbing state of a Markov chain is a state that, once entered, cannot be left.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

where $i = 0, 1, 2, \cdots T-1, j = 0, 1, 2, \cdots T-1$. Since z_k follows the standard normal distribution, given values of h_s, h_c, l and T, the above transition probability can be calculated. Particularly, for absorbing states E_T and E_{T+1}, we have $p_{T,T} = 1$ and $p_{T+1,T+1} = 1$. Let $P_* = \Pr(z_k \leq h_s)$. Let $P_i = \Pr\left(i\theta - \frac{\theta}{2} \leq z_k - l \leq i\theta + \frac{\theta}{2}\right)$. Let $F_i = \Pr\left(z_k - l \leq i\theta + \frac{\theta}{2}\right)$. Let $\mathbf{P}$ denote the transition probability matrix of the Markov chain modeling the proposed detector. Then, $\mathbf{P}$ can be written as in Fig. 6 (a).

$$\mathbf{P}=\begin{array}{c} \\ E_0 \\ E_1 \\ E_2 \\ \vdots \\ E_i \\ \vdots \\ E_{T-1} \\ E_T \\ E_{T+1} \end{array}\begin{array}{c} \begin{array}{ccccccccc} E_0 & E_1 & E_2 & \cdots & E_j & \cdots & E_{T-1} & E_T & E_{T+1} \end{array} \\ \begin{bmatrix} P_*F_0 & P_*P_1 & P_*P_2 & \cdots & P_*P_j & \cdots & P_*P_{T-1} & P_*(1-F_{T-1}) & 1-P_* \\ P_*F_{-1} & P_*P_0 & P_*P_1 & \cdots & P_*P_{j-1} & \cdots & P_*P_{T-2} & P_*(1-F_{T-2}) & 1-P_* \\ P_*F_{-2} & P_*P_{-1} & P_*P_0 & \cdots & P_*P_{j-2} & \cdots & P_*P_{T-3} & P_*(1-F_{T-3}) & 1-P_* \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ P_*F_{-i} & P_*P_{1-i} & P_*P_{2-i} & \cdots & P_*P_{j-i} & \cdots & P_*P_{T-1-i} & P_*(1-F_{T-1-i}) & 1-P_* \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ P_*F_{1-T} & P_*P_{2-T} & P_*P_{3-T} & \cdots & P_*P_{j-(T-1)} & \cdots & P_*P_0 & P_*(1-F_0) & 1-P_* \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} \end{array}$$

(a) The transition probability matrix before combining states E_T and E_{T+1}

$$\mathbf{P}'=\begin{array}{c} \\ E_0 \\ E_1 \\ E_2 \\ \vdots \\ E_i \\ \vdots \\ E_{T-1} \\ E_T \text{ or } E_{T+1} \end{array}\begin{array}{c} \begin{array}{ccccccccc} E_0 & E_1 & E_2 & \cdots & E_j & \cdots & E_{T-1} & E_T \text{ or } E_{T+1} \end{array} \\ \begin{bmatrix} P_*F_0 & P_*P_1 & P_*P_2 & \cdots & P_*P_j & \cdots & P_*P_{T-1} & 1-P_*F_{T-1} \\ P_*F_{-1} & P_*P_0 & P_*P_1 & \cdots & P_*P_{j-1} & \cdots & P_*P_{T-2} & 1-P_*F_{T-2} \\ P_*F_{-2} & P_*P_{-1} & P_*P_0 & \cdots & P_*P_{j-2} & \cdots & P_*P_{T-3} & 1-P_*F_{T-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ P_*F_{-i} & P_*P_{1-i} & P_*P_{2-i} & \cdots & P_*P_{j-i} & \cdots & P_*P_{T-1-i} & 1-P_*F_{T-1-i} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ P_*F_{1-T} & P_*P_{2-T} & P_*P_{3-T} & \cdots & P_*P_{j-(T-1)} & \cdots & P_*P_0 & 1-P_*F_0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 1 \end{bmatrix} \end{array}$$

(b) The transition probability matrix after combining states E_T and E_{T+1}

Fig. 6. The transition probability matrix of the Markov chain modeling the inspection process from line 10 to line 17 in Algorithm 1

The following two events are independent: (1) the event that the Markov chain changes from state $E_i, i = 0, 1, \cdots, T-1$ to state E_T; (2) the event that the Markov chain changes from state $E_i, i = 0, 1, \cdots, T-1$ to state E_{T+1}. Thus, the probability that the Markov chain changes from state $E_i, i = 0, 1, \cdots, T-1$ to an absorbing state (i.e., E_T or E_{T+1}) is as follows:

$$p_{i,T|T+1} = p_{i,T} + p_{i,T+1},$$

where "|" denotes an OR operation. Thus, if we combine states E_T and E_{T+1} into one state (which means that the proposed detector detects the existence of malicious users), the transition probability matrix $\mathbf{P}$ in Fig. 6 (a) is transformed into the transition probability matrix $\mathbf{P}'$ in Fig. 6 (b). The matrix $\mathbf{P}'$ has the following properties: (1) the summation of elements in one row is equal to one; (2) the last row consists of zeros except for the last element; (3) For the central $T-1$ columns, all elements along a line parallel to the main diagonal have the same value.

Let X_i denote the number of samples of $\bar{w}$ when the Markov chain starts from E_i to reach one of the absorbing states E_T or E_{T+1} for the first time. Let λ_i denote the average of X_i. Then, we have

$$\begin{aligned}\lambda_i &= \sum_{r=1}^{\infty} r \Pr(X_i = r) \\ &= \sum_{r=1}^{\infty} r \sum_{j=0}^{T-1} p_{i,j} \Pr(X_j = r-1) \\ &= \sum_{j=0}^{T-1} p_{i,j} \left[\sum_{r-1=0}^{\infty} (r-1) \Pr(X_j = r-1) + \sum_{r-1=0}^{\infty} \Pr(X_j = r-1) \right] \\ &= \sum_{j=0}^{T-1} p_{i,j} [\lambda_j + 1] = \sum_{j=0}^{T-1} p_{i,j}\lambda_j + 1.\end{aligned}$$

Let $\boldsymbol{\lambda} = [\lambda_0, \lambda_1, \cdots, \lambda_{T-1}]'$. Let $\mathbf{R}$ denote the matrix obtained from $\mathbf{P}'$ by deleting the final row and column. Let $\mathbf{I}$ denote the $T \times T$ unity matrix. Then, the above equation can be written in the matrix form as

$$(\mathbf{I} - \mathbf{R})\boldsymbol{\lambda} = \mathbf{1},$$

from which we can derive

$$\boldsymbol{\lambda} = (\mathbf{I} - \mathbf{R})^{-1}\mathbf{1}. \tag{14}$$

Apparently, given values of h_s, h_c and l, different vectors of $\boldsymbol{\lambda}$ can be obtained under different values of T according to Equation (14).

Assume that we have initialize $S_{\bar{w}}(k, j_1)$ as a specific value. Then, under different values of T, the Markov chain modeling the inspection process may start from different states. In other words, with a specific initial value of $S_{\bar{w}}(k, j_1)$, we can obtain different pairs of (T, λ_i) for different values of T. For example, assume that we have set $h_s = 3.5$, $h_c = 5$, $l = 0.5$ and initialize the value of $S_{\bar{w}}(k, j_1)$ as 1.5. Then, if $T = 5$, the intervals $\underbrace{\left[0, \frac{\theta}{2}\right]}_{\text{interval 0}}, \underbrace{\left(\frac{\theta}{2}, \frac{3\theta}{2}\right]}_{\text{interval 1}}, \ldots, \underbrace{\left(i\theta - \frac{\theta}{2}, i\theta + \frac{\theta}{2}\right]}_{\text{interval } i}, \ldots, \underbrace{(h_c - \theta, h_c]}_{\text{interval } T-1}$ are $\left[0, \frac{5}{9}\right], \left(\frac{5}{9}, \frac{5}{3}\right], \cdots, \left(\frac{35}{9}, 5\right]$. Since the initial value of $S_{\bar{w}}(k, j_1)$ (i.e., 1.5) locates at the second interval, the starting state of the Markov chain is E_1. According to Equation (14), when $T = 5$, we have $\boldsymbol{\lambda} = [611.45, 607.24, 592.55, 548.67, 430.82]'$. Thus, in this case, we can obtain the following pair of (T, λ_i): (5, 607.24). If $T = 8$, the above intervals become $\left[0, \frac{1}{3}\right], \left(\frac{1}{3}, 1\right], \left(1, \frac{5}{3}\right], \cdots, \left(\frac{13}{3}, 5\right]$. Since the initial value of $S_{\bar{w}}(k, j_1)$ (i.e., 1.5) locates at the third interval, the starting state of the Markov chain becomes E_2. According to Equation (14), when $T = 8$, we have $\boldsymbol{\lambda} = [703.35, 701.56, 697.29, 688.19, 669.83, 633.70, 565.50, 451.76]'$ In this case, we can obtain the following pair of (T, λ_i): (8, 697.29).

Then, at least three pairs of (T, λ_i) are used to fit the following formula with the least square method:

$$\lambda_i = c_0 + \frac{c_1}{T} + \frac{c_2}{T^2}.$$

In this way, the three constant coefficients c_0, c_1 and c_2 can be obtained. For example, in Fig. 7, we set $h_s = 3.5$, $h_c = 5$, $l = 0.5$ and the initial value of $S_{\bar{w}}(k, j_1)$ as 1.5. With the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

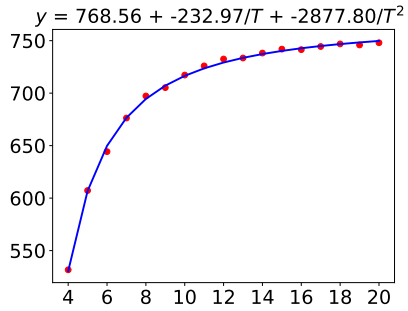


Fig. 7. An example of applying the formula $\lambda_i = c_0 + \frac{c_1}{T} + \frac{c_2}{T^2}$ to fit with at least three pairs of (T, λ_i), using the least square method. In this figure, we set $h_s = 3.5$, $h_c = 5$, $l = 0.5$ and the initial value of $S_{\bar{w}}(k, j_1)$ as 1.5.

value of T ranging from 4 to 20, we obtain 17 pairs of (T, λ_i). After we apply the above formula to fit these pairs of (T, λ_i), we obtain $c_0 = 768.56, c_1 = -232.97$ and $c_2 = -2877.8$. Afterwards, the average number of samples of $\bar{w}$ for the specific initial value of $S_{\bar{w}}(0, j_1)$ can be estimated as the asymptotic value of $c_0 + \frac{c_1}{T} + \frac{c_2}{T^2}$, i.e., c_0. Then, we answered Question 3.

VI. Experiments

In this section, we report the results of experiments, which are conducted in Python 3.6 on an integrated development environment platform - PyCharm Community Edition 2018.2.5. We assume that users' electricity consumptions are reported every 15 minutes. Also, we assume that user i's electricity consumptions during one period approximately follow a normal distribution with a mean u_i and a standard deviation σ_i, where $i \in U$. Specifically, the mean u_i is randomly chosen from interval $[1, 2]$ and the standard deviation σ_i is randomly chosen from interval $[0.2, 0.4]$. Users' periodical electricity consumptions are assumed to interfere with a noise that follows a normal distribution with a mean of 0.2 and a standard deviation of 0.3. The biases between the actual and the estimated technical losses are assumed to follow a random distribution with a mean of 0.8 and a standard deviation of 0.6. In the experiments, we first generate a specific number of users. Some of these users are set as honest users, and the others are set as malicious users. Note that users' electricity consumptions following a normal distribution have no relationship with users' reporting behaviors, i.e., whether they are malicious users or not since users' electricity consumptions are actual electricity consumptions whereas being malicious a user or not is about the user's reporting behavior. For the honest users, their reported electricity consumption is equal to the measured one. For the malicious users, their reported electricity consumption is less than the measured one, and the difference between a malicious user's measured and reported electricity consumption is expressed in the units of σ_i. We set the parameters $K_1 = 100$, $K_2 = 120$ and $V = 1$. Each piece of data in this section is averaged over 40 times of repeated experiments.

A. False positive rate and false-negative rate

Detection accuracy is defined as the ratio of the number of users correctly classified to the total number of users. In the real world, we usually have many more honest users than malicious users. In this case, if a detector simply classifies all the users as honest, the detection accuracy is still high. This implies that detection accuracy is not an appropriate metric to evaluate the performance of electricity theft detection algorithms. Thus, in this paper, we apply the following two metrics: (1) false-positive rate (FPR) which is defined as the ratio of the number of honest users that are mistakenly classified as malicious users to the total number of honest users; (2) false-negative rate (FNR) which is defined as the ratio of the number of malicious users that are mistakenly classified as honest users to the total number of malicious users.

In this subsection, the experiment settings are stated as follows: (1) In the user community, there are 100 users in total, among which 25 users are randomly set as honest users, and the remaining 75 users are set as malicious users. For the malicious users, we investigate the cases where their stolen amount of electricity is set as $0.05\sigma_i$, $0.07\sigma_i$, $0.09\sigma_i$, and $0.11\sigma_i$, respectively; (2) We set $\mu_w = 0.8$ and $\sigma_w = 0.32$; (3) In Phase I (i.e., electricity theft detection), we set $h_s = 3.5$, $h_c = 5$, $l = 0.5$, $m_w = 5$, $K_1 = 100$; and we set the initial value of $S_{\bar{w}}(k, j_1)$, i.e., $S_{\bar{w}}(0, j_1)$, as 0; (4) In Phase II (i.e., malicious user detection), if not otherwise stated, we set $h_s = 3.5$, $h_c = 5$, $l = 0.5$, $m_y = 5$, $K_2 = 120$; and we set the initial value of $S_{\bar{y}}(k, j_3)$, i.e., $S_{\bar{y}}(0, j_3)$, as 0.

We investigate how FPR and FNR change when parameters $h_s, h_c, l, S_{\bar{y}}(0, j_3)$ take different values in Phase II. We report the experiment results regarding false positive rates (FPR) for the honest users in Fig. 8. As shown in Fig. 8(a), with the increase of the number of subgroups of users' historical daily electricity consumption for parameter estimation in Phase II, FPR tends to decrease. This is consistent with the fact that parameters $\mu_{\bar{y}}$ and $\sigma_{\bar{y}}$ can be estimated more accurately with more subgroups of users' historical daily electricity consumptions. In Fig. 8(b) $\sim$ Fig. 8(e), we assume that we have three subgroups of users' historical daily electricity consumptions for parameter estimation. From Fig. 8(b), we can see that when the value of l increases from 0.1 to 0.9, the FPR decreases from 0.35 to almost 0. In Fig. 8(c), we can observe that the FPR has a tendency to increase with the value of $S_{\bar{y}}(0, j_3)$. From Fig. 8(d) and Fig. 8(e), we can observe that FPR has a tendency to decrease with values of h_s and h_c, respectively.

We report the experimental results regarding false negative rates (FNR) in Fig. 9.As shown in Fig. 9(a), Fig. 9(c), Fig. 9(d), and Fig. 9(e), for a given amount of users' stolen amount of electricity, FNR does not change a lot with the increase of the following factors: (a) the number of subgroups of users' daily electricity consumptions for estimating $\mu_{\bar{y}}$ and $\sigma_{\bar{y}}$, (b) the initial value of $S_{\bar{y}}(k, j_3)$, (c) the value of h_c, (d) the value of h_s, and e) the value of l. In contrast, we can observe from Fig. 9(b) that for a given amount of users' stolen amount of electricity, FNR increases monotonically with the value of l. Moreover, given any of the above five factors, i.e., factors (a) $\sim$ (e), FNR decreases with the increase of the stolen amount of electricity.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

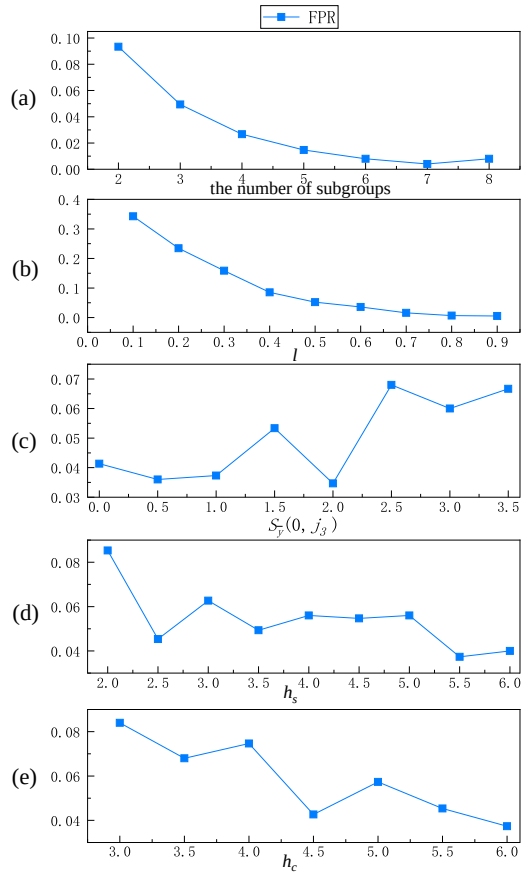


Fig. 8. Excrement results regarding how false positive rates change with the following parameters: (a) the number of subgroups of users' historical daily electricity consumption for estimating $\mu_{\bar{y}}$ and $\sigma_{\bar{y}}$; (2) l; (3) the initial value of $S_{\bar{y}}(k, j_3)$, i.e., $S_{\bar{y}}(0, j_3)$; (4) h_s; (5) h_c.

B. Efficiency

In this subsection, we evaluate the performance of the proposed detector in terms of efficiency. Based upon the discussions in Section V, we specifically investigate the following questions: (1) If malicious users steal electricity, how many samples of $\bar{w}$ (on average) should be involved for the proposed detector to signal the existence of reading anomalies? (2) If the proposed detector has detected the existence of malicious users, how many samples of $\bar{y}$ (on average) should be involved for the proposed detector to identify whether a user is malicious or not? Next, We report experimental results regarding the number of samples of $\bar{w}$ in Phase I (i.e., the electricity theft detection phase) and the number of samples of $\bar{y}$ in Phase II (i.e., the malicious user identification phase).

In this subsection, the experiment settings are stated as follows: (1) we generate 200 users in the community; (2) If the proposed detector can detect the existence of one malicious user, it must detect the existence of multiple malicious users. Thus, we assume that there is only one malicious user in the community. The amount of stolen electricity of this malicious user ranges from $0.1\sigma_i$ to σ_i. (3) We set $\mu_w = 0.8$ and $\sigma_w = 0.32$; (4) We set $K_1 = 100, K_2 = 120$, V=1 and $m_w = m_y = 5$; (5) If not otherwise stated, in both Phase I and Phase II, we set $h_s = 3.5, h_c = 5, l = 0.5$, and set the values of $S_{\bar{w}}(0, j_1)$ and $S_{\bar{y}}(0, j_3)$ as 0.

We report how parameters h_s, h_c, l and the initialized value of $S_{\bar{w}}(k, j_1)$ and $S_{\bar{y}}(k, j_3)$ (i.e., $S_{\bar{w}}(0, j_1)$ and $S_{\bar{y}}(0, j_3)$) impact the average number of samples of $\bar{w}$ and the average number of samples of $\bar{y}$ in Fig. 10, Fig. 11, Fig. 12, and Fig. 13, respectively. As shown in Fig. 10 $\sim$ Fig. 13, in either phase I (i.e., the electricity theft detection phase) or phase II (i.e., the malicious user identification phase), when given any of the following four parameters: (1) h_s, (2) h_c, (3) l, (4) $S_{\bar{w}}(0, j_1)$ and $S_{\bar{y}}(0, j_3)$, the number of samples of $\bar{w}$ (or $\bar{y}$) decreases quickly with the increase of the amount of users' stolen electricity. Particularly, a smaller h_s implies a smaller amount of users' stolen electricity when the number of samples of $\bar{w}$ (or $\bar{y}$) reaches 1. On the whole, for any given amount of stolen electricity, a larger h_s, h_c, or l implies a greater number of samples of $\bar{w}$ (or $\bar{y}$), while a larger $S_{\bar{w}}(k, j_1)$ and $S_{\bar{y}}(k, j_3)$ imply a smaller number of samples of $\bar{w}$ (or $\bar{y}$). On the whole, in all figures of Fig. 10 $\sim$ Fig. 13, when the number of samples of $\bar{w}$ (or $\bar{y}$) is greater than 1, it is the CUSUM control chart that really works in the proposed detector. When the number of samples of $\bar{w}$ (or $\bar{y}$) is 1, it is the Shewhart control chart that really works in the proposed detector.

C. Comparison of the proposed detector with baseline algorithms

In Fig. 14, we generate 200 users in the community, among which 40 users are randomly set as malicious users, and the remaining 160 users are set as honest users. For the malicious users, their amount of stolen electricity ranges from $0.1\sigma_i$ to $1.4\sigma_i$. We compare the proposed detector with the following two baseline algorithms: (1) baseline algorithm 1 which applies only the Shewhart control chart to analyze the above readings or measurements; (2) baseline algorithm 2 which applies only the CUSUM control chart to analyze the above readings or measurements. When the Shewhart and the CUSUM control charts are independently used, we set $h_c = 5, h_s = 3$, $l = 0.5$, $S_{\bar{w}}(0, j_1) = 0$ and $S_{\bar{y}}(0, j_3) = 0$, as recommended in [24]. For the proposed detector where the Shewhart and the CUSUM control charts are combined, we set $h_s = 3.5, h_c = 5$ and $l = 0.5$, as recommended in [39]. For the proposed detector, the values of $S_{\bar{w}}(0, j_1)$ and $S_{\bar{y}}(0, j_3)$ are set as 0 and $\frac{h_c}{2} = 2.5$, respectively. The amounts of malicious users' stolen electricity are expressed in the units of the standard deviation σ_w and σ_i in the electricity theft detection and malicious user identification phase, respectively, as shown on the x-axis.

From Fig. 14(a), we have the following observations: (1) For each detector, the number of samples of $\bar{w}$ decreases fast with the increase of the amount of the malicious user's stolen electricity and finally converges at 1. (2) When the amount of stolen electricity is less than $2.8\sigma_w$, the number of samples of $\bar{w}$ of baseline algorithm 1 is much larger than the detectors applying the CUSUM control chart, and is even too large to be plotted in Fig. 14(a). (3) For the baseline algorithm 2 and the proposed detector with $S_{\bar{w}}(0, j_1) = 0$, we find that given any amount of stolen electricity less than $2.4\sigma_w$, they have almost the same number of samples of $\bar{w}$. When the amount of stolen electricity is between $2.4\sigma_w$ and $5.8\sigma_w$, the number of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal

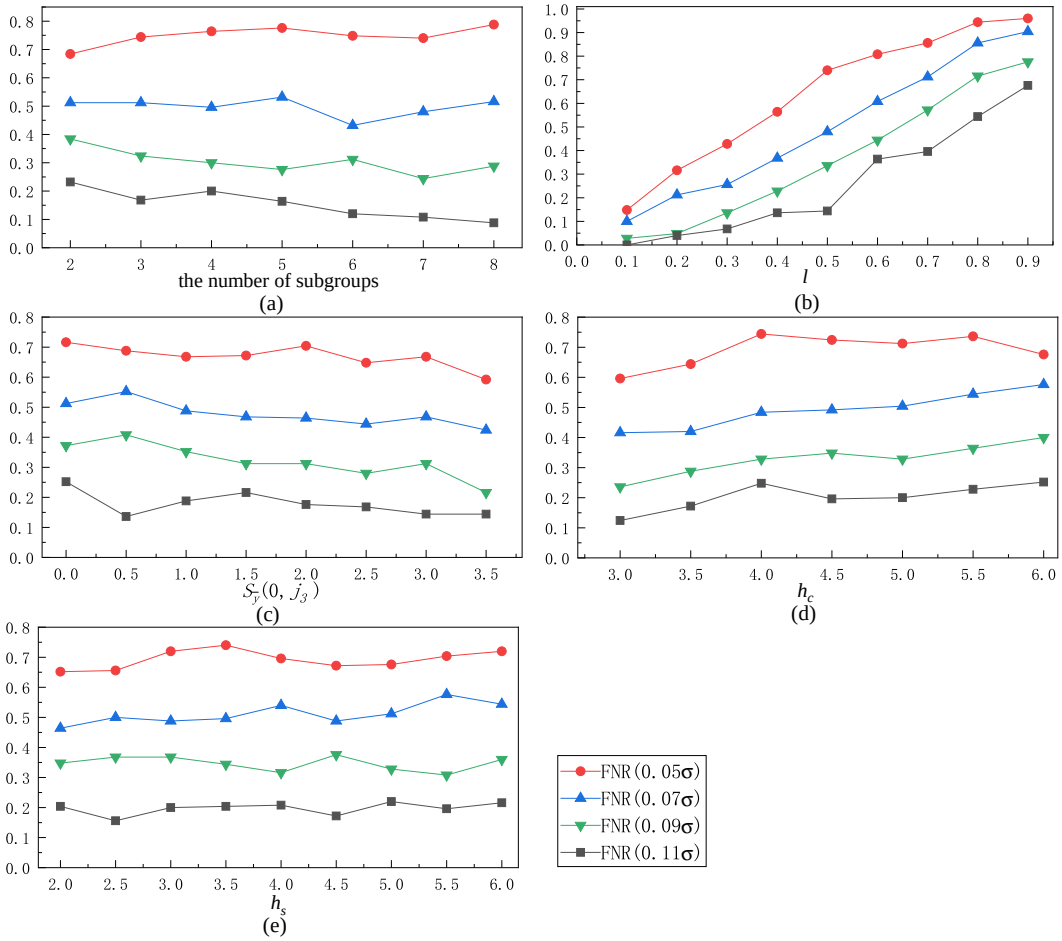
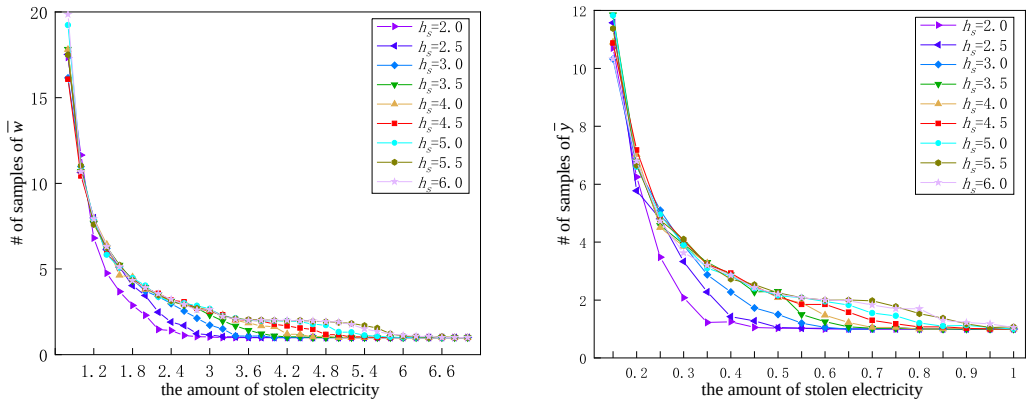


Fig. 9. Experiment results regarding how false negative rates (FNR) change with the following parameters: (a) the number of subgroups of users' historical daily electricity consumption for estimating $\mu_{\bar{y}}$ and $\sigma_{\bar{y}}$; (2) l; (3) the initial value of $S_{\bar{y}}(k, j_3)$, i.e., $S_{\bar{y}}(0, j_3)$; (4) h_s; (5) h_c.

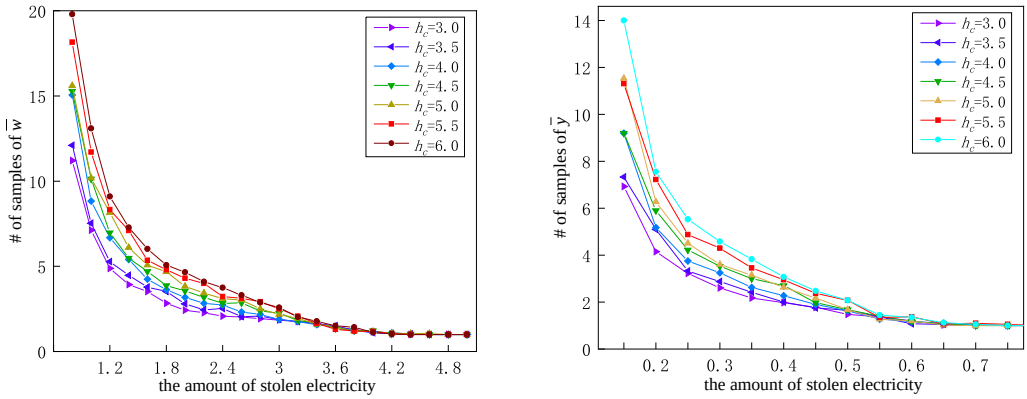


(a) Phase I: electricity theft detection

(b) Phase II: malicious user identification

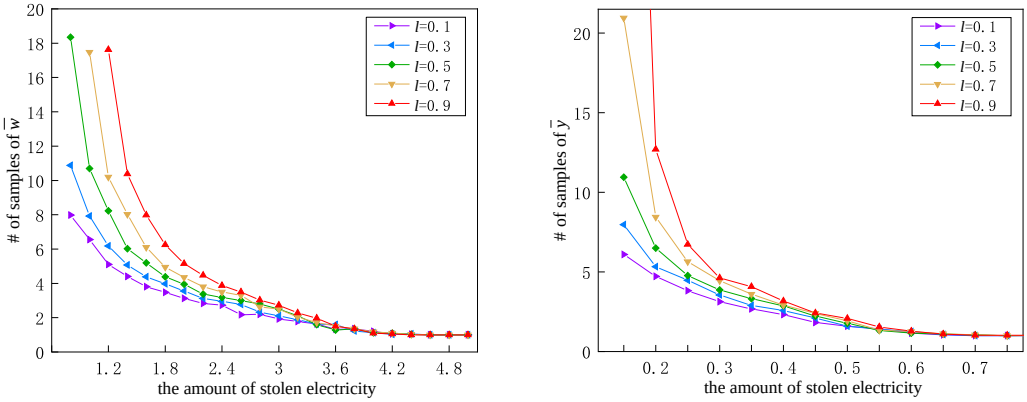
Fig. 10. Experiment results regarding how the parameter h_s affects the average number of samples of $\bar{w}$ in Phase I (or $\bar{y}$ in phase II) . Note: The amount of stolen electricity are measured in the units of the standard deviation σ_w (or σ_i).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal



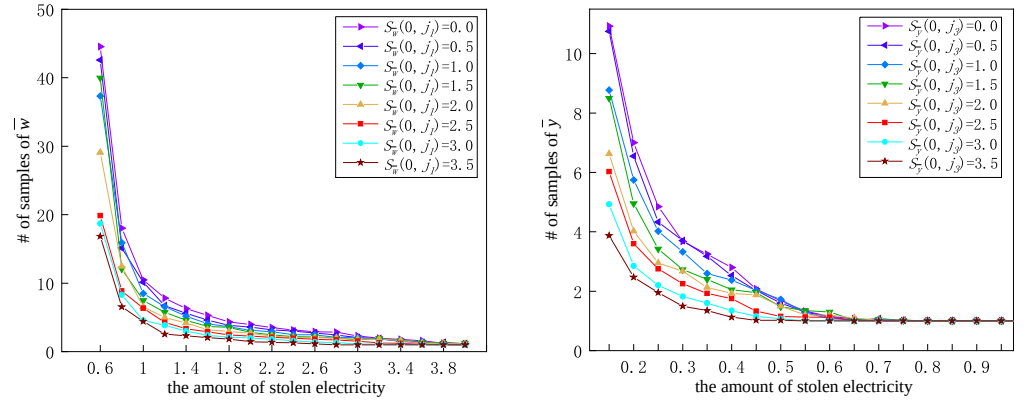
(a) Phase I: electricity theft detection (b) Phase II: malicious user identification

Fig. 11. Excrement results regarding how the parameter h_c affects the average number of samples of $\bar{w}$ in Phase I (or $\bar{y}$ in phase II). Note: The amount of stolen electricity are measured in the units of the standard deviation σ_w (or σ_i).



(a) Phase I: electricity theft detection (b) Phase II: malicious user identification

Fig. 12. Experiment results regarding how the parameter l affects the average number of samples of $\bar{w}$ in Phase I (or $\bar{y}$ in phase II). Note: The amount of stolen electricity are measured in the units of the standard deviation σ_w (or σ_i).



(a) Phase I: electricity theft detection (b) Phase II: malicious user identification

Fig. 13. Experiment results regarding how the parameter S_0 affects the average number of samples of $\bar{w}$ in Phase I (or $\bar{y}$ in phase II). Note: The amount of stolen electricity are measured in the units of the standard deviation σ_w (or σ_i). In Fig. 13(a) and Fig. 13(b), S_0 represents $S_{\bar{w}}(0, j_1)$ or $S_{\bar{y}}(0, j_3)$, respectively.

samples of $\bar{w}$ of the baseline algorithm 2 is greater than that of the proposed detector with $S_{\bar{w}}(0, j_1) = 0$. When the amount of stolen electricity is larger than $5.8\sigma_w$, the average number of samples of $\bar{w}$ is equal to 1. (4) For the proposed detector which applies the Shewhart and the CUSUM control charts together, the number of samples of $\bar{w}$ is obviously smaller in the case $S_{\bar{w}}(0, j_1) = 2.5$ than in the case $S_{\bar{w}}(0, j_1) = 0$.

In Fig. 14(b), we show the curves of the number of samples of $\bar{y}$ in phase II against the amount of stolen electricity for different algorithms. These curves have a similar trend to those in Fig. 14(a), and hence similar conclusions can be reached. Detailed analysis regarding Fig. 14(b) is omitted.

To sum up, we have the following conclusions: (1) when the amount of stolen electricity is very small, the detector which applies only the Shewhart control chart is less efficient than those applying the CUSUM control charts; (2) When the amount of stolen electricity is moderate, the detector which applies only the CUSUM control charts has a lower efficiency than those applying the Shewhart control charts; (3) For the detectors which apply both the Shewhart and CUSUM control charts, when the amount of stolen electricity is large, it is the Shewhart control chart that really works to detect the existence of reading anomalies; (4) For the detectors which apply both the Shewhart and CUSUM control charts, the efficiency is higher in the cases $S_{\bar{w}}(0, j_1) > 0$ than in the cases $S_{\bar{w}}(0, j_1) = 0$.

D. Comparison of the proposed detector with existing algorithms

In Fig. 15, we compare the proposed detector with two existing electricity theft detection techniques in terms of the false-negative rate (FNR). We generate a total number of 200 users in the community, among which 40 users are randomly set as malicious users, and the remaining users are set as honest users.

In Fig. 15(a), we compare it with one machine learning-based detection technique in [14], in which the basic idea is to apply the k-means clustering method and the support vector machine (SVM) classifier together to analyze whether users' electricity consumption patterns are abnormal. This method is termed as "k-Means+SVM" in Fig. 15(a). Let $\alpha(i, j)$ denote the ratio of reported readings and measured readings of user i at period j, i.e., $\alpha(i, j) = \frac{q'(i,j)}{q(i,j)}$. Then, for honest users, we have $\alpha(i, j) = 1$; for malicious users, we have $\alpha(i, j) \in [0, 1)$. This idea is similar to [41]. In Fig. 15(a), we assume that the ratio $\alpha(i, j)$ of malicious users ranges from 0.76 to 0.98. With the increase of $\alpha(i, j)$, which implies that the reported readings of malicious users are more close to their actual electricity consumption, the FNR of the "k-Means+SVM" method increases rapidly. Specifically, when $0.76 < \alpha(i, j) < 0.9$, the FNR of the "$k$-Means+SVM" method increases approximately linearly from almost zero to one. When $\alpha(i, j) \geq 0.9$, the FNR of the "k-Means+SVM" method remains at 1. As for the proposed detector, when $\alpha(i, j) \geq 0.96$, the FNR is lower than 0.05; when $\alpha(i, j) = 0.97$, the FNR is about 0.2; when $\alpha(i, j) = 0.98$, the FNR is about 0.4. To sum up, when the value of $\alpha(i, j)$ ranges from 0.76 to 0.98, the FNR of the proposed detector is much lower than that of the "k-Means+SVM" method in [14].

In Fig. 15(b), we compare the proposed detector with one measurement mismatch based detection technique, i.e., the Adaptive Binary Splitting Inspection (ABSI) algorithm [40], in which the basic idea is to leverage a group testing method to locate malicious users in smart grids. We assume that users' actual technical loss is 6% of their actual electricity consumptions, i.e., $f(i, j) = 0.06q(i, j)$. Furthermore, we assume that the ratio of user i's estimated technical loss to actual technical loss at period j is between 0.9 and 1.1, i.e., $\frac{\tilde{f}(i,j)}{f(i,j)} \in (0.9, 1.1)$. Among the 40 malicious users, there are 2 to 18 malicious users launching SET attacks. For these malicious users, we assume that the amount of their stolen electricity is a random number between $0.02\tilde{f}(i, j)$ and $0.14\tilde{f}(i, j)$. For other malicious users, we assume $\alpha(i, j) \in (0.1, 0.8)$. As shown in the figure, with the number of malicious users launching SET attacks ranging from 2 to 18, the FNRs of both the ABSI algorithm and the proposed detector increase. However, regardless of the number of malicious users launching SET attacks, the FNR of the proposed detector is always much lower than that of the ABSI algorithm.

VII. Conclusions

In this paper, we investigate the issue of electricity theft detection. To address the limitation that existing detection techniques can only detect Large-amount Electricity Theft (LET) attacks, in this paper, we propose a detector that can also detect Small-amount Electricity Theft (SET) attacks. Since the Shewhart and the CUSUM control charts can effectively detect large changes and small changes in the process, they are applied in the proposed detector to detect LET and SET attacks, respectively. The proposed detector consists of two phases: (1) an electricity theft detection phase which aims to detect the existence of electricity theft timely; (2) a malicious user identification phase which aims to identify malicious users exactly. In both phases, the above two control charts are jointly used to analyze users' reported readings and the central observer meter's measurements. We also analyze the efficiency of the proposed detector, mainly by modeling the detection process as a Markov chain. Extensive experiments are conducted to evaluate the proposed detector, and the results show that it has good performance in terms of several metrics.

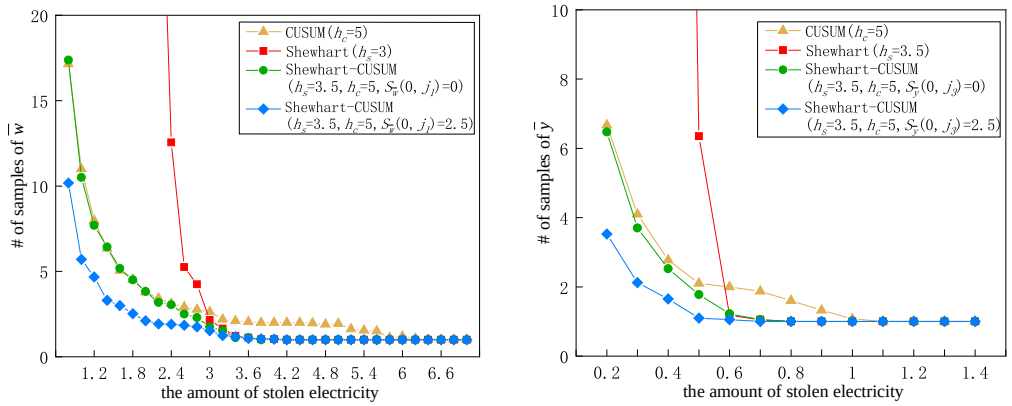
Acknowledgment

Xiaofang Xia, Jian Lin, Jiangtao Cui, and Yanguo Peng's work was supported in part by National Natural Science Foundation of China (NSFC) (No. 61902299, 61976168, 62172314), China Postdoctoral Science Foundation (No. 2019TQ0239, 2019M663636), the Key Research and Development Plan of Shaanxi Province (No. 2019ZDLGY13-09), the Natural Science Basic Research Program of Shaanxi Province (No. 2019CGXNG-023), the Natural Science Basic Research Program of Shaanxi Province (No. 2019CGXNG-023) and S&T Program of Hebei (no. 20310102D).

References

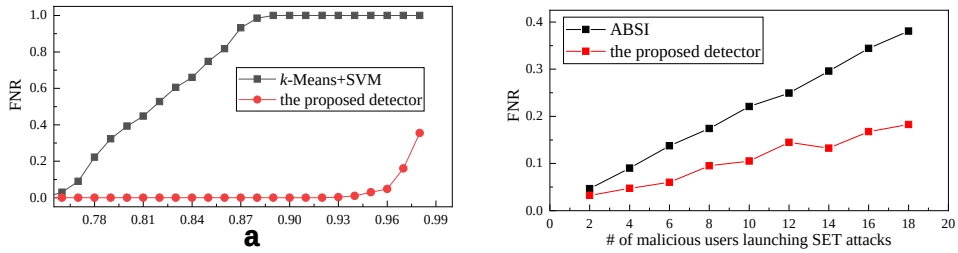
[1] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," *Future*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3113348, IEEE Internet of Things Journal



(a) Phase I: electricity theft detection (b) Phase II: malicious user identification

Fig. 14. Experiment results of comparing the proposed detector and baseline algorithms in terms of the average number of samples of $\bar{w}$ in Phase I (or $\bar{y}$ in phase II). Note: The amount of stolen electricity are measured in the units of the standard deviation σ_w (or σ_i).



(a) (b)

Fig. 15. Simulation results of comparing the proposed detector with: (a) the "k-Means+SVM" method [14]; (b) the ABSI method [40]

Generation Computer Systems, vol. 28, no. 2, p. 391–404, Feb. 2012.

[2] R. Cheena, T. Amgoth, and G. Shankar, "Emperor penguin optimised self-healing strategy for wsn based smart grids," *Int. J. Sens. Netw.*, vol. 32, no. 2, pp. 87–95, 2020.

[3] Grid20/20, inc. (2018) is the power grid going to pot? [Online]. Available: https://grid2020.com/site/download?filename=GRID2020_WP_Is_The_Power_Grid_Going_To_Pot.pdf

[4] 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.

[5] J. Jow, Y.Xiao, and W. Han, "A survey of intrusion detection systems in smart grid," *Int. J. Sens. Netw.*, vol. 23, no. 3, pp. 170–186, 2017.

[6] Northeast Group, LLC. (2014) World loses $89.3 billion to electricity theft annually, $58.7 billion in emerging markets. [Online]. Available: http://www.prnewswire.com/news-releases/world-loses-893-billion-to-electricity-theft-annually-587-billion-in-emerging-markets-300006515.html

[7] L. Northeast Group. (2017) 96 billion dollars is lost every year to electricity theft. [Online]. Available: https://www.prnewswire.com/news-releases/96-billion-is-lost-every-year-to-electricity-theft-300453411.html

[8] H. Arkell. (2014) How middle-class families are turning to crime by getting specialist gangs to 'hotwire' their gas and electricity supplies to beat soaring energy bills. [Online]. Available: http://www.dailymail.co.uk/news/article-2542487/Energy-theft.html

[9] (2018) Theft act 1968. [Online]. Available: https://www.legislation.gov.uk/ukpga/1968/60/contents

[10] Cormac campbell. (2018) dozens jailed for electricity theft over three years. [Online]. Available: https://www.bbc.com/news/uk-northern-ireland-43318845

[11] The jordan times. (2019) 8,836 cases of electricity theft recorded in first half of 2019. [Online]. Available: https://energycentral.com/news/8836-cases-electricity-theft-recorded-first-half-2019

[12] Nltimes. (2020) illegal cannabis cultivators stole €60 million electricity last year. [Online]. Available: https://imabuds.com/illegal-cannabis-cultivators-stole-e60-million-electricity-last-year/

[13] Robert bryce. (2020) how cannabis farms steal megawatts to grow mega-weed. [Online]. Available: https://www.forbes.com/sites/robertbryce/2020/04/20/an-epidemic-of-stealing-watts-for-weed/#7d43ea9372a5

[14] P. Jokar, N. Arianpoo, and V. C. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, May 2016.

[15] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and svm-based data analytics for theft detection in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[16] Z. Zheng, Y. Yang, X. Niu, H. N. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[17] S. E. N. Fernandes, D. R. Pereira, C. C. O. Ramos, A. N. Souza, D. S. Gastaldello, and J. P. Papa, "A probabilistic optimum-path forest classifier for non-technical losses detection," *IEEE Transactions on Smart Grid*, pp. 1–1, 2018.

[18] Z. Xiao, Y. Xiao, and D. H. C. Du, "Exploring malicious meter inspection in neighborhood area smart grids," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 214–226, Mar. 2013.

[19] X. Xia, Y. Xiao, and W. Liang, "SAI: A suspicion

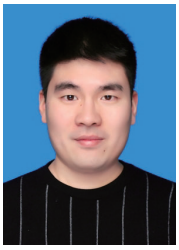
assessment-based inspection algorithm to detect malicious users in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 361–374, 2020.
[20] C. H. Lo and N. Ansari, "Consumer: A novel hybrid intrusion detection system for distribution networks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 33–44, June 2013.
[21] Y. Zhou, Y. Liu, and S. Hu, "Energy theft detection in multi-tenant data centers with digital protective relay deployment," *IEEE Transactions on Sustainable Computing*, vol. 3, no. 1, pp. 16–29, Jan 2018.
[22] W. Han and Y. Xiao, "NFD: non-technical loss fraud detection in smart grid," *Computers & Security*, vol. 65, pp. 187–201, Mar. 2017.
[23] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C. W. Phan, and S.-W. Tan, "Detection of energy theft and defective smart meters in smart grids using linear regression," *International Journal of Electrical Power & Energy Systems*, vol. 91, pp. 230–240, Oct. 2017.
[24] D. C. Montgomery, *Introduction to Statistical Quality Control*, 7th ed. Wiley, 2013.
[25] H. Cheng, J. Liu, T. Xu, B. Ren, and J. M. W. Zhang, "Machine learning based low-rateddos attack detection for sdn enabled iot networks," *Int. J. Sens. Netw.*, vol. 34, no. 1, pp. 56–69, 2020.
[26] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. S. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 105–120, Apr. 2014.
[27] Y. G. Qi, D. R. Martinelli, H. H. Teng, and P. Jiang, "An application of the cusum algorithm to freeway incident detection based on two contiguous detectors," vol. 39, no. 2, pp. 221–240.
[28] B. Sun, X. Shan, K. Wu, and Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks," *IEEE Systems Journal*, vol. 7, no. 1, pp. 13–25, March 2013.
[29] S. M. Ross, *A first course in probability*, 9th ed. Prentice Hall.
[30] K. Doddapaneni, A. Tasiran, F. A. Omondi, E. Ever, P. Shah, L. Mostarda, and O. Gemikonakli, "Does the assumption of exponential arrival distributions in wireless sensor networks hold?" *Int. J. Sens. Netw.*, vol. 26, no. 2, pp. 81–100, 2018.
[31] L. M. O. Queiroz, M. A. Roselli, C. Cavellucci, and C. Lyra, "Energy losses estimation in power distribution systems," *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 1879–1887, Nov 2012.
[32] M. Zanetti, E. Jamhour, M. Pellenz, and M. Penna, "A new svm-based fraud detection model for ami," in *Computer Safety, Reliability, and Security*, A. Skavhaug, J. Guiochet, and F. Bitsch, Eds. Cham: Springer International Publishing, 2016, pp. 226–237.
[33] J. L. Viegas, P. R. Esteves, and S. M. Vieira, "Clustering-based novelty detection for identification of non-technical losses," *International Journal of Electrical Power & Energy Systems*, vol. 101, pp. 301–310, 2018.
[34] J. L. Devore, *Probability and statistics for engineering and the sciences*, eighth edition ed. Cengage Learning.
[35] J. V. Paatero and P. D. Lund., "A model for generating household electricity load profiles," *International Journal of Energy Research*, vol. 30, no. 5, pp. 273–290, 2006.
[36] UCI Machine Learning Repository, (2012) Individual household electric power consumption data set. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/Individual+household+electric+power+consumption/
[37] K. Ghaboosi, M. Latva-aho, Y. Xiao, and B. Khalaj, "Modeling nonsaturated contention-based ieee 802.11 multihop ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3518–3532, Sept. 2009.
[38] D. Brook and D. A. Evans, "An approach to the probability distribution of cusum run length," *Biometrika*, vol. 59, no. 3, pp. 539–549, 12 1972.
[39] J. M. Lucas, "Combined shewhart-cusum quality control schemes," *Journal of Quality Technology*, vol. 14, no. 2, pp. 51–59, 1982. [Online]. Available: https://doi.org/10.1080/00224065.1982.11978790
[40] X. Xia, Y. Xiao, and W. Liang, "ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 445–458, 2019.
[41] W. Han and Y. Xiao, "Nfd: Non-technical loss fraud detection in smart grid," *Computers & Security*, vol. 65, p. 187–201, 2017.

Xiaofang Xia (Member, IEEE) is currently an assistant professor with the School of Computer Science and Technology, Xidian University, China. She received her Ph.D. degree in Control Theory and Control Engineering from Shenyang Institute of Automation, Chinese Academy of Sciences, China, in 2019. She was a visiting student at the Department of Computer Science, University of Alabama, USA, from August 2016 to February 2018. Her research interests are mainly in cyber physical systems, smart grid security, database management system and anomaly detection. Email: xiaofangxia89@gmail.com

Jian Lin is currently pursuing her master degree in the School of Computer Science and Technology, Xidian University, China. She received her B.S. degree in Computer Science and Technology from Xidian University, China, in 2019. Her research interests are mainly in image retrieval and smart grid security. Email: llinjiann@163.com

Yang Xiao (Fellow, IEEE) earned his B.S. and M.S. degrees in computational mathematics from Jilin University, Changchun, China, and his M.S. and Ph.D. degrees in computer science and engineering from Wright State University, Dayton, OH, USA. He is currently a Full Professor with the Department of Computer Science, The University of Alabama, Tuscaloosa, AL, USA. His current research interests include cyber-physical systems, the Internet of Things, security, wireless networks, smart grid, and telemedicine. He has published over 300 SCI-indexed journal papers (including over 60 IEEE/ACM transactions papers) and 250 EI indexed refereed conference papers related to these research areas. He was a Voting Member of the IEEE 802.11 Working Group from 2001 to 2004, involving the IEEE 802.11 (WIFI) standardization work. He is IEEE Fellow and an IET Fellow. He currently serves as the Editor-in-Chief of Cyber-Physical Systems (Journal). He has served as an Editorial Board or Associate Editor of 20 international journals, including the IEEE Transactions on Cybernetics since 2020, IEEE Transactions on Systems, Man, and Cybernetics: Systems (2014-2015), IEEE Transactions on Vehicular Technology (2007-2009), and IEEE Communications Survey and Tutorials (2007-2014). He has served as a Guest Editor over 20 times in different international journals, including the IEEE Transactions on Network Science and Engineering (2021), IEEE Network (2007), IEEE Wireless Communications (2006, 2021), IEEE Communications Standards Magazine (2021), ACM/Springer Mobile Networks and Applications (MONET) (2008), etc. Dr. Xiao had directed 20 doctoral dissertations and supervised 19 M.S. theses/projects in the past.

Jiangtao Cui (Member, IEEE) received the M.S. and Ph.D. degree both in Computer Science from Xidian University, Xi'an, China in 2001 and 2005 respectively. Between 2007 and 2008, he has been with the Data and Knowledge Engineering group working on high-dimensional indexing for large scale image retrieval, in the University of Queensland (Australia). He is currently the execute dean and a professor in School of Computer Science and Technology, Xidian University, China. He has published over 50 journal and conference papers, including VLDB, SIGMOD, ICDE, TKDE, VLDB J, IEEE Transactions on Big Data, etc. His current research interests include data and knowledge engineering, and high-dimensional indexing. He is a distinguished member and a fellow of CCF and is now committee members of CCF TCDB, CCF TCAPP, CCF TCBC. Email: cuijt@xidian.edu.cn



Yanguo Peng (Member, IEEE) received the B.Sc. degree in Network Engineering from North University of China, Taiyuan, China, in 2009, M.S. degree in Computer Software and Theory from Guizhou University, Guiyang, China, in 2012 and Ph.D. degree in Computer Systems Organization from Xidian University, China, in 2016. Currently he is an associate professor in School of Computer Science and Technology, Xidian University, China. he is now a master supervisor. His research interests include cloud security, data privacy protection and blockchain. Email: ygpeng@xidian.edu.cn

Yong Ma received the M.S. degree in computer science from Xidian University, in 2003, and the Ph.D. degree in computer science from Wuhan University, in 2006. In 2018, he worked on the integrated control and dispatching of energy in microgrid with Malardalens University, Sweden. He is now a professor with the School of Computer Information Engineering, Jiangxi Normal University. His current research focuses on cloud computing,edge computing, and data science. Email: may@jxnu.edu.cn