Electricity Theft Pinpointing through Correlation Analysis of Master and Individual Meter Readings

Partha P. Biswas[1], Hongyun Cai[2], Bin Zhou[1], Binbin Chen[3, 1], Daisuke Mashima[1], and Vincent W. Zheng[4]

[1]Advanced Digital Sciences Center, Singapore; e-mail: [partha.b, zhou.bin, daisuke.m]@adsc-create.edu.sg
[2]Tencent, China; e-mail: laineycai@tencent.com
[3]Singapore University of Technology and Design, Singapore; e-mail: binbin_chen@sutd.edu.sg
[4]WeBank, China; e-mail: vincentz@webank.com

***Abstract*—Electricity theft costs utility companies billions of dollars worldwide annually. The electricity consumption data recorded by consumers' smart meters, coupled with the aggregate energy supply data recorded by master meters provide a new opportunity to pinpoint the source of electricity theft. Existing works on electricity theft pinpointing either assume linear attack modes which often limit their capability in identifying nonlinear electricity theft behaviours, or incur extra cost for model training or sensor installation. Our insight hinges upon the fact that the value of electricity theft loss (ETL) should be more correlated to the meter readings of energy thieves than to those of honest consumers. Guided by this insight, we formulate the problem of electricity theft pinpointing as a time-series correlation analysis problem which does not require linearity assumption of attack modes or any cost of training. Two coefficients are defined to evaluate the suspicion level of a consumer's reported energy consumption pattern. A comprehensive set of experiments has been conducted on a real-world energy usage dataset with several types of attacks, and the results show that our proposed technique significantly improves the pinpointing accuracy when compared with other state-of-the-art methods.**

***Index Terms*—Advanced metering infrastructure (AMI); electricity theft; non-technical losses; data analytic for meter reading; correlation analysis.**

NOMENCLATURE

α, β	Factors to scale down original meter readings
δ	Honest coefficient
γ	Energy loss coefficient
$\mathcal{C}$	Set of consumers
$\mathcal{M}$	Set of master meter readings
$\mathcal{S}$	Set of readings reported by consumer smart meters
$\mathcal{T}$	Set of timestamps of meter data recording
$\mathcal{Z}$	List of detected thieves
θ	Threshold setting for honest coefficient
D	Number of days of electricity theft detection
f_s	Meter data sampling frequency per four
K	Selected prediction horizon for precision calculation
L	Set of data for electricity theft loss (ETL)
M'	Set of master meter readings excluding technical loss
N	Number of consumers
n	Indices of consumers, where $n \in \{1, 2, \cdots, N\}$
P	Number of timestamps of meter data recording
U	Set of actual energy usage by the consumers
W	Set of data for technical loss (TL)

I. INTRODUCTION

Electricity theft is defined as the illegal usage of electricity with the intention to evade utility charges. Examples include meter tampering, meter bypassing, tapping on secondary voltages, and more advanced techniques such as by synchronously switching power circuits [1]. A recent survey shows that electricity theft causes an annual loss of more than $89.3 billion worldwide [2], [3]. Detecting electricity theft and pinpointing the consumers who steal the electricity are thus of great importance to utility providers. The growing deployment of advanced metering infrastructure (AMI) has helped to minimize some types of losses [4]. With AMI, conventional mechanical meters are being replaced with smart meters (SM) which provide a two-way communication between utility providers and consumers.

Smart meters bring both new challenges and opportunities to the problem of electricity theft. On one hand, smart meters introduce possibility of new types of network-borne attacks which make the task of electricity theft pinpointing more challenging. On the other hand, unlike old mechanical meters, smart meters have many new features that allow remote monitoring of various electricity consumption indicators throughout the power system with finer granularity [5].

Besides smart meters for individual consumers, utility companies are increasingly deploying smart master meters (MM) that can measure the aggregate energy consumption and provide useful insights of the total consumption pattern of consumers in a neighbourhood area network (NAN). A comparison between the energy measurement by master meter and the sum of readings of all smart meters provides a direct and effective way to detect the occurrence of electricity theft. Note that, in this work, we assume that all meter readings are synchronized in time. We leave the study of electricity theft pinpointing from asynchronous meter readings for the future. When there is no electricity theft, the measurement by master meter and the sum of the measurements from all smart meters in the NAN should match (subject to measurement errors and technical losses). A significant deviation between the two, hence, provides a direct indicator for electricity theft.

Existing machine learning or software-based electricity theft detection and pinpointing methods can be broadly divided into four categories - classification-based, regression-based, state-

based, and game-theory-based. Each category has its own limitations. Firstly, as a supervised learning method, classification usually requires a large amount of labeled training data and extra training time (especially for neural networks). Secondly, the performance of linear regression is not as competitive for non-linear attack modes as it is for the linear attack mode. The attacks are assumed to be linear in many cases to facilitate the implementation of a linear regression model. Thirdly, state-based algorithms use the state from sensors to identify abnormal behaviours. Installation and deployment of these sensors lead to additional hardware and software cost. Lastly, game-theory-based methods can be useful for understanding the potential strategies and interactions among different players. However, the utility company still relies on the previously mentioned methods as the underlying detection mechanisms for electricity theft.

To overcome the above limitations, we propose a **C**orrelation **A**nalysis for **P**inpointing **E**lectricity **T**heft (**CAPET**) scheme. The method requires readings from all smart meters to perform a correlation analysis, thus, avoiding any need of training with datasets unlike machine learning algorithms. Given a smart grid architecture in a NAN, our objective is to find out the energy thieves among the consumers. As illustrated in Fig. 1, our first step is to collect the master meter readings from the distribution station, and the smart meter readings from each consumer's premises. Thereafter, we calculate the ETL (which is also a part of the non-technical losses) suffered by the utility provider by subtracting master meter reading from the sum of all smart meter readings and the technical losses (TL), such as transmission line loss, transformer loss, etc. We then analyze the correlation between the individual smart meter readings and the ETL, as well as between the individual smart meter readings and the master meter reading to derive an energy loss coefficient (γ) and an honest coefficient (δ) for each consumer. The coefficients are then analysed to identify whether or not a consumer is an electricity thief. Our main contributions of the paper are summarized as follows.

- We formulate an electricity theft pinpointing problem based on the availability of power usage readings from a (trusted) master meter and (potentially modified) consumer smart meters. We consider and evaluate few important and practical attack modes.
- We propose a novel correlation analysis-based approach named CAPET to solve the electricity theft pinpointing problem. Leveraging two novel coefficients as indicators, CAPET can effectively identify electricity theft behaviours without any extra training cost or linearity assumption on the attack modes.
- We conduct a systematic evaluation of our approach and compare it with the state-of-the-art baselines over a real-world meter reading dataset. The results show that CAPET outperforms the baselines on the aspects of accuracy for electricity theft pinpointing, robustness against noises and sensitivity to coarse-grained meter readings.

The rest of the paper is organized as follows. The previous works on electricity theft detection are briefly reviewed in Section II. Section III includes definition and formulation for the electricity theft pinpointing problem. Our CAPET scheme is elaborated in Section IV. The experimental set-up and simulation results are discussed in Section V. The article ends with concluding remarks in Section VI.

II. Related Work

Several methods have been employed and studied for electricity theft detection and pinpointing in the past. Viegas et. al. [6] classify the existing techniques on electricity theft detection broadly into three categories - theoretical study, hardware solutions and non-hardware solutions. Theoretical study is based on analyzing geography and demography of an area, while the hardware based methods require special design of metering and sensing equipment to detect frauds. The non-hardware-based solutions are the computational or machine intelligence techniques popularly adopted for electricity theft detection.

We review some of these non-hardware based techniques further and compare with our proposed method below. The **Classification** method trains a classifier based on a set of energy consumption samples. Each sample is labeled as either normal or abnormal behaviour. The trained classifier is then used to distinguish whether or not an unlabeled energy consumption pattern is suspicious. Support vector machine (SVM) is the most popular classification method used in electricity theft pinpointing (e.g., in [3], [7], [8], [9]). Existing efforts on SVM are mainly devoted to two directions. Some of these try different variants of SVM (e.g., one class SVM [10], weighted SVM [11]) to address the problem of imbalanced labels (i.e., the number of thieves is much smaller than the number of honest consumers). Others focus on improving methods for extracting more representative features to enhance detection performance [7], [12]. Recently, researchers have started to exploit deep learning techniques for classification [13]. Instead of feature engineering, a multi-layered neural network structure is constructed to automatically learn the features. Classification is done in the last layer of the neural network. In a recent article, Bihl et. al. [14] discuss the opportunities of data science and data mining methods in electricity theft detection.

Regression analysis finds a function to describe the relationship among variables. A recent work [4] adopts linear regression for electricity theft detection. A linear regression model estimates an anomaly coefficient for each consumer based on the relationship between the consumer's reported consumption and the meter reading discrepancy (i.e., the difference between total energy supply and the sum of meter readings).

State-based detection methods monitor system state to identify the abnormal behaviour in power system. The states can be derived from different sources such as mutual inspection [15], wireless sensor networks [16], control units [17], radio frequency identification [18], and so on. These data work as the supplementary information, which helps to model the electricity theft behaviours more accurately.

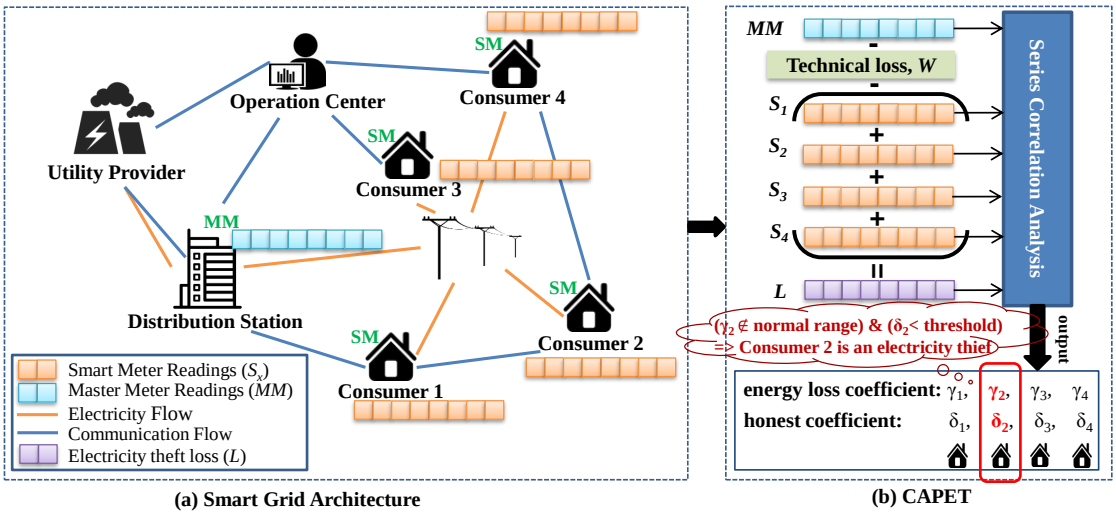


Fig. 1. Framework of CAPET

Another recent solution for electricity theft pinpointing is **game-theory-based** technique [19], [20]. For example, in [19], electricity theft and combat losses are modeled as a non-zero sum Stakelberg game. The distributors deploy AMI to maximize the likelihood of detecting energy thieves, while the attackers schedule their electricity theft behaviours so that the probability of being caught is minimized. A graph theoretic-approach to localize potential fraudulent area in a smart distribution network is proposed in [21].

More details about state-of-the-art electricity theft detection techniques, the attack modes, comparison among the techniques, discussion about some open challenges and potential solutions can be found in recent survey papers [22], [23]. In this article, our proposed CAPET is different from above-mentioned methods. Our scheme is simple, robust, efficient, and effective in identifying the electricity theft behaviour.

In a broader context beyond power systems, Chen et al. [24] studied how to identify a malicious node that injects bad data during a sensor reading aggregation process. However, their approach is to design a secure sensor aggregation protocol to pinpoint the malicious node, while our approach is purely based on the characteristic of the data.

III. Problem Statement

In this section, we formally define the problem of electricity theft pinpointing starting with the introduction of several key concepts.

A. Advanced metering infrastructure in Smart Grid

The architecture of smart grid in a NAN usually consists of four types of nodes: utility provider (UP), distribution station (DS), operation center (OC) and consumers [4]. Fig. 1(a) shows a simple example. UP monitors DS and consumers through OC. The power is distributed through DS to consumers. DS has a **master meter** (MM) to measure the aggregate power supply provided by UP at a predetermined time interval t_i, denoted as MM_i. Meanwhile, each consumer c_n where $n \in \{1, 2, \cdots, N\}$ has a **smart meter** (SM) installed at his premises to record the energy consumption at t_i, denoted as $s_{n,i}$. In the following, we consider readings from the MM and all SMs, and assume that those are time-synchronized.

B. Electricity Theft Attack Modes

Electricity theft is a serious security problem in the smart grid. The energy thieves attack smart meters to pay less electricity bill. Different types of attack modes have been extensively discussed in [10]. In general, there are three common ways of electricity theft.

- The `first` is to reduce the amount of energy consumption by a certain percentage, e.g., multiplying the real utility consumption at every t_i by a constant within $(0, 1)$. This can be carried out in a few different ways. For example, attackers can physically attach magnet to the external current transducers (CTs) to manipulate the current input for the smart meters. Attackers can also tamper a meter's registers that store the calibration coefficients for the meters.
- The `second` is to manipulate the energy consumption at peak time and off-peak time. As people tend to consume more energy at peak time when the electricity charges are higher, switching peak and off-peak time usages can effectively reduce the utility expense. This can be carried out, e.g., by manipulating a meter's clock, or by tampering the settings of the peak and off-peak hours in the meters.
- The `third` is to report some constant readings (e.g., daily average readings or a scaled-down version of it). Reporting daily average reduces the high electricity prices at peak time and achieves similar goal as the second type of attack mode. This can be carried out, e.g., by physically bypassing the actual power carrying circuits, or by manipulating the meter communication channel, e.g., through replay attacks.

In the rest of the paper, we will use these three types of attack modes as examples because they are common and prevalent in the network.

C. Problem Formulation

The input for solving electricity theft pinpointing problem is $\{\mathcal{M}, \mathcal{C}, \mathcal{S}, \mathcal{T}\}$, where $\mathcal{M} = \{MM_1, MM_2, \cdots, MM_P\}$ is the series of master meter readings with MM_i denoting

the master meter reading at time t_i. $\mathcal{C} = \{c_1, c_2, \cdots, c_N\}$ denotes a list of N consumers. $\mathcal{S} = \{S_1, S_2, \cdots, S_N\}$ is the set of readings reported by consumers' smart meters, where $\mathcal{S}_n = \{s_{n,1}, s_{n,2}, \cdots, s_{n,P}\}$ denotes the series of smart meter readings of consumer c_n, with $s_{n,i}$ representing the smart meter reading at the house of c_n at time t_i. Note that for energy thieves, their S_n's have been manipulated by themselves and do not equal to their real energy consumption. $\mathcal{T} = \{t_1, t_2, \cdots, t_P\}$ is the set of timestamps when the meter readings are recorded. The interval of every two consecutive timestamps in $\mathcal{T}$ is consistent and predetermined. Given $\{\mathcal{M}, \mathcal{C}, \mathcal{S}, \mathcal{T}\}$, our OBJECTIVE is to identify energy thieves from $\mathcal{C}$.

Our **assumptions** include: 1) all consumers have smart meters installed in their houses. 2) the master meter is installed at the low-voltage side of the transformer, i.e., it measures power consumption at the same voltage level as the smart meters. With this assumption, the power loss due to the transformer does not affect the relationship between the readings of the master meter and the smart meters. 3) an electricity thief can only attack the smart meter installed at his own house, but not the master meter. 4) the readings of smart meters and the master meter are available at regular intervals and are recorded in a synchronized manner. The first two assumptions hold true in many parts of the world today where advanced metering infrastructure has been deployed. The third assumption is also a natural one since the master meter is usually installed in the substation with physical protection. In relation to the third assumption it may also be noted that, if theft happens by tapping from a common bus or shared cable where more than one consumer is connected, the CAPET cannot pinpoint the thief consumer(s). The CAPET scheme is also unable to detect in a scenario when an electricity thief reports scaled-down readings of his own and at the same time shows overusage of other consumer(s), thus being able to elude mismatch at the master meter. The fourth assumption is valid when GPS-based clock synchronization is utilized.

It may further be noted that an electrical network has also another TL (apart from transformer loss) in the form of transmission line loss which is unavoidable due to inherent resistance of the conductors. The TL of electrical network can be calculated by study of the power system (e.g. power flow). When there is no theft, the readings of smart meters together with the TL would be equal to the reading of the master meter. Let us assume a scenario when one or more smart meter readings have been manipulated with the intention of electricity theft. The system TL can be obtained by running a power flow study using all the smart meter readings, whether tampered or not. Now, this TL value when added to all the smart meter readings will not be equal to the master meter reading. Thus, a case of electricity theft can be suspected. The correlation analysis described subsequently helps to find the consumers who have manipulated the readings for stealing electricity.

IV. CAPET SCHEME

The core idea of CAPET is to identify energy thieves by analyzing the correlations between each consumer's smart meter readings (S_n) and the ETL (L) that the utility provider (UP) suffers. The intuition is that the ETL exists due to the electricity theft behaviours. Hence the values of ETL over time should be more related to the smart meter readings of energy thieves than those of the honest consumers. Next, we will discuss on how to identify energy thieves by analyzing the correlation between ETL and smart meter readings.

A. Preparation

Firstly, we need to derive the values of ETL over time i.e., $L = \{l_1, l_2, \cdots, l_P\}$. The reliable master meter reading at time t_i is MM_i. The TL (say, w_i) is subtracted from the master meter reading to obtain a usable reading m_i i.e.

$$m_i = MM_i - w_i \tag{1}$$

Please note that the w_i at time t_i can be calculated by running power flow with all smart meter readings of consumers at time t_i (i.e., $s_{n,i}, \forall n \in [1, N]$) as mentioned before. Though some smart meters may have been compromised with the intention of electricity theft, the TL would not have been much different had all the meters reported legitimate consumption values. Moreover, the condition has insignificant influence on our correlation analysis. Now, ETL can be calculated by subtracting the sum of all smart meter readings from the usable master meter reading m_i. The usable master meter reading m_i is loosely termed as master meter reading in rest of the article. Mathematically, the ETL at time t_i can be expressed as:

$$l_i = m_i - \sum_{n=1}^{N} s_{n,i} \tag{2}$$

We denote the real energy usages for consumer n as $U_n = \{u_{n,1}, u_{n,2}, \cdots, u_{n,P}\}$, it is easy to derive that

$$m_i = \sum_{n=1}^{N} u_{n,i} \tag{3}$$

B. Correlation-based Electricity Theft Pinpointing

In this section, we use some common types of electricity theft attack modes (introduced in Sect. III-B) to illustrate why the correlation between L and S_n can be used to evaluate the suspicion level of a consumer.

The first question is how to derive the correlation between the two series. There exist many effective algorithms for series correlation analysis, such as Pearson correlation [25], cross-correlation analysis [26], Canonical correlation analysis [27], etc. In this paper, we adopt the most widely used correlation method, Pearson correlation analysis as an illustrative example. For two given variables, Pearson correlation analysis learns a correlation coefficient between $[-1, 1]$, which describes to what extent the two variables are related to each other. We can easily adapt our CAPET to other series correlation analysis methods. We denote the Pearson correlation between L and S_n as $PearsonCorr(L, S_n)$.

1) Attack I: Scale Down Readings by Proportion: Recall that one way of electricity theft is to multiply $u_{n,i}$ by a coefficient $\alpha_i \in (0,1)$. Then we get $s_{n,i} = \alpha_i u_{n,i}$ if consumer c_n is an electricity thief, and $s_{n,i} = u_{n,i}$ if c_n is honest. Based on Eq. 2 and Eq. 3, we can derive:

$$\begin{aligned} l_i &= m_i - \sum_{n=1}^{N} s_{n,i} = \sum_{n=1}^{N} u_{n,i} - \sum_{n=1}^{N} s_{n,i} \\ &= (\frac{1}{\alpha_i} - 1) \sum_{c \in thieves} s_{c,i} \end{aligned} \tag{4}$$

Since $\alpha_i \in (0,1)$, we have $(\frac{1}{\alpha_i} - 1) > 0$. ETL in Eq. 4 is **positively correlated** to the $s_{n,i}$'s of **energy thieves**.

2) Attack II: Decrease Peak Consumption and Increase Off-peak Consumption: Another type of electricity theft is to reduce the consumption at peak-time and increase the consumption at off-peak time. One way is to switch the peak-time energy usage with the off-peak-time usage. For example, the thieves can shift the daily consumption by certain hours (say t_{sh}). Assume the time interval of meter reading is one hour, then the daily smart meter readings become $s_{n,i} = u_{n,i+t_{sh}}$, where $i \in [1, 24]$. We then get:

$$\begin{aligned} l_i &= m_i - \sum_{n=1}^{N} s_{n,i} = \sum_{n=1}^{N} u_{n,i} - \sum_{n=1}^{N} s_{n,i} \\ &= \sum_{c \in thieves} (s_{c,i+t_{sh}} - s_{c,i}) \end{aligned} \tag{5}$$

Note that:

$$\begin{aligned} &PearsonCorr(L, S_n) = \frac{Cov(L, S_n)}{\sigma_L \sigma_{S_n}} \\ &= \frac{Cov(\sum_{c \in thieves} U_c, S_n) - Cov(\sum_{c \in thieves} S_c, S_n)}{\sigma_L \sigma_{S_n}} \end{aligned} \tag{6}$$

where $Cov(X, Y)$ is the covariance between X and Y. σ_X is the standard deviation of X, which is always larger than zero. Due to the peak-time and off-peak time utility usage pattern, for an electricity thief c_n, S_n is negatively correlated to $\sum_{c \in thieves} U_c$ and positively correlated to $\sum_{c \in thieves} S_c$. This has been verified on the real world dataset used in this work. Hence, ETL in Eq. 5 is **negatively correlated** to the reported consumption S_n's of **energy thieves**.

3) Attack III: Report Daily Average Readings: A third type of electricity theft is to report the energy consumption based on the average value, i.e., $s_{n,i} = \beta_i \text{mean}(U_n)$, where $\beta_i \in (0,1)$. The ETL in this case is:

$$\begin{aligned} l_i &= m_i - \sum_{n=1}^{N} s_{n,i} = \sum_{n=1}^{N} u_{n,i} - \sum_{n=1}^{N} s_{n,i} \\ &= \sum_{c \in thieves} (u_{c,i} - \beta_i mean(U_c)) \end{aligned} \tag{7}$$

Under this type of attack, Eq. 6 becomes:

$$\begin{aligned} &PearsonCorr(L, S_n) \\ &= \frac{Cov(\sum_{c \in thieves} U_c, S_n) - Cov(\sum_{c \in thieves} \beta_i mean(U_c), S_n)}{\sigma_L \sigma_{S_n}} \end{aligned} \tag{8}$$

Note that $\beta_i mean(U_c)$ in above equations is a nearly flat consumption pattern with little fluctuation decided by β_i, hence the second term $Cov(\sum_{c \in thieves} \beta_i mean(U_c), S_n)$ in Eq. 8 is nearly zero. Then $PearsonCorr(L, S_n)$ mostly depends on the first term $Cov(\sum_{c \in thieves} U_c, S_n)$.

Because consumers' daily energy consumption patterns share certain similarities, the correlation between any two honest consumers' consumption (i.e., the consumption before malicious tampering) falls within a reasonable range (see Sect. V-B and Fig. 6 for more details). Then for an honest consumer, $PearsonCorr(L, S_n)$ in Eq. 8 should be within a reasonable range. Based on our experiments (Sect. V-B), the lower bound of this range is usually larger than 0.001. Meanwhile, a dishonest consumer does not have the similar consumption pattern as he reports $\beta_i mean(U_c)$ instead. Consequently, he will derive a correlation score significantly smaller than the normal lower ranges. In our experiments, we find the energy thieves usually get a correlation score smaller than $1e-10$. In summary, the ETL in Eq. 7 has **an extremely small correlation** to the reported consumption of **energy thieves**, usually lower than $1e-10$.

4) Attack IV: Mixture of Multiple Attack Modes: The most complicated scenario is when all the above electricity theft attack modes exist at the same time. In this work, we assume that the attackers are not coordinated with each other. Under the setting of multiple types of attacks, $\sum_{c \in thieves} S_c$ in $PearsonCorr(L, S_n)$ (Eq. 6) is now the combination of multiple types of malicious readings. Then for each single electricity thief c_n, $Cov(\sum_{c \in thieves} S_c, S_n)$ would be relatively small (no matter positive or negative), because there is a mixture of hybrid consumption patterns in $\sum_{c \in thieves} S_c$. Consequently, the correlation $PearsonCorr(L, S_n)$ (Eq. 6) mostly depends on the value of $Cov(\sum_{c \in thieves} U_c, S_n)$. In multiple attack modes, $Cov(\sum_{c \in thieves} U_c, S_n)$ keeps the same as in single attack mode because $\sum_{c \in thieves} U_c$ is the real consumption before tampered. Thieves using attack mode I will receive large positive correlation values, while thieves using attack mode II will get large negative correlation values. Thieves adopting attack mode III will obtain extremely small correlation values.

From the above examples, we observe that there is a normal range of values for correlation between ETL and the honest consumers' smart meter readings. If the correlation between L and S_n is either too high (positively or negatively) or too low, c_n is very likely to be an electricity thief. Hence we can use correlation analysis to judge whether or not a consumer is an electricity thief. The next question is how to systematically define the suspicion level of a consumer based on the correlations.

C. Energy Loss Coefficient and Honest Coefficient

We now introduce two correlation-based coefficients used in our CAPET for electricity theft pinpointing.

Energy loss coefficient (denoted as $\gamma \in [0,1]$) describes the absolute value of the correlation between the ETL (L) and smart meter readings (S_n). Denote the correlation between L and S_n as $PearsonCorr(L, S_n)$, the γ_n of consumer c_n is defined as:

$$\gamma_n = |PearsonCorr(L, S_n)| \tag{9}$$

where $|x|$ is the absolute value of x. By using the absolute values of Pearson correlation coefficients, our energy loss coefficient unifies both positive and negative correlations. As mentioned before, γ values of honest consumers are within a normal range. The consumers with extreme small γ ($< 1e$–10) values are first identified as energy thieves. We then define the list of remaining consumers as $\mathcal{R}$ and arrange the list in descending order based on their γ values. The larger the γ is, the more likely that consumer has manipulated his smart meter readings.

Though many energy thieves possess large γ values, not all consumers with large γ values are energy thieves. For example, if consumer c_i has similar energy consumption behaviour with the electricity thief c_j, γ_i will also get a relatively large value due to the high correlation between S_i and S_j. If we rely only on γ to identify thieves, very likely c_i will be mistakenly judged as an electricity thief. In consideration of this limitation, we define another coefficient to refine the suspicious consumer list that has been derived based on γ, so as to decrease the false positive rate.

Honest coefficient (denoted as $\delta \in [0, \infty)$) describes the honest level of a customer. The idea is to compare $PearsonCorr(L, S_n)$ and $PearsonCorr(M', S_n)$ where $M' = \{m_1, m_2, ..., m_P\}$, the set of master meter readings excluding the TL. If the latter is larger, the consumer is more likely to be innocent even though his γ is relatively large. This is because master meter readings M' consist of the total consumption of all households in the neighbourhood while ETL (L) is related to the thieves' consumption only. A thief's consumption should be more related to ETL than to the master meter readings. We define δ_n of consumer c_n as:

$$\delta_n = \left| \frac{PearsonCorr(M', S_n)}{PearsonCorr(L, S_n)} \right| \tag{10}$$

A larger δ_n indicates that S_n is more related to the master meter reading (M') than to ETL (L). Hence the larger the δ_n is, the more honest the consumer c_n is. We can then use δ to refine the suspicious consumer list constructed based on γ, i.e., the consumers with δ bigger than a threshold will be considered as innocent and removed from the list $\mathcal{R}$. The value of the threshold can be tuned as described in Section V-B.

It is worth noting that an alternative way of correlation-based electricity theft pinpointing is to directly analyze the correlation between the smart meter reading of each consumer, S_n and the reading of master meter, M'. Intuitively, the energy consumption of honest consumers should have higher correlations with the master meter reading. However, due to the large number of smart meters, it is hard to correctly find the correlation between M' and each individual S_n, leading to a bad performance. In our CAPET, we utilize the advantage that only a limited number of thieves exist in the smart grid NAN. Therefore, instead of analyzing the correlation between S_n and M', we calculate the correlation between S_n and L to derive the energy loss coefficient, γ.

D. End-to-end Analysis

Given the input of $\{\mathcal{M}, \mathcal{C}, \mathcal{S}, \mathcal{T}\}$, we first find the TL ($w_i$) by running power flow analysis at time t_i with the available consumption data, and subsequently calculate usable master meter reading m_i using Eq. 1 and ETL (l_i) using Eq. 2 for each time stamp t_i where $t_i \in \mathcal{T}$ and $i \in [1, P]$. We formulate sets $W = \{w_1, w_2, ..., w_P\}$, $M' = \{m_1, m_2, ..., m_P\}$ and $L = \{l_1, l_2, ..., l_P\}$. After that, for each consumer c_n, we calculate an energy loss coefficient (γ_n in Eq. 9) and an honest coefficient (δ_n in Eq. 10). Next we identify consumers with $\gamma < 1e-10$ (if any) as energy thieves and then sort the rest of the consumers in descending order in a list (denoted as $\mathcal{R}$) based on their γ values. Thereafter, we refine the list $\mathcal{R}$ by removing the consumers with δ higher than a predefined threshold θ. In the end, the consumers with $\gamma < 1e$–10 take the top of our detected **List-of-thieves** (say $\mathcal{Z}$), followed by some consumers with few largest γ values. The steps involved in CAPET scheme for electricity theft pinpointing are provided in Algorithm 1. Finally, the list $\mathcal{Z}$ is utilized to calculate the average precision described in Sect. V-A.

Algorithm 1 : CAPET Scheme

```
Input : {M, C, S, T}, threshold θ; Output : List-of-thieves, Z
At time t_i, calculate TL (w_i) by running power flow using s_{n,i} ∀n ∈ C,
  where s_{n,i} ⊂ S
Subsequently, calculate usable master meter reading m_i (where m_i ⊂
  M) using Eq. 1 and ETL (l_i) using Eq. 2
Define sets W, M' and L with values of w_i, m_i and l_i, respectively,
  for all t_i ∈ T
Calculate energy loss coefficient (γ_n) for each consumer c_n applying Eq.
  9 that utilizes S_n (where S_n = {s_{n,1}, s_{n,2}, ..., s_{n,P}}) and L
Calculate honest coefficient (δ_n) for each consumer c_n applying Eq. 10
  that utilizes S_n, L and M'
Initialize Z = Empty set, ∅
for all c_n ∈ C do
    if γ_n < 1e−10 then
        Include c_n into Z
    end if
end for
Develop list R with consumers c_n for c_n ∈ C but c_n ∉ Z
Sort R in descending order based on γ values
for all c_n ∈ R do
    if δ_n > θ then
        Remove c_n from R
    end if
end for
Append list R to list Z so that Z = Z ∪ R
```

V. Evaluation

In this section, we study the performance of CAPET and evaluate it against the baselines on a real-world energy consumption dataset.

A. Experimental Setup

Dataset: We use the openly available Smart*[1][28] dataset. Smart* contains energy consumption data for 114 single-family apartments located in Western Massachusetts. We use

[1]http://traces.cs.umass.edu/index.php/Smart/Smart

the available real power consumption data of every minute for each apartment over 349 consecutive days in the year 2016, beginning from 1st January, 2016. Therefore, the raw dataset contains 349x24x60 real energy usage values for each apartment (i.e. each consumer). We format the dataset to 5-minute energy usage series by picking the wattage consumption values after every 5 minutes, starting from the 1st minute. After preprocessing, each consumer has 349x24x12 real energy usage values. For the sake of repeatability, we have published our data preprocessing and theft data generation codes in our Github repository[2].

Attack modes simulation: Due to lack of labeled electricity theft datasets in real world, we simulate the attack modes introduced in Sect. III-B. We follow the settings in a recent study [10], and adopt both time-invariant and time-dependent coefficients to scale down the original meter readings. We denote $u^d_{n,i}$ as the energy usage for consumer c_n on day d at timestamp t_i; then the energy usage series of c_n on day d (24 hours) is $U^d_n = \{u^d_{n,1}, u^d_{n,2}, \cdots, u^d_{n,24f_s}\}$, where f_s is the meter data sampling frequency per hour and it has a value of 12 for 5-minute sampling frequency. We randomly pick a certain percentage of consumers alongwith their consumption data daily to generate malicious samples. Each selected daily consumption data series is contaminated with one of the following six types of attacks where attack modes I, II and III relate to the modes described in Sect. IV-B:

- Attack I: Report scaled-down readings
  (a) $s^d_{n,i} = \alpha_n u^d_{n,i}$, generate $\alpha = random(0.1, 0.8)$
  (b) $s^d_{n,i} = \alpha_{n,i} u^d_{n,i}$, generate $\alpha = random(0.1, 0.8)$
- Attack II: Report time-shifted readings
  (a) $s^d_{n,i} = u^d_{n,mod(i+f_s t_{fsh}, 24f_s)}$
  (b) $s^d_{n,i} = u^d_{n,mod(i+f_s t_{vsh}, 24f_s)}$
  where t_{fsh} and t_{vsh} are the fixed and variable timeshifts, respectively, and $mod(p, CONST)$ operator loops back the variable index p to the beginning when $p > CONST$.
- Attack III: Report daily average readings
  (a) $s^d_{n,i} = \beta_{n,i}\text{mean}(U^d_n)$, generate $\beta = random(0.1, 0.8)$
  (b) $s^d_{n,i} = \text{mean}(U^d_n)$

Generation of above-mentioned malicious samples facilitates us to study and compare our CAPET with the baselines under multiple attack modes. Attack mode I(a) multiplies the readings by the same randomly chosen value for a consumer, while attack mode I(b) multiplies the readings by different random values at different timestamps. Attack mode II [i.e., II(a) and II(b)] considers timeshift of actual daily consumption data, as if in a cyclical manner. In reality, in this attack mode, the attacker will shift part of his daily energy usage series by certain hours which can maximize his gain. For our experiments, we consider a fixed timeshift i.e., $t_{fsh} = 4$ hours for all meters in attack mode II(a) and a meter specific time drift (t_{vsh}) in attack mode II(b). In attack mode II(b), the consumers will have randomly assigned timeshifts of any hours within the range of 1 to 6 hours. Attack modes III(a) and III(b) report the discounted and exact values of the average readings, respectively, over the day. Further, please note that there is one more attack mode in [10]. However, it can be easily solved by considering hourly meter readings and processing the hourly consumption pattern the same way as the daily consumption pattern. The master meter reading on day d at timestamp t_i can be derived as $m^d_i = \sum_{n=1}^{N} u^d_{n,i}$, while the ETL is calculated as $l^d_i = m^d_i - \sum_{n=1}^{N} s^d_{n,i}$. TL is not calculated in our experiment as the attack datasets are synthesized from real consumption data and distribution network parameters are not known. However, the same can be incorporated in the study as explained elsewhere in the article.

[2]https://github.com/ppbiswas/CAPET

Baselines: We choose two state-of-the-art baselines in electricity theft pinpointing: a classification-based method and a regression-based method.

- Consumption pattern-based energy theft detector (CPBETD) [10] is an SVM based electricity theft pinpointing model. It first shortlists the suspicious consumers by comparing the total amount of usage reported by the smart meters with the master meter readings. If a loss is detected, consumers in this area are selected as suspicious users. The method then trains an SVM classifier to predict whether a consumer is honest. Note that the labeled malicious data samples are simulated using some of the above-mentioned attack modes.

- Linear regression-based scheme for detection of energy theft and defective smart meters (LR-ETDM) [4] fits consumers' energy utilization behaviours and the ETL into a linear regression model, so as to learn an anomaly coefficient for each consumer.

- CAPET-γ is a degenerated version of our CAPET. The method identifies theft using only energy loss coefficient (γ) values. This is to verify the importance of considering δ together with γ.

Evaluation metric: We evaluate the performance of electricity theft pinpointing using mean average precision (MAP) [29] which is the mean of average precision for each query. As we detect the energy thieves daily, MAP is calculated as the mean of average electricity theft detection precision values of each day.

$$MAP@K = (\sum_{d=1}^{D} AveP@K(d))/D \tag{11}$$

where D is the number of days we detect energy thieves and the $AveP@K$ is defined as $AveP@K = \frac{\sum_{n=1}^{K} Prec(n) \times rel(n)}{min(N_{th}, K)}$, where $Prec(n)$ is the precision at the top n thieves in the detected list, K is the number of elements up to which prediction is considered for precision calculation, N_{th} is the actual number of thieves. $rel(n)$ equals to one if the n-th consumer in the list is a thief, zero otherwise. An MAP value of 1 signifies that all thieves have been correctly identified over all days accounted for. To further elaborate, suppose on a particular day, there are 10 electricity thieves. The CAPET scheme will output a predicted list of 10 or a different number of potential thieves. The order in the predicted list is important as AveP@K considers top K entries in the predicted list. If

top 5 thieves in the predicted list are actual thieves, AveP@5 will be 1. Now, when AveP@5 is 1 for all the days considered in the study, MAP@5 will also be 1. AveP@K will continue to yield 1 with the increase in K until we encounter the first wrongly identified thief in the predicted list. There are a couple of advantages in adopting MAP as the evaluation metric. Firstly, we can get rid of manual tuning of a threshold for γ. Secondly, $MAP@K$ evaluates the ranking performance instead of precision. In a case, the higher we rank energy thieves in the list, the larger the corresponding MAP is. This is consistent with the real needs of utility provider for decreasing the false positive rate.

B. Results and Analysis

We compare our CAPET with the baselines and evaluate the performance under different settings. We randomly pick certain percentages of daily energy consumption data - 1% in Case 1, 5% in Case 2 and 10% in Case 3 - to generate malicious samples under mixed mode of attacks. In each case, the process is repeated 30 times to create different attack datasets for performance evaluation. For CPBETD, we follow the settings of RBF kernel [10] and apply grid search to find the appropriate values for kernel parameter, ζ and a penalty term, Q in SVM (ζ = 0.01, Q=1). As CPBETD requires labeled data for training, we randomly select 80% of data for training, and the rest for testing. All baselines use the same test data for a fair comparison. For our CAPET, we assume one master meter in each dataset unless specified otherwise in a case study, and we tune to find the threshold of δ within the range $[0.7, 1.3]$ with the same validation set used by SVM. Finally, the threshold (i.e., θ) for δ is set at 1 for the dataset.

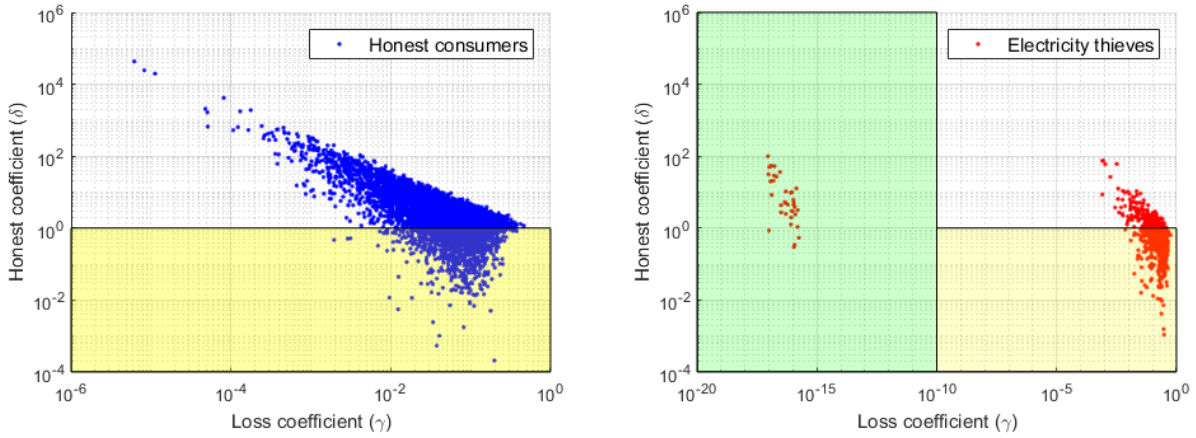
1) Comparison with baselines: Table I shows the statistical summary of results for electricity theft pinpointing across different attack datasets generated from multiple runs. Mean and maximum values of MAP obtained by CAPET are always the best for any number of thieves in the datasets and the K values. In the table, the best mean and maximum MAP values and those within 5% of the best are highlighted in bold font. The standard deviation is low in all cases, signifying a little variation in precision across different attack datasets. It is worthwhile to mention that in Case 1 (1% thief consumers), only one thief exists on each day. SVM fails to catch the thief consumer for any attack dataset, resulting in 0 precision values. CAPET (and CAPET-γ) correctly predicts the thief consumer in most occasions. However, the MAP value does not vary with the change in K as CAPET (and CAPET-γ) generated suspicious list contains one thief on each day, which is in congruence with the synthesized attack dataset. The LR-ETDM predicts more number of thieves per day.

Between CAPET and CAPET-γ, the combined usage of δ and γ in CAPET improves the MAP in all cases, and the improvement is significant when the number of thieves is higher (in Case 3 - 10% thief consumers). This fact reinstates the importance of both γ and δ in our CAPET. In general, the performance of LR-ETDM is found to be poor. This is due to the presence of many non-linear attack modes in our experimental setup. The linear regression model of LR-ETDM does not fit well in hybrid attack models.

TABLE I
STATISTICAL SUMMARY OF ELECTRICITY THEFT PINPOINTING

			MAP@K			
			LR-ETDM [4]	CPBETD [10]	CAPET-γ	CAPET
Case 1: 1% thief consumers	K = 2	Min	0.171	0.000	0.800	0.800
		Max	0.257	0.000	**0.857**	**0.857**
		Mean	0.201	0.000	**0.828**	**0.832**
		SD	0.020	0.000	0.013	0.016
	K = 4	Min	0.182	0.000	0.800	0.800
		Max	0.265	0.000	**0.857**	**0.857**
		Mean	0.211	0.000	**0.828**	**0.832**
		SD	0.020	0.000	0.013	0.016
	K = 6	Min	0.185	0.000	0.800	0.800
		Max	0.268	0.000	**0.857**	**0.857**
		Mean	0.218	0.000	**0.828**	**0.832**
		SD	0.019	0.000	0.013	0.016
	K = 8	Min	0.191	0.000	0.800	0.800
		Max	0.270	0.000	**0.857**	**0.857**
		Mean	0.222	0.000	**0.828**	**0.832**
		SD	0.018	0.000	0.013	0.016
	K = 10	Min	0.192	0.000	0.800	0.800
		Max	0.270	0.000	**0.857**	**0.857**
		Mean	0.224	0.000	**0.828**	**0.832**
		SD	0.018	0.000	0.013	0.016
Case 2: 5% thief consumers	K = 2	Min	0.000	0.307	0.950	0.964
		Max	0.021	0.382	**0.993**	**1.000**
		Mean	0.005	0.345	**0.974**	**0.983**
		SD	0.005	0.022	0.010	0.010
	K = 4	Min	0.000	0.174	0.667	0.709
		Max	0.011	0.222	**0.763**	**0.770**
		Mean	0.003	0.200	0.702	**0.739**
		SD	0.003	0.011	0.020	0.017
	K = 6	Min	0.000	0.153	0.555	0.586
		Max	0.009	0.192	**0.624**	**0.645**
		Mean	0.003	0.171	0.580	**0.614**
		SD	0.002	0.010	0.016	0.016
	K = 8	Min	0.000	0.153	0.558	0.589
		Max	0.009	0.197	**0.627**	**0.649**
		Mean	0.003	0.172	0.583	**0.617**
		SD	0.002	0.010	0.016	0.015
	K = 10	Min	0.000	0.153	0.560	0.590
		Max	0.009	0.197	**0.630**	**0.649**
		Mean	0.003	0.172	0.584	**0.618**
		SD	0.002	0.010	0.016	0.015
Case 3: 10% thief consumers	K = 2	Min	0.000	0.654	0.979	0.986
		Max	0.039	0.768	**1.000**	**1.000**
		Mean	0.008	0.718	**0.994**	**0.998**
		SD	0.009	0.028	0.005	0.004
	K = 4	Min	0.001	0.483	0.863	0.916
		Max	0.024	0.577	**0.954**	**0.975**
		Mean	0.006	0.534	**0.905**	**0.946**
		SD	0.005	0.023	0.017	0.014
	K = 6	Min	0.001	0.385	0.720	0.781
		Max	0.017	0.457	0.777	**0.852**
		Mean	0.005	0.422	0.748	**0.821**
		SD	0.004	0.016	0.015	0.016
	K = 8	Min	0.001	0.316	0.578	0.642
		Max	0.014	0.368	0.635	**0.712**
		Mean	0.004	0.344	0.609	**0.684**
		SD	0.003	0.013	0.015	0.015
	K = 10	Min	0.001	0.268	0.475	0.536
		Max	0.011	0.310	0.526	**0.600**
		Mean	0.003	0.290	0.504	**0.573**
		SD	0.002	0.011	0.012	0.014

Min: Minimum, Max: Maximum, Mean: Average, SD: Standard deviation.



(a) Honest consumers (b) Electricity thieves

Fig. 2. Loss (γ) and honest (δ) coefficients for the attack dataset of Case 3 resulting in the best $MAP@10$

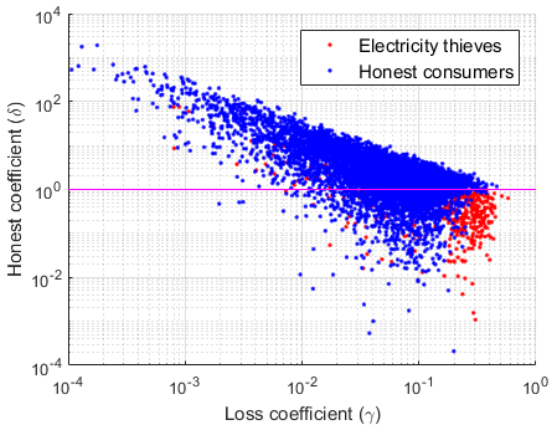


Fig. 3. Loss (γ) and honest (δ) coefficients for consumers with $\gamma > 1e-4$

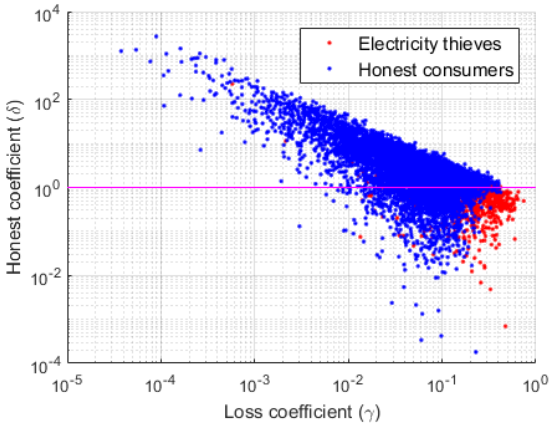


Fig. 4. Loss (γ) and honest (δ) coefficients under attack mode I only

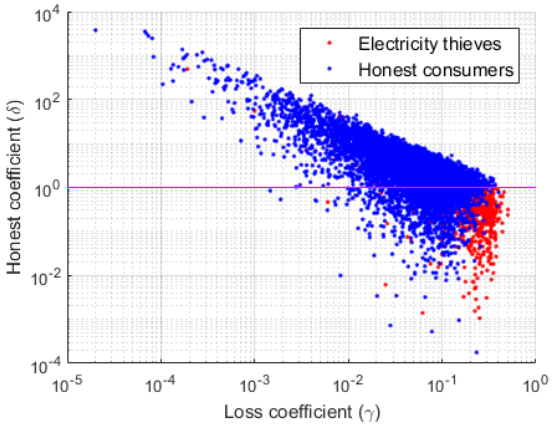


Fig. 5. Loss (γ) and honest (δ) coefficients under attack mode II only

The loss (γ) and honest (δ) coefficients for actual honest consumers and electricity thieves are plotted in logarithmic scale in Fig. 2(a) and Fig. 2(b), respectively, for the Case 3 attack dataset that results in the best $MAP@10$. It may be noted that the distribution of these coefficients is similar for attack datasets obtained in other runs. Fig. 2(b) does not include the thieves adopting attack mode III(b) (Sect. V-A) due to zero standard deviation across readings throughout the theft day. In no case, the γ values of honest consumers are found to be lower than $1e-6$. The consumers with extremely low γ values ($\gamma < 1e-10$, the green shaded region in Fig. 2(b)), are correctly identified as thieves. Many thieves have high γ values ($1e-4 < \gamma < 1$), some of whom have been correctly caught with their δ values being less than the threshold θ (here, selected $\theta = 1$ and the yellow shaded region denotes $\delta < \theta$). Some honest consumers have also been misjudged as thieves in the process. However, those are mostly ranked lower in the predicted list of thieves so that up to $K = 10$, we obtain reasonably high precision ($MAP@K$) values. The statement can be corroborated by studying Fig. 3, which is a superimposed scatter diagram of honest consumers and electricity thieves. For clarity, the diagram includes only consumers having $\gamma > 1e-4$. Most thieves are seen congregated in the bottom-right of the diagram, where γ is nearer to 1 and $\delta < 1$ (i.e., below the magenta line). The very fact justifies our selection of the threshold (i.e., θ = 1) for δ. Furthermore, in general, a thief is likely to have higher γ value than most of the honest consumers. Some thieves with δ higher than the threshold go undetected, however, the threshold θ = 1 is a trade-off between detection of maximum possible number of thieves and at the same time, reduction of the number of wrong verdicts on honest consumers.

The distributions of consumer coefficients under single

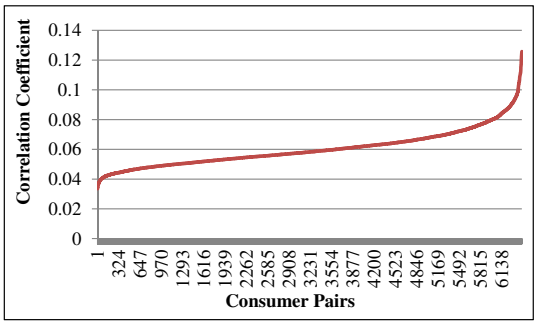


Fig. 6. Correlation between consumer pairs

attack mode are plotted in Fig. 4 for attack mode I only and in Fig. 5 for attack mode II only. The pattern of coefficient distribution does not change under single attack mode I or II from mixed attack mode, except that the small correlation values (when $\gamma < 1e{-}10$) do not exist in single attack mode I or II. As discussed in Sect. IV-A, the extreme small correlation is the result of attack mode III.

To further analyse the superior performance of CAPET, we plot Fig. 6 that shows the correlation between any pair of consumers in the Smart* dataset. The correlation coefficient values are within range $[0.033, 0.126]$. The low values of correlation coefficients indicate that the consumption across various consumers is quite different. This helps to identify the energy thieves with greater accuracy using CAPET. Therefore, CAPET is very effective for electricity theft detection in a consumption dataset with high degree of variability. Subsequently, we will show that in addition to higher accuracy, our CAPET is also robust against data noise and coarse grained meter readings. Moreover, by adding more master meters in the smart grid, the performance of our CAPET can be improved further.

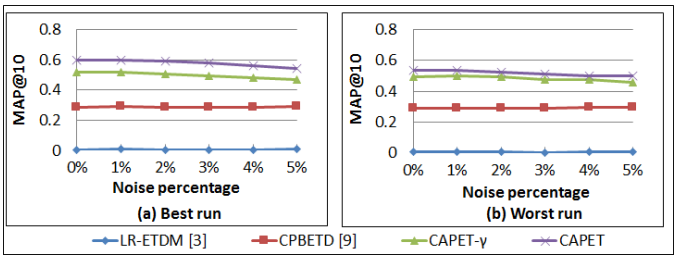


Fig. 7. MAP@10 for different noise levels added to Case 3 datasets

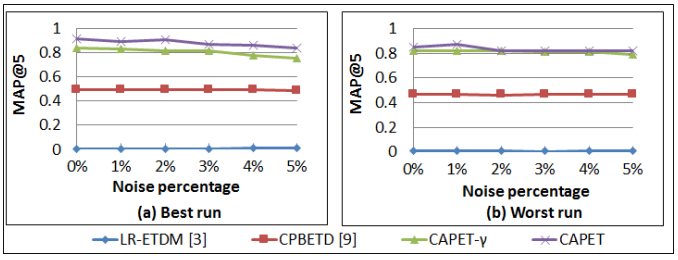


Fig. 8. MAP@5 for different noise levels added to Case 3 datasets

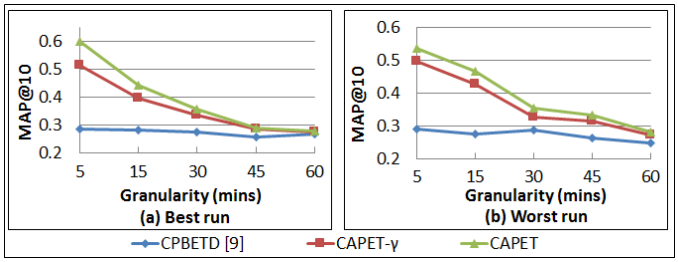


Fig. 9. Effect of granularity of meter readings

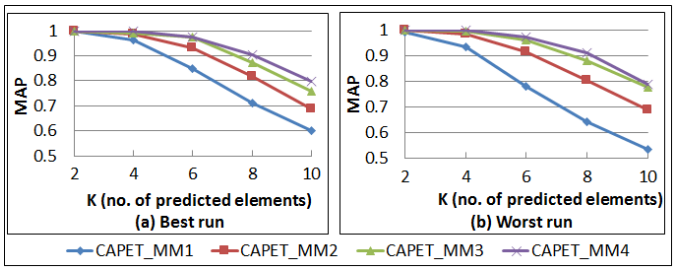


Fig. 10. Effect of the number of master meters

2) Effect of noise: To compare the robustness of our model against noise, we randomly add noise to all meter readings up to a certain percentage of their respective actual energy usages (i.e. the original meter readings). Different datasets are synthesized with contamination of maximum 1%, 2%, 3%, 4% and 5% of noise to all meter readings in Case 3 theft scenario. We compare CAPET performance at $MAP@10$ and $MAP@5$ with all baselines. The best run and worst run in Fig. 7(a) and 7(b), respectively, refer to the attack datasets that result in the best and worst $MAP@10$ values by CAPET. Fig. 8(a) and 8(b) can be interpreted in a similar manner for the best and worst $MAP@5$ values by CAPET. It may be noted that the best $MAP@K$ by CAPET may not correspond to the best $MAP@K$ by other methods. The results show that both our CAPET schemes, as well as the SVM-based CPBETD are robust up to 3% noise in the data. Though the performance of CAPET marginally degrades when the noise exceeds 3%, it consistently outperforms the other baselines.

3) Effect of the granularity of meter readings: To compare the robustness of the model for granularity of meter readings, we reduce the sampling rate to every 15, 30, 45 and 60 minutes for each consumer. We compare $MAP@10$ of all models in Fig. 9 by utilizing Case 3 datasets. The best and worst runs correspond to the attack datasets leading to the best and worst $MAP@10$ values, respectively, at 5-minute sampling frequency. Note that we skip LR-ETDM in this evaluation as linear regression requires the number of meter readings to be higher than the number of consumers. Although larger granularity leads to a performance drop in all methods, our CAPET consistently outperforms others at all granularity levels.

4) Effect of the number of master meters: We also evaluate the effect of the number of master meters in our CAPET. Intuitively, the more the number of master meters, the better the CAPET performs. This is because the number of households each master meter monitors is less. We test the performance

of our CAPET by changing the number of master meters from 1 to 4. The performance curve for the same is shown in Fig. 10. CAPET_MM*i* denotes CAPET results in a smart grid NAN with i master meters. The explanation of the best and worst runs is same as described above in meter granularity section. The results of the best run (Fig. 10(a)) show that the performance of CAPET can be further improved by up to 32.6% when the number of master meters is increased from 1 to 4.

VI. Conclusion

In this paper, we study the problem of electricity theft pinpointing in smart grid. We propose a novel correlation-analysis-based scheme (CAPET) which can effectively identify electricity theft behaviours without requiring labeled data for training or linearity assumption on the attack mode. Attack datasets are created incorporating a mixture of various types of attacks into a real-world energy consumption dataset. Extensive experiments have been conducted with the synthesized datasets using the proposed method. The results and comparisons show that our CAPET outperforms the state-of-the-art baselines on the aspects of electricity theft pinpointing accuracy, robustness against noises and sensitivity to coarse grained meter readings. In the future, we intend to explore other correlation methods such as Kendall Correlation, Spearman Correlation, etc. in electricity theft detection and identification problem. A more complex case of changing attack patterns within a day by the consumers remains a work front for the future. We also plan to work with industrial partners to use real energy consumption data with energy theft information to test our methods.

Acknowledgement

This research is supported in part by the National Research Foundation, Prime Minister's Office, Singapore under the Energy Programme and administrated by the Energy Market Authority (EP Award No. NRF2014EWT-EIRP002-040 and EP Award No. NRF2017EWT-EP003-047), and in part by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme. The work was partially done when Hongyun and Vincent were with ADSC.

References

[1] Y. Wu, B. Chen, J. Weng, Z. Wei, X. Li, B. Qiu, and N. Liu, "False load attack to smart meters by synchronously switching power circuits," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2641–2649, 2018.

[2] PR Newswire. (2014) World loses $89.3 billion to electricity theft annually, $58.7 billion in emerging markets. [Online]. Available: https://www.prnewswire.com/news-releases/world-loses-893-billion-to-electricity-theft-annually-587-billion-in-emerging-markets-300006515.html

[3] 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 Trans. Industrial Informatics*, vol. 12, no. 3, pp. 1005–1016, 2016.

[4] 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, 2017.

[5] D. Mashima and A. A. Cárdenas, "Evaluating electricity theft detectors in smart grid networks," in *Proceedings of the 15th International Conference on Research in Attacks, Intrusions, and Defenses*, 2012, pp. 210–229.

[6] J. L. Viegas, P. R. Esteves, R. Melício, V. Mendes, and S. M. Vieira, "Solutions for detection of non-technical losses in the electricity grid: a review," *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 1256–1268, 2017.

[7] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad, "Nontechnical loss detection for metered customers in power utility using support vector machines," *IEEE transactions on Power Delivery*, vol. 25, no. 2, pp. 1162–1171, 2009.

[8] P. O. Glauner, A. Boechat, L. Dolberg, R. State, F. Bettinger, Y. Rangoni, and D. Duarte, "Large-scale detection of non-technical losses in imbalanced data sets," in *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, ISGT*, 2016, pp. 1–5.

[9] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," *2011 IEEE/PES Power Systems Conference and Exposition*, pp. 1–8, 2011.

[10] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, pp. 216–226, 2016.

[11] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and A. M. Mohammad, "Detection of abnormalities and electricity theft using genetic support vector machines," in *TENCON 2008 - 2008 IEEE Region 10 Conference*, 2008, pp. 1–6.

[12] D. R. Pereira, M. A. Pazoti, L. A. M. Pereira, D. Rodrigues, C. C. O. Ramos, A. N. de Souza, and J. P. Papa, "Social-spider optimization-based support vector machines applied for energy theft detection," *Computers & Electrical Engineering*, vol. 49, pp. 25–38, 2016.

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

[14] T. J. Bihl and A. F. Zobaa, "Data-mining methods for electricity theft detection," in *Big Data Analytics in Future Power Systems*. CRC Press, 2018, pp. 107–124.

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

[16] S. E. McLaughlin, B. Holbert, A. M. Fawaz, R. Berthier, and S. A. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319–1330, 2013.

[17] C. Selvapriya, "Competent approach for inspecting electricity theft," *Int J Innov Res Sci, Eng Technol*, vol. 3, pp. 1763–1766, 2014.

[18] B. Khoo and Y. Cheng, "Using RFID for anti-theft in a chinese electrical supply company: A cost-benefit analysis," in *2011 Wireless Telecommunications Symposium, WTS 2011, New York City, NY, USA, April 13-15, 2011*, 2011, pp. 1–6.

[19] S. Amin, G. A. Schwartz, and H. Tembine, "Incentives and security in electricity distribution networks," in *Decision and Game Theory for Security - Third International Conference, GameSec 2012, Budapest, Hungary, November 5-6, 2012. Proceedings*, 2012, pp. 264–280.

[20] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in AMI systems," in *50th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2012, Allerton Park & Retreat Center, Monticello, IL, USA, October 1-5, 2012*, 2012, pp. 1830–1837.

[21] Y. Tang, C.-W. Ten, and L. E. Brown, "Switching reconfiguration of fraud detection within an electrical distribution network," in *2017 Resilience Week (RWS)*. IEEE, 2017, pp. 206–212.

[22] 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, 2014.

[23] P. Glauner, J. A. Meira, P. Valtchev, R. State, and F. Bettinger, "The challenge of non-technical loss detection using artificial intelligence: A survey," *arXiv preprint arXiv:1606.00626*, 2016.

[24] B. Chen and H. Yu, "Secure aggregation with malicious node revocation in sensor networks," in *2011 31st International Conference on Distributed Computing Systems*. IEEE, 2011, pp. 581–592.

[25] J. Benesty, J. Chen, Y. Huang, and I. Cohen, *Pearson Correlation Coefficient*, 2009, pp. 1–4.

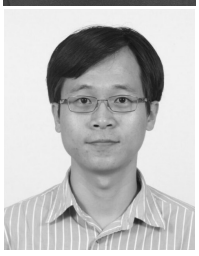
[26] B. Podobnik and H. E. Stanley, "Detrended cross-correlation analysis: A new method for analyzing two non-stationary time series," arXiv.org, Tech. Rep., 2007.

[27] H. Akaike, "Canonical correlation analysis of time series and the use of an information criterion," in *System Identification Advances and Case Studies*, ser. Mathematics in Science and Engineering, R. K. Mehra and D. G. Lainiotis, Eds., 1976, vol. 126, pp. 27 – 96.
[28] S. Barker, A. Mishra, D. Irwin, E. Cecchet, P. Shenoy, and J. Albrecht, "Smart*: An open data set and tools for enabling research in sustainable homes," in *SustKDD*, 2012.
[29] C. D. Manning, P. Raghavan, and H. Schütze, "Chapter 8: Evaluation in information retrieval," *Introduction to information retrieval*, pp. 151–175, 2008.

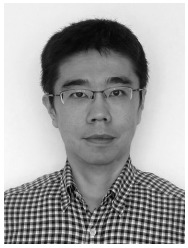
Partha P. Biswas received his Ph.D. degree from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore in 2019. Currently, he is working as a senior research engineer in Advanced Digital Sciences Center (ADSC), Singapore. Prior to joining ADSC, he worked in power industry for several years. His research interests include adopting computational intelligence and machine learning techniques in power system, smart grid security and resilience.

Hongyun Cai received her Ph.D. degree in Computer Science from the University of Queensland in 2016. She is currently a senior researcher in Tencent, China. Before joining Tencent, she was a postdoctoral researcher at the Advanced Digital Sciences Center, Singapore. Her research focuses on graph mining, social data management and analysis, graph representation learning, and time-series data analysis.

Bin Zhou received the bachelor degree in Computer Science from the National University of Singapore in 2015. He is a software engineer at the Advanced Digital Sciences Center, Singapore (ADSC). Before joining ADSC, he was working in Industrial Light and Magic as software developer. His experience and interests focus on visual computing and software development.



Binbin Chen received his B.Sc. from Peking University and Ph.D. from National University of Singapore, both in Computer Science. He is currently an Associate Professor at Singapore University of Technology and Design (SUTD), with a joint appoint at Advanced Digital Sciences Center (ADSC), a research center of the University of Illinois located in Singapore. His current research interests include wireless networks, cyber-physical systems, and cyber security for critical infrastructures.



Daisuke Mashima received his Ph.D. degree in Computer Science from Georgia Institute of Technology in 2012. He is currently a senior research scientist at the Advanced Digital Sciences Center (ADSC) in Singapore, where he is working on smart grid security research. Before joining ADSC, he worked as a member of research staff in the smart energy group at Fujitsu Laboratories of America, Inc. His research interest covers cybersecurity and privacy in cyber-physical systems in general.

Vincent W. Zheng received his Ph.D. degree in Computer Science from the Hong Kong University of Science and Technology in 2011. He is a deputy general manager in WeBank, China. Before joining WeBank, he was working as a senior research scientist at the Advanced Digital Sciences Center, Singapore. His research interests include transfer learning, federated learning, graph learning and information extraction.