Multi-timescale Electricity Theft Detection and Localization in Distribution Systems Based on State Estimation and PMU Measurements

Côme Carquex, Catherine Rosenberg
Dept. of Electrical and Computer Engineering
University of Waterloo, Ontario
[cacarque,cath]@uwaterloo.ca

ABSTRACT

Electricity theft is a serious issue for distribution companies around the world. Often linked to criminal activities, it is dangerous for the grid and the neighborhoods. While placing measurement points at each bus would allow an easy detection, it is not a practical approach. In this paper, a multi-timescale theft estimation (MISTE) method that takes advantage of smart-meters as well as the sparse grid sensing infrastructure that is being envisaged for state estimation is proposed. It combines power and voltage measurement across time to detect any inconsistency caused by electricity theft. Contrary to existing approaches which are snapshot-based and assume smart-meters to be able to measure instantaneous power consumption, the proposed method models smart-meters as energy measurement devices and combines the measurement timescales of the smart-meters and the PMUs in the computations. The detection performance of the proposed approach is compared to the state of the art theft detection methods. Both the true positive rate as well as the false negative rate are considered, which few papers have discussed previously. Insights on the impact of theft location on theft detection are also given.

CCS CONCEPTS

• **Hardware** → **Energy metering**; **Smart grid**;

KEYWORDS

Electricity theft, PMU, State estimation

ACM Reference Format:
Côme Carquex, Catherine Rosenberg. 2018. Multi-timescale Electricity Theft Detection and Localization in Distribution Systems Based on State Estimation and PMU Measurements. In *e-Energy '18: The Ninth International Conference on Future Energy Systems, June 12–15, 2018, Karlsruhe, Germany*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3208903.3208908

e-Energy '18, June 12–15, 2018, Karlsruhe, Germany

ACM ISBN 978-1-4503-5767-8/18/06…$15.00
https://doi.org/10.1145/3208903.3208908

1 INTRODUCTION

The nature of electricity theft varies depending on the region of the globe considered [48]. Social context is extremely important to understand electricity theft and its impact. In this work, theft in western countries is considered. Such energy losses are often referred to as non-technical losses (NTL) by utilities. NTL are a serious problem for local distribution companies (LDC). In the U.S. alone, several billion of dollars are lost every year due to this problem [29]. NTL are often linked to criminal activities. For example in the Netherlands, about 95% of electricity theft cases are associated with the cultivation of illegal drugs [25]. Illegal tapping of the secondary network is dangerous (if significant) for the electrical grid (overload of distribution transformers) as well as for the neighborhood (risk of fire and electrocution) [22]. This paper is therefore focused on the detection of "big" thefts, which are the results of the illegal tapping of the secondary of distribution transformer, since they are the most hazardous.

The simplest solution to the theft detection problem would be to install a central observer meter at each distribution transformer bus [8], and compute the energy balance. This approach is however very costly and not scalable. Nevertheless, utilities are increasingly monitoring the operations of their system using distribution system state estimation (DSSE), based on sparse bus voltage measurements from phasor measurement units (PMU) [7, 42, 52]. PMUs are devices capable of measuring the voltage magnitude and angle at a given bus. More and more countries have also rolled out smart-meters, that can provide periodic energy consumption data at the consumer level. Smart-meters and PMUs operate on different timescales; while PMUs are capable of producing measurements every few seconds, smart-meters report energy consumptions over the span of several minutes or hours. In this paper the existing measurement infrastructure put in place for DSSE along with smart-meters is used to perform theft detection. By combining energy and voltage measurements using state estimation, inconsistencies could in principle be detected. It is however not an easy task.

The research question answered is the following: how to detect and locate big energy theft efficiently by relying on the existing measurement infrastructure? A few recent papers have used state estimation to detect theft but they suffer from several drawbacks. In particular, they assume the smart-meters being capable of measuring instantaneous active and reactive power, as well as voltage magnitude. Moreover they rely on

snapshot-based state estimation, meaning that measurements acquired at two different times T_i and T_{i+1} are considered independently. They focus on the smart-meter timescale and take a PMU snapshot at T_i. Snapshot-based approaches have poor detection performances and trigger many false alarms. Hence, a new method that considers several PMU measurements across time is proposed. Specifically, the contributions of the paper are the following:

- A new method, MISTE, that improves the SoA on two fronts is proposed: the theft detection rate is improved and the false detection rate (false alarms) is decreased compared to existing snapshot-based methods.
- Insights on theft detection performances are provided. It is shown that detecting thefts located at buses close to the substation is harder than thefts located at the end of a feeder. Moreover, adding a few extra PMUs to the existing DSSE infrastructure can greatly improve the detection performances.
- Finally, theft localization performances are investigated. MISTE is able to locate theft with a good level of accuracy.

The rest of the paper is organized as follows. A literature review is presented in Section 2. The system model considered is detailed in Section 3. The two SoA methods are described in Section 4. The proposed method, MISTE, is introduced in Section 5. It is validated using real home consumption profiles and compared to the benchmark in Section 6. Finally conclusions are drawn in Section 7.

2 LITERATURE REVIEW

The literature regarding theft detection and localization in distribution systems is abundant. Table 1 presents a taxonomy of the existing work organized in several categories, described below:

(1) Review papers that discuss theft in broad terms and with little technical content. Those papers are useful to understand the context in which theft occurs, as it varies depending on the region of the world considered.
(2) Papers where consumption patterns are analyzed to detect theft. Such methods presuppose that regular users are stealing a fraction of their electric consumption and that such action can be detected via pattern analysis of historical data.
(3) Papers assuming false data injection and smart meter hacking or tampering.
(4) Papers that rely on measurement mismatch. Typically, measurements of different types are acquired (voltage, power, etc...). State estimation, power-flow equations or parametric statistics are then used to detect any incoherence between measurements. In Table 1 this category is split into two to emphasize methods that explicitly rely on state estimation (4a) from the other papers (4b).

This paper focuses on the detection of theft resulting from criminal activities, that is considered to be an illegal tapping of the secondary of a distribution transformer. Therefore, categories (1), (2) and (3) are out of scope.

Table 1: Taxonomy of related work

Category	Related papers
General analysis	[6, 15, 17, 18, 23, 48]
Patterns analysis and machine learning	[13, 14, 16, 24, 35, 37–41]
False data injection	[26, 27, 31]
Measurement mismatch (4a - state estimation)	[11, 19, 21, 23, 25, 28, 44, 45, 49, 51]
Measurement mismatch (4b - other method)	[8, 20, 30, 36, 43, 47, 53–55]

As mentioned, category (4) is split into two sub-categories. Papers in (4b) make heterogeneous assumptions and it is difficult to summarize them without looking at each paper individually. However, given that these approaches do not fit well within the focus of this paper, they will not be reviewed here.

Most of the papers in category (4a) - which look for measurement mismatch using state estimation - make three major assumptions: 1) they assume that the topology of the system as well as the line impedances are known; 2) every legal load is metered; 3) they assume that the measurements used are taken by synchronized smart-meters, located near the connected loads. They are assumed capable of reporting instantaneous active and reactive powers, as well as voltage magnitude, in real-time. The last assumption will be relaxed in this paper, smart-meters will be assumed to collect active and reactive energy consumptions over slots of fixed size, and sparse voltage measurements will be available from PMUs. While it is believed that these changes reflect the reality better, they also introduce two difficulties. The first one is that energy measurements are available instead of power measurements, which decreases the quality of information available. Moreover it is harder to work with sparse PMU measurements than ubiquitous smart-meters voltage magnitude measurements.

The two papers [21, 49] selected to represent the State of the Art (SoA) use a system model close to the one presented in Section 3.

Huang *et Al.* [21] are one of the first to leverage state estimation in distribution system to detect theft. Their approach is based on bad data detection, which consist in identifying corrupted measurements. Regarding electricity theft, a bad measurement would be a power measurement at a bus which is much lower than the actual bus consumption. Bad data detection is a common practice in state estimation [33]. The state of the system is estimated using a traditional snapshot-based weighted least square (WLS) objective function. The presence of bad data (outliers, such as under-reported consumption values) for a given time is tested using a chi-square test on the residuals.

In [49] the authors rely on state estimation and a WLS objective function to which a bias vector minimized by an L_1 norm is added. The use of the L_1 norm provides a sparse bias vector. However several points appear unclear such as the choice of

the weight of the L_1 norm with respect to the least-square part. Such approach is also snapshot-based.

On of the main limitations of the state of the art methods is that they rely on the optimistic assumption that smart-meters are capable of measuring instantaneous powers and voltage magnitude, in a synchronized fashion. It is shown in this paper that the SoA approaches are less efficient when this assumption is relaxed, hence motivating the need for a new approach.

3 SYSTEM MODEL

Theft detection is done online, meaning that theft detection can be performed once all the data have been collected, i.e. every ΔT_{SM} (the time scale of the smart-meter). The following information needs to be known by both MISTE and the SoA approaches.

Topology: a set of buses I and a set of branches B of known impedance characterize the distribution system. A reference voltage source of magnitude V_0 is used to model the substation transformer.

Voltage measurements: the subset $S \subseteq I$ of buses are equipped with PMUs that monitor every ΔT_{PMU} both the bus voltage magnitudes (V_s) and voltage angles (δ_s); ΔT_{PMU} is typically of the order of several seconds. The variance of the error of the PMU readings is known. Measurement errors are uncorrelated in time and across buses. The PMUs are placed in the distribution system according to a given mapping $\mathscr{S}$ obtained for DSSE.

Energy measurements: it is assumed that each and every "legal" load is metered by a smart-meter. While it is common for a few legal loads to be connected to the distribution system without being metered (for example, street lighting), such loads are however small in magnitude and relatively constant in power demand [2]. Since these loads do not remain unbilled, it is assumed that the LDC has enough information to estimate their value, and are treated as if they were metered in this work.

It is assumed that smart-meters report active and reactive energy consumption over time-slots of length ΔT_{SM}; a typical value of ΔT_{SM} varies from 10 minutes to 1 hour. The smart meter measurements are assumed to be unbiased and the variance of the error to be known. Typically a smart meter of category 0.2S will have an error of 0.2% on a power reading [3].

Instead of considering each individual load independently, the aggregated bus load is considered. It is supposed that the LDC can estimate technical losses on the low voltage side of the distribution transformer (such as line losses) with a known accuracy. Therefore an equivalent unique smart-meter is considered for the whole aggregated bus load.

Timescales and measurements: two timescales with different granularity coexist, one for the PMUs and one for the smart-meters. Smart-meter time-slots have a much bigger length than PMU slots ($\Delta T_{SM} \gg \Delta T_{PMU}$). Therefore, several PMU measurements are acquired within one smart-meter slot.

Theft: theft is modeled as a constant additional load, connected to the low-voltage side of a distribution transformer. It is not metered and corresponds to an illegal tapping of the line. The power factor of the stealing is close to 1 (meaning that little reactive power is consumed, it is mostly an active load). Such assumptions model a grow-house, where infrared lights are used to accelerate the growth of cannabis plants [25].

State vector: several equivalent state vectors are defined. Each one of them is chosen depending on its ease of use. $\mathbf{y}(t) = [\mathbf{V}(t)^T, \boldsymbol{\delta}(t)^T]^T$ is a possible state vector representation, where $\mathbf{V}(t)$ is the vector of voltage magnitudes at each bus, and $\boldsymbol{\delta}(t)$ the vector of voltage angles. Another way is to define $\mathbf{x}(t) = [\mathbf{P}(t)^T, \mathbf{Q}(\mathbf{t})^T]^T$ where $\mathbf{P}(t)$ and $\mathbf{Q}(t)$ denotes the vectors of active and reactive power injections at each bus, respectively. Note that the power-flow equations link the state-vectors $\mathbf{x}$ and $\mathbf{y}$. A third, $\boldsymbol{u}$, is defined as the vector of voltage measurements projected onto the real and imaginary axis; $\boldsymbol{u}$ is such that $\boldsymbol{u} = [\text{real}(V_1 e^{j\delta_1}), \cdots, \text{real}(V_{|I|} e^{j\delta_{|I|}}), \text{img}(V_1 e^{j\delta_1}), \cdots, \text{img}(V_{|I|} e^{j\delta_{|I|}})]^T$.

4 STATE OF THE ART

The proposed scheme will be benchmarked against two SoA methods that use state estimation. The methods have been adapted to the measurement infrastructure described above, i.e. the voltage information is given by PMUs, and smart-meters report energy consumption instead of instantaneous power.

Computations are done at the end of each smart-meter time-slots[1]. The following measurements are available: $2|I|$ active and reactive energy measurements for every bus $i \in I$ given by the smart-meters, and $2|S|$ voltage magnitude and angle measurements at buses $s \in S$, given by the PMUs, taken as a snapshot at the end of the smart-meter slot. Energy measurements cannot be used by state estimation directly. They are converted into an approximated power measurement by dividing their value by the smart-meter time-slot length ΔT_{SM}.

The vector $\mathbf{z}(t)$ of size $M \times 1$ ($M = 2|I| + 2|S|$) is used to represent the measurements reported at time t. The m^{th} measurement is denoted by $\mathbf{z}_m(t)$. Voltage measurements can be represented using two coordinate systems: polar (voltage magnitude and angle) or Cartesian (voltage phasor projected on the real axis and imaginary axis). Both representations are equivalent and can be exchanged depending on their ease of use in the problem considered.

Finally, let us denote by $\boldsymbol{f}(\cdot)$ the function that maps a state vector to a given measurement vector; $\boldsymbol{f}(\cdot)$ embeds the power flow equations in its formulation.

4.1 Typical bad data detection (SoA-1)

In a typical WLS formulation of state estimation, bad data detection is usually performed by doing hypothesis testing on the residuals [32] [21]. In the context of electricity theft, a bad data is an energy measurement reported at a bus that is lower than the actual bus consumption. Given a distribution system, the objective function to minimize is given by:

$$J_{WLS}(\mathbf{y}) = \Sigma_{m=1}^{M} \left(\frac{\mathbf{z}_m - \boldsymbol{f}_m(\mathbf{y})}{\sigma_m}\right)^2 \quad (1)$$

[1]Technically, the computations for the two SoA methods could be done every PMU time-slot. That would however not increase their performance, as they are snapshot based.

where σ_m^2 is the variance of the m^{th} measurement. The objective function J_{WLS} being minimized is the same used for DSSE in a snapshot based context. While its value is not important for DSSE, it is useful for theft detection. Let $\hat{\boldsymbol{y}}$ be the estimated state. Assuming that the measurement errors are normally distributed and independent, then the performance index is given by $J(\hat{\boldsymbol{y}})$ and follows a chi-square distribution with $M - 2|I| = 2|S|$ degrees of freedom [32]. For each smart-meter time-step, one observation $J_{WLS}(\hat{\boldsymbol{y}})$ of the random variable $J_{WLS}(\mathbf{y})$ is made. Based on this observation, a decision of whether or not it belongs to the chi-square distribution must be taken. Let α be the significance level of the statistical test used for $J_{WLS}(\hat{\boldsymbol{y}})$. The value of α varies between 0 and 1 and is chosen by the operator. Two hypotheses are envisaged; let H_0 be the null hypothesis and H_1 be an alternative hypothesis. In this case, the alternative hypothesis is the presence of theft. Two cases are distinguished:

(1) If $J(\hat{\boldsymbol{y}}) > C$ then reject H_0
(2) If $J(\hat{\boldsymbol{y}}) \leq C$ then accept H_0

where C is a threshold to be determined based on the choice of α. Let $\chi_{M-2|I|,1-\alpha}$ represents the $(1-\alpha)^{th}$ quantile of a chi-square distribution with $M - 2|I|$ degrees of freedom. Choosing $C = \chi_{M-2|I|,1-\alpha}$ means that a fraction α of the time, a value of $J(\hat{\boldsymbol{y}})$ greater than C will be observed by pure chance only.

4.2 Refined WLS [49] (SoA-2)

One of the shortfalls of least square estimation is that the error resulting from a measurement outlier tends to be spread over all the buses. To address this limitation it was suggested in [49] a slight modification of the WLS objective function for the purpose of theft detection. The method proposed by Su *et Al.* which we call *SoA-2* is still snapshot-based. The objective function minimized is such that:

$$J_{Su}(\mathbf{y}, \boldsymbol{b}) = \Sigma_{m=1}^{M} \left(\frac{\mathbf{z}_m - \boldsymbol{f}_m(\mathbf{y}) - \boldsymbol{b}_m}{\sigma_m}\right)^2 + \kappa \|\boldsymbol{b}\|_1 \qquad (2)$$

where κ is a parameter to be determined and $\boldsymbol{b}$ is a $M \times 1$ vector. Each non-zero $\boldsymbol{b}_m$ represents a bias on the m^{th} measurement. It is not specified in the paper how to choose the parameter κ nor if such formulation improves on typical bad data detection. The proposed theft detection method shares some similarities with this method.

5 PROPOSED METHOD: MISTE

Most state estimation based methods for theft detection (and the ones presented in the previous section) rely on snapshot-based approaches. Rather than looking at only on snapshot, MISTE considers all the PMU measurements time-steps at once over a smart-meter time-interval, in the objective function. Indeed it is easier to detect a bias in a power measurement (resulting from a theft) by looking at voltage measurements over a period of time rather than in a snapshot fashion. Hence the computation is run once every ΔT_{SM}, and the objective function being minimized is the sum of traditional snapshot-based WLS objectives, summed over all PMU time-slots. To each PMU time-slot within a smart-meter slot corresponds a measurement vector $\boldsymbol{z}(t)$ of size $M = 2|I| + 2|S|$ containing the $2|S|$ PMU measurements acquired within the PMU time-slot and the $2|I|$ power measurements, converted from the energy measurements given by the smart-meters. The conversion from energy to power is done in the same way as for the SoA.

Contrary to the SoA-2 method presented in Section 4, a bias vector will be estimated only for active power measurements since only this type of measurement is expected to be affected based on the theft model considered. To avoid possible bias, SoA-2 has been tried with the same assumption.

To allow the insertion of an estimation bias vector $\boldsymbol{a}$, the objective function has been broken down by type of measurements. The following two sets are defined:

- $M_P \subset [1, M]$ is the subset of indices (of size $|I|$) such that $\mathbf{z}_m(t), m \in M_P$ corresponds to an active power measurement.
- $M_{\not P} \subset [1, M]$ is the subset of indices (of size $|I| + 2|S|$) such that $\mathbf{z}_m(t), m \in M_{\not P}$ corresponds to any type of measurement except active power.

Given a discrimination parameter λ (its choice is explained in Section 6), the optimization problem is written:

$$\begin{aligned} \underset{\boldsymbol{x}(t), \boldsymbol{a}}{\text{minimize}} \quad & \Sigma_{t=T_0}^{T_0+\Delta T_{SM}} \left[\Sigma_{m \in M_{\not P}} \left(\frac{\mathbf{z}_m(t) - \boldsymbol{f}_m(\mathbf{x}(t))}{\sigma_m} \right)^2 \right] \\ & + \Sigma_{t=T_0}^{T_0+\Delta T_{SM}} \left[\Sigma_{m \in M_P} \left(\frac{\mathbf{z}_m(t) - \boldsymbol{f}_m(\mathbf{x}(t)) - \boldsymbol{a}_m}{\sigma_m} \right)^2 \right] \\ & + n\lambda \Sigma_{m \in M_p} \left| \frac{\boldsymbol{a}_m}{\sigma_m} \right| \\ \text{subject to} \quad & \boldsymbol{a} \geq 0 \end{aligned} \qquad (3)$$

where $n = \left(\frac{\Delta T_{SM}}{\Delta T_{PMU}} - 1 \right)$ is the number of PMU measurements within a smart-meter time-slot, minus 1; n and σ_m are used as scaling factors to make the value of λ easier to choose and understand. The discrimination parameter λ represents how far the estimated active power variable can deviate from the measurement, expressed in number of measurement standard deviation.

The minimization problem (3) is non-linear and non-convex. A simple back of the envelope calculation shows that solving this problem on the 33-Bus system with PMU time-slots of 6 seconds and smart-meter time-slots of 10 minutes would require about 16,000 variables and 8,000 non-linear relationships between variables. Even-though solvers like MINOS are able to handle such big problems, computation time is prohibitive. Instead a linear formulation of the power-flow equation around the system operating point is chosen. The system operating point can be determined solely based on available power measurements, computed from the smart-meter energy measurements.

Multiple linear power flow formulations exist with different granularity in their assumptions, such as the ones described in [4, 50] for example. The first iteration of the backward-forward sweep is chosen for the linear formulation of the power-flow. The topology of the system is encoded in the distribution load

flow matrix $\mathscr{M}$ (see [50] on how to compute $\mathscr{M}$). The linear power-flow equations are derived in the Appendix. A linear relationship between the state vectors $\boldsymbol{u}$ and $\boldsymbol{x}$ such that $\boldsymbol{u} = \mathrm{PF}(\boldsymbol{x})$ is obtained. Using a linear formulation of the power-flow equations makes the optimization problem convex. It can thus be solved much quicker. The problem is now written:

$$\begin{aligned} \underset{\boldsymbol{u}(t),\boldsymbol{x}(t),\boldsymbol{a}}{\text{minimize}} \quad & \Sigma_{t=T_0}^{T_0+\Delta T_{SM}} \left[\Sigma_{m\in M_P} \left(\frac{\mathbf{z}_m(t) - F_m \begin{bmatrix} \mathbf{x}(t) \\ \mathbf{u}(t) \end{bmatrix}}{\sigma_m} \right)^2 \right] \\ & + \Sigma_{t=T_0}^{T_0+\Delta T_{SM}} \left[\Sigma_{m\in M_P} \left(\frac{\mathbf{z}_m(t) - F_m \mathbf{x}(t) - \boldsymbol{a}_m}{\sigma_m} \right)^2 \right] \\ & + n\lambda \Sigma_{m\in M_P} \left| \frac{\boldsymbol{a}_m}{\sigma_m} \right| \\ \text{subject to} \quad & \boldsymbol{a} \geq 0, \\ & \boldsymbol{u}(t) = \mathrm{PF}(\boldsymbol{x}(t)) \end{aligned} \tag{4}$$

where F_m is a selection matrix, which selects the one variable corresponding to the the m^{th} measurement.

The output of interest of this optimization problem is the estimated bias vector $\boldsymbol{a}$. Each non zero variable $\boldsymbol{a}_i$ of this vector (of length $|M_P| = |I|$) represents an estimated bias on the active power at bus i, being what is interpreted as a power theft. Conversely, if $\boldsymbol{a} = 0$ then it is interpreted as no theft being reported in the system. This optimization can be solved in a few seconds when considering $\Delta T_{SM} = 10$ minutes and $\Delta T_{PMU} = 30$ seconds, and in under 2 minutes for $\Delta T_{SM} = 10$ minutes and $\Delta T_{PMU} = 6$ seconds. The discussion on theft localization is deferred to Section 6.

6 VALIDATION AND RESULTS

6.1 Test System

The improvement in performance achieved by MISTE over SoA-1 and SoA-2 is evaluated by simulating on the 33-bus test distribution system [9]. Its topology is given Fig. 1. Each optimization problem is modeled in the GAMS environment [12]. The SoA methods are solved using the MINOS solver [34] while the proposed method uses MOSEK [1]. As mentioned earlier, SoA-2 method is slightly modified. In its original version, the bias vector $\boldsymbol{b}$ can potentially detect a bias on any measurement. It is restricted to estimate bias only on active power measurements. The inputs of the three methods are the system topology, the PMU measurements, the smart-meter measurements and the accuracy of each measurement considered. Recall that the energy measurements are converted into power measurements. The evaluation of the accuracy of such measurements is explained below.

Load profiles: for each bus, they are generated by using fine-grained home energy consumption data. The dataset is described in [5]. The instantaneous active power consumption from 20 homes was recorded over eight months, with a resolution of 6 seconds. No distinction is made between the size of the houses nor the time of the year. Overall, a collection of a few thousands traces is available. Two subsets are created, by splitting randomly the data. One set is used for deriving the variance of the power measurements (training set) and the other one is used for the validation process (testing set).

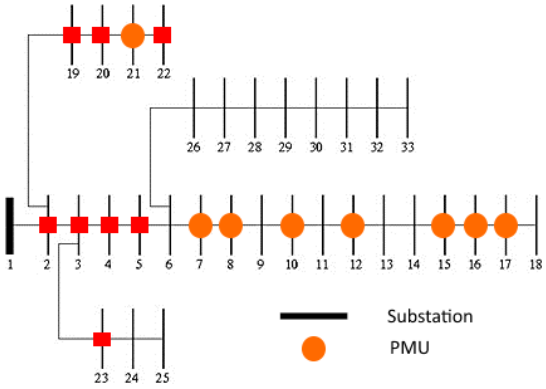

Figure 1: One-line diagram of the 33-bus system. Orange circles represent the PMUs placed and the red squares the "difficult" buses.

The 33-bus test feeder includes static active and reactive power consumptions at each bus; bus-1 is the substation transformer bus. Its voltage is set to $V_0 = 12.66$ kV. The number of houses n_i aggregated at each bus i is such that $n_i = n_{11} P_i^{33bus} / P_{11}^{33bus}$, where $n_{11} = 10$ houses and P_i^{33bus} is the static 33-bus active power load. Bus 11 is chosen since P_{11} is the smallest and a minimum number of 10 houses per bus is desired. Active power load profiles are generated by aggregating the desired number of traces from the testing set. The profiles are then scaled so that their mean matches the static values.

Since no reactive power data is available, reactive profiles are generated from the same dataset, independently of their active power counterpart, in the same fashion as active power traces, by aggregating the desired number of traces and scaling to match the static reactive power value.

Theft model: the system average bus load is computed such that $P_{avg} = \mathrm{avg}(P_2^{33bus}, \cdots, P_{32}^{33bus})$. An illegal load is modeled as a constant active power sink. The load value is taken to be x% of P_{avg} (where x will be either 10 or 30). During a smart-meter time-slot, a single illegal load is connected to the network, at a given bus.

6.2 Measurement Model

PMU: PMU measurement errors are simulated as additive white Gaussian noise of nominal variance σ_{PMU}^2, for both the voltage magnitude and angle. A value of $\sigma_{PMU} = 0.1\%$ is chosen, meaning that the variance of a voltage magnitude or voltage angle measurement error β is such that $\boldsymbol{E}[\beta^2] = \sigma_{PMU}^2 \beta^2$. The errors are independent across buses. The voltage magnitude error is independent from the angle error. Given a number of PMUs, they are placed sequentially according to a greedy method (described in [46] and targeted at DSSE). Such placement method is nearly optimum for state estimation (which

is the primary reason why an LDC places PMUs in the system). The number of PMUs is selected to be 8 [10]. The PMU locations are shown in Fig. 1 with the orange circles. ΔT_{PMU} is chosen to be equal to 6s.

Power measurements: power measurements are constant for a smart-meter time-slot; ΔT_{SM} is set to 10 minutes. They correspond to the mean of the true bus active load profile (respectively reactive profile), to which a Gaussian error is added (constant for a smart-meter slot), corresponding to measurement inaccuracy. The standard deviation of the error is taken to be 1% of the nominal value and corresponds to a simulated added noise.

The variation of the bus power within a smart-meter interval is modeled by a normal distribution, which is a typical choice in state estimation [32]. The standard deviation corresponding to the error made between the true instantaneous power and the power measurement is estimated on the training dataset. Its value is estimated to be 10% of the nominal power measurement. This value is used by σ_m in the objective function when m refers to a power measurement.

6.3 Comparison of MISTE to the Benchmark

MISTE is compared to the two SoA methods. Receiver operating characteristic (ROC) curves are used to assess the performances. Each point on the curve corresponds to a different value of the underlying parameter (i.e. α for SoA-1, κ for SoA-2 and λ for MISTE). A ROC curve represents on a 2D graph two measures: the true positive rate (TPR) and the false positive rate (FPR) of each theft detector. A higher true positive rate means that theft is better detected, and a lower false positive rate means that less false alarms are triggered, which is desirable. Ideally, the perfect theft detector would have a ROC curve reaching the point {TPR = 1, FPR = 0}. The ROC curves for each method are given in Fig. 2.

For a given discrimination parameter and for a given bus i, the TPR and FPR measures are computed over several realizations. A realization is defined as follow: there are two classes of realizations. One with theft and one without. Realizations with theft are used to compute the TPR, while the others are used to compute the FPR. For both types, bus load profiles of duration ΔT_{SM} are generated. For realizations with theft, an additional constant load is added at the considered bus i, of magnitude $x \times P_{avg}$. Synthetic smart-meter and PMU measurements are then computed, to which artificial noise is added. In Fig. 2, the TPR and FPR values reported are computed for 20 realizations with theft on bus i and 20 without per bus, and are averaged over all the 32 load buses considered.

For MISTE as well as SoA-2, a theft is detected if the sum of the respective bias vector variables (respectively $\Sigma_i \boldsymbol{a}_i$ and $\Sigma_i \boldsymbol{b}_i$) is greater than zero, meaning that a measurement bias was detected. For SoA-1, a theft is detected if the value of the objective function is above the threshold C[2].

Based on Fig. 2, it appears clearly that MISTE significantly outperforms the two SoA approaches. The ROC curve of the proposed method is way above the others and the closest to

[2]As a reminder, C is dependent on the choice of α as explained in Section 4.1.

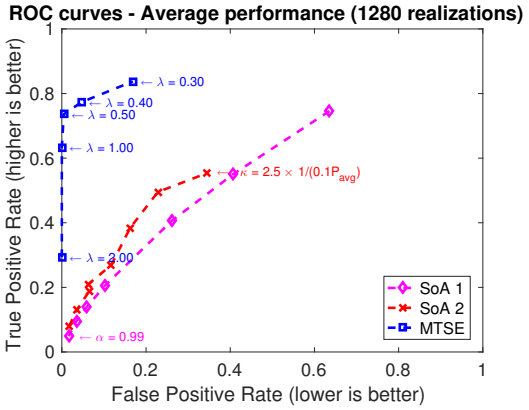

Figure 2: Receiver operating characteristic (ROC) curves for MISTE and the 2 SoA approaches. Parameters: $\Delta T_{PMU} = 6$s, $\Delta T_{SM} = 10$mins, $P_{theft} = 0.3 P_{avg}$. An ideal detector would have a point at the top left corner of the plot.

the ideal point. Indeed MISTE is robust to false positives while having a good theft detection rate. Given a PMU time-step of 6 seconds, a smart-meter time-slot length of 10 minutes, and a theft magnitude of $30\% P_{avg}$, an FPR of almost 0 is attained by choosing a value of $\lambda = 0.5$, while the TPR is above 0.7 (70%). This validates the method and the fact that considering measurements across time improves the detector performances. It also appears clearly that the two SoA methods perform poorly. Indeed, snapshot approaches require high measurement redundancy (i.e., many more voltage measurements) to be effective.

6.4 Impact of the theft magnitude and PMU time-slot length on the performance

The influence of two parameters, the PMU time-slot length ΔT_{PMU} and the theft magnitude, on the detector's performance is studied in this section.

The number of PMU measurements taken within a smart-meter time-slot is inversely proportional to ΔT_{PMU}. A smaller ΔT_{PMU} means that more PMU measurements are available, but also increased the computational burden for MISTE, as this increases the number of optimization variables. Considering a PMU time-slot length ΔT_{PMU} of 30 seconds instead of 6 seconds.(i.e., going from 100 PMU slots to 20 within a smart-meter slot) leads to faster computations without any degradations in the ROC curve. This shows that while considering several PMU measurements over a smart-meter time-slot improves the performance compared to the SoA methods, there exist a limit where considering even more does not lead to any further improvements[3].

Fig. 3 shows the ROC curves when the theft magnitude is reduced from $0.3 P_{avg}$ (shown in Fig. 2) to $0.1 P_{avg}$. Clearly the theft magnitude does not impact the false positive rate of

[3]By contrast, the PMU measurement period cannot be increased too much without any loss of performance, and as it comes closer to the smart-meter period, the performance of MISTE will converge to the one of SoA-2.

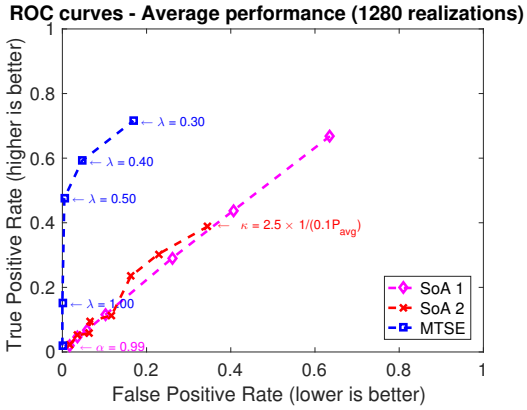

Figure 3: Receiver operating characteristic (ROC) curves for MISTE and the 2 SoA approaches. Parameters: $\Delta T_{PMU} = 6$**s,** $\Delta T_{SM} = 10$**mins,** $P_{theft} = 0.1P_{avg}$**.**

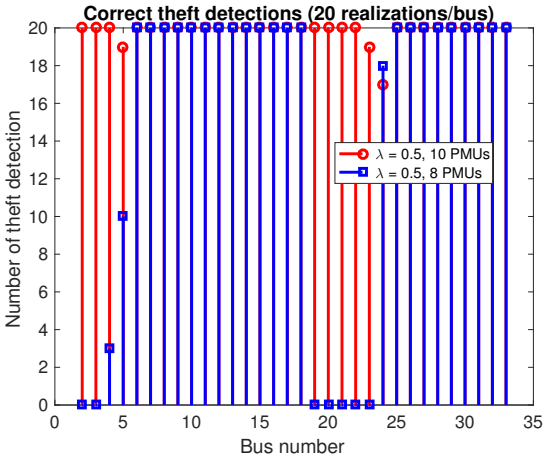

Figure 4: Influence of the theft location on the detection performance. For each bus, 20 realizations with theft are computed. The number of detections is reported. Parameters: $\Delta T_{PMU} = 6$**s,** $\Delta T_{SM} = 10$**mins,** $P_{theft} = 0.3P_{avg}$**,** $\lambda = 0.5$**.**

any detector, only the true positive rate is changed. Reducing the theft magnitude leads to a lower detection rate for all the methods. The performance of MISTE remains much better than the two SoA methods, which do not perform better than a random guess. Indeed a theft magnitude of $0.1P_{avg}$ is of the order of magnitude of the load variations around a 10 minute average value. It is therefore very hard to detect with a snapshot-based method.

6.5 Voltage Measurement Insights

This section focuses on MISTE and a value of $\lambda = 0.5$ is fixed. Such value is chosen since it corresponds to the highest TPR while having almost zero false positives. Figure 4 illustrates the number of theft detections for each bus, when 20 realizations with theft were simulated, per bus. When 8 PMUs are considered, it appears clearly that it is much harder to detect theft at buses located close to the substation (buses 2 to 5 and 19 to 24) than buses located at the end of the feeder. Those "difficult" buses are represented by a red square in Fig. 1.

When used for DSSE, PMUs are mostly placed near the leafs of a distribution systems, which leaves the buses located close to the substation with less measurement points. Moreover, an illegal load located at a bus near the substation will have little impact on the overall system voltage measurements, given that the power it consumed travels through a limited number of lines, and sees a smaller impedance than if it was located at the end of a feeder. By adding 2 extra PMUs at buses 2 and 3 (close to the substation, and at the feeder connection with two branches), on top of the 8 already there and placed for DSSE (thus giving a total of 10 PMUs in the system), the theft detection performance can be greatly improved, as illustrated by Fig. 4. Where previously it was impossible to detect theft located at those "difficult" buses, the detection performance has now significantly increased. The engineering insight conveyed is that by adding a couple of extra PMUs close to the substation on top of the existing ones placed for DSSE, the theft detection performance can be greatly improved. Moreover this implies that optimal PMU placement for theft detection is different than for DSSE.

6.6 Theft Localization

While theft detection is important, being able to localize the offending bus is even more crucial. Given that the two SoA methods are not able to detect theft well, localization performance is not computed for them. The localization performance of MISTE is evaluated as follows; for each bus i, 20 realizations with theft at that bus are computed. The output bias vector $\boldsymbol{a}$ of size $|I| \times 1$ is used for localization. $k^* = \underset{k}{\text{argmax}}(\boldsymbol{a}_k)$ (i.e., the bus) is reported as the theft location.

The localization performance is illustrated by Fig. 5, when 10 PMUs are placed in the system (8 for DSSE and 2 extra at buses 2 and 3 & $\lambda = 0.5$). The average distance in number of hops in the graph representing the system topology (i.e., Fig. 1) between the reported theft location and the true location is plotted. For most locations, the average distance between the true bus at which theft is happening and the reported one is less than one bus. The worst case is when a theft happens at bus 21. In that case out of 20 realizations, bus 1 (which is 4 buses away from bus 21) gets reported all the time instead. While this is not perfect, this would help the LDC limit significantly its search space.

7 CONCLUSION

A novel method, MISTE, for detecting dangerous theft in distribution system is presented. It relies on available grid power and PMU measurements, and combines them across time using state estimation to detect inconsistencies. The proposed method improves significantly the state of the art with a small cost in complexity: for a given system, a higher detection rate can be reported while limiting the number of false alarms. The

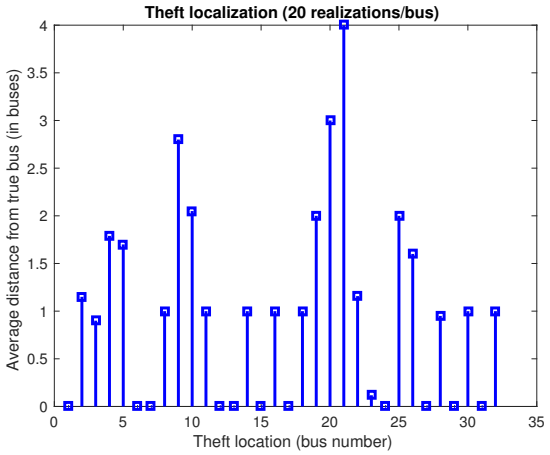

Figure 5: Theft localization performances when 10 PMUs are placed in the system (8 for DSSE and 2 extras). For each bus, 20 realizations with theft are computed. The average distance between the reported bus and the true bus is plotted. Parameters: $\Delta T_{PMU} = 6$**s,** $\Delta T_{SM} = 10$**mins,** $P_{theft} = 0.3P_{avg}$**,** $\lambda = 0.5$**.**

localization performance of the proposed method is quantified and reported; very few theft are reported further away than one hop from the bus where theft is happening. Engineering insights regarding PMU placement are given; the optimal placement for theft detection is different than for DSSE.

Future research directions include the study of multiple thefts. Even though only the case of a single theft has been studied here, MISTE can be generalized to a multiple thefts environment. However the performance evaluation study becomes more complex in this case. Moreover, the influence of distributed generation (DG) on theft detection as well as the detection of DG theft (false reporting of injected power for monetary gain) are also left for future research.

A APPENDIX - LINEARIZED POWER-FLOW EQUATIONS

The linearized power-flow equations are obtained as follows, for each smart-meter time-slot:

(1) For a given smart-meter time-slot, power measurements available at each bus are used to compute the average state of the system; i.e. the voltage phasor vector $[\underline{v}_1^*, \cdots, \underline{v}_{|I|}^*]$ is determined. The voltage profile can be computed using any power flow solver. Such vector represents the operating point of the system over the considered smart-meter time-slot.

(2) Using the distribution load flow matrix $\mathscr{M}$, the linear power-flow equations are written:

$$\begin{bmatrix} \underline{w}_1 \\ \vdots \\ \underline{w}_{|I|} \end{bmatrix} = \begin{bmatrix} V_0 \\ \vdots \\ V_0 \end{bmatrix} - \mathscr{M} \times \begin{bmatrix} \overline{S}_1 / \underline{v}_1^* \\ \vdots \\ \overline{S}_{|I|} / \underline{v}_{|I|}^* \end{bmatrix} \tag{5}$$

Where for each bus i, S_i is related to the state vector $\boldsymbol{x}$ such that $S_i = \boldsymbol{x}_i + j\boldsymbol{x}_{2i}$ and $\underline{w}_i$ is the voltage phasor. Equations (5) can be expressed in Cartesian coordinates in order to relate state vectors $\boldsymbol{u}$ and $\boldsymbol{x}$, such that $\boldsymbol{u} = \mathrm{PF}(\boldsymbol{x})$ where $\mathrm{PF}(\cdot)$ refers to the linear formulation of the power flow in Cartesian coordinates.

REFERENCES

[1] [n. d.]. MOSEK Modeling Cookbook âĂŤ MOSEK Modeling Cookbook 2.3. ([n. d.]). https://docs.mosek.com/modeling-cookbook/index.html

[2] 2013. Review of Cost Allocation Policy for Unmetered Loads. (2013). Available at https://www.oeb.ca/industry/policy-initiatives-and-consultations/review-cost-allocation-policy-unmetered-loads.

[3] 2015. SENTINEL multimeasurement meter. (2015). Available at https://www1.itron.com/PublishedContent/100196SP-08_SENTINEL_Multimeasurement_Meter_web.pdf.

[4] H. Ahmadi, J. R. Marti, and A. von Meier. 2016. A Linear Power Flow Formulation for Three-Phase Distribution Systems. *IEEE Transactions on Power Systems* PP, 99 (2016), 1–10. https://doi.org/10.1109/TPWRS.2016.2533540

[5] Omid Ardakanian, Srinivasan Keshav, and Catherine Rosenberg. 2011. Markovian Models for Home Electricity Consumption. In *ACM SIGCOMM*. https://doi.org/10.1145/2018536.2018544

[6] V. Arya and B. Narayanaswamy. 2014. Loss localisation in smart distribution networks. In *2014 Sixth International Conference on Communication Systems and Networks (COMSNETS)*. 1–8. https://doi.org/10.1109/COMSNETS.2014.6734879

[7] D. Atanackovic and V. Dabic. 2013. Deployment of real-time state estimator and load flow in BC Hydro DMS - challenges and opportunities. In *2013 IEEE Power Energy Society General Meeting*. https://doi.org/10.1109/PESMG.2013.6672408

[8] C.J. Bandim, Jr. Alves, J.E.R., Jr. Pinto, A.V., F.C. Souza, M.R.B. Loureiro, C.A. Magalhaes, and F. Galvez-Durand. 2003. Identification of energy theft and tampered meters using a central observer meter: a mathematical approach. In *Transmission and Distribution Conference and Exposition, 2003 IEEE PES*, Vol. 1. 163–168 Vol.1. https://doi.org/10.1109/TDC.2003.1335175

[9] M. E. Baran and F. F. Wu. 1989. Network reconfiguration in distribution systems for loss reduction and load balancing. *IEEE Trans. on Power Del.* (1989).

[10] C. Carquex, C. Rosenberg, and K. Bhattacharya. 2017. State Estimation in Power Distribution Systems Based on Ensemble Kalman Filtering. *arXiv:1712.01317 [eess]* (2017). http://arxiv.org/abs/1712.01317

[11] Lijuan Chen, Xiaohui Xu, and Chaoming Wang. 2011. Research on anti-electricity stealing method base on state estimation. In *2011 IEEE Power Engineering and Automation Conference (PEAM)*, Vol. 2. 413–416. https://doi.org/10.1109/PEAM.2011.6134972

[12] GAMS Development Corporation. 2013. General Algebraic Modeling System (GAMS) Release 24.2.1. Washington, DC, USA. (2013). http://www.gams.com/

[13] S.S.S.R. Depuru, Lingfeng Wang, and V. Devabhaktuni. 2011. Support vector machine based data classification for detection of electricity theft. In *Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES*. 1–8. https://doi.org/10.1109/PSCE.2011.5772466

[14] S.S.S.R. Depuru, Lingfeng Wang, V. Devabhaktuni, and P. Nelapati. 2011. A hybrid neural network model and encoding technique for enhanced classification of energy consumption data. In *2011 IEEE Power and Energy Society General Meeting*. 1–8. https://doi.org/10.1109/PES.2011.6039050

[15] Soma Shekara Sreenadh Reddy Depuru, Lingfeng Wang, and Vijay Devabhaktuni. 2011. Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. *Energy Policy* 39, 2 (Feb. 2011), 1007–1015. https://doi.org/10.1016/j.enpol.2010.11.037

[16] Soma Shekara Sreenadh Reddy Depuru, Lingfeng Wang, Vijay Devabhaktuni, and Robert C. Green. 2013. High performance computing for detection of electricity theft. *International Journal of Electrical Power & Energy Systems* 47 (May 2013), 21–30. https://doi.org/10.1016/j.ijepes.2012.10.031

[17] Aryadevi Remanidevi Devidas and Maneesha Vinodini Ramesh. 2015. Power theft detection in microgrids. In *2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*. 1–8.

[18] L. T. Faria, J. D. Melo, and A. Padilha-Feltrin. 2016. Spatial-Temporal Estimation for Nontechnical Losses. *IEEE Transactions on Power Delivery* 31, 1 (Feb. 2016), 362–369. https://doi.org/10.1109/TPWRD.2015.2469135

[19] Y. Gu, T. Liu, D. Wang, X. Guan, and Z. Xu. 2013. Bad data detection method for smart grids based on distributed state estimation. In *2013 IEEE International Conference on Communications (ICC)*. 4483–4487. https:

//doi.org/10.1109/ICC.2013.6655273
[20] Wenlin Han and Yang Xiao. 2014. NFD: A practical scheme to detect non-technical loss fraud in smart grid. In *2014 IEEE International Conference on Communications (ICC)*. 605–609. https://doi.org/10.1109/ICC.2014.6883385
[21] Shih-Che Huang, Yuan-Liang Lo, and Chan-Nan Lu. 2013. Non-Technical Loss Detection Using State Estimation and Analysis of Variance. *IEEE Transactions on Power Systems* 28, 3 (Aug. 2013), 2959–2966. https://doi.org/10.1109/TPWRS.2012.2224891
[22] BC Hydro. [n. d.]. Electricity theft. ([n. d.]). Available at https://www.bchydro.com/safety-outages/power-lines-and-your-health/electricity-theft.html.
[23] Rong Jiang, Rongxing Lu, Ye Wang, Jun Luo, Changxiang Shen, and Xuemin Shen. 2014. Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology* 19, 2 (April 2014), 105–120.
[24] P. Jokar, N. Arianpoo, and V.C.M. Leung. 2015. Electricity Theft Detection in AMI Using Customers' Consumption Patterns. *IEEE Transactions on Smart Grid* PP, 99 (2015), 1–1. https://doi.org/10.1109/TSG.2015.2425222
[25] P. Kadurek, J. Blom, J.F.G. Cobben, and W.L. Kling. 2010. Theft detection and smart metering practices and expectations in the Netherlands. In *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*. 1–6. https://doi.org/10.1109/ISGTEUROPE.2010.5638852
[26] Ting Liu, Yun Gu, Dai Wang, Yuhong Gui, and Xiaohong Guan. 2013. A novel method to detect bad data injection attack in smart grid. In *2013 Proceedings IEEE INFOCOM*. 3423–3428. https://doi.org/10.1109/INFCOM.2013.6567175
[27] Chun-Hao Lo and N. Ansari. 2013. CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid. *IEEE Transactions on Emerging Topics in Computing* 1, 1 (June 2013), 33–44. https://doi.org/10.1109/TETC.2013.2274043
[28] W. Luan, G. Wang, Y. Yu, J. Lin, W. Zhang, and Q. Liu. 2015. Energy theft detection via integrated distribution state estimation based on AMI and SCADA measurements. In *2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*. 751–756. https://doi.org/10.1109/DRPT.2015.7432350
[29] P. McDaniel and S. McLaughlin. 2009. Security and Privacy Challenges in the Smart Grid. *IEEE Security Privacy* 7, 3 (May 2009), 75–77. https://doi.org/10.1109/MSP.2009.76
[30] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz. 2013. A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures. *IEEE Journal on Selected Areas in Communications* 31, 7 (July 2013), 1319–1330. https://doi.org/10.1109/JSAC.2013.130714
[31] S. McLaughlin, B. Holbert, S. Zonouz, and R. Berthier. 2012. AMIDS: A multi-sensor energy theft detection framework for advanced metering infrastructures. In *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*. 354–359. https://doi.org/10.1109/SmartGridComm.2012.6486009
[32] A. Monticelli. 1999. *State Estimation in Electric Power Systems*. Springer.
[33] A. Monticelli. 2000. Electric power system state estimation. *Proc. IEEE* 88, 2 (Feb. 2000), 262–282. https://doi.org/10.1109/5.824004
[34] B. A. Murtagh and M. A. Saunders. 1983. *MINOS 5.0 User's Guide.*:. Technical Report. Defense Technical Information Center, Fort Belvoir, VA. https://doi.org/10.21236/ADA138522
[35] J. Nagi, K.S. Yap, S.K. Tiong, S.K. Ahmed, and A.M. Mohammad. 2008. Detection of abnormalities and electricity theft using genetic Support Vector Machines. In *TENCON 2008 - 2008 IEEE Region 10 Conference*. 1–6. https://doi.org/10.1109/TENCON.2008.4766403
[36] Daniel Nikolaev Nikovski, Zhenhua Wang, Alan Esenther, Hongbo Sun, Keisuke Sugiura, Toru Muso, and Kaoru Tsuru. 2013. Smart meter data analysis for power theft detection. In *Machine Learning and Data Mining in Pattern Recognition*. Springer, 379–389.
[37] A.H. Nizar, Z.Y. Dong, and Y. Wang. 2008. Power Utility Nontechnical Loss Analysis With Extreme Learning Machine Method. *IEEE Transactions on Power Systems* 23, 3 (Aug. 2008), 946–955. https://doi.org/10.1109/TPWRS.2008.926431
[38] A. H. Nizar, Z. Y. Dong, J. H. Zhao, and P. Zhang. 2007. A data mining based NTL analysis method. In *Power Engineering Society General Meeting, 2007. IEEE*. IEEE, 1–8.
[39] L.A.M. Pereira, L.C.S. Afonso, J.P. Papa, Z.A. Vale, C.C.O. Ramos, D.S. Gastaldello, and A.N. Souza. 2013. Multilayer perceptron neural networks training through charged system search and its Application for non-technical losses detection. In *Innovative Smart Grid Technologies Latin America (ISGT LA), 2013 IEEE PES Conference On*. 1–6. https://doi.org/10.1109/ISGT-LA.2013.6554383
[40] C.C.O. Ramos, A.N. de Sousa, J.P. Papa, and A.X. Falcao. 2011. A New Approach for Nontechnical Losses Detection Based on Optimum-Path Forest. *IEEE Transactions on Power Systems* 26, 1 (Feb. 2011), 181–189. https://doi.org/10.1109/TPWRS.2010.2051823
[41] C.C.O. Ramos, A.N. Souza, J.P. Papa, and A.X. Falcao. 2009. Fast Non-Technical Losses Identification Through Optimum-Path Forest. In *15th International Conference on Intelligent System Applications to Power Systems, 2009. ISAP '09*. 1–5. https://doi.org/10.1109/ISAP.2009.5352910
[42] R. N. Rodrigues, J. K. Zatta, P. C. C. Vieira, and L. C. M. Schlichting. 2016. A low cost prototype of a Phasor Measurement Unit using Digital Signal Processor. In *IEEE Biennial Congress of Argentina*. https://doi.org/10.1109/ARGENCON.2016.7585328
[43] S. Salinas, Ming Li, and Pan Li. 2012. Privacy-preserving energy theft detection in smart grids. In *2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*. 605–613. https://doi.org/10.1109/SECON.2012.6275834
[44] S. Salinas, Changqing Luo, Weixian Liao, and Pan Li. 2014. State estimation for energy theft detection in microgrids. In *2014 9th International Conference on Communications and Networking in China (CHINACOM)*. 96–101. https://doi.org/10.1109/CHINACOM.2014.7054266
[45] S. A. Salinas and P. Li. 2016. Privacy-Preserving Energy Theft Detection in Microgrids: A State Estimation Approach. *IEEE Transactions on Power Systems* 31, 2 (March 2016), 883–894. https://doi.org/10.1109/TPWRS.2015.2406311
[46] L. Schenato, G. Barchi, D. Macii, R. Arghandeh, K. Poolla, and A. Von Meier. 2014. Bayesian linear state estimation using smart meters and PMUs measurements in distribution grids. In *SmartGridComm*. https://doi.org/10.1109/SmartGridComm.2014.7007708
[47] T.A. Short. 2013. Advanced Metering for Phase Identification, Transformer Identification, and Secondary Modeling. *IEEE Transactions on Smart Grid* 4, 2 (June 2013), 651–658. https://doi.org/10.1109/TSG.2012.2219081
[48] Thomas B Smith. 2004. Electricity theft: a comparative analysis. *Energy Policy* 32, 18 (Dec. 2004), 2067–2076. https://doi.org/10.1016/S0301-4215(03)00182-4
[49] C. L. Su, W. H. Lee, and C. K. Wen. 2016. Electricity theft detection in low voltage networks with smart meters using state estimation. In *2016 IEEE International Conference on Industrial Technology (ICIT)*. 493–498. https://doi.org/10.1109/ICIT.2016.7474800
[50] Jen-Hao Teng. 2003. A direct approach for distribution system load flow solutions. *IEEE Transactions on Power Delivery* (July 2003). https://doi.org/10.1109/TPWRD.2003.813818
[51] R.D. Trevizan, A. Rossoni, A. Suman Bretas, D. da Silva Gazzana, N. Geraldo Bretas, R. de PodestÃą Martin, A.L. Bettiol, A. Carniato, and L.F. do Nascimento Passos. 2015. Non-technical losses identification using Optimum-Path Forest and state estimation. In *PowerTech, 2015 IEEE Eindhoven*. 1–6. https://doi.org/10.1109/PTC.2015.7232685
[52] A. von Meier, D. Culler, A. McEachern, and R. Arghandeh. 2014. Micro-synchrophasors for distribution systems. In *ISGT, IEEE PES*. https://doi.org/10.1109/ISGT.2014.6816509
[53] S. Weckx, C. Gonzalez, J. Tant, T. De Rybel, and J. Driesen. 2012. Parameter identification of unknown radial grids for theft detection. In *2012 3rd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*. 1–6. https://doi.org/10.1109/ISGTEurope.2012.6465644
[54] Zhifeng Xiao, Yang Xiao, and D.H. Du. 2013. Exploring Malicious Meter Inspection in Neighborhood Area Smart Grids. *IEEE Transactions on Smart Grid* 4, 1 (March 2013), 214–226. https://doi.org/10.1109/TSG.2012.2229397
[55] Zikun Xu. 2015. *A Design of Theft Detection Framework for Smart Grid Network*. Master's thesis. University of Waterloo, Canada. https://uwspace.uwaterloo.ca/handle/10012/9837