Electrical Power and Energy Systems 101 (2018) 301–310

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

Clustering-based novelty detection for identification of non-technical losses

Joaquim L. Viegas[a,*], Paulo R. Esteves[b], Susana M. Vieira[a]

[a] IDMEC, Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais, 1, 1049-001 Lisbon, Portugal
[b] PowerData, Portugal

ARTICLE INFO

Keywords:
Clustering
Data mining
Detection of non-technical losses
Electricity theft
Novelty detection
Smart metering

ABSTRACT

The reduction of non-technical losses is a significant part of the total potential benefits resulting from implementations of the smart grid concept. This paper proposes a data-based method to detect sources of theft and other commercial losses. Prototypes of typical consumption behavior are extracted through clustering of data collected from smart meters. A distance-based novelty detection framework classifies new data samples as malign if their distance to the typical consumption prototypes is significant. The proposed method works on the space of four different indicators of irregular consumption, enabling the easy interpretation of results. A use case based on real data is presented to evaluate the method. The threat model considers sixteen different possible types of changes in consumption pattern that result from non-technical losses, including attacks and defects present since the first day of metering. The proposed clustering-based novelty detection method for identification of non-technical losses, using the Gustafson-Kessel fuzzy clustering algorithm, achieves a true positive rate of 63.6% and false positive rate of 24.3%, outperforming other state-of-the-art unsupervised learning methods.

1. Introduction

In electrical grids, non-technical losses (NTLs) are equal to the difference between electricity supplied and electricity paid for, subtracting the energy lost through heat in lines, transformers and other equipments. NTLs are the result of electricity theft, fraud or deficient metering assets and have significant financial impact to utilities and economies. Theft is widespread in many developing economies, such as India, where theft has been estimated to amount to more than 1% of the country gross domestic product (GDP) [1]. The impact of NTLs is also significant in developed countries, in the UK electricity theft is estimated at £173 million every year [2], in the US it may be worth up to $6 billion [3].

The growing proliferation of the smart grid concept and implementation of advanced metering infrastructure (AMI) systems results in grids with many digitally interconnected assets, enabling complete remote control and monitoring. Two-way communications between assets and utility systems have the potential to enable better grid management. Meanwhile, this wide use of cyber-physical systems opens the door for hacking and cyber-attacks.

Usually, the reported sources of NTLs are fraud through meter manipulation, tapping distributions lines and non-payment [4–6]. Deficient meters and utility systems that compromise measurements and collusion with utility employees can also result in losses. The use of smart meters (SMs) for remote control and consumption data collection widens the attack surface for electricity theft [7,8]. Through meter hacking, manipulation and spoofing of communication individuals can enact false data and bad data injection (BDI) attacks [9].

Multiple data-based classification and estimation techniques have been tested to detect NTLs, such as state estimation [10], clustering [11], neural-networks [12], support-vector machines (SVM) [13] and decision trees [14,15]. Some of the studies only deal with electricity theft while other studies deal with aggregated NTLs, not being able to pin-point the exact location of their source [16,17]. Multiple authors are starting to deal with the resulting potential threats that come from the extended attack-surface due to smart meters [7,18,19]. Recent research focuses on challenges in dealing with large and imbalanced datasets collected through smart grid assets, usually using artificial intelligence techniques [15,20,21].

Taking into account the potential of sophisticated fraudsters and cyber-attacks, [22,23] propose game-theoretic frameworks to deal with electricity theft. In [18], multiple classifiers are evaluated in an adversarial environment, analyzing the worst case scenario assuming attackers have knowledge of the detection technique used. In [7], supervised and non-supervised classification techniques are tested to detect a synthetic consumption pattern that result from theft, achieving best results with SVM classification.

This paper proposes a method to detect sources of NTLs in smart grids. We focus on all types of losses that can result in changes in the consumption data that is collected by a SM and communicated to the

* Corresponding author.
E-mail address: joaquim.viegas@tecnico.ulisboa.pt (J.L. Viegas).

https://doi.org/10.1016/j.ijepes.2018.03.031
Received 12 October 2017; Received in revised form 21 February 2018; Accepted 21 March 2018
Available online 31 March 2018
0142-0615/

utility. Firstly, indicators of irregular consumption are computed from the collected consumption data, representing changes in behavior or irregularities in comparison to similar consumers. Secondly, the data of a set of benign consumers is clustered to uncover the prototypes of legitimate behavior, representing the different patterns of indicators that result from normal consumption. Thirdly, the prototypes are used in a distance-based novelty detection method. The farther away data from an analyzed consumer is from the normal prototypes, the higher their NTLs score is, indicating they may be stealing electricity or metering equipment is malfunctioning.

We propose the use of fuzzy Gustafson-Kessel clustering (GK) to detect consumption patterns resulting from the presence of NTLs, which we show is well suited for the application and has not been used in the current literature on novelty detection. A novelty detection framework has not been used before in the field of detection of NTLs and electricity theft. The method is tested on a use case that extends the threat models proposed in [7,21,24]. A complete set of possible changes of consumption, including sources of NTLs active from day of connection, are considered. Results of the use case show the potential of the method, achieving good results, out-performing other tested techniques proposed in the literature to deal with equivalent data. The proposed indicators enable an easy interpretation of the scores given by the detection method, which contrasts to the non-transparent nature of most techniques used in the literature.

We believe the method is well suited to be used in areas of a smart grid where significant aggregated NTLs are detected through calculation of the difference between supplied and billed electricity. In this case, the method can pin-point the thieving individual or faulty equipment.

2. Threat model

The considered threat model identifies the possible attack vectors and main system vulnerabilities related to electricity theft in smart grids. The term *attack vectors* refers to the ways an individual can maliciously affect the electricity network or the utilities systems to pay less than the full amount they owe for the electricity they consume. Other kinds of NTLs can also be detected using this framework, as they also result in changes or irregularities in the consumption data sent to the utility by the SM.

We propose a model that extends the ones presented in [7,21,24]. This paper presents an extended analysis of the attack surface, considers false data attacks with higher complexity such as proposed in [21], and includes cases where the losses start on the first day of consumption data acquisition (we refer to these cases as first-day attacks).

This paper considers a smart grid environment with an AMI system, characterized by presence of SMs at all the consumption endpoints. SMs have advanced communication capabilities and automatically send consumption data to the utility. The attack surface is said to be increased with the use of SMs. New cyber and data attack/vulnerabilities, such as the possibility of sending false readings, appear with the use of these equipments [7,25,26]. BDI can be used to steal electricity and breakdown grid assets, possibly having catastrophic consequences [9]. Current literature on detection of theft and NTLs and electricity is giving an increased importance to this issue [27–31].

The different NTLs sources and attack/vulnerability vectors are pictured in Fig. 1. The encircled points indicate the different possible attack vectors.

NTLs can be detected through the analysis of metering data. The proposed method deals with the types of NTLs that result in a change or irregular consumption pattern (e.g. if a consumer connects an equipment to a distribution line their consumption is lowered). Table 1 lists the different attack/vulnerability vectors, scenarios and expected changes in metered consumption data. Column *Point* indicates the related point in Fig. 1. The first-day attack scenario is considered. Note most scenarios are expected to result in a variation or irregularity of the metered consumption data.

Scenarios relating to billing were not listed because they result in changes done after the processing consumption data collected by SMs. They include non-payment (point 4), collusion with utility employees (points 5 and 6), cyber attacks to commercial systems and erroneous billing (point 7).

Cases resulting in a constant reduction of consumption, such as the disconnection of a meter or use of a strong magnet to interfere with it, can be detected through straightforward methods such as slope analysis and rule-based systems [14,32]. If the attackers are highly resourceful, they may send false consumption data (e.g. BDI) which is seemingly legitimate [7,18]. In an adversarial environment the attacker evolves trough time and information on past attacks may not be useful to prevent future ones [18]. Also, if the attack is made from the day of connection to the grid (first-day), no reduction or change in consumption can be detected, only the comparison to similar consumers is effective [33].

As past examples of theft may not be suitable, different types of attacks are generated to test the proposed detection technique. Also, according to [7,8,10], real data samples of electricity fraud are not easily available as the smart grid is not fully implemented yet. Six of the attacks are the ones presented in [7]. The two other complex attacks are proposed by [24]. One deals with the manipulation of data to shift a significant amount of consumption from peak hours to lower valley hours, taking advantage of two-part and three-part tariffs that are higher at peak time. The other considers a especially resourceful thief, manipulating their consumption data to look completely legitimate while lowering their total bill. Each one of the 8 types of attacks is considered in two versions, starting in a day posterior to the first day of consumption data and starting in the first day, resulting in a final set of 16 attack types. h_1 to h_8 are attacks that start later than the day the metering starts and h_{10} to h_{80} represent the first-day versions of the attacks.

1. Random constant reduction of consumption (h_1 and h_{10} for the zero day scenario);
2. Drop of consumption to zero during a random period of the day (h_2 and h_{20});
3. Random hourly reduction of consumption (h_3 and h_{30});
4. Random hourly consumption pattern with reduced average consumption (h_4 and h_{40});
5. Constant hourly consumption equal to the average (h_5 and h_{50});
6. Reversed hourly consumption: switch consumption of hour 1 with hour 24, etc. (h_6 and h_{60});
7. Shift of consumption from peak hours to the rest of the day (h_7 and h_{70});
8. Shift the consumption data to the one of a legitimate consumer with lower electricity needs (h_8 and h_{80})

The following notation is adopted: we work with a smart metering dataset M with N consumers. $\mathbf{m}_i$ are the meter consumption readings from consumer i. The dimension of $\mathbf{m}_i$ is $n = r \times n_d$ where n_d is the number of days and r is the number of consumption readings per day. In this work 24 readings per day are used (one per hour), the simplified notation is: $m_i^{d,t}$ is the consumption in day d for hour t. $\mathbf{m}_i^d = (m_i^{d,1}, m_i^{d,2}, \ldots, m_i^{d,24})$ is the 24 h vector of metered data of consumer i in day d.

To compare similar consumers, a dataset of consumer characteristics S is used. $\mathbf{s}_i$ are the characteristics of consumer i with dimension p equal to the number of characteristics. The following equations describe the way an attack starting on day d by consumer i affects their consumption data. These are used to generate the synthetic attacks used to test the proposed method. μ represents the average function.

- $h_1(m_i^{d,t}) = \alpha m_i^{d,t}, \quad \alpha = \text{random}(0.1, 0.8)$
- $h_2(m_i^{d,t}) = \beta^h m_i^{d,t}$

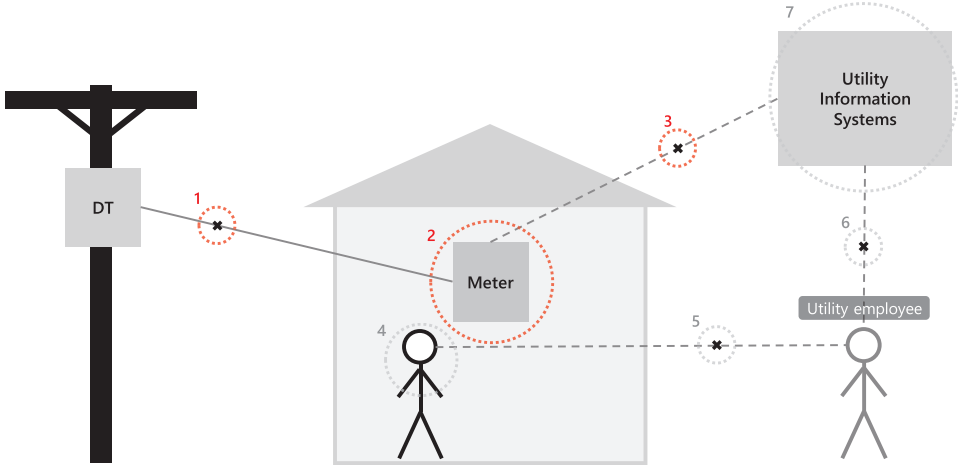


Fig. 1. NTLs sources and attack/vulnerability points: (1) Distribution feeder; (2) Smart meter; (3) Meter communications; (4) Consumer; (5) Relation between consumer and utility employee; (6) Manipulation of data by utility employee; (7) Utility information systems.

$$\beta_t = \begin{cases} 0, & t_{start} < t < t_{end} \\ 1, & \text{else} \end{cases}$$

$t_{start} = \text{random}(0,19)$

$\delta = random(4,24)$

$t_{end} = t_{start} + \delta$

- $h_3(m_i^{d,t}) = \gamma_t m_i^{d,t}, \quad \gamma_t = \text{random}(0.1,0.8)$
- $h_4(m_i^{d,t}) = \gamma_t \mu(m_i^d), \quad \gamma_t = \text{random}(0.1,0.8)$
- $h_5(m_i^{d,t}) = \mu(m_i^d)$
- $h_6(m_i^{d,t}) = m_i^{d,24-t}$
- $h_7(m_i^{d,t}) = \begin{cases} m_i^{d,t} - \lambda m_i^{d,t}, & p_{start} < t < p_{end} \\ m_i^{d,t} + \epsilon/21, & \text{else} \end{cases}$

  p_{start} is the starting hour of the highest consumption three hour period

  $p_{end} = p_{start} + 3$

  $\epsilon = \sum_{j=1}^{3} m_i^{d,p_{start}+j-1}$

- $h_8(m_i^{d,t}) = m_r^{d,t}$

  $r$random consumer with $\mu(m_r^{d,t}) < \mu(m_i^{d,t})$

3. Irregular consumption indicators

Data based techniques for detection of NTLs usually make use of raw consumption data [7,18], limiting the ability to easily understand and interpret their results. We consider the interpretability of the detection method of utmost importance in this application. As we try to detect irregular patterns and threats currently unknown, presenting the reasons why a consumer is flagged by the method is very important. Known studies presenting techniques for visualization of results from NTLs detection have focused on the spatial representation of fraud estimation, accurately presenting in a map the zones with highest losses [16,20,34]. Studies proposing techniques for which the estimation or prediction mechanism is interpretable normally make use of decision trees, these are supervised classification models [14,29]. Techniques such as auto-regressive schemes, enabling detection of irregularities through deviations of average consumption are also easily interpretable [35], but do now allow the detection of the advanced types of NTLs analyzed in this paper.

Four irregular consumption indicators are developed and presented, making the proposed method transparent, as its output is based on these variables. Current literature indicates the importance of two types of indicators, the first type deals with the evolution of the consumption of an individual [36,37] and the second compares individual behavior to other consumers [38,39]. Both these types of indicators can be used regarding absolute energy consumption or the hourly profile. Indicators were developed to deal with hourly data as it is commonly used in NTLs detection and electricity load profiling [15,40]. Types of attacks considered in the threat model only affect consumption at an hourly resolution. Using data with a higher sampling rate could result in better detection performance if attacks that affect the consumption dynamic at a higher resolution (e.g. half-hourly) were considered. In [7], a

Table 1
Attack/vulnerability vectors and expected changes in consumption data.

Attack/vulnerability vectors	Point	Scenarios	Changes in consumption data
Before meter			
Connecting throw-ups on feeder [6]	1	Connection of equipment	Reduction
		Connection of new equipment	Lower than similar consumers
		Connection by non-consumer	None
Meter			
Reverse or disconnect meter [28]	2		Zero consumption
Bypass meter to remove loads [28]	2	From day zero	Lower than similar consumers
		Not from day zero	Reduction
Interference with meter [7]	2	From day zero	Lower than similar consumers
		Not from day zero	Reduction
Remote network exploit, firmware modification, meter hacking [28]	2/3	False data from day zero	Low or irregular pattern in comparison to similar consumers
		False data not from day zero;	Reduction or pattern change
Errors in meter reading [11]	2	From day zero	Low or unusual pattern
		Not from day zero	Reduction

sampling rate of 12 samples/day resulted in the best detection performance in a similar use case to the one presented in this paper.

The indicators are computed for a consumer i and a certain day d, using their consumption data. If the attack starts on day d the change of pattern should be reflected on a change of consumption behavior in comparison with the past. In the case the attack started before, it should result in a different consumption behavior when compared with similar consumers.

The developed indicators are the following:

- I_1: Indicator of consumption variation. Ratio between current and past consumption;
- I_2^e,I_2^c: Indicators of hourly consumption pattern change.
- I_3: Indicator of consumption difference in comparison to consumers with similar characteristics.
- I_4^e,I_4^c: Indicators of hourly consumption pattern difference in comparison to consumers with similar characteristics.

The indicator of consumption variation I_1 is a ratio between the consumption of the last α days and the last β periods of α days.

$$I_1(i,d) = \frac{\sum_{j=1}^{\alpha}\sum_{k=1}^{24} m_i^{d-j,k}}{\frac{1}{\beta}\sum_{l=1}^{\alpha\beta}\sum_{k=1}^{24} m_i^{d-\alpha-l,k}} \tag{1}$$

Indicators of hourly consumption pattern change I_2^ν relates the hourly pattern of a day with the mean hourly pattern of the α days before. If ν is the euclidean distance ($\nu = e$), changes in absolute consumption will be the most relevant for the indicator. If ν is the Pearson correlation ($\nu = c$), changes of dynamic can be detected.

$$I_2^\nu(i,d) = \nu(m_i^d, \mu(m_i^{d-1-\alpha},\ldots,m_i^{d-1})) \tag{2}$$

I_3 is the indicator of consumption difference in comparison the consumers $r \in R$ with the greatest similarity. It compares the mean consumption of the last α days to the mean consumption for the same days for the consumers with the most similar characteristics. R are the τ consumers in $\{1,2,\ldots,N\}$ with lowest similarity between their characteristics $\mathbf{s}_i$.

The similarity between consumer r and i is calculated by $\nu(\mathbf{s}_r,\mathbf{s}_i)$ with ν being the euclidean distance.

$$I_3(i,d) = \frac{\frac{1}{\alpha}\sum_{l=1}^{\alpha}\sum_{k=1}^{24} m_i^{d-j-\alpha-1,k}}{\mu\left(\left\{\frac{1}{\alpha}\sum_{l=1}^{\alpha}\sum_{k=1}^{24} m_r^{d-j-\alpha-1,k} \;\forall\; r \in R\right\}\right)} \tag{3}$$

I_4^e and I_4^c are the indicators of hourly consumption pattern difference in comparison to consumers with the greatest similarity. I_4^ν relates the mean hourly consumption of the last α days between consumers.

$$I_4^\nu(i,d) = \nu(\mu(m_i^{d-\alpha},\ldots,m_i^d), \mu(\{(m_r^{d-\alpha},\ldots,m_i^d) \;\forall\; r \in R\})) \tag{4}$$

4. Detection of non-technical losses

A novelty detection framework is adopted for the development of the detection method, this removes the need of having access to past examples of NTLs. Data-based classifications techniques usually need examples of both positive (fraud/NTLs) and negative (legitimate/benign) classes, which can be a significant challenge when starting to tackle this problem or non-legitimate consumers follow advanced strategies [7,18].

The proposed method is pictured in Fig. 2:

- The feature extraction is used to transform the benign dataset and sample from the analyzed consumer i in irregular consumption indicators, as described in Section 3. This enables an easy interpretation of the scores given by the detection technique;
- Fuzzy clustering is applied on the benign data, as explained in the following paragraphs, resulting in prototypes that represent "normality";
- The clustering-based novelty detector infers, using (6), the NTLs score for a consumer i. This is done through comparison of the sample from that consumer and the prototypes.

The following paragraphs explain how the irregular consumption indicators presented in prior Section 3 are used to infer the NTLs score through a novelty detection framework.

4.1. Novelty detection

Novelty detection is able to detect new samples through identification of the structure and distribution of past data. The models used are usually derived from a set of "normal" data, they are able to classify incoming data points as coming from the "normal" distribution or being "abnormal"/novel. This type of framework is commonly used in medical diagnostic problems, credit card and mobile phone fraud and failure detection [41].

In our case, taking novelty detection as a framework, the data of benign consumers is considered as "normal". The objective is to classify data collected from consumption end-points as legitimate or attacked (source of NTLs). Due to the possible evolving nature of adversaries and lack of data from real attacks, we consider this framework specially well suited.

Schemes for novelty detection are divided into probabilistic, distance-based, reconstruction-based and domain-based techniques. The proposed method uses a type of distance-based novelty detection based on clustering. One or more prototypes of benign data are used in a distance-based method, if the data from a consumption end-point falls far away from the prototypes, it results in an high NTLs score.

4.2. Clustering-based novelty detection

Assuming the data collected from the benign consumers can only be reproduced by multiple statistical distributions, simple distance-based novelty methods are not suitable, these only compare the data to one prototype (usually the mean or median of the benign data).

Clustering tries to partition a set of individuals, usually represented by data vectors, into clusters of minimum intra-cluster and maximum inter-cluster distances. The distance function λ measures the dissimilarity between two points.

It is easy to imagine that the behavior of legitimate consumers can vary by a significant amount (e.g. households with full time workers with children in comparison to a retired couple). Schemes such as K-means have been used extensively in the literature to find the multiple types of consumption behaviors in large sets of electricity consumers [42,43]. Clustering can be used to extract a number of prototypes from the benign data. The closer prototype to incoming data can be used to derive a NTLs score.

$\mathbf{x}_{id}$ is the feature vector associated to consumer i in a certain day d. The vector $\mathbf{x}_{id} = (I_1,I_2^e,I_2^c,I_3,I_4^e,I_4^c)$ is composed of the indicators presented in Section 3. $X \in \Re^6$ is the feature dataset for N consumers composed of the indicators of n_d days:

$$X = (\mathbf{x}_{11},\mathbf{x}_{12},\ldots,\mathbf{x}_{1n_d},\mathbf{x}_{21},\ldots,\mathbf{x}_{2n_d},\ldots,\mathbf{x}_{N1},\ldots,\mathbf{x}_{Nn_d}) \tag{5}$$

Adopting the notation for fuzzy clustering presented in [44], clustering partitions X into C clusters $A_1,\ldots,A_C$. The partition is defined by partition matrix $U = \{u_{ki}\}$, where u_{ki} represents the degree to which point i belongs to cluster k, we call this the membership degree. Each cluster is represented by a prototype or center v_k with dimension equal to the data points, the set of all centers is V.

The clusters centers V represent the benign data, we intend to give the highest novelty score to points that don't fit into any of the C clusters [41]. In the proposed method the score $y(\mathbf{x}_{id}|V)$, for a certain data point i, is equal to the minimum distance to a cluster center, as presented in (6).

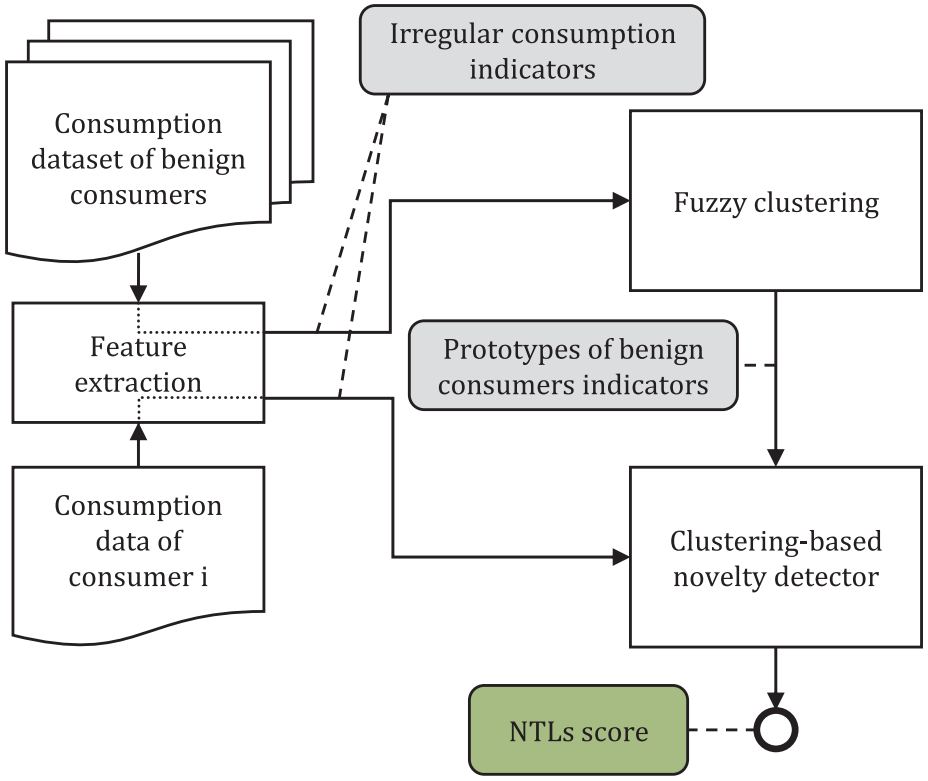


Fig. 2. Diagram of the clustering-based NTLs detection method.

$$y(\mathbf{x}_{ij}|V) = \min_k d(\mathbf{x}_{ij},v_k) \tag{6}$$

In the context of this paper, $y(\mathbf{x}_{ij}|V)$ is the NTLs score of consumer i on day j. In practice this score is transformed in a binary classification using a certain threshold ζ, when $y(\mathbf{x}_{ij}|V) < \zeta$ the consumer is legitimate, if $y(\mathbf{x}_{ij}|V) \geqslant \zeta$ it indicates that the consumption end-point of consumer i is the source of NTLs (attacked).

The proposed scheme is able to score the samples from a set of consumers that is never used for extraction of benign prototypes. The clustering methods work on the space of a set of benign consumers, extracting multiple prototypes of normal behavior which can be then used for comparison with any other consumer. The consumption behavior of a consumer is compared to benign consumers and not to their past, enabling the detection of first-day attacks.

4.2.1. Fuzzy C-means clustering

Fuzzy C-means (FCM) [44,45] is a clustering method that iteratively minimizes the sum of distances between points and cluster centers. Distances are weighted by the membership degree of a point to each cluster and the fuzzifier parameter m adjusts the "fuzziness" of the partition. (7) presents the FCM objective function using the euclidean distance.

$$J(U,V) = \sum_{i=1}^{n}\sum_{k=1}^{C}(u_{ki})^m d^2(\mathbf{x}_i,v_k) \tag{7}$$

$$\lambda^2(x_{id},v_k) = (\mathbf{x}_i - v_k)^{\mathrm{I}} I (\mathbf{x}_i - v_k) \tag{8}$$

4.2.2. Fuzzy Gustafson-Kessel clustering

The fuzzy Guastafson-Kessel (GK) scheme [46,47,44] can be seen as extension of euclidean distance FCM using cluster-specific fuzzy Mahalanobis distances:

$$\lambda^2(x_{id},v_k) = (\mathbf{x}_i - v_k)^{\mathrm{I}} \Sigma_k^{-1} (\mathbf{x}_i - v_k) \tag{9}$$

Σ_k represents the fuzzy covariance matrix of the cluster. This type of dissimilarity measure results in hyperellipsoidal clusters. The different clusters may assume different shapes. Compared to FCM, GK offers greater flexibility in terms of the shapes of clusters it can find in the data. To estimate the fuzzy covariance matrix the following equation is used [46]:

$$\Sigma_k = \frac{\sum_{i=1}^{n}(u_{ki})^m (\mathbf{x}_i - v_k)(\mathbf{x}_i - v_k)^{\mathrm{I}}}{\sum_{i=1}^{n}(u_{ki}^m)} \tag{10}$$

4.2.3. Methods used for comparison

We compare the performance of the proposed method to the following methods: simple distance-based novelty detection; equivalent method using K-Means (KM) and Gaussian mixture models (GMM); DBSCAN clustering and support vector machines (SVM) as these two methods are used in studies that deal with comparable data [7,24].

Simple distance-based novelty detection, consists on using the same method presented in (6) but with "one cluster" whose center is the average of the benign data points [41]. Two distances are used in this method, the Euclidean distance of (8) and the Mahalanobis distance of (9).

KM is a particular case of the FCM scheme [44] when the fuzzifier m tends to 1. This scheme results in crisp membership degrees. This is on of the most commonly used clustering schemes in the literature. GMM estimate the density of a set of distributions from training data [48]. The parameters of the different Gaussian distributions are fitted by maximum likelihood, using the expectation-maximization algorithm [41,49]. SVM [50] is a commonly used machine learning method, specially suited for classification. This is the technique used in [7] that deals with comparable data. DBSCAN is a density-based clustering algorithm [51], it has been proposed to detect integrity attacks on the electricity grid in [24], which deals with the same type of data as the scheme proposed in this paper.

The DBSCAN approach employed follows the scoring method presented in (6), substituting the set of cluster centers V with the set of core points determined from the set of benign data. This way, using

Table 2
Parameters used for the indicators of irregular consumption presented in Section 3.

Indicator	Parameters	Indicator relates:
I_1	$\alpha = 1,\beta = 10$	Consumption of the past day and average from last 10 days
I_2^v	$\alpha = 10$	Pattern of the last 24 h and average pattern from last 10 days
I_3	$\tau = 10,\alpha = 10$	Consumption of the last 10 days with 10 most similar consumers
I_4^v	$\tau = 10,\alpha = 10$	Average hourly pattern of the 10 days with the one of the 10 most similar consumers

DBSCAN, the score given to a consumer is inversely proportional to the distance of their data to the closest benign data core point.

4.3. Interpretation

To interpret the score given by the method, we propose the analysis of the different indicators in comparison to the benign prototypes. Using the mean and standard deviation estimates of the benign cluster, the absolute variation in number of standard deviations (NSTDs) Δ is defined as:

$$\Delta_l(\mathbf{x}_{ij}|V,\delta) = \frac{|x_{ij}^l - v_k^l|}{\delta_k^l}, \quad k = \text{argmin}_k d(\mathbf{x}_{ij},v_k) \tag{11}$$

This is the variation, for variable l (one of the irregular consumption indicators), of point $\mathbf{x}_{ij}$ in comparison to the closest cluster k, represented by its prototype v_k^l and standard deviation δ_k^l. Visual representation of NSTDs, as presented by the examples of Section 5, enables a straightforward interpretation of the result of the proposed method.

5. Experimental results

A use case was developed to evaluate the performance of the proposed method. The dataset was constructed similarly to what is proposed in [7], we use real smart metering consumption data and construct synthetic attacks based on the threat model presented in Section 2.

5.1. Dataset

The data used comes from approximately four thousand Irish households, it was collected during one and a half years (2009–2010) as part of a smart metering trial from the Commission for Energy Regulation. We assume these households are free from the types of sources of NTLs considered in the threat model. The data is made available by the Irish Social Science Data Archive [52]. Collected data consists on consumption logged every thirty minutes and surveys responded before the trial began. The data is aggregated hourly for use of the proposed method.

The use case consists on training the method on a set of benign data and then evaluating it on a different set comprising benign data and sixteen synthetic attacks constructed for each benign sample. We chose to separate the consumers used for training and testing to reduce the bias of the results, as the techniques can potentially overfit to the behavior of consumers. The data from five random days of each season was used. The full evaluation dataset is extracted following these steps:

1. Randomly select five working days for each season;
2. For all consumers:
   (a) Generate the 16 curves resulting from the synthetic attacks presented in the threat model;
   (b) Calculate the irregular consumption indicators for benign and synthetic attacks.

Survey questions are used to compute the similarity between consumers used in indicators I_3,I_4^e and I_4^c. These are: age, social class, employment status, number of adults in the household, number of children and type of home. Only households without any missing consumption or data from surveys are used, the final dataset consists of 2515 consumers. As we use only benign data for half the consumers and benign and attack data for the other half, the total number of samples in the use case is: $1258 \times 5 \times 4 + 1257 \times 17 \times 5 \times 4 = 452540$. The testing set presents a balance of 6% negative samples (from benign consumers), which results from the creation of sixteen synthetic attacks from each benign sample. The training set presents a balance of 100% negative samples as required in the proposed unsupervised classification scheme.

5.2. Parameters

Two different types of parameters are used: the parameters for the irregular consumption indicators presented in Section 3 and for the techniques presented in Section 4.

The parameters used to compute the indicators and their meaning is listed in Table 2. For the parameter α in I_1 a value of 1 is used, because higher values affect the capacity of the indicator to represent small consumption changes that are possible under the considered threat model. For the remaining parameters, the performance of the proposed method was tested for different configurations of the parameters with values varying in the following way: β (I_2^v,I_3), α (I_2^v,I_4^v) $\in$ [1,5,10,15];$\tau \in$ [5,10,15,20]. The best configuration found was for both sets of parameters equal to 10, meaning current consumption is compared with two weeks of past and the ten most similar consumers are used for comparison.

The evaluation of the proposed method and different techniques in the presented use case is done by randomly dividing the dataset in training and testing sets. The training set is used for clustering and deriving the SVM model, consisting on the benign samples from a set of randomly selected consumers (50% of all consumers). The remaining consumers (50%) are used for performance evaluation. The testing set presents a balance of 6% negative samples (from benign consumers), the training set presents a balance of 100% negative samples as required in unsupervised classification. Four different performance metrics are used:

- True Positive Rate (*TPR*): Number of samples identified as attacks divided by the number of all samples with attacks;
- False Positive Rate (*FPR*): Number of samples incorrectly identified as attacks divided by the number of benign samples;
- Area Under the Receiver Operating Characteristic Curve (*AUC*): The curve represents the behavior of the detector for a range of thresholds in terms of *TPR* and *FPR*. This measure is robust to the presence of class imbalances on the data [53].

To determine the best parameters for the method and techniques presented in Section 4, a grid search was done using the *AUC* as performance metric. Grid-search tests all possible parameter combinations from the sets of values: the number of clusters was tested between 2 and 36, the fuzziness parameter m was tested for the values [0.5,0.6,...,1.9,2],ν for the values [0.1,0.2,...,0.9,1],γ for the values [0.5,0.6,...,1.4,1.5],*eps* for the values [0.5,1,3,6,12,24] and the min_s for the values [25,50,100,200,400,800]. The resulting final parameters are listed in Table 3. The threshold selected to present the results is the one that maximizes $TPR-FPR$, this is done individually for each evaluation.

5.3. Results and discussion

The performances of the proposed method and comparison techniques are listed in Table 4, it lists, for the four different metrics, results

Table 3
Parameters used to evaluate the proposed method and techniques presented in Section 4, resulting from grid search for *AUC* maximization.

Technique	Parameters
KM	$C = 25$
GMM	$C = 7$
FCM	$C = 30, m = 1.6$
GK	$C = 2, m = 1.2$
SVM	$\nu = 0.3, \gamma = 1.2$
DBSCAN	$eps = 12, min_s = 100$

Table 4
Results of the performance evaluation.

Metric	Method	All	Non first-day	First-day
AUC	Euc.	0.645	0.594	0.697
	Mahal.	0.700	0.666	0.616
	KM	0.714	0.729	0.699
	GMM	0.730	0.729	0.730
	FCM	0.729	0.756	0.702
	GK	0.741	0.751	0.731
	SVM	0.711	0.715	0.708
	DBSCAN	0.707	0.718	0.696
TPR	Euc.	0.643	0.783	0.734
	Mahal.	0.696	0.705	0.811
	KM	0.620	0.711	0.687
	GMM	0.587	0.676	0.708
	FCM	0.644	0.711	0.714
	GK	0.623	0.743	0.754
	SVM	0.636	0.663	0.739
	DBSCAN	0.606	0.708	0.672
FPR	Euc.	0.413	0.614	0.367
	Mahal.	0.361	0.390	0.540
	KM	0.275	0.327	0.325
	GMM	0.229	0.310	0.304
	FCM	0.270	0.269	0.347
	GK	0.243	0.327	0.337
	SVM	0.291	0.296	0.349
	DBSCAN	0.276	0.351	0.317

for all attacks, only non first-day attacks and only first-day attacks. The Euc. and Mahal. techniques consist on simple distance-based novelty detection using the distances as explained in Section 4. The proposed method using GK clustering performed the best overall (0.741 *AUC*, 0.623 *TPR* and 0.243 *FPR*). Using FCM, the method achieves the best performance for non first-day attacks (0.756 *AUC*).

Evaluation with *AUC* is pictured in Fig. 3. For all attacks GK clearly outperforms other tested methods while FCM and GMM achieve very similar performance. For non first-day attacks the FCM achieves the best performance, closely followed by GK and KM. For first-day attacks GK and GMM achieve similar performance, resulting in an overall better performance of GK clustering.

To compare the method to the state of the art, the achieved results are compared to [7], in which an unsupervised method was used to deal with a similar set of data considering a lower number of complex attacks (h_1 to h_6). In [7], a *TPR* of 76% and *FPR* of 29% were obtained using unsupervised SVM, resulting in a *TPR*−*FPR* of 47%. We achieve a *TPR* of 23.3% and *FPR* of 24.3% with GK, resulting in a *TPR*−*FPR* of 38.0%. The data that generated the former two sets of results are different, making the direct comparison unsuitable. The SVM method used in [7] was tested on the use case presented in this paper, achieving a *TPR*−*FPR* of 34.5%, being outperformed by the clustering scheme. To further validate our results, the proposed method was tested on the attacks used in [7], achieving a *TPR* of 80.0% and *FPR* of 28.7% using GK clustering. We are not able to compare directly to results presented in [21,24], in which synthetic attacks are also simulated from the same data, as the evaluation methods and dataset different, making direct comparison unsuitable.

Current literature presents studies with detection method evaluated with real data. In [54], the authors achieve a precision (number of correctly predicted attacks) of 64% on a dataset with more than 150 k consumers from Malaysia, using supervised SVM. In [55], an optimum-path forest classifier achieves a 96.5% accuracy on a dataset of 5 k Brazilian consumers. High accuracies can seem important, but in use cases where the data is imbalanced (majority of negative or positive class), the measure is not adequate. For example, if a dataset contains 95% negative class samples and the model classifies all as negative, it will still have an accuracy of 95%. Datasets used for detection of NTLs are imbalanced [14,56]. In studies dealing with consumers from Spain [14] and Brazil [57], accuracies over 80% are achieved, resulting in *TPR* of 24% and 29%, *FPR* of 4% and 16%. In [56], fuzzy modeling and SVM are used in a scheme tested with 100 k samples from Brazil, achieving a *TPR*−*FPR* of around 10%. In comparison to the aforementioned studies and taking into account the complexity of some of the synthetic attacks simulated, the results attained by the proposed method are encouraging.

The poor performance of the Euc. and Mahal. techniques presents a strong indicator that the data from benign consumers can only be approximated with multiple distributions. The performance of SVM was worst than the proposed method with any of the clustering techniques tested, proving the suitability of the method for this application,

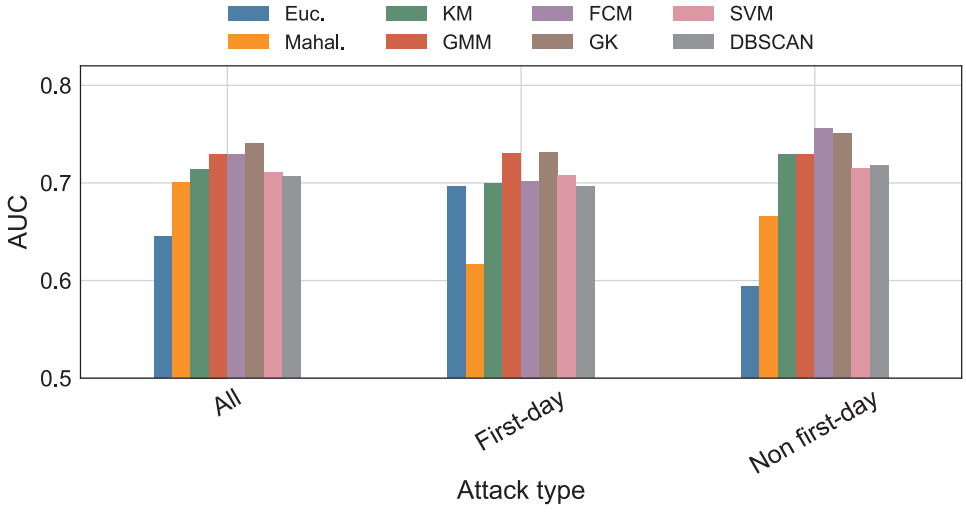


Fig. 3. Performance comparison with the *AUC* metric.

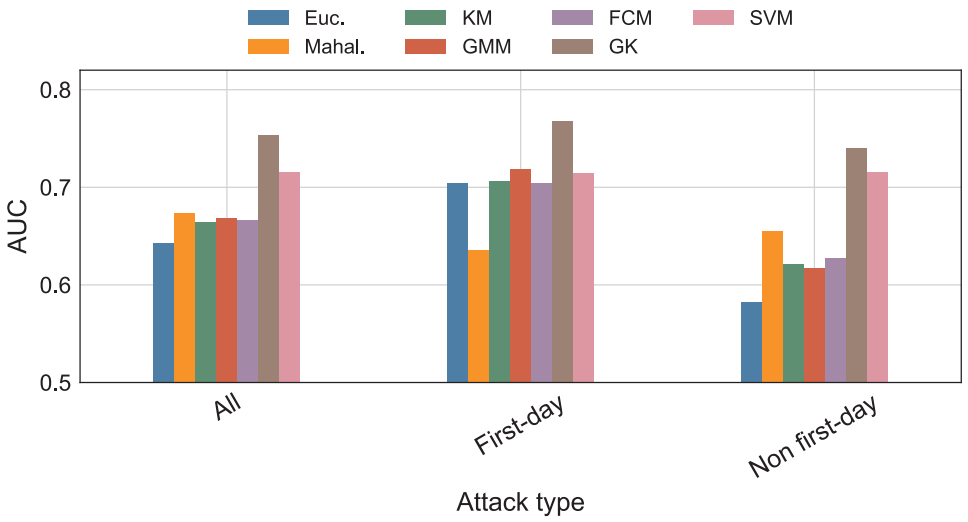


Fig. 4. Performance comparison with $C = 2$.

providing performance and interpretable results.

GK clustering is specially well suited for this use-case, as it was able to divide the benign data in only two clusters while achieving better performance than the other techniques with higher numbers of clusters (7 for GMM, 25 for KM and 30 for FCM). As the number of clusters needed for GMM is also significantly lower in comparison to KM and FCM, it is clear that spherical clusters are not a good fit for the data.

To conclude on the differences of performance with different numbers of clusters, we tested the method using only two clusters in all techniques, resulting it the *AUCs* pictured in Fig. 4. Besides GK, all other clustering techniques were not able to achieve satisfying performance with two clusters, thus showing the suitability of this algorithm.

Table 5 details the *AUC* results for each of one of the attacks considered.

5.4. Examples

Two examples on the use of the proposed method are presented next. We randomly selected a benign sample and one of a h_1 attack. The scores given by the techniques tested are picture in Fig. 5. The bar is red if the sample is classified as an attack and blue if classified as benign. If correctly classified, the example with no attack should be in blue and the example of attack in red.

The benign sample and the NSTDs resulting from the method are

Table 5
AUC results of the performance evaluation for each one of the attack types. The best performance for each type of attack is in bold.

Attack	Euc.	Mahal.	KM	GMM	FCM	FGK	SVM	DBSCAN
All	0.645	0.700	0.714	0.730	0.729	**0.741**	0.711	0.707
h_1	0.557	0.627	0.716	**0.758**	0.733	0.709	0.717	0.700
h_{10}	**0.659**	0.561	0.566	0.620	0.566	0.612	0.598	0.559
h_2	0.639	0.696	0.752	0.722	**0.784**	0.769	0.749	0.733
h_{20}	0.699	0.684	0.745	0.759	0.748	**0.790**	0.754	0.742
h_3	0.543	0.632	0.728	0.743	**0.759**	0.714	0.722	0.702
h_{30}	**0.628**	0.526	0.544	0.590	0.552	0.569	0.536	0.567
h_4	0.640	0.720	0.798	0.746	**0.874**	0.843	0.795	0.766
h_{40}	0.870	0.629	0.833	0.879	0.832	**0.883**	0.870	0.837
h_5	0.553	0.737	0.780	0.848	0.800	**0.876**	0.728	0.803
h_{50}	0.825	0.656	0.939	0.959	0.942	**0.966**	0.927	0.948
h_6	0.755	0.806	0.883	0.862	0.896	**0.910**	0.868	0.883
h_{60}	0.824	0.828	0.962	0.969	0.960	**0.978**	0.950	0.957
h_7	0.485	0.478	0.482	**0.506**	0.484	0.487	0.469	0.482
h_{70}	0.499	0.488	0.474	**0.518**	0.478	0.487	0.486	0.466
h_8	0.579	0.629	0.693	0.648	**0.721**	0.697	0.670	0.672
h_{80}	**0.567**	0.557	0.532	0.550	0.537	0.562	0.539	0.495

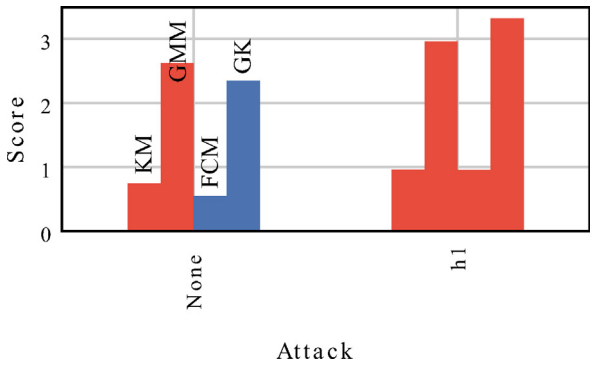
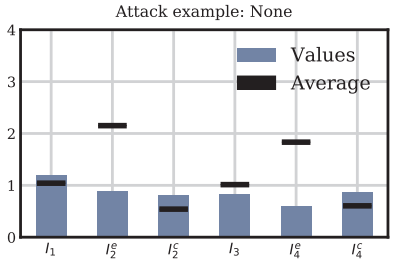
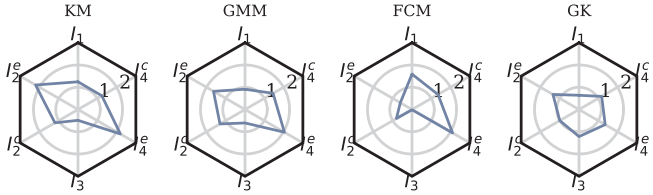


Fig. 5. Scores given by the proposed method. The bars are colored red if the sample is classified as an attack and blue if classified as benign. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)



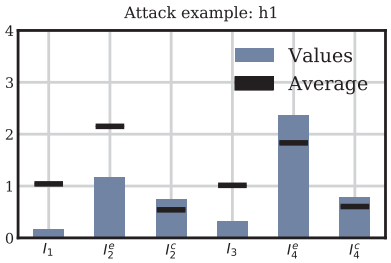
(a) Feature values.



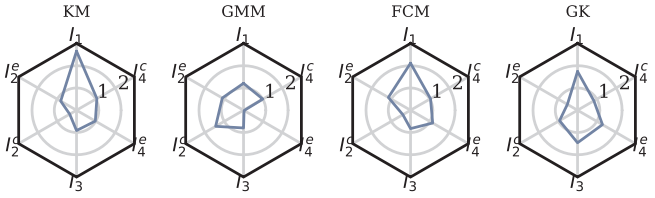
(b) Feature variation from sample to closest cluster center: low values represent sample closer to a center.

Fig. 6. Example of response to a benign sample.

pictured in Fig. 6. Fig. 6(a) presents in blue the value of the indicators for the sample and in black their average value for the benign dataset. The benign sample is close to the average for most indicators. The low



(a) Feature values.



(b) Feature variation from sample to closest cluster center: low values represent sample closer to a center.

Fig. 7. Example of response to a h1 attack sample.

values of I_2^e and I_4^e are expected, as they represent the distance of the consumption pattern to the past and similar consumers. Fig. 6(b) pictures response of the method in terms of NSTDs, showing the deviation to the closest cluster center. Besides I_2^e and I_4^e, the indicators seem to be close to a cluster center, indicating the clustering techniques are capturing the shape of the benign dataset.

The example of an h_1 attack and the NSTDs resulting from the method are pictured in Fig. 7. Fig. 7(a) I_1 and I_3 present unusually low values in comparison to the benign average, indicating a significant reduction of consumption in comparison to both the past and similar consumers. Fig. 7(b) I_1 is the main driver of distance between the attack sample and the closest center.

6. Conclusions

This paper proposes a method to detect NTLs in smart grids. It works on high resolution consumption data collected from smart meters. Irregular consumption indicators are proposed to reduce the dimensionality of data and allow the easy interpretation of results. We follow a novelty detection framework, making use of fuzzy clustering to find the structure of data when there are no NTLs resulting from the consumption point. When analyzing the data communicated by a smart meter, if its resulting indicators present a significant distance to the clusters identified, it is probably responsible for NTLs. A use case was developed to evaluate the performance of the method. It uses real data from a set of more than two thousand households and encompasses multiple types of possible complex changes to normal consumption data.

The method achieved a performance of up to 0.741 *AUC*, 63.6% true positive rate and 24.3% false positive rate, out-performing the use of SVM proposed in a comparable study. The use of fuzzy clustering, more specifically the Gustafson-Kessel scheme, resulted in the best performance.

In the future, the method should be made part of a more encompassing solution that analyzes losses at different levels of the grid, only being used in zones where there is an identified unbalance between supply and consumption. The techniques used should be analyzed in the framework of big data and high performance computing to understand if it could be used with millions of consumers, the presented use case is encouraging as it deals with close to half a million samples.

Acknowledgements

This work was supported by FCT, through IDMEC, under LAETA, project UID/EMS/50022/2013. The work of J. L. Viegas was supported by the PhD in Industry Scholarship SFRH/BDE/95414/2013 from FCT and Novabase. S. M. Vieira acknowledges support by Program Investigador FCT (IF/00833/2014) from FCT, co-funded by the European Social Fund (ESF) through the Operational Program Human Potential (POPH).

References

[1] Depuru SSSR, Wang L, Devabhaktuni V. Electricity theft: overview, issues, prevention and a smart meter based approach to control theft. Energy Policy 2011;39(2):1007–15.
[2] IBM. Energy theft: incentives to change. Tech rep; 2012.
[3] Energy Association of Pennsylvania. Energy theft kills, costs innocent pennsylvanians millions; 2007.
[4] Smith TB. Electricity theft: a comparative analysis. Energy Policy 2004;32(18):2067–76.
[5] Aguero JR. Improving the efficiency of power distribution systems through technical and non-technical losses reduction. In: IEEE PES T&D conference and exposition; 2012. p. 1–8.
[6] Lewis FB. Costly throw-ups': electricity theft and power disruptions. Electr J 2015;28(7):118–35.
[7] Jokar P, Arianpoo N, Leung VCM. Electricity theft detection in AMI using customers' consumption patterns. IEEE Trans Smart Grid 2016;7(1):216–26.
[8] Yip SC, Wong KS, Hew WP, Gan MT, Phan RC, Tan SW. Detection of energy theft and defective smart meters in smart grids using linear regression. Int J Electr Power Energy Syst 2017;91:230–40.
[9] Wang D, Guan X, Liu T, Gu Y, Sun Y, Liu Y. A survey on bad data injection attack in smart grid. In: 2013 IEEE PES Asia-Pacific power and energy engineering conference (APPEEC); 2013.
[10] Sahoo S, Nikovski D, Muso T, Tsuru K. Electricity theft detection using smart meter data. In: IEEE power & energy society innovative smart grid technologies conference (ISGT); 2015.
[11] Nizar AH, Dong ZY. Identification and detection of electricity customer behaviour irregularities. In: IEEE PES power systems conference and exposition (PSCE'09); 2009. p. 1–10
[12] Jiang R, Tagaris H, Lachsz A, Jeffrey M. Wavelet based feature extraction and multiple classifiers for electricity fraud detection. In: IEEE PES T&D conference and exhibition 2002: Asia Pacific (volume: 3); 2002.
[13] Aravkin A, Wolf M. Analytics for understanding customer behavior in the energy and utility industry. IBM J Res Develop 2016;60(1):1–13.
[14] Monedero I, Biscarri F, León C, Guerrero JI, Biscarri J, Millán R. Detection of frauds and other non-technical losses in a power utility using Pearson coefficient, Bayesian networks and decision trees. Int J Electr Power Energy Syst 2012;34(1):90–8.
[15] Viegas JL, Esteves PR, Melício R, Mendes VMF, Vieira SM. Solutions for detection of non-technical losses in the electricity grid: a review. Renew Sustain Energy Rev 2017;80(December):1256–68.
[16] Faria L, Melo J, Padilha-Feltrin A. Spatial-temporal estimation for nontechnical losses. IEEE Trans Power Deliv 2015;8977:1.
[17] Buevich M, Jacquiau-Chamski A, Schnitzer D, Thacker J, Escalada T, Rowe A. Short paper: microgrid losses - when the whole is greater than the sum of its parts. In: 2nd ACM int conf on emb systems for energy-efficient built environments; 2015. p. 95–8.
[18] Mashima D, Cárdenas AA. Evaluating electricity theft detectors in smart grid networks. Lect Notes Comput Sci 2012;7462: 210–29.
[19] Jiang R, Lu R, Wang Y, Luo J, Shen C, Shen XS. Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci Technol 2014;19(2):105–20.
[20] Glauner P, Meira JA, Valtchev P, State R, Bettinger F. The challenge of non-technical loss detection using artificial intelligence: a survey. Int J Comput Intell Syst 2017;10:760–75.
[21] Krishna VB, Lee K, Weaver GA, Iyer RK, Sanders WH. F-DETA: a framework for detecting electricity theft attacks in smart grids. In: Proceedings – 46th annual IEEE/IFIP international conference on dependable systems and networks, DSN 2016; 2016. p. 407–18.
[22] Cardenas AA, Amin S, Schwartz G, Dong R, Sastry S. A game theory model for electricity theft detection and privacy-aware control in AMI systems. In: 2012 50th annual Allerton conference on communication, control, and computing, Allerton 2012; 2012. p. 1830–7.
[23] Amin S, Schwartz GA. Game-theoretic models of electricity theft detection in smart utility networks. IEEE Control Syst Magaz (February 2015); 2015.
[24] Krishna VB, Weaver GA, Sanders WH. PCA-based method for detecting integrity attacks on advanced metering infrastructure. In: International conference on quantitative evaluation of systems. Springer; 2015. p. 70–85.
[25] McLaughlin S, Podkuiko D, Miadzvezhanka S, Delozier A, McDaniel P. Multi-vendor penetration testing in the advanced metering infrastructure. In: 26th Annual computer security applications conference (ACSAC '10) I; 2010. p. 10.
[26] Grochocki D, Huh JH, Berthier R, Bobba R, Alvaro AC, Sanders WH. AMI threats, intrusion detection requirements and deployment recommendations. In: 2012 IEEE

int conf on smart grid communications; 2012. p. 395–400.
[27] Lo C-H, Ansari N. CONSUMER: a novel hybrid intrusion detection system for distribution networks in smart grid. IEEE Trans Emerg Top Comput 2013;1(1):33–44.
[28] McLaughlin S, Holbert B, Fawaz A, Berthier R, Zonouz S. A multi-sensor energy theft detection framework for advanced metering infrastructures. In: 2012 IEEE int conf on smart grid communications (smartgridcomm), vol. 31; 2013, 7. p. 1319–30.
[29] Jindal A, Dua A, Kaur K, Singh M, Kumar N, Mishra S. Decision tree and SVM-based data analytics for theft detection in smart grid. IEEE Trans Indus Inform 2016;12(3):1005–16.
[30] Leite JB, Mantovani JRS. Detecting and locating non-technical losses in modern distribution networks. IEEE Trans Smart Grid Pre-print 2016.
[31] Yang X, Zhang X, Lin J, Yu W, Zhao P. A Gaussian-mixture model based detection scheme against data integrity attacks in the smart grid. IEEE Internet Things J Pre-print 2016.
[32] Spirić JV, Dočić MB, Stanković SS. Fraud detection in registered electricity time series. Int J Electr Power Energy Syst 2015;71:42–50.
[33] Zhou G, Zhao W, Lv X, Jin F, Yin W. A novel load profiling method for detecting abnormalities of electricity customer. In: IEEE PES general meeting — conference & exposition; 2014.
[34] Porras JA, Rivera HO, Giraldo FD, Correa BSA. Identification of non-technical electricity losses in power distribution systems by applying techniques of information analysis and visualization. IEEE Latin Am Trans 2015;13(3):659–64.
[35] Krishna VB, Iyer RK, Sanders WH. ARIMA-based modeling and validation of consumption readings in power grids. Lect Notes Comput Sci (Including Subseries Lect Notes Artif Intell Lect Notes Bioinform, vol. 9578; 2016. p. 199–210.
[36] Muniz C, Figueiredo K, Vellasco M, Chavez G, Pacheco M. Irregularity detection on low tension electric installations by neural network ensembles. In: Proceedings of the int joint conf on neural networks; 2009. p. 2176–82.
[37] Guerrero JI, Leon C, Biscarri F, Monedero I, Biscarri J, Millan R. 'Increasing the efficiency in Non-Technical Losses detection in utility companies. In: 2010 IEEE Mediterranean electrotechnical conference; 2010. p. 136–41.
[38] León C, Biscarri F, Monedero I, Guerrero JI, Biscarri J, Millán R. Variability and trend-based generalized rule induction model to NTL detection in power companies. IEEE Trans Power Syst 2011;26(4):1798–807.
[39] Faria P, Vale Z. Analysis of consumption data to detect commercial losses using performance evaluation methods in a smart grid. In: IEEE PES T&D conference and exposition, 2011; 2014. p. 1–5.
[40] Rhodes JD, Cole WJ, Upshaw CR, Edgar TF, Webber ME. Clustering analysis of residential electricity demand profiles. Appl Energy 2014;135:461–471 Dec.
[41] Pimentel MAF, Clifton DA, Clifton L, Tarassenko L. A review of novelty detection. Signal Process 2014;99:215–49.
[42] Räsänen T, Voukantsis D, Niska H, Karatzas K, Kolehmainen M. Data-based method for creating electricity use load profiles using large amount of customer-specific hourly measured electricity use data. Appl Energy 2010;87(11):3538–45.
[43] Viegas JL, Vieira SM, Melício R, Mendes V, Sousa JM. Classification of new electricity customers based on surveys and smart metering data. Energy 2016;107:804–17.
[44] Keller JM, Liu D, Fogel DB. Fundamentals of computational intelligence: neural networks, fuzzy systems, and evolutionary computation. 1st ed. Wiley-IEEE Press; 2016.
[45] Bezdek JC. Pattern recognition with fuzzy objective function algorithms. New York and London: Plenum Press; 1981.
[46] Gustafson D, Kessel W. Fuzzy clustering with a fuzzy covariance matrix. IEEE Conf Decis Control 1978(2):761–6.
[47] Bezdek JC, Keller J, Krisnapuram R, Pal NR. Fuzzy models and algorithms for pattern recognition and image processing. Norwell, MA: Kluwer Academic Publishers; 1999.
[48] Hastie T, Tibshirani R, Friedman J. The elements of statistical learning. 2nd ed. Springer Series in Statistics; 2008.
[49] Tarassenko L, Hayton P, Cerneaz N, Brady M. Novelty detection for the identification of masses in mammograms. In: Fourth international conference on artificial neural networks; 1995.
[50] Cortes C, Vapnik V. Support-vector networks. Mach Learn 1995;297:273–97.
[51] Ester M, Kriegel HP, Sander J, Xu X. A density-based algorithm for discovering clusters in large spatial databased with noise. In: KDD-96 proceedings; 1996.
[52] ISSDA. Data from the Commission for Energy Regulation – <http://www.ucd.ie/issda>.
[53] Hanley JA, McNeil BJ. The meaning and use of the area under a receiver operating characteristic (ROC) curve. Radiology 1982;143(4):29–36.
[54] Nagi J, Yap KS, Tiong SK, Ahmed SK, Mohamad M. Nontechnical loss detection for metered customers in power utility using support vector machines. IEEE Trans Power Deliv 2010;25(2):1162–71.
[55] Ramos CC, Souza AN, Chiachia G, Falcão AX, Papa JP. A novel algorithm for feature selection using Harmony Search and its application for non-technical losses detection. Comput Electr Eng 2011;37(6):886–94.
[56] Glauner P, Boechat A, Dolberg L, State R, Bettinger F, Rangoni Y. Large-scale detection of non-technical losses in imbalanced data sets. In: IEEE PES innovative smart grid technologies; 2016.
[57] Costa BC, Alberto BLA, Portela AM, Maduro W, Eler O, Horizonte B. Fraud detection in electric power distribution networks using an ANN-based knowledge-discovery process. Int J Artif Intell Appl (IJAIA) 2013;4(6):17–23.