Electric Power Systems Research 158 (2018) 250–266

Contents lists available at ScienceDirect

Electric Power Systems Research

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

Review

Review of non-technical loss detection methods

George M. Messinis*, Nikos D. Hatziargyriou

Department of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece

ARTICLE INFO

Article history:
Received 14 June 2017
Received in revised form 19 October 2017
Accepted 2 January 2018
Available online 3 February 2018

Keywords:
Data mining
Distribution network analysis
Electricity fraud
Fraud detection
Non-technical losses
Smart metering

ABSTRACT

Electricity theft has been a major issue for many years. Distribution System Operators (DSOs) have been trying to detect electricity theft, however the phenomenon insists, while simple meter inspection methods cannot adequately identify most cases of fraud. In this paper the most recent and characteristic research papers on Non-Technical Loss (NTL) detection are reviewed and their key features are summarized. NTL detection schemes are organized in three large categories: data oriented, network oriented and hybrids. Data oriented and network oriented methods are further divided to subcategories, according to the main concept behind NTL detection. Apart from categorizing the various methods the authors focus on algorithms, data types and size, features, evaluation metrics and NTL detection system response times. An overview of the algorithms used by NTL detection systems is presented focusing on why they are suitable for the specific application. The data types consumed by each NTL detection system are defined and features typically extracted from these data types are presented. In addition, the authors provide a comprehensive list of performance metrics used and comment on their importance. Finally, a qualitative comparison of NTL detectors is provided focusing on performance issues, costs, data variety/quality issues and system response times.

Contents

* Corresponding author.
E-mail addresses: gmessinis@power.ece.ntua.gr (G.M. Messinis), nh@power.ece.ntua.gr (N.D. Hatziargyriou).

https://doi.org/10.1016/j.epsr.2018.01.005
0378-7796/

Nomenclature

ACI	Anomaly coverage index
ACL	Asymmetric control limit
AMI	Advanced metering infrastructure
ANN	Artificial Neural Network
ANOVA	Analysis of variance
ARIMA	Auto-Regressive Integrated Moving Average
ARMA	Auto-Regressive Moving Average
AUC	Area Under Curve
BDR	Bayesian Detection Rate
BP-MLP	Back propagation multi layer perceptron
CS-SVM	Cost sensitive Support Vector Machine
CUSUM	Cumulative sum
DBSCAN	Density based spatial clustering of applications with noise
DER	Distributed energy resource
DR	Detection rate
DSE	Distribution state estimation
DSO	Distribution System Operator
DT	Decision tree
ELM	Extreme learning machine
EWMA	Exponentially weighted Moving Average
FDI	False data injection
FDS	Fraud detection system
FIS	Fuzzy inference system
FN	False negative
FNR	False negative rate
FP	False positive
FPR	False positive rate
GAM	Generalized Additive Model
GIS	Geographical information system
IDS	Intrusion detection system
KLD	Kullback–Leibler divergence
LOF	Local Outlier Factor
MGD	Multivariate Gaussian distribution
MST	Minimum spanning tree
NILM	Non intrusive load monitoring
NTL	Non-technical losses
OPF	Optimum Path Forrest
OS-ELM	Online sequential extreme learning machine
PCA	Principal component analysis
PPV	Positive predictive value
RBF	Radial basis function
ROC	Receiver operating characteristic
RTU	Remote technical unit
SCADA	Supervisory control and data acquisition
SOM	Self organized map
SVM	Support Vector Machine
TN	True negative
TNR	True negative rate
TP	True positive
TPR	True positive rate
WLS	Weighted least squares

1. Introduction

Electricity theft has been a major issue for many years. It is a widely spread phenomenon occurring globally and performed in a variety of ways [1]. It is considered as part of the non-technical losses that also include missing or wrong meter readings, etc. Distribution System Operators (DSOs) have been trying to detect electricity theft in order to reduce non-technical losses that may have various financial and technical consequences. However, despite DSO efforts to detect electricity theft and the application of legal deterrents, the phenomenon insists, especially when traditional methods (simple meter inspection) having several technical and social limitations are applied.

There is a large global experience on non-technical losses. Fraud in the electricity domain might be more intense in developing countries (World Bank reports over 50% of theft [2]), but it is still a reality in developed countries, too. Overall, it has been reported that utility companies worldwide, lose more than $25 billion every year due to electricity theft [3].

Various effects of non-technical losses have been reported in literature, the most important being the loss of revenue which in most cases leads utility companies to pass these losses to benign consumers via tariffs [3]. In addition, the quality of electricity supply is affected (voltage violation, infrastructure damage etc), black-outs might occur and public safety might be at risk [3–7].

In this review, research on Fraud Detection Systems (FDS) does not include why/how Non Technical Losses (NTLs) occur and this is why papers providing a socio-economical analysis of the phenomenon have been omitted. In addition, the authors choose to focus on the technical aspects of FDS (algorithms, data requirements, metrics etc), while omitting research on attacker-defender behavior modeling and utility business models (the choice of FDS according to utility costs and incomes from detecting frauds) [8]. Such factors, including a cost-revenue analysis, should not be neglected though, when designing a real life FDS.

Previous attempts on reviewing this domain include [9–13]. Ref. [9] provides a good overview of the area, it includes however only papers up to 2013. In fact only 17% of the works presented in this review are covered in Ref. [9]. A more recent review published in 2016, is [11] (thus reviewing articles up to 2015). The authors in this case provide a detailed description of a number of important journal and conference papers, but an overview of the domain is missing (Ref. [11] covers approximately 25% of the papers presented in this review). Another attempt to review the field, [10] (published in 2013) does not provide a complete and coherent overview of the domain and it has no overlaps with this work. The more recent work of Glauner et al. [13] presents an overview of data oriented methods (machine learning) covering approximately 20% of this work. Finally, a completely different view of NTL detection (with no significant overlap), that of communications and security, is presented in Ref. [12].

2. Categorization of non-technical loss detection methods

The study of scientific papers on NTL detection shows that there is no common methodology followed for detecting frauds. Researchers adopt methods from different fields of knowledge with the most common ones being machine learning, anomaly detection, cybersecurity and of course distribution network analysis. The various NTL detection schemes are organized in three large categories: data oriented, network oriented and hybrids. What differentiates data oriented from network oriented methods is the use of power grid data (for example network topology or network measurements). Data oriented methods make use of consumer related data only (for example energy consumption, consumer type etc.). Hybrids are methods that use data from both categories. The main categories are presented in Fig. 1.

Data oriented and network oriented methods can be further divided to subcategories, according to the main concept behind NTL detection. Data oriented methods are divided to supervised and unsupervised. Methods that make use of both labels (known positive/fraud and negative/not-fraud classes) are supervised, while methods that make no use of labels are unsupervised. Methods that make use of a single label are categorized as unsupervised and typ-

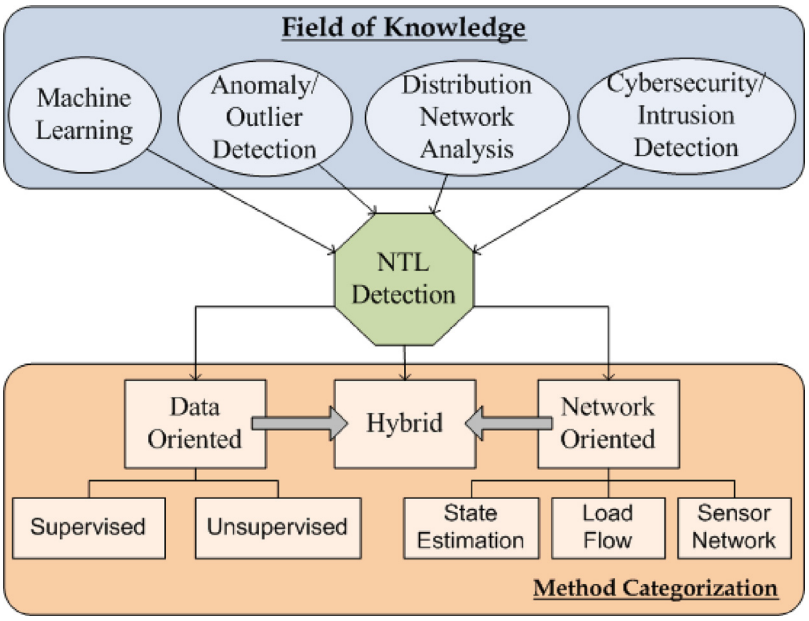

Fig. 1. NTL detection methods categorization.

ically fall under the unsupervised anomaly detection domain. Such methods are used when one of the two classes (e.g. fraud class) contains a very small number of samples. This is usual in various fraud detection applications (e.g. credit card fraud) apart from NTL detection. In this case both labels are known, but the scarcity of the positive label (fraud) prohibits the use of supervised learning methods. The interested reader can find a detailed review of anomaly detection algorithms and applications in Ref. [14]. Finally, there are cases where labeled samples from both classes are available but their number is too small compared to unlabeled samples. Semi-supervised learning methods [15] utilize unlabeled samples too and have recently become more popular due to unlabeled data abundancy and cost of producing labeled samples. Apart from the work presented in Ref. [16] this approach has not been demonstrated enough for detecting NTL and thus only supervised and unsupervised methods are presented next.

Network oriented methods typically neglect labels, since they are based on network analysis and the physical rules that describe such systems. These methods are categorized according to the main concept/algorithm used, i.e. state estimation, load flow or special sensors for detecting frauds.

Hybrid methods borrow concepts from all categories mentioned above. For example, a state estimation method may be used on MV level to detect NTL at MV/LV transformer level. After detecting parts of the network with NTLs, a supervised classification method can be used for localizing NTL at consumer level. Summarizing, the parameters typically found in all NTL detection papers are:

- **Category and Concept**: The category and subcategory a specific work belongs to (Fig. 1).
- **Algorithm(s)**: The main algorithms used for detecting NTL. In most cases, more than one algorithms may be used. For each work however, all algorithms mentioned are listed, even if they are only used for comparative studies. Algorithms implemented in each paper are described in Chapter 5 and listed in Tables 3 and 4.
- **Data type(s)**: The data required by each method. This is a critical parameter when designing a NTL detection method or choosing from existing ones. A detailed presentation of data types is found in Chapter 3.
- **Data set size**: The size of the data set used for the analysis of the NTL detection system is determined by the number of consumers (simulated or not) implicated. Data set size is considered large for 1000 consumers or more, medium for 100–1000 and small for less than 100. The data set size is important, since it provides feedback on the scalability of NTL detection systems. Details on data set size can be found in Tables 3 and 4.
- **Features**: In many cases raw data (described as data types above) are first processed in order to extract features to be used for classification. Although a lot of researchers use features for detecting NTLs, there is no indication of which features should be used. The authors list features and associate them with data types and algorithms, thus making it easier to choose appropriate features either using domain expertise or feature selection algorithms. Features frequently used for NTL detection are presented in Table 1 and relative discussion can be found in Chapter 3.
- **Metrics**: Performance metrics are used to assess the performance of NTL detection methods under various circumstances and to compare systems. A number of metrics are mentioned in literature. The authors' goal is to provide a full list of metrics, under a unique identifier, together with the reason they should (or shouldn't) be used for. Definitions of metrics are provided in Table 2 and relative discussion can be found in Chapter 4.
- **Response time**: The time required for a NTL detection system to decide if a consumer commits fraud. This should not be confused with the time it takes for a classifier to produce a result given the relative input data (which is highly dependent on machine and coding). In contrast, the response time depends on the time required to obtain the input data. Response times are presented in Tables 3 and 4.

3. Data types categorization and definitions

In this chapter the various data types used in literature are organized in broad categories. The main reason for this categorization is to ensure that researchers are not restricted to specific data types to select their algorithm, but they are able to choose their NTL detection system according to the available data. The data type hierarchy is presented in Fig. 2.

Table 1
Families of main features used for NTL detection.

Feature name	Description
Average, Max/Min, Standard Deviation	Standard statistics calculated for a specific time period.
Power/Energy factor	The power factor is defined as the rate of active (kW) to reactive power consumption (kVAr). Instant power measurements are required for this calculation. High resolution (less or equal to 15 min) data must be used for a good estimation. Energy factor is the reactive energy (kVArh) consumed in a time period to the active energy (kWh) consumed in the same period
Load factor	The ratio between the average active energy consumption (kWh) to the maximum active energy consumption (kWh) for a specific time period (for example a month).
Streaks	The number of times the consumption curve goes above and below a mean line (defined as a moving average of the consumption curve).
Daily consumption to contracted power	The sum of active energy consumption in a period (kWh) to the contracted power (kW)
Pearson coefficient	The pearson coefficient of the active energy consumption curve in a specific (typically large) time period. The pearson coefficient measures how well a linear equation describes the relation between active energy consumption and time.
Billed-consumed energy coefficient	Difference of energy billed (kWh) to consumed active energy (kWh) divided by the contracted power (kW).
Predicted kWh	A prediction of the active energy consumption (kWh) given by any forecast model or the difference of this prediction and the measured value.
Wavelet coefficients	The difference of the Wavelet coefficients calculated from the consumption curve to be classified and the Wavelet coefficients of previous years consumption curves.
Fourier coefficients	The difference of the Fourier coefficients calculated from the consumption curve to be classified and the Fourier coefficients of previous years consumption curves. In addition, the phase of the first five Fourier coefficients of the active energy consumption curve can be used.
Polynomial fit coefficients	The difference of the coefficients of the polynomial that best fits the consumption curve to be classified and the coefficients of the polynomial that best fits previous years' consumption curves.
Euclidean distance to mean customer	Euclidean distance of an active energy consumption curve to a consumption curve calculated as the mean consumption of all consumers in the data set.
Consumption curve slope	The slope of the linear equation that best fits the active energy consumption curve time series.
PCA components	A number of components that are calculated from Principal Component Analysis (PCA) or Kernel Principal Component Analysis (KPCA) on the active energy consumption curves. Not all of the components need to be used. The mean of specific components may be used to.
Fractional order dynamic errors	Features that express the difference between a profiled meter usage and a real time consumption time series.
Mismatch ratio	The difference between consumption measured in the MV/LV transformer and the sum of smart meter measurements and estimated technical losses divided by the nominal power of the substation.
Seasonal consumption rates	Total consumer consumption (kWh) in a specific season (for example winter) to consumption (kWh) of another season (for example summer). Total consumer consumption (kWh) in a specific season (for example winter) to the average consumption of consumers on the same substation at the same season (for example winter).
Discrete Cosine Transform coefficients	The k first coefficients of the discrete cosine transformation.
Consumption decrease compared to previous period	A reduction of x% in consumption during a time period of length T in comparison to a past time period of the same length or compared to the average.
Estimated readings	Number of meter readings that are estimated by utility due to inability to access the meter.

Table 2
List of metrics used to evaluate NTL detection methods.

Metric	Definition
Accuracy	$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$
Detection rate (DR)	$DR = \frac{TP}{TP+FN}$
Precision	$Precision = \frac{TP}{TP+FP}$
FPR	$FPR = \frac{FP}{FP+TN}$
TNR	$TNR = \frac{TN}{FP+TN}$
FNR	$TNR = \frac{FN}{FN+TP}$
F1 score	$F_1 score = \frac{2TP}{2TP+FP+FN}$
AUC (Area Under Curve)	The area under the ROC (Receiver Operating Curve) of the binary classifier.
Recognition Rate	$Rec.Rate = 1 - 0.5\left(\frac{FP}{N} + \frac{FN}{P}\right)$
Bayesian Detection Rate	$BDR = \frac{P(I)\cdot DR}{P(I)\cdot DR+P(\neg I)\cdot FPR}$
Support	Applies to rule based systems. Defined as the number of data on which a rule applies to the total number of data.
Training time (s)	The time (s) required to train a NTL detection system.
Classification time (s)	The time (s) it takes for a NTL detection system to classify an instance.
Cost of undetected attack	Defined as the cost of the worst possible undetected attack.
Energy balance mismatch	Defined as the difference between the sum of consumer level active energy and substation level active energy
Average bill increase	Defined as the average bill increase if the NTLs where distributed among all consumers.
Normalized labor cost	Defined as the cost for inspecting all cases classified as NTL by the detection system.
Anomaly coverage index	Defined as the ratio between anomalous consumers under RTUs and the total number of anomalous consumers.
RTU cost	Defined as the total cost of acquiring RTUs
Minimum detected deviation	Defined as the minimum deviation (from a pre-specified typical profile) that can be detected.
Decrease in electricity stolen	The decrease of stolen electricity when a specific FDS is applied.

3.1. Raw data used in NTL-detection

Data are first organized according to the location of their physical source. Data concerning individual consumers (for example, active energy measurements) are classified as "Consumer Level" data, while data concerning an area (for example network topology) are classified as "Area Level" data. Data belonging to both categories can be further classified as time series and static data. Data can then be organized in more granular classes (Table 5).

Literature review reveals that there is a gap in the use of area level static data (especially those not related with the network topology). In fact, only one work [17] uses area level data for NTL detection. In addition, high resolution energy data and environmental data (temperature) are rarely used. Data oriented methods

Table 3
Overview of data oriented methods.

Ref.	Category	Concept	Algorithm	Data types	Data set size	Features	Metrics	Response time
[17]	Data oriented	Supervised	Generalized Additive Model	Consumer Non-technical, Area Non-technical, Area Technical	Large	–	Hit Rate	Year
[29]	Data oriented	Supervised	SVM	Low Resolution Energy, Consumer Non-technical	Large	Average	Accuracy, Hit Rate	Year
[30]	Data oriented	Supervised	SVM, Rule Induction	Low Resolution Energy, Consumer Non-Technical	Large	Average, max/min	Accuracy, Hit Rate	Year
[33]	Data oriented	Supervised	ANN, SVM	Low Resolution Energy	Medium	Average	Accuracy, Hit Rate	Year
[22]	Data oriented	Supervised	SVM, OPF, Decision Tree	Low Resolution Energy	Large	Average, predicted kWh, Fourier coefficients, Wavelet coefficients, Polynomial fit coefficients, Euclidean distance to mean customer, variance of the consumption curve, Slope of linear fit	Hit Rate, Precision, TNR, Fβ score	Year
[38]	Data oriented	Supervised	SVM, Decision Tree	Low Resolution Energy	Large	Readings carried from DSO to other readings, maximum allowable consumption, number of irregularities, days since inspection/update, payment delays	Hit Rate, Accuracy, Precision, F1 score	Year
[19]	Data oriented	Supervised	OPF	Medium Resolution Energy, Consumer Technical	Large	Max/min, Load factor	Accuracy, Training Time, Classification Time	Months
[20]	Data oriented	Supervised	OPF	Medium Resolution Energy, Consumer Technical	Large	Max/min, Load factor, Power factor	Accuracy, Recognition Rate	Months
[21]	Data oriented	Supervised	OPF, SVM, ANN, SOM, k-NN	Medium Resolution Energy, Consumer Technical	Large	Max/min, Load factor, Power factor	Accuracy, Recognition Rate	Months
[47]	Data oriented	Supervised	Rule Induction, Decision Trees	Low Resolution Energy, Consumer Technical, Consumer Non-Technical	Large	Max/min, power factor, variability, streaks, daily consumption to contracted power	Accuracy, Precision, Support	Year
[49]	Data oriented	Supervised	Rule Induction, Decision Trees, Bayesian Classifiers	Low Resolution Energy, Consumer Technical, Consumer Non-Technical	Large	Max/min, power factor, variability, streaks, daily consumption to contracted power, pearson coefficient, billed-consumed energy Coefficient	Accuracy, Hit Rate, Precision, Support	Months
[41]	Data oriented	Supervised	ANN	Low Resolution Energy, Consumer Technical, Consumer Non-Technical	Large	–	Accuracy, Hit Rate, Precision, FPR	Year
[23]	Data oriented	Supervised	OPF, k-nn, SOM, SVM, ANN	Medium Resolution Energy, Consumer Technical	Large	Max/min, power factor, load factor, PCA components	Accuracy, Training Time	Months
[24]	Data oriented	Supervised	SVM	Medium Resolution Energy, Consumer Technical	Large	Max/min, power factor, load factor	Accuracy	Months
[36]	Data oriented	Supervised	SVM, k-nn, clustering	Medium Resolution Energy	Large	Max/min, PCA components	Accuracy, Hit Rate, Precision	Days
[42]	Data oriented	Supervised	ANN	Medium Resolution Energy, Consumer Technical	Large	max/min, Load factor, Power factor	Accuracy, Training time	Months

Table 3 (*Continued*)

Ref.	Category	Concept	Algorithm	Data types	Data set size	Features	Metrics	Response time
[25]	Data oriented	Supervised	Bayesian Classifiers, k-nn, Decision Tree, ANN, SVM	Low Resolution Energy, Consumer Non-Technical, Consumer Technical, Environmental, Area Non-Technical	Large	Max/min, pearson coefficient, billed-consumed energy coefficient, Consumption decrease compared to previous period, number of readings	F1 score, AUC	Months
[46]	Data oriented	Supervised	OPF	Medium Resolution Energy	Large	Discrete Cosine Transform coefficinets	Hit Rate, Precision, F1 score	Year
[35]	Data oriented	Supervised	SVM, Rule Induction	Medium Resolution Energy	Large	Encoding	Accuracy	Days
[39]	Data oriented	Supervised	ANN	Medium Resolution Energy	Large	–	Accuracy, Training Time, Classification Time	Days
[43]	Data oriented	Supervised	ANN	Medium Resolution Energy	Large	–	Hit Rate, FPR, TPR, FNR	Hours
[44]	Data oriented	Supervised	ANN, Decision Tree	Medium Resolution Energy, Environmental	–	–	–	Days
[48]	Data oriented	Supervised	Rule Induction	Low Resolution Energy, Consumer Technical, Consumer Non-Technical	Large	–	–	Year
[40]	Data oriented	Supervised & Unsupervised	Rule Induction, Expert Systems, ANN	Low Resolution Energy, Consumer Technical, Consumer Non-Technical	Large	Average, max/min, standard deviation	–	Months
[37]	Data oriented	Supervised &Unsupervised	SVM, Expert System	Low Resolution Energy, Consumer Non-Technical	Large	Average, Consumtion curve slope	Accuracy, Hit Rate, FPR, TNR. FNR, AUC	Year
[50]	Data oriented	Supervised &Unsupervised	Bayesian Classifiers, Clustering	High Resolution Energy, Smart Meter Network Data	Small	–	Accuracy, Training Time, Classification Time, FPR, FNR	Days
[4]	Data oriented	Unsupervised	Clustering	Low Resolution Energy, Consumer Non-Technical, Average Area Consumption	Large	Average, max/min, standard deviation	Hit Rate, Precision	Months
[58]	Data oriented	Unsupervised	Regression Models	Medium Resolution Energy	Medium	Average, standard deviation, predicted kWh	Electricity stolen	Hours
[52]	Data oriented	Unsupervised	Clustering	Low Resolution Energy, Consumer Non-Technical, Average Area Consumption	Small	Average, max/min, standard deviation	–	Months
[45]	Data oriented	Unsupervised	OPF, clustering, Multivariate Gaussian Distribution	Medium Resolution Energy, Consumer Technical	Large	Max/min, power factor, load factor	Accuracy, Recognition Rate, F1 score	Months
[53]	Data oriented	Unsupervised	Clustering	Medium Resolution Energy	Large	PCA components	FPR, FNR	Weeks
[54]	Data oriented	Unsupervised	Expert System	Medium Resolution Energy	Small	Fractional order dynamic errors	–	Hours
[60]	Data oriented	Unsupervised	Non-cooperative game (NCG) with FOSE system	Medium Resolution Energy	Small	Fractional order dynamic errors	–	Hours
[61]	Data oriented	Unsupervised	Cooperative game (NCG) with FOSE system	Medium Resolution Energy	Small	Fractional order dynamic errors	–	Hours
[55]	Data oriented	Unsupervised	Statistical Control	Low Resolution Energy	Medium	–	Hit Rate, FNR	Months
[57]	Data oriented	Unsupervised	Statistical Control	Medium Resolution Energy	Medium	–	Hit Rate, Energy Balance Mismatch, average bill increase, normalized labor cost	Days
[51]	Data oriented	Unsupervised	SOM	Medium Resolution Energy	Medium	–	Hit Rate, FPR, TPR, FNR	Weeks
[59]	Data oriented	Unsupervised	Kullback–Leibler divergence	Medium Resolution Energy	Medium	–	Hit Rate, electricity stolen	Weeks
[56]	Data oriented	Unsupervised	Statistical Control, Regression Models, Local Outlier Factor	Medium Resolution Energy	Medium	–	FPR, cost of undetected attack	Hours

Table 4
Overview of network oriented and hybrid methods.

Ref.	Category	Concept	Algorithm	Data types	Data set size	Features	Metrics	Response Time
[5]	Network oriented	Load Flow	Distribution grid power flow	Medium Resolution Energy, Smart Meter Network, Observer Meter Data, Network Topology	Medium	–	–	Hours
[63]	Network oriented	Load Flow	Paramter identification for technical loss estimation	Medium Resolution Energy, Smart Meter Network Data, Observer Meter Data	Small	–	Hit Rate	Hours
[62]	Network oriented	Load Flow	Stochastic Petri Nets & Singular Value Decomposition	Medium Resolution Energy, Smart Meter Network Data, Observer Meter Data, FRTU data, average area consumption	Small	–	Minimum detected deviation from typical	Hours
[64]	Network oriented	Load Flow	Distributed solution of linear systems	Medium Resolution Energy,Observer Meter Data,Network Topology	Medium	–	–	Hours
[65]	Network oriented	Load Flow	distribution grid probabilistic power flow	Low Resolution Energy, Smart Meter Network Data, Observer Meter Data, Network Topology	Large	–	–	Days
[66]	Network oriented	Load Flow	Voltage sensitivities identification with linear least squares	High Resolution Energy, Smart Meter Network, Observer Meter Data, Network Topology	Small	–	–	Hours
[67]	Network oriented	Load Flow	Recursive Least Squares for meter behavior modelling	Medium Resolution Energy, Observer Meter Data, Network Topology	Small	–	Hit Rate, Classification Time	Hours
[73]	Network oriented	Sensor Network	Conditional Random Field & Cross Entropy	High Resolution Energy, Network Topology	Small	–	anomaly coverage index, FRTU cost	Days
[74]	Network oriented	Sensor Network	Dynamic Programming	Smart Meter Network Data, Network Topology	Medium	–	anomaly coverage index, FRTU cost	Days
[75]	Network oriented	Sensor Network	Integer Linear Programming	FRTU data, average area consumption, Network Topology	–	–	FRTU cost	Days
[76]	Network oriented	Sensor Network	Tree search algorithms	Medium Resolution Energy, Observer Meter Data, Network Topology	Medium	–	Hit Rate, Classification Time	Hours
[68]	Network oriented	State Estimation	Distributed solution of Kalman filter	Smart Meter Network Data, Observer Meter Data Data, Network Topology	Medium	–	Accuracy	Minutes
[69]	Network oriented	State Estimation	MV (LV) WLS state estimator	Medium Resolution Energy,Observer Meter Data, FRTU data, Network Topology	Small	–	–	Minutes
[70]	Network oriented	State Estimation	MV and LV state estimation	High Resolution Energy, Smart Meter Network, FRTU data, Network Topology	Small	–	–	Minutes
[71]	Network oriented	State Estimation	MV WLS state estimation and bad data detection	Medium Resolution Energy, FRTU data, Network Topology	Small	–	–	Minutes

Table 4 (*Continued*)

Ref.	Category	Concept	Algorithm	Data types	Data set size	Features	Metrics	Response Time
[72]	Network oriented	State Estimation	network clustering and bad data detection	FRTU data, Network Topology		–	–	Hours
[6]	Network oriented	State Estimation & Sensor Network	DC state estimator, grid placed sensor algorithm	Smart Meter Network Data, Network Topology	Medium	–	Hit Rate	Hours
[79]	Hybrid	State Estimation & Unsupervised	MV state estimator and ANOVA	Medium Resolution Energy, FRTU data, average area consumption, Network Topology	Small	–	–	Hours
[80]	Hybrid	State Estimation & Unsupervised	WLS state estimator (semi-definite programming) and ANOVA	High Resolution Energy, Smart Meter Network Data, FRTU data, Network Topology	Small	–	–	Minutes
[31]	Hybrid	Supervised & Load Flow	SVM with observer meter	Medium Resolution Energy, Observer Meter Data, Network Topology	Large	–	Hit Rate, FPR, DR-FPR, Bayesian Detection Rate	Days
[32]	Hybrid	Supervised & Load Flow	SVM, Decision Tree with observer meter	Medium Resolution Energy, Consumer Technical, Consumer Non-Technical, Observer Meter Data, environmental, Network Topology	Medium	Predicted kWh	Accuracy, Hit Rate, FPR, Classification Time	Months
[82]	Hybrid	Supervised & State Estimation	OPF and MV state estimation	Low Resolution Energy, FRTU data, Network Topology	Large	–	Precision, Hit Rate	Months
[77]	Hybrid	Supervised and Load Flow	Rough set theory with technical loss estimation	Low Resolution Energy,Consumer Technical, Consumer Non-Technical, obeserver meter, Network Topology	Large	Average, season consumption rates	–	Months
[78]	Hybrid	Unsupervised & Load Flow	Statistical control with observer meter	Low Resolution Energy, Network Topology	Large	–	–	Months
[81]	Hybrid	Unsupervised & State Estimation	Multivariate Gaussian Distribution and MV WLS state estimator	Low Resolution Energy, FRTU data, Network Topology	Large	–	Accuracy. Hit Rate	Months
[83]	Hybrid	Unsupervised and Load Flow	Statistical control and A-star (A*) derivative algorithm	Smart Meter Network Data, FRTU data, average area consumption, Network Topology	Medium	–	Hit Rate	Minutes
[34]	Hybrid	Unsupervised, Supervised & Sesnor Network	Clustering, SVM with network clustering	Medium Resolution Energy, Observer Meter Data, FRTU data, average area consumption, Network Topology	Medium	Average, mismatch ratio	FPR, FNR	Days

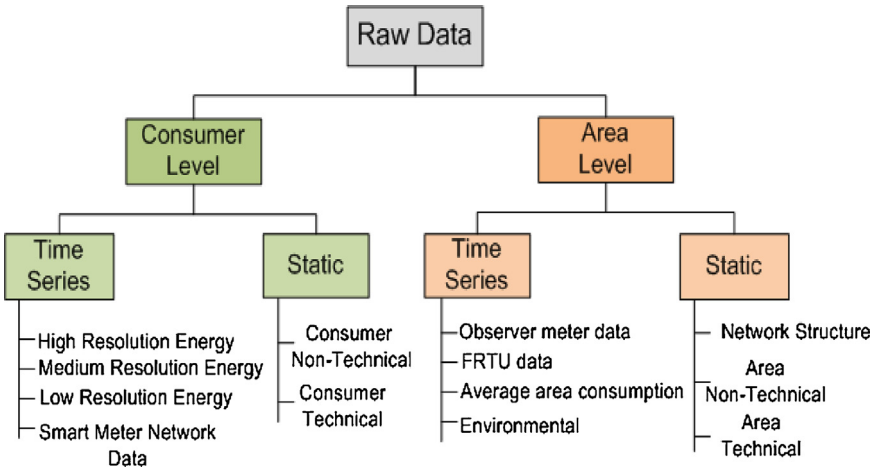

Fig. 2. Data type categorization for NTL detection applications.

Table 5
Data used for NTL detection.

Consumer Level	Time Series	High resolution energy	active/reactive energy measurements with a time resolution lower than or equal to 10 min
		Medium resolution energy	active/reactive energy measurements with a time resolution between 15 min and 1 h
		Low resolution energy	active/reactive energy measurements with a time resolution of one month or more
		Smart meter network data	non-energy smart meter data (voltage, current, line resistance, alarms)
	Static	Consumer technical	data providing technical characteristics of the consumer infrastructure (demand contracted (kW), installed power(kW), power transformer (kVA), voltage level, number of phases, use of remote system for space heating, number of appliances, etc.)
		Consumer non-technical	data describing consumer behavior, e.g inspection remarks, geographical area, economic activity etc.
Area Level	Time Series	Observer meter data	voltage, current and power measurements of a meter installed on the LV side of the secondary distribution network transformer to provide total feeder measurements
		Remote technical unit (RTU) data	current, voltage and power from RTUs installed in LV or MV network
		Average area consumption	average consumption of monitored area
		Environmental	usually temperature, but may include other factors too
	Static	Network structure	MV or LV network topology (might include line type and length). Network structure related data, for example the transformer to which a consumer is connected or the percentage of technical losses
		Area technical	data that characterize an area from a technical point of view (percentage of irregular consumer per transformer, percentage of irregular consumers in the area, number of transformers in the area, etc.)
		Area non-technical	data that characterize an area from a social/economic point of view (average number of residents, average income, percentage of rented residences, percentage of residences with water, percentage of residences with garbage collection, percentage of residences with pavements, percentage of literates, campaign actions against frauds in the area, etc.)

almost exclusively use consumer level time series and static data. In fact, all methods use time series energy consumption data and about half of them include static data. Network oriented methods make use of high or medium resolution energy consumption data, as well as voltage and current measurements. In addition, they strongly rely on measurements from other devices (observer meters or RTUs) and knowledge of MV or even LV network topology. As expected, hybrid methods use all data types.

3.2. Features used in NTL-detection

It is common for data oriented (and sometimes hybrid) NTL detection methods to use not only the raw data described above, but also features extracted from that data. Features commonly used are listed here. It must be noted that these features are almost always calculated from consumer level time series data and more specifically from active energy consumption curves. The time resolution of these features is thus highly dependent on the time resolution of the raw data. It is thus difficult to exactly define all features used in each work. Instead, the authors choose to define families of features thus presenting a more generalized view of the domain. A list of feature families most commonly used in literature is provided in Table 1.

The use of features instead of the time series itself is common in data mining (classification/clustering) tasks. Classification metrics may be improved, while making it possible to reduce a data set's size and provide a level of anonymization. Initially, a large number of features can be extracted from a time series (take Table 1 for example), however features representative of NTL detection only should be considered. In addition, the time period for which a feature is calculated must be carefully chosen, e.g. a daily average of 15 min active energy data for some years carries different information from a seasonal (3 months) average.

Given a list of features and the NTL detection method, feature selection algorithms can be used for defining an optimal set of features. A large number of feature selection algorithms are available in machine learning literature [18]. There are cases though were feature selection has been studied for optimizing the performance of classifiers used in NTL detection. Such techniques have been used in Refs. [19–24]. In Ref. [19] the small number of features permits testing all possible combinations. Authors in Ref. [20] use a number of different heuristic methods, focusing on binary black hole optimization and comparing it with Harmony Search (HS), Particle

Swarm Optimization (PSO), Differential Evolution (DE) and Genetic Algorithm (GA). In Ref. [23] the use of Harmony Search is evaluated and compared to PSO. The same authors [21] evaluate the Binary Gravitational Search Algorithm (BGSA) and compare it with PSO and HS. Social Spider Optimization is utilized in Ref. [24] both for feature selection and parameter tuning. In Ref. [22] the authors propose filter and wrapper methods for feature selection without further specifying the type of algorithms used.

4. Non-technical loss detection performance metrics

A well defined and updated list of performance metrics is important, primarily for comparing NTL detection methods. A list of metrics most commonly used in literature is provided in Table 2. Most of them require the calculation of the traditional confusion matrix, where TP are true positives, TN are true negatives, FP are false positives and FN are false negatives. P represents all positive samples (P = TP + FN), while N represents all negative samples (N = TN + FP). $P(I)$ is the probability of NTL occurrence.

The first seven (accuracy, detection rate, precision, false positive rate (FPR), true negative rate (TNR), false negative rate (FNR), F_1 score) metrics are frequently used in classification tasks and calculated from the confusion matrix. In NTL detection literature the most common metrics are the accuracy and detection rate, which appear in almost every case of data oriented methods. Increased accuracy indicates that the system generally works well, classifying correctly both positive and negative samples. It is not enough though, when dealing with an imbalanced data set (typical in NTL detection), where one class (negatives) is excessively larger than the other (positives).

The second most commonly used metric is the detection rate (DR), also known in literature as recall, true positive rate, success in detecting NTL or hit rate. This metric expresses the proportion of samples classified as NTL to the total number of NTLs in the data set. Typically, large values of DR indicate a well operating detection system, but for this to be true other metrics must be taken into account. In general, both DR and accuracy must be considered to assess the system's performance.

The next two most commonly used metrics are precision and false positive rate (FPR). Precision, also known as positive predictive value — PPV, assertiveness or confidence, is calculated as the number of NTLs detected divided by the total number of NTL alarms. Increased precision means that most of the samples classified as positives (NTL) will be actual positives. It must be noted here that precision and recall are antagonizing metrics, i.e. increase of the one will decrease the other, thus the right balance between the two metrics must be sought for. This balance is expressed by calculating the F_1 score (a particular case of F-measure or Fβ score were $\beta = 1$) which is the harmonic mean of detection rate and recall. Increased F_1 score values indicate that the system detects many frauds with low false alarms. Although rarely used in NTL detection literature (examples include Refs. [22,25,26]), this is one of the most important and indicative metrics, especially when dealing with class unbalanced problems (like NTL detection and generally detection of frauds). In fact, a lot of work has been published on this problem, proposing a number of solutions and performance metrics for reliable evaluation of classifiers [27].

FPR is calculated as the number of samples falsely classified as positives (false alarms) to the total number of negatives. This is one of the most important metrics, since false positives lead to large operational costs to organizations responsible for NTL detection due to unnecessary meter inspections. Typically, low values of FPR must be sought for, although the threshold value depends on the relative size of the two classes. Assuming a data set of 1000 consumers of which 10 commit fraud an FPR as low as 10% would mean that 99 consumers without NTLs are classified as positives (NTL), leading to 99 unnecessary meter inspections in order to detect 10 cases of fraud. FPR = 1% means that 10 false alarms would occur in detecting the 10 real cases of fraud.

The choice of metrics is important especially when dealing with class imbalanced problems, like NTL detection. Combinations of metrics must be used in this case including accuracy, DR, FPR and TNR. Another metric, not frequently used in NTL detection literature, is the Bayesian Detection Rate (BDR) [28]. It mostly applies to data oriented NTL detectors and is dependent on the probability of fraud $P(I)$, DR and FPR while it expresses the probability of a false alarm in real life conditions. DR and FPR are characteristics of the classifier used, while the probability of fraud is an external parameter. In the fraud and intrusion detection domains this parameter usually obtains small values, since fraud is typically not frequent. Given the small value (for example 1%) of $P(I)$, in order to achieve a high value for BDR (i.e. minimize false alarms) an extremely low value for FPR must be achieved, even if DR is high.

5. Algorithms used in non-technical loss detection systems

Each fraud detection system is unique, since it uses different data in different ways. Some systems present a simple structure (for example a single Support Vector Machine (SVM) for classifying consumers), while others are more complex (including for example prior data cleaning and clustering phases, classifier ensembles, power system analysis etc.). Each technique can be characterized from a small number of algorithms which form the core of the fraud detection method. Most of them are already well established and defined in other research papers and thus no detailed descriptions will be provided. NTL detection methods are categorized as Data Oriented, Network Oriented or Hybrids, as presented in Chapter 2.

5.1. Data oriented methods

Data oriented methods are solely based on data analytics and machine learning techniques. These methods are organized in two main categories: supervised and unsupervised and are presented in the following chapters. Both supervised and unsupervised approaches though follow a common methodology presented in Fig. 3 and described next.

Data processing & model selection: given a set of raw data the model used for detecting NTL should be chosen. The availability (or not) of labeled data dictates the choice of supervised or unsupervised methods, while data quality/variety dictates the algorithm to be used. The choice of algorithm may exclude some parts of the raw data (data selection phase). The next phase includes data cleaning (typical in the knowledge discovery process) and feature extraction, if necessary.

Modeling: this process is different for supervised and unsupervised models. Unsupervised models do not use labeled data in the training phase, but only for evaluation. Supervised methods split the data set in the training set and the test set. After defining the training set (typically with cross-validation) feature selection is frequently used for training the model, while parameter optimization makes use of metrics that can be calculated due to label availability.

Application: new data (not belonging to the "Raw Data" set) are used for verifying model performance and operation. Classification results are further processed for producing a suspect list, i.e. a list that contains the probability of each consumer committing fraud. This phase can belong to a pilot operation of the NTL detection model or its simulation. Pilot operation on real life sites is of extreme importance in case feedback (by manual meter inspections) is available.

The development of supervised and unsupervised classifiers is based on well established Artificial Intelligence (AI) methods that

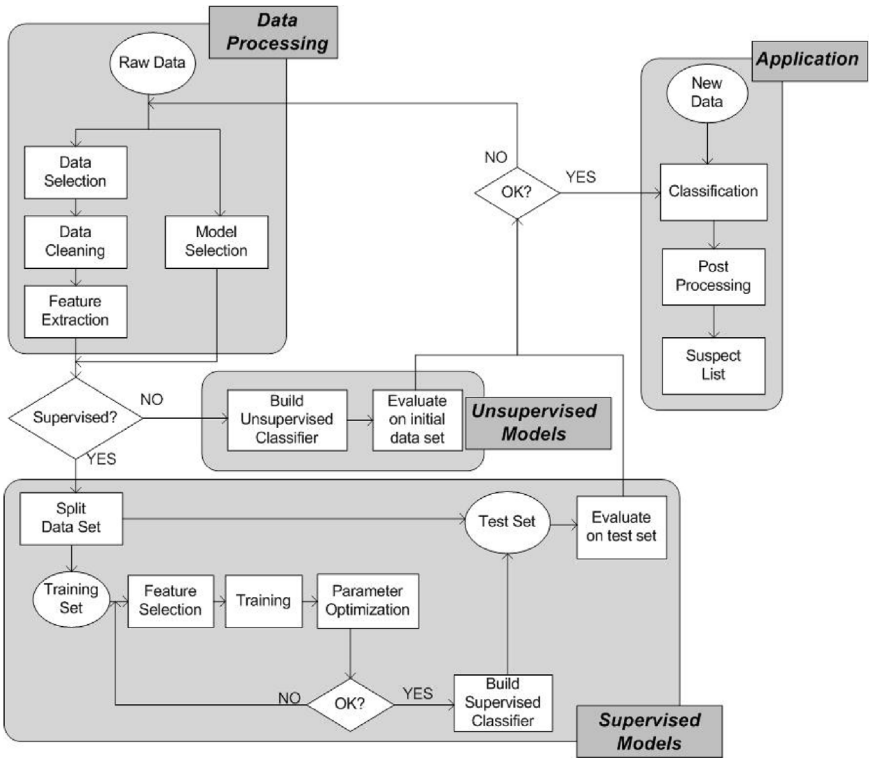

Fig. 3. Data oriented methods outline.

can be easily found in the literature. The following sections focus on their application to the NTL detection problem.

5.1.1. Supervised methods

5.1.1.1. Support Vector Machine (SVM) [21–26,29–38]. SVMs have been used as binary classifiers, since they are quite resilient to the class imbalance problem. A number of different implementations can be found including the One-Class SVM and the CS-SVM (cost sensitive SVM). The One-Class SVM may be considered as an anomaly detection method (unsupervised), since it is only trained on samples belonging to a single class (typically the negative, i.e. benign consumers). The CS-SVM provides the ability to assign different weights to different types of classification error. For example one can assign a high cost to misclassifications of the minority class which can lead to higher performance metrics (low FPR, high BDR). Relative literature implies that SVMs can be trusted for detecting NTL, although it can be quite difficult and time consuming to tune them. The Radial Basis Function (RBF) kernel SVM (SVM-RBF) is frequently used, although the linear kernel (Linear-SVM) has also been demonstrated. In the case of SVM-RBF, the cost (C) and gamma (γ) parameters need to be tuned (in Linear-SVM only the cost must be tuned). This is usually done by the grid search algorithm (with cross-validation). Tuning the SVM increases the time for constructing the model in cases of large data sets, thus making it a bad solution for online applications. Finally, SVMs may be combined with other classifiers (for example fuzzy inference system-FIS, Decision Trees, Neural Networks) for enhancing classifications results and they are a common baseline solution for comparing classification and feature selection techniques.

5.1.1.2. Artificial Neural Network (ANN) [21,33,39–44]. The most traditional version of ANN, the Multi-Layer Perceptron (MLP) trained with backpropagation (BP-MLP) has been used as a binary classifier for detecting NTL. In addition, ANN has also been used for electricity consumption time series forecasting. The deviation between predicted value and measured value is used for detecting frauds. The choice of deviation threshold and the possibility that fraudulent data influence the ANN output must be taken into account. In both cases (binary classification or forecast) the structure of the network must be chosen before training. Although a lot of literature exists on choosing the optimal network structure, most methods adopt a trial and error approach to find the number of hidden layers and respective number of neurons. In this case cross-validation must be used in order to assure that the model generalizes well. Apart from the BP-MLP, another type of neural network, the Extreme Learning Machine (ELM) has been proposed (binary classification or forecast). ELMs have a single hidden layer and weights connecting the input layer with the hidden layer are assigned randomly, while weights between the hidden layer and the output are calculated in a single step. ELMs can thus be trained faster without performance deterioration. The online version of ELM (OS-ELM, online sequential extreme learning machine) has been proposed for applications where the model needs to be retrained online due to possible changes in consumer characteristics (that may not be reflected to the current training set). Online or not, the only parameter that needs tuning is the number of hidden layer neurons.

5.1.1.3. Optimum Path Forrest (OPF) [19–23,45,46]. OPF is a graph based algorithm that may be used for clustering and classification applications. In contrast to previous algorithms, OPF does not try to find the optimal hyperplane that separates two classes, but each labeled sample of the training set is considered as a graph node with coordinates being the feature values. The objective is to partition the graph in two or more trees (optimum path trees), each representing a class. Each tree is rooted to a prototype and the collection of trees forms the OPF classifier. A new sample inherits the label of the optimum path tree that conquers it (according to a cost function). OPF can handle overlapping classes and has low training time, which allows for online training of the fraud detection sys-

tem. Such a characteristic is important in case the testing samples substantially differ from the training samples used (for example when a new class of consumers is introduced).

5.1.1.4. Rule induction [30,35,40,47–49]. A set of IF-THEN-ELSE rules can be used to distinguish malicious users. The simplest way to define such rules is by using expert knowledge (unsupervised) and statistical analysis. In many cases such expertise is absent or insufficient, however rule induction techniques can be used to extract rules hidden in data (usually labeled). The goal is to predict the class of a sample given the values of other related attributes (features). Although various works use rule based systems (expert systems) for detecting NTL the rule induction process is not transparent. In some cases, in order to better emulate the reasoning process of the expert, fuzzy rules (fuzzy inference system) have been used. Rule based systems are usually combined with other classifiers (SVM, Decision Tree, Bayesian Networks etc.) thus forming an improved FDS which utilizes human expert knowledge.

5.1.1.5. Decision trees (DT) [22,25,38,44,47,49]. Decision trees have been rarely used for NTL detection. DT is a classifier, whose output is a set of rules used to classify new samples. These rules may help an individual to better understand the characteristics of NTL. DT rules have also been combined with rules defined by experts and other classifiers forming ensembles. DTs are sensitive to the class imbalance problem and highly dependent to the training set. Various DT types have been used in NTL detection, namely the C4.5, CART and QUEST. Apart from the ability of DTs to extract simple and comprehensible rules, another advantage is their ability to handle categorical variables, which is often the case with consumer data such as the consumer type (residential, industrial etc.) or contract information etc.

5.1.1.6. Nearest neighbor (k-NN) [21,23,36]. Nearest neighbors is probably the simplest supervised classification algorithm for detecting NTL and has mainly been used as a baseline for comparisons with other algorithms. A new sample is placed on the feature space and assigned to the class most common among its k nearest neighbors (majority vote). The only parameter that requires tuning is the number of neighbors voting (k), but the way distance between samples is measured affects algorithm performance.

5.1.1.7. Bayesian classifiers [49,50]. The Naïve Bayes Classifier is a probabilistic classifier based on the assumption of strong independence between features. The algorithm requires prior knowledge of NTL probability which may be obtained by national statistics, if available. Using non-intrusive load monitoring (NILM) the system learns the probability of each appliance being used per consumer [50]. When a new sample arrives NILM is again performed and the probability of theft is calculated. Such systems require a lot of a priori knowledge (probability of theft and conditional probabilities) which may strongly influence the classifier's output.

Another type of Bayesian classifier is the Bayesian network [49], which represents the joint probability (Bayesian probability) of a set of variables in a graphical way. One of the most important advantages of Bayesian networks is that they can be easily interpreted by humans. This allows the user to understand which features of a time series are most influenced by NTL. Given a fully labeled data set and Bayesian network structure the objective is to learn the conditional probabilities. The class of a new sample may then be inferred together with the probability of the sample belonging to the predicted class. This allows to choose the number of meters to be inspected, since a probability threshold may be set according to the FDS user's needs and business characteristics, e.g. a high threshold is chosen if it is not possible to perform a large number of inspections.

5.1.1.8. Generalized Additive Model (GAM) [17]. The spatial distribution of NTL has been modeled with GAM. This method is inspired from the field of epidemiology and assumes that NTL spreads over an area according to various social and technical (network related) characteristics. Given a set of consumers with and without NTL together with the social and technical characteristics of their area, GAM can be used to estimate the probability of NTL per area and the influence of each social or technical parameter. Next, a Markov chain is used to model how NTL may spread over a specific area in the future. Although this algorithm does not detect fraud, but rather computes the spatial distribution of the probability of fraud, it can be helpful when designing long term policies (including hardware installation, legislation change, campaigns etc.) for reducing frauds.

5.1.2. Unsupervised methods

5.1.2.1. Self Organizing Map (SOM) [19,21,23,51]. SOM can be considered as a special type of Neural Network frequently used as a clustering or unsupervised classification tool. It typically produces a 2D representation of the data set and therefore acts as a method for dimensionality reduction. Another advantage of SOM is that it produces a visual representation of the data that may be comprehended by humans. The final output is a set of clusters (for example NTL/no-NTL) that need to be evaluated by experts or fed to a secondary level of logic in order to decide on the set of meters to be inspected. The number of clusters might be more than 2, if atypical behaviors are taken into account that may form clusters but are not frauds. The unsupervised nature of SOM leads to reduced classification accuracy and this is probably the reason why it rarely appears in NTL detection literature.

5.1.2.2. Clustering algorithms [4,36,45,50,52,53]. Clustering has been used in many FDS works, mainly at the data preprocessing level. It is used to group similar consumers extracting atypical, but non malicious behaviors or different types of consumers, and then train classifiers on these groups. This step enhances the classification process and reduces false positives. Clustering is also used to calculate baseline power profiles or prototypes. If a new sample significantly differs from these profiles, fraud may be suspected.

Clustering can be also used as an unsupervised classification tool with the distance of a new sample to the center of its cluster considered as an indicator of fraud. Fuzzy clustering (fuzzy c-means) has been also used [4] by associating each new sample with a probability of theft, rather than a label. This allows the FDS developer to tune the system according to business models and other external parameters (choosing the most probable cases of fraud).

Finally, the Density Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm has been proposed. It is used after applying Principal Component Analysis (PCA) on the electricity consumption data and representing each consumer with the first two components in a two dimensional space. This representation enables the DBSCAN to separate malicious from anomalous consumers in an efficient manner and provides visualization capabilities [53].

5.1.2.3. Expert systems [37,40,54]. These are systems based on rules defined by experts, e.g. technical personnel responsible for tracking NTL. Although such systems do not require learning, they are considered unsupervised (fuzzy rules are also included, usually after fuzzification of simple rules). Rules may be defined by various means, but most of the times an accurate model of how NTL is expressed or inspector knowledge is required. For example, one can easily derive a rule stating that in cases of negative consumption mean shifts larger than 50% a meter must be inspected. A rule

stating that, if reactive power is larger than active power the meter must be inspected, is proposed as an example in Ref. [40]. Such rules may be extremely simple and still achieve good classification results. In addition, there are cases of rules (such as the case of consumption mean shift were the 50% limit is arbitrarily set) that can be tuned in order to improve specific aspects (metrics) of the NTL detector.

5.1.2.4. Statistical control [55–57]. Statistical process control has been also proposed for detecting NTL. Control charts, typical for time series data, are used for monitoring an individual consumption and for defining regions, where the time series may be considered anomalous. The XMR (moving range) [55] control chart identifies time series variability that may occur due to theft by defining control limits (upper control limit, lower control limit and other intermediate limits dependent on the standard deviation). The XMR control chart monitors both the actual consumption values (X chart) and their moving range (MR charts). Rules are formed in order to indicate which violations are frauds and require inspection.

Other charts include the Exponentially-weighted Moving Average (EWMA) control chart and the nonparametric cumulative sum (CUSUM) control chart [56]. These charts are well established in industry for quick detection, they operate online and provide the possibility for visual inspection of data. Quick detection may cause a lot of false positives however, thus reducing the system's performance. Another statistical data analysis tool proposed for NTL detection is Bollinger bands [57], widely used in stock trading. Again, upper and lower bands are computed as a function of the N-period standard deviation and a N-period moving average of the time series is monitored. In case energy usage at a specific time slot exceeds the limit of that time slot fraud is suspected. The main drawback of the aforementioned methods is that, since their main purpose is to detect change, they fail to detect fraud, if it takes place from the beginning of the monitoring period. In addition, such methods may interpret other types of consumption change as fraud, producing false positives.

5.1.2.5. Regression Models [56,58]. Regression Models like the Auto-Regressive Moving Average (ARMA) and Auto-Regressive Integrated Moving Average (ARIMA) have been used for forecasting a time series. Their use for NTL detection is based on the comparison between measured and forecasted values, assuming that the forecasting model has been trained with non-malicious data. The largest the difference, the highest the probability of fraud. Both ARMA and ARIMA are well established models for time series forecast, however ARIMA models have been shown to outperform ARMA for domestic consumers.

5.1.2.6. Outlier detection [45,56,59]. Various concepts borrowed from outlier detection may also be used for detecting NTLs. The Multivariate Gaussian Distribution (MGD) is used in Ref. [45]. Assuming a data set free of frauds, each cluster of samples is modeled as a Gaussian distribution. Given a new sample, the probability of the sample belonging to each of the distributions is calculated. The highest of these probabilities is compared to a threshold value in order to decide if the sample is an anomaly or not. The main challenge in this case is deciding on the number of clusters and effectively the parameters of the Gaussian distributions. K-means and E-M are typically used although OPF has also been proposed. The Local Outlier Factor (LOF) is used in Ref. [56]. LOF is a density based indicator for fraud. It is used to calculate the local density of a sample and compare it to the average local density of the sample's k nearest neighbors. Samples with local density substantially lower than their neighbors may be considered anomalies. This method does not require a clean data set, but high LOF does not necessarily mean fraud. Thus, apart from choosing a threshold for LOF, additional rules must be set before labeling a sample as fraud, e.g. high LOF and low consumption. Finally, the Kullback–Leibler divergence (KLD) is used in Ref. [59]. KLD is a measure of distance between two probability distributions and can be used for comparing the distribution of a set of measurements with a baseline, obtained from the historic distribution. It is proposed for detecting a smart attack (given different pricing schemes) that disguises malicious use as benign by fitting it to a legitimate ARIMA model. A main advantage is that it may still detect frauds even if they are already included in the training set.

5.1.2.7. Game theoretic approaches [60,61]. Games theory has been used to model the attacker (malicious user) and defender (FDS system) behavior [8]. Its use as a core part of a FDS is not yet mature though. Attempts include decision making mechanisms modeling fraud as a cooperative or non-cooperative game.

5.1.3. Qualitative comparison

Most data oriented fraud detection systems utilize supervised learning methods due to their superior performance. Training a supervised classifier however requires labeled data from malicious and benign users, that are not always available or are not representative of all the population the FDS is aiming at. Finally, even if labeled data exist, it is most probable that class imbalance problems will arise. Unsupervised methods do not require labels (only partially, in case of anomaly detection methods), thus they can be applied easier with lower performance, characterized by a higher FPR. Unsupervised methods are also used in case a large number of negative (benign) samples are available, while positive samples (fraud) are scarce or not available. In fact, some anomaly detection methods (outlier detection) make no assumption of class labels for training the classifier. Another advantage of unsupervised methods is their resilience to zero day attacks. Supervised methods are trained to detect specific types of fraud. In case a new fraud behavior appears (one that is missing from the training set) the supervised classifier will probably fail to detect it. In contrast, unsupervised methods are independent at least from the positive class training set.

5.2. Network oriented methods

Network oriented methods leverage data obtained from distribution grid sensors (next to smart meters) and take advantage of the physical rules that govern the underlying electrical network, in order to detect frauds. Apart from sensor data, they make use of network related data, like network topology and consumer transformer/phase connectivity. A number of researchers use power flow tools in order to assess the size of NTL and identify its source by checking the energy balance with an observer meter, if available. Furthermore, several approaches use distribution state estimation and bad data detection. These approaches tend to be more accurate, although not always possible to implement. The use of dedicated sensors for detecting frauds is also proposed. Sensor placement algorithms are reported, in order to calculate the minimum number of sensors and their position in the grid ensuring fraud detection.

5.2.1. Load flow approach [5,62–67]

An obvious way to detect NTL is by checking the energy balance of a network or part of network. The installation of a meter monitoring the LV side of a distribution transformer (also called an observer meter) is required in this case. The sum of consumer smart meter measurements is compared to the observer meter measurement. Given a percentage for technical losses (using either a typical value according to network characteristics or leveraging advanced technical loss calculation methodologies) the mismatch between

energy input and energy output is calculated. The larger this mismatch, the higher the probability of NTL. With this approach, NTL can be detected up to secondary substation level, however individual suspects cannot be identified and an observer meter is required, which is not always the case. Furthermore, a fairly accurate estimation of technical losses per network is required which can be difficult. This concept is central in Refs. [64] and [67]. In fact, in Ref. [64] privacy issues are also taken into account by solving the problem in a distributed fashion. In Ref. [67] the authors model the meter behaviour (for example by a linear model) and model parameters are calculated via various methods (for example WLS). Model parameters are then compared to those of a "normal" meter. Differences indicate fraud while the detection of various types of fraud on the same meter at the same time is also possible. Finally, for cases where technical losses or network structure are unknown, authors in Refs. [62] and [63] propose a methodology for identifying network parameters and then calculating technical losses which leads to better calculation of NTL.

Authors in Ref. [65] use a probabilistic power flow approach for detecting non-technical losses. One or more observer meters are required and fraud is detected at network level, i.e. it is possible to know if there is fraud under a specific observer meter. Energy balance is again used, this time in a probabilistic manner. Calculating the probability distributions for total and technical losses and subtracting them by convolution gives the probability of NTL occurrence in a specific sub-network.

In Ref. [5] the authors propose a smart substation concept, where both smart meters and observer meters are available. Given the network topology, the first step is to check the energy balance between observer and smart metering data. If a significant mismatch occurs, the FDS moves on to localize NTL at consumer level. The FDS uses the measured currents from smart meters to calculate respective voltages that are compared to measured voltages. A similar concept has been developed in Ref. [66] by using smart metering data (without theft) to identify network voltage sensitivities. These sensitivities are used as a network model for estimating voltages given active power measurements.

5.2.2. State estimation approach [6,68–72]

Distribution state estimation (DSE) using smart metering data, is used to make the grid observable and therefore appears as a great tool for fraud detection. Distribution state estimation however has been mainly used for MV networks, thus NTLs can be detected on substation level only (detection of MV/LV transformer serving malicious users). Nevertheless, NTL may be expressed as bad data or as false data injection (FDI) attacks, terms more relevant to state estimation theory. The main difference between the two is that bad data typically occur in an isolated and random manner, while FDIs may include several interacting bad data and are more difficult to detect. Launching FDI attacks successfully however, implies tricking a traditional state estimation bad data detector. This would require at least partial knowledge of grid parameters by the attacker, which is not the typical case when dealing with NTLs.

In Ref. [68] the centralized solution of the Kalman filter state estimator is initially proposed to find line currents and biases. Users with biases larger than a predefined threshold are assumed to commit fraud. Next, privacy is ensured by proposing a distributed solution of the Kalman filter, where the operator does not need access to power and voltage measurements of users. Although the proposed method presents promising results, it should be noted that it is applied for microgrids with small line lengths.

In Ref. [6] the malicious user is assumed to have at least partial knowledge of the network structure and the capability to increase/decrease the measurements of a number of smart meters at the same time. Such attacks will go undetected by traditional energy balance methods. The authors propose methods for detecting this type of attacks including sensor placement, meter and communication network inspections.

In Refs. [69–71] the authors propose a WLS state estimator to estimate the loading of MV/LV transformers from three phase voltage, current, active and reactive power measurements. In case of significant difference between measured and estimated values NTL may be assumed. Finally, authors in Ref. [72] propose a network clustering and division approach before state estimation for bad data detection is applied. The process of network partition and bad data detection for each of the networks is repeated until bad data are localized on bus level.

5.2.3. Sensor network approach [6,73–76]

Another trend in network oriented NTL detection methods is the installation of dedicated sensors in the distribution grid. The objective in this case is to find the optimal number and position of sensors (RTUs) in order to better detect and localize NTL, while minimizing infrastructure costs. This process typically requires accurate knowledge of the network topology and is strongly connected to state estimation theory, since almost all methods aim at increasing network observability. Apart from optimizing the place and number of RTUs there are works examining the placement of redundant smart meters [76]. In this case an observer meter as well as an inspector box (containing a number of inspector smart meters) are installed before consumer smart meters. The inspector meters exchange data with consumers' smart meters comparing consumption measurements. Differences between readings indicate possible fraud.

5.2.4. Qualitative comparison

Network oriented methods are based on power systems analysis and usually require the availability of network devices such as the observer meter. Power flow and energy balance methods are most popular, mainly due to their simplicity and applicability in distribution networks (especially LV). They have low data requirements, since next to smart metering data, they usually require observer meter data and sometimes network topologies. In contrast, state estimation methods present higher complexity, especially if applied to large low voltage (three phase, unbalanced) networks. In addition, they typically require more reliable and higher resolution data, including detailed network topologies and data coming from RTUs (especially if state estimation is performed at MV and LV level). On the other hand, state estimation methods perform better and can even detect "smarter" false data injection attacks. Both methods have been used for localizing fraud at substation level and consumer level, but state estimation seems to perform better than power flow/energy balance methods in consumer level localization. Optimal number of sensors and their placement for increasing network observability can be considered as part of NTL detection. After the devices are installed energy balance or state estimation methods may be implemented.

5.3. Hybrid methods

Hybrid methods adopt a combination of algorithms and techniques described above, in order to detect NTL with higher accuracy. Authors in Ref. [31] use observer meters together with SVMs. The SVM output is crosschecked with the observer meter used to evaluate active power balance of the relative network. The algorithm estimates the network technical losses and evaluates the active power balance mismatch. If the mismatch exceeds the predefined threshold and the SVM produces a positive output (or number of positive outputs since the system classifies daily consumption as fraud or not), the consumer is classified as malicious and must be further inspected. The same concept has been proposed in Ref. [32], this time using a combination of SVM and decision trees in

conjunction with balancing at distribution and transmission grid levels.

Authors in Ref. [34] incorporate RTUs to detect NTL. The distribution network is initially divided in sub-networks according to RTU availability and trustworthiness. The proposed framework specifies sub-networks with NTLs using measurements from RTUs and smart meters and running distribution network power flows to evaluate technical losses. If the mismatch ratio exceeds a specific threshold, meter tampering is suspected. A third level based on fuzzy c-means and SVM is applied to detect individual consumers committing frauds.

In Ref. [77] the estimation of the number of consumers committing frauds is based on network loss analysis. Rough sets are then used by calculating a suspect boundary region. The same team of researchers has also proposed the use of Asymmetric Control Limit (ACL) Tukey's control charts [78] where the upper and lower control limits are those ensuring balance between total measured energy (by means of an observer meter), invoiced energy (by metering consumption) and total losses (calculating or estimating technical losses).

A different approach is proposed in Ref. [79] using state estimation and ANOVA. Smart metering data (voltage and power), RTU data (voltage angle and magnitude of the HV/MV substation secondary) and network structure are required. A distribution state estimator is implemented using the aggregated smart meter consumption (per MV/LV transformer) as pseudo-measurement. In order to localize anomalous consumption at LV transformer level, the normalized residual test is used. The NTL detection problem is thus transformed to a bad data detection problem, where large gross errors indicate probable NTL. The authors then propose a second level for consumer level localization, using ANOVA and comparing the result with previously validated (i.e. without NTL) usage baselines. The results from ANOVA can be fed back to the state estimation module for replacing bad data with better estimates. The same idea has been developed in Ref. [80] describing a different solution for the state estimation problem though with semi definite programming.

In Ref. [81] the reverse procedure is proposed, where anomaly detection (unsupervised outlier detection based on a Gaussian distribution) is first applied for calculating the density of anomalies (i.e. how often and to what extent fraud takes place) per transformer. This density is then used to adjust the weight matrix of the state estimator which calculates transformer loading using load forecasts as pseudo-measurements. Technical and non-technical losses can be then estimated at transformer level. In Ref. [82] state estimation is proposed as a first step for evaluating the extent of NTL (as the difference between estimated load and forecasted/measured load) and combined with a supervised OPF classifier.

A hybrid method combining state estimation, multivariate control charts and the A* path search algorithm is proposed in Ref. [83]. Initially, state estimation is performed on MV level using data originating from field devices. The (per sample) difference between measured and estimated voltage/current for each field device is used for defining a multivariate process monitoring problem. If one of the aforementioned differences is outside a reliable region, NTL is suspected and the A* algorithm is launched to localize theft.

6. Conclusions

A large number of fraud detection methods and algorithms have been reported in recent literature. All these methods share characteristics that group them according to Chapter 2. Of course, other categorizations can be suggested and future work may impose new categories. Each method/algorithm has its own advantages and disadvantages and comparison of all proposed methods is impossible due to lack of testbed data sets and scenarios. Different sets of consumers, different network topologies and different types of fraud are studied in most works, while commonly applied performance metrics are lacking. A qualitative comparison can be provided on the basis of:

- Performance: performance can be measured by metrics presented in Chapter 4. A general conclusion is that network oriented methods usually perform better than data oriented and hybrid methods, mainly due to the utilization of a physical underlying model, i.e. the power system. Data oriented methods build models that fit existing data in a statistical way, making them sensitive to training sets and prone to false positives. This happens for example, when changes in a consumption profile due to changes in household residents or usage of electrical devices might make it look like a fraud, unless these models are retrained. Hybrid methods show an average performance depending on the use of the underlying model. Just adding an energy balance condition to a data oriented method though, can substantially improve performance
- Cost: performance comes with a cost. At this point we refer to costs related to purchasing, installing and maintaining any software and hardware equipment. The costs that may occur due to bad performance (large number of false positives that leads to increased manual inspection costs or lost income) are not considered. Network oriented FDSs generally cost more to implement, since they usually require observer meters or other RTUs that may have additional communication requirements. The software components of network oriented FDSs are more complex increasing development and operation/training costs. Data oriented methods use almost exclusively smart metering data (medium to low resolution), that are often available as part of Automatic Meter Reading (AMR) for billing purposes. Thus, a data oriented system can be easily built using existing infrastructure with small development costs. The cost of hybrid methods varies between the two methods according to the network oriented component. A cost benefit analysis can be performed in order to estimate the added value of new devices in detecting NTLs
- Resources (data volume/data variety): data oriented methods inherently require large volumes of data in order to ensure generalization and in many methods data must be labeled. In a smaller extent, this is also true for hybrid methods. Network oriented methods do not require large volumes of data, but high resolution and high quality data. In addition, they require a larger variety of data obtained from smart meters (power/voltage), observer meters and RTUs as well as network structure data. It may be concluded that both hybrid and network oriented methods need data of large variety, but not necessarily large volume, while data oriented methods consume large data sets of small variety
- Class imbalance: data oriented methods mostly rely on existing and validated cases of fraud either for training or validation, however since frauds are scarce, it is difficult to obtain these samples, unless another FDS (unsupervised/anomaly detection) or a manual inspection campaign are used. Even if sufficient fraud samples are obtained however, special techniques must be used to ensure that the classifier does not discriminate towards the majority class. Most of the reviewed hybrid methods face similar problems. Network oriented methods are immune to this problem, since they do not require training and fraud may be even simulated (without loss of generality) if positive samples are not available for testing
- Response time: network oriented methods achieve lower response times than most data oriented and hybrid methods. The first reason is that the verification of the underlying physical

model does not require a lot of data, meaning that the system does not need to wait for the accumulation of data before reaching a decision. The second is that a lot of devices used in network oriented methods provide high resolution and in some cases fast (even real time) data which speeds up the process. Data oriented methods on the other hand may rely on monthly or yearly consumer profiles which slows down the decision making process. Hybrid methods experience the bottleneck of the data oriented component.

References

[1] R. Czechowski, A.M. Kosek, The most frequent energy theft techniques and hazards in present power energy consumption, IEEE Proc. 2016 Jt. Work. Cyber-Physical Secur. Resil. Smart Grids, CPSR-SG 2016 -This Work. Is Part CPS Week 2016 (2016), http://dx.doi.org/10.1109/CPSRSG.2016.7684098.

[2] P. Antmann, Reducing technical and non-technical losses in the power sector, in: Background Paper for the WBG Energy Strategy, Tech. Rep., Washington, DC, USA: The World Bank, 2009, n.d.

[3] S.S.S.R. Depuru, L. Wang, V. Devabhaktuni, Electricity theft: overview, issues, prevention and a smart meter based approach to control theft, Energy Policy 39 (2011) 1007–1015, http://dx.doi.org/10.1016/j.enpol.2010.11.037.

[4] E.W.S. Dos Angelos, O.R. Saavedra, O.A.C. Cortés, A.N. De Souza, Detection and identification of abnormalities in customer consumptions in power distribution systems, IEEE Trans. Power Deliv. 26 (2011) 2436–2442, http://dx.doi.org/10.1109/TPWRD.2011.2161621.

[5] P. Kadurek, J. Blom, J.F.G. Cobben, W.L. Kling, Theft detection and smart metering practices and expectations in the Netherlands, in: 2010 IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT Eur.), IEEE, 2010, http://dx.doi.org/10.1109/ISGTEUROPE.2010.5638852, pp. 1–6.

[6] C.-H. Lo, N. Ansari, CONSUMER: a novel hybrid intrusion detection system for distribution networks in smart grid, IEEE Trans. Emerg. Top. Comput. 1 (2013) 33–44, http://dx.doi.org/10.1109/TETC.2013.2274043.

[7] L.G. Arango, E. Deccache, B.D. Bonatto, H. Arango, P.F. Ribeiro, P.M. Silveira, Impact of electricity theft on power quality, IEEE PES ICHQP 2016 – 17th Int. Conf. Harmon. Qual. Power. (2016) 557–562.

[8] A. a. Cardenas, S. Amin, G. Schwartz, R. Dong, S. Sastry, A game theory model for electricity theft detection and privacy-aware control in AMI systems, in: 2012 50th Annu. Allert. Conf. Commun. Control. Comput., IEEE, 2012, http://dx.doi.org/10.1109/Allerton.2012.6483444, pp. 1830–1837.

[9] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, X.S. Shen, Energy-theft detection issues for advanced metering infrastructure in smart grid, Tsinghua, Sci. Technol. 19 (2014) 105–120, http://dx.doi.org/10.1109/TST.2014.6787363.

[10] A. Chauhan, S. Rajvanshi, Non-technical losses in power system: a review, in: 2013 Int. Conf. Power, Energy Control, IEEE, 2013, pp. 558–561, http://dx.doi.org/10.1109/ICPEC.2013.6527720.

[11] A. Fragkioudaki, P. Cruz-Romero, A. Gómez-Expósito, J. Biscarri, M.J. de Tellechea, Á. Arcos, in: F. de la Prieta, M.J. Escalona, R. Corchuelo, P. Mathieu, Z. Vale, A.T. Campbell, S. Rossi, E. Adam, M.D. Jiménez-López, E.M. Navarro, M.N. Moreno (Eds.), Detection of Non-technical Losses in Smart Distribution Networks: A Review, Springer International Publishing, Cham, 2016, pp. 43–54, http://dx.doi.org/10.1007/978-3-319-40159-1_4.

[12] S. McLaughlin, D. Podkuiko, P. McDaniel, Energy theft in the advanced metering infrastructure, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) (2010) 176–187, http://dx.doi.org/10.1007/978-3-642-14379-3_15.

[13] P. Glauner, J.A. Meira, P. Valtchev, R. State, F. Bettinger, The challenge of non-technical loss detection using artificial intelligence: a survey, Int. J. Comput. Intell. Syst. 10 (2017) 760, http://dx.doi.org/10.2991/ijcis.2017.10.1.51.

[14] V. Chandola, A. Banerjee, V. Kumar, Anomaly detection, ACM Comput. Surv. 41 (2009) 1–58, http://dx.doi.org/10.1145/1541880.1541882.

[15] L. Wei, E. Keogh, Semi-supervised time series classification, in: Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min. — KDD '06, ACM Press, New York, New York, USA, 2006, http://dx.doi.org/10.1145/1150402.1150498, p. 748.

[16] J. Tacón, D. Melgarejo, F. Rodríguez, F. Lecumberry, A. Fernández, Semisupervised Approach to Non Technical Losses Detection, 2014, http://dx.doi.org/10.1007/978-3-319-12568-8_85, pp. 698–705.

[17] L. Faria, J. Melo, A. Padilha-Feltrin, Spatial-temporal estimation for nontechnical losses, IEEE Trans. Power Deliv. 8977 (2015), http://dx.doi.org/10.1109/TPWRD.2015.2469135, 1-1.

[18] G. Chandrashekar, F. Sahin, A survey on feature selection methods, Comput. Electr. Eng. 40 (2014) 16–28, http://dx.doi.org/10.1016/j.compeleceng.2013.11.024.

[19] C.C.O. Ramos, A.N. De Sousa, J.P. Papa, A.X. Falcão, A new approach for nontechnical losses detection based on optimum-path forest, IEEE Trans. Power Syst. 26 (2011) 181–189, http://dx.doi.org/10.1109/TPWRS.2010.2051823.

[20] C.C.O. Ramos, D. Rodrigues, A.N. de Souza, J.P. Papa, On the study of commercial losses in brazil: a binary black hole algorithm for theft characterization, IEEE Trans. Smart Grid 1 (2016), http://dx.doi.org/10.1109/TSG.2016.2560801.

[21] C.C.O. Ramos, A.N. De Souza, A.X. Falcão, J.P. Papa, New insights on nontechnical losses characterization through evolutionary-based feature selection, IEEE Trans. Power Deliv. 27 (2012) 140–146, http://dx.doi.org/10.1109/TPWRD.2011.2170182.

[22] M. Di Martino, F. Decia, J. Molinelli, A. Fernández, A novel framework for nontechnical losses detection in electricity companies, in: P. Latorre Carmona, J.S. Sánchez, A.L.N. Fred (Eds.), Pattern Recognit. — Appl. Methods, Springer, Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 109–120, http://dx.doi.org/10.1007/978-3-642-36530-0_9.

[23] C.C.O. Ramos, A.N. Souza, G. Chiachia, A.X. Falcão, J.P. Papa, A novel algorithm for feature selection using Harmony Search and its application for non-technical losses detection, Comput. Electr. Eng. 37 (2011) 886–894, http://dx.doi.org/10.1016/j.compeleceng.2011.09.013.

[24] D.R. Pereira, M.A. Pazoti, L.A.M. Pereira, D. Rodrigues, C.O. Ramos, A.N. Souza, J.P. Papa, Social-Spider Optimization-based Support Vector Machines applied for energy theft detection, Comput. Electr. Eng. 49 (2016) 25–38, http://dx.doi.org/10.1016/j.compeleceng.2015.11.001.

[25] B. Coma-Puig, J. Carmona, R. Gavalda, S. Alcoverro, V. Martin, Fraud detection in energy consumption: a supervised approach, in: 2016 IEEE Int. Conf. Data Sci. Adv. Anal., IEEE, 2016, http://dx.doi.org/10.1109/DSAA.2016.19, pp. 120–129.

[26] G. Messinis, et al., Utilizing smart meter data for electricity fraud detection, CIGRE Sci. Eng. J. (June) (2017).

[27] X. Guo, Y. Yin, C. Dong, G. Yang, G. Zhou, On the class imbalance problem, in: 2008 Fourth Int. Conf. Nat. Comput., IEEE, 2008, http://dx.doi.org/10.1109/ICNC.2008.871, pp. 192–201.

[28] S. Axelsson, The base-rate fallacy and the difficulty of intrusion detection, ACM Trans. Inf. Syst. Secur. 3 (2000) 186–205, http://dx.doi.org/10.1145/357830.357849.

[29] J. Nagi, K.S. Yap, S.K. Tiong, S.K. Ahmed, M. Mohamad, Nontechnical loss detection for metered customers in power utility using support vector machines, IEEE Trans. Power Deliv. 25 (2010) 1162–1171, http://dx.doi.org/10.1109/TPWRD.2009.2030890.

[30] J. Nagi, K.S. Yap, S.K. Tiong, S.K. Ahmed, F. Nagi, Improving SVM-based nontechnical loss detection in power utility using the fuzzy inference system, IEEE Trans. Power Deliv. 26 (2011) 1284–1285, http://dx.doi.org/10.1109/TPWRD.2010.2055670.

[31] P. Jokar, N. Arianpoo, V.C.M. Leung, Electricity theft detection in AMI using customers' consumption patterns, IEEE Trans. Smart Grid 7 (2016) 216–226, http://dx.doi.org/10.1109/TSG.2015.2425222.

[32] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, S. Mishra, Decision tree and SVM-based data analytics for theft detection in smart grid, IEEE Trans. Ind. Informatics 12 (2016) 1005–1016, http://dx.doi.org/10.1109/TII.2016.2543145.

[33] K.S. Yap, S.K. Tiong, J. Nagi, J.S.P. Koh, F. Nagi, Comparison of supervised learning techniques for non-technical loss detection in power utility, Int. Rev. Comput. Softw. 7 (2012) 626–636.

[34] Y. Guo, C.W. Ten, P. Jirutitijaroen, Online data validation for distribution operations against cybertampering, IEEE Trans. Power Syst. 29 (2014) 550–560, http://dx.doi.org/10.1109/TPWRS.2013.2282931.

[35] S.S.S.R. Depuru, L. Wang, V. Devabhaktuni, R.C. Green, High performance computing for detection of electricity theft, Int. J. Electr. Power Energy Syst. 47 (2013) 21–30, http://dx.doi.org/10.1016/j.ijepes.2012.10.031.

[36] J. No, S.Y. Han, Y. Joo, J. Shin, Conditional abnormality detection based on AMI data mining, IET Gener. Transm. Distrib. 10 (2016) 3010–3016, http://dx.doi.org/10.1049/iet-gtd.2016.0048.

[37] P. Glauner, A. Boechat, L. Dolberg, R. State, F. Bettinger, Y. Rangoni, D. Duarte, Large-scale detection of non-technical losses in imbalanced data sets, in: 2016 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf., IEEE, 2016, http://dx.doi.org/10.1109/ISGT.2016.7781159, pp. 1–5.

[38] J.P. Kosut, F. Santomauro, A. Jorysz, A. Fernandez, F. Lecumberry, F. Rodriguez, Abnormal consumption analysis for fraud detection: UTE-UDELAR joint efforts, in: 2015 IEEE PES Innov. Smart Grid Technol. Lat. Am. (ISGT LATAM), IEEE, 2015, http://dx.doi.org/10.1109/ISGT-LA.2015.7381272, pp. 887–892.

[39] A.H. Nizar, Z.Y. Dong, Y. Wang, Power utility nontechnical loss analysis with extreme learning machine method, IEEE Trans. Power Syst. 23 (2008) 946–955, http://dx.doi.org/10.1109/TPWRS.2008.926431.

[40] J.I. Guerrero, C. León, I. Monedero, F. Biscarri, J. Biscarri, Improving Knowledge-Based Systems with statistical techniques, text mining, and neural networks for non-technical loss detection, Knowledge-based Syst. 71 (2014) 376–388, http://dx.doi.org/10.1016/j.knosys.2014.08.014.

[41] B.C. Costa, B.L.A. Alberto, A.M. Portela, W. Maduro, E.O. Eler, Fraud detection in electric power distribution networks using an Ann-based knowledge-discovery process, Int. J. Artif. Intell. Appl. 4 (2013) 17–23, http://dx.doi.org/10.5121/ijaia.2013.4602.

[42] L.A.M. Pereira, L.C.S. Afonso, J.P. Papa, Z.A. Vale, C.C.O. Ramos, D.S. Gastaldello, A.N. Souza, Multilayer perceptron neural networks training through charged system search and its application for non-technical losses detection, in: 2013 IEEE PES Conf. Innov. Smart Grid Technol. (ISGT Lat. Am.), IEEE, 2013, http://dx.doi.org/10.1109/ISGT-LA.2013.6554383, pp. 1–6.

[43] V. Ford, A. Siraj, W. Eberle, Smart grid energy fraud detection using artificial neural networks, in: 2014 IEEE Symp. Comput. Intell. Appl. Smart Grid, IEEE, 2014, http://dx.doi.org/10.1109/CIASG.2014.7011557, pp. 1–6.

[44] D. Labate, P. Giubbini, G. Chicco, F. Piglione, Shape: the load prediction and non-technical losses modules, CIRED 23rd Int. Conf. Electr. Distrib. (2015), pp. 15–18.

[45] L.A. Passos Júnior, C.C. Oba Ramos, D. Rodrigues, D.R. Pereira, A.N. de Souza, K.A. Pontara da Costa, J.P. Papa, Unsupervised non-technical losses identification through optimum-path forest, Electr. Power Syst. Res. 140 (2016) 413–423, http://dx.doi.org/10.1016/j.epsr.2016.05.036.
[46] R.D. Trevizan, A.S. Bretas, A. Rossoni, Nontechnical losses detection: a discrete cosine transform and optimum-path forest based approach, in: 2015 North Am. Power Symp., IEEE, 2015, http://dx.doi.org/10.1109/NAPS.2015.7335160, pp. 1–6.
[47] C. León, F. Biscarri, I. Monedero, J.I. Guerrero, J. Biscarri, R. Millán, Variability and trend-based generalized rule induction model to NTL detection in power companies, IEEE Trans. Power Syst. 26 (2011) 1798–1807, http://dx.doi.org/10.1109/TPWRS.2011.2121350.
[48] C. León, F. Biscarri, I. Monedero, J.I. Guerrero, J. Biscarri, R. Millán, Integrated expert system applied to the analysis of non-technical losses in power utilities, Expert Syst. Appl. 38 (2011) 10274–10285, http://dx.doi.org/10.1016/j.eswa.2011.02.062.
[49] I. Monedero, F. Biscarri, C. León, J.I. Guerrero, J. Biscarri, R. Millán, 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. 34 (2012) 90–98, http://dx.doi.org/10.1016/j.ijepes.2011.09.009.
[50] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, S. Zonouz, A multi-sensor energy theft detection framework for advanced metering infrastructures, IEEE J. Sel. Areas Commun. 31 (2013) 1319–1330, http://dx.doi.org/10.1109/JSAC.2013.130714.
[51] J.E. Cabral, J.O.P. Pinto, E.M. Martins, A.M.A.C. Pinto, Fraud detection in high voltage electricity consumers using data mining, in: 2008 IEEE/PES Transm. Distrib. Conf. Expo., IEEE, 2008, http://dx.doi.org/10.1109/TDC.2008.4517232, pp. 1–5.
[52] T.V. Babu, T.S. Murthy, B. Sivaiah, Detecting unusual customer consumption profiles in power distribution systems — APSPDCL, in: 2013 IEEE Int. Conf. Comput. Intell. Comput. Res., IEEE, 2013, http://dx.doi.org/10.1109/ICCIC.2013.6724264, pp. 1–5.
[53] V. Badrinath Krishna, G.A. Weaver, W.H. Sanders, PCA-based method for detecting integrity attacks on advanced metering infrastructure, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) (2015), http://dx.doi.org/10.1007/978-3-319-22264-6_5, pp. 70–85.
[54] S.-J. Chen, T. Zhan, C. Huang, J. Chen, C. LinNontechnical Loss and, Outage detection using fractional-order self-synchronization error-based fuzzy petri nets in micro-distribution systems, IEEE Trans. Smart Grid 6 (2015) 411–420, http://dx.doi.org/10.1109/TSG.2014.2345780.
[55] J.V. Spirić, M.B. Dočić, S.S. Stanković, Fraud detection in registered electricity time series, Int. J. Electr. Power Energy Syst. 71 (2015) 42–50, http://dx.doi.org/10.1016/j.ijepes.2015.02.037.
[56] D. Mashima, A.A. Cárdenas, Evaluating Electricity Theft Detectors in Smart Grid Networks, 2012, http://dx.doi.org/10.1007/978-3-642-33338-5_11, pp. 210–229.
[57] Y. Liu, S. Hu, Cyberthreat analysis and detection for energy theft in social networking of smart homes, IEEE Trans. Comput. Soc. Syst. 2 (2015) 148–158, http://dx.doi.org/10.1109/TCSS.2016.2519506.
[58] V.B. Krishna, R.K. Iyer, W.H. Sanders, ARIMA-based Modeling and Validation of Consumption Readings in Power Grids, Springer International Publishing, Cham, 2016, http://dx.doi.org/10.1007/978-3-319-33331-1.
[59] V.B. Krishna, K. Lee, G.A. Weaver, R.K. Iyer, W.H. Sanders, F-DETA: a framework for detecting electricity theft attacks in smart grids, in: 2016 46th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks, IEEE, 2016, http://dx.doi.org/10.1109/DSN.2016.44, pp. 407–418.
[60] C. Lin, S.-J. Chen, C. Kuo, J. Chen, Non-cooperative game model applied to an advanced metering infrastructure for non-technical loss screening in micro-distribution systems, IEEE Trans. Smart Grid 5 (2014) 2468–2469, http://dx.doi.org/10.1109/TSG.2014.2327809.
[61] T.-S. Zhan, C.-L. Kuo, S.-J. Chen, J.-L. Chen, C.-C. Kao, C.-H. Lin, Non-technical loss and power blackout detection under advanced metering infrastructure using a cooperative game based inference mechanism, IET Gener. Transm. Distrib. 10 (2016) 873–882, http://dx.doi.org/10.1049/iet-gtd.2015.0003.
[62] M. Tariq, H.V. Poor, Electricity theft detection and localization in grid-tied microgrids, IEEE Trans. Smart Grid 3053 (2016), http://dx.doi.org/10.1109/TSG.2016.2602660, 1-1.
[63] D.N. Nikovski, Z. Wang, A. Esenther, H. Sun, K. Sugiura, T. Muso, K. Tsuru, Smart meter data analysis for power theft detection, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 7988 LNAI (2013) 379–389, http://dx.doi.org/10.1007/978-3-642-39712-7_29.
[64] S. Salinas, M. Li, P. Li, Privacy-preserving energy theft detection in smart grids: a P2P computing approach, IEEE J. Sel. Areas Commun. 31 (2013) 257–267, http://dx.doi.org/10.1109/JSAC.2013.SUP.0513023.
[65] E.A.C. Aranha Neto, J. Coelho, Probabilistic methodology for technical and non-technical losses estimation in distribution system, Electr. Power Syst. Res. 97 (2013) 93–99, http://dx.doi.org/10.1016/j.epsr.2012.12.008.
[66] S. Weckx, C. Gonzalez, J. Tant, T. De Rybel, J. Driesen, Parameter identification of unknown radial grids for theft detection, in: 2012 3rd IEEE PES Innov. Smart Grid Technol. Eur. (ISGT Eur.), IEEE, 2012, http://dx.doi.org/10.1109/ISGTEurope.2012.6465644, pp. 1–6.
[67] W. Han, Y. Xiao, A novel detector to detect colluded non-technical loss frauds in smart grid, Comput. Netw. 117 (2017) 19–31, http://dx.doi.org/10.1016/j.comnet.2016.10.011.
[68] S.A. Salinas, P. Li, Privacy-preserving energy theft detection in microgrids: a state estimation approach, IEEE Trans. Power Syst (2015) 1–12, http://dx.doi.org/10.1109/TPWRS.2015.2406311.
[69] Lijuan Chen, Xiaohui Xu, Chaoming Wang, Research on anti-electricity stealing method base on state estimation, in: 2011 IEEE Power Eng. Autom. Conf., IEEE, 2011, http://dx.doi.org/10.1109/PEAM.2011.6134972, pp. 413–416.
[70] W. Luan, G. Wang, Y. Yu, J. Lin, W. Zhang, Q. Liu, Energy theft detection via integrated distribution state estimation based on AMI and SCADA measurements, in: 2015 5th Int. Conf. Electr. Util. Deregul. Restruct. Power Technol., IEEE, 2015, http://dx.doi.org/10.1109/DRPT.2015.7432350, pp. 751–756.
[71] Yuan-Liang Lo, Shih-Che Huang, Chan-Nan Lu, Non-technical loss detection using smart distribution network measurement data, in: IEEE PES Innov. Smart Grid Technol., IEEE, 2012, http://dx.doi.org/10.1109/ISGT-Asia.2012.6303316, pp. 1–5.
[72] Y. Liu, Y. Wang, X. Guan, A novel method to detect bad data injection attack in smart grid, in: 2013 Proc. IEEE INFOCOM, IEEE, 2013, http://dx.doi.org/10.1109/INFCOM.2013.6567175, pp. 3423–3428.
[73] C. Liao, C.W. Ten, S. Hu, Strategic FRTU deployment considering cybersecurity in secondary distribution network, IEEE Trans. Smart Grid 4 (2013) 1264–1274, http://dx.doi.org/10.1109/TSG.2013.2256939.
[74] Y. zhou, X. Chen, A. Zomaya, L. Wang, S. Hu, A dynamic programming algorithm for leveraging probabilistic detection of energy theft in smart home, IEEE Trans. Emerg. Top. Comput. (2015), http://dx.doi.org/10.1109/TETC.2015.2484841, 1-1.
[75] L.G. de O. Silva, A.A.P. da Silva, A.T. de Almeida-Filho, Allocation of power-quality monitors using the P-median to identify nontechnical losses, IEEE Trans. Power Deliv. 31 (2016) 2242–2249, http://dx.doi.org/10.1109/TPWRD.2016.2555282.
[76] Z. Xiao, Y. Xiao, D.H.-C. Du, Exploring malicious meter inspection in neighborhood area smart grids, IEEE Trans. Smart Grid 4 (2013) 214–226, http://dx.doi.org/10.1109/TSG.2012.2229397.
[77] J.V. Spirić, S.S. Stanković, M.B. Dočić, T.D. Popović, Using the rough set theory to detect fraud committed by electricity customers, Int. J. Electr. Power Energy Syst. 62 (2014) 727–734, http://dx.doi.org/10.1016/j.ijepes.2014.05.004.
[78] J.V. Spirić, S.S. Stanković, M.B. Dočić, Determining a set of suspicious electricity customers using statistical ACL Tukey's control charts method, Int. J. Electr. Power Energy Syst. 83 (2016) 402–410, http://dx.doi.org/10.1016/j.ijepes.2016.04.035.
[79] S.-C. Huang, Y.-L. Lo, C.-N. Lu, Non-technical loss detection using state estimation and analysis of variance, IEEE Trans. Power Syst. 28 (2013) 2959–2966, http://dx.doi.org/10.1109/TPWRS.2012.2224891.
[80] C. Su, W. Lee, C.-K. Wen, Electricity theft detection in low voltage networks with smart meters using state estimation, in: 2016 IEEE Int. Conf. Ind. Technol., IEEE, 2016, http://dx.doi.org/10.1109/ICIT.2016.7474800, pp. 493–498.
[81] A. Rossoni, R. Trevizan, A. Bretas, D. Gazzana, A. Bettiol, A. Carniato, L. Passos, R. Martin, Hybrid formulation for technical and non-technical losses estimation and identification in distribution networks: application in a brazilian power system, CIRED 23 Rd Int. Conf. Electr. Distrib. (2015), pp. 15–18.
[82] R.D. Trevizan, A. Rossoni, A.S. Bretas, D. da Silva Gazzana, R. de Podesta Martin, N.G. Bretas, A.L. Bettiol, A. Carniato, L.F. do Nascimento Passos, Non-technical losses identification using Optimum-Path Forest and state estimation, in: 2015 IEEE Eindhoven PowerTech, IEEE, 2015, http://dx.doi.org/10.1109/PTC.2015.7232685, pp. 1–6.
[83] J.B. Leite, J.R.S. Mantovani, Detecting and locating non-technical losses in modern distribution networks, IEEE Trans. Smart Grid 3053 (2016), http://dx.doi.org/10.1109/TSG.2016.2574714, 1-1.