Energy theft detection for AMI using principal component analysis based reconstructed data

Sandeep Kumar Singh[1] ✉, Ranjan Bose[2], Anupam Joshi[3]

[1]Department of Electronics and Communication Engineering, Indian Institute of Information Technology Pune, Pune 412109, India
[2]Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110 016, India
[3]Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore MD 21250, USA
✉ E-mail: sandeepsingh012@gmail.com

Abstract: To detect energy theft attacks in advanced metering infrastructure (AMI), we propose a detection method based on principal component analysis (PCA) approximation. PCA approximation is introduced by dimensionality reduction of high dimensional AMI data and the authors extract the underlying consumption trends of a consumer that repeat on a daily or weekly basis. AMI data is reconstructed using principal components and used for computing relative entropy. In the proposed method, relative entropy is used to measure the similarity between two probability distributions derived from reconstructed consumption dataset. When energy theft attacks are injected into AMI, the probability distribution of energy consumption will deviate from the historical consumption, so leading to a larger relative entropy. The proposed detection method is tested under different attack scenarios using real-smart-meter data. Test results show that the proposed method can detect theft attacks with high detection percentage.

1 Introduction

The recent technological advancements in information technologies and communication systems have led to the transformation of traditional power grid into the smart grid. Nowadays, nations are changing their existing power grid system to smart grid system. Smart grid manages power demand in reliable, sustainable and economical manner. The smart grid is made practical by two-way communication technologies, advanced computer processing, and modern control systems. The advantages associated with the smart grid are efficient electricity transmission, faster electricity restoration after power disturbance, reduction in peak demand, less operational and management cost for utility companies, and improved security. Advanced metering infrastructure (AMI) is a key part of smart grid.

AMI is an integration of various techniques such as smart meters, communication networks, meter data management system that enable two-way communication between customers and utility companies. The smart meter is low cost advanced electronic meter that collects time base electricity consumption data and transmits it to meter data management system through the communication network. Some security measures have been taken in smart meters, but these measures are not sufficient to secure it from cyber threat [1, 2]. If we add more security measures in smart meters, it will increase the cost of smart meters. Energy theft is one of the key attacks in AMI. The non-technical losses due to energy theft in India are around $16.2 billion a year [3]. Government of India is planning to install five million smart meters in the near future [4]. In the United States, the economical loss due to energy theft is ~$6 billion a year [5].

Many methods have been proposed in the literature to detect energy theft in AMI. In state-based energy theft detection method, radio-frequency identification tags and wireless sensors are used to detect attacks. It will increase the total cost of detection. In [6], a CONSUMER attack model is discussed to improve detection accuracy using grid sensor placement algorithm. In [7], a multi-sensor theft detection framework is proposed to detect an attack in AMI. In [8], radio-frequency identification (RFID) technology is proposed to prevent energy theft in AMI. Xiao et al. [9] discussed a mutual inspection strategy to identify compromised meters. In game-theory based methods, a game is played between the utility

company and the energy thief, but the formation of the utility function for all players is a tough task in this method. In [10], Amin et al. discussed about the incentives of the utilities to combat non-technical losses when company is subject to tariff regulation. They proposed that regulators should incorporate explicit targets for permissible losses to solve the problem of incentive misalignment. In [11], a game between energy thief and utility is played to detect energy theft. The aim of the electricity thief is to steal a fixed amount of electricity while reducing the possibility of being detected, while the utility wants to maximise the probability of detection. The game-theory-based methods present low cost and reasonable solution to detect electricity theft detection in AMI.

Classification based methods have been discussed in the literature to detect energy theft. These methods have advantages of the detailed energy consumption data of AMI. AMI data follows a certain statistical patterns under normal conditions. Malicious AMI data have irregular statistical patterns. In classification-based method, machine learning and data mining techniques are used to train the classifier. A new sample is tested using this trained classifier. Due to availability of the smart meter data, these methods have moderate cost. In [12], Angelos et al. discussed C-means fuzzy clustering algorithm to detect malicious measurement. In [13], a peer-to-peer computing is used to identify the malicious consumer using users' honesty coefficients. In [14], a theft detection algorithm based on classification is proposed using customers' consumption pattern. In [15], non-technical losses (NTL) are discussed. The main portion of NTL is electricity theft and irregular billings. To detect NTL, support vector machines are trained with the data form smart meters and the data is classified as per rules. In [16], Depuru et al. proposed a neural network model to detect illegal consumers using consumers load profile. In [17], Martino et al. presents a fraud detection scheme based on class imbalance. The authors proposed automatic detection tool combining classification strategies. In [18], a threat model for the use of data analytics in detecting electricity theft is proposed. Data imbalance is one of the prime concern in classification based method. The number true data samples and malicious data samples are not in the same range. True data samples are readily available using historical dataset but malicious samples are rarely available for any particular consumer. Unavailability of malicious data samples limits the detection rate (DR). Vulnerability to

Table 1 Advantages and limitations of defence techniques against electricity theft attacks in AMI

Defence techniques	Advantages	Limitations
state-based methods [6–9]	Employ specific devices, like radio-frequency identification (RFID) tags and wireless sensors to provide high detection efficiency	The price of extra investment required for the monitoring system including system implementation cost, software cost, device cost, and training/operating cost
game-based methods [10, 11]	Electricity theft detection problem is formulated as a game between the utility and the electricity thief. Low cost and reasonable solution for reducing electricity theft	Formulation of the utility function of all players, including regulators, distributors, and thieves is a challenging task
classification-based method [12–18]	Machine learning and data mining schemes are used to train a classifier. Moderate cost methods	Non-malicious factors can alter the consumption pattern. Vulnerable to contamination attacks and data imbalance
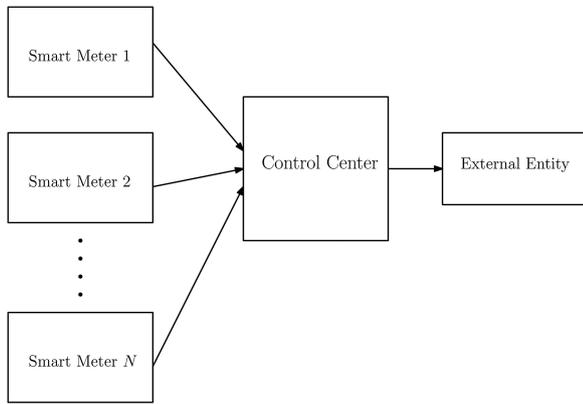
Fig. 1 *Network model*

contamination attacks is second concern with classification based methods. An adversary can deceives the learning algorithm by granular changes in data and polluting the dataset. Due to this, the learning algorithm accepts a malicious pattern as a normal one. Next issue with classification based scheme is that many non-malicious factors can change the consumption pattern such as change of alliances, change of residents, seasonality. Improper dealing with such factors will lead in high false positive rate (FPR). To train a new model for the case of change in user's pattern, the new sample is stored in a temporary database. If in the next coming days this consumption pattern repeated frequently, the old dataset is discarded and the new dataset based on the samples in the temporary dataset will be generated. After the large size of dataset, we retrain the model. In AMI, false positives cause a costly procedure. On-site inspection is needed for final verification. Table 1 summarises various defence techniques to detect electricity theft attacks in AMI reported in the literature.

In [19], Krishna *et al.* have proposed a method to detect integrity attacks on AMI using principal component analysis (PCA) and density-based spatial clustering of applications with noise (DBSCAN). In the proposed method, the first two principal components (PCs) have been used. In [20], classification of theft attacks has been discussed and detection methodology based on Kullback–Leibler (KL) divergence has been proposed. In [21], meter fraud in the context of distributed energy resources (DERs) has been discussed and the economic impact of cyber-attacks has been quantified. In this paper, we propose a method to detect energy theft attacks in AMI based on PCA [22] approximation method. The proposed method transforms the meter energy consumption vector into a linear combination of a vector with uncorrelated component. PCA approximation is introduced by dimensionality reduction of high dimensional AMI data into a low-dimensional data. We reconstruct the AMI data using PCs and use the reconstructed data to compute relative entropy [23]. Relative entropy for a data sample is computed using reconstructed historical dataset. We compare the relative entropy with a pre-defined threshold value. If the relative entropy is larger than the threshold value, the newly received data sample is likely to be malicious. The threshold value is calculated using benign historical dataset. The performance of the proposed electricity theft detection method is analysed using real-smart-meter dataset [24] on different attack scenarios. The dataset includes all factors such as temperature, weekend/weekday/holiday data that can impact the

energy consumption pattern. Test results show that the proposed method detects electricity theft attacks with high DR. The main contributions of this paper are as follows:

i. We design a method to detect energy theft against AMI by reducing the dimensionality of large size AMI data using PCA approximation. Control centre has to process small size AMI data due to the PCA approximation. Detection is done by computing the relative entropy of reconstructed data. Here, we perform relative entropy (same as KL divergence) after PCA.

ii. The problem of imbalance data is addressed by the generation of synthetic attack dataset. A wide range of attack pattern can be generated and the performance of the proposed method is tested under different attack patterns.

iii. We test the performance of the proposed detection methodology with real smart meter dataset of Irish Social Science Data Archive (ISSDA) [24]. The ISSDA dataset is publicly available.

iv. We compare the performance of the proposed methodology with most recent theft detection method using ISSDA data. The results show that the proposed method is more effective.

The rest of the paper is organised as follows. Network model and attack model are discussed in Section 2. The proposed detection methodology to detect energy theft attack in AMI is given in Section 3. A case study is discussed in Section 4. Section 5 presents the test results. Section 6 concludes the paper.

2 Network model and attack model

2.1 Network model

Fig. 1 shows the network model [25]. In this model, N smart meters send consumption readings to the control centre at a pre-defined time interval. Control centre sends the final aggregate to the external entity. External entity may be a grid manager or a third party service provider. All security measures have been taken at the control centre to secure AMI form cyber threat. We assume that control centre is secure and cannot be compromised.

2.2 Attack model

The objective of the adversary is to compromise smart meters and send the malicious consumption readings other than true consumption readings to the control centre to take financial benefit. Different types of energy theft techniques are discussed in the literature [7, 25]. These techniques can be categorised into three types: (i) physical attacks, (ii) cyber attacks; and (iii) data attacks.

i. *Physical attacks*: This type of attacks includes meter tampering, reversing or disconnecting the meters and bypassing the meters to remove loads form measurements.

ii. *Cyber attacks*: These types of attacks can be done within the smart meter or over the link between the control centre and smart meter. These attacks include compromising the smart meter through the remote location, interrupting readings, intercepting communication between smart meters and the control centre and altering the storage on smart meters.

iii. *Data attacks*: Data attacks can be launched through physical and cyber attacks. The objective of data attack is to target the electricity consumption measurements of smart meters.

Table 2 Summary of different electricity theft techniques in AMI

Electricity theft techniques	
physical attacks	Disconnect the meter, reverse the meter, break into the meter, bypass the meter to remove loads from measurements
cyber attacks	To compromise the meter through remote network exploit, intercept and alter the communication, steal password to login to meter, change the storage of meters
data attacks	Report zero consumption, stop reporting the consumption, change appliances load profiles, withdraw heavy appliances from measurements

Energy consumers, professional hackers and utility company insiders are the primary attackers in AMI. They can launch one or more type of the energy theft attacks to get a financial benefit. Table 2 summarises various electricity theft techniques.

3 Proposed detection methodology

Energy theft is one of the prime concerns in AMI. In this paper, we propose a method based on PCA approximation to detect energy theft in AMI. The energy consumption of smart meters is shown by a data matrix X having size $m \times n$, where m is the total number of observation and n is the number of variables.

3.1 Principal component analysis

Before exploring the proposed detection methodology, the basic principles of PCA [22] are discussed. The PCA is a statistical analysis method to reduce the dimensions of a given high dimensional data while retaining its spatial attributes as much as possible. The PCA transform the unlabelled dataset into a new coordinate system so that the projection on this new coordinate system has maximum variance. Similarly, we can find the successive coordinates. principal components (PCs) having maximum variance have more information about statistical characteristics of consumption data and the opposite is true for PCs having lower variance. So, we can extract underlying consumption trends that reappear on a daily or weekly basis. We have applied theft detection schemes in a space span by the consumptions of all consumers. So, it becomes harder for an adversary to do reverse engineering and circumvent the detection because the adversary would require complete information of all the meters in the AMI network.

In our case, we have taken energy consumption of smart meter by data matrix X and the size of X is $m \times n$. m is the number of observations and n is the number of variables. The dimension of data matrix X is n. We have applied PCA on the dataset X and compute different PCs. All these PCs are orthogonal to each other and are a linear combination of n variables. In PCA, most of the variance in data matrix X is retained by the first few PCs. Before applying PCA to the data matrix, we pre-process the data. The new data is the original data centred by subtracting the column means from corresponding columns.

The first principal component is given as

$$p_1 = w_1^T X = w_{11}x_1 + w_{12}x_2 + \cdots + w_{1n}x_n = \sum_{j=1}^{n} w_{1j}x_j \quad (1)$$

In (1), the coefficients $w_1 = (w_{11}, w_{12}, \ldots, w_{1n})^T$ are selected to maximise the variance $\text{var}(p_1) = w_1^T \sum_x w_1$ subject to condition that $|w_1|^2 = \sum_{j=1}^{n} w_{1j}^2 = 1$. Here, the first PC contains the maximum variance.

Similarly, the second principal component is given as

$$p_2 = w_2^T X = w_{21}x_1 + w_{22}x_2 + \cdots + w_{2n}x_n = \sum_{j=1}^{n} w_{2j}x_j \quad (2)$$

In (2), the coefficients $w_2 = (w_{21}, w_{22}, \ldots, w_{2n})^T$ are selected to maximise the variance $\text{var}(p_2) = w_2^T \sum_x w_2$ subject to the condition that $|w_2|^2 = \sum_{j=1}^{n} w_{2j}^2 = 1$ and $[w_2^T w_1 = 0]$. Hence, the second principal component retains the second largest variance and coefficients w_2 is orthogonal to w_1.

Similarly, we define n principal components in decreasing order of variance. The coefficients $w_1, w_2, \ldots, w_n$ are called vector of coefficients or loadings, and $p_1, p_2, \ldots, p_n$ are called PCs. Most of the variance of the data matrix is retained by the first few PCs. We select the first few PCs and reconstruct the data using these PCs.

(a) Daily electricity consumption, (b) histogram of weekly electricity consumption

3.2 Relative entropy

Relative entropy [23] is a measure of similarity between two probability distributions. Let us consider two probability distributions p and q. The relative entropy $D(p \parallel q)$ is defined as

$$D(p \parallel q) = \sum_x p(x)\ln\frac{p(x)}{q(x)}$$
$$= E_p\ln\frac{p(x)}{q(x)} \quad (3)$$

In (3), we consider that $0\log(0/0) = 0$, $0\log(0/q) = 0$, and $p\log(p/0) = \infty$. Relative entropy is the expectation of the logarithmic of the likelihood ratio. It is also called Kullback–Leibler distance. $D(p \parallel q)$ is always non-negative, $D(p \parallel q) \geq 0$. Relative entropy is not symmetric, $D(p \parallel q)$ is not equal to $D(q \parallel p)$. It does not follow the triangle inequality.

As shown in Fig. 1, N smart meters send their consumption readings to the control centre at a pre-defined time interval. Control centre applies PCA on the dataset to find loadings and transform high-dimensional data into low-dimensional data. We reconstruct the data X using the first k PCs. The reconstructed data $\hat{X}$ is given as

$$\hat{X} = SW^T \quad (4)$$

where W is the coefficient matrix and S is the score matrix for the k retained PCs [26] and T represents the transpose. The coefficient matrix W includes k largest eigenvectors (first k vector of coefficients or loadings). The score matrix S is computed as

$$S = XW \quad (5)$$

where X is the pre-processed data matrix and W is the coefficient matrix.

Relative entropy is calculated from (3) using reconstructed data $\hat{X}$. To calculate relative entropy, distribution q is the distribution of historical energy consumption data, and p represents the distribution of current observation. When there is no energy theft attack in AMI, the relative entropy would be small. If an adversary has launched energy theft attacks in AMI, the relative entropy will increase. We compare the runtime relative entropy with a pre-defined threshold value. If the runtime relative entropy is larger than the threshold, it concludes that adversary has launched energy theft attack. The control centre will take an appropriate action after detecting the attacks.

We summarise the proposed detection methodology as follows:

i. Pre-process the data matrix X;
ii. Generate the vector of coefficients or loadings by applying PCA on X;
iii. Select first k PCs retaining the maximum variance;
iv. Reconstruct the data $\hat{X}$ using first k PCs;
v. Compute the runtime relative entropy of the reconstructed testing data sample using reconstructed historical dataset;

vi. Classify testing data sample as malicious sample or true sample based on the comparison of the runtime relative entropy with the pre-defined threshold value. If the runtime relative entropy is outside the threshold, the sample is considered as malicious, otherwise the sample is considered true.

4 Case study

To test the performance of the proposed scheme, we used the real smart meter data from ISSDA [24]. Smart meter sends their consumption readings to the control centre at a pre-defined time interval. In [24], 30 min time interval is chosen. For lth day, the smart meter true consumption is $c_l = [c_{l1}, c_{l2}, \ldots, c_{l48}]$ and malicious consumption is $m_l = [m_{l1}, m_{l2}, \ldots, m_{l48}]$. Fig. 2a shows the daily electricity consumption of a typical consumer. Fig. 2b shows the histogram of weekly electricity consumption of a typical consumer.

To detect energy theft in AMI, we assume that historical data is benign. The size of historical data matrix X is $56,000 \times 336$ ($m = 56,000$, $n = 336$). This historical data includes 56 weeks data of 1000 consumers. Each row of X represents the weekly consumption of a specific consumer. Weekly consumption data consists of 336 readings. The data matrix X is pre-processed by subtracting the column means from corresponding columns. We apply PCA on X and find out PCs. First PC retains the largest variance, second PC retains the second largest variance and so on. Fig. 3 shows the variance captured by first 10 PCs. The first 22 PCs retain three-fourth of the total variance. So, we have chosen first 22 PCs for further analysis. Hence, the dimensionality of the data decreases from 336 to 22. Dimensionality reduction is one of the main objectives of PCA. We reconstruct the historical data using first 22 PCs. Similarly, we applied PCA on the next four weeks data, find out its PCs and reduce the dimensionality from 336 to 22. We reconstruct this four-week data using first 22 PCs.

Relative entropy is calculated between the above calculated two reconstructed datasets using (3). Distribution q is computed from historical reconstructed data and distribution p is computed using four weeks reconstructed data. Fig. 4 shows the histogram of relative entropy under no attack scenario. In this case, mean of the relative entropy is 0.83. Minimum and maximum value of relative entropy is 0.31 and 4.36, respectively.

An adversary can send malicious consumption readings other than true consumption to the control centre to gain financial profit. We have chosen five weeks data of $N = 1000$ meters to test the performance of proposed scheme under attack scenario. The size of this malicious data matrix is 5000×336. PCA is applied to this data and the data is transformed to the low dimensional dataset. We reconstruct the data using first 22 PCs. Relative entropy is calculated using (3). Distribution p is computed using reconstructed malicious data samples and distribution q is computed from historical reconstructed data. Fig. 5 shows the histogram of relative entropy under energy theft attack scenario. In this case, the mean of relative entropy is 2.80 and minimum and maximum value of relative entropy is 2.40 and 3.30, respectively. From this analysis, we see that the mean of relative entropy is increased under energy theft attack scenario. We calculate the runtime relative entropy at every observation and compare it with the pre-defined threshold. If the runtime relative entropy is larger than the threshold, it means that the adversary launch energy theft attack in AMI, and that observation is a malicious observation. The control will discard that sample and take appropriate action.

Selection of a proper threshold value is an important part of the proposed scheme. If we do not select threshold properly, it will
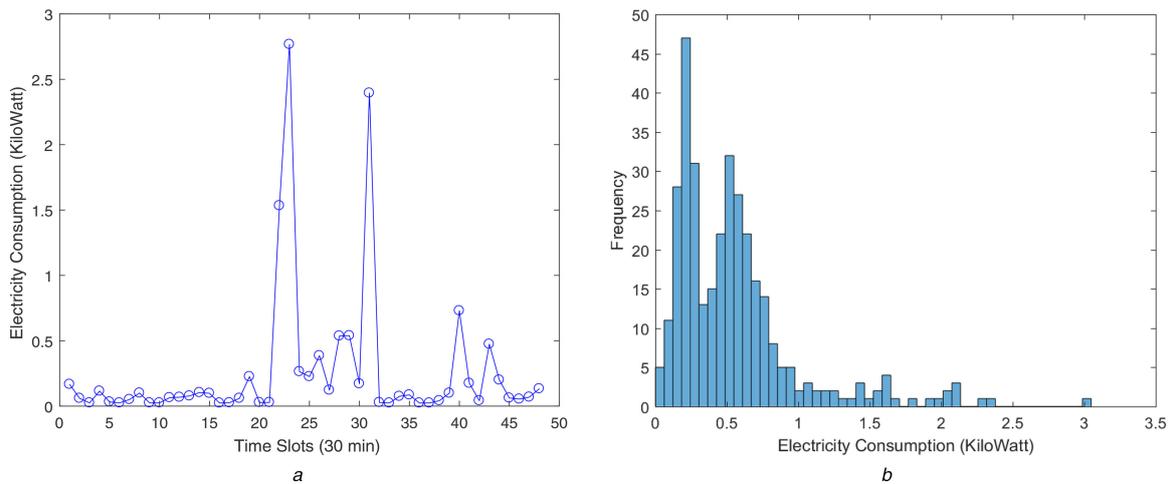

Fig. 2 *Example of electricity consumption of a typical consumer*
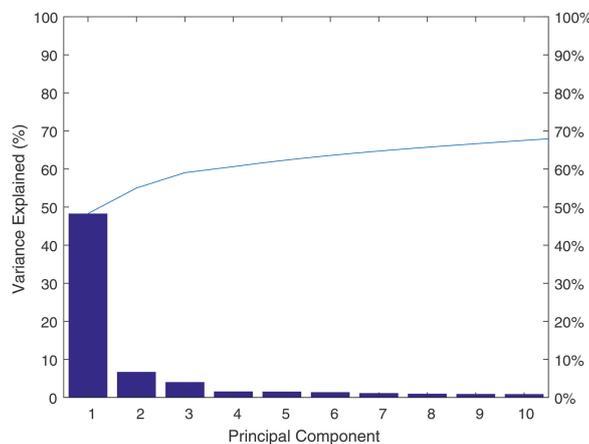*(a)* Daily electricity consumption, *(b)* Histogram of weekly electricity consumption
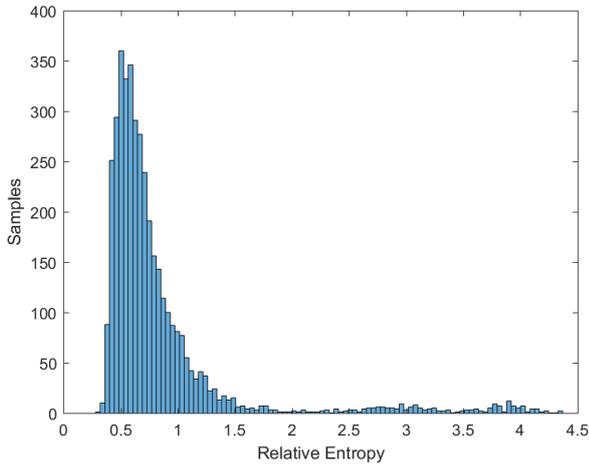

Fig. 3 *Variance captured by PCs*

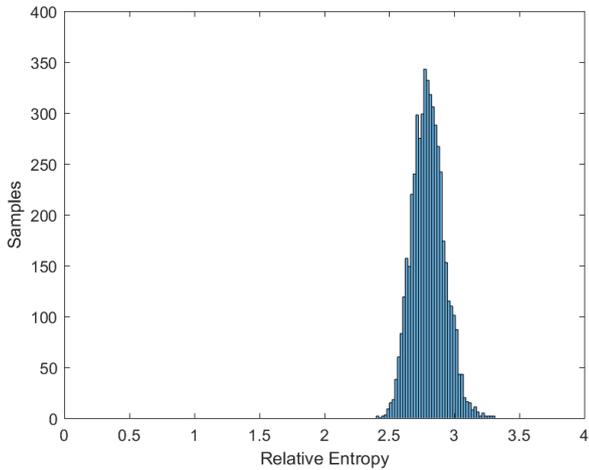**Fig. 4** *Histogram of relative entropy (no attack)*

Fig. 5 *Histogram of relative entropy (with attack)*

Table 3 Summery of test results for energy theft attacks

Type of attack	Detected samples, %
attack 1	77.56
attack 2	86.81
attack 3	100

result in high FPR and low DR. In [27], the threshold is selected from the historical dataset to detect false data injection attacks in smart grid. Similarly, in the proposed scheme, we set the threshold using mean of historical relative entropy with certain variation. So, the threshold is set to $[(1 + \gamma) \times \mathrm{mean}(\mathrm{Relative\,Entropy})]$. If the runtime relative entropy for a sample is outside this threshold, the sample is considered as malicious. To calculate the threshold, we have made an assumption that the historical data is benign. Real historical data from ISSDA is used for this purpose. In the testing phase of the proposed method, the attacked data is used. So, the mean of the testing data is biased due to the attack.

5 Results and discussions

To check the performance of proposed scheme, we have done all simulation on MATLAB R2016b on DELL PC with 3.20 GHz Intel Core i7 processor. For lth day, true electricity consumption for a typical consumer is given as $c_l = [c_{l1}, c_{l2}, \ldots, c_{l48}]$. The malicious sample $m_l = [m_{l1}, m_{l2}, \ldots, m_{l48}]$ can be created using the following type of attack scenarios [14, 19]:

i. $A1$: In this case, the attacked sample is defined as:

$$m_l = \beta c_l \tag{6}$$

In (6), β is a parameter equal to random($\beta_{\mathrm{MIN}}, \beta_{\mathrm{MAX}}$). In this attack, adversary multiplied all consumption measurements by parameter β which is uniformly distributed between β_{MIN} and β_{MAX}.

ii. $A2$: In the second type of attack, the malicious sample is given as

$$m_l = \beta_l c_l \tag{7}$$

In (7), parameter β_l is given as $\beta_{l1}, \beta_{l2}, \ldots, \beta_{l48}$, where each β_{li} is given as random($\beta_{li\mathrm{MIN}}, \beta_{li\mathrm{MAX}}$). Here, each consumption reading is multiplied by different β_{li}, which is uniformly distributed between $\beta_{li\mathrm{MIN}}$ and $\beta_{li\mathrm{MAX}}$.

iii. $A3$: In this case, the attacked sample is defined as

$$m_l = \beta_l \,\mathrm{mean}(c_{l-1}) \tag{8}$$

In $A3$ attack scenario, mean of previous day consumption is multiplied by β_l and send it to the control centre.

Receiver operating characteristics [28, 29] curve is used to check the performance of the proposed scheme. ROC curve is a plot to see the tradeoffs between FPR and DR. DR (sensitivity) is a measure of accurate identification of true positives and FPR (1-specificity) is a measure of accurate identification of true negatives

$$\mathrm{Sensitivity} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{9}$$

$$\mathrm{Specificity} = \frac{\mathrm{TN}}{\mathrm{TN} + \mathrm{FP}} \tag{10}$$

In (9) and (10), FP, FN, TP and TN show false positives, false negatives, true positives and true negatives, respectively.

5.1 Test result

To test the performance of proposed scheme, real-time smart meter data from ISSDA [24] is used. To solve data imbalance problem, synthetic attack dataset is generated using (6)–(8). Sixty weeks historical consumption data is used to compute threshold. The next five weeks data is used to check the performance of the proposed scheme. One of the key properties of AMI is that the energy consumption of all smart meters follows a certain statistical pattern. We consider an attack in a coordinated manner in which adversary launch attacks on smart meters such a way that the control centre may not raise a flag about an attack. Attack can be created using (6)–(8). We choose β_{MIN} and β_{MAX} equal to 0.2 and 0.8. In the test setup, N is chosen to 1000. The value of γ is chosen to 0.1.

Table 3 summarises the test results under different attack scenarios. From Table 3, attacks $A1$ and $A2$ are detected with a detection rate of 77.56% and 86.81%, respectively. Attack $A3$ is detected with 100% detection rate. These results show that the proposed scheme can detect theft attacks with high detection probability.

Classification-based methods [12–18] are widely used to detect electricity theft attacks against AMI. In classification-based methods, SVM is used under different scenarios to counter theft attacks [14, 15, 17]. To compare the performance of the proposed scheme, we implemented the SVM-based theft detector and tested its performance using ISSDA dataset [24]. In SVM, the classifier is trained using benign and malicious data samples. Sixty weeks consumption data of smart meters is used to train the classifier and five weeks consumption data is used in a testing phase. Fig. 6 shows the performance comparison of multi-class SVM and the proposed method for all three attacks. From Fig. 6, SVM performs better than the proposed theft detection method when FPR is below 0.6, 1.1 and 0.4 for attack A1, A2 and A3, respectively. When FPR increases, the proposed theft detection method outperforms the SVM-based theft detector. Test results show that DR for the

IET Cyber-Phys. Syst., Theory Appl., 2019, Vol. 4 Iss. 2, pp. 179-185

183

Table 4 Comparision among energy theft detection methods

Theft detection methods	DR, %
SVM-based theft detector	A_1: 59.92
	A_2: 60.67
	A_3: 91.49
ARMA-GLR detector [18]	67
P2P [13]	A_1: 96
	A_2: NA
	A_3: NA
PCA-DBSCAN [19]	8.1
KL-divergence	A_1: 88.17
	A_2: 99.95
	A_3: 100
proposed method	A_1: 77.56
	A_2: 86.81
	A_3: 100

Table 5 Effect of threshold on detection performance

γ	FPR, %	DR, %		
		Attack 1	Attack 2	Attack 3
0.05	26.32	78.93	90.56	100
0.10	22.80	77.56	86.81	100
0.15	19.74	72.92	82.02	100
0.20	17.24	68.69	76.57	100
0.25	15.14	69.81	70.56	100
0.30	13.86	63.26	63.83	100
0.35	12.66	61.82	56.60	100
0.40	11.34	50.23	48.98	100
0.45	10.14	46.43	41.13	100
0.50	9.32	47.72	33.87	100

Table 6 Effect of β on detection performance

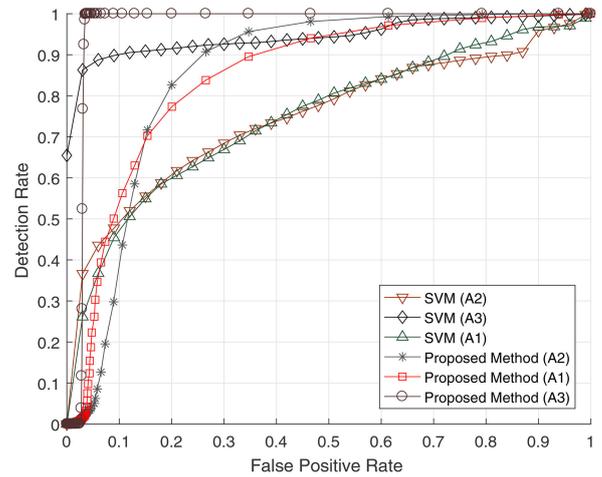| β		DR, %		
β_{MIN}	β_{MAX}	Attack 1	Attack 2	Attack 3
0.1	0.9	74.90	86.97	100
0.2	0.8	77.56	86.81	100
0.3	0.7	83.19	87.06	100
0.4	0.6	88.24	87.61	100
0.5	0.5	87.72	87.72	100

Fig. 6 *ROC curve for SVM and proposed method*

PCA-DBSCAN method. We have also compared the proposed method with KL-divergence method. DR for the proposed method and KL-divergence method is 77.56%, and 88.17% for attack $A1$, 86.81% and 99.95% for attack $A2$ and 100% and 100% for attack $A3$, respectively. The KL-divergence method performs better than the proposed method because all PCs have been included in KL divergence; hence there is no information loss. On the other hand, only 22 PCs are used in the proposed method due to dimensionality reduction; hence DR decreases as compare to KL-divergence method. Table 4 gives the comparison among electricity theft detection methods.

The advantageous of the proposed method over the KL divergence method is the dimensionality reduction of large size AMI data. In the proposed method, PCA is used for dimensionality reduction. In [19], first two PCs retaining 63.63% of total variance are chosen. The number of selected PCs should retain the variance in such a way that the underlying consumption trends that repeat on a daily or weekly basis can be extracted and the dimensionality should be reduced at the same time. We observe that the first 22 PCs retain three-fourth of the total variance. So, we have chosen first 22 PCs for further analysis. Hence, the dimensionality of the data reduces from 336 to 22. The impact of number of PCs on the performance of the proposed method is discussed in the subsequent subsection.

5.2 Effect of threshold on performance

In the proposed scheme, the threshold is a key parameter to detect energy theft in AMI. We select threshold value using historical dataset. Threshold value depends on the parameter γ. We checked the performance of the proposed scheme for different values of γ. Table 5 shows the FPR and DR for different γ when adversary launches attack $A1$, $A2$ and $A3$. From Table 5, we see that if we set high γ, low DR is achieved, and if we decrease γ, DR is increased. We set γ on a value where high DR and tolerable FPR are achieved. So, in this paper, γ is chosen to 0.1.

5.3 Effect of β on performance

In the proposed scheme, we have formulated different theft attacks using the parameter β. Table 6 shows the effect of β on detection performance under different attacks. We have selected five different pairs of β given as (0.1,0.9), (0.2,0.8),(0.3,0.7),(0.4,0.6) and (0.5,0.5). From Table 6, we observe that the proposed scheme detects theft attacks for different pairs of β with high DR.

5.4 Impact of principal components (PCs) on performance

In the proposed scheme, the underlying consumption patterns that repeat on a weekly basis are extracted using PCA. The proposed detection scheme is applied in a space span by the consumption of all consumers. We analysed the impact of number of PCs on detection accuracy. Table 7 shows the impact of PCs on detection

proposed method and the SVM-based theft detector is 77.34% and 59.92% for attack A1, 88.61% and 60.67% for attack A2, and 100% and 91.49% for attack A3 when FPR is 20%. Hence, we conclude that the proposed scheme detects all energy theft attacks with high DR as compared to SVM based theft detector with tolerable FPR.

We have also compared the performance of the proposed scheme with ARMA-GLR detector [18]. ARMA-GLR detector detects the electricity theft attacks with 67% DR when FPR is 28% [14], which is lower than the performance of our proposed scheme. Similarly, the performance of lower upper decomposition algorithm [13] based on P2P computing is bad for attack A2 and A3, while it detects attack A1 effectively with 96% DR and 9% FPR [14]. PCA-DBSCAN-based method [19] detects random scale attack with 84.9% DR but it did not perform good in the case of average attack. DR for average attack is only 8.1% and FPR for 36.3% consumers is also large. We implemented the PCA-DBSCAN method in our attack scenarios and tested its performance with ISSDA dataset. The DR of PCA-DBSCAN method with the proposed attacks in this paper is 64.26%, 71.52%, and 87.49% for attack $A1$, $A2$, and $A3$, respectively, which is lower than the proposed method. So, the proposed method outperforms

Table 7 Impact of PCs on detection performance

k	Variance, %	DR, %		
		Attack 1	Attack 2	Attack 3
2	55	60.81	49.08	100
14	70.6	71.93	83.01	100
22	75	77.56	88.61	100
54	85	85.43	95.30	100
336	100	88.17	99.95	100

accuracy. In Table 7, k represents number of PCs, second column shows the variance retained by PCs. First two PCs retains 55% of the total variance. If we choose number of PCs as 2, 14, 22, 54 and 336, DR is 49.08%, 83.01%, 88.61%, 95.30% and 99.95%, respectively, for $A2$ attack. Table 7 concludes that if the number of PCs is increased, DR also increased.

6 Conclusion

Energy theft is one of the key concerns in AMI. It causes billions of dollars per year financial loss to utility companies. In this paper, we have proposed a method based on PCA approximation to detect energy theft attacks in AMI. Energy consumption vector is transformed into a linear combination of a vector with uncorrelated component. With PCA approximation, dimensionality of high dimensional AMI data is reduced. Theft detection scheme is applied to a space span by the consumption of all consumers. To detect theft attacks, relative entropy is computed using reconstructed data and compared with the threshold.

We have tested the performance of the proposed scheme under different attack scenarios. Test results show that the proposed scheme detects attacks with high detection percentage. We have compared the performance of the proposed scheme with classification-based method like SVM. Test results show that the proposed scheme outperforms SVM. We have also analysed the effect of different parameters like γ and β on detection performance. Impact of number of principal components on detection accuracy is also analysed. Decreasing FPR in energy theft detection for AMI is our ongoing research.

7 References

[1] Wright, J.: 'Smart meters have security holes', 2010. Available at http://www.nbcnews.com/id/36055667#.Vd1Ifl96Uk
[2] Ward, M.: 'Smart meters can be hacked to cut power bills', October 2014. Available at http://www.bbc.com/news/technology-29643276
[3] Kulkarni, N.: 'Smart power', July 11, 2017. Available at http://www.thehindubusinessline.com/opinion/smart-power-metering-in-india/article9760558.ece
[4] Usmani, A.: 'Larsen and Toubro wins bid for Indias smart meter pilot project to cut utility losses', October 9, 2017. Available at https://www.bloombergquint.com/business/2017/10/09/lt-wins-bid-for-indias-smart-meters-pilot-project-to-cut-utility-losses
[5] McDaniel, P., McLaughlin, S.: 'Security and privacy challenges in the smart grid', *IEEE Secur. Privacy*, 2009, **7**, (3), pp. 75–77
[6] Lo, C.-H., Ansari, N.: 'Consumer: a novel hybrid intrusion detection system for distribution networks in smart grid', *IEEE Trans. Emerg. Top. Comput.*, 2013, **1**, (1), pp. 33–44
[7] McLaughlin, S., Holbert, B., Fawaz, A., *et al.*: 'A multi-sensor energy theft detection framework for advanced metering infrastructures', *IEEE J. Sel. Areas Commun.*, 2013, **31**, (7), pp. 1319–1330
[8] Khoo, B., Cheng, Y.: 'Using RFID for anti-theft in a Chinese electrical supply company: a cost-benefit analysis'. Wireless Telecommunications Symp. (WTS), New York City, NY, USA, April 2011, pp. 1–6
[9] Xiao, Z., Xiao, Y., Du, D.H.C.: 'Non-repudiation in neighborhood area networks for smart grid', *IEEE Commun. Mag.*, 2013, **51**, (1), pp. 18–26
[10] Amin, S., Schwartz, G.A., Tembine, H.: 'Incentives and security in electricity distribution networks'. Int. Conf. Decision and Game Theory for Security GameSec, Berlin, Germany, 2012, pp. 264–280
[11] Crdenas, A.A., Amin, S., Schwartz, G., *et al.*: 'A game theory model for electricity theft detection and privacy-aware control in AMI systems'. 2012 50th Annual Allerton Conf. Communication, Control, and Computing, Allerton, October 2012, pp. 1830–1837
[12] Angelos, E.W.S., Saavedra, O.R., Corts, O.A.C., *et al.*: 'Detection and identification of abnormalities in customer consumptions in power distribution systems', *IEEE Trans. Power Deliv.*, 2011, **26**, (4), pp. 2436–2442
[13] Salinas, S., Li, M., Li, P.: 'Privacy-preserving energy theft detection in smart grids: a p2p computing approach', *IEEE J. Sel. Areas Commun.*, 2013, **31**, (9), pp. 257–267
[14] Jokar, P., Arianpoo, N., Leung, V.C.M.: 'Electricity theft detection in AMI using customers consumption patterns', *IEEE Trans. Smart Grid*, 2016, **7**, (1), pp. 216–226
[15] Depuru, S.S.S.R., Wang, L., Devabhaktuni, V.: 'Support vector machine based data classification for detection of electricity theft'. Power Systems Conf. Exposition (PSCE), 2011, Phoenix, AZ, USA, March 2011, pp. 1–8
[16] Depuru, S.S.S.R., Wang, L., Devabhaktuni, V., *et al.*: 'A hybrid neural network model and encoding technique for enhanced classification of energy consumption data'. IEEE Power and Energy Society General Meeting, Detroit, MI, USA, July 2011, pp. 1–8
[17] Martino, M.D., Decia, F., Molinelli, J., *et al.*: 'Improving electric fraud detection using class imbalance strategies'. ICPRAM, Algarve, Portugal, 2012
[18] Mashima, D., Cárdenas, A.A.: '*Evaluating electricity theft detectors in smart grid networks*' (Springer, Heidelberg, Berlin, 2012), pp. 210–229
[19] Krishna, V.B., Weaver, G.A., Sanders, W.H.: '*PCA-based method for detecting integrity attacks on advanced metering infrastructure*' (Springer International Publishing, Cham, 2015), pp. 70–85
[20] Krishna, V.B., Lee, K., Weaver, G.A., *et al.*: 'F-DETA: a framework for detecting electricity theft attacks in smart grids'. 2016 46th Annual IEEE/IFIP Int. Conf. Dependable Systems and Networks (DSN), Toulouse, 2016, pp. 407–418
[21] Krishna, V.B., Gunter, C., Sanders, W.H.: 'Evaluating detectors on optimal attack vectors that enable electricity theft and DER fraud', *IEEE. J. Sel. Top. Signal. Process.*, 2018, **12**, (4), pp. 790–805
[22] Jolliffe, I.: '*Principal component analysis*' (Springer Verlag, New York, 2002)
[23] Cover, T.M., Thomas, J.A.: '*Elements of information theory*' (Wiley-Interscience, New York, USA, 2006)
[24] 'Irish social science data archive'. Available at http://www.ucd.ie/issda/data/commissionforenergyregulationcer/
[25] Singh, S.K., Bose, R., Joshi, A.: 'Entropy-based electricity theft detection in AMI network', *IET Cyber-Phys. Syst., Theory Appl.*, August, 2017, **3**, (2), pp. 99–105
[26] Principal Component Analysis. 2017. Available at https://in.mathworks.com/help/stats/pca.html
[27] Singh, S.K., Khanna, K., Bose, R., *et al.*: 'Joint transformation based detection of false data injection attacks in smart grid', *IEEE Trans. Ind. Inf.*, 2018, **14**, (1), pp. 89–97
[28] Fawcett, T.: 'Roc graphs: notes and practical considerations for researchers', Tech. Rep., 2004
[29] Zweig, M.H., Campbell, G.: 'Receiver-operating characteristic (roc) plots: a fundamental evaluation tool in clinical medicine', *Clin. Chem.*, 1993, **39**, (4), pp. 561–577