The l0th International Conference on Control, Automation and Information Sciences
Xi'an, China - October 14-17, 2021

Non-Intrusive Load Monitoring based Demand Prediction for Smart Meter Attack Detection

Nahal Iliaee
Departement of Electronics
Carleton University, Ottawa, Canada
NahalIliaee@cmail.carleton.ca

Shichao Liu
Department of Electronics
Carleton University, Ottawa, Canada
shichaoliu@cunet.carleton.ca

Wei Shi
School of Information Technology
Carleton University, Ottawa, Canada
wei.shi@carleton.ca

***Abstract*— The global implementation of smart meters that measure and communicate residential electricity consumption has resulted in the creation of new energy efficiency services such as automated energy management systems and billing systems. In view of the vulnerability of smart meters to cyber and physical attacks, this research presents a short-term load prediction method that uses energy disaggregation, to detect the False Data Injection (FDI) attack on smart meters. This method is constructed of an edge detection based Non-Intrusive Load Monitoring (NILM) module for energy disaggregation and a load forecaster. In the first step, we attempt to determine when the appliances are switching on/off. Second, the acquired switching events would be utilized as an input for machine learning algorithms including Support Vector Regression (SVR) and Elman Neural Network (ENN) to improve performance of the load forecaster for detecting FDI attacks. Validation of the results based on the data collected from twenty actual UK houses has indicated that the recommended method is a great solution for detecting cyberattacks on residential smart meters.**

Keywords— Non-Intrusive Load Monitoring, load forecasting, FDI attacks, Support Vector Regression, Elman Neural Network

I. INTRODUCTION

Due to the digitalization initiatives of the energy sector, smart meters are currently rolled out in the electricity market whose extensive deployment represents the first step into digitalization solutions for many utilities. Smart meters record the consumption behavior of the end-users with a much higher resolution than classical electricity meters, such as in a minute time scale and second time scale [1-3]. The data can be utilized for automated energy management systems to profile high-energy-consumption equipment, allowing them to create energy-saving techniques like rescheduling high-power-demanding processes for off-peak hours. However, digital smart meters and communication-based smart meter networks are vulnerable to cyber attacks. For instance, the U.S. Federal Bureau of Investigation reported an organized energy theft attempt against AMI which could cost a utility company up to $400 M annually in 2009 [4]. Advanced innovations that can accurately detect cyberattacks on smart meter and their networks are in urgent need.

Although still being in the infant, securing smart meters against cyberattacks has attracted increasing attentions in the past decades due to its significant importance. Advanced encryption [5] and authentication [6] have been presented to secure the smart meter data. However, it has been found that these cryptographic technologies alone may not be sufficient for fully sustaining the security of smart meters [7]. Innovative intrusion detection systems that can monitor the data and detect malicious behaviors in real-time or near real-time fashion are critical and needed to add another defense layer for securing smart meter data record and storage [8]. For example, a collaborative intrusion detection mechanism was proposed against false data injection (FDI) attacks for smart meters with the consideration of constrained computation and storage capacities of smart meters [9]. In [10], a model-based intrusion detection mechanism as well as a machine learning-based intrusion prevention system was designed to protect the network against various cyberattacks on ZigBee-based Home Area Networks (HANs). While these methods are promising, they could be vulnerable to insider attacks which might be conducted by authorized personnel such as current and/or former employees [11]. In [12], customers' consumption patten is used for detecting energy theft. This work is exciting, although it focused on protecting a network of smart meters and not on single residential smart meter.

In this paper, we present a Non-Intrusive Load Monitoring (NILM) based electricity consumption prediction for detecting FDI attacks on smart meters of residential homes. NILM is the procedure of disaggregating electrical loads by just examining appliance-specific power consumption signatures within aggregated load data measured by a smart meter through a variety of signal processing or pattern recognition techniques [13-15]. It is worth mentioning that this method is considered to be non-intrusive as it avoids any equipment installed inside the user's house. Attackers may be able to compromise the smart meter via physical or cyber interferences. This study applies an edge detection based NILM for load disaggregation, to find when an appliance is turned on/off based on the edges and each device's load signatures. Second, the load disaggregation method is combined with machine learning algorithms to enhance load pattern forecast. The NILM extract the individual load patten from the available historical aggregated load data and these new appliance-specific load pattens increase the training data window for the forecaster and achieve a significant enhancement for its prediction performance. Then, a detailed analysis and comparison of two forecasting algorithms including Support Vector Regression (SVR) and Elman Neural Network (ENN) based on the load disaggregation. At the end, the proposed NILM based electricity consumption prediction is applied to detected FDI attacks on smart meters of residential homes.

The rest of the paper is organized as below: Section II describes the energy disaggregation system based on edge detection and the short-term load forecasting methods including SVR and ENN. Section III apply the proposed NILM based electricity consumption prediction to detect FDI attacks. Finally, we conclude in Section IV.

II. NON-INTRUSIVE LOAD MONITORING BASED DEMAND PREDICTION

The basic concept of the algorithm is to automatically break down the total power usage to device level by utilizing data collected from the smart electricity meter and then forecast the loads for the next days. In the following sections, we will first define the general idea and concept of the NILM

2021 International Conference on Control, Automation and Information Sciences (ICCAIS) | 978-1-6654-4029-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCAIS52680.2021.9624524

algorithm based on edge detection and then the description of how to estimate the load of the next day is provided.

A. NILM Algorithm

The consumption of power in a household varies over time depending on how particular devices are employed by the occupants. The change in electricity consumption due to the operation of the devices is represented by the difference in real power (dP). The key concept of this algorithm is to utilize these differences (dPs) to recognize device-switching events in the load curve based on an appliance signature database.

To begin, we locate time points in the load curve where major changes between two levels of power consumption occur. Then, once an edge has been detected, the differences in various physical variables between these subsequent stages were computed, and then the shift as a possible appliance-switching event was identified. Finally, we compare each of these changes to a known set of differences from an appliance signature database, then we map the edge to a specific device based on its load characteristics. Fig .1 illustrates the overview the algorithm. The above-mentioned steps are explained specifically in this section:

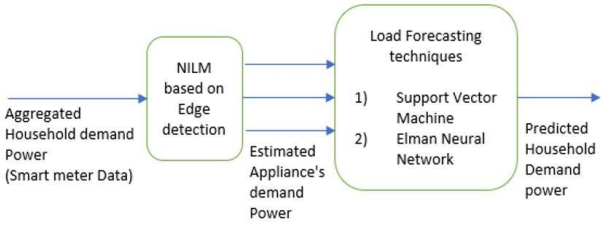

Fig. 1. Block diagram for the NILM load forecasting technique.

- Edge Detection

The apparent power was utilized as an input vector to find edges in the recorded electricity consumption data that correspond to the appliance switching events in this study. The proposed algorithm computes the absolute values of the differences in the apparent power between two consecutive values in the data series. If the absolute value of a difference is greater than a pre-defined threshold, the value may be considered an edge. However, there can be much more potential edges than appliance-switching events which would result in a high number of spurious events. The use of a smoothing filter can aid in the removal of these false detections. In order to decrease the number of spurious events, we tested a median filter. It is worth mentioning that the most significant positive point of the median filter is the ability to remove outliers. In this study utilizing a median filter decreases the number of potential edges significantly without missing a true device-switching event.

- Power Level and Delta Level

The next stage is to extract power levels that connect two edges in the smoothened signal after the relevant edges have been found. The algorithm retrieves the delta vectors that are used to match the edge to a specific device from two consecutive power levels separated by an edge.

- Recognition and Labeling

The algorithm's recognition section tries to match known appliance signatures from the signature database with delta vectors extracted in the previous phase. First, the algorithm calculates the Euclidean distance in the two-dimensional vector space. If this is less than a pre-determined length of value plus an oscillation value, a potential match is found. The oscillation term is the length of a vector with the first component being the maximum of the standard deviation in real power at level x or x+1. Following that, each distance is connected with a collection of possible recognition candidates from the signature database. It is worth noting that this set of possible associated recognitions could be empty as well. The relevant distance, in this case, could not be linked to a known signature. This could be caused by a detected edge that does not correspond to an appliance switching event, or by the database not having a corresponding signature that matches distance. Second, the nearest neighbor match is done on all potentially matching distances that have been connected with the appliance. Finally, the algorithm labels the load profile with the device names that correspond to it. The schematic of the steps is shown in Fig .2.

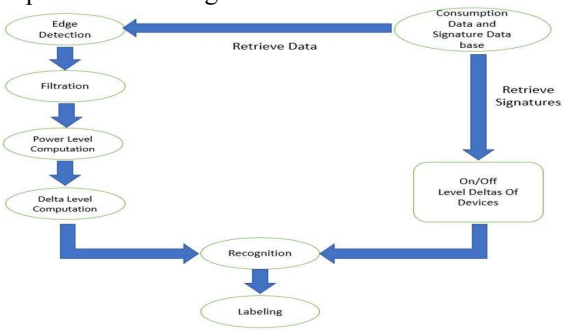

Fig. 2. Overview of the steps of the proposed NILM algorithm.

B. Short Term Load Forecasting

Support Vector Regression (SVR) and Elman Neural Network (ENN) were employed for a short-term load forecasting goal in this work. For better energy management and demand-side management, load forecasting for households must be combined with energy disaggregation methods.

In machine learning, Support Vector Regressions (SVR) are considered as supervised learning models that uses an algorithm to identify the relationship between dependent and independent variables. The purpose of the SVR [16] algorithm for the linear case is to find a linear regression function that is as flat as possible while best approximating the actual output vector y with an error tolerance ε. However, linear function approximation is of limited practical use in most real-world problems. The solution is to map the input data into a higher-dimensional feature space where the training data may be linear, and then perform linear regression in this feature space. The following convex optimization problem can be represented as a solution to the regression problem for the linear case:

$$\begin{cases} \min \frac{1}{2}\sum_{i,j=1}^{N}(\alpha_i-\bar{\alpha}_i)\left(\alpha_j-\bar{\alpha}_j\right)\langle x_i.x_j\rangle + \\ \quad \varepsilon\sum_{i=1}^{N}(\alpha_i+\bar{\alpha}_i)-\sum_{i=1}^{N}y_i(\alpha_i-\bar{\alpha}_i) \\ S.t\sum_{i=1}^{N}(\alpha_i-\bar{\alpha}_i) \quad 0\le\alpha_i\le c\ \ \forall i \\ \qquad\qquad\qquad\quad 0\le\bar{\alpha}_i\le c\ \ \forall i \end{cases} \tag{1}$$

where $\langle x_i . x_j \rangle$ is the inner product of x_i and x_j. In addition, α_i and $\bar{\alpha}_i$ are Lagrange multipliers.
Therefore, the approximate function can be expressed as:

$$f(x_i) = \sum_{i,j=1}^{N} (-\alpha_i + \bar{\alpha}_i) \langle x_i . x_j \rangle + b \quad (2)$$

The data about the inside of the ε-insensitive tube is represented by the values $(-\alpha_i + \bar{\alpha}_i)$, which are zero. As a result, the final decision function only considers the remaining nonzero coefficients of $(\alpha_i + \bar{\alpha}_i)$ and the data with nonzero Lagrange multipliers are referred to as support vectors. As a result, support vectors are made the definition of the approximate function, while other data can be considered redundant. Finally, we may rewrite the approximate function as follows:

$$f(x_i) = \sum_{i=1}^{N} (\alpha_k + \bar{\alpha}_k) \langle x_i . x_j \rangle + b \quad (3)$$

$$k = 1,2, \dots N$$

where x_k denotes the support vector and N denotes the total number of support vectors.

Elman introduced the ENN, a simple recurrent neural network, in 1990 [17]. This network has three layers: an input layer, a hidden layer, and an output layer. It is analogous to a three-layer feed-forward neural network in this regard. It does, however, include a context layer that feeds back the hidden layer outputs from previous time steps. The neurons in each layer are used to transfer information from one layer to the next. The following is the dynamics of the change in hidden state neuron activation in the context layer [18,19]:

$$S_i(t) = g\left(\sum_{k=1}^{K} V_{ik} S_k(t-1) + \sum_{j=1}^{J} W_{ij} I_j(t-1)\right) \quad (4)$$

where $S_k(t)$ and $I_j(t)$ denote the output of the context state and input neurons, respectively; V_{ik} and W_{ij} denote their corresponding weights, and $g()$ is a sigmoid transfer function.

Fig. 3 shows a simple structure of an ENN. As can be seen, the context neurons receive input from the hidden layers and pass their output to the hidden layers. The context layers always store the output from the hidden layer and relay this information in the next iteration. This behavior allows them to form a sort of short-term memory.

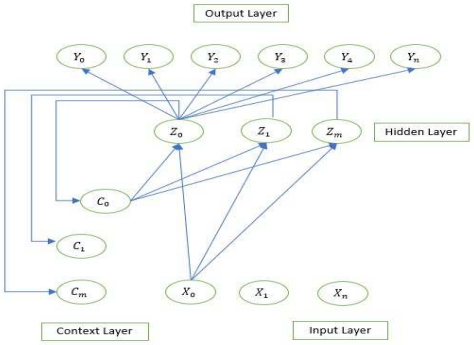

Fig. 3. The architecture of Elman Naural Network

III. Application in Smart Meter Attack Detection

The energy consumption of each household must be available to apply Energy Disaggregation (ED) to improve household forecasting performance. As a result, the UK dataset for 20 households [20] was employed. This is one of the first publicly available datasets collected primarily to promote ED research. The REFIT electrical load measurements dataset includes whole-house aggregate loads and nine individual appliance measurements at 8-second intervals per house, the data collected continuously from 20 houses over a two-year period. During the monitoring, the occupants went about their daily activities. In this work, we will concentrate on only household number one. Table. I sums up the appliances in the first house and their real power consumption range measured by separate energy sensors.

TABLE. I. Details of House #1 Appliances

Appliances	Range of consumptions (*W*)
Fridge (Hot Point)	12-2056
Freezer (Beko)	21-1071
Freezer (Unknown)	66-1094
Washer dryer (Creda)	10-2710
Washing Machine (Beko)	10-2664
Dish Washer (Bosch)	30-2525
Computer (Lenovo)	23-58
Television Site (Toshiba)	57
Electric Heater (GLEN)	1-2076

A. On/Off Status Detection of Applicances

The first objective of the experiment is to identify when the devices are on/off. During the experiment, the algorithm successfully detected the on/off events of all devices except the Electric Heater. This can be explained that the electric heater is considered as controllable load and is always on during the experiment. The maximum number of appliances that are working together is three. In addition, we use the lowest boundary to ensure that the algorithm recognizes the edges accurately because sometimes the median filter may cancel the actual small changes [21]. The daily data is sampled per 10 minutes. The real power consumption for one day and the detected switching events before and after applying the median filter is shown in Fig. 4.
As can be seen in Fig.4 utilizing a median filter reduces the number of potential edges by up to 70% without missing a true device-switching event. In addition, Fig. 5 provides an overview of the identified devices that are operating simultaneously.

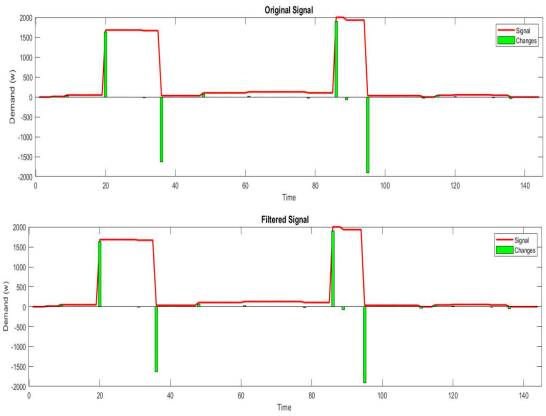

Fig. 4. Detected switching events for aggregated data during one day before and after the implementation of the median filter

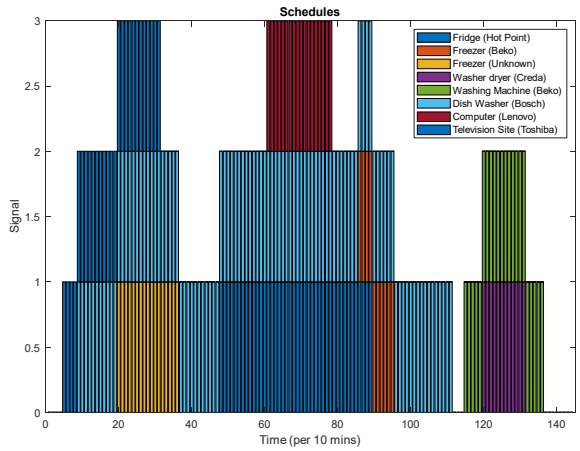

Fig. 5. Operation period and switching time of each appliance

B. SVR and ENN Based Load Predictions

Given this initial response from the NILM algorithm, we combined supervised machine learning algorithms to forecast the next 24 hours consumption and their switching events. In this study, the Support Vector Regression is utilized as the first forecaster. We implement 70% of the data from the first three days for training and 30% for evaluation. Because the linear SVR method is used, the linear kernel function is implemented. Besides, ε is set 7.0423 with the bias of 6.4197.

Elman Neural Network is employed as the second forecaster to compare with SVR. The Elman Neural network uses 8 input nodes, 10 hidden layers, and 8 output nodes to forecast aggregated power demand and each appliance's switching demand for one day ahead. These input data are inputs from the disaggregation stage as well as inputs from the aggregated demand of the home for the current and previous hours of historical data for a total of 144 reduced scenarios. These eight inputs nodes represent the load changes for the eight major appliances listed in table 1. Fig.6 shows training vectors for both SVR and ENN.

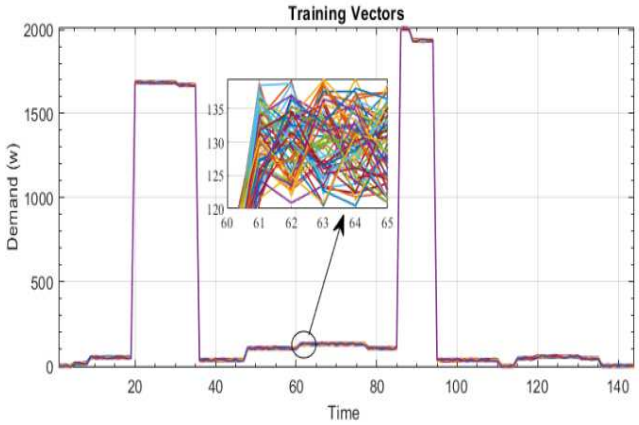

Fig. 6. Training vectors for SVR and ENN

Fig.7 show the actual load and forecasted load for the first home using SVR and ENN methods. The metrics root mean squared error (RMSE) are used to assess the performance of the proposed methods in forecasting residential household demand. This metrics describe the performance of the forecaster. The RMES is useful for calculating average error while taking error direction into account. In other words, regardless of the direction of the error, the RMSE can provide an estimate of the average error between the predicted and actual signal. The formula for RMSE metrics is as below:

$$RMSE = \sqrt{\frac{\sum_{i=1}^{N}(\hat{y}_t - y_t)^2}{N}} \quad (5)$$

where $\hat{y}_t$ denotes the estimated output, y_t denotes the actual output, and N denotes the number of data points.

Fig. 8 and Fig. 9 show the performance of the SVR and ENN according to the RMSE metrics. The results show that ENN outperforms SVR. However, it is worth mentioning that the training time for the ENN is almost double the training time of the SVR due to the feedback input in the context layer.

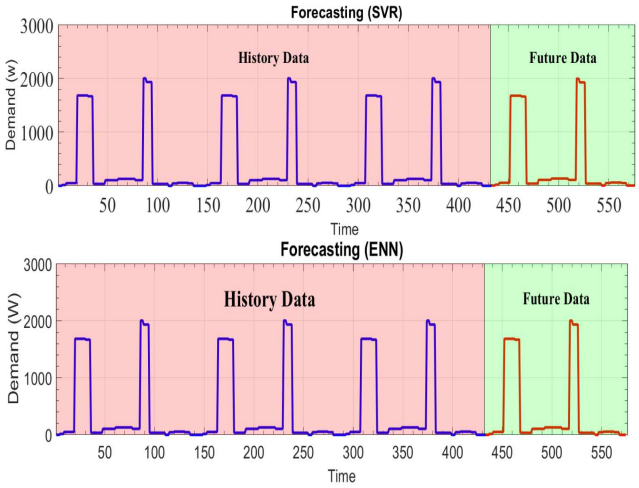

Fig. 7. Next day load forecasting via SVR and ENN

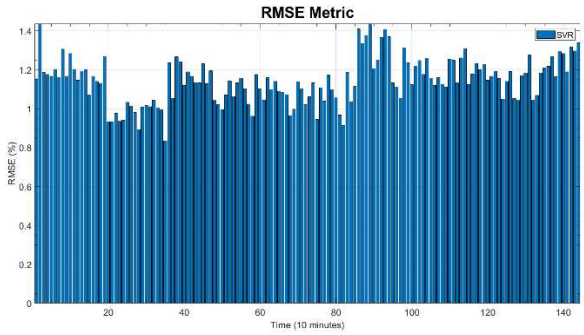

Fig. 8. RMSE metrics for SVR

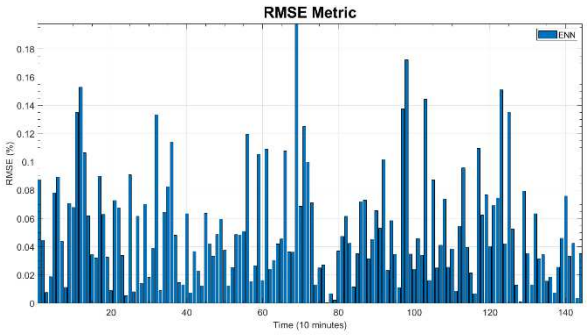

Fig. 9. RMSE metrics for ENN

C. Application for FDI Attack Detection in Smart Meter

Although FDI attacks can modify the smart meter data via physical or cyber interferences. However, it is difficult to attack appliance-specific power consumptions as there are not submeters installed due to NILM is used in this work. The

entire home load predication is done via NILM and therefore it will be resilient to cyberattacks. A pre-defined RSME threshold (RMSE=1.5 for SVR) can be used to detect malicious meter data. Three FDI attack cases are considered. Case 1: meter data from time step 25 to 35 are modified to a constant 200 *W; Case 2*: meter data from time step 65 to 77 are modified to a constant 2000 *W;* Case 3: meter data from time step 85 to 95 are modified to random integers within [0, 1000] *W.* Fig. 10 illustrates the effectiveness of FDI attack detection by applying the SVR based load predictions on disaggregated appliance-specific data.

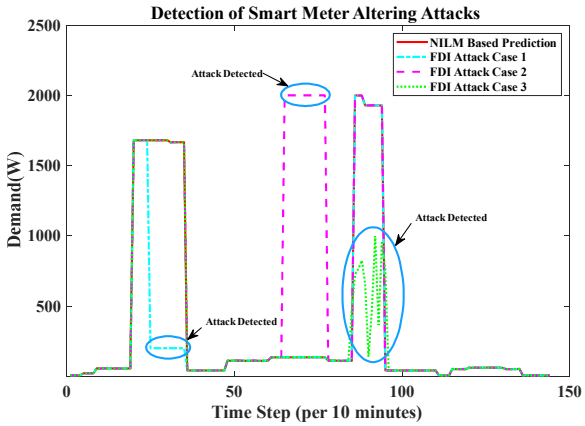

Fig. 10. Detection of FDI attacks on smart meter data

IV. CONCLUSION

To detect cyberattacks on residential smart meters, we present a load disaggregation-based energy consumption prediction method that allows for automatic recognition of electric appliance switching events and forecasting the load demand based on the predicted appliances' on/off statuses. Compared to the prediction without energy disaggregation, the NILM extract the individual appliance consumption patten from the aggregated load data and these new appliance-specific load pattens increase the training data window for the forecaster and improve its prediction performance. Support vector regression (SVR) and Elman neuro network (ENN) are used to perform house energy forecast for detecting FDI attacks. Case studies on the obtained metering data of UK households verify the effectiveness of the load disaggregation-based demand prediction for detecting FDI attacks on smart meters.

REFERENCES

[1] Y. Wang, Q. Chen, T. Hong and C. Kang, "Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges," IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3125-3148, May 2019

[2] R. Davies, "Hydro one's smart meter initiative paves way for defining the smart grid of the future," 2009 IEEE Power & Energy Society General Meeting, 2009, pp. 1-2.

[3] F. L. Quilumba, W. Lee, H. Huang, D. Y. Wang and R. L. Szabados, "Using Smart Meter Data to Improve the Accuracy of Intraday Load Forecasting Considering Customer Behavior Similarities," in IEEE Transactions on Smart Grid, vol. 6, no. 2, pp. 911-918, March 2015

[4] FEDERAL BUREAU OF INVESTIGATION. (2010) Cyber intelligence section: Smart grid electric meters altered to steal electricity.[Online].https://krebsonsecurity.com/2012/04/fbi-smartmeter-hacks-likely-to-spread/

[5] Z. Wan, G. Wang, Y. Yang and S. Shi, "SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids," IEEE Transactions on Industrial Electronics, vol. 61, no. 12, pp. 7055-7066, Dec. 2014

[6] Y. Yan, Y. Qian and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," 2011 IEEE Wireless Communications and Networking Conference, 2011, pp. 909-914

[7] N. Saxena, B. J. Choi and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 907-921, May 2016

[8] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang and X. S. Shen, "Differentially Private Smart Metering With Fault Tolerance and Range-Based Filtering," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2483-2493, Sept. 2017

[9] X. Liu, P. Zhu, Y. Zhang and K. Chen, "A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure," IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2435-2443, Sept. 2015

[10] P. Jokar and V. C. M. Leung, "Intrusion Detection and Prevention for ZigBee-Based Home Area Networks in Smart Grids," in IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1800-1811, May 2018

[11] Z. Liu and L. Wang, "Defense Strategy Against Load Redistribution Attacks on Power Systems Considering Insider Threats," IEEE Transactions on Smart Grid, vol. 12, no. 2, pp. 1529-1540, March 2021

[12] P. Jokar, N. Arianpoo and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns," in IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 216-226, Jan. 2016,

[13] Zoha, Ahmed, Alexander Gluhak, Muhammad Ali Imran, and Sutharshan Rajasegarar. "Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey." Sensors 12, no. 12 (2012): 16838-16866.

[14] Hart, George William. "Nonintrusive appliance load monitoring." Proceedings of the IEEE 80, no. 12 (1992): 1870-1891.

[15] Norford, Leslie K., and Steven B. Leeb. "Non-intrusive electrical load monitoring in commercial buildings based on steady-state and transient load-detection algorithms." Energy and Buildings 24, no. 1 (1996): 51-64.

[16] Clarke, Stella M., Jan H. Griebsch, and Timothy W. Simpson. "Analysis of support vector regression for approximation of complex engineering analyses." (2005): 1077-1087.

[17] Elman, Jeffrey L. "Finding structure in time." Cognitive science 14, no. 2 (1990): 179-211.

[18] Chandra, Rohitash, and Mengjie Zhang. "Cooperative coevolution of Elman recurrent neural networks for chaotic time series prediction." Neurocomputing 86 (2012): 116-123.

[19] Cacciola, Matteo, Giuseppe Megali, Diego Pellicanó, and Francesco Carlo Morabito. "Elman neural networks for characterizing voids in welded strips: a study." Neural Computing and Applications 21, no. 5 (2012): 869-875.

[20] Murray, David, Lina Stankovic, and Vladimir Stankovic. "An electrical load measurements dataset of United Kingdom households from a two-year longitudinal study." Scientific data 4, no. 1 (2017): 1-12.

[21] Weiss, Markus, Adrian Helfenstein, Friedemann Mattern, and Thorsten Staake. "Leveraging smart meter data to recognize home appliances." In 2012 IEEE International Conference on Pervasive Computing and Communications, pp. 190-197. IEEE, 2012