INTELLIGENT TECHNIQUE FOR ELECTRICITY THEFT IDENTIFICATION USING AUTOREGRESSIVE MODEL

[1*] ABDULLATEEF, Ayodele Isqeel, [2] SALAMI, Momoh-Jimoh Eyiomika,
[1] AKOREDE, Mudathir Folohunso
[1,3]Department of Electrical and Electronics Engineering, University of Ilorin, Ilorin, Nigeria
[2]Dangote Foundation, Lagos, Nigeria
*Corresponding author's e-mail address: abd_lateef.aii@unilorin.edu.ng

ABSTRACT:

Various studies have investigated electricity theft, an illegally act, perpetrated to the detriment of the electricity power providers, however, less attention has been given to identification of the types of electricity theft. Data were acquired from the Consumer Load Prototype developed at two different levels using Sensor-A connected to the Pole Terminal Unit and Sensor-B connected to the Consumer Terminal Unit. The output of the sensors were connected to BNC-2110 device and linked to the PCI 6420E channel, which log the data in the computer for further analysis. LABVIEW (2012) software was programmed to acquires data at a sampling frequency of 500Hz and decimated at 10s interval before logging into the computer hard disk. The feature extraction of the data acquired was achieved using autoregressive technique and model order selectionwas based on minimum description length. The model coefficient AR (20), data acquired and predicted data were used for theft identification. Meter-bypassing theft was identified when the energy consumption from sensor A and sensor B are different, however sensor B reads zero value and there are disparities in the model coefficients. Illegal connection before the meter theft was identified whenever there is difference in energy consumption as evaluated form sensor A and sensor B and there is no zero value recorded from sensor B, while Meter tampering was detected when the energy consumption as evaluated form sensor A and sensor B are different and there are no disparities in the model coefficients.

Keywords: Autoregressive technique, Distribution network,Electricity theft identification, Model coefficients

INTRODUCTION

Electricity theft, which is the illegal consumption of electricity without the company's authorization or consent, is a major problem facing power distribution companies worldwide. The actis perpetrated, mainly, to reduce the amount of electricity consumption charges payable to power providers. Itoccurs on the distribution networks that link the consumers. Electricity theft include billing irregularities, meter tampering and unpaid bills [1]. It has caused huge losses of revenue to the power provides on one hand while cases of loss of lives on the part of the perpetrators have been reported[2-6]. Electricity theft is a global phenomenon with high prevalence in most developing world and this may be attributed to low technical know-how in monitoring of the consumers on the power distribution networks[7].

Several methods of detecting and estimation of electricity theft that have been proposed and developed by various researchers [8-12], focused, majorly, onthe detection of illegal consumers based on difference between power consumed at the pole and at the consumer end. Automatic meter reading system incorporated with tampering detection and various communication media such as Global System for Mobile Communications (GSM) and Zigbee, have been proposed to track electricity theft [13-15]. Similarly, Nagi, et al. [16], Wang and Devabhaktuni [17] and Nizar and Dong [18] have reported the application of Artificial Intelligent System (AIS) such as Support Vector Machine (SVM) for the detection of electricity theft based on the energy consumption pattern of the consumer.

In addition, the power line impedance technique considers the difference between network impedance and installed impedance which indicates electricity theft location with respect to the location of legitimate consumer was proposed by Pasdar and Mirzakuchaki [19]. Bandim, et al.[20] proposed a Central Observer Meter (COM) to monitor and identify the perpetrators while the method proposed by Cavdar [12], uses two energy meters to track illegal connection. Meter tampering detection based on changes between live and neutral currents as well as voltage monitoring at the meter input terminals to depict electricity theft has been proposed by Naiman, et al. [21]. The injection of unwanted harmonics into the distribution network to cause damage to the appliances of the suspected illegal users was proposed by Depuru et al., [22]. Genuine consumers were identified and isolated from the electricity grid before the harmonics is injected. Similarly, Bat-Erdene et al. [11] incorporated a smart resistance in smart meter as a mode of detecting illegal electricity usage. Theft is detected by comparison between the main energy meter located at the substation and the consumers' smart meter.

Other studies that attempted the identification of theft was based on consumers' data, yet the theft activities were not classified. In the light of this, this study considers that classification of electricity

theft will provide a technical basis to know which types of theft being carried out by the perpetratorsis prevalent and how to concentrate on finding solution to it.

Model Coefficient Feature Extraction

The coefficients of the data used were extracted using linear prediction technique, which is a time series technique that has been applied in the analysis of speech signal, image processing, electroencephalogram (EEG) analysis and in communication [23-26]. The coefficients of a forward linear predictor are determined by minimizing the prediction error and the current value of the time series *y(n)* is expressed linearly in terms of its previous values and a white noise *x*(n) such that

$$y(n) = -\sum_{k=1}^{p} a_k y(n-k) + x(n) \tag{1}$$

wherea_1, . . . , $a_p$are the coefficients or weights to be determined, p is the model order and x(n)isthe white noise with zero mean and variance σ^2. In the same manner, equation 1 is also referred to a "forward prediction". The acquired data was subjected to AR modelling in order to extract the relevant feature that best represent the actual data. To achieve this, the data, represented as $y(n)$, in equation 1. Many techniques for the estimation of a_k such as Covariance, Burg, Least Square and Autocorrelation have been used to estimate the coefficients of AR model [27]. However, in this study, autocorrelation technique that is based on Yule-Walker equation is adopted. If the predicted consumer power consumption is defined as:

$$\hat{y}(n) = -\sum_{k=1}^{p} a_k y(n-k) \tag{2}$$

Then prediction error, $e(n)$ which is the difference between the value of $y(n)$ and its estimated value $\hat{y}(n)$ estimated value is expressed as:

$$e(n) = y(n) - \hat{y}(n) \tag{3}$$

Thus, a_k is found by minimizing the error based on the assumption that $y(n)$ is windowed such that $y(n) = 0$ for n < 0 and n >N where N is the data length. This gives rise to normal equation expressed as:

$$\sum_{k=1}^{p} a_k r_{yy}(l-k) = -r_{yy}(l) \quad ; \quad l = 1, 2, \ldots p \tag{4}$$

where

$$r_{yy}(l) = \sum_{n=l}^{N} y(n) y^*(n-l) \; l \geq 0$$

$$\varepsilon_p = r_{yy}(0) + \sum_{l=1}^{p} a_l \, r_{yy}^*(l) \tag{5}$$

Equation (5) is also called Yule-Walker equations [27, 28].

$$\begin{bmatrix} r_{yy}(0) & r_{yy}(-1) & r_{yy}(-2) & \ldots & r_{yy}(p-1) \\ r_{yy}(1) & r_{yy}(0) & r_{yy}(-1) & \ldots & r_{yy}(p-2) \\ . & . & . & & . \\ . & . & . & \ldots & . \\ . & . & . & & . \\ r_{yy}(p-1) & r_{yy}(p-2) & r_{yy}(p-3) & \ldots & r_{yy}(0) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ . \\ . \\ . \\ a_p \end{bmatrix} = - \begin{bmatrix} r_{yy}(1) \\ r_{yy}(2) \\ . \\ . \\ . \\ r_{yy}(p) \end{bmatrix} \tag{6}$$

The AR coefficient can be estimated from autocorrelation sequence by solving Eq (6) using methods such as Burg method and Levinson Durbin algorithm however, the latter is computationally effective and used.

AR Model Order Selection

One of the challenges in time series prediction and modelling is estimation of optimum model order, which is essential for using parametric model. Generally, the estimation of the model order is based on methods, which incorporate a penalty function that increases with the model order. These methods include but not limited to Final Prediction Error (FPE), Akaike Information Criterion (AIC), Hannan-Quinn Information Criterion (HQC) and Schwaez Information Criterion (SIC).

Final Prediction Error Technique

The final prediction error (FPE) is a technique of selecting the model order by minimising the variance of the prediction error. FPE selects the system model order so that the average error variance for a one-step prediction is minimised [29, 30] and this is expressed as

$$FPE(p) = \sigma_p^2 \left(\frac{N+p}{N-p} \right) \tag{7}$$

where σ_p^2 is the estimated error variance of the model, N is the number of data points, and p is the model order.

When the sample mean is subtracted from the signal then Equation (7) is adjusted as

$$FPE(p) = \sigma_p^2 \left(\frac{N+p+1}{N-p-1} \right) \tag{8}$$

And the variance is expressed as

$$\sigma_p^2 = \frac{1}{N} \sum_{n=1}^{N} \varepsilon_p^2(n) \qquad = 1, 2, 3, \ldots N) \tag{9}$$

where the error is

$$\varepsilon_p = x_p(n) - \tilde{x}_p(n)$$

If F is the maximum model order that could be obtained, evaluating p from 1 to F increases the model orders Equation (9) and this increases the uncertainty of the estimate of the predicted error variance. The optimum model order is the one that gives the minimum value of FPE (p), $1 \leq p \leq F$.

Akaike Information Criterion

The Akaike Information Criterion (AIC) is expressed, mathematically, as

$$AIC(p) = NIn(\sigma_p^2) + 2p \quad (10)$$

The term '2p' represents the penalty for higher order selection that does not change in substantial reduction in the prediction error variance of the model. The inconsistency in model order estimation under this method has been reported by Kashyap and Chellappa [31], although, it is popularly used in model estimation. The performance of FPE and AIC model order selection methods is similar; however, AIC method is recommended for short data [32].

Hannan and Quinn Criterion

Hannan and Quinn criterion technique that counteracts the over fitting nature of AIC. It is expressed as

$$HNQ(p) = ln(\sigma_p^2) + \frac{2pIn(InN)}{N} \quad (11)$$

Minimum Description Length

Minimum description length (MDL) was developed to correct the inconsistency associated with the FPE and AIC methods and is represented mathematically as

$$MDL(p) = NIn(\sigma_p^2) + pIn(N) \quad (12)$$

This increases the penalty factor incurred by using higher order as compare to AIC, thus favouring the selection of lower model order and it has been proven to be consistent statistically [29, 33]. The detail model order selection has been reviewed [34].

METHODOLOGY

Data acquisition and Processing

The data used in this study was acquired from the Consumer Load Prototype (CLP) developed[35] and the prototype presents real time information rather than software simulation, which has hitherto been used in the study of electricity theft.Electrical appliances such as refrigerator, incandescent bulb, fluorescent lamp, table fan, electric kettle, induction cooker, microwave oven and electric iron, which represent typical consumer loads connected to distribution network, were connected to the prototype at a schedule time. The consumer load data was acquired at two different levels using current sensors (ACS785, Allegro MicroSystem Inc., USA), in order to identify the type of theft. The Pole Terminal Unit (PTU) is represented by Sensor-Aand the Consumer Terminal Unit (CTU) or energy meteris represented by Sensor-B (Figure 1).The output of the sensors were connected to BNC-2110 device (National Instrument, USA) and linked to the PCI 6420E channel, which log the data in the computer for further analysis.

LABVIEW (2012) software was programmed to acquires data at a sampling frequency of 500Hz and decimated at 10s interval before logging into the computer hard disk. This was carried out due to the limitation of the software, which makes the buffer of the PCI 6420E card; fill up when sampled at a lower frequency**.** Moreover, sampling at a lower frequency would make the sampled data almost the same without extracting any meaningful information. The complete schematic diagram of the experimental setup is illustrated in Figure 1 while the LABVIEW screen shot for the monitoring of consumer load acquisition code is shown in Figure 2.

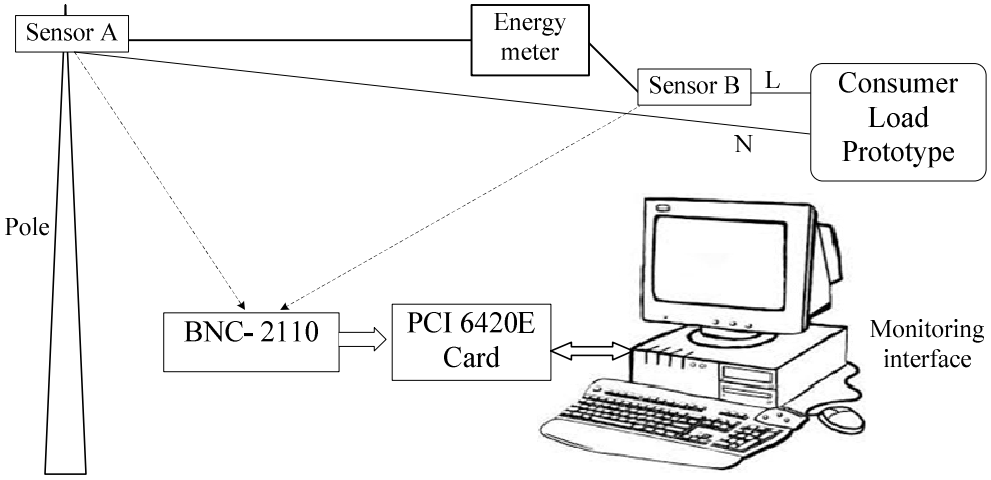

Figure 1: Schematic Diagram of Experimental Set Up

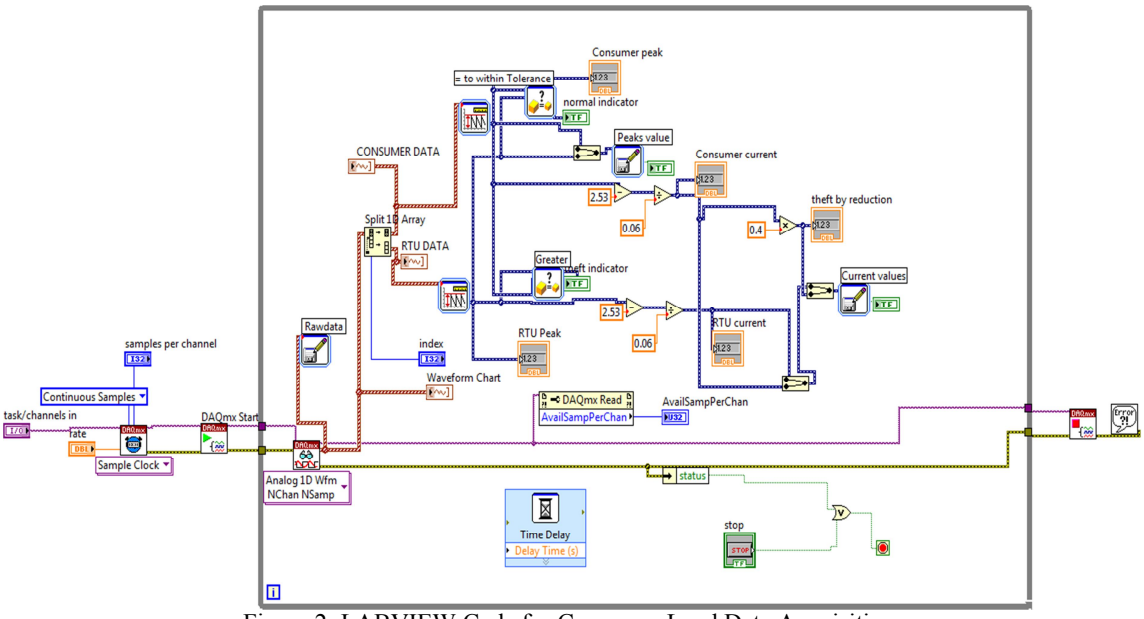

Figure 2: LABVIEW Code for Consumer Load Data Acquisition

Electricity Theft Cases and Data Profiling

Case A: Illegal connection before the meter

This type of theft involves connection of the load before the energy meter and was realized by either connecting the load directly to the fuse input (Figure 4a) or to a bare conductor meant for such purpose (Figure 4b).

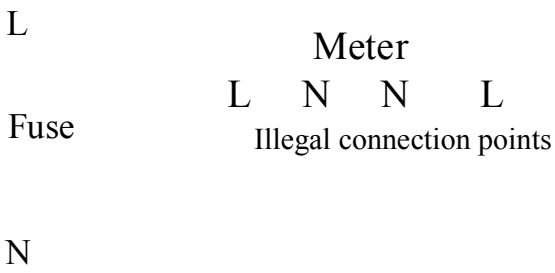

Figure (a)

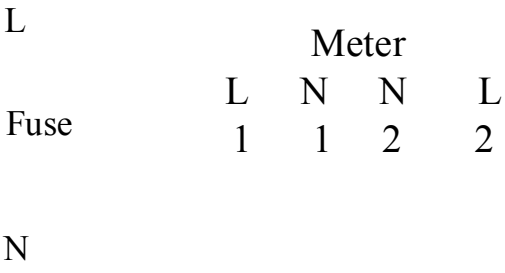

Figure (b)

Figure 4

Case B: Bypassing the Energy Meter

Energy meter bypassing was represented by connecting two cables to one end of the sensor (live output terminal); one out of these cables was connected to the CLP while the other is left unconnected. The sensor's live input terminal is connected to the meter (Figure 5a), thus, indicating the normal situation. However, to achieve meter bypassing, the cable from the sensor live input terminal, connected to the meter is disconnected, while the unconnected cable from the live output terminal of the sensor was connected to the meter (Figure 5b). In other words, the sensor is made inactive (bypassed) and the output reads zero. Hence, zero data was acquired from the sensor, while electricity was being consumed. The meter was left in the circuit to compare the kWh consumed with the calculated energy from the sensor during this period.

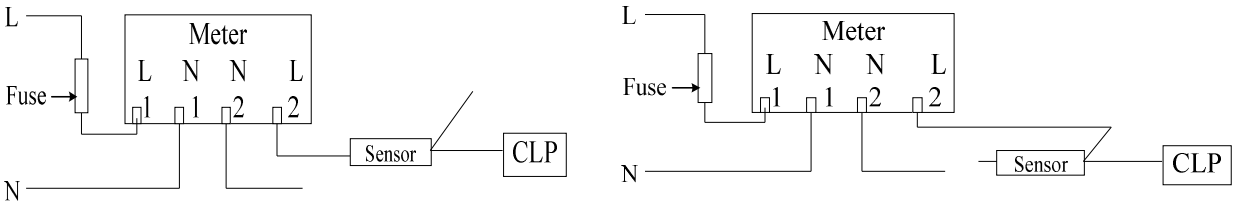

Figure 5

Case C: Tampering with the Meter

Meter tampering was imitatedby configuring the software to reduce the data acquired from sensor B with a fixed factor.Since tampering with energy meter is to reduce the amount of energy registered by the meter, reducing the data with a factor means that the kWh will also be reduced simultaneously.

DATA PROCESSING

This involves conversion as well as evaluation of data acquired from the sensors. The flowchart of data processing is shown in Figure 6.

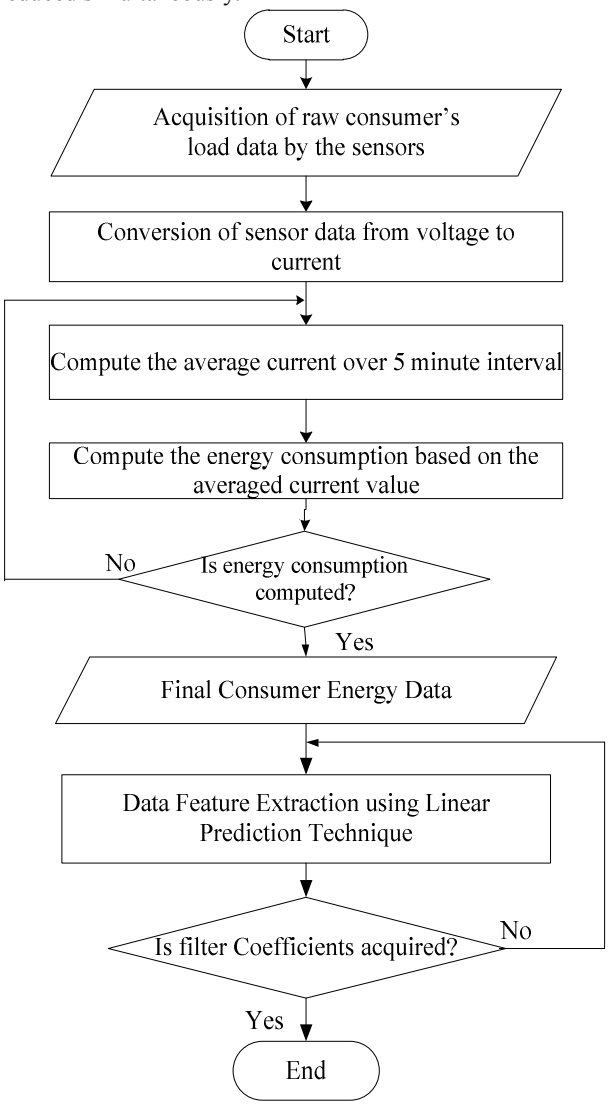

Figure 6: Data Processing Flowchart

Data Feature Extraction

Data consumed for different types of theft, particularly, meter bypassing, meter tampering and illegal connection before the meter were captured after acquiring data for the normal operation without theft. These data were analyzed using autoregressive technique with the aim of extracting the coefficients of the filter that best represents the data.

RESULTS AND DISCUSSION

Normal Operation without Theft

The energy consumption from sensors A and B as well as the predicted loads from the consumer load modelare depicted in Figure 7 and Figure 8. The load consumptions from the two sensors are the same as expected since there is no theft on the distribution network. This is indicated in Figure 7 where the two-energy consumption overlaps and appeared like a single plot. Furthermore, the prediction of these loads based on model order 20 (Figure 8), which is also identical. The model coefficients are also the same as shown in Table 1.In other words, the actual energy consumptions, the predicted energy consumptions, model coefficients and model order are practically the same.

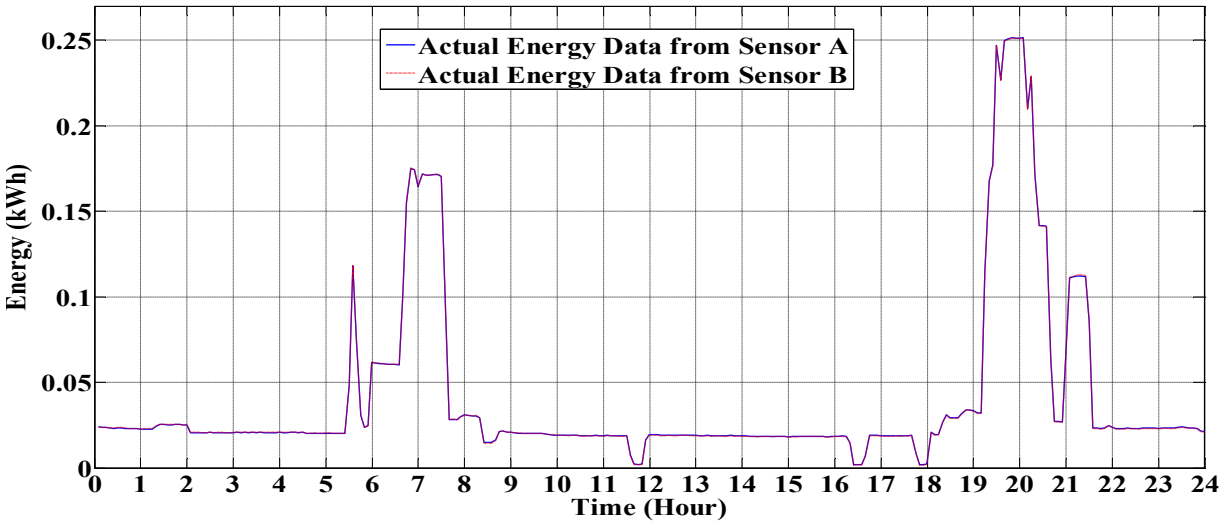

Figure 7Consumer Load without Electricity Theft for Day 1 from Sensor A and B

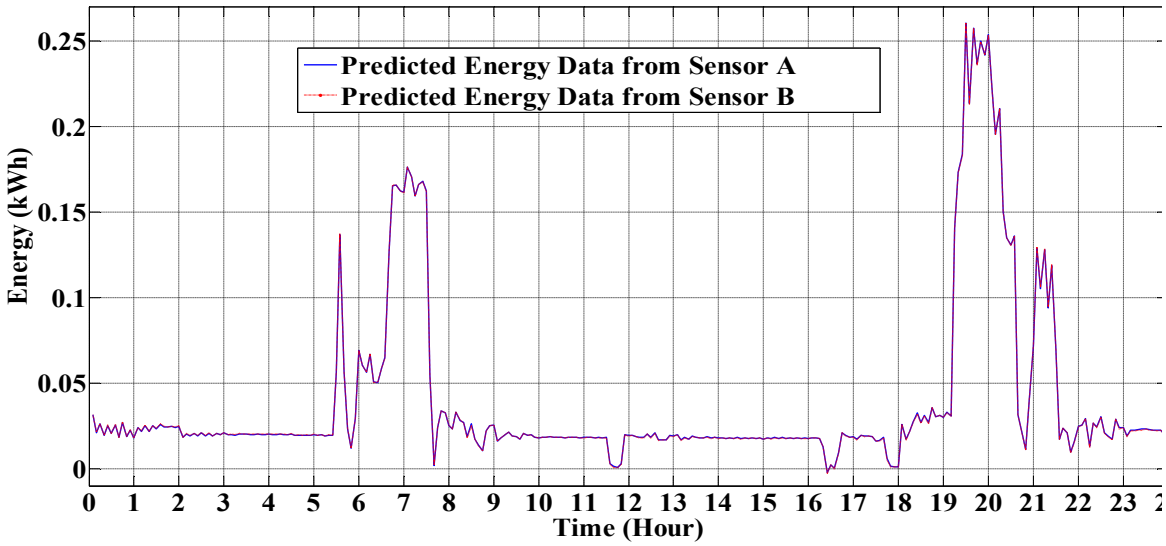

Figure 8Actual and Predicted Load based on Consumer Load Model of Order 20

Table 1: AR(20) Model Coefficients for Actual Energy data from Sensor A and theft energy data from Sensor B for various types of theft.

	Normal situation		Meter bypassing		Illegal connection before the meter		Meter Tampering	
	A	B	A	B	A	B	A	B
	1	1	1	1	1	1	1	1
	-1.3139	-1.3130	-1.0500	-1.0050	-1.1309	-1.1502	-1.1360	-1.1338
	0.4064	0.4050	0.1795	0.2294	0.2444	0.3029	0.1692	0.1664
	-0.1996	-0.1976	-0.208	-0.2739	-0.1168	-0.1811	-0.0144	-0.0133
	0.2586	0.2552	0.1426	0.2029	0.0794	0.3350	0.0119	0.0108
	-0.2339	-0.2287	-0.0824	-0.1229	-0.0376	-0.5080	0.0166	0.0185
	0.2027	0.1979	0.0748	0.1121	0.0110	0.2101	-0.0961	-0.0965
	-0.2058	-0.2034	0.0577	0.1510	0.0234	0.0183	0.2287	0.2272
	0.2780	0.2773	-0.1036	-0.1309	-0.0194	0.0821	-0.1325	-0.1312
	-0.3602	-0.3621	-0.0489	-0.0438	-0.0658	-0.1780	-0.0412	-0.0423
	0.3418	0.3441	0.1259	-0.0253	0.1391	0.0841	-0.0146	-0.0142
	-0.1526	-0.1529	0.0615	-0.0017	0.0564	0.0593	0.1756	0.1763
	0.1664	0.1639	-0.0767	-0.0003	-0.0627	-0.0135	-0.1113	-0.1104
	-0.2281	-0.2214	-0.0173	0.0131	-0.0720	-0.0255	0.0154	0.0142
	0.0761	0.0691	-0.0996	0.0365	-0.1123	0.0452	0.0349	0.0337
	-0.1373	-0.1353	0.0788	-0.0332	0.1632	-0.0011	-0.0980	-0.0975
	0.2414	0.2426	-0.1398	-0.0065	-0.0906	-0.0038	0.1093	0.1089
	-0.1175	-0.1202	0.2116	-0.0203	-0.0505	-0.0554	-0.0560	-0.0541
	0.0597	0.0640	-0.0685	0.0278	0.0737	0.0428	0.0644	0.0634
	-0.1105	-0.1136	0.0092	-0.0135	-0.0229	-0.0777	-0.1040	-0.1030
	0.0592	0.0599	-0.0157	0.0028	0.0244	0.0450	0.0074	0.0064

Detectionof Meter Bypassing

The actual energy consumption from sensors A and B as well as the predicted energy based on consumer model are shown in Figure 9 and Figure 10respectively. There is difference in load consumption between the two sensors and this implies that there was electricity theft. However, the type of theft is not known. These differences in the load occurred between 1and 6 hrs 50 mins as well as between 19 hrs 50 mins and 24 hrs. The model coefficients are different while the model order is the same (Table 1), thus, depicting theft due to bypassing of the meter. Therefore, theft due to meter bypassing occurs whenever there is a difference in energy consumptions as acquired by the sensor A and sensor B,while sensor B indicates zeros reading at some points. In addition, the predicted energy consumption and the model coefficients are different while the model order is the same.

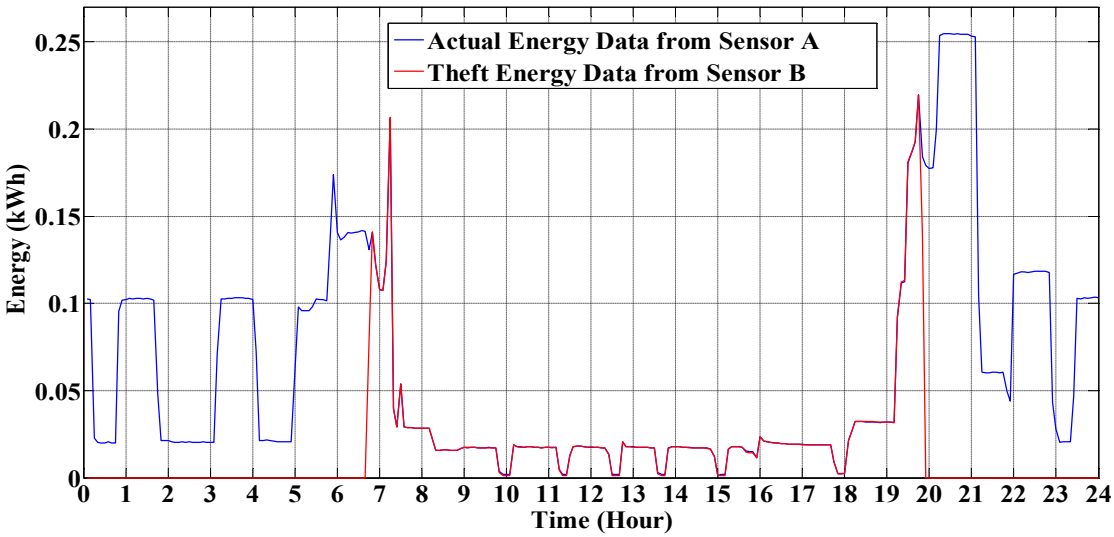

Figure 9:Consumer Load withMeter bypassing Theft

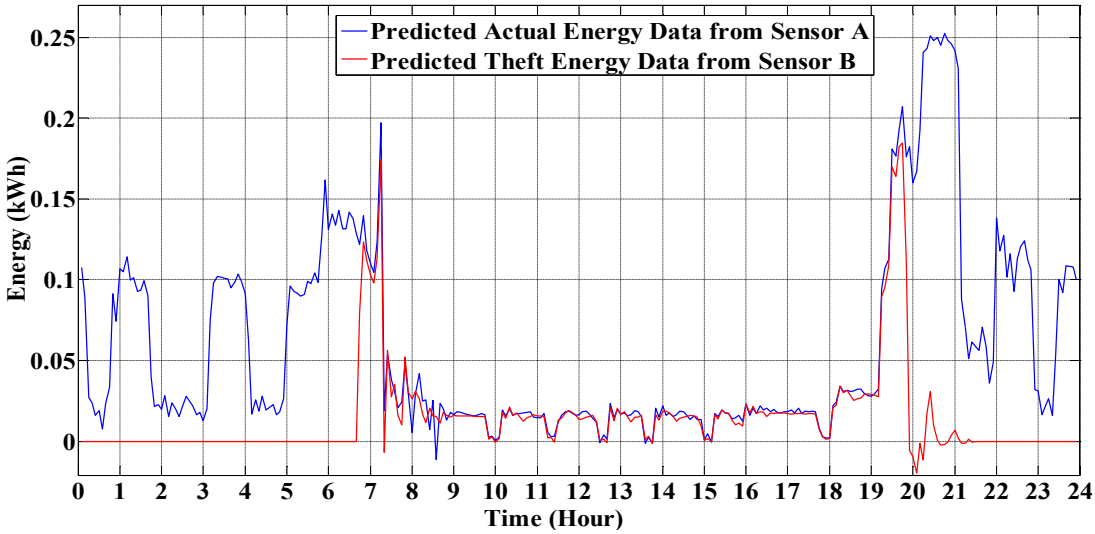

Figure 10:Actual and Theft Predicted Loads based on Consumer Load AR (20) Model

Illegal Connection before the Meter

Figure 11 shows the actual energy consumption based on the data from sensors A and B while Figure 12depicts the predicted energy of actual and theft data, respectively. There is a difference in the load consumption from the two sensors as Sensor-B's reading is lower than that of sensor A (Figure 11). This occurred between 1 and 6 hrs 10 mins as well as 20 hrs and 21 hrs 20 mins, respectively. However, there is no zero reading from sensor B, which shows a reduced consumption. Furthermore, the prediction of these loads, based on model order 20, (Figure 15) and their model coefficients, which are different,is indicated in Table 1. The model order is however the same. Consequently, theft before the meter is identified when there are disparities in energy consumptions from the sensors but data from sensor B has no zero readings, the model coefficients are different but model order is the same.

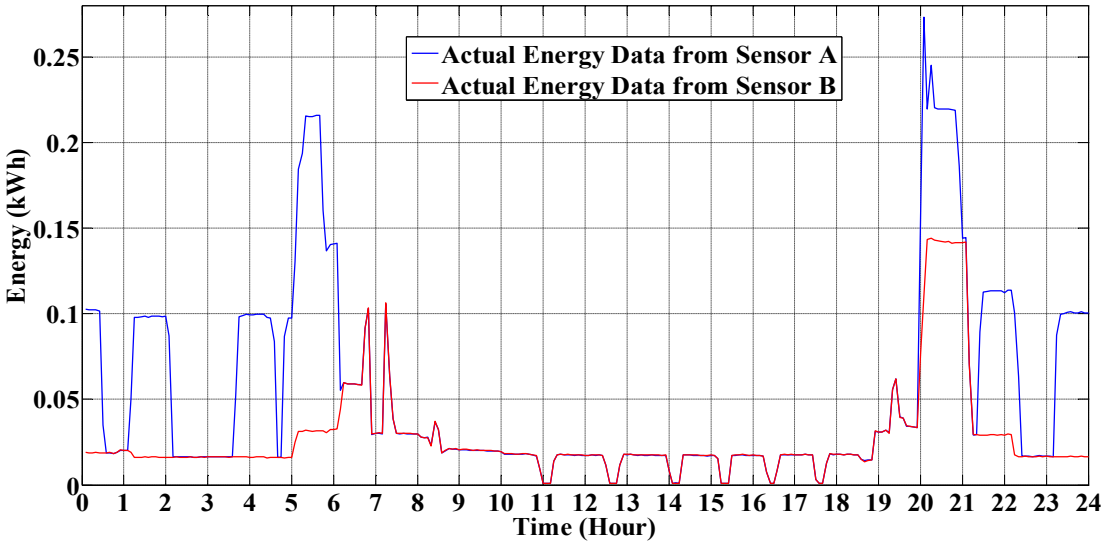

Figure 11:Consumer Load with Illegal Connection before the Meter Theft

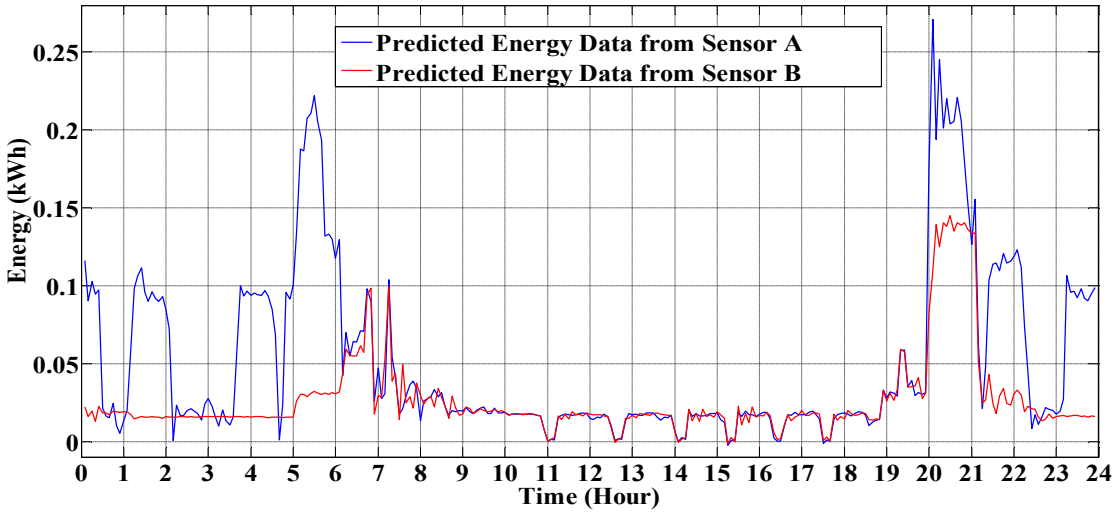

Figure 12Actual and Theft Predicted Loads based on Consumer Load AR (20) Model

Meter Tampering

The energy consumptions as detected by sensors A and B are shown in Figure 13, while Figure 14 illustrates the predicted energy of actual and theft data. The load consumptions from the two sensors are different and the load from sensor B is a reduced version of that of sensor A as depicted in Figure 13. Furthermore, the coefficients of the modelis based on model order 20, (Table 1).It was observed that the model coefficients, under meter tampering column, are practically the same as well as the model order despite the disparities in the load consumption. Hence, theft due to meter tampering was identified when there is a disparity in the load consumptions whereas the model coefficients are practically the same. The summary of AR (20) consumer model for detection and identification of the type of electricity theft is illustrated in Table 2.

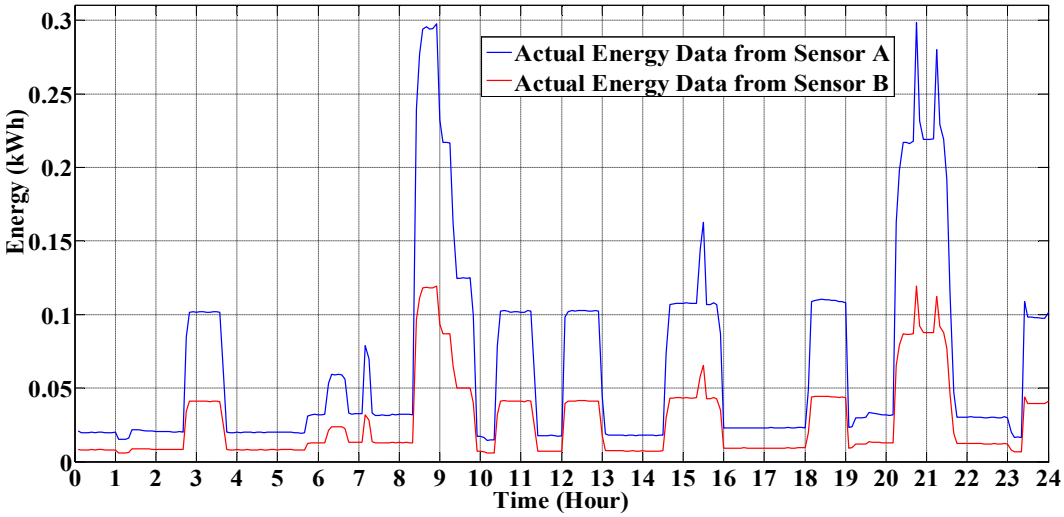

Figure 17:Consumer Load with Electricity Theft (Meter Tampering)

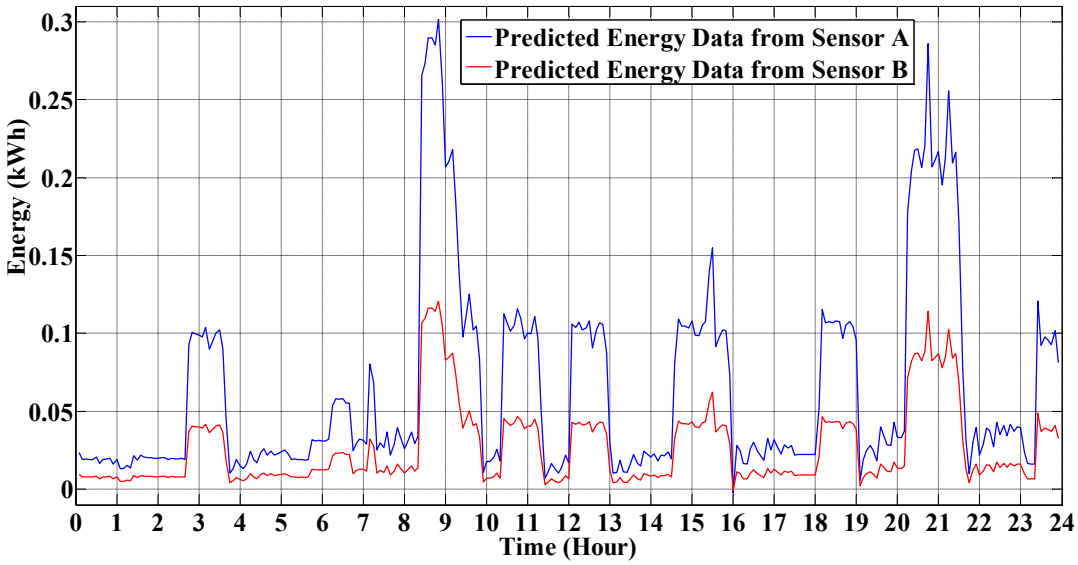

Figure 18:Actual and Theft Predicted Loads based on Consumer Load AR (20) Model

Energy consumption		Responses	
Sensor-A	Sensor-B	Model coefficients disparities	Theft identification
Normal	Normal	No	Normal situation
Normal	Not Normal (zero value recorded)	Yes	Meter bypassing
Normal	Normal (no zero value recorded)	Yes	Illegal connection before the meter
Normal	Normal (reduced version of Sensor-A)	No	Meter tampering

CONCLUSION

Identification of electricity theft such as illegal connection before the meter, meter tampering and bypassing of the meter based on consumers data has be addressed in this study. The consumer energy data used was acquired using LABVIEW hardware equipment and software package. Feature extraction of the data acquired was achieved using autoregressive technique. The identification-involved knowledge of the model coefficient, acquired data and prediction of acquired.In the results show in the three cases, there is difference in energy consumption, however for meter bypassing theft one of the sensors read zero value and there were disparities in the model coefficients. In illegal connection before the meter theft, no zero value wasrecorded from one of the sensors however there were disparities in the model coefficients. Furthermore, in meter tampering theft, a reduced version of one of the sensors reading was indicated by the other sensor and therewere no disparities in the model coefficients.

References

[1] T. B. Smith, "Electricity theft: a comparative analysis," *Energy Policy,* vol. 32, no. 18, pp. 2067-2076, 2004.

[2] J. McShan. (2010, May 18). *Electricity theft: Dangerous trend that's costing honest Houstonians money*. Available: http://www.khou.com/news/crime/Electricity-theft-a-dangerous-trend-thats-costing-honest-Houstonians-money-92450694.html

[3] CBC-News. (2010, August 8). *Electricity theft by B.C. grow-ops costs $100M a year*. Available: http://www.cbc.ca/news/canada/british-columbia/story/2010/10/08/bc-hydro-grow-op-theftw.html

[4] Reuters. (2010, August 5). *R4bn lost to electricity theft*. Available: http://www.fin24.com/Economy/R4bn-lost-to-electricity-theft-20100323

[5] L. Babirye. (2012, April 3). *Six killed in illegal electricity connections* Available: http://www.newvision.co.ug/news/633444-six-killed-in-illegal-electricity-connections.html

[6] Jonckie. (2012, April 2). *Man fights for life after illegal connection electrocution*. Available: http://www.accidents.co.za/2012/08/01/m

an-fights-for-life-after-illegal-connection-electrocution/

[7] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, "Measures and setbacks for controlling electricity theft," in *North American Power Symposium (NAPS)*, Texas, 2010, pp. 1-8: IEEE.

[8] P. Kadurek, J. Blom, J. Cobben, and W. Kling, "Theft detection and smart metering practices and expectations in the Netherlands," in *Innovative Smart Grid Technologies Conference Europe (ISGT)*, Gothenburg 2010, pp. 1-6: IEEE.

[9] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," in *Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES*, 2011, pp. 1-8: IEEE.

[10] M. Oyun-Erdene, B.-E. Byambasuren, E. Matson, and D. Kim, "Detection and localization of illegal electricity usage in power distribution line," (in English), *Multimedia Tools and Applications,* pp. 1-16, 2014/05/11 2014.

[11] B. Bat-Erdene, S. Y. Nam, and D. H. Kim, "A Novel Remote Detection Method of Illegal Electricity Usage Based on Smart Resistance," in *Future Information Technology*, J. J. Park, L. T. Yang, and C. Lee, Eds. Berlin Heidelberg: Springer, 2011, pp. 214-223.

[12] I. H. Cavdar, "A solution to remote detection of illegal electricity usage via power line communications," *Power Delivery, IEEE Transactions on,* vol. 19, no. 4, pp. 1663-1667, 2004.

[13] L. Cao, J. Tian, and Y. Liu, "Remote wireless automatic meter reading system based on wireless mesh networks and embedded technology," 2008, pp. 192-197: IEEE.

[14] G. Fuxiang, X. Wenxin, and L. Langtao, "Overview on remote meter reading system based on GPRS," in *2nd International Conference on Industrial and Information Systems (IIS)*, Dalian, 2010, vol. 2, pp. 270-273: IEEE.

[15] H. G. R. Tan, C. Lee, and V. Mok, "Automatic power meter reading system using GSM network," in *International Power Engineering Conference (IPEC)*, Singapore, 2007, pp. 465-469: IEEE.

[16] J. Nagi, K. Yap, S. Tiong, S. Ahmed, and A. Mohammad, "Detection of abnormalities and electricity theft using genetic support vector machines," in *TENCON 2008-2008 IEEE Region 10 Conference*, Hyderabad 2008, pp. 1-6: IEEE.

[17] L. Wang and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," in *Power Systems Conference and Exposition (PSCE)*, Phoenix, AZ, 2011, pp. 1-8: IEEE.

[18] A. Nizar, Z. Dong, and Y. Wang, "Power utility nontechnical loss analysis with extreme learning machine method," *Power Systems, IEEE Transactions on,* vol. 23, no. 3, pp. 946-955, 2008.

[19] A. Pasdar and S. Mirzakuchaki, "A solution to remote detecting of illegal electricity usage based on smart metering," in *2nd International Workshop on Soft Computing Applications (SOFA)*, Oradea, 2007, pp. 163-167: IEEE.

[20] C. Bandim *et al.*, "Identification of energy theft and tampered meters using a central observer meter: a mathematical approach," in *Transmission and Distribution Conference and Exposition*, Rio de Janerio, 2003, vol. 1, pp. 163-168: IEEE.

[21] S. Naiman, M. Kissaka, and N. Mvungi, "Energy meter reading and tampering protection through powerline communication channel," in *7th AFRICON Conference in Africa*, 2004, vol. 2, pp. 821-826: IEEE.

[22] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy,* vol. 39, no. 2, pp. 1007-1015, 2011.

[23] J. Makhoul, "Linear prediction: A tutorial review," *Proceedings of the IEEE,* vol. 63, no. 4, pp. 561-580, 1975.

[24] J. G. Proakis and D. G. Manolakis, *Digital signal processing: Principles, algorithms, and applications*. Prentice Hall (Upper Saddle River, NJ), 1996.

[25] E. Möller, B. Schack, M. Arnold, and H. Witte, "Instantaneous multivariate EEG coherence analysis by means of adaptive high-dimensional autoregressive models," *Journal of Neuroscience Methods,* vol. 105, no. 2, pp. 143-158, 2001.

[26] A. O'Cinneide, D. Dorran, and M. Gainza, "Linear Prediction: The Problem, its Solution and Application to Speech," *Dublin Institute of Technology, Online PDF, http://eleceng. dit. ie/papers/92. pdf,* 2008.

[27] M. Hayes, *Statistical digital signal processing and modeling*. John Wiley & Sons (New York), 1996.

[28] D. G. Manolakis, V. K. Ingle, and S. M. Kogon, "Statistical and adaptive signal processing," ed: McGraw-Hill New York, 2000.

[29] S. L. Marple Jr, "Digital spectral analysis with applications," *Englewood Cliffs, NJ, Prentice-Hall, Inc., 1987, 512 p.,* vol. 1, 1987.

[30] H. Akaike, "Fitting autoregressive models for prediction," *Annals of the institute of Statistical Mathematics,* vol. 21, no. 1, pp. 243-247, 1969.

[31] R. Kashyap and R. Chellappa, "Stochastic models for closed boundary analysis: Representation and reconstruction," *Information Theory, IEEE Transactions on,* vol. 27, no. 5, pp. 627-637, 1981.

[32] T. J. Ulrych and M. Ooe, "Autoregressive and mixed autoregressive-moving average models and spectra," in *Nonlinear Methods of Spectral Analysis*, vol. 34, S. Haykin, Ed. (Topics in Applied Physics: Springer Berlin Heidelberg, 1983, pp. 73-125.

[33] M. Wax and T. Kailath, "Detection of signals by information theoretic criteria," *Acoustics, Speech and Signal Processing, IEEE Transactions on,* vol. 33, no. 2, pp. 387-392, 1985.

[34] A. I. Abdullateef, M.-J. E. Salami, M. A. Musse, and M. A. Onasanya, "Consumer Load Prediction and Theft Detection on Distribution Network Using Autoregressive Model," *International Journal of Scientific & Engineering Research,* vol. 4, no. 12, pp. 1609-1615, 2013.

[35] A. I. Abdullateef, M. J. E. Salami, M. A. Musse, M. A. Onasanya, and M. I. Alebiosu, "New consumer load prototype for electricity theft monitoring," *IOP Conference Series: Materials Science and Engineering,* vol. 53, no. 1, p. 012061, 2013.