Consumer power prediction based on neural network for electricity theft detection

A Tjahjono¹, S Raziqurrahman¹, R N Wardhani²

¹ Departement of Electrical Engineering, Politeknik Elektronika Negeri Surabaya, Jalan Raya ITS, Surabaya, Indonesia
² Departement of Electrical Engineering, Politeknik Negeri Jakarta, Jalan Prof. DR. G.A. Siwabessy, Depok, Indonesia

E-mail: anang.tj@pens.ac.id

Abstract. Currently the state electricity enterprise, known as PLN, monitors the active power of customers by recording meters every month and is still prone to electricity theft because of location of the electricity measuring devices placed in each customer's home. In this paper, we propose an electric theft detection device with an ARM microcontroller, placed centrally on the side of distribution transformer panel to measure active power in each customer and total active power in distribution transformer. The total active power of all customers is used to predict total active power in distribution transformer by the neural network method. By comparing the active power measured in distribution transformer with prediction of the active power from the neural network method and comparing the total active power of all customers with the total active power in the distribution transformer, devices that have been made are capable of detecting electrical theft if there is percentage of error between predicted value of active power on IED Master and active power measured on IED Master above 1 percent, and also the percentage of errors between the total active power from 2 pieces of IED Slave and active power measured in IED Masters above 1 percent.

1. Introduction

Electricity is one of the vital needs, especially for people with economic activities that require electricity as the main driving force for their production activities. At this time the electricity measuring device prepaid and postpaid still has a weakness where there are still many cases of electricity theft committed by various elements with various theft modes. This is because an electric measuring device is placed in each customer's home. Electricity supply companies at this time also still use old method to detect cases of electricity theft by checking the pattern of electricity bills obtained from manual recording by officers. This of course requires a large cost to detect electricity theft. Electrical theft prevention methods have been discussed in various studies. One of them is making electrical power predictions for consumers at certain time periods by using artificial intelligent with the NARX method. Data collection was carried out for one month at 5 minute intervals to produce a prediction of consumer load [1]. In other studies to make predictions of consumer electrical power using neural network methods with a certain period of time [2]. From this research theft is detected by comparing the predicted results with the real load that is measured on the consumer. But in this research the process of predicting consumer load is offline with simulations using matlab software. In other studies, to detect theft of electricity can be done by a prepaid...
system on an electric measuring device. If there is electricity usage in the condition that the consumer has not paid the bill, then the electricity will be disconnected via relay [3-5]. However, this research only prevents theft of electricity caused by consumers not paying bills. Then in other studies where the prevention of electricity is prevented by installing sensors on electric measuring devices and theft of electricity because changes in the design of electrical measuring devices can be prevented [6-8]. Also in other studies electricity theft is prevented by taking electrical data in each house and the distribution transformer, and electricity theft can be detected by considering the loss of power lines [9, 10]. In this paper, a device that functions to detect electricity theft by ARM microcontroller is developed, placed centrally on the side of the distribution transformer panel to measure and predict the active power in the distribution transformer and to measure the active power in each customer.

2. Methodology

2.1. System design of intelligent electronic device (IED)
Intelligent electronic device (IED) has a function as a centralized electrical measuring device and placed on distribution transformer panel. The panel consists of IED Master and IED Slave. IED Master will measure the power of each phase of distribution transformer and IED Slave will measure the power of each customer to replace the electric measuring device installed in the customer's home.

![Figure 1. IED on distribution transformer panel.](image)

IED Master and IED Slave are automatically connected with internet. The IED will send the electricity measurement data to the database then transfer it to the website that has been created. The IED Master has an additional function which is the consumer load prediction feature with input from total power of each IED Slave. By using neural network method, the value of active power used on the IED Master at a certain time can be predicted. So electricity theft can be easily detected and power usage on each phase network can be monitored online via the website.
2.2. *The process to detecting electricity theft*

The process to detecting electricity theft as follows.

- Each IED Slave contained in distribution transformer panel has the function of measuring electricity in each customer. Each IED Slave represents an electrical measurement device for each customer home.
- Active power measurement data for each IED Slave then added and sampled for a specified period of time. After that the prediction of the active power in IED master is made using the neural network method. This process is carried out at the IED master so that the IED master has a more complex function than IED Slave.
- After obtaining the predicted value of active power of the IED Master at a certain time, then compare the value with real value of active power of the IED Master. If there is an error percentage below 1% then there will be information that the system is running normally. However, if there is an error percentage above 1%, real value of the active power of the IED Master is compared again with total value of active power measured on the IED Slave which is in the same phase as the IED Master. If there is a percentage error above 1%, there will be detected theft information on the website.

2.3. *Neural network*

Neural network used to predict is the most important part of this paper, so complex planning is needed on this method. Predictions with neural networks in this paper are very short term predictions. Neural network method is used to predict the active power of the IED Master at 60th seconds per minute. By learning manually with MATLAB software, the input of the neural network method is total active power of Slave 1 and Slave 2 at the 10th second, 20th second, 30th second, 40th second, and 50th second in the same minute with a power range of 95 W to 1509 W as a representation of power usage at customer's load in the low voltage line. Neural network learning process has 433 iterations using the lavenberg marquadt training method. After learning process is completed then the results of learning can be seen by selecting the regression button on the plots.
Figure 3. Structure of neural network.

The overall regression for training, validation and test is close to 1, which means that the neural network design is nearly identical with data learned. After learning process is completed using MATLAB software and obtained weight and bias values in each neuron in hidden layer and output layer. Then neural network can be used as a function to predict a certain value, the weight and bias values are included in the mathematical calculation that is written as follows:

\[
\text{Normalization}(x_1) = \frac{(x_1 - x_{\text{min}})(1 - (0))}{x_{\text{max}} - x_{\text{min}}} + (0) \tag{1}
\]

\[
\text{Hidden Layer}(y_1) = x_1(Wh) + Bh \tag{2}
\]

\[
\text{Logsig Activation}(y_1) = \frac{1}{1 + \exp^{-y_1}} \tag{3}
\]

\[
\text{Output Layer} (Z) = y_1(Wo) + Bo \tag{4}
\]

\[
\text{Purelin Activation} (N) = Z \tag{5}
\]

\[
\text{Denormalization}(x_1) = \frac{(x_{\text{max}} - x_{\text{min}})(N - (0))}{1 - (0)} + x_{\text{min}} \tag{6}
\]

The neural network design for determining number of neurons in hidden layer by trial and error process. Logsig activation function for the hidden layer and purelin activation function for the output layer based on references from previous research who used neural network method functions as a prediction. Process of determining the number of neurons with step 2 neurons, starts from 2 neuron to 10 neuron. Then for testing, the neural network that has been created is given a total active power in slave 1 and slave 2 at the 10th second, 20th second, 30th second, 40th second, and 50th second with the active power target at IED Master in 60th seconds in the same minute.

Hidden layer which has 8 number of neurons with the logsig activation function and output layer has 1 neuron and using the purelin activation function has the smallest error percentage, compared to the hidden layer which has 2, 4, 6, and 10 number of neurons. The percentage error of each number of neurons in the hidden layer can be seen in Table 1.
Table 1. Determine number of neurons.

| s10  | s20  | s30  | s40  | s50  | Result | %Error |
|------|------|------|------|------|--------|--------|
| 1202.43 | 1204.4 | 1200.77 | 1200.07 | 1203.07 | 1202.77 |         |

2 neuron hidden layer and 1 neuron output layer  
4 neuron hidden layer and 1 neuron output layer  
6 neuron hidden layer and 1 neuron output layer  
8 neuron hidden layer and 1 neuron output layer  
10 neuron hidden layer and 1 neuron output layer

The percentage error chart from each number of neurons in the hidden layer can be seen in Figure 4.

Figure 4. Mean square error each number of neurons.

After getting the right number of neurons and obtained weight and bias values from learning process using matlab, then a mathematical calculation of neural network is entered into microcontroller program at IED Master and tested to produce real consumer load predictions. So the IED system can be used to detect electricity theft.

3. Results and discussion

In IED system, STM32f407 on IED board that has been made will process the data from active power measured from IC ADE7880 in phase A, phase B, and phase C. Phase A of IC ADE7880 is used for active power measured at the power source as a representation of the IED Master. Phase B and phase C of IC ADE 7880 are used to measure active power in consumer load 1 and consumer load 2 as a representation of IED Slave 1 and IED Slave 2. Data measurement and prediction results from neural network method that has been processed with the STM32f407 microcontroller will be sent using serial communication to GSM SIM900 module. Data received by SIM900 GSM module will be sent online to database and website that has been created.

For electricity theft detection parameter test when there is a difference between results of predicted value from active power on IED Master at 60th seconds with real active power on IED Master at same time and there is a difference between value of total active power from 2 pieces IED slave at 60th seconds with real active power on IED master which is representing power usage in that group at 60th seconds. In Table 2. Numbers 8 and 9. We can see the percentage of error between value from summing of active power from 2 pieces of IED Slave (reality) with active power measured on the IED Master (transformer power) in range 15%. And percentage of errors between predicted value of active power on IED Master (forecast) and active power measured on IED Master (power transformer) in range 15%. Electricity theft detection parameter test is performed to representation of violations committed by passing the phase of measurement or changing electric measuring device design. This test is performed by CT and plug 220V in Slave1 or Slave2 are not connected to phase B or phase C on the IED board.
So there is no measurement of power in phase B or phase C. While at the same time there is power consumption in Slave 1 or Slave 2.

![Figure 5](image_url)  
*Figure 5. Comparison between prediction power and transformer power.*

Then for load change parameters test is performed to represent there is a difference between the predicted results of active power on the consumer with the actual active power usage on the consumer. This is because usage of electricity in consumers are influenced by various factors such as behavior, habits, temperature, new electrical device, etc. It make usage active power in consumers can increase or decrease at any time. We can see in Table 2. Number 7. The percentage of error between predicted value of active power on IED Master at 60th seconds with active power measured at IED Master at 60th seconds is 6%, but there is no difference between total active power from 2 IED Slave and active power measured on IED Master (values in range below 0.5%).

For normally parameter test, we can see in Table 2, numbers 1 to 6, and number 10. Percentage of error between total active power from 2 pieces of IED Slave (reality) with active power measured on IED Master (power transformer) in range below 0.5% and the percentage of errors between predicted value of active power on IED Master (forecast) and active power measured on IED Master (power transformer) in range below 0.5%. Normally condition parameter test are performed to represent that CT and Staker 220 V in phase B and phase C on the IED board are connected to the load and there is an active power measurement. This test are performed to represent there is no electricity theft and the electricity measuring device is functioning properly.

| No | Time       | s-10 | s-20 | s-30 | s-40 | s-50 | forecast | Power IED Master | Total Power IED Slave | status        | Error IED Master power (%) | Error IED Master power and Total Power IED Slave (%) |
|----|------------|------|------|------|------|------|----------|-------------------|-----------------------|---------------|------------------------|-----------------------------------------------|
| 1  | 12/06/2019 12:08 | 403.88 | 403.54 | 403.98 | 404.37 | 403.93 | 403.96 | 404.1 | 403.14 | Normal | 0.20                          | 0.24                               |
| 2  | 12/06/2019 12:06 | 403.3 | 404.05 | 403.82 | 404.01 | 403.68 | 404.21 | 404.25 | 403.47 | Normal | 0.18                          | 0.19                               |
| 3  | 12/06/2019 12:04 | 404.26 | 403.91 | 403.22 | 403.25 | 404.08 | 403.15 | 404.3 | 403.36 | Normal | 0.05                          | 0.23                               |
| 4  | 12/06/2019 12:03 | 403.95 | 404.1 | 404.13 | 403.91 | 404.82 | 404.71 | 404.66 | 403.79 | Normal | 0.23                          | 0.22                               |
| 5  | 12/06/2019 12:02 | 1202.43 | 1204.4 | 1203.07 | 1200.87 | 1200.77 | 1202.84 | 1203.35 | 1202.77 | Normal | 0.01                          | 0.05                               |
| 6  | 12/06/2019 12:01 | 1200.9 | 1201.4 | 1204.03 | 1203.91 | 1203.31 | 1205.81 | 1203.15 | 1202.55 | Normal | 0.27                          | 0.05                               |
| 7  | 12/06/2019 12:00 | 1010.92 | 1199.12 | 1197.11 | 1199.65 | 1199.2 | 1274.85 | 1201.18 | 1200.63 | Load Change | 0.18                          | 0.05                               |
| 8  | 12/06/2019 11:59 | 1010.16 | 1088.4 | 1010.78 | 1011.84 | 1009.77 | 1010.38 | 1008.31 | 1196.13 | Theft Detection | 15.53                          | 15.78                              |
| 9  | 12/06/2019 11:57 | 1012.2 | 1011.86 | 1009.36 | 1008.7 | 1008.64 | 1007.47 | 1007.49 | 1195.38 | Theft Detection | 15.72                          | 15.72                              |
| 10 | 12/06/2019 11:54 | 1195.86 | 1197.62 | 1196.25 | 1196.97 | 1196.69 | 1197.45 | 1195.92 | 1195.16 | Normal | 0.19                          | 0.06                               |

4. Conclusions
In integration test of Intelligent Electronic Device system. The IED detect electricity theft if there is percentage of error between predicted value of active power on IED Master and active power measured on IED Master above 1%, and also the percentage of errors between the total active power from 2 pieces
of IED Slave and active power measured in IED Masters above 1%. The information of electricity theft detection is displayed in the status on website that has been created with a comparison chart between predicted power and real power measured on IED master.

5. References
[1] Abdulateef M, Salami J E and Tijani I B 2016 *International Conference on Computer and Communication Engineering*
[2] Wang X, Zhao T and Liu H 2019 *International Conference on Cloud Computing and Big Data Analysis*
[3] Saad M, Tariq M F, Nawaz, Amna and Jamal M Y 2017 *IEEE International Conference Control Science and System Engineering*
[4] Darshan N and Radhakrishna K A R 2015 *International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering* 4 6482-6491
[5] Sahoo S, Daniel N, Toru M and Kaoru T 2015 *Conference IEEE Power & Energy Society Innovative Smart Grid Technologies*
[6] Ogu R E and Chukwudebe G A 2017 *International Conference Electro-Technology for National Development (Owerri: Nigeria)*
[7] Sridhar S, Bharath H, Vishvesh V, Gowtham K V and Girish H 2016 *International Journal of Engineering Research* 5 992-1128
[8] Anushree S V and Shanthi T 2016 *International Journal of Innovative Research in Computer and Communication Engineering* 4 19801-19805
[9] Talwar P D and Kulkarni S B 2016 *International Journal of Recent Trends in Engineering and Research* 2
[10] Singh M and Sanduja E V 2015 *International Journal of Advanced Research in Computer and Communication Engineering* 4 326-329

Acknowledgments
This research is supported by Ministry of Research, Technology and Higher Education of Republic Indonesia and Politeknik Elektronika Negeri Surabaya (PENS) that have facilitated Intelligent Electronic Device board testing and calibration sites and we are also grateful to those who provided insights and expertise that greatly assisted this research.