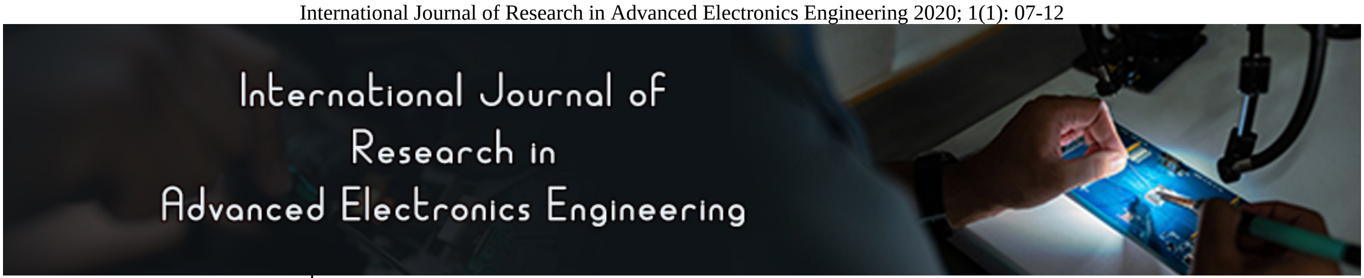

E-ISSN: 2708-4566
P-ISSN: 2708-4558
IJRAEE 2020; 1(1): 07-12

www.electrojournal.com
Received: 03-11-2019
Accepted: 04-12-2019

Albin Thomas
Department of Computer Science, SAS SNDP Yogum College, Konni, Kerala, India

Correspondence
Albin Thomas
Department of Computer Science, SAS SNDP Yogum College, Konni, Kerala, India

Design and Simulation of electricity theft detection in radial distribution system

Albin Thomas

Abstract
Theft of electricity is a significant problem faced by both developed as well as developing countries. It affects both the power as well as economic situation. It also at times is the root cause of blackouts. This paper proposes a method based on the forward-backward load flow and artificial neural networks to detect electricity theft in a radial distribution network. Simulations have been performed in MATLAB Simulink and the results have been presented.

Keywords: Electricity Theft; Electricity Protection; Electricity Theft Detection; Smart Meter; Smart-Grid

Introduction
Modern life cannot be imagined without electricity. It has grown into such a necessity that it has been declared as a fundamental right. The value of electricity cannot be undermined in this technology-driven world where our daily lives are dominated by appliances and gadgets. Yet there are still places where electricity is not available yet and still; there are people who do not enjoy this fundamental right as we do. There are various reasons for this such as the insufficient power generation, losses, various geographical terrains etc. But among these, one of the major reason is electricity theft. Several works have been undertaken to address this issue. In the research done by P. Jokar, N. Arianpoo and V. C. M. Leung [1], consumption patterns of customers are analyzed to identify malicious activities. In another research by M. Tariq and H. V. Poor [2], a stochastic Petri net formalism is used to detect and localize the occurrence of theft in grid-tied MGs. Theft detection using smart meters in the consumer's side and service provider side has also been proposed [4]. The data from the meters are analyzed to determine the non-technical losses. Decision tree and support vector machine classifiers can be for analysis of real-time electricity consumption data to detect theft [8, 9]. Genetic algorithms with support vector machines are also proposed to detect theft [10].
In this paper, a dual method based on the forward-backward load flow and artificial neural network has been proposed. Based on the knowledge of the existing network parameters and results from a trained network, the theft of electricity can be determined.

Theoretical Background
Smart Grid
A smart grid adds sensors and software to the existing grid. With the integration of renewable energy sources into the grid, communication among the loads and sources, and intelligent management has become a necessity. Re-routing of power during faults, optimal generation scheduling, demand-side management are some of the advantages with the smart grid.

Smart Meters
Smart meters, as shown in Figure 1, are energy meters with many additional features, communication with the service provider being the most important one. These meters enable two-way communication between the meter and the central system. Communications from the meter to the network may be wireless, or via fixed wired connections such as power line carrier (PLC). Wireless communication options in common use include cellular communications (which can be expensive), Wi-Fi (readily available), wireless ad hoc networks over Wi-Fi, wireless mesh networks, low power long-range wireless (LODA), ZigBee (low power, low data rate wireless), and Wi-SUN (Smart Utility Networks), etc.

Fig 1: Smart Meter

Artificial Neural Network (ANN)

It is a computational model, which mimics the biological neural networks of living beings. Information that flows through the network affects the structure of the ANN. The neural networks are initially trained with known sets of input-outputs, to establish a relationship between them. Once the training is completed, they can be implemented to find the output for any valid inputs.

ANNs have three or more layers that are interconnected. The first layer consists of input neurons. These neurons send the data to the neurons of intermediate layers, which in turn sends the processed output to the neurons of the third layer. Training an artificial neural network involves choosing from allowed models for which there are several associated algorithms. Figure 2 shows the plot of data validation of ANN.

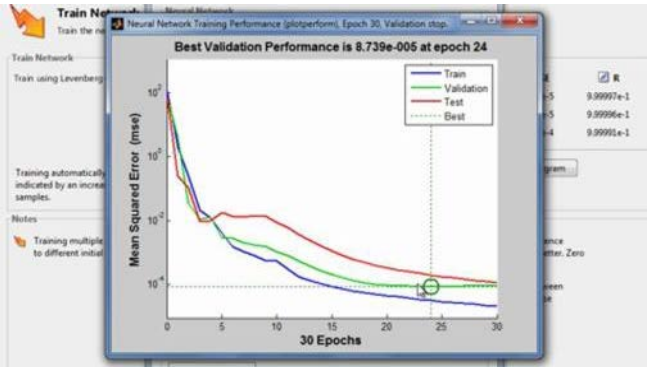

Fig 2: Data Validation Plots of ANN

Load Flow in Radial Distribution System

Load flow studies are performed to estimate the various parameters of a power system, which basically includes the bus voltages, bus angles, power at the busses, total loss etc. Load flow methods like Newton-Raphson, for the mesh network, has been in use for many decades. However, load flow for radial distribution system as shown in Fig. 3cannot be directly solved using these methods. One of the most popular methods for solving load flow in the radial distribution system is the backward-forward sweep method. It is an iterative method in which, the load flow can be solved iteratively from two sets of recursive equations. The first sets of equations are or calculation of the power flow through the branches starting from the last branch and proceeding in the backward direction towards the root node. The other sets of equations are for calculating the voltage magnitude and angle of each node starting from the root node and proceeding in the forward direction towards the last node. Nodal voltages are updated in the forward sweep. The backward sweep is basically a current or power flow solution. The voltage values obtained in the forward path are held constant during the backward propagation and updated power flows in each branch are transmitted backward along the feeder using backward path.

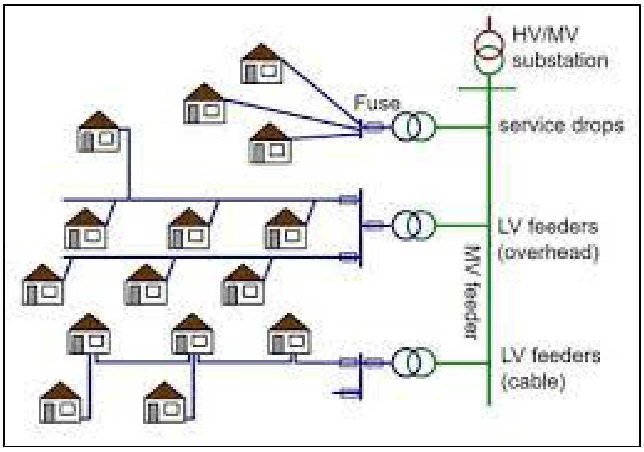

Fig 3: Radial Distribution System

Electricity theft detection using forward backward sweep method

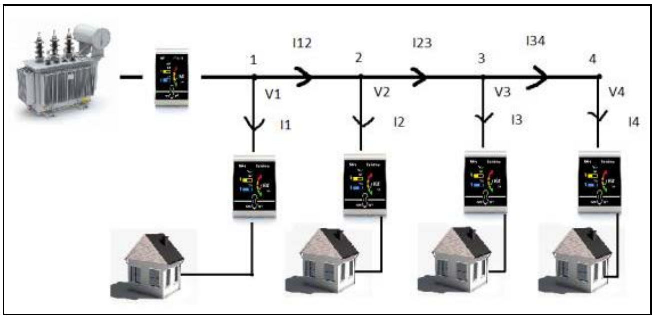

Fig 4: System Design

$$I_{34}=I_4$$
$$V_4=V_3-I_{34}Z$$
$$V_4=V_3-I_4Z_{23}$$
$$V_3=V_2-I_{23}Z_{23}$$
$$V_3=V_2-(I_3+I_4)Z_{23}$$
$$V_2=V_1-I_{12}-Z_{12}$$
$$V_2=V_1-(I_{23}+I_2)Z_{12}$$
$$V_2=V_1-(I_3+I_4+{}_{12})Z_{12}$$
$$V_1=V_0-(I_2+I_3+I_4+I_1)Z_{12}$$

If we take no of nodes = m, then

$$V_n=V_{n-1}-(I_n+I_{n+1}+\dots+I_m)Z_{n,n-1}$$
$$P=P_1+P_{12}+P_2+P_{23}+P_3+P_{34}+P_4$$
$$P=P_1+I^2{}_{12}R+P_2+I^2{}_{23}R_{23}+P_3+I^2{}_{34}R_{34}+P_4$$

The above equation is the general equation for the algorithm.

In the proposed method, the real-time data available from all the smart meters connected to the consumer and the transformer supplying these consumers are being used for detection of the electricity theft. Smart meters have been taken into considerations, which are assumed to be already in use. This method is based on the forward-backward sweep method of power flow solution of distribution systems. The data read by the smart meters and previous knowledge of network parameters will be used to estimate the real power supplied by the source; in this case, it can be the distribution transformer. The smart meter of the transformer shall give the measured power delivered to the distribution network. Now the estimated power and the measured power shall be compared, and if the error is found to be greater than a predetermined threshold, theft can be ascertained. Apart from the detection of theft, localization is also possible. Figure 4 shows each node with their voltage and current. The node voltage, currents and total power are determined based on the following equations.

Simulation

The method discussed above was implemented in Simulink (MATLAB). The distribution system is being shown in Figure 5. The supply transformer is represented by a voltage source, while the loads are represented by resistive loads. Each load and the supply transformer have a meter of its own, which will act as a smart meter. And then, there is the data center, where all the calculations and comparisons will take place. The theft is represented by a resistive load without a meter

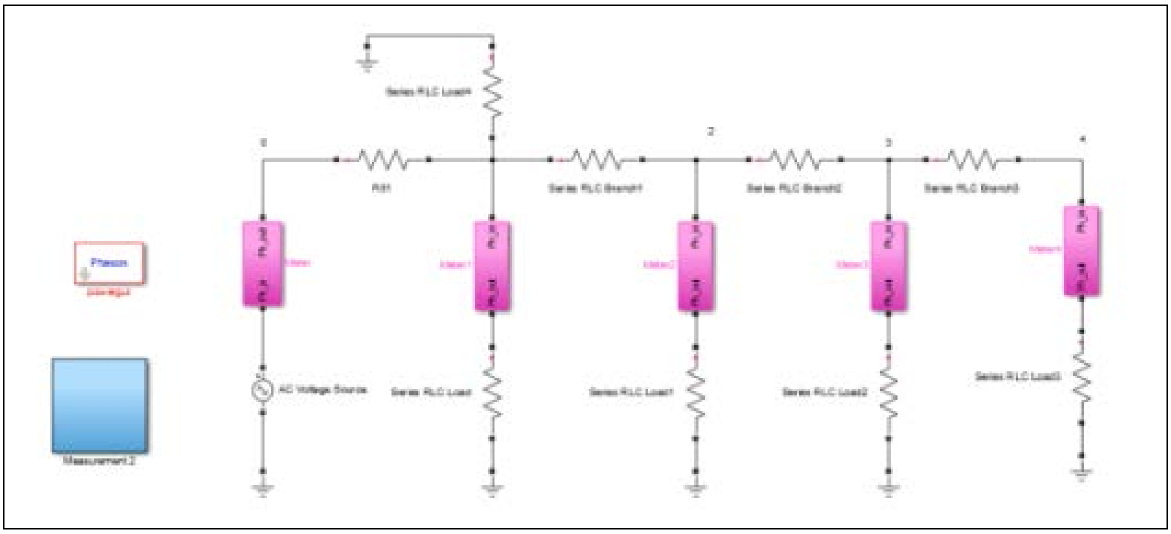

Fig 5: Simulink Model of the Distribution System

The meter that has been added to each load and the supply transformer is depicted in Figure 6. Here, there are measurement provisions for current, voltage and real power. These provisions will give all the real-time values of current, voltage and power.

All the real time values of current, voltage and power are sent to the data center in Fig. 7 to implement the equations. The equation is as follows:

$$V_n=V_{n-1}-(I_n+I_{n+1}+\ldots+I_m)Z_{n,n-1}$$

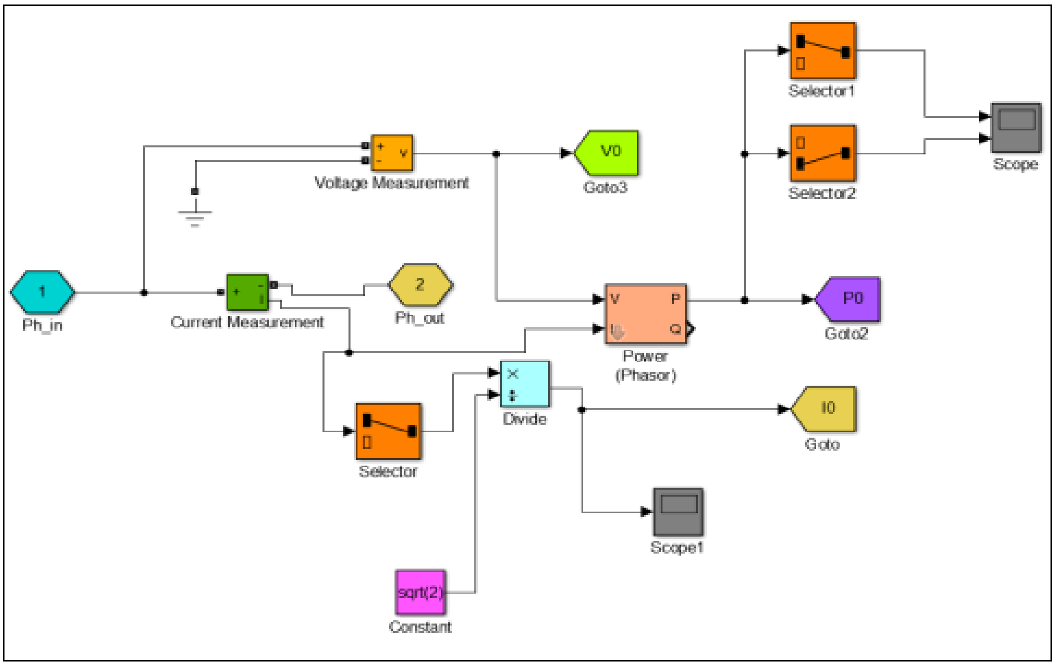

Fig 6: Simulation Sub-System of the Smart Meter

Different mathematical blocks are used to realize the above equation. The various blocks are assembled in this single unit to provide a unit place for calculations.

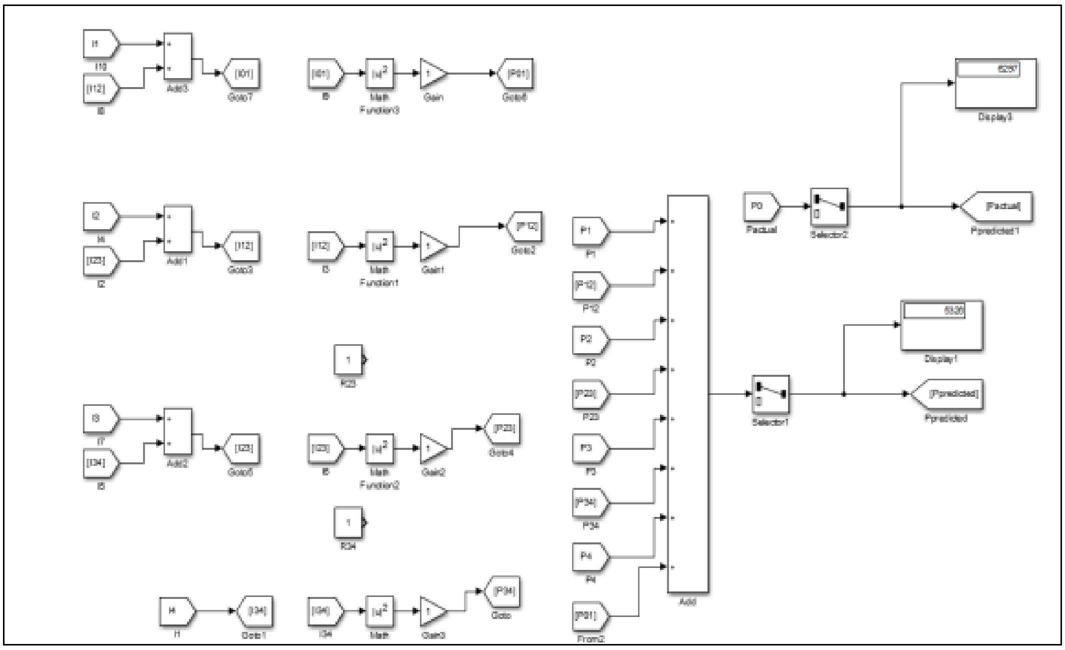

Fig 7: Data Centre Sub-System in Simulink

Electricity theft detection using ANN

ANN has proved quite efficient in application involving data fitting. The theft detection problem, in this case, can also be considered as a data-fitting problem. So if ANN network is trained with the various electrical parameters for different load conditions under no theft condition, this trained model can then be used to predict the total power under a given set of load conditions .Then the predicted load and the actual load can be compared to detect electricity theft. The following section describes the development and implementation of this method in Matlab.

Training the Networks

To train the network, the distribution network shown in Figure 8 has been used. Data sets are created by changing the loads and measuring the network parameters. This dataset configures the ANN to predict outputs for a given set of inputs under no theft conditions. This is shown in Figure 9.

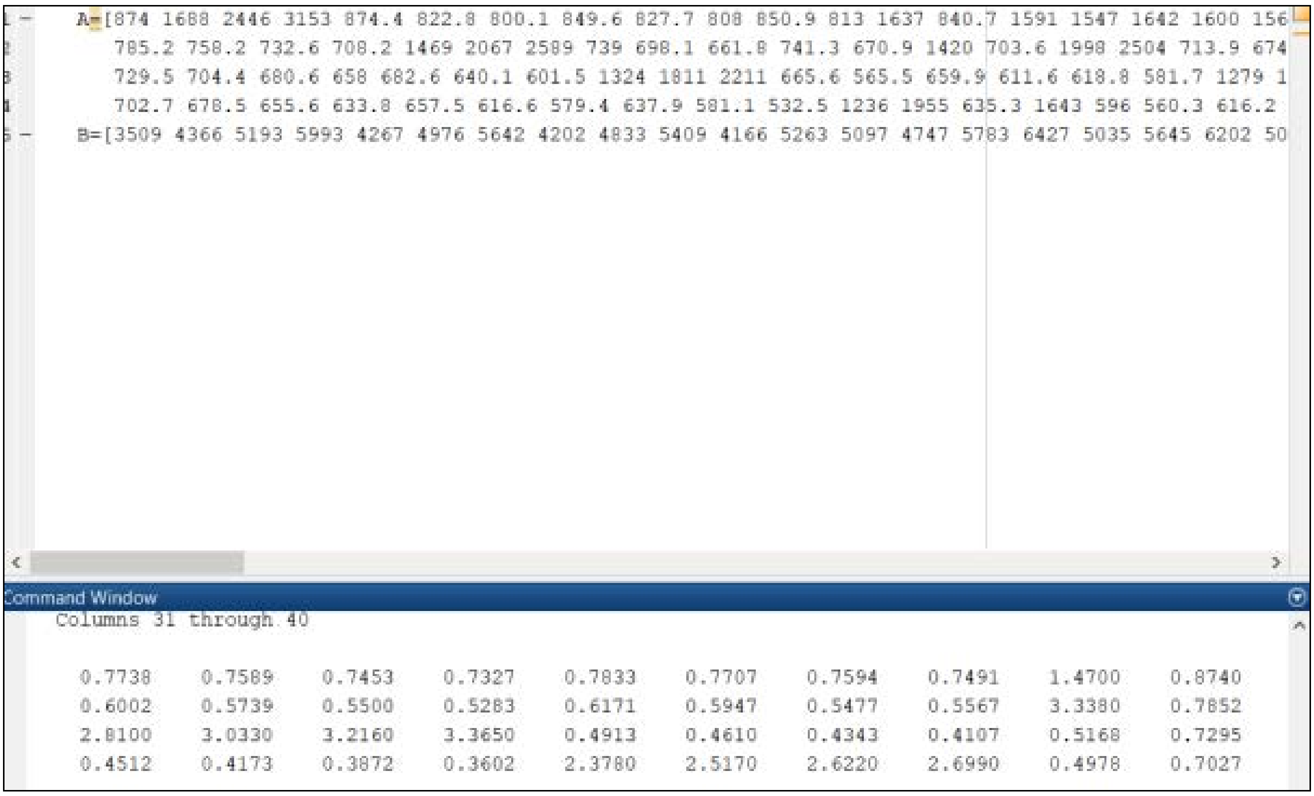

Fig 9: Training Data Set

Testing the network

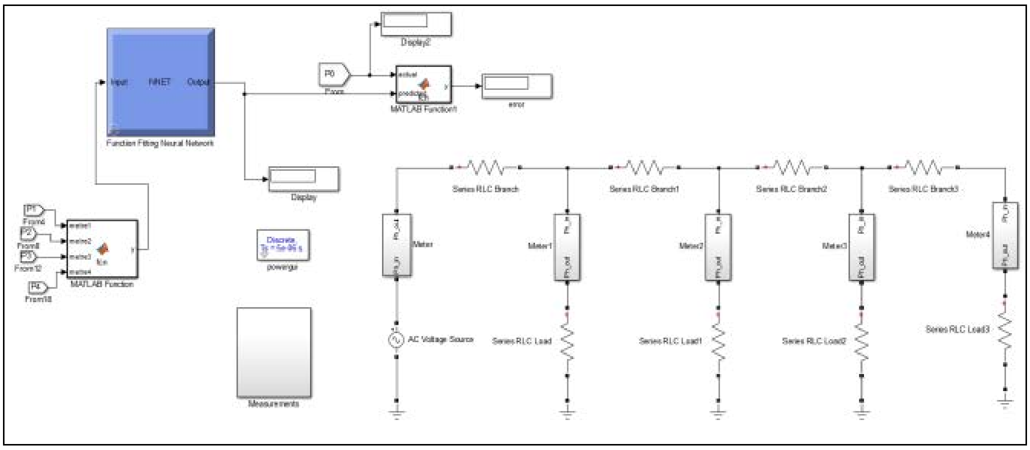

Fig 10: Neural Network Sub-System

The ANN is tested by validating the outputs for different loading and no theft conditions. The error in the predicted and the actual readings are recorded.

Results and Discussion
Results of ANN

Table 1: ANN Results

Theft at Node	Error
No Theft	3.511%
1	20.11%
2	33.89%
3	43.69%
4	21.53%

The error between the ANN network and the normal distribution has been shown in Table. 1. The error shows a pattern where at least a minimum of 10% error occurs when there is a theft. Without theft, there is an error of 3%. This error can be credited to the losses.

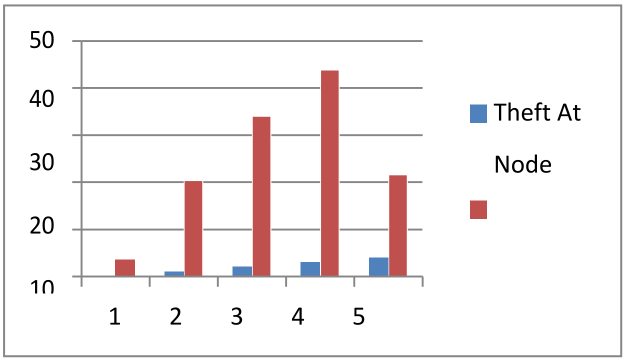

Fig 11: Error Results of ANN

Results of forward-backward sweep method

Table 2: Results from Forward- Backward Sweep

Theft at Node	Error
No Theft	0
1	15.45
2	26.67
3	25.94
4	25.21

The error for Forward-Backward Sweep Method is shown in Table. 2As seen from the table as the method takes the exact values of all the parameters, the error with no theft is 0%, however with theft the error between the measured value and the estimated value is about 15%. Hence, the two methods when used together, provide a more robust method to detect the theft.

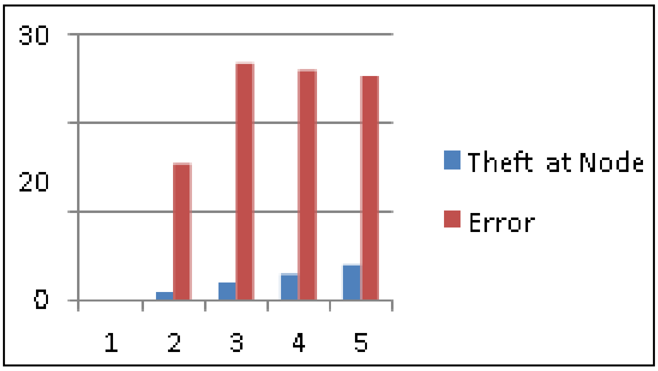

Fig 12: Error results of the forward-backward sweep method

Discussion

The error has a pattern; this pattern can be used to formulate a system to detect electricity theft. This system will be a robust system in terms of detection as it relies on the percentage of error.

Conclusion

In this paper, a dual method using forward- backward sweep and ANN has been proposed to detect electricity theft in radial distribution systems. The method has been tested in MATLAB Simulink. Simulation results demonstrate that the estimated power of the system and the measured power of the distribution transformer differ significantly under theft.

References

1. Jokar P, Arianpoo N, Leung VCM. Electricity Theft Detection in AMI Using Customers' Consumption Patterns, in IEEE Transactions on Smart Grid, 2016; 7(1):216-226.
   doi: 10.1109/TSG.2015.2425222
2. Tariq M, Poor HV. Electricity Theft Detection and Localization in Grid-Tied Microgrids, in IEEE Transactions on Smart Grid, 2018; 9(3):1920-1929.
   doi: 10.1109/TSG.2016.2602660.
3. Dick AJ. Theft of electricity-how UK electricity companies detect and deter, European Convention on Security and Detection, Brighton, UK, 1995, 90-95.
   doi: 10.1049/cp:19950476
4. Mohammad N, Barua A, Arafat MA. A smart prepaid energy metering system to control electricity theft, 2013 International Conference on Power, Energy and Control (ICPEC), Sri Rangalatchum Dindigul, 2013, 562-565. doi: 10.1109/ICPEC.2013.6527721
5. Kumar S, Electricity Theft: Empowering People & Reforming Power Sector, Institute for Development and Communication, Manohar, New Delhi, 2004.
6. Agarwal A, Power Theft in India, Project Guru, 2012. [Online]. Available: https://www.projectguru.in/publications/powe r-theft-india/ [Accessed: 21 July, 2018]
7. Kelly-Detwiler P, Energy Theft: A Bigger Issue Than You Think," Forbes, April, 2013. [Online]. Available: https://www.forbes.com/sites/peterdetwiler/2013/04/23/electricity-theft-a-bigger-issue-than-you-think/#693d7aa75ed7 [Accessed: 21 July, 2018]
8. Jindal A, Dua A, Kaur K, Singh M, Kumar N, Mishra S. Decision Tree and SVM-Based Data Analytics for Theft Detection in Smart Grid, in IEEE Transactions on Industrial Informatics, 2016; 12(3):1005-1016.
   doi: 10.1109/TII.2016.2543145\
9. Nagi J, Mohammad AM, Yap KS, Tiong SK, Ahmed SK. Non-Technical Loss analysis for detection of electricity theft using support vector machines, 2008. IEEE 2nd International Power and Energy Conference, Johor Bahru, 2008, 907-912.
   doi: 10.1109/PECON.2008.4762604
10. Nagi J, Yap KS, Tiong SK, Ahmed SK, Mohammad AM. Detection of abnormalities and electricity theft using genetic Support Vector Machines, Tencon 2008-2008 IEEE Region 10 Conference, Hyderabad, 2008, 1-6. doi: 10.1109/TENCON.2008.4766403
11. Smith TB. Electricity Theft: a comparative analysis, Energy Policy, 2004; 32(18):2067-2076.
    doi: https://doi.org/10.1016/S0301- 4215(03)00182-4
12. Ghajar RF, Khalife J. Cost/benefit analysis of an AMR system to reduce electricity theft and maximize revenues for Électricité du Liban, Applied Energy, Elsevier, 2003; 76(1-3):25-37. September. Available: https://ideas.repec.org/a/eee/appene/v76y2003i1-3p25-37.html.