Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 9 Issue 4, April - 2022

Development of an Energy Theft Detection and Location System for Low Voltage Power Distribution Networks

Eric Nta [1] **Dr. Kingsley Udofia** [2] **Dr. Nseobong Okpura** [3]

Department of Electrical/Electronic and Computer Engineering, University of Uyo, Uyo, Nigeria
engrericnta@gmail.com kingsleyudofia@uniuyo.edu.ng nseobongokpura@uniuyo.edu.ng

***Abstract* — Many households indulge in different forms of electricity theft and illegal tampering of electric metering devices leading to system faults and overload as well as loss of revenue by distribution companies. This work presents a unique method for energy theft detection in a low voltage power distribution networks involving analysis of line parameters with focus on radial network. The power distribution network was modelled with typical network parameters and consumer loads. Again, a real network was inspected and the physical structure modelled with simulated consumer and theft loads. Under conditions of no theft using the smart meter electrical outputs at each consumer end and section line parameters, the developed program was first initialized. The resulting matrix of consumer service conductor resistances obtained was stored for used in the theft detection algorithm. Energy theft detection including multiple energy theft was achieved by comparing the pole node voltages at each pole computed with reference to all connected consumer nodes using the stored service conductor resistances. The differences were evidence of energy theft, unpermitted power/energy consumed was estimated. For energy meter bypass, evidence of energy theft was due to the differences between consumer branch currents and meter current or significant drop in voltage at consumer end. Where zero reading was obtained from energy meter, total disconnection of meter was suspected. Again, theft power/energy was estimated. Results showed 99 percent accuracy in service line resistance computation. A variation in computed/detected illegal energy within nodes and sections was in the range of 50Wh to 210Wh and above 92 percent accuracy of theft detection was obtained. With this work, legal consumers will be protected from the negative impact of energy theft while distribution companies will be able to increase revenue and potential for sustainable electricity supply.**

Keywords— Electricity theft; distribution system; meter bypassing & tampering; Power Distribution; Electrical Energy Theft Detection.

I. INTRODUCTION

Electricity is one of the greatest technological innovations of mankind. It has now become a part of our life and one cannot think of a world without electricity. Almost all devices at home and industries run because of electricity. Electricity needs to be protected for efficient power delivery to consumers. Generation, transmission and distribution of electrical energy involve many operational losses. Such losses are inevitable in the provision of electrical energy; even technologically advanced countries cannot make all the electricity generated available for consumers. These losses are broadly divided into two: technical and non-technical losses. Technical losses occur because the electrical equipment used in the power system, by nature have losses associated with them which cannot be totally eliminated. On the other hand, non-technical losses (also called commercial losses) occur due to energy theft, poorly estimated billing, defective metering equipment (either deliberately tampered with or not), unpaid bills etc. They are generally caused by actions external to the power system and cannot be empirically computed like the technical losses [1].

Electricity theft has been defined as the illegal use of electric power with the intent of evading tariff payment [2-3]. Energy theft can be done by tampering with meters to make them undercount, bypassing the meters, making illegal connections, colluding with utility company meter readers to falsify consumption data or billing department to alter the bill issued to the customers [1-2,4]. Basically, there are four main ways that electricity can be accessed illegally. Electricity can be fraudulently accessed through illegal hook-ups, meter tampering or bypass, billing irregularities and unpaid bills [5].

Many households indulge in different forms of electricity theft and illegal tampering of electric metering devices leading to system faults and overloading of power lines, increase billing on the part of legal consumers as well as loss of revenue by distribution companies [5]. A huge amount of revenue is lost due to electricity theft [6]. Poor power quality, network infrastructure challenges (overloading of the

transmission line, feeders and transformer), fire, load shedding/grid energy inefficiency and instability, equipment failure/damages, death, irregular supply, fault, tariff challenges and revenue shortfalls (non-cost reflective tariffs, low collection efficiency), metering challenges (huge metering gap, estimated billing, poor meter maintenance), operational challenges (long feeders, quality of workforce, large operational areas), funding challenges and unemployment are some of the technical consequences of electricity theft [7].

The Nigerian scenario of electricity theft is a pathetic one. The development of poor countries like Nigeria has been hampered by electricity shortage [8]. One of the problems preventing the development of the electricity sub-sector in Nigeria is the history of the nation, which sees it emerging from a mentality that views electricity as a non-tangible item with worthless value. Until recently, many Nigerians did not see electricity theft as a crime against the provider of the commodity as well as a crime against other consumers. Recently, there has been the development of more policies and stronger legislative power to deal with those who take part in the fraudulent extraction of electricity. Under the law, electricity theft is punishable in Nigeria [2,9]. Electricity theft is a threat to the entire value chain. Although its impact is borne substantially by the Discos in terms of loss of revenue, the overall effect of theft of electricity affects the value chain in totality. Distribution companies recently published that it loses N21billion annually to electricity theft, thus amounting to an estimated average of N231 billion for the entire industry [10]. The Enugu Electricity Distribution Company (EEDC) reported a loss of about 43% of its expected monthly revenue to energy theft. There is an estimated average loss of about N21 billion annually in the power sector to energy theft [11-12].

In this paper, we present a unique method of electricity theft detection and location in a fully metered smart grid through analysis of line parameters. Modelling/simulation was done with MATLAB. This paper is organized as follows: Heading II, describes the network structure, parameters/electrical variables used for analyzing the network and development of algorithm; heading III explains the different scenarios of theft detection model that were developed; the results from a case study network including conclusion are presented in heading IV. Acknowledgement and references make up heading V.

II. DESCRIPTION OF NETWORK STRUCTURE, LINE PARAMETERS, ELECTRICAL VARIABLES AND ALGORITHM

An overhead radial network is selected for this work based on the typical installation in the Nigerian power distribution system as shown in Figure 1. The three-phase transformer primary is supplied at 11 kV while the secondary produces a rated voltage of 0.415 kV, phase to phase and 240V, phase to ground. Consumers are supplied at the phase voltage of 240 V. The three phases of the transformer as well as the neutral are connected to the distribution lines suspended from concrete or wooden poles with insulators. Stranded bare aluminium conductors - All Aluminium Conductors (AAC) are used for the distributors; while four-core 0.6/1 kV aluminium cable with cross linked polyethylene (XLPE) insulation and polyvinyl chloride (PVC) sheath, sometimes with steel wire armoured (SWA) is used for the cable riser connection from the feeder pillar to the first pole of the network. The conductor parameters of critical importance in this work are the resistance, capacitance and inductance; values sourced from a typical manufacturer (13). The distribution network was therefore modelled as a short line with the impedance computed for each distributor. The same treatment is applied to the service entry conductor although its impedance value is assumed to be unknown and is determined through the algorithm presented in this work. Consumer loads are connected to the network at poles; the loads are modelled as a mix of constant impedance and constant power loads. The smart meter for each consumer is expected to transmit readings of the load current, voltage and other parameters to the central station for the network analysis; the meter at the distribution station transmits the total current drawn from the transformer and terminal voltage.

A. Line Parameters and Electrical Variables

Fig.1 shows the network labelled with parameters to be used for the analysis of the distribution network; a description of each parameter is provided in Table 1. A description of electrical variables used is also provided in table 2.

Table 1: Network Parameters for Energy Theft Detection

Parameters	Description
R_{d1}	Impedance of XLPE riser cable – known
R_{dn}	Impedance of distributor or section-known
R_{sn_m}	Service conductor resistance from pole n to consumer node n_m, is unknown and is calculated using the algorithm.
P_n	Poles or nodes are located and numbered serially
P_{n_m}	Consumer node m connected to pole node n
V_{n_m}	Voltage at n_m to be calculated for pole nodes but known for consumer nodes.
I_{n_m}	Current at n_m to be calculated for pole nodes but known for consumer nodes.

Table 2: Network Electrical variables monitored for energy theft detection.

Electrical Variables	Description
Total transformer current, I_1 in amperes (known)	Compared with total current of legal consumers to identify theft.
Service conductor or branch current at each consumer node, I_{n_m} in amperes (Known)	Used for computations to determine pole node voltage and for comparison with total transformer current.
Transformer phase to ground voltage, V_0 in volts (known).	Utilized for the computation of pole node voltages.
Voltage at each consumer node, V_{n_m} in volts (Known).	Applied for the computation of pole node voltages for comparison.
Smart Meter Current and Voltage, I_{n_m} and V_{n_m}(Known)	To determine possible cases of Meter bypass

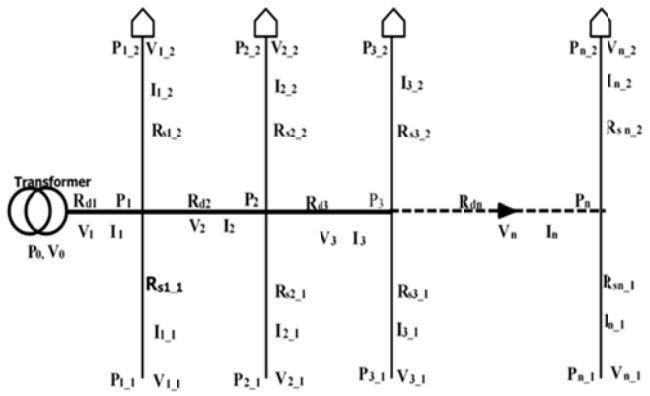

Fig. 1. Radial Network for Low Voltage Power distribution (Urban Area)

B. *Development of Algorithm*

The approach is to detect the differential change in the pole node voltage as a result of energy theft. For instance, under no-theft conditions, with reference to node P_{2_2}, V_2 can be obtained as follows;

$$V_2 = V_{2\_2} + I_{2\_2} R_{s2\_2} \quad (1)$$

The same voltage can be projected from P_0 and P_{2_1} to give (2) and (3) respectively.

$$V_2 = V_{2\_1} + I_{2\_1} R_{s2\_1} \quad (2)$$

$$V_2 = V_1 - I_2 R_{d2} \quad (3)$$

Similar analysis can be replicated across the entire network. These computed pole node voltages are equal provided there is no unauthorized connection at one of the nodes.

III. MATHEMATICAL MODELING OF ENERGY THEFT DETECTION

The system is first initialized under condition of no theft. The initialization process occurs only under conditions of no theft and it involves using the available system voltage/current data to compute the unknown consumer branch resistances in order to verify accuracy of the model and store branch resistance data for use in future theft detection computations. The pole node voltages are computed using (3) and Kirchhoff's Current Law (KCL) repeatedly along the line. The consumer branch resistances are then computed using (1) or (2) and stored for use in the theft detection algorithm.

It must first be established using (4) that the sum of reported currents from the smart meters at all the customer nodes, I_{n_m} is less than current I_1, supplied from the transformer. If this is true, then such difference will be indicative of energy consumption that is unauthorized. The specific location of theft is determined as a percentage of service of service line using the theft detection algorithm. For the section line, location of theft was estimated as a fraction of the total length of the section conductor or distance between poles estimated as 25 metres for urban area. Five different scenarios including energy meter bypass, theft along service conductor, direct online tapping from section conductor, direct multiple tapping from section conductor and illegal tapping at pole node were identified. They have been analyzed as follows;

$$\sum_1^n \sum_1^m I_{n\_m} \quad \neq \quad I_1 \quad (4)$$

A. *Scenario 1 – Energy Meter Bypass*

Fig. 2 demonstrates three cases of energy meter bypass at three different consumer locations. These are shorting of phase line, disconnection of meter from loads and outright disconnection of meter from load and supply line. Let the theft currents for each of the bypass be, I_{A_m}, I_{B_m} and I_{C_m} respectively while current recorded by energy meter is I_m.

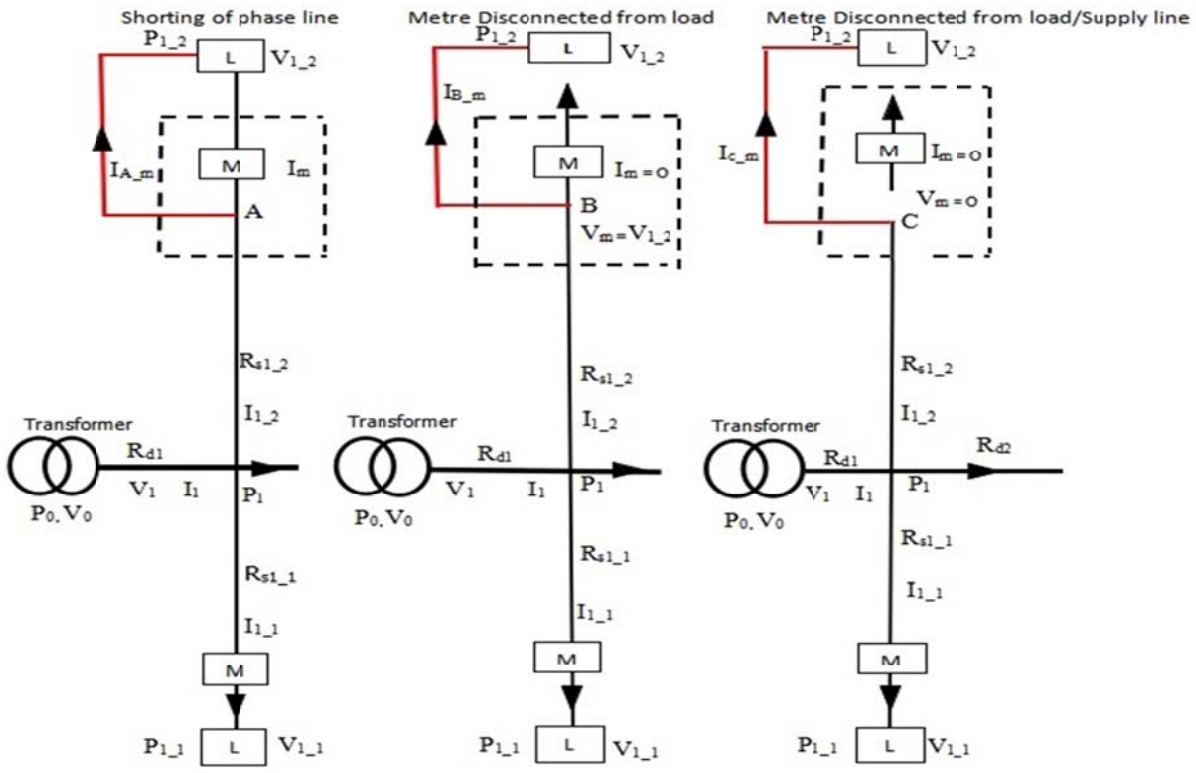

Fig. 2. Energy Meter Bypass

Case A: Shorting of the Phase Line at Point A: Much of the current and power is passed through the shorting wire to the load so that I_{A_m} is greater than I_m. Theft voltage, V_t is the same as terminal voltage, V_{1_2}.

$$\text{Theft current, } I_1 = I_{A\_m} + I_m + I_{1\_1} \quad (5)$$

$$\text{Theft power, } P_t = I_{A\_m}(V_1 - I_{1\_2}R_{s1\_2}) \text{ or } I_{A\_m} V_{1\_2} \quad (6)$$

CASE B: Disconnection of meter from Consumer loads: The analysis is similar except that consumer current, I_{1_2} is the same as theft current, I_{B_m} since the meter is recording zero current, $I_m = 0$. Theft voltage (V_t) or meter voltage is the same as the terminal voltage, V_{1_2}.

CASE C: Complete Bypass of Energy Meter: Consumer load and supply line are completely disconnected from energy meter and connected directly so that meter current, I_m and voltage across meter, V_m are zero. Theft current, I_{c_m} is equivalent to consumer branch supply current, I_{1_2} and energy theft voltage, V_t is the actual voltage received by the consumer (terminal voltage).

B Scenario II – Direct Online Tapping from Section Conductor

Consider the case where there is energy theft at a point A which is L_{2A} meters from P_1 as depicted in Fig. 3 resulting in flow of theft current I_{2A}. The length of the distributor or section P_1 - P_2 is L_2. The resistance of the conductor between P_1 and theft point A is R_{d2A}. Let the calculated current flowing in the section P_1–P_2 (using the reported consumer load currents with no knowledge of energy theft) and entering the node P_2 be I'_2 and the associated node voltage at node P_2 be V'_2. The actual current reaching P_2 is still I_2 (though I_2 + I_{2A} is leaving P_1) and the actual node voltage is still V_2. Detection and location of the theft is accomplished by application of (7) to (11).

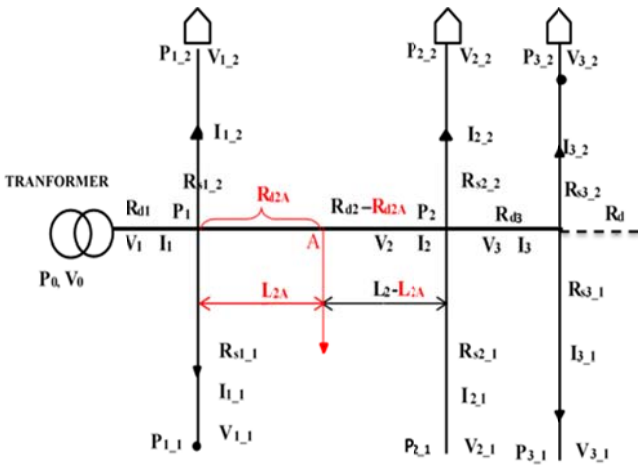

Fig. 3. Distribution Network with Energy Theft along Section Conductor

$$V_t = V_2 - V'_2 = I_{2A}(R_{d2} - R_{d2A}) \quad (7)$$

$$I_{2A} = I_1 - I_{1\_1} - I_{1\_2} - I_{2\_1} - I_{2\_2} - I_3 \quad (8)$$

$$R_{d2A} = R_{d2} - \frac{V_t}{I_{2A}} \quad (9)$$

$$\text{Location of theft point, } L_{2A} = \left(\frac{R_{d2A}}{R_{d2}}\right) L_2 \quad (10)$$

$$P_t = I_{2A} (V_1 - (I_2 + I_{2A}) R_{d2A}) \quad (11)$$

C Scenario III – Energy Theft along Service Conductor

Fig. 4, demonstrates illegal connection at point, A which results in the flow of theft current, I_{1_2A}. Branch resistance up to point A is R_{S1_2A}. The pole node voltage, V'_1 calculated using (12) with reported consumer node current I_{1_2} and without knowledge of power theft is expected to be different from the actual node voltage, V_1 by '$I_{1\_2A}R_{S1\_2A}$'. If **V** is the vector matrix of the different values of voltages for a pole node estimated from its connected service conductors, then, theft detection and theft power can be computed using (13) to (18) where L_{1_2A} is the distance from the pole to the theft point and P_t is the estimated theft power.

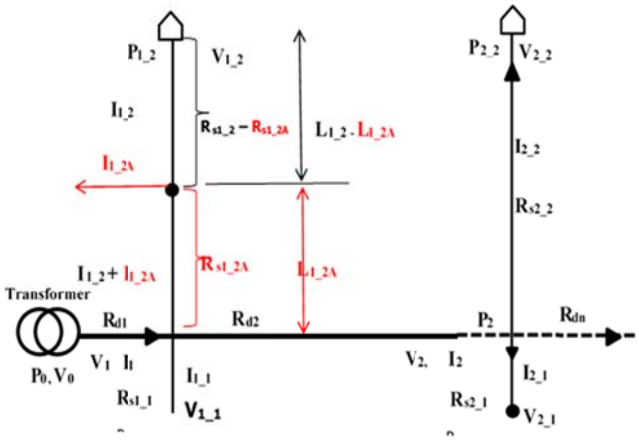

Fig. 4. Distribution network with energy theft along service Conductor.

$$V_1 = V_{1\_2} + I_{1\_2} R_{s1\_2} \quad (12)$$

$$V_t = \max(\mathbf{V}) - \min(\mathbf{V}) = I_{1\_2A} R_{S1\_2A} \quad (13)$$

$$I_2 = \frac{V_1 - V_2}{R_{d2}} \quad (14)$$

$$I_{1\_2A} = I_1 - I_{1\_2} - I_{1\_1} - I_2 \quad (15)$$

$$R_{s1\_2A} = \frac{V_t}{I_{1\_2A}} \quad (16)$$

$$L_{1\_2A} = \left(\frac{R_{S1\_2A}}{R_{S1\_2}}\right) L_{1\_2} \quad (17)$$

$$P_t = I_{1\_2A} (V_1 - (I_{1\_2} + I_{1\_2A}) R_{s1\_2A}) \quad (18)$$

D Scenario IV – Illegal Tapping at Pole Node

It is treated as a special instance of scenario II with the length, L_{2A} and impedance, R_{2A} being zero. The algorithm described for scenario II can be validly applied for the detection and location of this theft.

E Scenario V – Detection of Multiple Theft

First, is to establish using (4) that the sum of reported currents from the smart meters at all the customer nodes, I_{n_m} is less than current I_1, supplied from the transformer. Such difference is evidence of unauthorized energy consumption. Using the approached established for theft detection, the first illegal tapping closest to the supply end is detected. The value of this known energy theft is used for subsequent projection and detection of other energy thefts within the network as we gradually move away from the feeding point. But naturally, in a smart grid system, once it is designed to detect theft, the system implements and detect all energy theft automatically irrespective of the number of theft in the network. Installation of smart energy meter, computation of service line resistances and pole node currents/voltages are basic requirements for implementation.

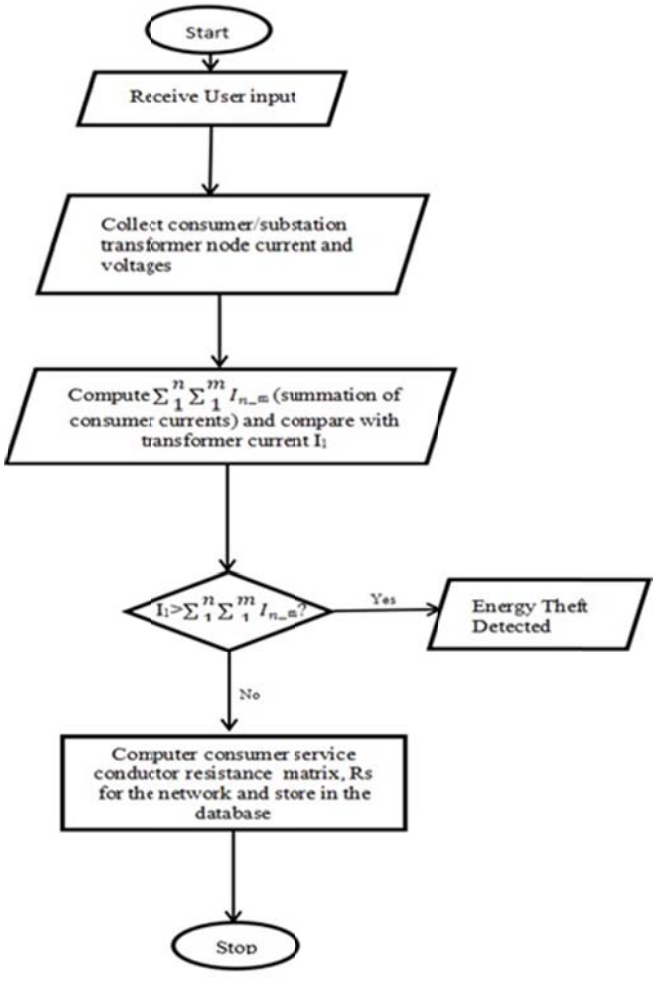

Fig. 5. Flow diagram for system initialization

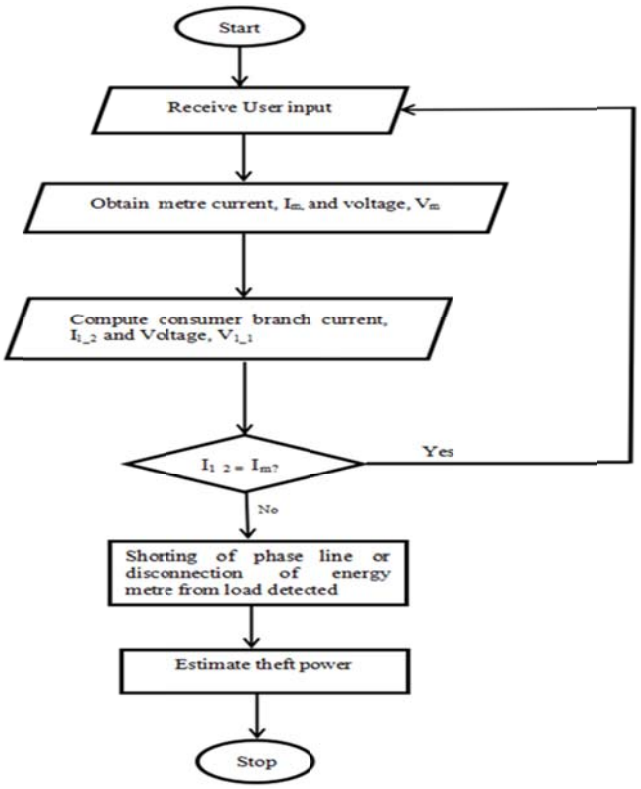

Fig. 6. Flow diagram for energy meter bypass detection algorithm (Shorting of Phase Line/Disconnection of Energy Meter from Load)

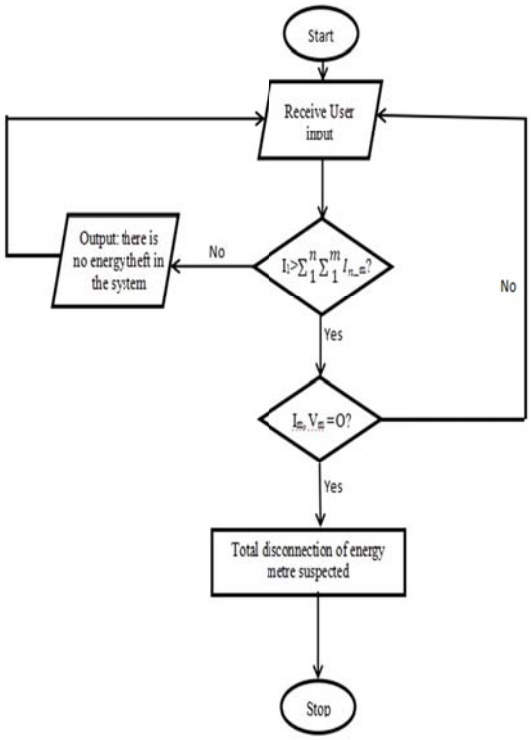

Figure 7: Energy Meter bypass (Total Disconnection of Meter)

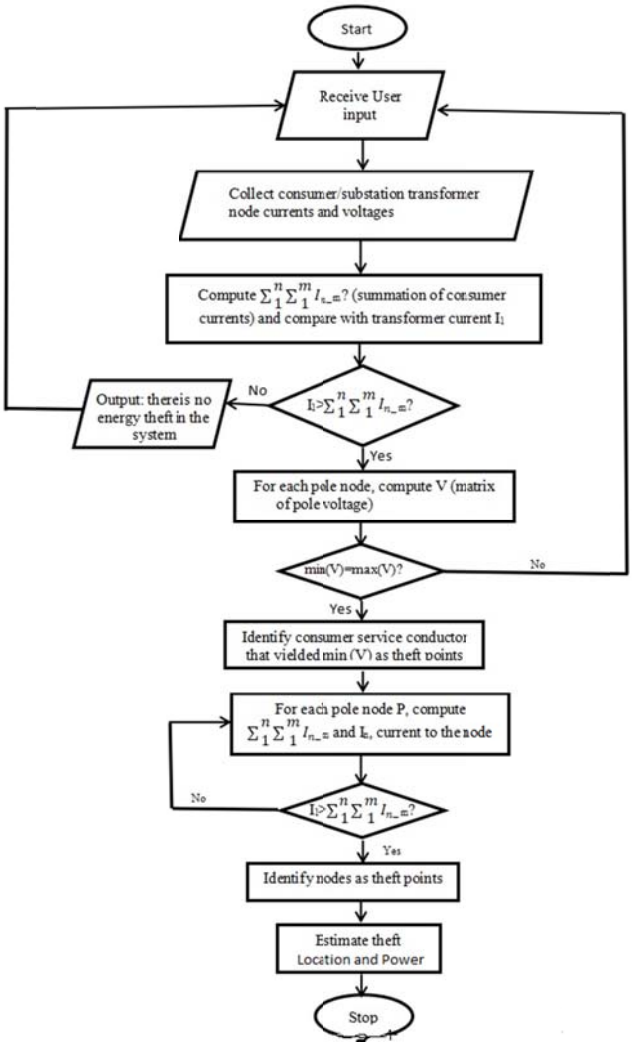

Fig. 8. Flow diagram of energy theft detection algorithm for the Study

IV. CASE STUDY: ETIM OKON USANGA STREET SECONDARY DISTRIBUTION NETWORK, UYO

Field survey was conducted at Etim Okon Usanga Street, a predominantly residential area in Uyo, Nigeria. The number of poles, distances between poles, conductor size of section; number, conductor size and length of consumer branches at each pole were enumerated. The network structure—a low voltage distribution system with aluminium conductors suspended from poles—was sketched. There are twenty-four poles and a total of sixty seven consumer nodes distributed across them. The section conductors are made of 95 mm^2 bare aluminium conductors while the branch conductors are made of 16 mm^2 single core aluminium cable. Riser cable is made of four-core 0.6/1 kV aluminium cable with cross linked polyethylene (XLPE) insulation and polyvinyl chloride (PVC) sheath with steel wire armoured (SWA). Conductor resistance were obtained from a cable manufacturer data book [13] while consumer load values were synthesized.

A. System Modelling, Energy Theft Detection and Location

The system was modelled in MATLAB (Simulink) on a balanced system basis. The system is designed for a symmetrical three phase system in a steady state. No unbalanced operations due to fault or short circuit is anticipated. It was first initialized under condition of no theft. The initialization process occurs only under conditions of no theft and it involves using the transformer and smart meter voltage/current data as input to compute the pole node voltages followed by unknown consumer service line resistances in order to verify accuracy of the model and store such resistance data for use afterward. 99 percent accuracy in service line resistance computation was obtained. Synthesized theft loads were subsequently connected to different points of the modelled network (Consumer end, section line, consumer service line and pole nodes) and the theft detection program was run to detect and locate the theft points. The theft loads inserted in the model were labelled as "modelled theft" while the values detected independently by the theft detection algorithm are labelled as "computed theft''.

For meter bypass, the synthesized theft loads were introduced to the consumer end such that it significantly suppressed the voltage output. Detection program was run to detect energy theft at consumer end. Output power of zero was returned when theft load was much higher indicating complete meter bypass.

Again, for multiple theft, several theft loads were connected to different points of the modelled network, program was run to detect them starting from the theft closest to the feeding point, one after the other as we progressed toward the end of the network. This is consistent with the earlier multiple theft model developed. But in practice, in a smart grid system, the theft detection system implements and detects all energy theft automatically irrespective of the number of theft in the network.

Procedure for locating theft point was by consumer node, pole location and estimation of the distance of the theft location from a reference pole in terms of percentage of service line using the theft detection algorithm. For the section line, location of theft was estimated as a fraction of the total length of the section conductor or distance between poles estimated as 25 metres for urban area. Unpermitted instantaneous rms power and energy consumed were obtained using the theft detection algorithm developed.

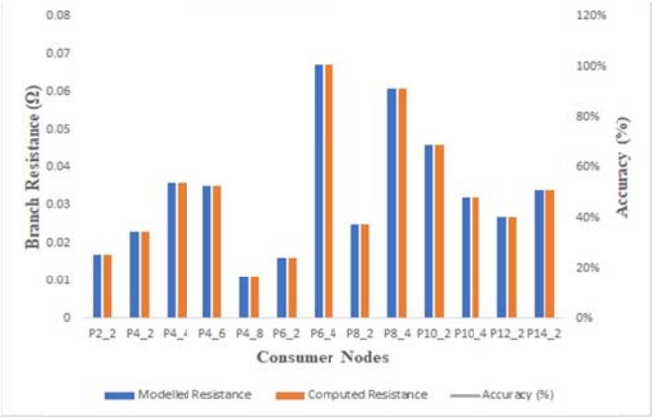

Fig. 9:Modelled/Computed Service Line Resistances (even)

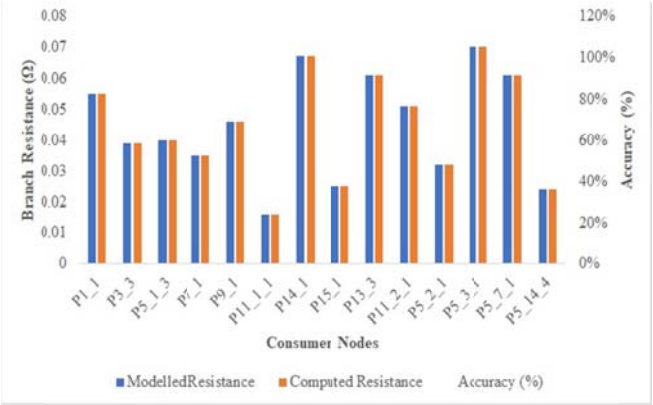

Fig. 10: Modelled/Computed Service Line Resistances (odd)

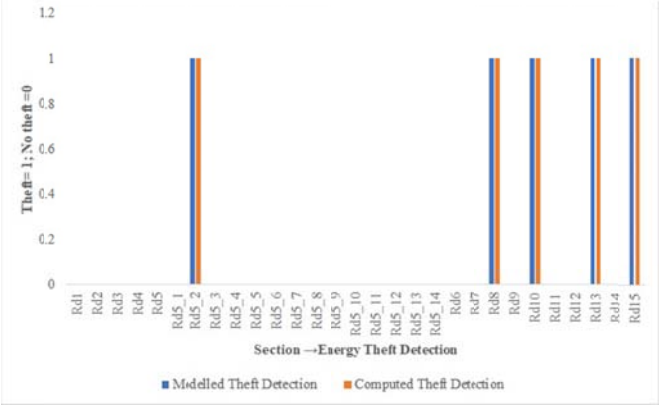

Fig 11: Modelled/Computed Energy Theft (Section)

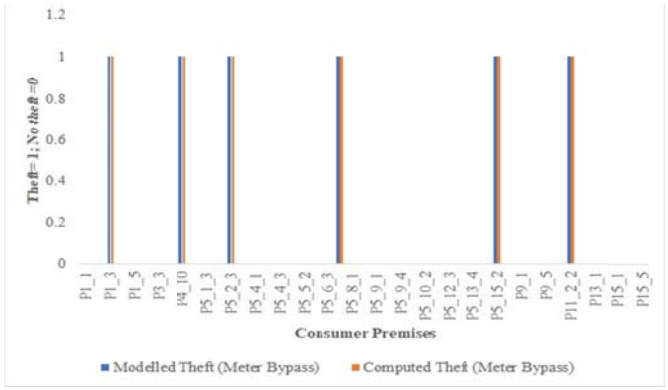

Fig 12: Bypassing of Energy Meter (Consumer End)

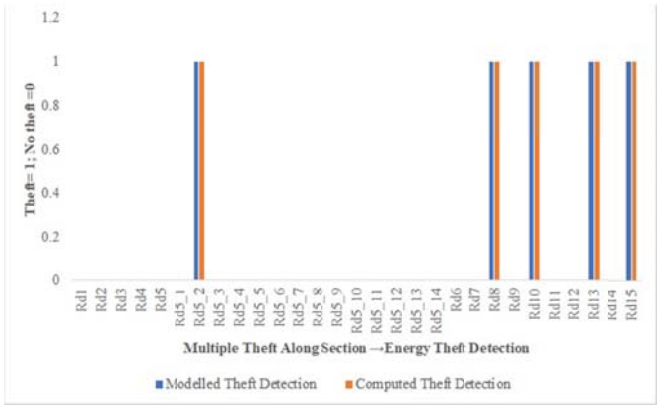

Fig. 13: Multiple Energy Theft along Section Line

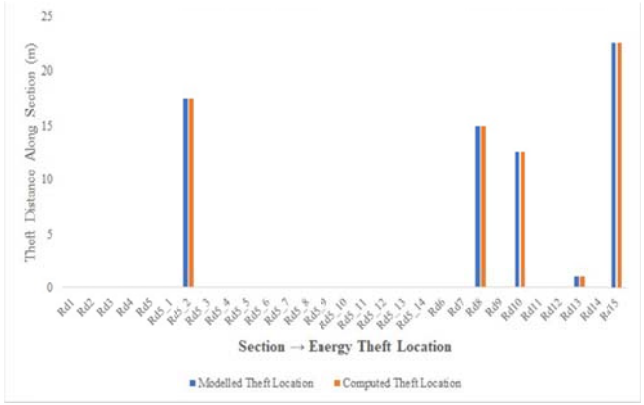

Fig. 15: Energy Theft Location along Section Line

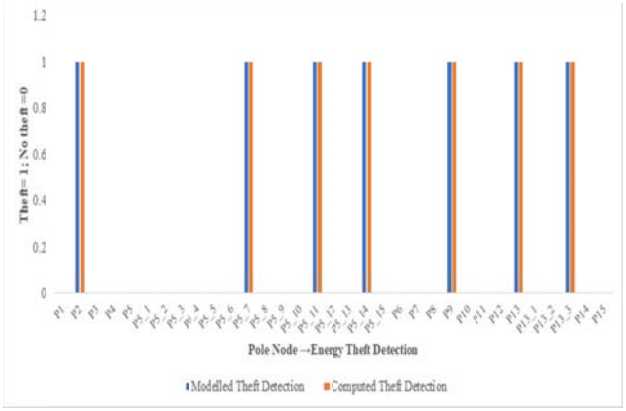

Fig. 14: Modelled/Computed Energy Theft at Pole Node

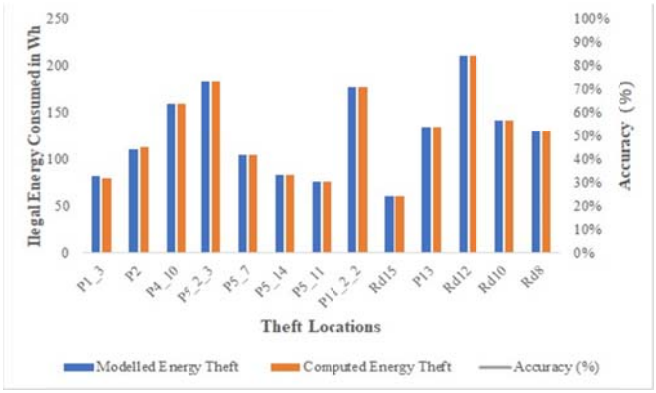

Fig. 16: Minimum Computed/Detected Illegal Energ

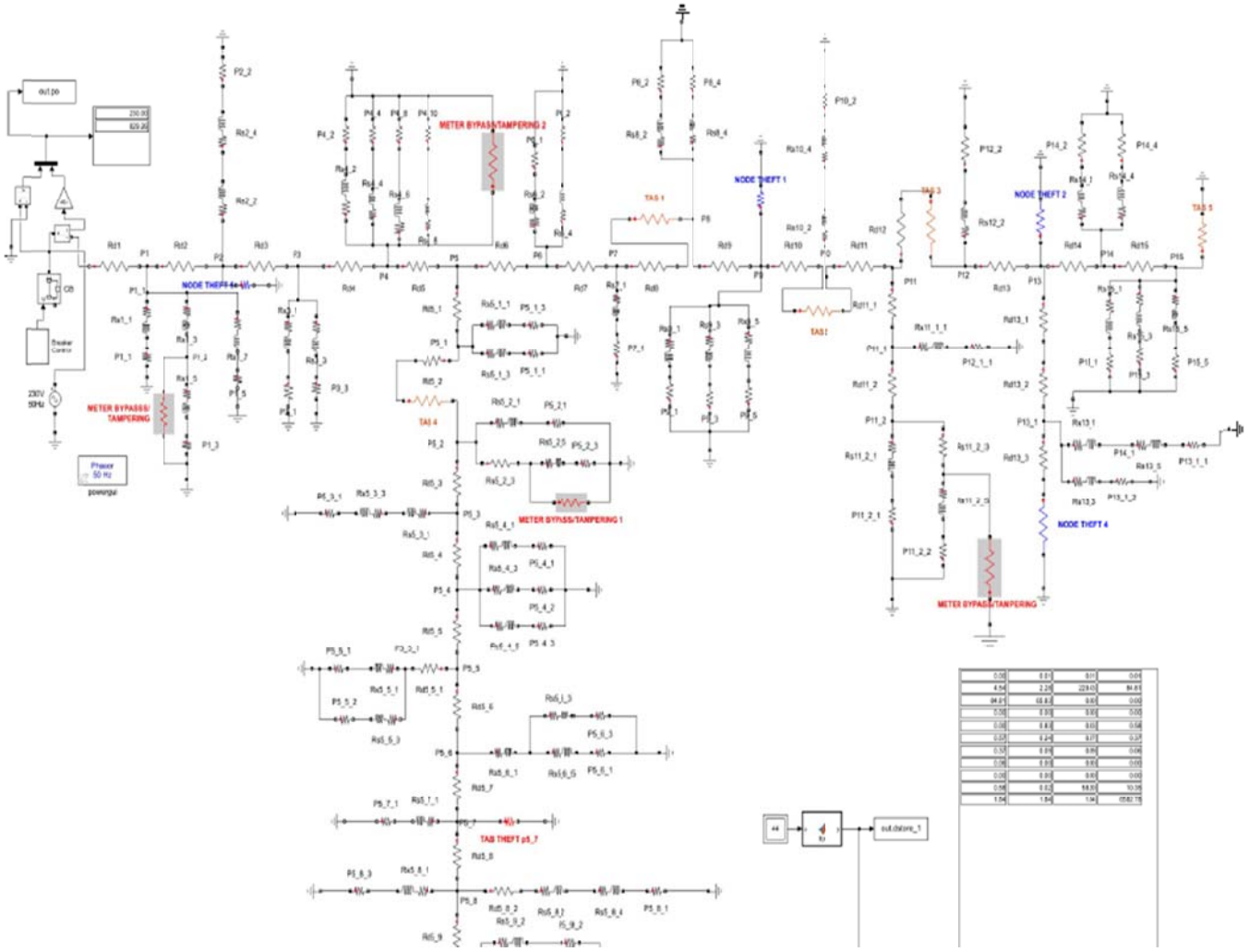

Fig 17: MATLAB Model of Etim Okon Usanga Low Voltage Distribution Network

B Conclusion

Many households indulge in different forms of electricity theft and illegal tampering of electric metering devices leading to system faults and overload as well as loss of revenue by distribution companies. This work presents a method for energy theft detection in a low voltage power distribution networks involving analysis of line parameters in order to detect differential line voltages for energy theft detection and location. The power distribution network was modelled with typical parameters and consumer loads. A case study network was also inspected and the physical structure modelled with simulated consumer and theft loads. The study also used the same method to detect different cases of energy meter bypass. Multiple energy theft scenario was also detected. With the necessary hardware for field application, this method is the answer to the perennial problem of pilferage of electricity.

V ACKNOWLEDGMENT

We would like to thank the Department of Electrical/Electronic Engineering, University of Uyo, Nigeria for providing the platform for this research.

REFERENCES

[1] O. M. Komolafe and K. M. Udofia, “Review of Electrical Energy Losses in Nigeria”. *Nigerian Journal of Technology (NIJOTECH), Vol. 39:* 246 – 254, 2020

[2] A. Adeniran, "Mitigating Electricity Theft in Nigeria," 14 March 2018. [Online]. Available: http://cpparesearch.org/nu-en-pl/mitigating-electricity-theft-nigeria/#. [Retrieved 20 May 2020]

[3] O. M. Komolafe and K. M. Udofia, “A Technique for Electrical Energy Theft Detection and Location in Low Voltage Power Distribution Systems”. *Engineering and Applied Sciences*. 5(2): 41-49, 2020.

[4] G. A. Abdulkareem, “Evaluation and Mitigation of Technical Losses on Power Lines: A Case Study of Nigeria 330-Kv Network”. PhD Thesis, Covenant University, Ota, Nigeria. 277p, 2016.

[5] D. O. Dike, U. A. Obiora, E. C. Nwokorie and B. C. Dike, "Minimizing Household Electricity Theft in Nigeria Using GSM Based Prepaid Meter", *American Journal of Engineering Research(AJER),* pp. 59-69, 2015.

[6] S. Arivazhagan, T. A. Atiso and M. A. Seid, "GSM and Arduino based Power Theft Detection and Protection". *International Journal of Advance Research, Ideas and Innovations in Technology*, 5: 581 – 588, 2019.

[7] S. Amin, G. A. Schwartz, A. A. Cardenas, S. S. Sastry, "Game Theoretic Models of Electricity Theft Detection in Smart Utility Networks," IEEE CONTROL SYSTEMS MAGAZINE, 35(1). 66-81, Feb.2015.

[8] M. Golden and B. Min, "*Theft and loss of electricity in an Indian State*. IGC-ISI India Development Policy Conference, University of California, Los Angeles. 2th – 4th January, 2012, 38p,

[9] S. Garba and D. C. Akpeneye, "Order on Unauthorized Access, Meter Tampering and By-Pass. Abuja: The Nigerian Electricity Regulatory Commission". 2017. https://www.energymixreport.com/nerc-reviews-penalties-electricity-theft-meter-passing/ (Retrieved on 25th May, 2020).

[10] O. G. Olaoluwa, "Electricity Theft and Power Quality in Nigeria". *International Journal of Engineering Research & Technology (IJERT)* Vol. 6, 1180 – 1184, 2017

[11] I. O. Joseph, "Issues and Challenges in the Privatized Power Sector in Nigeria". *Journal of Sustainable Development Studies*, 6(1):161 -174, 2014.

[12] A. Osigwe and C. Onyimadu, "Electricity Theft in Nigeria: How Effective Are the Existing Laws?" *Journal of Energy Technologies and Policy*, 8: 8 – 13, 2018.

[13]Coleman Cables and Wire, "Coleman Cables and Wire,"[Online].Available:http://www.colemancables.com/products/catalogCTIL_Aerial_Cable_Brochure/AERIAL/AAC/ACSR%20CABLE/.[Accessed 15 October 2021].