IoT Based Non-Technical Loss Detection and Mitigation System for Power Distribution Networks

Emmanuel M. Eronu, Matthew O. Oboh, Emeka S. Ezeh, Gafar Tiamiyu, and Farouq E. Shaibu

Abstract—Electrical Energy crisis is a major problem faced in the world today and it's increasingly significant in this part of Africa. A perfect solution seems not to be feasible as several solutions have been proposed in the past by various authors with little impact on the power sector. In this work, we present a method of Non-Technical Loss (NTL) detection consisting of a microcontroller interfaced with a current sensor that measures the current on the power line. A sensor node is placed at the supply end of the pole while two or more others sensor nodes are connected to the output of the pole depending on the number of consumers. The measured value of current is sent via the microcontroller to a web cloud that is accessible by the consumers and the utility company from any part of the world by simply logging on to the website; www.electricity-theft.herokuapp.com. The design uses the principle of Kirchhoff Current Law (KCL) to achieve this aim. The consumers can therefore monitor their power consumption from any location in the world and prevent theft on the network. The results obtained from the installation of the sensor nodes were analyzed using correlation and regression analysis. A correlation analysis of the data results gave us a correlation coefficient of 0.9802, while a regression analysis provided us with a linear relationship between the dependent and independent variable expressed mathematically thus $Y = 0.916x + 0.254$. A regression graph is also plotted. Furthermore, a T-Test and F-Test was conducted to statistically test the sensor nodes. A NodeMCU Wi-Fi microcontroller and a self-powered Phidget current sensor is used for the sensor node design. Communication between the sensor nodes is via Wi-Fi while a 4G router was used to provide internet services.

Keywords —NTL, IOT, 8266 microcontroller unit, Phidget current sensor, KCL.

I. INTRODUCTION

Electricity has become a very essential tool in this growing technological age and time. It is important for the day to day running of both the private and public sectors of a country. It is essential for the growth and development of the society and so therefore needed by everyone. The development of any country is a function of its electricity generation and distribution and also its demand is directly proportional to the population of the country. The availability of electricity is in question in most developing countries especially in Nigeria. The Nigerian power company formerly called National Electric Power Authority (NEPA) was privatized some years ago so as to improve on the availability of power to its citizens

but till today no meaningful progress has been made whatsoever. Even with billions of dollars invested by several administrations on the power section, there have been no visible positive changes in the sector of the economy. A major problem has been as a result of consumers not willing to pay for what they use which results to Non-Technical Losses. According to Amar P. *et al* [2], Electricity is more than a necessity in the modern world. The power utility companies are saddled with the responsibility of providing adequate electricity to the masses but are most times crippled with the amount of losses associated with power systems, therefore the need to adequately reduce NTL in the system. NTL are common in developing nations as compared to developed nations. As population increases, so also the demand on electricity increases. A major problem associated with the non-availability of electricity is electricity theft. Electricity theft can be defined as using electricity by illegal means with the aim of not paying for it [4]. [5] Defined electricity theft as a criminal practice of stealing electrical power. Power theft leads to commercial losses. Commercial losses are also called non-technical losses (NTL) and come in several forms such as [2] meter bypassing, unpaid bills, irregular bills, rigging the power line, underpaid bills etc. The other type of loss is the Technical Loss (TL). Technical losses (TL) are losses that occur naturally and consist mainly of power dissipation in electricity system components such as the transmission and distribution lines, transformers, and measurement systems [4], [6]. TL are existent because the equipment used for power generation, transmission and distributions are non-ideal [7] and by nature have losses associated with them.

The major forms of TL are at the distribution level [9]. These includes the I^2R losses at the distribution lines, dielectric losses in cables, transformer winding losses, hysteresis loss, eddy current losses and even losses on the meters. The difference between TL and NTL can be seen from the fact that while TL can be calculated and estimated but cannot be eliminated from the system, NTL can be eliminated or reduced to a barest minimum. TL can be reduced by use of standard quality materials and obeying stipulated regulations [9], [11].

NTL on the other hand are losses external to the power systems. NTL are estimated as the difference between the total losses and the TL [12]. These forms of losses can be estimated and represent a major form of revenue loss to the Power utility companies. For example, it is estimated that electricity theft cost the USA / global power industry \$6

Submitted on November 29, 2021.
Published on December 29, 2021.
Emmanuel. M. Eronu, University of Abuja, F.C.T, Nigeria.
(e-mail: eronu.majiyebo@uniabuja.edu.ng)
Matthew. O. Oboh, University of Abuja, F.C.T, Nigeria.
(e-mail: omofabregas@yahoo.com)

Emeka S. Ezeh, University of Abuja, F.C.T, Nigeria.
(e-mail: ezehspeemeka@yahoo.com)
Gafar Tiamiyu, University of Abuja, F.C.T, Nigeria.
(e-mail: ktiamiyu1967@gmail.com)
Farouq E. Shaibu, Federal Radio Corporation of Nigeria, F.C.T., Nigeria.
(e-mail: farouqebira@gmail.com)

billion / \$25 billion annually respectively [13]. A survey of Nigeria electric power system losses due to theft was estimated between 2014 & 2018 and the result shows a loss of 56% of total power distributed. Electricity theft has been recorded to resulting to about 30% revenue loss of power utilities [14]. In Nigeria, the NTL far exceeds the TL [7] and these has made the utility companies to either run at a lost or over bill the legal costumers which makes it seems as though electricity is expensive. The need to adequately and automatically reduce non-technical loss is the main purpose of this project work. Detection of electricity theft and NTL involves a very difficult process and requires continuous monitoring to reduce fraud [9]. Over the years, several methods and techniques have been developed to reduce NTL on power systems; these methods will be discussed further in the literature review. This dissertation work aims at designing a model that will monitor usage of electricity by consumers and send same data to a web cloud for analysis and to detect electricity theft occurring at power poles and energy meters. The model is a pole mounted design and will be connected just before supplying the consumer's building. The design uses the simple model of Kirchhoff's current law (KCL) which states that the total current entering a node is equal to the sum of all the current leaving the node. A constructed 3 sensor nodes are used for this purpose. These 3 sensor nodes are IOT (Internet of Things) based devices and communicate with one another via Wi-Fi and powered by a 4G Internet connection. The current value entering the pole is estimated by a sensor node and it is used to compare the current values leaving the node to the respective consumers measured by two other sensor nodes and uploads the results to a website. The design uses a NodeMCU (node microcontroller unit) and a Phidget current sensor as the major components of the construction. The current sensor and NodeMCU microcontroller are specially chosen because of the properties they have that is useful for power systems and space. Other components used for this construction includes op amp, diodes, resistors, filters and other discrete components. The results obtained are uploaded to www.electricity-theft.herokuapp.com and is accessible to everyone by simply logging in. The results are tabulated in several columns and the difference between the currents input and output at the node explained by KCL is also determined by the sensor nodes and uploaded. So, by just viewing the website, we can easily see when there is a theft on the network or not. Some statistical analysis was carried out to test the sensor nodes and the results obtained. This analysis includes correlation analysis and regression analysis. Also, a T-Test and an F-Test was used to test how statistically viable the results are.

Several techniques were proposed in the past for detecting and reducing non-technical losses (NTL). Electricity theft is synonymous with NTL and can be defined as using electricity from the grid network with the intention of not paying. In other words, power theft is using electricity illegally. To be able to fully understand and detect non-technical losses in the system, we need to evaluate and put into consideration the technical losses that are part of the system [7], losses that are due to the operation and transmission of energy [7] in the distribution network. Technical loss is equivalent to I^2R loss and cannot be avoided as long as conductors are concerned. From I^2R loss formula, the loss depends on value of current

and it has maximum value during peak load. Technical loss can also be caused by phase imbalance, improper joint & extraneous factors such as tree touching [15]. Non-Technical losses are the other forms of losses accounted for in the system. They are avoidable forms of losses which can be drastically reduced by putting in measures to stop theft of electricity.

The technical losses are due to energy dissipated in the conductors, equipment used for transmission line, transformer, sub transmission line and distribution line and magnetic losses in transformers. Technical loss occurred at transmission lines, power transformer, feeder and terminal which it depends on current in lines (I^2R) [16]. TL occurs because of the joules effect on power lines and transformer loss during the transportation of electricity [16]. The TL cannot be stopped completely, but it can be reduced by applying some modification and techniques throughout the system. It is worthy of note that the unit of electric energy generated by Power Station does not match with the units distributed to the consumers. Some percentage of the units is lost in the distribution network.

There are two types of Technical Losses in the power systems which are Permanent / Fixed Technical losses and Variable Technical losses [18]. Permanent losses do not vary with current while variable technical losses vary with changes in current values.

Non-Technical losses are losses due to electricity theft, non-payment of electricity bills or undetected load. It can also be called commercial losses because its mainly power used by consumer and not paid for, thereby causing increase in tariff on the legal consumers [19].

Non-technical losses include but are not limited to the following causes reported in [20]:

- Meter tampering in order to record lower Consumptions;
- Bypassing meters by rigging lines from the power source;
- Arranged false meter readings by bribing meter readers;
- Faulty or broken meters;
- Rigging of the power lines;
- Unauthorized tapping;
- Estimated billing;
- Unmetered supply;
- Technical and human errors in meter readings, data processing and billing.

In recent times, cyber tampering has become a way to malevolently change the consumption data patterns of the smart meter, which decreases the bill for the users [21].

II. METHODS

The block diagram in figure 1 is a typical diagram showing the principal parts of the design of non-technical loss detection and mitigation sensor node. It consists of the microcontroller block which is the brain behind the design. The microcontroller used for this project is ESP8266 Wi-Fi Microcontroller. It is a reprogrammable type of controller that is Wi-Fi enabled. The microcontroller can be programmed to communicate with other controllers. The current sensor is another important component used in this design. The current sensor used for this project is a Phidget current sensor. It's a

self-powered sensor that estimates with very low degree of error the amount of current passing through its opening. Other blocks include the voltage divider and the power supply block.

Fig. 1. Block Diagram of a Typical Sensor Node.

The sensor node used for this design is pole mounted to prevent access to by consumers. For the purpose of this work, we have designed 3 sensor nodes, one sensor node will be used to measure the current from the source (sensor node c), while the other 2 sensor nodes will be used to measure 2 household connected to the source on the same pole i.e., sensors node A and B. So, at every point in time, when there is power supply from the source, the source current (I_s) must be equal to I_T the sum of the currents at consumer points 1 and 2; i.e., I_1 and I_2 obeying Kirchhoff's current law.

Fig. 2. Conceptual framework diagram.

Mathematically,

$$I_s = I_T = I_1 + I_2 \quad (1)$$

If at any point there is a big difference between the source current I_s and the total of the consumer's current I_T , then it is assumed that an illegal consumer is on the network thereby detecting theft.

$$I_s \approx I_T \text{ no theft} \quad (2)$$

$$I_s \neq I_T \text{ theft} \quad (3)$$

The basic component of the design consists of a NodeMCU microcontroller and a Phidget sensor as its major components. Other discrete components are used also for the design.

A. Phidget Current Sensor

I-Snail-VC is a self-powered AC Current transducer. It provides a 0-5V dc analog signal proportional to the AC

Current flowing through the device wire window. It is an ideal device for load monitoring without the need for an external power supply. It has fixed ranges to ensure superior accuracy and eliminate configuration and adjustments in the field, thereby saving time. However, I-Snail-VC current transducer measures the current in a single AC wire (either positive or negative) that passes through the window opening. If both wires (+ and -) are put in the same window, the resultant is a null voltage value.

The formula for converting output voltage to AC amp (RMS) is:

$$AC \text{ Amps (RMS)} = V \times 20 \quad (4)$$

1) Sensor properties

Sensor type – current.

Output voltage – 0-5 V.

Input current – 0-100Amps.

Current measurement resolution – 100mA.

Fig. 3. Connection of a Phidget current sensor.

B. NodeMCU Microcontroller

The microcontroller used for this design is an ESP 8266 NodeMCU (Node Micro-Controller Unit) chip. The abbreviation ESP stands for Expressif systems platform. It is a high performance, high integration wireless chip designed for space and power constrained designers. It offers a complete and self-contained Wi-Fi solution. It is amongst the most integrated Wi-Fi chip in the industry and can be integrated to an external sensor and other applications through its GPIO (General Purpose Input and Output Interface).

Its low power consumption is a feature that makes it most suitable for mobile, wearable electronics and Internet of things applications. It operates its power architecture in 3 modes: active mode, sleep mode and deep sleep mode. It uses 3.3 V supply and 25°C ambient. It is embedded with memory controller including SRAM and ROM, RAM size <36 kb. An external spi flash is used together with the MCU to store user programs up to 16Mb memory capacity can be supported. There are 17 SRAM pins that are configurable.

(a)

(b)

Fig. 4. (a) NodeMCU microcontroller unit (b) NodeMCU microcontroller pin assignment.

III. CONSTRUCTION OF THE SENSOR NODE MODELS

The sensor nodes A and B as shown in Fig. 2 is connected to the consumers 1 and 2 to measure their current usage, while sensor node C is connected at the source end of the pole to measure the current that gets to the pole from the distribution transformers.

Fig. 5. Sensor node A.

Fig. 6a and 6b are the pictorial views of the designed sensor nodes used for the detection of electricity theft on the distribution network.

IV. CIRCUIT DIAGRAM

The circuit diagram for the sensor node design is shown in figure 10 below. The sensor node consists basically of the Phidget current sensor, a Wi-Fi NodeMCU microcontroller, a reset module, and a power supply module.

The design consists of basically of 3 sensor nodes, 1 sensor node measures the current at the input side of the distribution network, while the other 2 measures the current through the load wires of 2 consumers connected to the distribution network via the same pole. These 3 devices are IOT (Internet of Things) devices and communicate with one another through Wi-Fi and Internet connections. They are connected to the Internet by any Internet enabled 4G device to enhance fast transmission of information about the current usage of

each consumer to the cloud which can be accessed by anyone around the world by simply logging on to the website.

(a)

(b)

Fig. 6. (a) Sensor node A and B (b) Sensor node C.

V. COMMUNICATION MODULE

Communication between the sensor nodes is via Wi-Fi while communication between the sensor nodes and the internet is via 4G. A router or Hotspur is provided for internet services so that the sensor nodes can send and receive data. The sensor nodes were programmed with a username and password for connecting to the internet. The embedded device is programmed to work with a back-end server. This is where the operations of the sensor nodes are carried out. The users/consumers communicate with the front-end server;

this makes it possible for the users to view their current usage on the website when they login.

VI. WORKING PRINCIPLE

When a current carrying conductor passes through the window of a Phidget current sensor, since it is a self-powered sensor, it gives the equivalent voltage value of the measured current passing through its window. This voltage equivalent of the current is fed into a microcontroller unit. For this design, the current sensor has an input of 0 - 100amp rating and an output of 0 - 5v. The microcontroller receives the

voltage input, processes it and sends the information about current consumption to the cloud service. The sensor node was programmed to receive and update data every minute. The microcontroller samples data every 10 seconds. Therefore, it obtains 6 data values in 1 minute, finds the average and sends it to the cloud service which can be accessed by the consumers and the utility company by logging to the website. This real time data values are constantly uploaded to the website so long there is power supply from the utility company and availability of Internet service. The sensor nodes are designed with 2 LED lights to serve as indicators for power and Internet connection.

Fig. 7. Circuit diagram.

Fig. 8. Testing the workability of the sensor models.

VII. ANALYSIS OF THE DATA RESULTS

The results obtained from the installation and testing of the sensor nodes are about 1288 data values and about 456 data values was used for our statistical analysis. This data points can be accessed anytime by logging into www.electricity-theft.herokuapp.com. It is expected that from the results

obtained, the sum of the current into the consumer's units be approximately equal to the source current from the pole. But this is not so, the difference between the source and total is either a positive or negative value. So, a relationship was established to explicitly explain the results.

Whenever source current is greater than the total currents to the consumers, we detect a form of illegal usage of power which could be as a result of theft.

But when source current is less than the total current to the consumers then there is no theft.

i.e., when source current $\gg$ total current = theft

Source current $<$ total current = no theft

So, at the points where source current $>$ total current, we obtain a positive difference value of current between the source and total and theft is assumed to have taken place as a result of illegal usage by a third party resulting in a higher source current value as compared to the total current sum from the legal users. But whenever the source current value

is less than the total current value (source < total), we obtain a negative difference value. Although this negative difference is not an ideal result as total current leaving a node cannot be greater than the total entering it. So, it is assumed that it's an error from the sensor nodes due to insensitivity of the Phidget sensor to small current values. So therefore, for a negative difference between the source current and the sum of the legal house currents, it is a no theft scenario.

One of the major importance of this design is to enable consumers calculate and estimate what they consume so that they don't feel cheated when they are billed by the utility companies.

A regression analysis is used to describe the relationship between a set of independent variables and the dependent one. "Regression", in simple terms is the average value of a dependent value y as a "function" of the independent variable x, that is, y with respect to x.

Regression analysis is carried out using the Microsoft excel software and results in a regression equation. The equation has coefficients representing the relationship between each independent variable and the dependent variable. The regression equation can also be used to make predictions and estimations. The result obtained using Microsoft excel tool is given in the Table I.

TABLE I: REGRESSION ANALYSIS SUMMARY OUTPUT

Regression Statistics	
Multiple R	0.980164
R Square	0.960722
Adjusted R Square	0.960635
Standard Error	0.906563
Observations	456

The Analysis of Variance (ANOVA) provides information about the levels of variability within the regression model. The Significance F-value is the most important value in the analysis of variance output. Significance F is the P-value of F. It gives an idea of how statistically reliable the results are. If Significance F is less than alpha (0.05), then the model is OK. But if it is greater than 0.05, then the sensor models are not effective.

Significance F = 0.

The value for significance, f, shows that the model is OK.

TABLE II: ANALYSIS OF VARIANCE
ANOVA

	df	SS	MS	F	Significance F
Regression	1	9126.365	9126.365	11104.56	0
Residual	45	373.123	0.82185		
Total	45	9499.48			
	5	8			

The most useful component in this section is the coefficients which enable one to build a linear regression

equation in excel. The regression analysis produces a linear equation which is related thus:

$$y = bx + a \quad (5)$$

'y' is the dependable variable which represents the sensor node C while x is independent variable which is a summation of the current variables of sensors node A and B.

Our linear regression formula goes thus:

$$Y = (\text{coefficient of node A+B})x + \text{Intercept}$$

Rounding up a and b values to three decimal places, and substituting in the equation gives:

$$Y = 0.916x + 0.254 \quad (6)$$

VIII. CONCLUSION

Non-technical losses accounts for a high percentage of total losses in the power systems. It takes a major form of power theft on distribution networks which has resulted in high cost of electricity production and high billing rate on the users. The major points of theft on the network are at the pole side and on the meter point. The pole side theft is normally carried out at nighttime when the service providers won't be able to go on inspections and sometimes during the day using a hook line method for use in a short period. At the meter point, the meters are either bypassed or manipulated to work slower than it's designed. So, the best means to solve this problem of theft is by electronic means through the use of current sensors that measure current usage at each pole to detect theft. This project work has proven to solve the problem of theft on the system by applying Kirchhoff's current law on each pole of the distribution network. The real time current values obtained from the website are analyzed for theft detection. Whenever the source current entering the pole is far greater than the total current coming out of the pole, it is assumed that an illegal consumer is on the network and adequate actions are taken. The sensor node design has proven to be a good innovation to the Power sector.

ACKNOWLEDGMENT

We sincerely appreciate the staff of the department of electrical and electronic engineering and the experts who have contributed towards the success of this work.

CONFLICT OF INTEREST

We do not have any conflict of interest.

TABLE III: REGRESSION ANALYSIS COEFFICIENTS

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95.0%	Upper 95.0%
Intercept	0.254299	0.079366	3.204139	0.00145	0.098329	0.41027	0.098329	0.41027
X Variable 1	0.916125	0.008694	105.3782	0	0.89904	0.93321	0.89904	0.93321

REFERENCES

- [1] Amar P, Shaikh N, Chowdhri B, Shariq A. Power Theft Detection Using Wireless System: A Distributed Approach for Power Theft Prevention. *International Journal of Student Research in Technology & Management*, 2015; 1(1):58-64.
- [2] Wikipedia. Electricity Theft. [wikipedia.org/wiki/electricity theft](https://en.wikipedia.org/wiki/Electricity_theft). 2020 Reference list.
- [3] Reddy DS, Lingfeng W, Vijay D. Electricity Theft: Overview, Issues, Prevention and a Smart Meter Based Approach to Control Theft. *Energy Policy*. 2010; 39:1007-1015.
- [4] Pavani JP, Sharma NK, Sapra S. Technical and Non-Technical Losses in Power System and Its Economic Consequence in Indian Economy. *International journal of electronics and computer engineering*, 2012; 1(2):757-761.
- [5] Pedro A. Reducing Technical and Non-Technical Losses in The Power Sector. background paper for the World Bank group energy sector strategy.2009.
- [6] Parmar J. Total Losses in Power Distribution and Transmission Lines. electrical engineering portal. 2013.
- [7] Antmann P. Reducing Technical and Non-Technical Losses in the Power Sector. Technical report, World bank.2009.
- [8] Wanniarachchi HRP, Wijayapala DAS. Modelling of Distribution Losses in an Urban Environment and Strategies for Distribution Loss Reduction. *The institute of engineers*, 2016; 45 (3):21-32.
- [9] Otuoze AO, Mustapha MW, Mohammed OO, Saeed MS, Surajudeen-bakinde NT, Salisu S. Electricity Theft Detection by Sources of Threat for Smart City Planning. *The institute of engineering and technology*, 2019; 1-9.
- [10] Olaoluwa OG. Electricity Theft and Power Quality in Nigeria. *International Journal of Engineering Research & Technology*, 2017; 6(6) 1180-1184.
- [11] Mahmood M, Shivam O, Kumar P, Krishnan G. Real Time Study of Technical Losses in Distribution Systems. *International journal of advanced research in electrical, electronics and instrumentation engineering*, 2014; 3(1)131-137.
- [12] Alumona TL, Nwosu OM, Ezechukwu AO, Chijioke J. Overview of Losses and Solutions in Power Transmission Lines. *Network and complex systems*, 2014; 4(8)24-31.
- [13] Balraj B, Chidambaram VS, Pari M, Gokul B, Prasath N. Detection for Power Theft Prior to Feeding Energy Meter and Intimating to Control Room. *International journal of pure and applied mathematics*, 2018; 118(20)2055-2064.
- [14] Navani JP, Sharma NK, Sapra S. Technical and Non-Technical Losses in Power System and Its Economic Consequence in Indian Economy. *International journal of electronics and computer science engineering*, 2013; 1(6)757- 761.
- [15] Glauner P, Meira JA, Valtchev P, State R, Bettinger F. The Challenge of Non-Technical Loss Detection Using Artificial Intelligence: A Survey. *International journal of computational intelligence systems*, 2017; 10:760-773.
- [16] Hasan H, Toma RN, Nahid A, Islam MMM, Kim J. Electricity Theft Detection in Smart Grid Systems: A Cnn-Lstm Based Approach energies.2019.
- [17] David FC, James AC, Onyinye AH. Controlling Electricity Theft, A Smart Meter Approach: Case Study Nigeria. <https://www.researchgate.net/publication/330637678>, 2017; 1-17.
- [18] F. C. David FC, A. C. James AC, Onyinye AH. Abating Electrical Power Theft in Nigeria Using Smart Meters and Data Analysis. <https://www.researchgate.net/publication/330159303>, 2019; 1-17.
- [19] Chauhan A, Rajvanchi S. Non-Technical Losses in Power Systems, A Review. *Proceedings of 2013 international conference on power, energy and control*, 2013; 558 -561.
- [20] Dineshsundar M, Rathika R. Development of Electricity Theft Detection Using Smart Meter in Power Distribution Network Based on Wireless Technology. *International journal of advanced research in electrical engineering*, 2018; 1(1) 25-33.
- [21] Komolafe OM, Udofia KM. A Technique for Electrical Energy Theft Detection and Location in Low Voltage Power Distribution Systems. *Engineering and applied sciences*, 2020; 5(2)41-49.