Embedded Power System Monitoring Of Illegal Power Connections In Kenyan Domestic Supply

Karobia Pauline N.
Department of Electrical and Electronics
Murang'a University of Technology
Murang'a, Kenya.
karophiuris2013@gmail.com

Ngoo Livingstone
Department of Electrical and Electronics
Murang'a University of Technology
Murang'a, Kenya.
Lngoo@MMUT.ac.ke

Muriuki James
Department of Electrical and Electronics
Kenya Power and Lighting Company
Nairobi, Kenya.
jmkinyua@KPLC.co.ke

Abstract— Globally Technical Losses (TLs) and Non-Technical Losses (NTLs) are a significant challenge for power distribution systems. Mostly NTLs is caused by illegal power connection which can be as much as half of all the energy supplied in some countries. This implies that power generated may not meet the demand and therefore the power utilities are diverting to other types of power generation that are cheaper, reliable and cost effective. High demand for electric power that does not match the current power generated always leads to shortage thus increasing the cost per unit of electric energy consumed. This highly affects the economy of any nation. Most utility company experiences loss of revenue since illegally consumed power cannot be measured or billed. The difference between the total energy sent to the consumers and the sum of energy consumed by all the connected consumers can be determined, and the total amount of NTLs in the distribution line evaluated. Also, the high losses incurred are a burden to the legally connected consumers since it is factored out in their bills. The scenario of NTLs is not restricted to underdeveloped countries and the percentage varies depending with the connected electric users. The techniques used are illegal tap wiring and meter tampering through security seal violations. The existing system in Kenya does not identify the location where illegal connection has occurred. The suggested embedded system will remotely locate the users who attempts to tap power at the service head which is not billed. The system will communicate with the utility company immediately about the status of the affected connection via Global System Communication. This will protect the distribution network in Kenya from high NTLs caused by illegal connections thus lowering the cost of electricity.

Key word- Distribution systems, Domestic consumers, Embedded system, Non-technical losses, Service head,

I. INTRODUCTION

An ordinary Kenyan domestic distribution line is as shown in figure 1. It has a drop line carrying 230 volts at a frequency of 50 hertz. A service fuse (cutout) is connected before the meter for breaking the circuit if a fault occurs. From the meter a circuit breaker is connected which link the rest of the final sub-circuit with the meter. The service drop, cutout and the energy meter are utility properties installed at the distribution board.

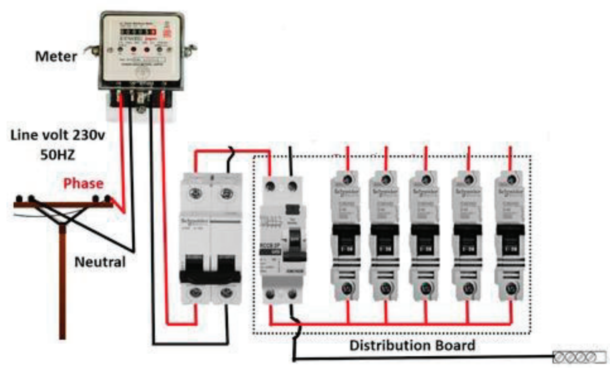

Fig.1. A typical distribution

A. OVERVIEW OF ELECTRICITY SECTOR IN KENYA

Electricity is an important entity in any household in Kenya and almost seventy-Five percent (75%) of domestic consumers are connected to electric energy. Kenya Generating company (KEN- GEN) and Kenya Electricity Transmission users are more variable and changes rapidly over the day and night in response to consumer's needs and appliance use. The cost of electrical power has continued to escalate with time thus raising concerns to electricity consumers. This has compelled consumers to find illegal ways of getting power without paying. This element has resulted to an increase in non-technical losses in the distribution network. Company Limited (KENTRACO) are responsible for generation and Transmission of power in Kenya respectively. Kenya Power and Lighting company (KPLc) distribute electricity to consumers in Kenya. Electricity consumers on the distribution system are categorized as industrial, commercial and residential. The usage of power by industrial consumer's is almost constant during the day and night over the season. Residential and commercial

B. ANALYSIS OF POWER LOSSES IN KENYAN POWER SYSTEM

Losses incurred in electrical power systems have two components

- Technical losses and
- Non-technical losses (Commercial losses)

In Kenya, losses are usually experienced from generation, through transmission and distribution up to the consumer

978-1-7281-6746-6/20/$31.00 ©2020 IEEE

intake point. In normal cases, majority of losses which can be avoided occurs at the distribution network. In the world, distribution companies operate with a well-defined degree of losses where Kenya is not exceptional. Combined technical and non-technical losses account for (28%) of energy losses in the distribution network according to Kenya Power and Lighting Company (KPLC) data base. This is over and above the allowable percentage by Energy Regulatory Commission (ERC) energy policy which only considers (15%) of losses in the distribution network. The remaining (13%) is absorbed by KPLc into their revenue. These losses are a form of revenue loss where for every one percent (1%) loss is equivalent to one billion shillings (9.4M USD). This information is from KPLC. Non-technical losses which takes the highest percentage are due to;

- Tampering with Energy meters resulting in the meter reading erroneous values.
- Component breakdown that drastically increase losses before they are replaced
- False data due to fraud caused by the utility staff.
- Meter bypassing or having illegal connection on the intake point.
- Electricity users not paying the billed units.

C. RELATED STUDIES

Several illegal electric energy monitoring and detection technologies have been considered in the review. In [1] a unit for determining illegal power usage through a Remote wireless detection method has been proposed. The unit detects illegally connected consumers using concurrent data before using previously analyzed recorded data. The system also secures the electricity user by eliminating completely high-resolution data of the customers by destroying the high-quality data prompt electricity usage recorded by the user energy meter. Internet communication is applied to identify the user(s) where information pertaining the illegal user is sent to the energy company with the identification details of the suspected energy meter and the value of the unbilled load. The use of expert systems in the investigation of causes of NTLs is a good move according to [2]. application of artificial intelligence in solving illegal power tapping and connection is proposed especially in the use of artificial neural networks in finding solutions of the studied problem. This approach allows analysis of consumer's electricity usage through a set of inspection results as well as a set of consumers generated inspections in different distribution networks. The technology involves sampling of customers who can be considered as a representative of all consumers connected in that specific radius. Since random sampling is applied then there is bias. This means that the inspection does not represent all the consumers connected. This bias is learned from inspection results which makes the predictions. The data which is captured includes the meter type and connection type for several consumers.

. For M customers 0; 1..........; M 1 for the past N months, 0; 1.........N 1 feature of matrix F is computed, where element F^m is considered to be the daily average kWh consumption feature during the month. Therefore:

$$F_d^m = \frac{L_d^m}{R_d^m - R_{d\_1}^m} \tag{1}$$

Where; L^m is the Kilo watt hour consumption increase on the energy meter to the date R^m while the latter date $R_d^m - R_{d-1}^m$ being the number of days of energy meter reading for customer M. The use of Artificial Neuro Network for analyzing the periodic data of electricity consumption is problematic due to the following reasons:

1) Some data collected regarding electricity consumption has errors and has noise.

2) Since the data being analyzed is big, it is difficult to determine the periodicity of the consumed electricity especially in 1-D time series.

3) Electricity consumption data is very complex and therefore generalization capability is limited.

The research also highlighted that the use of wide component learning which frequently utilizes the 1-D time series, every layer calculates the consumed electricity unit using the following equation;

$$y_j := \sum_{i=n}^{\infty} w_{ij} x_1 + b_1 \tag{2}$$

Where; y_j is taken as the output of the fully connected layer of j th neuron, n being the length of 1-D data input (x) and w_{ij} is the weight of the neuron having a bias b. The calculated data is then be sent to the next layer through activation function for determining the extent of effect of the next predicted consumer. The activation function is given by;

$$u_j := f(y_j) = max(0, y_j) \tag{3}$$

Where; u_j is the output after the determined activation. But the challenge with this approach is that it considers the positive values only which make it not sufficient for the determination of power tapping [3]. This paper addresses illegal electricity connection using universal anomaly detection to obtain real-time identification in a smart system. A number of consumers connected to one transformer were monitored to find anomalies based on electricity consumed data, change in the rate of data regarding electricity usage, dates and time when the consumption figures were recorded. In [4], electricity users provided with energy bills in the past few years were analyzed so as to find the reason of increased losses in the distribution lines. Fourteen years was subdivided into five successive spells and the starting was taken for one year. Fuzzy logic is used as a mean for finding out a number of suspected illegally connected energy users in the first phase of determination. In this phase, every energy user is put in the area with high increase in technical losses for analysis. For every customer, a time series of billed electricity units are set-up. Chosen time series data and the relationship is applied to put down the fuzzy sets of suspected users. Then, total guessed value of every customer is set by fuzzy logic. All users, whose percentage guessed value is more than the allowable value, are stated as illegal electricity users. [5], identifies the amount of electricity illegally consumed through finding the area where tapping has occurred and manage the illegal consumption in

978-1-7281-6746-6/20/$31.00 ©2020 IEEE

the identified area using neuro-fuzzy logic. Advanced Metering Infrastructure is being used with relative entropy to calculate the difference between probability distribution gotten from power usage disparity [6], [7]. Another technology which is put in to consideration is the GSM based technology for determination of illegal power usage [8], [9].

II. PROPOSED SYSTEM

In this paper, an identification conceptual framework is designed based on intelligent computing as shown in figure 2. The proposed embedded hybrid control contain five major parts and will be installed at the meter box where power tapping mostly occurs.

1) The sensing component

2) The display component

3) Data processing module

4) Interrupting module

5) Communication module

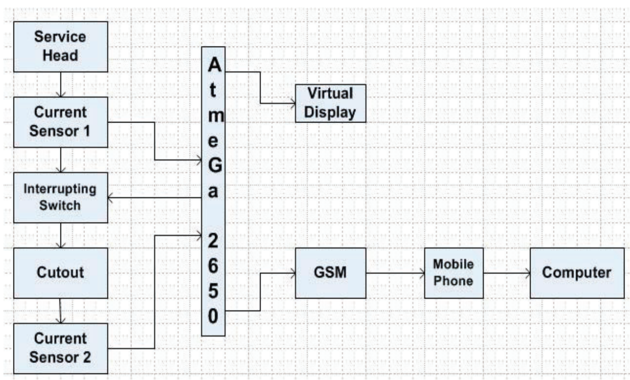

Fig. 2. Conceptual Framework

As shown in figure 2, illegal connection identification is based on the following assumptions:

• Current sensor one is supposed to sense the incoming current from the service line,

• Current sensor two is supposed to record the same value as current sensor one if it's a properly connected load,

• Current sensor two is supposed to sense a different value of current in an event of illegal connection that may happen at the output terminals of the cutout. This value will not be the same as that indicated by current sensor one,

• The microcontroller processes the two data coming from the two sensors in an event of illegal connection, triggers the interrupting switch which cut-off the load from the main supply,

• Immediately when the power flow is interrupted the microcontroller process another signal containing the details of the affected energy meter in form of an short message via a GSM to a receiving device at the utility company.

• The same information is sent to a computer via Bluetooth for the utility staff to view the status of the interrupted meter. This process is secure and saves the utility company from loss of revenue, power interruptions due instability caused by unaccounted demand and protects genuine consumers from inflated bills.

III. EXPERIMENTATION

Development of the embedded system model, analysis of the monitored information and detected data are carried out using MATLAB SIMULINK program and Proteus VSM. A proteus software is used because it has features that allow modeling, simulating and analyzing a system. Proteus software also contain libraries for interaction with a micro-controller and any analogue or digital system connected to it. Proteus simulation is used to design a prototype for a randomly selected electric power user. The prototype is as shown in figure 3. The system mainly deals with current values. It comprises of a service line delivering a voltage of 240 volts, two sensing modules, one before and the other one after the cutout. The sensor before the cutout monitors and determines the incoming current from the supply while the sensor after monitors and determines the current drawn by the load, a microcontroller for data processing, three connected loads (bulbs), a control switch, an interrupting switch and an LCD for display. A

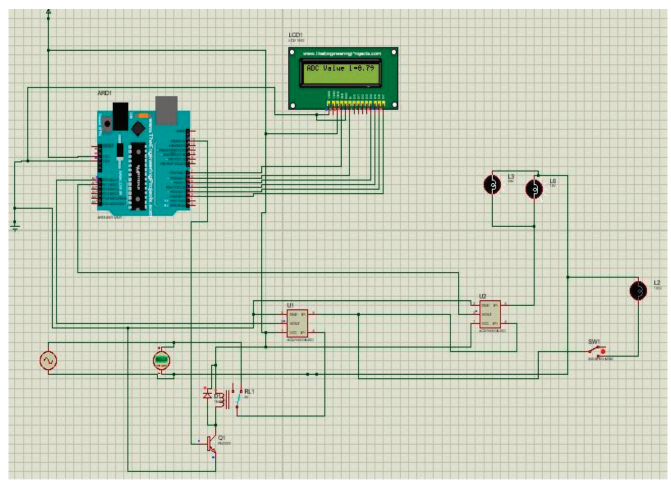

Fig. 3. Simulated Model

serial monitor will be connected to generate the information to be sent to the utility company.

IV. RESULTS AND DISCUSSION

In an ideal case, the microcontroller identifies the two values of the current sensor. If the two values are the same, for instance (Current 1= Current 2= 47.4A) as shown in figure 4 and 5 then there is no illegal connected load that is detected. This indicates s that the current from the supply equals the current drawn by the load after the cutout. It shows that the power consumed by the consumer is correct and will therefore correspond with the value recorded by the energy meter for billing. In case there is a considerable difference in the two sensed current values, for example (Current 1= 126A, Current 2=13.4A), as indicated in figure 6 and 7, then it means that there is an uncounted load which is illegally connected. The microcontroller activates the GSM module thereby sending a text to the nearby utility company with the information ("KPLC MANAGER, METER NO. 37163131529 disconnected. User ID:22143443"). Consequently the microcontroller will activate the relay module ON as shown in figure 6 hence disconnecting the entire installation from the main supply.

978-1-7281-6746-6/20/$31.00 ©2020 IEEE

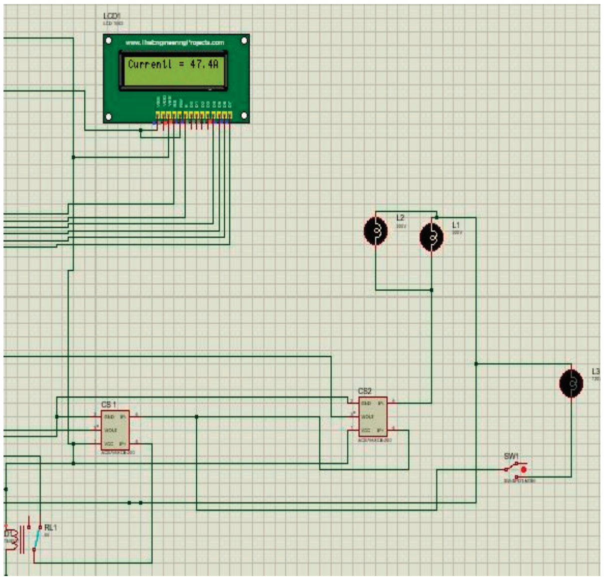

Fig. 4. Normal operation (Sensor 1)

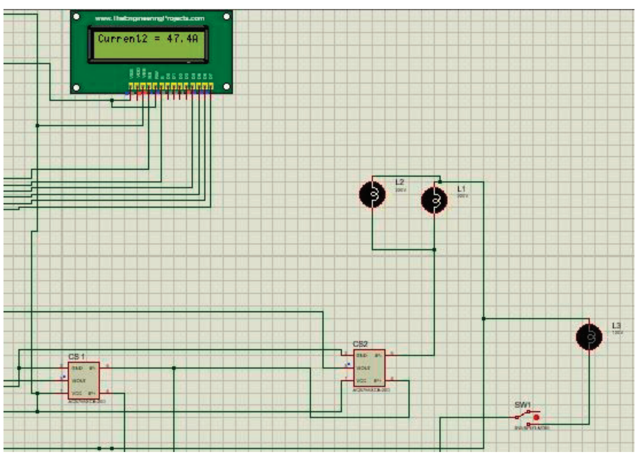

Fig. 5. Normal operation (Sensor 2)

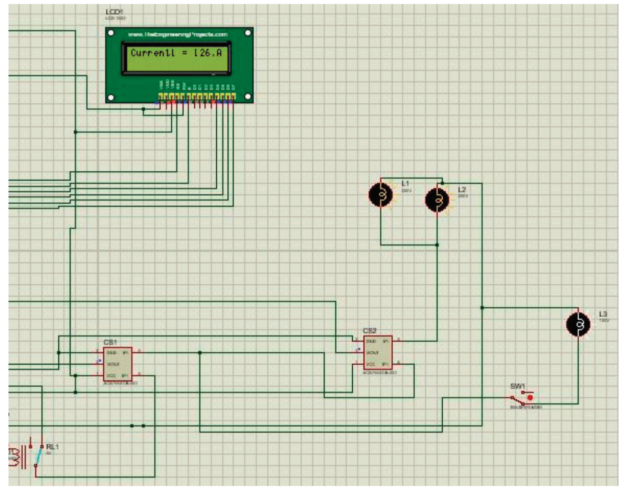

Fig. 6. Abnormal operation (sensor 1)

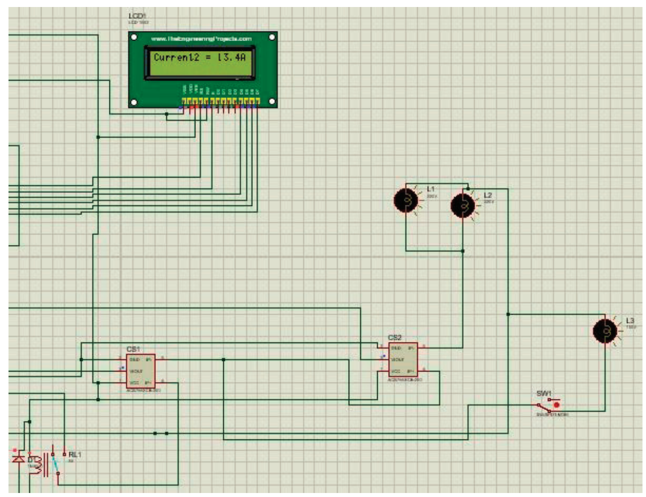

Fig. 7. Abnormal operation (sensor 2)

V. CONCLUSION

The design and simulation of an experimental embedded power system to monitor and detect illegal power connection in Kenya has been achieved in this work. It has considered illegal power tapping at the surface head which leads to NTLs leading to a reduction of power revenue to the utility companies and power instability in the distribution lines which is due to uncontrolled loads. Genuine connected power users are as well safeguarded from inflated electricity bills brought by NTLs. The system is automated and with remote monitoring of illegal connection and sending SMS whenever there are abnormal readings at the customer intake point, the developed system is able to help utility company to reduce the incidences of household electricity theft. An automatic interrupting switch is integrated into the unit so as to remotely cut OFF the power supply to any consumer who tries to indulge in illegal connection. This design, therefore, removes the manual inspection with its attached consequences of time-consuming.

978-1-7281-6746-6/20/$31.00 ©2020 IEEE

REFERENCES

[1] A Bin-Halabi, A Nouh, M Abouelela, ”Remote detection and identification of illegal consumers in power grids,” 2019 vol 7,pp 71529–71540.

[2] P Glauner, JA Meira, P Valtchev, R State, ”The challenge of nontechnical loss detection using artificial intelligence”: A survey, 3rd ed., 2016

[3] R Razavi, A Gharipour, M Fleury, Martin and IJ Akpan, ”A practical feature-engineering framework for electricity theft detection in smart grids,” 2019, vol.238, pp.481-494.

[4] JV Spiric, SS Stankovi ́ c, MB Do ́ ciˇ c,”Identification of suspicious ́ electricity customers,” 2018, vol. 95,pp.635-643.

[5] S Palaniyappan, ”Fuzzy Logic Based Electricity Theft Identification in Distribution Systems,”2019, vol.4, No.4,pp.13-18.

[6] SK Singh, R Bose, R Ranjan and A Joshi,”Entropy-based electricity theft detection in AMI network,” Theory & Applications, 2018, vol. 3, No.2, pp. 99-105.

[7] M Nabil, M Ismail, M Muhammad, M Shahin ,”Deep LearningBased Detection of Electricity Theft Cyber-Attacks in Smart Grid AMI Networks,” 2019, pp 73–102.

[8] NK Mucheli, U Nanda, ”Smart Power Theft Detection System,” 2019, pp.302–305.

[9] M Saad, MF Tariq, A Nawaz, ”Theft detection based GSM prepaid electricity system,” 2017 3rd IEEE International Conference on Control Science an Systems Engineering (ICCSSE),pp.435–438.

978-1-7281-6746-6/20/$31.00 ©2020 IEEE