IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 12, Issue 2 Ver. II (Mar. – Apr. 2017), PP 42-45
www.iosrjournals.org

Load Monitoring and Detection of Tampering in Power Lines Using Internet of Things (Iot)

N. Pranau[1], T. Raghuraman[2], S. V. Vishnuguhan[3], Dr. B. Meenakshi[4]
[1,2,3]*Student Department of Electrical and Electronics Engineering, Sri Sairam Engineering College, Anna University, Chennai, India*
[4]*Professor Department of Electrical and Electronics Engineering, Sri Sairam Engineering College, Anna University, Chennai, India*

Abstract: *The term load monitoring depicts the monitoring and auditing the load consumption patterns in low voltage customer side. Since energy becoming the more concerned topic of the era the work for proper auditing is a required improvement to be made in today's power system. The existing digital meters are up to accurate level of measuring data. Smart meters when compared to electro mechanical meters have to reduce man power and it should ensure capability of communicating with utility sector. Hence by using INTERNET OF THINGS, the technology of modern era and which is going to be well strengthened by forth coming 5G, there will be a successful load monitoring process. In this project the process of monitoring concentrates over the harmonics, excess loading of transformer especially in distribution side, power factor monitoring, voltage disturbances etc., Indeed the major part of the project is detection of tampering by establishing a summation algorithm between the power distributed from the transformer in distribution ends and the consumers. The power consumption and distributed data are retrieved from respective meters through and then fed to the monitoring page of electricity board. Tampering being one of the major hindrance to the electricity generation and distribution, this method of monitoring could detect any theft and immediate site inspection can resolve the issue. On the whole, monitoring the power consumption via internet of things ensures effective monitoring and detection of tampering in low voltage side of the power grid.*

Keywords: *esp8266 Wi-Fi module, MOD Bus protocol, RS485, Tampering, TTL*

I. Introduction

This project deals with tampering detection in power lines, and we are going to achieve this with the help of Internet of things (IOT). The work was inspired by the idea of the approach on Internet of things so as to develop a solution to minimize the uninformed excessive power usage by the consumers or power theft detection. In our state, electricity board supplies very few number of energy meters in High Tension (HT) side (bulk consumers) and passably they provide more number of energy meters in Low Tension (LT) side (domestic consumers). Thus antithesis to it in High Tension side more revenue is obtained rather than Low Tension side since our current tariff system is based on the usage of energy by a single consumer. As there are very few meters in High Tension side we can easily detect any power theft occurrence. The problem comes at the Low Tension side. The consumers in Low Tension side are quite high in number. With this huge population its very difficult to find out theft in power by inspecting every individual consumer. Thus we go for improvising our energy meters. Our old analog energy meters can't detect the small amount of power rating usage like mobile chargers, etc. So detecting theft with this was quite difficult. Then we updated ourselves with modern electronic energy meters. These electronic meters are easily understood with seven segment readout unlike the analog type, you need to take a closer look into the meter scales.With this seven segment, readout accuracy and precision are increased. In electronic energy meter we can even read negative values as output in displace. These electronic energy meters also provide us a provision to fetch out digital data. Our project says the way how we are fetching out data from energy meter and how frequently we are fetching it. The concept of load- monitoring is achieved by fetching data like line voltage, line current, power with power factor and energy from every single energy meter from consumer side and detection of tampering in power line is accomplished by installing an energy meter in distribution transformers for fetching the same data as mentioned above, so as to compare both the data of distribution transformer as a whole and the algorithmic summation of consumers data. We are going to fetch out the data using internet of things technique. Here we are going to place a Wi-Fi module with every energy meter and it is going to collect data and send it to the server once it has been connected to the LAN module. The same process is repeated near distribution transformers energy meter and all the data are updated in server.

II. Related Works

In our paper, communication strategy of dynamic data transmission from a module to the server storage is discussed with different types of ways using Internet of things. This data in cloud storage is analysed using user interfaces and thus excessive power consumption can be monitored.[2] The paper then presents the vision

of the next-generation monitoring, control functions, and analysis. The current monitoring, control technology, and analysis for transmission networks may not be able to meet these increasingly diverse future challenges and theft.[4] [6] Wi-Fi is easily available almost everywhere. Due to this, there is increasing interest in harnessing this communication technology.[3] Our system detects anomalous meter readings on the basis of models built using machine learning techniques on past data , it can incrementally incorporate the result of field checks to grow the database of fraud and non-fraud patterns.[1] Hence, security related power system operation strategies have to be adapted to face the new kinds of theft situations.[5]

III. Proposed Work

In this project to give a solution for tampering in power line is discussed, with continuous monitoring of load. The data is obtained from the distribution side transformer as well as consumer side and the load curve and load consumption is continuously updated in server system. From the server the load is monitored, if any deviation in current more than the tolerance rate is sensed then it alerts as tampering is detected. The flow can be explained with the block diagram in the figure1. The requisite data is fetched from the energy meters and updated in server and thus from server continuous monitoring of load flow is done.

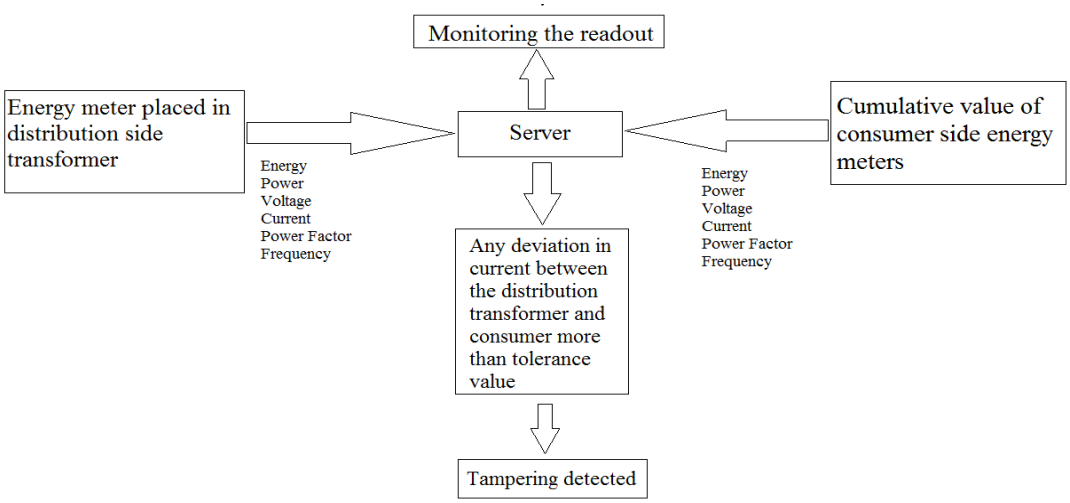

Fig-1: System Architecture

IV. Implementation

We have used a Wi-Fi module called esp8266 mod12 for transferring data from energy meters to the server in the presence of internet connectivity. But the energy meter communicates in MOD Bus protocol with RS485(Recommended Standard 485) whereas Wi-Fi module communicates with TTL (Transistor-transistor Logic). Thus we need a converter to convert RS485 to TTL. RS485 is a serial communication method which can have maximum of 32 drivers with the mode of operation as half duplex and its network topology is multipoint. Modbus is a serial communication protocol. The device requesting the information and the devices supplying information are called as the Modbus Master and Modbus Slaves respectively. In a standard Modbus network, there is one Master and up to 247 Slaves and each Slave has a unique Address. The Master can also write information to the Slaves. The information stored in the Slave device is of four types two stores on/off discrete values (coils) and other two stores numerical values (registers). Read-only as well as read-write is available in both coils and registers. RS485 to TTL converter provides two way serial communications signal conversion between the RS485 to and from a TTL. It has Auto Direction control, making it easier to use as Serial Interface replacement. Transistor-transistor logic (TTL) is a digital logic design in which bipolar transistors act on direct-current pulses. A TTL device employs transistors with more than one emitter in gates having more than single input. Wi-Fi module esp8266 mod 12 uses this TTL logic to communicate. Fig .2 explains the working circuit of this paper with all wired and wireless connection provided.

Table I: Defining data address of coils and registers

Coil/Register Numbers	Data Addresses	Type	Input/Output type
1-9999	0000 to 270E	Read-Write	Discrete Output Coils
10001-19999	0000 to 270E	Read-Only	Discrete Input Contacts
30001-39999	0000 to 270E	Read-Only	Analog Input Registers
40001-49999	0000 to 270E	Read-Write	Analog Output Holding Registers

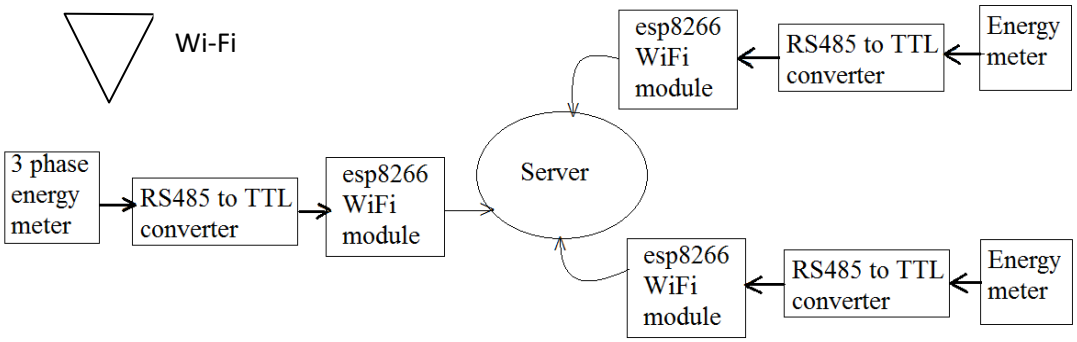

Fig-2: Block diagram of circuit; Block line-wired connection; Normal line- wireless

V. Results And Conclusion

When we introduce this idea in our modern system then we can easily monitor the load consumed by every meter individually and improve the tariff system accordingly and we can even detect the tampering done in the power line and give the necessary penalty charges for the extra consumption of load. We are alerting the theft in the server page with a necessary alarm near the server so that the theft can be stopped as soon as possible or it can be charged. The theft calculation analysis for a meeting conducted in road illegally, say with ten 40 watts tube light and two 3000 watts speakers give rise to pretty high tampering as shown in fig-3

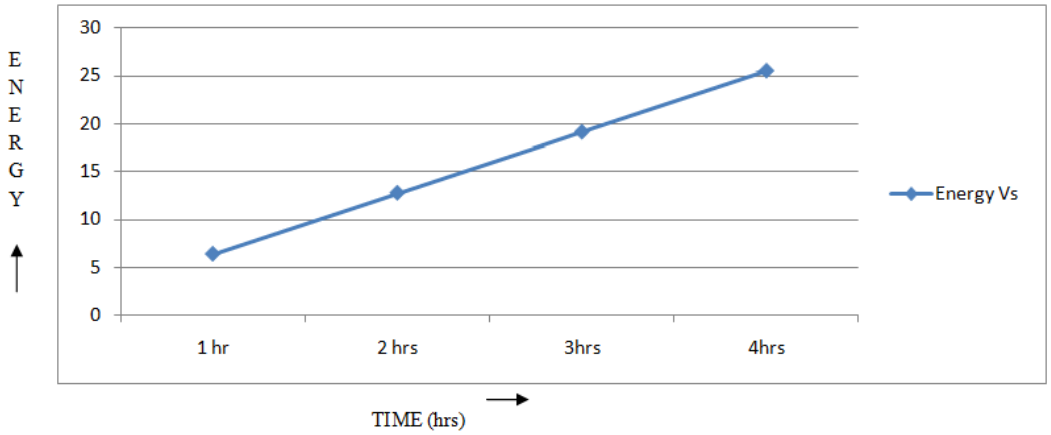

Fig-3: Energy vs Time graph when tampering occurs

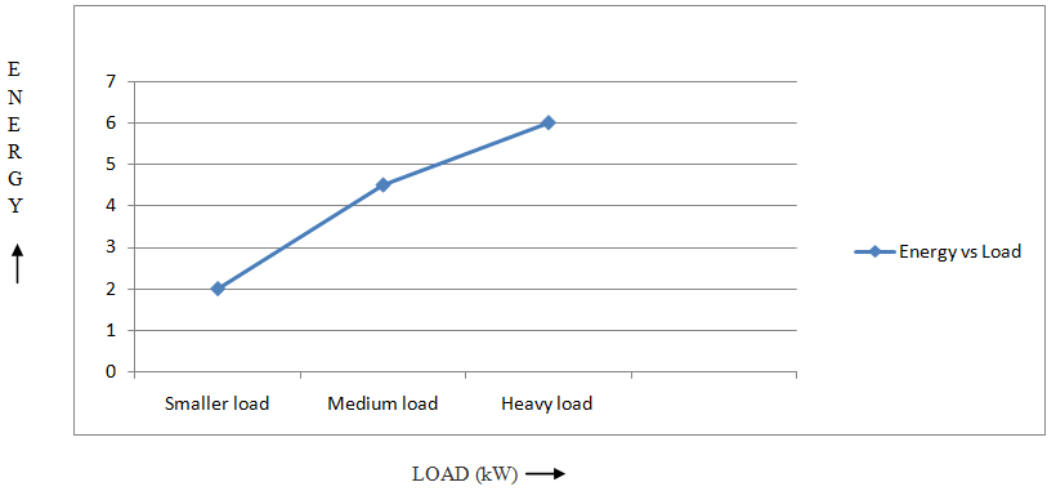

Fig-4: Energy vs Load graph for different tampering levels

The comparison chart between the different kinds of load tampered is also represented in graphical format in fig-4.

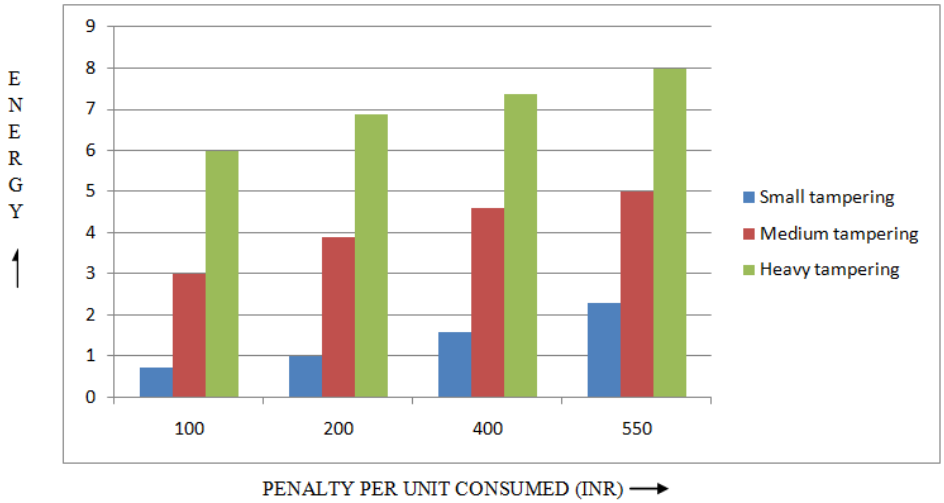

Fig-5: Energy vs Penalty charged for different tampering levels at different locality

These can be less than 2kw (Smaller load tampered), less than 6kw (Medium load tampered) or more than 8kw (Heavy load tampering). Finally when cost estimation is done the bar chart is designed between the different loads tampered for a period of time and thus how much penalty can be charged on that theft is calculated. According to the locality where the theft occurs penalty varies.

Reference

[1]. A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in ami systems", *Communication Control and Computing (Allerton) 2012 50th Annual AllertonConference on*, pp. 1830-1837, Oct 2012.

[2]. J. Sandeep Sonil, Smita Pareek, "Role of Communication Schemes for Power System operation and Control", *International Journal Of Electronics And Communication Engineering & Technology*, pp. 163-172, November 2013.

[3]. ANDREJ ŠKRABA, ANDREJ KOLOŽVARI, "STREAMING PULSE DATA TO THE CLOUD WITH BLUETOOTH LE OR NODEMCU ESP8266" , 2016 5TH MEDITERRANEAN CONFERENCE ON EMBEDDED COMPUTING (MECO)

[4]. Z. Pei, L. Fangxing, and N. Bhatt, "Next-Generation Monitoring, Analysis, and Control for the Future Smart Control Center," Smart Grid, IEEE Transactions on, vol. 1, pp. 186–192, 2010.

[5]. *Modern grid initiative*, U.S. Dept. Energy, Natl. Energy Technol. Lab.

[6]. R. Krebs, B. M. Buchholz, Z. A. Styczynski, K. Rudion, C. Heyde, Y. Sassnick, "Vision 2020—security of the network operation today and in the future. German experiences", Proc. IEEE Power Eng. Soc. Gen. Meet. 2008, pp.1-6