International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Power Theft and Fault Detection using IoT Technology

Rohit Tatte[1], Mayuri Chaudhari[2], Minal Khrabe[3], Pranjali Lokhnade[4], Pranjali Muneshwar[5], Dhanshree Yenorkar[6]

[1,2,3,4,5,6]*Student, Dept. of Electrical Engg., Datta Meghe Institute of Engineering Technology & Research, Wardha*

Abstract - *Generation, transmission and distribution of electrical energy involve many operational losses. We can defined the losses in generation technically but distribution and transmission losses cannot be precisely quantified with the sending end information. This illustrates the involvement of nontechnical parameter in transmission and distribution of electricity. Moreover technical losses occur naturally and are caused because of power dissipation in transmission lines, transformers, and other power system components. Technical losses in Transmission & Distribution are computed with the information about total load and the total energy bill. While technology in the raising slopes, we should also note the increasing immoral activities. The system prevents the illegal usage of electricity. At this point of technological development the problem of illegal usage of electricity can be solved without any human control using IoT. With the implementation of this system will save large amount of electricity, and there by electricity will be available for more number of consumer then earlier, in highly populated country such as India, China. Power theft can be defined as the usage of the electrical power without any legal contract with the supplier.*

Key Words: Power Theft, Fault Detection, IoT,

1. INTRODUCTION

Theft of electricity is the criminal practice of stealing electrical power. It is a crime and is punishable by fines and/or incarceration. It belongs to the non-technical losses. In recent days power theft which causes lot of loss to electricity boards is the biggest problem. In countries like India, these situations are more often, if we can prevent these thefts we can save lot of power. To detect an unauthorized tapping on distribution lines electrical power theft detection system is used. Distribution network of electrical power supply system is the main implementation part of this system. It is not possible for existing system to identify the exact location of tapping. Our system finds out on which electrical line there is a tapping. This is a real time system. In moderately developing nation in development of nation power sector provides one of the most important input. The consumption of electricity in India is increasing at much faster rate. Therefore a need has aroused to generate, transmit & distribute electric power at most economical way. [3] Electrical power system is been divided into generation, transmission & distribution. Losses in transmission system are much lower than losses in distribution side and also fault are not frequent in distribution side.

Most of the losses are caused by fault and theft in distribution system. In this paper the focus is on single phase to ground fault in power line. When single phase to ground fault occurs, it becomes significant to detect fault quickly and with accuracy. It becomes challenging for the power company to detect and repair the fault as quickly as possible. Protection systems are designed to identify the location of faults and isolate only the faulted section in order not to damage the whole equipment in power system. In the proposed concept with the use of wireless sensor network exact location of fault can be diagnosed. There by providing optimum operation of electric power. The objective of this paper is to provide with a simple way to detect the fault and show the exact location of occurred fault which will ultimately lead to optimum operation of the whole system and to improve the reliability of distribution network.

Electrical networks, machines and equipment's are often subjected to various types of faults while they are in operation. When a fault occurs, the characteristic values (such as impedance) of the machines may change from existing values to different values till the fault is cleared. There may be lot of probabilities of faults to appear in the power system network, including lighting, wind, tree falling on lines, apparatus failure, etc.

The fault inception also involves in insulation failures and conducting path failures which results short circuit and open circuit of conductors. Under normal or safe operating conditions, the electric equipment's in a power system network operate at normal voltage and current ratings. Once the fault takes place in a circuit or device, voltage and current values deviates from their nominal ranges. Usually power system networks are protected with switchgear protection equipment's such as circuit breakers and relays in order to limit the loss of service due to the electrical failures after the occurrence of fault. The design of systems to detect and interrupt power system faults is the main objective of power-system protection. The main types of faults are symmetric and asymmetric.

2. RELATED WORK

2.1 Internet of Things (IoT)

The Internet of Things (IoT) envisions a near future and is a recent communication paradigm, in which the objects of everyday life are equipped with microcontrollers, transceivers for communication, and suitable protocol stacks

that will make them able to communicate with one another and with the users, becoming an integral part of the Internet. This system aims at making the Internet even more immersive and pervasive. Also by enabling easy access and interaction the internet of things will foster the development of a number of applications that make use of the potentially enormous amount and variety of data generated by such objects to provide new services to citizens, companies, and public administrations by using variety of devices such as, for instance, home appliances, surveillance cameras, monitoring sensors, actuators, displays, vehicles, and so on,

Our System indeed finds application in many many domains, such as automation in homes, industrial, medical aids, mobile healthcare, elderly assistance, intelligent energy management and smart grids, automotive, traffic management, etc. However, such a heterogeneous field of application makes the identification of solutions capable of satisfying the requirements of all possible application scenarios a formidable challenge. This difficulty has led to the proliferation of different and, sometimes, incompatible proposals for the practical realization of IoT systems. Therefore, from a system perspective, the realization of an IoT network, together with the required backend network services and devices, still lacks an established best practice because of its novelty and complexity. In addition to the technical difficulties, the adoption of the IoT paradigm is also hindered by the lack of a clear and widely accepted business model that can attract investments to promote the deployment of these technologies.

Below, it is provided a glossary defining the Internet of Things:

- **Internet of Things:** A network of internet-connected objects able to collect and exchange data using embedded sensors.
- **Internet of Things device:** Any stand-alone internet-connected device that can be monitored and/or controlled from a remote location.
- **Internet of Things ecosystem:** All the components that enable businesses, governments, and consumers to connect to their IoT devices, including remotes, dashboards, networks, gateways, analytics, data storage, and security.
- **Entity:** Includes businesses, governments, and consumers.
- **Physical layer:** The hardware that makes an IoT device, including sensors and networking gear.
- **Network layer:** Responsible for transmitting the data collected by the physical layer to different devices.
- **Application layer:** This includes the protocols and interfaces that devices use to identify and communicate with each other.
- **Remotes:** Enable entities that utilize IoT devices to connect with and control them using a dashboard, such as a mobile application. They include smartphones, tablets, PCs, smart watches, connected TVs, and nontraditional remotes.
- **Dashboard:** Displays information about the IoT ecosystem to users and enables them to control their IoT ecosystem. It is generally housed on a remote.
- **Analytics:** Software systems that analyze the data generated by IoT devices. The analysis can be used for a variety of scenarios, such as predictive maintenance.
- **Data storage:** Where data from IoT devices is stored.
- **Networks:** The internet communication layer that enables the entity to communicate with their device, and sometimes enables devices to communicate with each other.

3. WORKING PRINCIPLE

There are various types of electrical power theft, including Tapping a line or bypassing the energy meter. According to a study[citation needed], 80% of worldwide theft occurs in private dwellings and 20% on commercial and industrial premises. The various types of electrical power theft include:

1) Direct hooking from line

What's known as "Cable Hooking" is the most used method. 80% of global power theft is by direct tapping from the line. The consumer taps into a power line from a point ahead of the energy meter. This energy consumption is unmeasured and procured with or without switches.

2) Bypassing the energy meter

In this method, the input terminal and output terminal of the energy meter is short-circuited, preventing the energy from registration in the energy meter.[3]

3) Injecting foreign element into the energy meter

Meters are manipulated via a remote by installing a circuit inside the meter so that the meter can be slowed down at any time. This kind of modification can evade external inspection attempts because the meter is always correct unless the remote is turned on.

4) Physical obstruction

This type of tampering is done to electromechanical meters with a rotating element. Foreign material is placed inside the meter to obstruct the free movement of the disc. A slower rotating disk signals less energy consumption.

5) ESD attack on electronic meter

This type of tampering is done on electronic meter to make it either latent damage or permanent damage. Detection can be done correctly in high end meters only.

The three phase parameter i.e. voltage of overhead line will get continuously sensed using phase voltage sense section. Once the fault takes place in overhead line, voltage and current values deviates from their nominal ranges. The faults like all series & shunt faults get detected & classified here. During occurrence of any series voltage get sensed and respective signals are given to microcontroller. . Relay is connected for detecting fault in fault display section. Relay is operated by micro-controller and switched after the occurrence of faulty condition. Microcontroller programing is done on the basis of characteristics conditions of overhead line voltages on occurrence of fault. The type of fault gets analyzed by microcontroller. If the fault gets occurred wireless technology GSM (global system for mobile communication) is used to send SMS to a responsible person on mobile. Type of fault will display on fault display section. Simultaneously fault will clear. The fault clearing system uses various protection devices such as relays and circuit breakers to detect and clear the fault. The three phase voltage sensed is continuously given to microcontroller. The implemented system completely meets the demand of low cost by using the microcontroller and mobile communication technology with the aim to detect the abnormality and fault occurred in the overhead electric line.

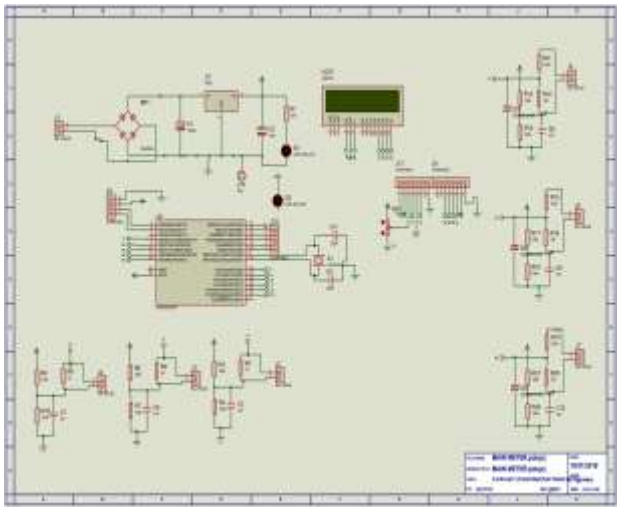

Figure 1.1 Circuit Diagram

The circuit consists of Arduino, GSM, LCD, ESP module and Current transformers. Meters cannot be used for high currents so current sensing is done by current transformers. Two CTs are used, one is connected at load side to measure the current through load and other C.T is connected at supply terminals to measure the current supplied by source.

The main component in this circuit is Arduino controller. It receives current signal from two current transformers by the means of bridge rectifier. Then it compares those two current magnitudes by the conditional operator. Since there is no theft load, the two C.T.s shows almost the same values. Here the system is in healthy condition. The Arduino cannot access current signal. So we have to interface the C.T. by means of voltage only. Here we have to convert the current signal into voltage signal. It can be converted by placing a resistor in series and taking voltage across the resistor and passing that voltage signal to arduino. Resistor is used because the secondary of current transformer should never be open circuited. The corresponding current can be obtained by doing calibration. Calibration can be done by connecting various loads and measuring different voltages and currents respectively.

Power tapping can be detected by comparing the power distributed to the line and the power actually consumed by the load. This is done by installing an electronic energy meter at the load side and the meter readings are send wirelessly to the distribution unit. This reading is received by the wireless receiver and is compared with the actual power given to the load. The difference in readings indicate the error and this error signal is given to a controller which in turn controls the secondary voltage of the transformer, thus causing the transformer to stop the supply of power. Thus power theft by tapping is detected and it is prevented by halting the power to the line totally.

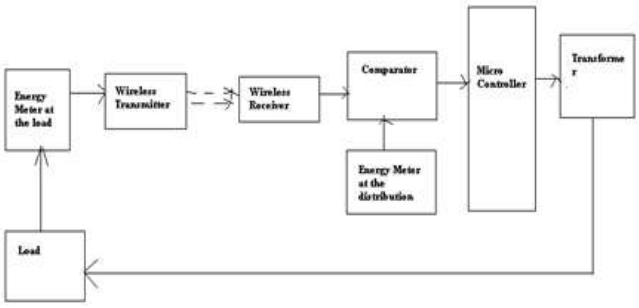

Figure 1.2 Power Tapping Detection

4. CONCLUSION

The implemented system design mainly concentrates on overhead electric power lines. It provides the way to detect all series and shunt fault on transmission and distribution lines. Voltage of the line will get continuously sensed using phase voltage sense section. Using IoT, power theft detector kit has been implemented and the same also done using GSM

for the purpose of backup protection. Using IoT, power theft detector kit has been implemented and the same also done using GSM for the purpose of backup protection.

REFERENCES

[1] Ashwini Yenegur, Basawaraj.S.Mathpati "An algorithm for fault node recovery of wireless sensor network" Volume: 03 Special Issue: 03 | May-2014 | NCRIET-2014.

[2] He Yi Li Chang-binWu Ai-guo Meng Qing-yu "Research of Phase-to-ground Fault Location in The Distribution Line Based on Wireless Sensor Networks".

[3] S. Tamronglak, S. E Horowitz, A. G. Phadke, J. S. Thorp "Anatomy of power system blackouts: preventive relaying strategies" IEEE Transactions on Power Delivery, Vol. 11, No. 2, April 1996.

[4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[5] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, "Convergence of MANET and WSN in IoT urban scenarios," IEEE Sens. J., vol. 13, no. 10, pp. 3558–3567, Oct. 2013.

[6] A. Laya, V. I. Bratu, and J. Markendahl, "Who is investing in machine-to machine communications?" in Proc. 24th Eur. Reg. ITS Conf., Florence, Italy, Oct. 2013, pp. 20–23.

[7] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, "Smart cities and the future internet: Towards cooperation frameworks for open innovation," The Future Internet, Lect. Notes Comput. Sci., vol. 6656, pp. 431–446, 2011.

[8] D. Cuff, M. Hansen, and J. Kang, "Urban sensing: Out of the woods," Commun. ACM, vol. 51, no. 3, pp. 24–33, Mar. 2008.

[9] Ms.Devjani Banerjee, Prof Dr.Mrs.N.R.Kulkarni , "T hree Phase Parameter Data Logging and Fault Detection Using GSM T echnology", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013 1 ISSN 2250-3153.

[10] P.A. Gulbhile, J.R. Rana, B.T . Deshmukh, " Review for overhead line fault detection using GSM technology", International Journal of Advanced Research in Electrical, Electronics and Intrumentation Engineering,Volume5, Issue12, December 2016 ISSN 2278-8875.

[11] C. Zhang and L. Zhou, "220kv Transmission Line Fault Diagnosis and Analysis," 2012 Second International Conference on Intelligent System Design and Engineering Application, Sanya, Hainan, 2012, pp. 1343-1345.

[12] S. Singh and D. N. Vishwakarma, "Intelligent techniques for fault diagnosis in transmission lines — An overview," 2015 International Conference on Recent Developments in Control, Automation and Power Engineering (RDCAPE), Noida, 2015, pp. 280-285.

[13] Joe-Air Jiang, Jun-Zhe Yang, Ying-Hong Lin, Chih-Wen Liu, Member, IEEE, and Jih-Chen Ma, "An Adaptive PMU Based Fault