Power Theft Identification Using Embedded System

Mr. Kankan Sarkar
Department of Mechanical Engineering Raipur Chhattisgarh India
kankansarkar@gmail.com

Article History

Article Submission
27 May 2013
Revised Submission
27 July 2013
Article Accepted
25 August 2013
Article Published
30 September 2013

Abstract

Today, power theft plays the key role in transmission losses of electricity from the generating station to the consumer end. About 30% of power produced is being theft. Though the electricity boards know that there is power theft in the area under their vigilance, they are not able to locate the area or location of theft. So, to identify the power theft and to communicate to the EB there needs a system to be developed. Here comes the system developed by us which will find the power theft if it happens and sends the information about the place of the theft to the nearby Electricity Board.
Keywords: *Power theft, Power Line Communication, Microcontroller, Multiplexer, GSM module, Digital Ammeter, Energy meter*

I. Introduction

In India, the power theft is becoming a very serious issue in the power sector of the World. About 20-30% of the power produced is being theft. This causes a major loss to the Electricity boards. So it becomes inevitable task these days, during which power shortages occur frequently, to find a solution to identify the power thefts and to eradicate them. There are various methods by which power is being theft in the distribution lines. The most commonly used methods are: Energy meter tampering, illegal tapping from the distribution lines and bypassing the feeders.

In meter tampering, the energy meter in the consumer side is made to malfunction by introducing materials which make the energy meter not to read its original readings. This is usually done by introducing magnets near the energy meter which work on electromagnetic principles, such that the magnetic forces are made to malfunction and hence the meter readings. Illegal tapping from distribution lines is the very popular method of power theft which usually happens in the villages and in the industrial areas where the hooks, which are made of conductive materials, introduced directly into the distribution lines and hence the power is utilized without the licence. Though this method of theft is particularly dangerous, the power thieves do not care much about this and this method continues to be the favourite method for many. Power theft also occurs through bypassing of feeders.

II. Power Theft Detection System

According to the principle of electric power transmission, the sending end current should be equal to the sum of the receiving end current provided that there is no leakage in the line. So when there is any discrepancy in this equation, then it can be concluded that the power should have been theft at some area between the input and the output. This is a microcontroller which can be used for a variety of operations such as doing computations, signal generations, controlling appliances. The multiplexer is a device which gives the output according to the select input given to it. If there are 2N inputs to the multiplexer then it gives only one input to be given as output depending on the 'N' select inputs. This multiplexer is of two types: parallel multiplexer, serial multiplexer. In the parallel multiplexer, N set of n-inputs can be given and only one n-set input can be obtained in the output. In case of serial multiplexer, if N inputs are given then only one output can be obtained.

ISSN: 2250-0839

The proposed architecture of the power theft detection system is shown in figure 1.

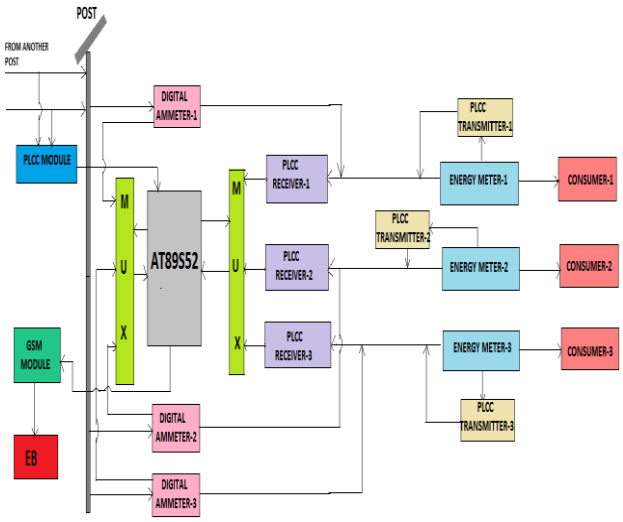

Fig.1: proposed architecture of the power theft detection system

As said in above sections by using the principle said before, the sending current from the post should be equal to the load current in the consumer section. If this is not equal then it can be detected that there is power theft in that particular line. So the power theft can be found in this way. Here it is assumed that digital meters in-built with current sensors are present in the consumer sides. If analog meters are present then the ADC module is to be introduced. The system to avoid meter tampering using embedded system is shown in figure 2.

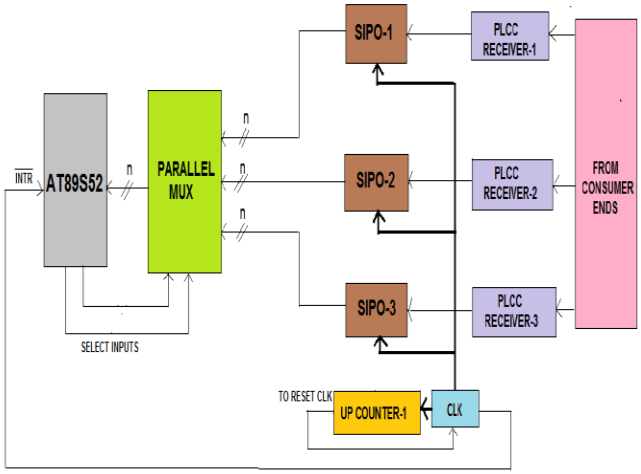

Fig.2: proposed system to avoid meter tampering using embedded system

Here only the current is set to be measured. The sensor takes 20 ms to measure the one cycle of current. This current will be of 8-bit data. This digital data is sent through the PLCC transmitter and is received in the PLCC receiver module. This data is again sent to the serial-in parallel-out shift register, whose clock signal is for about 20 ms before it gets resetted. The time period of one clock signal is about 2.5 ms. This data from the shift register is again sent to the parallel multiplexer which gives output depending on the select inputs. The input to be selected is said by the microcontroller to the multiplexer. The select input to the multiplexer is given only after the external interrupt INTR of the microcontroller gets changed. This select input will be the address of the particular line and is shown in figure 3.

ISSN: 2250-0839

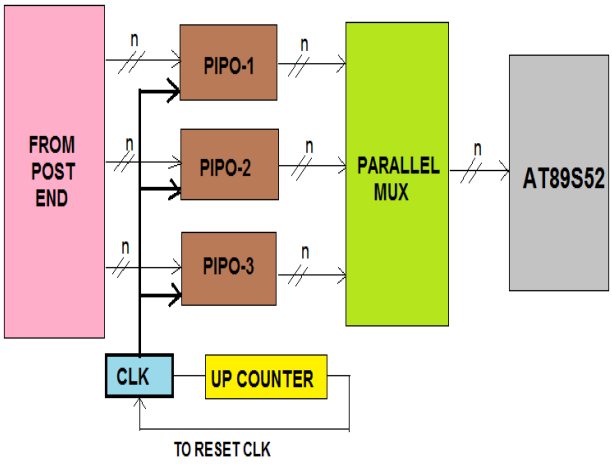

Fig. 3: proposed system to avoid illegal tapping using embedded system

According to the select input given to the multiplexer, it gives the output. The outputs are sent to the microcontroller in each 1 ms. Thus the complete data of the consumers say about 20, is sent within 20 ms. If the consumers are 40 in number then the output is sent to the controller within 0.5 ms such that the input received and the processing speed of the controller remains the same to avoid data getting hanged.

III. Simulation Results Of Power Theft Detection System

In the controller, the data from the consumer end is compared with the data from the digital ammeter which is kept near the post. This data is of 8-bit and is selected by using the data from the post about the particular line is selected by using the address of the line. Now the data from sending end is sent to the controller in every 1 ms. The comparison of data from the consumer end and the post end will take place at a very high speed of about 20 micro-seconds in the microcontroller. But next data will be arriving after 1 ms only. So during this time interval, if there is any mismatch in the data in comparison, then the controller sends the address of the line and the post to the GSM module, which again sends the data to the Electricity Board. This simulation is shown in figure 4 and simulations are performed using proteus. The simulation result for the proposed system to avoid meter tampering using embedded system is shown in figure 4.

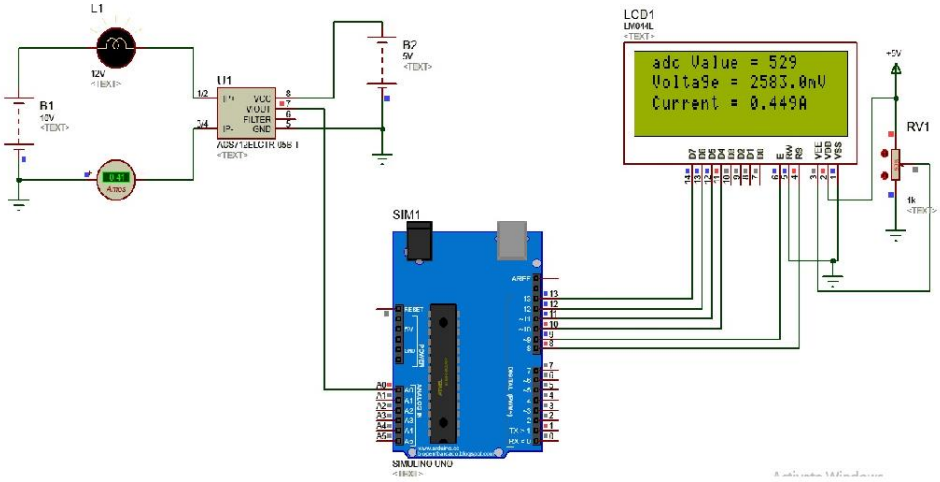

Fig.4: simulation result of proposed system to avoid meter tampering using embedded system

The simulation result for the proposed system to avoid illegal tapping using embedded system is shown in figure 5.

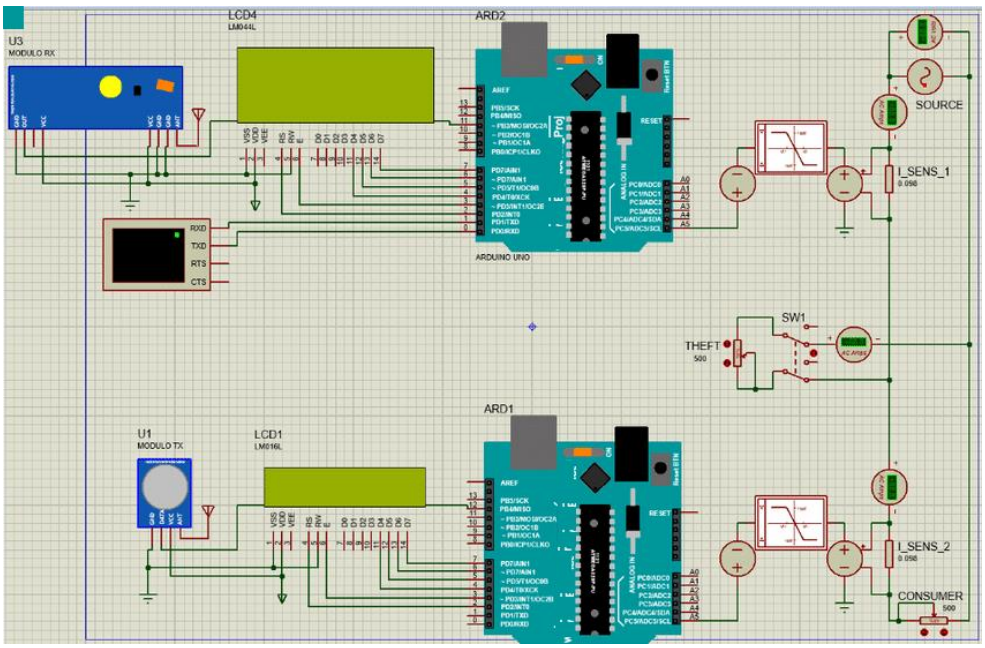

Fig.5: simulation result of proposed system to avoid illegal tapping using embedded system

Usually the input is kept high for the GSM module. This can be made ready to receive data about the address of the line and the post by making it low using the ISR interrupt. This interrupt gets enabled when there is any discrepancy in comparison. This entire process of comparison takes about 20 ms and hence for receiving another set of data after 20 ms, the clock is reset by using the up-counter, i.e., after 8 clock pulses. Now it can be noted that the entire cycle of comparison takes about 40 ms. during the reception of the next cycle data i.e within 20 ms, the other two types of thefts are verified. Hence the power theft due to meter tampering or tapping from feeders can be identified and sent to the Electricity Board.

IV. Conclusion

The power theft can be detected by adding all the data from the consumer side and comparing the same with that of the input to the post. Usually the digital ammeter data are added and compared. If there is any discrepancy in the comparison of these data then the GSM module is activated and then the address of the particular post is sent to the Electricity Board. This comparison is done once when all the data of consumer are compared for meter tampering. To detect this type of theft, the sending end current from one post, say post A to the other post, say B is compared. If the data compared are not equal in this comparison then the addresses of the both posts is sent to the Electricity Board. This is usually done after the comparison of the above said two comparisons.

References

1. I. H. Cavdar, “Performance analysis of FSK power line communications systems over the time-varying channels: Measurements and modeling,” IEEE Trans. Power Delivery, vol. 19, pp. 111–117, Jan. 2004.
2. Tom D Tamar kin “Automatic Meter Reading”, Public Power magazine Volume50, Number5 September-October 1992
3. R. Amarnath, N. Kalaivani and V. Priyanka, "Prevention of power blackout and power theft using IED," *2013 IEEE Global Humanitarian Technology Conference (GHTC)*, San Jose, CA, 2013, pp. 82-86.

4. S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier and S. Zonouz, "A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures," in IEEE Journal on Selected Areas in Communications, vol. 31, no. 7, pp. 1319-1330, July 2013.
5. F. Aslam, A. Nasser, E. Ulhaq and A. Umar, "Intelligent Modeling Scheme for Detection of Line Losses in Power Distribution System," 2013 UKSim 15th International Conference on Computer Modelling and Simulation, Cambridge, 2013, pp. 218-223.
6. Chan-Nan Lu, Shih-Che Huang and Yuan-Liang Lo, "Non-technical loss detection using state estimation and analysis of variance," 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, 2013, pp. 1-1.
7. T. V. Babu, T. S. Murthy and B. Sivaiah, "Detecting unusual customer consumption profiles in power distribution systems — APSPDCL," 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, 2013, pp. 1-5.
8. Juqin Zhang and Liqin Yue, "The design of multi-zone wireless burglar alarm system," International Conference on Cyberspace Technology (CCT 2013), Beijing, China, 2013, pp. 469-473.
9. A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in AMI systems," 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, 2012, pp. 1830-1837.
10. A. Rial and G. Danezis, "Privacy-preserving smart metering," in Proceedings of the 2011 ACM Workshop on Privacy in the Electronic Society, WPES, October 2011.
11. K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in Privacy Enhancing Technologies - 11th International Symposium, PETS, July 2011.
12. S. McLaughlin, B. Holbert, S. Zonouz, and R. Berthier, "AMIDS: A multi-sensor energy theft detection framework for advanced metering infrastructures," in Proceedings of the third IEEE International Conference on Smart Grid Communications (SmartGridComm), November 2012.
13. E. De Buda, "System for accurately detecting electricity theft," US Patent Application 12/351978, Jan. 2010.

.