IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Prevention of Power Theft Using Concept of Multifunction Meter and PLC

Uma Soni[1] Uma Kumari[2]

Mody University of Science and Technology, Lakshmangarh, Indore

Available online at: www.ijcseonline.org

Accepted: 06/Dec/2018, Published: 31/Dec/2018

***Abstract*:-** In the system and networks, abnormal behavior is detected by anomaly-based IDS (Intrusion Detection System). If the working of a computer system is different from normal working is considered as an attack. The difference of comparison relies on traffic rate, a variety of packets for every protocol etc. Malicious traffic or data on a system is detected by intrusion detection process. To detect illegal, suspicious and malicious information and data, IDS can be a part of the software or a device. First is Detection of an attack then using different method to stop, Prevent an attack and disaster is the user's highest priority. Anomaly-based IDS satisfy their requirement and demand.In present scenario electricity theft isa major hurdle in front of government. This problem affects Indian economy. The loss on quantity of theft is mirrored in the electricity company.People are affording more charges because intruders steal electricity by many ways.

***Keywords*: -** Intrusion detection system, Anomaly based system, Electricity theft, Intruders.

I. INTRODUCTION

Using different techniques of detection we are just guaranteed sure levels of security and can't decide received information is actual and precise [5]. For security, we tend to use ADS (Anomaly based system) algorithms. ADS algorithms use the system status data knowledge received to make a decision whether the working of the system is reliable or not. So we tend to set up investigation of various ADS algorithms to dissect their conduct utilizing least knowledge to accomplish objective and check discovery ability [7]. Verification and privacy issue are solved with cryptographic arrangements and avoid integrity attacks. Checksums and Message Authentication Codes used for unmarked alterations of bundles in transmission. The goal hub disposes of the parcel if they got the bundle and also the code created by the message trait system does not coordinate. IDS techniques looking for signatures for database assault. An attack signature could be a succession of activities that are typically recorded in a security log. In the event that a grouping of events matches with known signatures then it will give an alarm. Within the event that a grouping of occasions matches with known marks then a caution has arisen. This type of detection is useful to acknowledge assaults with standard conduct or exceedingly dependable administrations. Intrusion detection methods ways looking for irregularities will acknowledge changes within the framework that don't coordinate the traditional or normal behavior. When we see towards the power distribution sector of our country then we will get to know that, a major part of power in getting theft in many manners. Now we could not do much to stop it. The old system is still as it is. In present time we are very much advance in automation technology then why not to use automation for electricity distribution. If we are implementing the automation technology in this field then we can get an amazing return and result both. So this was the major motivation behind this idea. If somebody steal electricity in a building then every honor that lives in that building have to pay extra money [10]. I choose this idea by comparative study of different idea of different authors. In this project present a comprehensive view of smart electricity meters and their utilization to remove intruders attack. We explain in brief that how to meter process and what technologies and software are used to increasing more security and reliability.

Ways of Theft:-

There are various types of electrical power theft include:-

Direct hooking from line

It is the maximum used approach for theft of energy. Eighty% of total energy theft anywhere in the global is done through manner of direct tapping from line. The customer taps into a direct energy distribution line from ahead of the electricity meter. This strength supply consequently is unmeasured in its consumption and procured without or with switches [3].

Bypassing the electromechanical meter

In this method the input terminal and output terminal of the energy meter has been shorten by a wire. So energy cannot be registered in the energy meter.

Injecting foreign element into the electromechanical meter:-Sometimes professional individuals inject foreign factors along with transistors, resistors or IC chips into the electric meter which reasons a lower consumption of power.

Drilling holes into electromechanical energy meter: - This sort of tampering is accomplished to electromechanical type's meters. The person inserts overseas material within the meter to obstruct the free motion of the rotating disc.

Inserting film: - By inserting the film inside meter will slow down the speed of the disc, that will slow the meter readings.

Depositing a highly viscous fluid: - The friction causes the fluid to flow very slowly so consumption of electricity became lower.

Using strong magnets like neodymium magnets: -Strong magnets are used to slow the meter down. These types of magnet put both the sides of meter. So it become slow and show lower consumption.

Changing the incoming and outgoing terminals of the meter: - Changing the input output terminals will change the direction of electromagnetic field and that will change the rotating direction of disc, so the reading digits will move in reverse direction.

Damaging the coil of the meter: - Injecting excess current in meter current coil will damage the coil and due to that meter will not get the current input that will affect the meter readings.

Resetting electromechanical meter reading: - By physical damaging the meter they will rotate and reset the digits of the meter. A meter is used to record various parameters in an electrical circuit. It can be used to record values like voltage, current, resistance, frequency, and extra factors depending on the meter. It is the process of meter that takes analog signal as an input signal and then change into digital signal as an output. These output signals represent binary digits read by microprocessor. The processor can be programmed to interpret the incoming information which is shown at the screen [3][8].

Damage by mechanical shock:-A meter is damaged bymechanical shock. A mechanical shock is a unexpected acceleration caused, as an example, by means of impact, drop, kick, and explosion. Shock is a brief bodily excitation.

II. METHODS OF POWER THEFT CONTROL

To control power theft HVDS system. If someone tries to steal electricity from meter by any type of theft method then it controls them and damage machines [3]. Neural networks using SVM model and smart meters use to control theft. Now a day's all the countries are using advanced metering infrastructure and power theft control via plc system [8]. All countries are using Intelligent modeling scheme for detection of line losses in power distribution system [11]. All the methods are using these methods to control theft but some problems are still there.

Smart meters are used or installed in homes and in other region of world [1]. USA and Europe have been using smart meters. Australia and Canada are also using this. About all countries of the world like Eastern Europe America, North Africa, South Africa and Asia using meters. Use of smart meters more in 2018 than previous years. Now if we talk about present scenario all countries using smart meters to save energy and cost from intruders attack. It include easier Billing , processing automatic reading, detection of energy losses and early warning of intrusion and fast detection of disturbances in energy supply[2]. In these meters we cannot find exact location of theft. On the basis of readings we decide there may be possibility of theft.

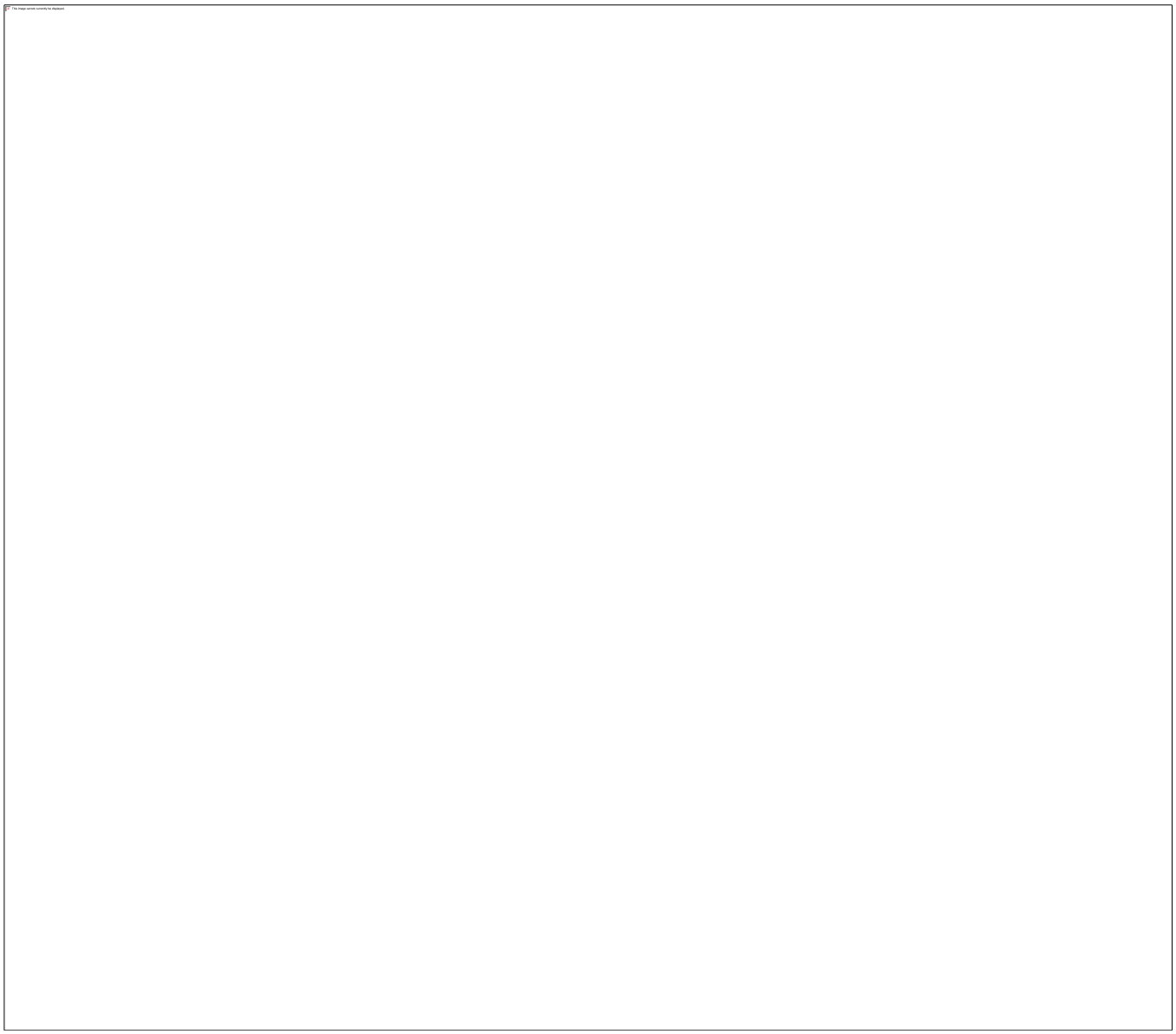
To overcome these ways of theft we use different idea of save energy and intrusion detection in energy by using MFM meters, profibus cable, PLC and SCADA to take exact readings on every second and give information about consumption of energy daily, weekly, monthly and yearly. We find out energy stealing point at that time when intruder steal energy [9]. Take action according to type of intrusion as soon as possible. So chances of theft decease. It creates easy billing, reduce man power cost and safe and secure system than others.

Proposed Algorithm:-

We propose an algorithm to control and overcome these ways of theft and save energy and reduce cost. So these steps are using for further procedure to control theft completely.

[1]. Install MFM meter on lighting pole.
[2]. Connect input (current and voltage) to MFM meter.
[3]. Install PLC and computer system in working office of electrical board.
[4]. Install software (simatic manager and SCADA software) in computer system.
[5]. Connect PLC to system by Ethernet cable.
[6]. Communicate PLC and system (PLC to SCADA).
[7]. Assign node address to MFM.
[8]. Communicate MFM to PLC with profibus DP cable.
[9]. Specify about MFM in PLC and assign address to input.
[10]. Create point configuration in SCADA and assign address for each signal as specify in PLC.
[11]. Now all information about a node will display on screen (output).
[12]. If there is any hurdle in communication and I/O then check again step 3.

Flowchart:-



Installation and communication:-

First Install MFM meter on lighting pole and Connect input (current and voltage) to MFM meter. Install PLC and computer system in working office of electrical board. Install software (simatic manager and SCADA software) in computer system. Connect PLC to system to Communicate and Assign node address to MFM. Communicate MFM to PLC with profibus DP cable and Specify about MFM in PLC and assign address to input. Then Create point configuration in SCADA and assign address for each signal as specify in PLC. Now all information about a node will display on screen (output).

After installation we defining Hardware Configuration and Specify the CPU hardware details in the program and also define communication protocol. Then Specify the MFM hardware details in the hardware configuration through GSD file. After installing GSD we will find catalog box where we can find hardware and model no. detail of MFM which we are communicating.

Select the particular MFM meter with correct model no. from catalog box and Specify the memory address in CPU and data required from MFM. In the same manner we can add multiple meters in the same network through profibus cable. For showing the input values on computer screen which is sent by MFM to PLC, we need to create point configuration in SCADA. By the help of this proposal we track online and save energy and money both.

III. RESULTS

We generate result of all meters in this way. We track all meters regularly to know where theft is. So we can easily monitor every meter. If there is any problem related to bus communication and distribution line then easily monitored and repaired to save energy.

Fig:-1Showing the report on voltage, current and power factors of meter.

We generate power report according to result daily, weekly, monthly and yearly basis.

Total Report

	Today	Yesterday	Current Month	Previous Month
WBSEDCL	7.05 MW	8.99 MW	25.54 MW	31.59 MW
LC4 Packing Plant SS	330 kW	1825 kW	3019 kW	2780 kW
MCC10 (Water Supply)	21 kW	49 kW	119 kW	174 kW
MCC7A (Compressor & Dryer)	1551 kW	2233 kW	6193 kW	5441 kW
MCC12 (Blending System)	289 kW	376 kW	1197 kW	1923 kW
MCC9 (Coal Mill & Auxilary)	1447 kW	180 kW	1691 kW	1505 kW
MCC5 (Flyash Handling)	405 kW	173 kW	799 kW	661 kW

	Today	Yesterday
Mill Running Hours	0.00 h	0.00 h
Total Feed	12 t	50 t
Clinker Feed	0 t	0 t
Slag Feed	12 t	49 t
Limestone Feed	0 t	0 t
Gypsum Feed	0 t	0 t
Flyash Feed	0 t	0 t

Fig:-2 Daily and monthly basis report.

IV. CONCLUSION

Using this algorithm we reduce the ways of electricity theft. To control power theft smart meters are used. Energy Consumption is calculated by using electronic smart meters. it's a two-way communication any power theft or problem in power system it recognizes. Here in this method we are going to use smart meters to control power theft. Generally consider an apartment consists of 'n' number of users. In the middle we need to set up an inspector box and another two meters from transmission & receiving side. The current flows through head, inspector & users. If there is any type of theft occurs, it creates difference in flow. So inspector gives an alarm to control power theft who regularly monitor.

Here we have reviewed some methods of power theft and control over power system .This consists of methods & controlling techniques of power theft loses occurring in

transmission are of two types technical& non-technical losses. Technical loses are common but these non-technical losses cannot be controlled. To control theft, there are so many techniques like smart meters, HVDS system, neural networks and PLC system. These controlling methods are reviewed in this paper with the comparison of proposed method . We have thoroughly studied and compared different types of power theft and methods to control them.

REFERENCES

[1]. D. Alahakoon and Xinghuo Yu, "Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey" , IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 12, NO. 1, FEBRUARY 2016 .

[2]. Q. Sun, H. Li, Z. Ma, "A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks" , January 2015.

[3]. B.Saikiran, R.Hariharan, "Review of methods of power theft in Power System" ,International Journal of Scientific & Engineering Research, Volume 5, Issue 11, November-2014.

[4]. N. Mohammad , A. Barua and M.Arafat," A Smart Prepaid Energy Metering System to Control Electricity Theft", 2013 International Conference on Power, Energy and Control (ICPEC).

[5]. S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy Theft in the Advanced Metering Infrastructure", International Conference on Critical Information Infrastructures Security, 2016.

[6]. R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions" , 2010 First IEEE International Conference on Smart Grid Communications.

[7]. Victor C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns", IEEE Transactions on Smart Grid · May 2015.

[8]. J. Nagi, K. S. Yap, S. K. Tiong," Detection of Abnormalities and Electricity Theft using Genetic Support Vector Machines", IEEE paper on march 1, 2009.

[9]. Thomas B.Smith, "Electricity theft: a comparative analysis" Elesvier 2004.

[10]. R.Rashed, M.AlanFung, F.Mohammadi, K.Raahemifar, "A survey on Advanced Metering Infrastructure",International Journal of Electrical Power & Energy Systems, Volume 63, December 2014.

[11]. A. Rial and G. Danezis, "Privacy-Preserving Smart Metering", Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, 2011.

[12]. K. Laeeq, W.Laeeq, "A comparative study among possible wireless technologies for smart grid communication networks", In: First international conference on modern communication & computing technologies; 2014.

[13]. R.Kalaivani, M.Gowthami,S.Savitha, N.Karthick, S.Mohanvel," GSM Based Electricity Theft Identification in Distribution Systems", International Journal of Engineering Trends and Technology (IJETT) – Volume 8 Number 10- Feb 2014.

