SMART POWER THEFT DETECTION SYSTEM USING WIRELESS COMMUNICATION

Kavitha.Chennareddy[1] ,Mohan BS [2]

[1]Assistant Professor,[2]Assistant professor,
[1]Electrical &Electronics Engineering,
[1]New Horizon college of Engineering ,Bangalore ,India

Abstract— Electricity theft is responsible for economic problems for the electric utility due to revenue loss caused by electricity consumers that are not paying for it. In this report, a Smart Power Theft Detection System (SPTDS) with instantaneous SMS alert is proposed. The set up contains an Smart Statistical Meter (SSM), placed at the transformer end and or on Electric High Pole. It communicates with the various consumer meters as well as linked with it through wireless communication i.e, WiMax. It monitors and records the readings from the consumer end and sets it as a reference value. Whenever this reference value is exceeded, unmetered load (illegal) is detected and this information is sent to Utility Company through WiMax channel for further action. The algorithm for this proposed project is modeled in MATLAB/SIMULINK and satisfactory results are expected at the end.

INTRODUCTION

Expeditious globalization has proved electricity to be more significant than any necessary commodity. Thus, there is an increased need of electricity which has increased power theft issues. Hence, there is an urgent need to develop a system which can detect power thefts in complex network. Distribution line losses are comprised of two types: Technical losses and Non-Technical losses. However, as per sample studies carried out by independent agencies including TERI, these losses have been estimated to be as high as 50% in some states. In a recent study carried by SBI capital markets, The Transmission and Distribution losses have been estimated as 58%. India is the fifth largest producer and consumer of electricity in the world,however,24*7 power supply still remains a dream unfulfilled. Despite an ambitious rural electrification programme, India is facing frequent blackouts. While 84.9% of Indian villages have at least an electricity line, just 46 percent of rural households have access to electricity. Electricity grids in the developed markets expect losses below 15%, but the losses by India's state utilities, over the past five years, were as high as 30% equal to about 1.5% of the country's GDP. About one-third of that loss is technical, but the rest is either given away for free or at subsidized rates to farmers, or lost to pilferage. Utility generation companies have little control over that; the losses are mainly due to the distribution companies which are mostly state owned enterprises. These distribution companies also conduct regular load shedding and intentional blackouts in certain areas to manage demand, as revenue collection doesn't always cover the bills to power generators. Although India has almost doubled its energy generation in the past decade by adding over 85GW of capacity, its old and inefficient distribution and transmission network lose more than 30GW of this generated power. This is a huge wastage of a commodity which is one of the most environmentally unfriendly to produce. The World Resources Institute estimates electricity transmission and distribution (T&D) losses in India to be 27 percent- the highest in the world. The T&D losses are due to variety of reasons, substantial energy sold at low voltage, sparsely, improper billing and high pilferage. The provision of power to the whole of India, urban and rural, is critical for India's transition to being a modern economy. Currently the quality and quantity of electricity is far from desirable. The technical losses are inherent in a system and can be reduced to an optimum level.

1.METHODOLOGY

This model includes SSM (Smart Statistical Meter) that are installed at the distribution transformers and at high poles. These SSM compare frequent power readings outgoing from each of the distribution transformers with reference power samples as registered by consumers with utility. If there is any difference between referenced readings and instantaneous readings recorded by the SSM, then SSM sends the message to utility for immediate visit to field for necessary action against such illegal load detected. This model includes SSM (Smart Statistical Meter) that are installed at distribution transformers and at high poles. These SSM's compare frequent power readings outgoing from each of the distribution transformers with reference power samples as registered by consumer with utility. If there is any difference between reference reading and instantaneous readings recorded by the SSM, then SSM send the message to the utility for immediate visit to field for necessary actions against such illegal load detected.
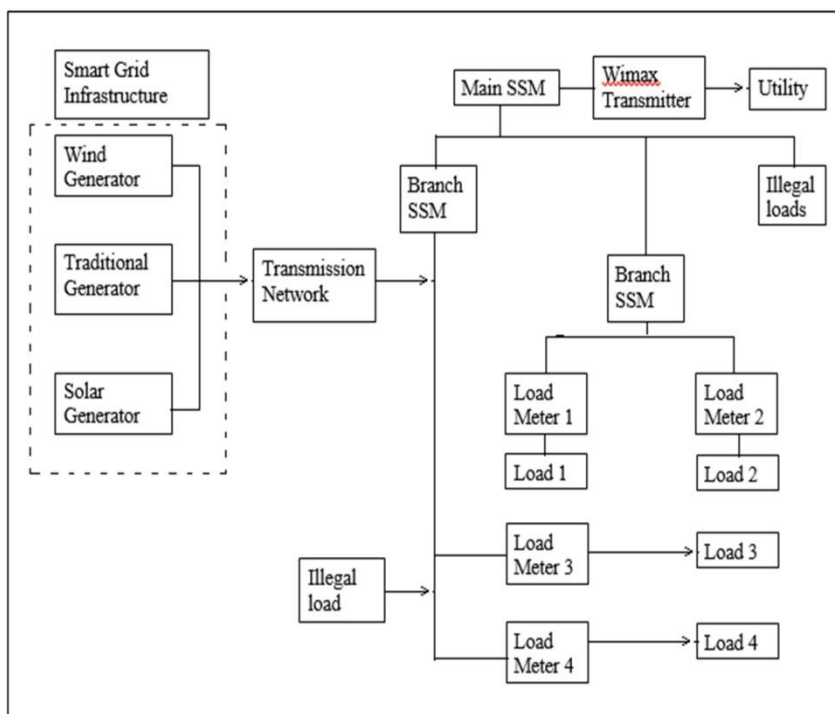
Fig.1 Block Diagram of proposed system

II.DATA ACQUISITION SYSTEM

1.Current Sensor:

A current sensor is a device that detects electrical current (AC or DC) in a wire, and generates a signal proportional to it. The generated signal could be analog voltage or current or even digital output. It can be then utilized to display the measured current in an ammeter or can be stored for further analysis in a data acquisition system or can be utilized for control purpose. Hall Effect current sensor is a type of current sensor which is based on phenomenon of Hall Effect discovered by Edwin Hall in 1879. Hall Effect current sensors can measure all types of current signals i.e. AC, DC or pulsating current. The Hall Effect is the production of a voltage difference (the Hall voltage) across an electrical conductor, transverse to an electric current in the conductor and a magnetic field perpendicular to the current.

2.Power transformer

The 230 V, 50 Hz is step downed using voltage transformer and current sensor is used to extract the waveforms of current. The output of the voltage transformer is proportional to the voltage across the load and output of current transformer is proportional to the current through the load. These waveforms are fed to Voltage Comparators constructed using LM317A op-amp. Since it is a zero crossing detector, its output changes during zero crossing of the current and voltage waveforms. A zero crossing detector is used as analog circuit to achieve the converting process of the current and voltage It consists of diode Rectifier Bridge which converts ac to dc and a voltage comparator. These outputs are fed to the PIC16F877A which does the further power factor calculations.

III.SUPERVISIORY CONTROL SYSTEM

1.8051 Microcontroller :

The Intel 8051 is an 8-bit microcontroller which means that most available operations are limited to 8 bits. There are 3 basic "sizes" of the 8051: Short, Standard, and extended. The Short and Standard chips are often available in DIP (dual in-line package) form, but the Extended 8051 models often have a different form factor, and are not "drop-in compatible".

Pin No.	Symbol	I/O Type	Description
1 2	/CSA /CSB	I	Chip selection When CS1=L,CS2=H, select IC1 When CS1=H,CS2=L, select IC2
3	VSS	Supply	Ground
4	VDD	Supply	Power supply
5	V0	Supply	LCD driver supply voltage
6	D/I		Data input/output pin of internal shift register MS SHL DIO1 DIO2 H H Output Output H L Output Output L H Input Output L L Output Input

7	R/W		Read or Write
			
			RW Description
			H Data appears at DB[7:0] and can be read by the CPU
			while
			    E= H CS1B=L,CS2B=L and CS3=H.
			L Display data DB[7:0] can be written at falling edge of E
			    when CS1B=L, CS2B=L and CS3=H.

8	E		Enable signal E Description H Read data in DB[7:0] appears while E= "High". L Display data DB[7:0] is latched at falling edge of E.
9~16	DB0~ DB7	I/O	Data bus [0~7] Bi-directional data bus
17	/RST	I	Reset signal. When RSTB=L 【1】ON/OFF register becomes set by 0.(display off) 【2】display start line register becomes set by 0 (Z-address 0 set, display from line 0) 【3】After releasing reset , this condition can be changed only by instruction.
18	VEE	Power	VEE is connected by the same voltage.
19	A		Back-light anode
20	K		Back-light cathode

Fig.3 Pin Description

2. LCD :

LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters (unlike in seven segments), animations and so on.A 16x2 LCD means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data. The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the LCD. The data is the ASCII value of the character to be displayed on the LCD.
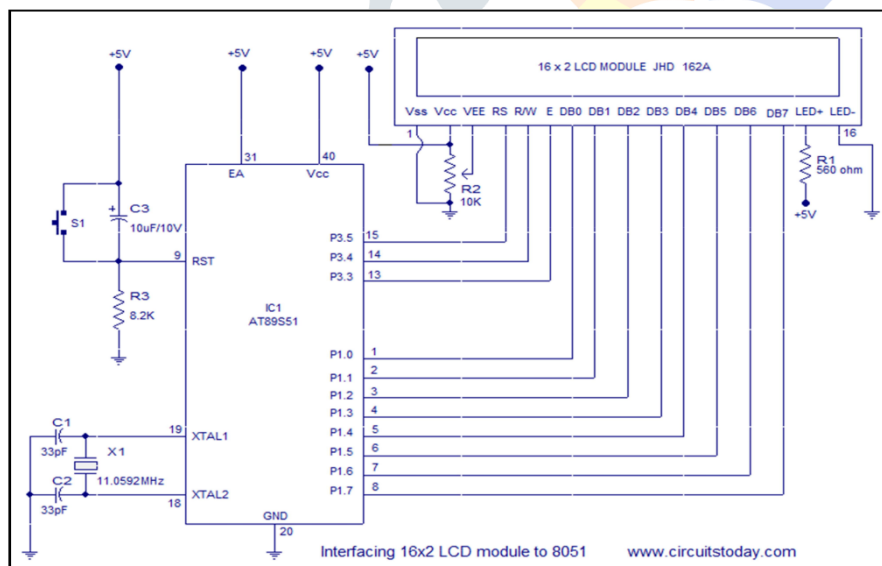
Fig.4 Interfacing LCD with 8051 Microcontroller

3.RS232 :

Computer uses serial communication to communicate with PIC16F17A. To allow compatibility among data communication equipment made by various manufacturers, an interfacing standard called RS 232 was set by electronics industries association (EIA) in 1960. Since the standard was set long before the advent of TTL logic family, its input and output voltage levels are not TTL compatible. In RS232,a 1 is represented by -3 to -25 V, while a 0 bit is +3 to +25 V, making -3 to +3 undefined. For this reason, to connect any RS232 to a microcontroller system we must use voltage converters such as MAX232 to convert the TTL logic levels to the RS232
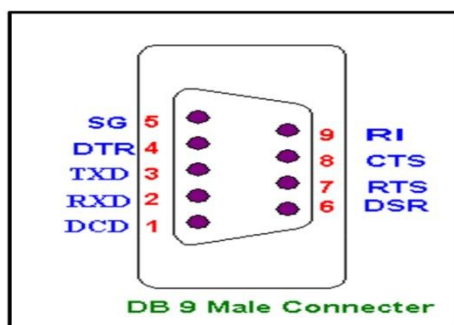
Fig.5 DB-9 Cable

4. MAX232

The MAX 232 converts from RS232 voltage levels to TTL voltage levels, and vice versa. One advantage of the MAX 232 chip is that it uses a +5V power source which, is the same as the source voltage for PIC16F877A.The MAX 232 has two set of line drivers for transferring and receiving data. The line drivers used for TxD are called TR1 and TR2, while the line drivers for RxD are designated as RE1 and RE2.The MAX232 has two receivers (converts from RS-232 to TTL voltage levels), and two drivers (converts from TTL logic to RS-232 voltage levels). This means only two of the RS-232 signals can be converted in each direction. Typically, a pair of a driver/receiver of the MAX232 is used for TX and RX signals, and the second one for CTS and RTS signals voltage levels, and vice versa.

Fig.6 Circuit diagram of MAX232
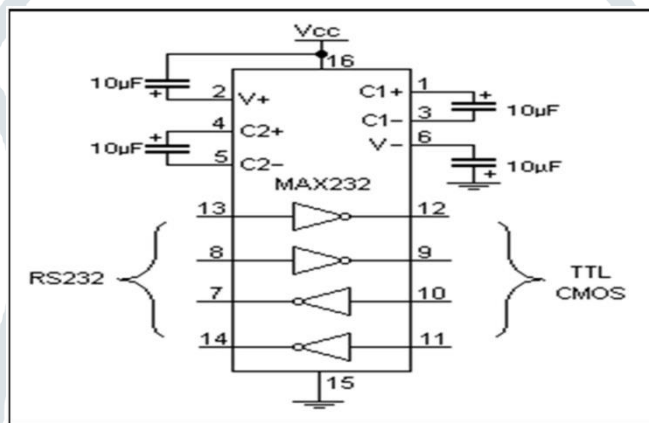
5. Power supply:

Regulated power supplies are commonly used in engineering projects. Power supply is food of any circuit. The circuit consists of a 9V step down transformer, voltage regulator IC (7805) and some capacitors, used for filtering purpose. The step down transformer, down-converts the high voltage AC input (230V, 50 Hz) to a 9V, 2A; because the transformer we used here having a specification of 9V/A. The alternating voltage from secondary terminal of the transformer is given to a bridge rectifier. The bridge rectifier converts alternating voltage to unidirectional voltage with the switching action of diodes. This voltage is finally fed to a 5V regulator IC through a 470uF, 50V electrolytic capacitor, which eliminates the ripples and make the output stable. After regulation we get a 5V DC voltage at the output of 7805 IC.

IV. DETAILS OF WiMAX

 The IEEE 802.16e is an amendment of 802.16d standard. The aim of such an amendment is to incorporate mobility with large range of coverage. Mobile WiMAX uses OFDMA (Orthogonal Frequency Division Multiple Access) technique. The OFDMA system divides signals into sub channels so that resistance to multipath interference gets enlarged. Thus, the problem of Inter Symbol Interference (ISE) vanishes and supports Long Term Evaluation (LTE) leading to the path of 4G.

WiMAX Physical and MAC Layer Architecture:

WiMAX utilizes two layers of OSI (Open System Interconnection) reference mode. They are, physical and MAC (Medium Access Control) of data link layer. This layer provides connection among communicating devices and enables transmission of bit sequence. Two types of transmission techniques are adopted by the physical layer; they are, OFDM and OFDMA. A frequency band below 11GHz is supported by these techniques. Duplexing technology used are TDD and FDD. The basic function of WiMAX MAC is to interface the physical layer and the upper transport layer.

TABLE I

OSI DATA LINK LAYER	Service Specific Convergence Layer	
	Privacy sub Layer	
	MAC (Medium Access Control)	
OSI PHYSICAL LAYER	Physical Layer (PHY)	

Performance Simulation Block Diagram of Mobile WiMAX:

The performance of mobile WiMAX is studied with WiMAX transmitter and WiMAX receiver module which are designed separately in MATLAB/Simulink software.
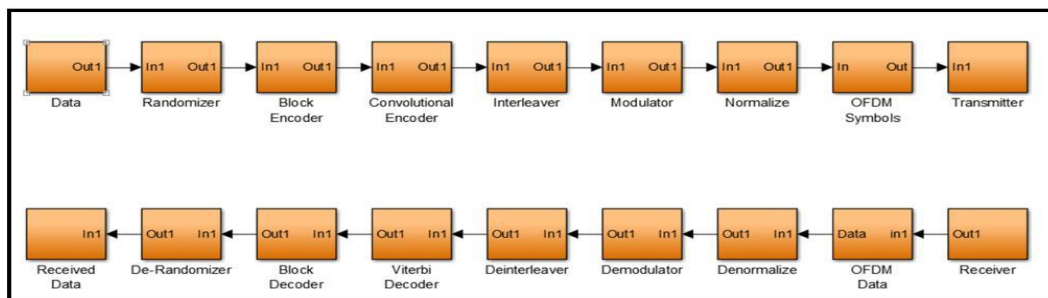

Fig.7 Simulink Diagram of WiMAX Transmitter Module

Encoder:

1. Reed Solomon Encoder: Here a polynomial is generated from the data symbols to be transmitted. Then this generated polynomial is over sampled to send instead of sending original symbols.

2. Convolutional Encoder: After Rs-Encoding step, the convolutional encoder is used to combine (multiply) the generator polynomial and primitive polynomial sampled data.

3. Puncturing Process: It systematically removes bits from the output of an encoder of low rate. It is with a view to minimize amount of data transmitted. This convolution and encoding is directly supported by Simulink and the same is implemented in single block.

4. Inter-leaver: This is used to combine available bits using 12 interleaving levels. The effect of this is similar to spreading the bits with different symbols where they are then combined to get new symbols. These new symbols are of the same size but are having rearranged bits

5. Modulation: The data is modulated depending on their size with different schemes like BPSK (Binary Phase Shift Keying), QPSK (Quadrature Phase Shift Keying). Here QPSK modulation is used. The total incoming bits are grouped among i groups such that there are 2i points. The size of i for a QPSK modulation is 2.

6. IFFT: The source symbols are converted from frequency domain to time domain. If N numbers of subcarriers are chosen to evaluate performance of WiMAX, the primary function of IFFT is to receive the N number of symbols and sinusoidal at a time. Output of IFFT is N sinusoidal signals

7. Subcarrier: The carriers are sinusoidal OFDM system. When the integral product of two periodic signals is zero over a single period then such signals are called as orthogonal to each other. These carrier signals are essential to avoid inter channel interference. Since, they are used as guard band in this system.

8. CP (Cyclic Prefix): A CP is to be inserted before a transmitted symbol so as to avoid Inter Symbol Interference (ISI). This CP maintains frequency orthogonality with reduction in delay due to multipath propagation. Therefore if the length 'L' of CP is greater than multipath delay then, ISI problem is totally eliminated. After this step the data is transmitted through physical medium.
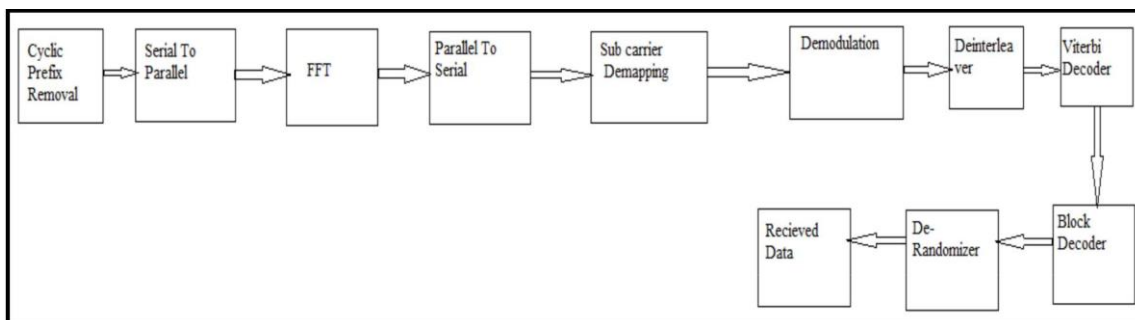
Wi MAX Receiver Module:

Fig.8   WiMAX Receiver Module

CP Removal: After synchronization, the data received contains CP of each of OFDM signal which is removed.

FFT (Fast Fourier Transform): Using the appropriate number of samples the FFT converts time domain signal to frequency domain. To carryout OFDM of 256points, the zeroes are added at beginning and ending of OFDM signal. Here in receiver module these zeroes are removed.

Denormalizer or Disassembler: This deals with separating the signal either in time or frequency domain. By this data, pilots, training are obtained.

RESULTS

In this paper, a Smart Power Theft Detection Model (SPTDS) is developed for detecting power theft. Power theft detection is carried out with two models. In each cases the SPTDS is aware of registered loads and if any illegal load is connected to system in the form power theft then a message is given to the utility through WiMAX Communication protocol. Here the same results have been proved with both the models and power theft message sent to utility is just shown as a pop-up message.

SMART GRID MODEL

This model consists of a substation representing the integrated energy from both renewable and non renewable sources of generation. This energy is supplied to six Domestic house loads, one heavy industry load and five industry load. Each of these loads are modelled and their consumption data is
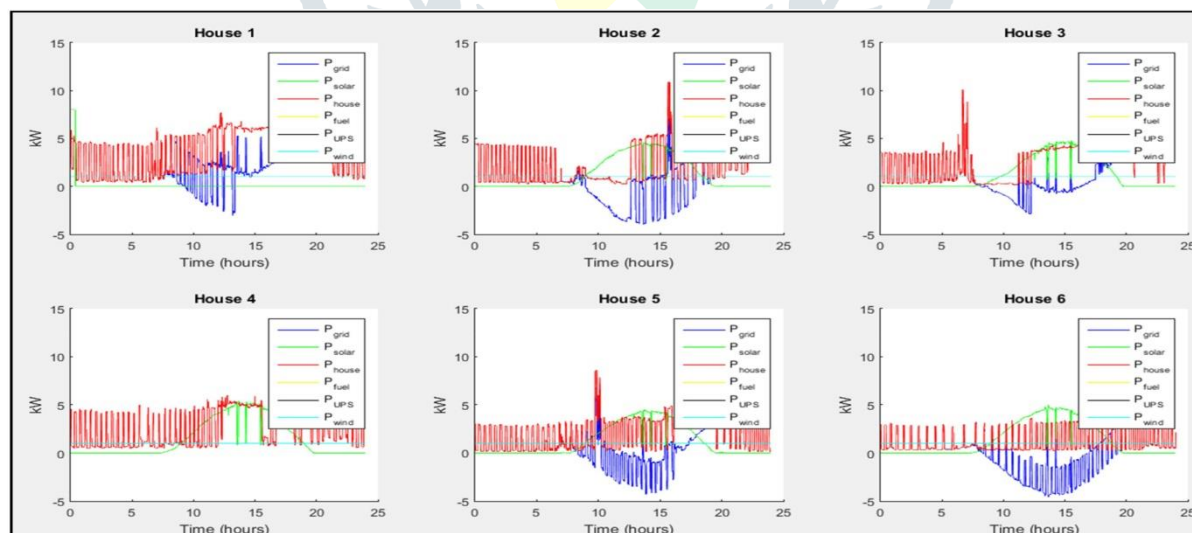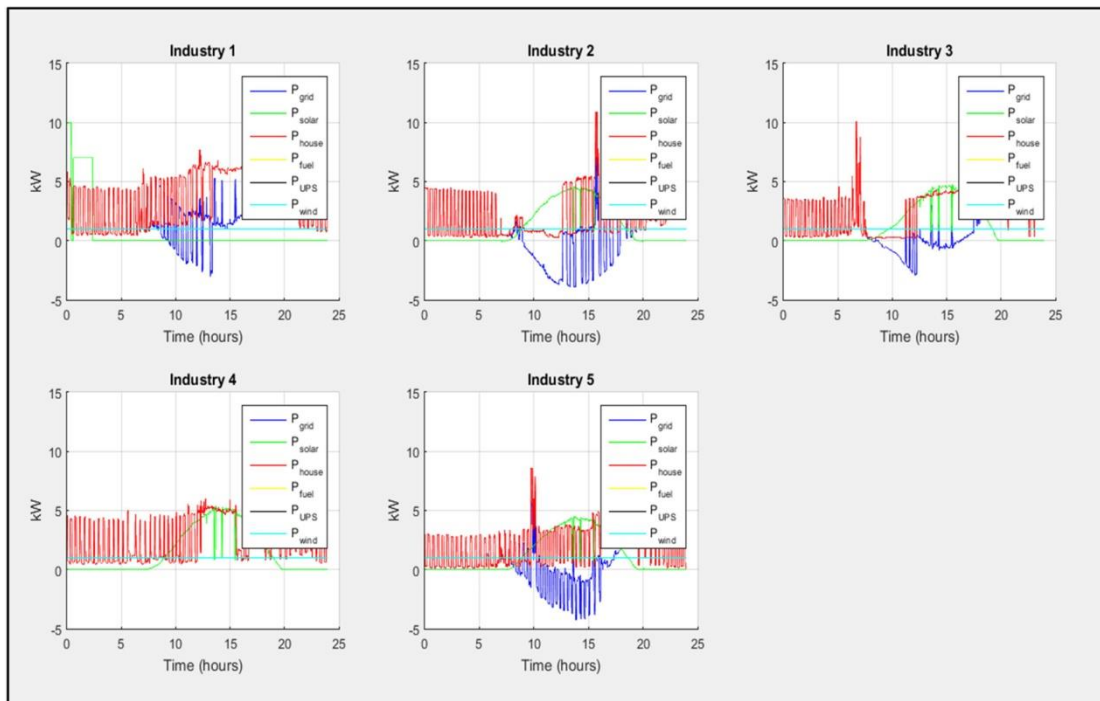

Fig.9 Energy consumption data of House Load

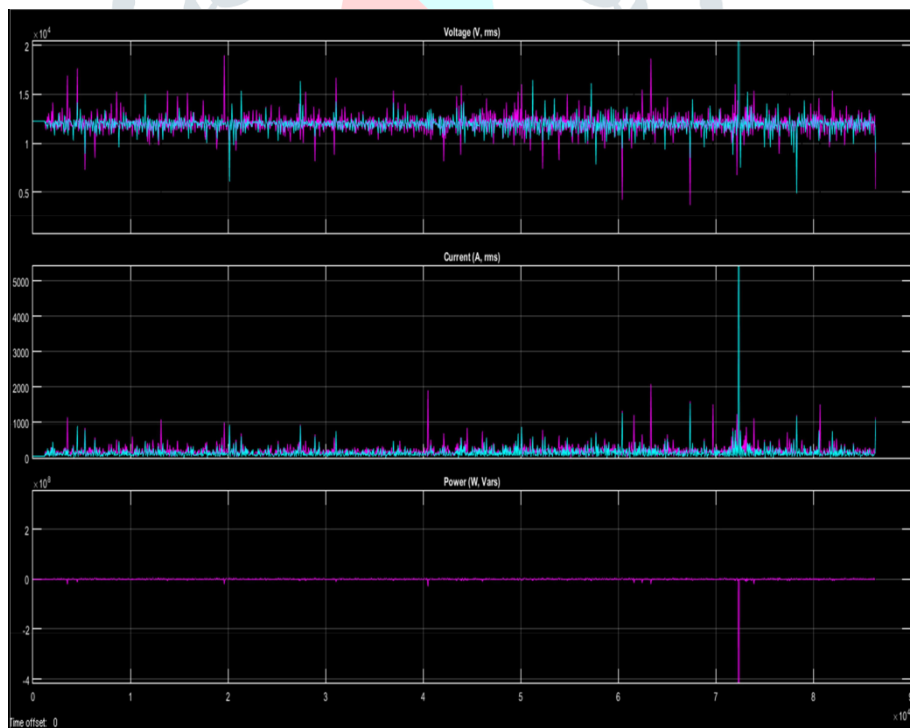Fig.10 Energy consumption data of Industry load

Fig.11 Input to the Substation from generating units

Substation parameters in Smart Grid Simulink model

Phase to phase rms voltage(V)	Frequency(Hz)	3 phase short circuit level at base voltage(VA)	Base voltage (Vrms ph-ph)	X/R ratio
12.47e3	60	2e6/0.05	12.47e3	10

Simulink Model: Smart grid model is designed in the Simulink software. The distribution transformers supply the required power to the loads. Smart stastical meter   is connected in between the branch to collect the energy supplied by the distribution transformers in addition to this also telemeters certain illegal loads connected in between the distribution transformer and distribution network.Thus , all the data from Smart Stastical Meters is collected and is added which is then compared against a   reference value.The reference value is nothing but the registered load to the utility; if the given power is more than the refernce value then theft is detected and the same is sent to utility using WiMAX , here the theft message is popped up on the screeen.
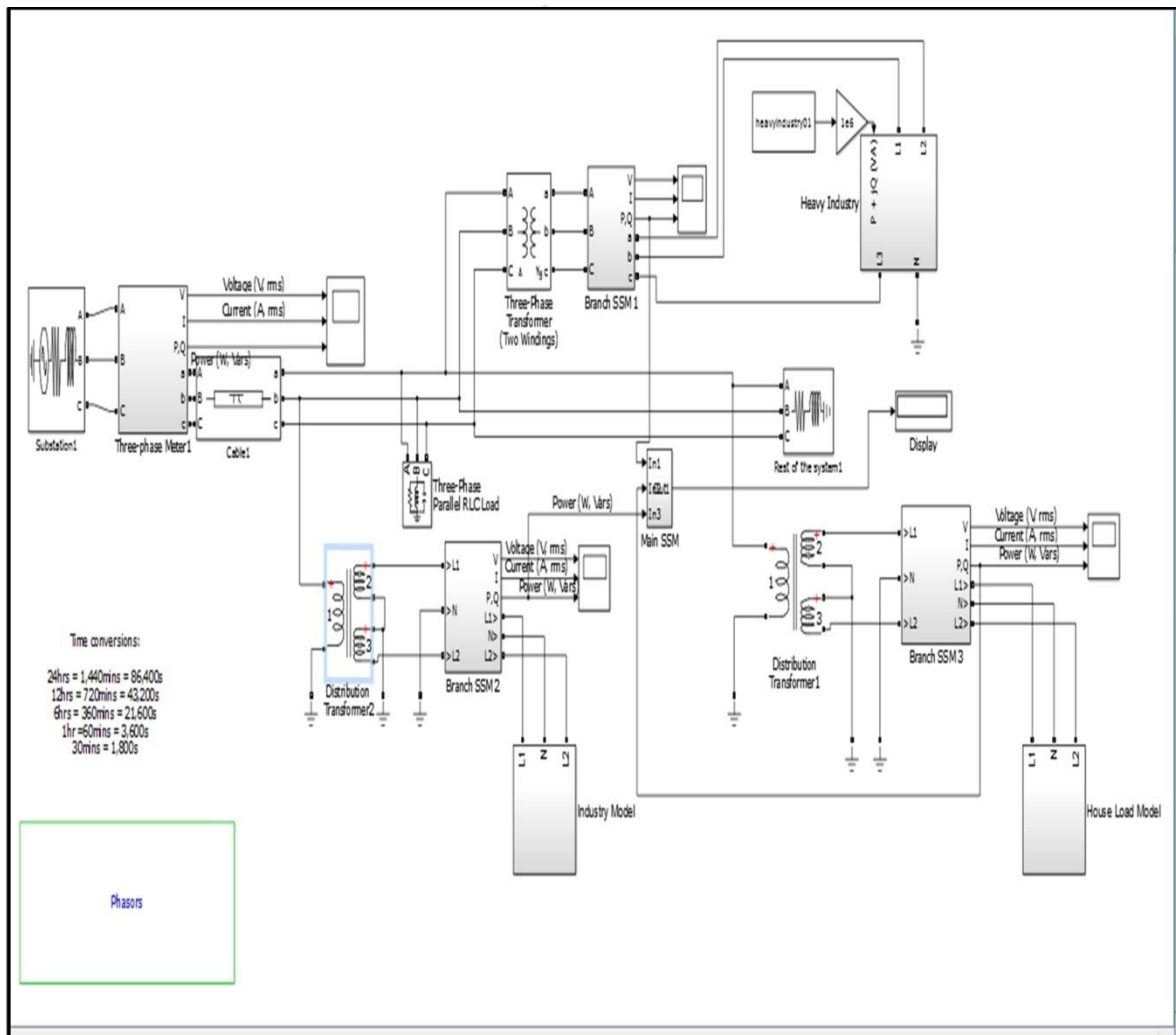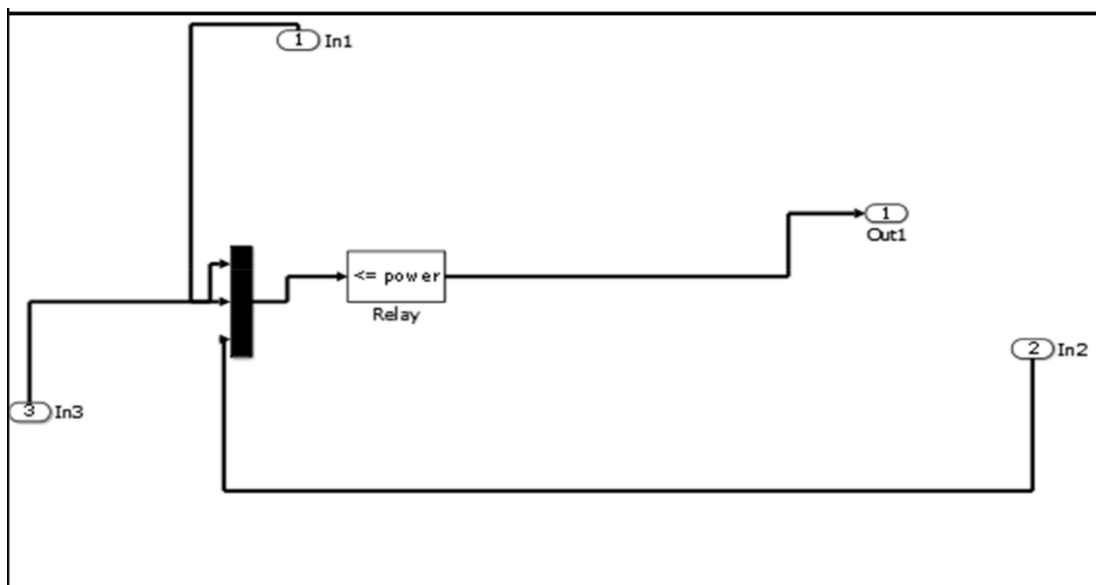

Fig.12 Grid Simulink Model

Fig.13 Masked View of SPTDS (Smart Power Theft Detection System)

Fequency(Hz)	Positive and zero sequence resistance(ohms/km) (r1,r0)	Positive and zero sequence inductance(H/km)	Positive and zero sequence capacitance(F/km)	Line length(km)
	0.01273	0.9337e-3	12.74e-9	
60	0.3864	4.1264e-3	7.751e-9	10

Cable parameters used in Grid Simulink model

Total registered load for this model is 15 kilo watt.

Results of Grid Model:

S.No	Power recorded by SSM	Pop-Up Message
1.	18kW	Theft Detected
2.	10kW	Theft not Detected

CONCLUSION:

The intense utilization of information technologies makes the power grid vulnerable to cyber-attacks. Due to the high cost for protecting the whole power system, an alternative is the development of cost-efficient methodologies able to reduce commercial losses caused by cyber-attacks that corrupt energy metering data. The proposed methodology employs resources of metering, communication and information from the smart grid, and mathematical tools that are typically used in statistical quality control. The system algorithm is very satisfactory as it continuously sums up total energy measurements of all consumers' meters linked with it; and uses this "value" as a reference value to detect unmetered load. The designed system has a high degree of reliability, sensitivity and efficiency. If design is fully implemented then revenue loss due to power theft will be greatly reduced while revenue collection will greatly increase. Through this is a new scheme of integrated detection of energy theft in power grid network especially in distribution side, we can hopefully control the extent of Power theft.

REFRENCES

[1] Jônatas B. Leite, Member, José R. S. Mantovani," Detecting and Locating Non-technical Losses in Modern Distribution Networks ".
[2] Arango, L.G., Deccache, E., Bonatto, B. D., Arango, H., Ribeiro, P.F., Silveira, P. M. CERIn "Impact of Electricity Theft on Power Quality ", Center of Excellence in Smart Grids UNIFEI - Federal University of Itajuba Itajuba-MG, Brazil

[3] B. O. Omijeh Deptt. of EC Engineering, University of Port Harcourt, Port Harcourt,G. I. Ighalo "Intelligent Power Theft Detection Model for Prepaid Energy Metering In Nigeria "

[4]False Data Injection on State Estimation in Power Systems — Attacks, Impacts, and Defense: A Survey Ruilong Deng, Member, IEEE, Gaoxi Xiao, Member, IEEE, Rongxing Lu, Senior Member, IEEE, Hao Liang, Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE

[5] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security Privacy, vol. 7, no. 3, pp. 75-77, May 2009.

[6] A. –H. Mohsenian-Rad, and A. Leon-Garcia, "Distributed InternetBased Load Altering Attacks Against Smart Power Grids," IEEE trans. on Smart Grid, vol. 2, no. 4, pp. 667-674, Dec. 2011.

[7] S. M. Amin, "Smart grid security, privacy, and resilient architectures: Opportunities and challenges," in IEEE PES General Meeting, San Diego, USA, 2012, pp. 1-2.

[8] D. Wei, Y. Lu, M. Jafari, P. M. Skare and K. Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks," IEEE trans. on Smart Grid, vol. 2, no. 4, pp. 782-795, Dec. 2011.

[9] Y. Guo, C.-W. Ten and P. Jirutitijaroen, "Online Data Validation for Distribution Operations Against Cybertampering," IEEE trans. on Power Syst., vol. 29, no. 2, pp. 550-560, Mar. 2014z

[10] Y.-H. Chang, P. Jirutitijaroen and C.-W. Ten, "A simulation model of cyber threats for energy metering devices in a secondary distribution network," in Proc. 5th Int. CRIS on Critical Infrastructure, Beijing, China, Sep. 2010, pp. 1-7.