International Journal For Technological Research In Engineering *ISSN (Online): 2347 - 4718*
National Conference on Importance of Inter-disciplinary Studies in Higher Education in the areas of Engineering, Science, Management and Humanities
(February – 2018)

WIRELESS POWER THEFT MONITORING SYSTEM

Luv Sharma[1], Dr. Pranay Joshi[2], Mukesh Sharma[3], Deepak Tak[4]
Department of Electronics & Communication Engineering,
SS College of Engineering, Udaipur, Rajasthan, India.

Abstract: Electricity theft is at the center of focus all over the world but electricity theft in India has a significant effect on the Indian economy, as this figure is considerably high. While technology in on the raising slopes, we should also note the increasing immoral activities. With a technical view, Power Theft is a non –ignorable crime that is highly prevent, and at the same time it directly affected the economy of a nation. Electricity theft is a social evil, so it has to be completely eliminated. Power consumption and losses have to be closely monitored so that the generated power is utilized in a most efficient manner. Power theft is the biggest problem now days, which causes huge loss to electricity boards. And to cover these losses ultimately, price are increased. So if we can prevent these thefts, we can save lot of power. By keeping track of electricity used, you determine where the greatest opportunity for energy savings lies. This project of ours is aimed at reducing the heavy power and revenue losses that occur due to power theft by the customers. Becoming aware of overall energy use involves keeping track of the readings on the readings on the electric meter. The normal practice for power theft is to short the input and output terminals or to place a magnet on the wheel in care of old meters. So by sensing current flow through the line & energy feedback we can prevent it using a circuit breaker.

Keywords: Electricity Theft, Non-technical losses, Transmitter section, Receiver Section.

I. INTRODUCTION

Electricity theft is at the center of focus all over the world but electricity theft in India has a significant effect on the Indian economy, as this figure is considerably high. While technology in on the raising slopes, we should also note the increasing immoral activities. With a technical view, Power Theft is a non –ignorable crime that is highly prevent, and at the same time it directly affected the economy of a nation. Electricity theft is a social evil, so it has to be completely eliminated. Power consumption and losses have to be closely monitored so that the generated power is utilized in a most efficient manner.

The system prevents the illegal usage of electricity. At this point of technological development the problem of illegal usage of electricity can be solved electronically without any human control .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.

In this system, a micro controller is interfaced with an energy metering circuit, current sensing circuit, RF communication link, & a contactor to make or break power line. At the sub-station end, a pc is connected with a RF link to communicate with all energy meters &a buzzer in normal condition, micro controller reads energy pulses & current signals. If current is drawing &energy pulses are normal, then no power theft is being done & the o/p is connected. If current is drawing & energy pulses are not coming, then it indicates that power theft.

For implementing this system we have designed two sections:

- Transmitter Section
- Receiver section

The Transmitter section is placed at consumer house while receiver section is placed at nearby local substation.
The general block diagram of the system together is given below

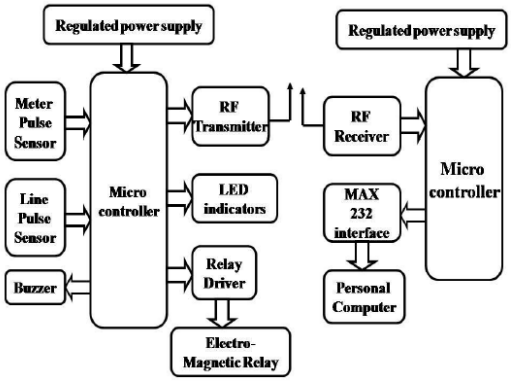


Fig.1 Wireless Power Theft Monitoring System

The regulated power supply converts the standard 220 volts, 50 or 60 Hz AC available at wall outlets into a constants DC voltage. It is one of the most common electronics circuits that we can find. The DC voltage produce by a power supply is used to power all the types of electronic circuits, such that television receiver, stereo system, CD players and laboratory equipment. The regulated dual voltage DC power supply is to be used for the FM receiver. The regulated power supply is to provide the necessary dc voltage and current, with low levels of ac ripple and with stability and regulation. There are various methods of achieving a stable dc voltage from ac mains. The two methods are more commonly used. These are used;

- A linear voltage regulator and
- A switching mode regulator.

Several types of both linear and switching regulators are available in integrated circuit (IC) form. By using the linear voltage regulator method, we must get the regulated dual dc power supply.

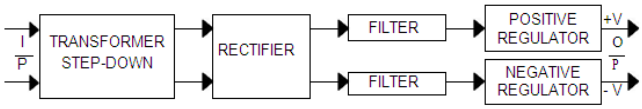


Fig.2 Regulated Dual DC Power Supply

Regulated power supply is an electronic circuit that is designed to provide a constant dc voltage of predetermined value across load terminals irrespective of ac mains fluctuations or load variations. A regulated power supply essentially consists of an ordinary power supply and a voltage regulating device, as illustrated in the figure. The output from an ordinary power supply is fed to the voltage regulating device that provides the final output. The output voltage remains constant irrespective of variations in the ac input voltage or variations in output (or load) current. This section applied in the houses with energy meter. In the transmitter section, at the time of theft the energy meter sensor and line sensor reads and calibrates the pulses. The detector detects the theft and the output of it is amplified using high power amplifier. The amplified signal is fed to level comparator. Level comparator is set to given reference value. In normal condition the input signal value is lower than reference signal value and provides logic 1 to MCU. But in abnormal condition, the input signal value exceeds the set reference value and provides logic 0 to MCU. The MCU unit works on conditional logic of "If – then – else" and produces output to encoder. The encoder encodes the signal into assembly language and transmits it to RF Transmitter for transmission through antenna.

II. ELECTRICITY THEFT

Generation, transmission and distribution of electrical energy involve many operational losses. Whereas, losses implicated in generation can be technically defined, but T&D losses cannot be precisely quantified with the sending end information. This illustrates the involvement of nontechnical parameters in T&D of electricity. Overall technical losses occur naturally and are caused because of power dissipation in transmission lines, transformers, and other power system components. Technical losses in T&D are computed with the information about total load and the total energy billed. NTL cannot be precisely computed, but can be estimated from the difference between the total energy supplied to the customers and the total energy billed.

NTL are caused by the factors external to the power system. In many developing countries, NTL are a serious concern for utility companies as they account to about 10 to 40% of their total generation capacity. Data regarding NTL is uncertain and it is very difficult to analyze theft in terms of actions that cause these losses. Electricity theft forms a major chunk of the NTL. Electricity theft includes bypassing, tampering with the energy meter and other physical methods to evade payment. Illegal tapping of electricity from the feeder and tampering with the meter are the most identified and accounted ways of theft.

Electricity theft can also be defined as, using electricity from the utility company without a contract or valid obligation to alter its measurement is called electricity theft.

A combination of software, hardware and additional mechanical parts that together forms a component of a larger system, to perform a specific function. It's a technology, characterized by high reliability, restricted memory footprint and real time operation associated with a narrowly defined group of functions. Automation has made the art of living comfortable and easy. "Technology have taken the world by storm performance ratings and exceptionally value for money prices" .Our project throws light on automated monitoring of theft identification, which is an application of embedded controllers 'Electricity theft' as covered in this project encompasses areas itemize known as 'Illegal uses or by bypassing it completely.

Many developing countries confront widespread theft of electricity from government owned power utilities. In India electricity theft leads to annual losses estimated at US$4.5 billion, about 1.5 percent of GDP. The losses, experts say, are currently 29% of the total generation which equals a shocking Rs 45000 crore in the fiscal year 2009-10. According to experts, if not for these losses over decade now, India could have built two mega power plants of around 4,000 MW capacity every year power losses in 2001-02 was 32.86% and increased to 34.78% in 2003-04.in 2008-2009, it stood at 28.44% but currently the figure is again 29%.it is as high as 51% in Jharkhand, 45% in Madhya Pradesh and 40% in Bihar.
Who are the losers? Honest consumers, poor people, and those without connections, who bear the burden of high tariffs, system inefficiencies, and inadequate and unreliable power supply. Line faults may be caused due to over current or earth fault. If there happens to be a connection between two phase lines then over current fault occurs. Earth fault occurs due to the earthing of phase line through cross arm or any other way. Now in India, there is not any technique to detect the specific location of the fault immediately. Power theft is one of the major problem faced by Indian electrical system.

These problems can be solved effectively through this project. By the proposed architecture the above mentioned problems can be solved. The motivation for us to take up this project is the current inefficient distribution system of the electricity boards all over the world. Also the present inability of the authorities in applying the existing laws in a stringent form has encouraged more and more people to involve in such unlawful activities. In case we develop an

effective system to remotely monitor the use of power and are able to detect power theft at the exact location in a accurate and cost effective way, such huge losses can be prevented. This kind of money could definitely be used for the development of the quality of electricity board and its service. The severe power shortage can be overcome by the implementation of our simple system. More over this kind of implementation of proper billing to all the customers would reduce the reckless use of power and would surely help us to build a greener and more eco-friendly environment for ourselves. As the majority of the power we generated is by burning coal, which adds to the already severe problem of the greenhouse effect. Thus our group has been motivated to bring up this completely unique method of remotely sensing power theft in most of the possible ways.

III. EFFECTS OF ELECTRICITY THEFT

Negative effects of electricity theft are severe and dangerous. Primarily, electricity theft affects the utility company and then its customers. In addition, electricity theft overloads the generation unit. In energy market, utility companies expect their money back from the customers for the electricity supplied, most of which is lost by them due to the NTL (Non-technical losses).Electricity theft is a serious concern for utility companies as they are under threat of survival because of these incurring economic losses. It is evident that some utility companies in developing countries are losing about 10 to 30 percent of their total revenue, which shows that they could not invest on measures to reduce the electricity theft. These economic losses affect the utility company's interest in development of the devices in view of improving the quality of supply or for electrification process.

IV. IDENTIFICATION OF THEFT

- Financial Rewards: Utility companies encourage consumers to report electricity theft, sometimes offering big rewards for information leading to conviction of anyone stealing electricity. Unfortunately, most cases are never identified in the apartment industry due to lack of timely information.
- Periodic Checks: Electricity theft frequently takes place after service has been disconnected. Some utility companies periodically check disconnected meters if the customer has not contacted them to reconnect service. This labor-intensive, manual process has little chance of success given that the apartment industry averages 70% turnover of tenants annually.
- Meter Readers: Utility meter readers typically suspect that electricity theft is taking place when they find a broken meter tag or other signs of tampering. But as more utility companies outsource the meter reading function to third parties, training meter readers to detect theft is becoming more difficult and less efficient. In addition, third party meter readers do not read disconnected meters.

V. PREVIOUS POWER THEFT DETECTION WORK

Bandim C.J. et al. proposed utilization of a central observer meter at secondary terminals of distribution transformer. Vigilant energy metering system (VEMS) is an advanced energy metering system that can fight against electricity theft Nagi J. et al. proposed a novel approach of using genetic algorithm- support vector machines (GA-SVM) in detecting electricity theft.

Modern detecting tools: There are many modern tools that assist in power theft identification. Some of them are:-

- Tamper proof seals and labels.
- Meter leaders.
- Tamper resistant screws / locks. AC Check meter and remote meter readers.
- Tamper alarms and sensors.

VI. DETECTION AND ESTIMATION OF THEFT

Researchers have proposed and developed several techniques for detection and estimation of electricity theft. Of which, a few methods are illustrated in this section. Total phase currents at all the distribution transformers and feeder lines over a period of time are collected. These two values of the current are compared to estimate the total electricity being lost by the utility company in the form of theft.

Bandim C.J. et al. proposed utilization of a central observer meter at secondary terminals of distribution transformer. Value of energy read by the central observer meter is compared with the sum of energy consumption values read by all energy meters in range. These two values of the current are compared to estimate the total electricity that is being consumed illegally. Vigilant energy metering system (VEMS) is an advanced energy metering system that can fight against electricity theft. It has the ability to collect, transfer and process data between other energy meters, local station and base station. It also identifies probable locations of theft and helps the utility companies to control theft. A remote billing system can also be developed modifying this model.

Illegal consumption of electricity can be detected using a remote check meter based on the amount of losses and the time stamp of the check meter. This method is implemented before inspecting the illegal consumers personally by the vigilance officials, based on the data at proper frequency of the consumer measurements.

Analysis of Losses in Power Systems: Losses incurred in electrical power systems have two components:
• Technical losses and
• Non-technical losses (Commercial losses)
Technical Losses-Technical losses will always arise as the physics of electricity transport means that, no power system

can be perfect in its delivery of energy to the end customer. The instantaneous power loss Plot (t) in a transmission line can be expressed as:

P (t) P (t) P (t) loss source load = − 1

Where P source (t) is the instantaneous power that the source injects into the transmission line and P load (t) is the instantaneous power consumed by the load at the other end of the Non-Technical Losses (Commercial Losses)-Losses incurred by equipment breakdown are quite rare. These include losses from equipment struck by lightning, equipment damaged by time and neglect. Most power companies do not allow equipment to breakdown in such a way and virtually all companies maintain some form of maintenance policies. Other probable causes of commercial losses are:

- Non-payment of bills by customers
- Errors in technical losses computation
- Errors in accounting and record keeping that distort technical information.
- Inaccurate or missing inventories of data on customers.

VII. CONCLUSION

This paper defines electricity theft in social, economic, regional, political, infrastructural, literacy, criminal and corruption points of view. This paper illustrates various cases, issues and setbacks in the design, development, deployment, operation, and maintenance of electricity theft controlling devices. In addition, various factors that influence people to steal electricity are discussed. We by this design would like to conclude that the power theft can be effectively curbed by detecting where the power theft occurs inform the authorities. Also an automatic circuit breaker may be integrated to the unit so as to remotely cut off the power supply to the house or consumer who tries to indulge in power theft. The ability of our system to inform or send data digitally to a remote station using wireless radio link adds a large amount of possibilities to the way the power supply is controlled by the electricity board. We have come up with is fool proof when it comes to detecting and preventing the power theft as, we have taken into consideration a large number of possibilities in which the power theft may occur and have designed accordingly to prevent it. Thus by the above mentioned design we can successfully and effectively address the problems related to power theft by the consumers, in a completely automated, wire-free, cost effective and most importantly a reliable way.

REFERENCES

[1] A. R. Devidas, M. V. Ramesh, "Wireless Smart Grid Design for Monitoring and Optimizing Electric Transmission in India," IEEE 2010 Fourth International Conference on Sensor Technologies and Applications

[2] "Electrical Power Supply System for India," www.wikipedia.org, February 2010

[3] "Smart Grid," www.wikipedia.org

[4] "National Electricity Policy," The Gazette of India, EXTRAORDINARY PART I - Section 1, Ministry of Power, New Delhi, Dated the 12th, February, 2005, RESOLUTION No. 23/40/2004-R&R (Vol.II)

[5] "Electricity Crisis in India," www.ElectriciyInIndia.com

[6] Yang Junjie, Lv Jian, Wei Chunjuan "A Wireless Solution for Substation Perimeter Safety Monitoring System Based on ZigBee Communication Technology," 2010 International Conference On Computer Design And Applications (ICCDA 2010).

[7] S. N. Singh, "Electric Power Generation, Transmission and Distribution",2nd ed. Prentice-Hall of India Private Limited,2003.

[8] C.J. Bandim J.E.R. Alves A.V. Pinto F.C. Souza M.R.B. Loureiro C.A. Magalhaes F. Galvez-Durand "Identification of energy theft and tampered meters using a central observer meter: a mathematical approach" Proceedings of IEEE PES Transmission and Distribution Conference and Exposition. vol. 1 pp. 163-168 Sept. 2003.

TRANSMISSION IMPAIRMENTS

Most of the transmission technologies in Wireless Sensor Network are RF based. A lot of radio-transmission engineering has to do with how to deal with the noise problem; the goal is nearly always to optimize the signal-to-noise ratio, subject to specified constraints (e.g., bandwidth requirements, cost, reliability, power consumption, equipment and antenna size).[4] Signal strength fluctuations caused by the fact that the composite signal received comprises a number of components from the various sources of reflection from different directions as well as scattered and/or diffracted signal components affect both mobile and stationary receivers. Care is needed when placing sensors in order to minimize interference. One needs to keep WNs away from other sources of radio-frequency interference (RFI), Interference can also be caused by other legitimate or illegitimate users of a given frequency band. However, the benefits of a wireless solution are undeniable: lower installation and maintenance costs, increased flexibility, a broader set of addressable applications, and the freedom to take measurements almost anywhere phenomena like reflection, Diffraction, Scattering because radio signal distortions and signal fading.

CHALLENGES WITH WIRELESS SENSOR NETWORK APPLICATION

The main application areas for WSNs are categorized according to the type of Information measured or carried by the network. Applications, on top of the stack, set requirements that drive the selection of protocols and

transmission techniques; at the other end, the wireless channel poses constraints to the communication capabilities and performance. Based on the requirements set by applications and the constraints posed by the wireless channel, the communication protocols and techniques are selected.

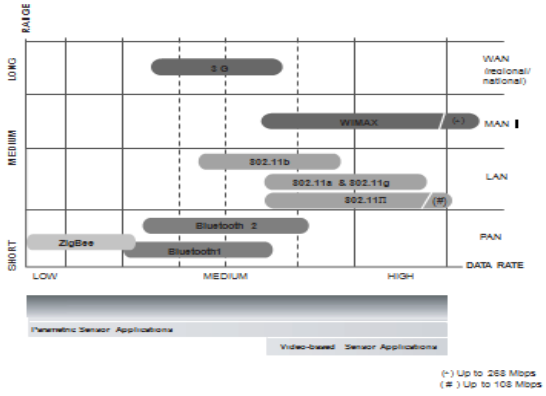
Though wireless nature of WSNs has many advantages over wired network, it also includes some challenges when it comes to implementation or selecting the transmission technology.

- Security is the major concern in WSNs; it is easy for hackers to hack the network. We have to select the networking technology as well as security algorithm accordingly.
- Due to limited resources and dynamic topology, it is very difficult to design a reliable routing scheme for WSNs.
- In some application the sensors may be placed in harsh environment. Before designing the network or selecting the transmission technologies, the crucial environment conditions must be considered.
- Energy constraint is yet another crucial factor in Wireless Sensor Network because the sensor nodes have small battery size. To conserve energy, traffic scheduling and optimization of power consumption should be done.

DIFFERENT TRANASMISSION TECHNOLOGIES

As large number of WSN applications use battery operated nodes, WPANs are used more often in Wireless Sensor Networks. Wireless Sensor Network is highly application specific in nature. Wireless communication in Wireless Sensor Networks is mostly based on standardized technologies around 802.11 and 802.15 standard families, also known as Wireless Local Area Networks (WLAN) and Wireless Personal Area Networks (WPAN) respectively. WLAN offers higher throughput & range at the cost of higher energy utilization compared to WPAN. As large number of WSN applications use battery operated nodes, WPANs are used more often in Wireless Sensor Networks. Let's compare transmission capabilities, energy budget & geo-location accuracy for some of the prevailing technologies.

Figure.1 Different Transmission Technologies



A). BLUETOOTH: Bluetooth wireless technology is a short-range communication system intended to replace the cables in WPANs. The key features of Bluetooth wireless technology are robustness, low power, and low cost. The technology has restricted performance characteristics by design; hence, its applicability to WSN is rather limited in most cases. The Bluetooth specification defines a low-power, low-cost technology that provides a standardized platform for eliminating cables between mobile devices and facilitating connections between products. Bluetooth 4.0 is designed to be more intelligent (hence: Bluetooth Smart) about managing those connections, especially when it comes to conserving energy.[1] The new generation of Bluetooth technology places less emphasis on maintaining a constant stream of information. Instead, it focuses on sending smaller bits of data when needed and then puts the connection to sleep during periods of non-use. IEEE 802.15.1 standard, popularly known as Bluetooth, offers moderate data rates at lower energy levels. Due to this, it is ideally suited for high end WSN applications that require higher data rates with harder real time constraints. Bluetooth is used in star topology because of its basic characteristics. Bluetooth devices communicate with each other using set of standard Bluetooth profiles defined by standard body.

B). Wi-Fi: Wi-Fi represents group of WLAN technologies defined under IEEE 802.11 standard body. In addition to transmission standards like 802.11a/b/g/n, it also includes 802.11s standard for mesh networking. Wi-Fi technologies are capable of providing very high throughput (>100 Mbps) at longer range but required very high power budget. Also, Wi-Fi can locate end point location to the accuracy of several meters only. Because of this limitation, use of Wi-Fi is mostly restricted to devices with fixed power supply. It operates in unlicensed 2.4 GHz radio spectrum use Direct Sequence Spread Spectrum for modulation (DSSS), and has a range of about 50 meters default and it can be increased. . WNs typically transmit small volumes of simple data. For within-building applications, designers ruled out Wi-Fi (wireless fidelity, IEEE 802.11b) standards for sensors as being too complex and supporting more bandwidth than is actually needed for typical sensors.

C).Wi-Max: Wi-MAX is a Wireless Man technology. Wi-MAX comes under Broadband Wireless Access and is based on IEEE 802.16 standard. It operates on both licensed and unlicensed band less than 6 GHz. seeking to deploy high-performing, cost-effective broadband wireless networks

WiMAX provides two to four times the performance of 3G solutions today, with the ability to scale to ten times the performance in the future. WiMAX is more scalable than many other wireless technologies. It has two mandatory encryption modes which makes it more secure in its simple form. WiMAX has a better flexibility than Wi-Fi as it does

not need Line-of-Sight with the base station.

D). 3G: 3G enables increased data handling rates and high speed bandwidth; It ranges from 144 kbps to 2.4 Mbps. Implementation of 3G may be expensive for some applications. 3G systems have fixed bandwidth unlike WiMAX which can have variable bandwidth. These systems have higher complexities due to addition of multiple antenna support.

E).UWB: Ultra wide band is a technology for transmitting information spread over a large bandwidth (>500 MHz) and it is ideally suited for short distance, high speed communications with very low power budget. As it is based on wide band technology, it can achieve very high geo-location accuracy to the sub-meter levels. UWB provides one of the best options for WSN networking only limited by its shorter range. It is a short range high speed wireless technology nearly 10 times faster than 802.11b. UWB is designed to replace cables with short range, wireless connection but it offers the much higher bandwidth. UWB does not use an RF carrier. Thus it provides global interoperability. It uses frequency from 3.1 GHz to 10.6 GHz. Because of the low power requirement it is feasible to be used in wireless sensor network. With the characteristics of low power, low cost and very high data rates at limited range it is positioned to be better than high speed WPAN.

F). Zigbee: IEEE 802.15.4 wireless technology is a short range communication system intended to provide application with realized throughput and latency requirements in WPAN. ZigBee offers low complexity, low cost, low data rates at very low energy levels. Due to this, it is ideally suited for applications requiring infrequent smaller data transfers where battery life is an important issue[3]. This technology allows to basic topologies: star topology and peer to peer topology.
Star topology preferable in case coverage area is small and low latency is required by the application. In latter, the area covered should be large and latency is not a critical issue.
G). 6LowPAN: 6LowPAN is an open standard in order to use IPv6 over 802.15.4. 6LowPAN stands for IPv6 over Low-Power WPANs. It is a protocol definition describing how to utilize IPv6on top of low power, low data rate, low cost personal area network.[3]

The fundamental difference between 6LowPan and Zigbee is the IP interoperability of the first. For an application in which there is no need to interface with IP devices or the packet size is small, it is not necessary to implement 6LowPAN, which performs fragmentation.

S. No	Technology	Area covered	Power consumption	Interference resilience	Complexity and cost	Data rate	Application
1.	Bluetooth	~100 meters	High	High	High	Bluetooth: V1.2 = 1Mbit/s V2.0 = 3Mbit/s	Health monitoring, environmental monitoring and security
2.	Wi-Fi	Long up to 100 meters	500mW-1W	Medium	High	High, 11 Mbps for 802.11b ,100+Mbps for 802.11n	Generally used in LAN systems
3.	WiMAX	radius of **30 miles** (50 km)	500mW-1W	Medium	Very High	30-40 Mbits/s	Residential users in a colony or society
4.	Zigbee	Short, <30 meters	Low, 20 mW-40mW	Low	Low	Low, 250 kbps	Medical care application, Fire emergency
5.	UWB	Short, <3o meters	Low, 30mW	High with high complexity receivers, low with simple	Low, medium, high all are possible	Medium, 1Mbits/s mandatory	Hospital locating, tracking in communication system

Table.1 Comparesion of Different Technology

CONCLUSION

The aim of this article is to discuss some of the most relevant issues of WSNs, from the application, design and technology viewpoints. For designing a practical WSN solution, we need to select right technology with necessary customization. We have still not touched upon the challenges of designing miniature, low-power, accurate sensor systems for various measurements. In summary, WSN offers some of the revolutionary applications for consumers & industry but its design & implementation needs to be carried out. Cellular and WAN standards such as GPRS, WiMAX, and EDGE provide significant throughput and range, but these standards consume a significant amount of power, making them unfit as the communication protocol for long-term, and battery-powered deployments such as wireless sensor networks.
Conversely, the Bluetooth protocol requires very little power, but does not provide adequate range for WSN systems in which communication distance requirements can be upwards of 100 to 500 meters. . For designing a practical WSN solution, we need to select right technology with necessary customization. For within-building applications, designers ruled out Wi-Fi standards for sensors as being too complex and supporting more bandwidth than is actually needed for typical sensors. WiMAX provides superior throughput and spectral efficiency compared to 3G and Wi-Fi.

REFERENCES

[1] Chiara Buratti , Andrea Conti, Davide Dardari and Roberto Verdone, " An Overview on Wireless Sensor Network Technology and Evolution" vol 9, no 9, pp. 6869-6896.
[2] Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications" 1st ed., John Wiley and Sons, 2007.
[3] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," IEEE Wireless Commun., vol. 12, no. 1, pp. 12-16,

Feb. 2005.

[4] Baker, N. "ZigBee and Bluetooth: Strengths and weaknesses for industrial applications," IEE Computing & Control Engineering, vol. 16, no. 2, pp 20-25, April/May 2005

[5] J. S. Lee and Y. C. Huang, "ITRI ZBnode: A ZigBee/IEEE 802.15.4 platform for wireless sensor networks," in Proc. IEEE Int. Conf. Systems, Man & Cybernetics, Taipei, Taiwan, Oct. 2006, pp. 1462-1467.

[6] P. S. Neelakanta and H. Dighe, "Robust factory wireless communications: A performance appraisal of the Bluetooth and the ZigBee collocated on an industrial floor," in Proc. IEEE Int. Conf. Ind. Electron. (IECON'03), Roanoke, VA, Nov. 2003, pp. 2381-2386.

