International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Smart Security Management for Zigbee GPRS Protocol Using IoT Gateway

Dr. M. Newlin Rajkumar, K. Karthigeyan
Anna University Regional Campus, Coimbatore, Tamil Nadu, India

ABSTRACT

One pathway through which present day energy issues can be labelled through the minimization of energy usage in households. The actual service system only provides criticism at end of the month in form of a bill and consumed kilowatt hours (kWh). A landlord has contradiction to track their power usage on a more immediate basis. The Arduino based wireless power meter is a non-interfering current meter for household power with a Matlab interface. Current is measured using split core current transformers. This data is then transmitted over an 802.11b connection through the home's wireless router to the base station and Matlab interface. The project aims to furnish a fair picture of a home's existent usage, and through this data provide an estimate to power consumption. The project also aims to analyse which appliances turn on and off by analysis of this current data. The goal of provided such data to a user is that they will optimize and reduce their power usage.

Keywords : IoT, Zigbee, GSM, Sensors, M2M, WSN

I. INTRODUCTION

The Internet of things (IoT) is internetworking of phenomenal devices, fabrication and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "infrastructure of information society." The IoT allows gadget to be anticipated and organized remotely across physical network framework, creating occasion for more assimilation of the physical world into computer-based systems, and resulting in enhanced efficiency, accuracy and economic benefit. When IoT is develop with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also besets technologies such as smart grids, smart homes, intelligent transportation and smart cities.

IoT wants to connect all possible objects to collaborate each other on internet to provide security and satisfaction life for human. Internet of Things (IoT) makes the world as desirable as linked together. Embedded computing devices would be discovered to internet impact.

Common examples for embedded computing devices are MP3 players, MRI, traffic lights, microwave ovens, washing machines and dishwashers, GPS even heart monitoring implants or biochip and etc. IoT tries to authorize advanced integration among these suggested device or systems or services in order to little by little makes automation in all areas. Image that all thing is connected together and all data information would be collaborated with each other over standard orthodox and different protocol domain and applications.

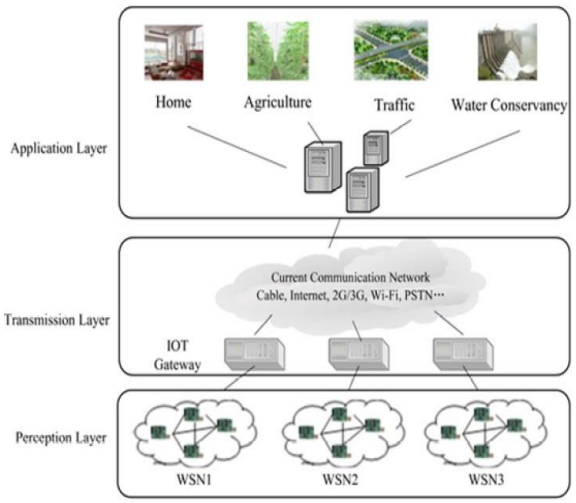

Figure 1. Typical IoT Applications

The IOT Gateway is a key component in IOT application systems, which is working as a bridge

between telecommunication network or Internet and the WSN. A prototyping implementation of IOT Gateway based on Zigbee-GPRS protocols, which realizes data forwarding, protocol transformation, WSN management and control. It has the problem of not using advanced functions of IOT Gateway including fault handling and security management.

The objective of our work is to investigate how to measure and control the voltage and current through Web and Android Application. we have designed and implemented a GSM Module which provides information and we can find the details like Current and Voltage Measurement given to the database of the web server and the output is parsed to the android application.

II. RELATED WORKS

Major sanctioning factor of this promising standard is the integration of several technologies and communications solutions. Identification and tracking technologies, enhanced conversation protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most common. One can simply imagine, any serious contribution to advance of Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge like telecommunications, informatics and electronics.

In such complicated scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Various views of Internet of Things patterns are described and enabling technologies reviewed. What appear is that still extensive issues shall be faced by the research community.

In “Internet of Things" the existing world becomes centralizing with computer networks. Embedded computers or optic beacons on everyday items that allows things and information about them to be handles by software in implicit world. However, this assimilation is based on competing standards or hacks and thus requires technical expertise and is time consuming. Subsequent long end of Web 2.0 mashups operations, proposed an identical access for blending real-world devices to web, granting for them to be easily connected with other virtual and physical assets and discuss possible integration approaches, in particular how we apply REST principles to wireless sensor networks and bold gadgets. Finally, demonstrate how these two implementations can used to quickly create new prototypes in a mashup manner. n this paper we have contribute to a step towards the realization of the Web of Things. By creating RESTful APIs to integrate the services afforded by devices and objects in actual world alike wireless sensor networks, embedded devices and household appliances with any other Web con- tent. We have described two ways to integrate devices to the Web using REST, a direct integration based on the advances in embedded computing and a Smart Gateway-based approach for resource-limited devices. We have further illustrated these methodologies by implementing them on two different platforms.

As a new high technology, Internet of Things (IOT) technology has been obtaining great development and becomes more and more popular; meanwhile it is widely used in all industries. Moreover, with the current technologies and economic development having made remarkable achievements the environment of human beings is going from bad to worse. IOT technology provides ideas and technology feasibility for environmental protection. Based on the requirements of the present monitoring project of energy-saving section in industry, in this paper, firstly, we present the development of IOT in recent years then analyses the basic concept and key technologies of IOT and present an integral investigation on IOT in environment protection, in addition, analyze and summarize the network structure and the current application situation. Although IOT is the great breakthrough in information technology development, there still have many deficiencies. Finally, we discuss the advantages of IOT in environment protection and challenges IOT is facing and future work for environment protection of IOT. Machine to Machine (M2M) communication services are already showing strong revenue growth with the number of deployments steadily increasing. Large-scale handles M2M services will become a feature of industry, but today the technology landscape is fragmented, which discourages investment.

The ETSI M2M Release 1 paradigm enable assimilation of various M2M technology options into one managed platform. ETSI M2M Release 1 is built

upon proven and mature standards from ETSI and other bodies such as the IETF, 3GPP, the Open Mobile Alliance and the Broadband Forum. The business profits are clear: shortened complication of M2M deployments, shortened deployment time for new M2M services, and ultimately reduced CAPEX and OPEX. The ETSI M2M standards indicates architectural factors combining M2M accessories, gateways with associated interfaces, applications, access technologies as well as the M2M Service Capabilities Layer. They also endeavor security, traffic arranging, device detection and lifecycle management aspects. The ETSI M2M Release 1 standards are presented as set of three particularization which are available for download from website.

Auto-ID is poised to be the next big wave to hit the supply chain. Emerging from the research and development of bar codes, bar code readers, and universal product codes, the tagging of items for sale has been used in the retail industry since the 1950s. A new development is Auto-ID, or radio frequency identification tags (RFIDs) embedded as a chip in each item a manufacturer produces. Incorporating a 96-bit electronic product code, the chip is affixed to each physical object. The numbering scheme means the tags can be used to uniquely identify more than one hundred million manufacturers, along with one million of their products, yet leave enough numbers for items to be produced and tagged in the future. Antennas enable the chips to communicate wirelessly with radio frequency readers. The readers trace where a particular item is in the supply chain.

The manufacturer can place wireless readers strategically along the supply chain, so the unique Auto-ID is transmitted to the Internet (where more detailed information about the product can be stored) and communicated to manufacturers, distributors, retailers, and even third-party logistics providers, on demand. The only way to address the problems challenging implementation of Auto-ID technology is through a more inclusive collaborative partnership among the various players in the supply chain. The Auto-ID Center, formed by a consortium of 88 companies and academic institutions, is a positive step in this direction.

III. EXISTING SYSTEM

In Existing System, proposed an IOT Gateway system based on Zigbee and GPRS protocols according to the typical IOT application scenarios and requirements from telecom operators and presented the data transmission between wireless sensor networks and mobile communication networks, protocol conversion of different sensor network protocols and control functionalities for sensor networks and finally gave an execution of prototyping system and system validation.

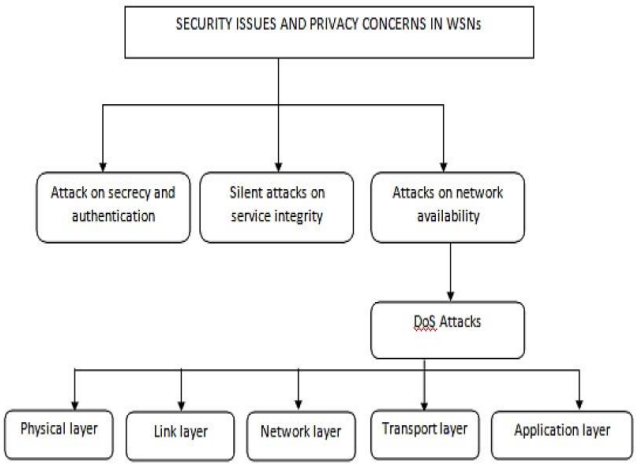

Figure 2. Security in WSN

IOT Gateway is in the middle layer between sensor node and application platform, it not only receives sensed data from sensor node and commands from application platform, but also transmits data to application platform. GPRS Interaction module and Ethernet Interaction module are deployed in gateway to exchange data with application platform. Serial Transceiver module is deployed to exchange data with sink node. the main functions of the gateway are to read data from serial port, write data to the serial port and forward sensed data. Our design provides two modes of interaction with the remote server: GPRS Interaction and Ethernet Interaction. The former one starts GPRS module by sending AT commands, which also sets the serial communication speed to establish socket connection for data transmission. The latter one establishes the socket connection by setting the remote server's IP address and listening port. Both of them provide a unified interface, so the main program selects one of them to start easily.

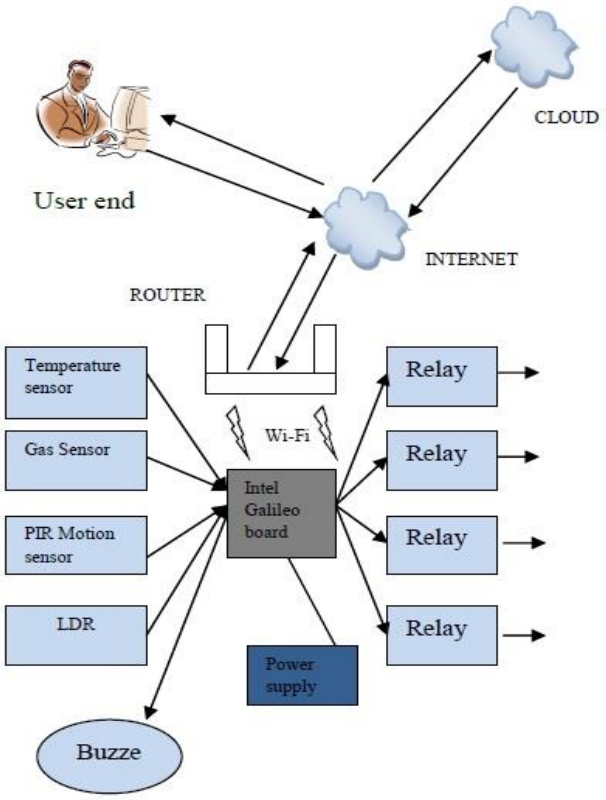

Figure 3. IoT Model of Home Appliances Control System

After all the modules initialized, IOT Gateway starts with port listening and waiting for external events interruption. Once the interruption events are detected, the main program determines the appropriate response by checking the type of data. If the data is received from remote server which means that the data is a command, the main program analyzes the command and sends it to the WSN. If the command asks for reporting the gateway information or gateway log to server, the main program calls the remote server interaction module's interface to send logging and configuration data to the remote server. If the command is target with the sensor nodes, the main program analyzes the command by calling the protocol analysis module's interface, and then calls serial data transceiver's interface to send information to the sink sensor. If the data is received from WSN, the main program analyzes the data by calling protocol analysis module, and then calls the remote server interaction module to send sensed data to the remote server.

IV. GATEWAY SYSTEM

In proposed system, current and voltage of single phase ac loads measured by current and voltage sensors. In order to measure the power consumed in each appliance, current should be monitored. To serve this purpose Electricity module based on the current transformer that has capability to change large alternating current into small amplitude. This sensor can measure alternating current up to 5A.

Description	Arduino pin	ATMega328 pin
Slave select (SS)	10	PortB.2
Clock (SCK)	13	PortB.5
Master in, Slave out (MISO)	12	PortB.4
Master out, slave in (MOSI)	11	PortB.3
MCU interrupt	2	PortD.2
LED connection light	9	PortB.1

Table 1. WiShield connections to Arduino

Zigbee network communicates between local area, ZigBee is a mesh network appropriation for low-power wireless local area networks that covered a broad area. It is used in industrial autonetics and physical plant operation, it is generally related with machine-to-machine (M2M) communication and Internet of Things(IoT).

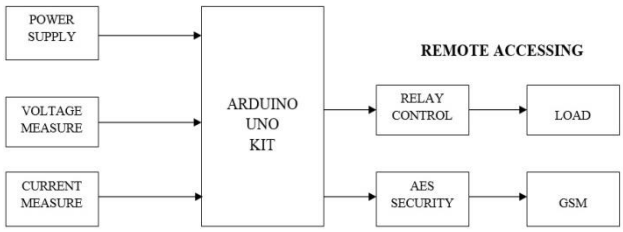

Figure 4. Overview of Architecture

Arduino used for monitoring and controlling of single phase ac loads, the average energy consumption of the appliances is reduced since they are turned off when unused, the energy consumption hourly monitor and control the system. Parameters such as the temperature, humidity etc., has to be monitored and the required electronic devices has to be controlled. All the sensors which is used to be first connected to ZigBee routers and the identical codes for the sensor to sense the data are dumped into the microcontroller.

For remote monitoring design uses android application, scheme is drafted to control the large or complex accessible such as factories, power plants, network operations centers, airports, and spacecraft, with some degree of automation. M&C scheme receive data information from sensors, formal streams, user inputs, and pre-programmed procedures.

V. CONCLUSION AND FUTURE ENHANCEMENT

The system will be successful in measuring the current within tolerable range of error, and sending that message at a higher update rate than previous similar projects have done. Moving time high floating point calculations off Arduino and achieving them on base station supported to stimulate execution time, but difficulties with plotting data and receiving the packets on the base station side lowered performance.

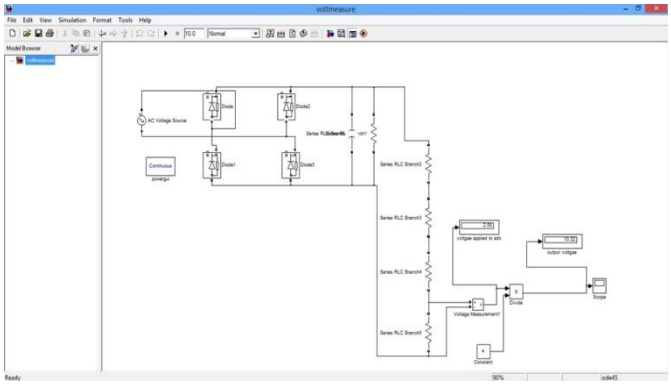

Figure 5. MATLAB Output Simulation

The device detection feature may still realize if update rate could be recovered from the lost packet issue, but more likely a detailed analysis of shape of waveform would be needed to do such turn on and turn off detection. Parameters like harmonics, distortion of waveform for both current and voltage would be useful in identifying which devices are running.

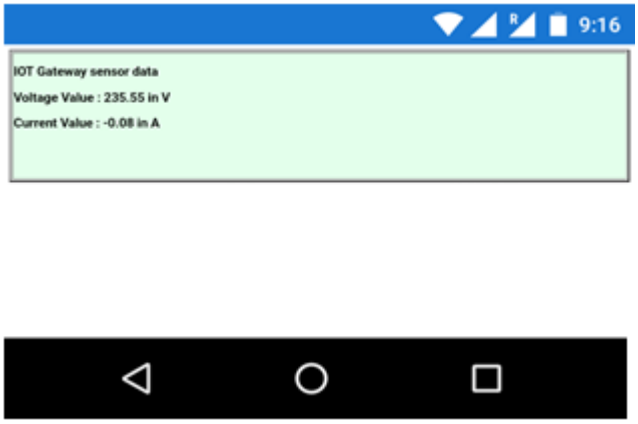

Figure 6. Output of Android Application

The project has valuable experience in the design, implementation and testing of a system that involved several discrete hardware and software components. The use of an open source project for such a central function like IP stack in the project was initially planned to be a large drain in design time, but ended up greatly accelerating the design of the wireless part of embedded system. Moreover, available for the current measurement circuit, which was able to go through several designs before an acceptable one was reached.

VI. REFERENCES

[1]. L. Atzori, A. Iera and G. Morabito," The Internet of Things: A Survey", Computer Networks, Vol. 54, No. 15, pp. 2787-2805, Oct. 2010

[2]. I. Bose and R. Pal," Auto-ID: managing anything, anywhere, anytime in the supply chain", Communications of the ACM, Vol. 48, No. 8, pp. 100-106, Aug. 2005.

[3]. ITU," ITU Internet Reports 2005: The Internet of Things", The Internet of Things, Nov. 2005.

[4]. Q. Liu, L. Cui, HM. Chen," Key technologies and applications of Internet of Things", Computer Science, Vol. 37, No. 6, 2010.

[5]. ETSI M2M Standardization, http://www.eti.org/Website/Technologies/M2M.aspx

[6]. H. Jin, WC. Liu, JT. Han and YL Ding," Application Study of Internet of Things in Home", Telecommunications Science, Vol. 26, No. 2, 2010.

[7]. D. Guinard and V. Trifa," Towards the Web of Things: Web Mashups for Embedded Devices", in 2nd Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), Madrid, Spain, April 2009.

[8]. Nagarajapandian M, Ram Prasanth U, Selva Kumar G, Tamil Selvan S, Automatic irrigation system on sensing soil moisture content, International journal of innovative research in electrical, electronics, instrumentation and control engineering vol. 3, Issue 1, January 2015.

[9]. Surabhi Singh, Neetika, Satish Kumar, Automated Agriculture Monitoring using ZigBee in Wireless Sensor Network-A Review, International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161 ©2016 INPRESSCO.