[International Journal of Instrumentation Control and Automation](https://www.interscience.in/ijica)

Volume 1 | Issue 3 Article 11

October 2011

Authentication and Centralized Control of Electrical Devices Using Zigbee Protocol

Abhishek. M. B.
Dept of E & C, DSCE, Bangalore, Karnataka, India, abhishek.mb@gmail.com

Sreenivasan. A
Dept of E & C, DSCE, Bangalore, Karnataka, India, dr_asreenivasan@yahoo.com

Sairam Kummara
Honeywell, Bangalore, Karnataka, India, Sairam.kummara@honeywell.com

Authentication and Centralized Control of Electrical Devices Using Zigbee Protocol

Abhishek. M. B.[1], Sreenivasan.A[2] & Sairam Kummara[3]

[1&2]Dept of E & C, DSCE, Bangalore, Karnataka, India
[3]Honeywell, Bangalore, Karnataka, India
E-mail : abhishek.mb@gmail.com[1], dr_asreenivasan@yahoo.com[2], Sairam.kummara@honeywell.com[3]

Abstract - In buildings, lighting accounts for more total energy cost, reducing this energy consumption is a major goal of this project. Energy reduction comes from turning off lights when they are not needed, optimizing light levels to suit worker needs. Through the use of modern enterprise-class wireless networking technology, the difficulty of control wiring is eliminated. In this project, the analysis, design and implementation of an intelligent office room whose two main components are realized using two emergent wireless technologies, namely, wireless sensor networks (ZigBee) and Radio-frequency identification (RFID) tags. The combination of these two technologies produces a powerful and versatile solution that can offer automated access control to an office room as well as the monitoring of entry or exit of an employee and also to perform automated job as described in the profile.

I. INTRODUCTION

Most buildings posses a Building Automation System (BAS) with the required functionality for monitoring, controlling and managing number of subsystems. The management of crucial building resources such as power, room lighting, air conditioning, and communications are few typical services offered by a BAS. Legacy BAS consisted of an unsorted collection of pneumatic and electromechanical devices. BAS were evolving towards automatized control systems with connections to digital network, with the advent of modern and cheap microcontrollers and microprocessors. Nowadays BAS can be seen as a sophisticated distributed system, where the different modules are usually interconnected via wired or wireless internet and/or intranets to front-end computers and human interface devices.

Majority of BAS networks consist of a main bus that interconnects high-level controllers with lower-level controllers. Specialized processors such as Programmable Logic Controllers (PLCs), or even, in some cases, independent work stations are used. Partially because of the fact that in the recent past different BAS vendors experienced several compatibility problems due to modern BAS communication protocol standards for a wide range of products. BACNet, LonWorks, Modbus are among the important BAS protocols that can be used. Due to various legacy and compatibility issues, the BAS protocol standardization process can be still considered as an on-going process. This kind of systems was designed using wired-connection architecture. The aforementioned feature may be due to historical reasons as well as an effort to attain a better level of robustness in the system. Nevertheless, the ever increasing number of control devices and monitoring systems has more often than not created bottleneck problems for the correct and timely upgrading and maintenance of the BAS. When the peripheral devices are physically outside of the control device, the associated cabling brings a number of practical problems such as, installation cost, security vulnerabilities, lack of scalability, and lesser feasibility, among others.

The most applicable solution for the above mentioned drawbacks is to install a wireless technology though the solution implies a whole new set of challenges like: feeble signal propagation and signal interference, wireless security vulnerabilities, frequency spectrum regulations, etc. The technology to overcome the challenges is available which might turn out to be expensive due to the associated extra complexity of a wireless system.

It can be possible to afford the costs of adding a high-end wireless communication system that includes in its architecture costly elements like cell phones, wireless LANs, etc under certain circumstances. On the other hand and in the other side of the spectrum, some applications can improve their cost-benefit tradeoff if a low-cost wireless communication solution is put in place. The high scalability of a wireless BAS architecture is a remarkable advantage of a wireless solutions which contrasts with the fixed size present in the majority of wired BAS solutions.

The main intention of the emerging wireless technology is the automatic identification of objects or users using Radio Frequency Identification (RFID). Exchange of data via radio frequency signal communication is allowed by the system nodes or tags is allowed by this technology. After receiving a radio signal, the tags process this information in order to answer back the basic data required for identifying the tag uniquely. Alternatively, the identification protocol can be as complex as a series of challenge-response messages coded through some cipher algorithm. This data is processed in the reader side with the help of software tools such as an auxiliary database or some other communication system. Object and good authentication, access control for vehicles and humans, race timing, animal identification, product tracking and inventory systems, etc are some of the most popular applications of the RFID technology.

The paramount aspect for any distributed system is security and privacy. But in the case of wirelessly connected networks, the challenge associated to these two issues is more difficult to cope with the dynamics, spontaneity, heterogeneity and the sort of invisible nature associated to this platform . An additional problem is that the RFID devices do not have enough computing power to execute customary cryptographic algorithms traditionally used in client-server transactions.

Data security plays a major role in the system functionality in order to enforce access control, user and node authentication, data integrity, among other security services. These security services avoid common attacks such as eavesdropping and impersonation that can one way or the other compromise the network resources.

Unfortunately, the RFID technology has frequently been used in a wide variety of areas with little or no-consideration at all of the security vulnerabilities.

The project aims to design and implement an intelligent office room, whose two main components are realized using two emergent wireless technologies, namely, wireless sensor networks (ZIGBEE) and Radio-frequency identification (RFID) tags.

The rest of this paper is organized as follows. In Section II we briefly describe the two wireless technologies used in this work. Then, in Section III we list the set of design requirements associated to the intelligent room application addressed in this paper. Section IV describes the main modules of the proposed architecture for the realization of the system, whereas Section V presents its actual implementation. Finally we draw some concluding remarks in Section VI.

II. WIRELESS TECHNOLOGIES

In the rest of this Section we briefly describe the two wireless technologies used in this work, namely, RFIDs and wireless sensor networks.

A. RFID

RFID stands for Radio Frequency Identification. RFID is one member in the family of Automatic Identification and Data Capture (AIDC) technologies and is a fast and reliable means of identifying objects.

RFID, Barcode, Smart Card are some of the technologies that are commonly used for identification. Following, various features are presented in Table I to provide the basis of selecting RFID for this research project.

Table 1 : Comparisons of identification technologies

	RFID	Barcode	Smart Card
Line of Sight	Not required (in most cases)	Required	Required (exposed to reader)
Memory	Small	No memory	Large
Cost	Medium	Low	High
Range	Inches to 100's of feet	Inches to feet	Inches
Reusability	Yes	No	Yes
Read rate	Multiple simultaneously	One at a time	One at a time
Security	Medium (Authentication)	Very Low (Coding)	High (Encryption)

The main application of RFIDs is the identification and tracking of products using radio frequency signals for establishing communication among the tags and one or more reader. An RFID system can be viewed as a collection of constrained nodes (known as tags) that can be physically added, an even inserted into the object under observation that can be merchandise, an animal, or a person. Most tags have a reading range of several meters and beyond in the line of sight of the reader.

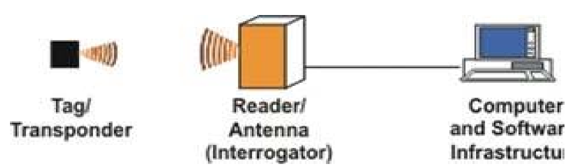

Fig. 1 : Overview of RFID operation

More precisely, an RFID system is composed of the following elements:

- The reader: This element is an electronic device that can read and write several classes of tags. Moreover, in the case that this device is equipped with cryptographic functionality, it can authenticate tags. Commonly, a reader is connected to a host or sometimes it can work as an independent device. If the system includes tags that have writing capabilities, then the reader can store data in the tag memory addresses.

- The Antenna: This device is able to send and receive radio signals. It is composed by a set of conductors especially designed for emitting an electromagnetic field when the device is exposed to the presence of an external electromagnetic field. In fact, if the antenna is close to an electromagnetic field, it generates an electrical current that is physically induced by the so-called Hall effect. The actual size of an antenna directly depends on the wavelength of the received/transmitted radio frequency signal. The antenna size should be a multiple or sub multiple of that wavelength. As a consequence, the higher the frequency is the smaller the antenna.
- Tags: These are the RFID devices that will be incorporated to the product that one wants to identify. There exist three different types of tags: active, passive and semi-active nodes.
    - Passive tags are generally smaller, lighter and less expensive than those that are active and can be applied to objects in harsh environments, are maintenance free and will last for years. These transponders are only activated when within the response range of an RFID Reader. The passive tags do not have any power supply. In fact, the electrical current is induced via the electromagnetic field which is sufficient for the identifier to wake-up and respond to the reader request. The passive tag has a smaller reading range and lesser capability for data storing when compared with an active identifier.
    - Active tags differ in that they incorporate their own power source, where as the tag is a transmitter rather than a reflector of radio frequency signals which enables a broader range of functionality like programmable and read/write capabilities. An active tag is equipped with a battery as its main power supply. This allows for a higher communication range and improved storing capabilities. A battery can last several years in an active device.
    - A semi-active identifier is a device that uses the electrical current induced by the electromagnetic field as a mechanism to wake-up, effectively switching the tag to the ready state. However, it sends messages to the reader by using its batteries as a power supply. This architecture amplifies the distance in which the identifier can be detected. The chief reason for this is that a passive tag can receive energy from a reader even when it stays far away from it, however the energy that receives may not be enough for responding because of that distance. The main idea of semi-active tags is that by adding a supplementary power source the tag is able to send its answer to a wider range of coverage.

Currently, the vast majority of tags are passive ones due to their lower cost and power source independence.

Additionally, the tags can be classified by the operating frequency as shown In Figure 2.

Low Frequency	125-134 Khz
High Frequency	13.56 Mhz
Ultra High Frequency	868-956 Mhz
Microwave	2.45 Ghz

Fig. 2 : RFID tags classification by operating frequency

B. Zigbee

ZigBee is a specification for a suite of communication protocols based on the IEEE 802.15.4-2003 standard, which targets wireless personal area networks. We note that Zigbee operates in the network layer using as a transport layer the services provided by the IEEE 802.15.4-2003 protocol. Actually, the IEEE 802.15.4 defines two physical layers both of them operating in three frequency bands that happen to be free of licenses. The first physical layer works in the 868 to 915 MHz frequency band at a 40kbps transfer rate. This band can be only used in United States, Australia, New Zealand, Israel and Europe. The second physical layer is located at 2.4GHz with a maximum transfer rate of 250 kbps. There are no restrictions for using this band around the world. Additionally, there exists a channel 0 that operates at 868 MHz, with a maximum transfer rate of 20 kbps.

1) Zigbee Device Types: There exist three types of Zigbee devices:

- The Zigbee Coordinator (ZC): This is the most powerful Zigbee device. The coordinator can be seen as the root of the network topology and it can also be utilized as a gateway to other piconets. Sometimes the coordinator is used as a trust entity that can maintain the system’s key repository
- Zigbee Router (ZR): This device can execute a common application and it can work as intermediate router in order to send data to other Zigbee devices
- Zigbee End Device (ZED): This device has a limited functionality such as exchanging

information with the ZC or the ZR device. A ZED cannot forward data to other devices. The main feature of this device is that most of the time it stays in the low-power consumption mode. This allows the saving of significant battery life time. This device requires less amount of memory and is the cheapest Zigbee device.

Table 2: Comparisons of wireless standards

Wireless Parameter	Bluetooth	Wi-Fi	ZigBee
Frequency band	2.4 GHz	2.4 GHz	2.4 GHz
Physical/MAC layers	IEEE 802.15.1	IEEE 802.11b	IEEE 802.15.4
Range	9 m	75 to 90 m	Indoors: up to 30 m Outdoors (line of sight): up to 100 m
Current consumption	60 mA (Tx mode)	400 mA (Tx mode) 20 mA (Standby mode)	25-35 mA (Tx mode) 3 µA (Standby mode)
Raw data rate	1 Mbps	11 Mbps	250 Kbps
Protocol stack size	250 KB	1 MB	32 KB 4 KB (for limited function end devices)
Typical network join time	>3 sec	variable, 1 sec typically	30 ms typically
Interference avoidance method	FHSS (frequency-hopping spread spectrum)	DSSS (direct-sequence spread spectrum)	DSSS (direct-sequence spread spectrum)
Minimum quiet bandwidth required	15 MHz (dynamic)	22 MHz (static)	3 MHz (static)
Maximum number of nodes per network	7	32 per access point	64 K

III. ANALYSIS

In this paper we show the implementation of an intelligent office room using a wireless sensor network and RFID technology. The main design requirements of this project are the following,

- Access control using RFID: An office should be accessible only by authorized people. Unauthorized people should not be able to access to the intelligent space. This feature is typical on applications that involve restricted areas and also to prevent theft.
- Lighting control: In order to make efficient use of energy, we propose the usage of a lighting control according to the reading when an authenticated person enters the room, its ID is matched against its profile and the preset electrical appliances turn ON or vice-versa happens when the person leaves the room. It helps to reduce costs and conserve energy by turning OFF when they are not required.
- High-scalable communications: In general, buildings to be automated may have different layouts, unknown number of rooms and floors and so on. Hence, our solution must be capable of dealing with this kind of characteristics. In order to allow scalability, our proposal must include a routing protocol that can help to add more sensor nodes to the network. In this project uses RS 232 serial communication protocol and wireless network protocol.

IV. DESIGN

This section describes the main modules of the proposed architecture for the realization of an intelligent classroom as shown in Figures 3 & 5. This architecture may be replicated several times within a building, without major modifications.

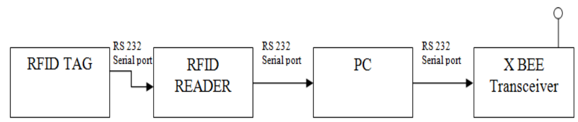

Fig. 3 : Access Control End (Transmitting End)

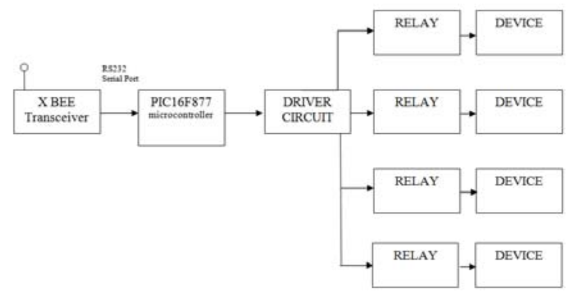

Fig. 4: Lighting Control End (Receiving End)

The main components of the architecture are:

- PC or Embedded system : This element is responsible of processing the data collected by the wireless sensors, identifying tags from the RFID reader and it is in-charge of generating the control signals required for the correct handling of the Driver circuit i.e., When an authenticated person enters the room, its ID is matched against its profile and the preset electrical appliances turn on or vice-versa happens when the person leaves the room. PC displays the person information from the RFID tag.
- RFID reader : performs readings of the RFID tags that must be later sent to the micro controller with the help of XBee transceiver.
- Xbee module : Xbee module acts as a Transceiver which collects data from the RFID reader through RS232 serial port and transmits wirelessly to microcontroller.
- Driver circuit **:** Once person identified has a valid ID, the micro controller sends the signal to driver circuit which performs the room automation job as described in its profile i.e. to turn ON or OFF the electrical appliances.

V. IMPLEMENTATION

The implementation of our intelligent room system is organized according to a four-layer architecture as shown in Figure 5. The following sections describes the contents of each layer.

APPLICATION

SOFTWARE

COMMUNICATION

HARDWARE

Fig. 5 : Implementation

A. Hardware

The components used to implement the system are wireless sensor network and micro controllers

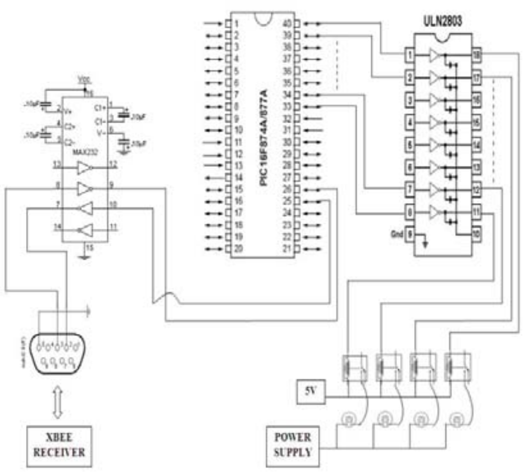

Fig. 6 : Circuit Diagram of Lighting control

Figure 6 shows the circuit diagram of lighting control. In the receiving end the Xbee module receives the information. Xbee module is connected to PIC Microcontroller using RS232 serial port. Since RS232 signals is not compatible with PIC microcontroller signals. So MAX232 is used. The MAX232 is an integrated circuit that converts signals from an RS-232 serial port to signals suitable for use in TTL compatible digital logic circuits. The MAX232 is a dual driver/receiver and typically converts the RX, TX, CTS and RTS signals. From Microcontroller the signal is given to the driver circuit to drive the devices.

B. Communication protocols

A reliable communication between the RFID reader module and any host is established using RS-232 serial communication protocol. The RS-232 serial communication protocol is a standard protocol used in asynchronous serial communication. The Xbee OEM RF Modules interface to a host device through a logic-level asynchronous serial port. Through its serial port, the module can communicate with any logic and voltage compatible UART; or through a level translator to any serial device.

C. Software and Application

The programming languages used for this project are Embedded C, Java and SQL language. Java and SQL are used in ACCESS CONTROL DESIGN and Embedded C is used in LIGHTING CONTROL DESIGN.

SQL (Structured Query Language) is a database computer declarative language designed for managing data in relational database management systems (RDBMS). SQL is used to build a table (A table is a collection of related data entries and it consists of columns and rows) that shows some data from a database, you will need the following:

- An RDBMS database program (i.e. MS Access, SQL Server, MySQL)
- A server-side scripting language, like PHP or ASP
- SQL
- HTML / CSS

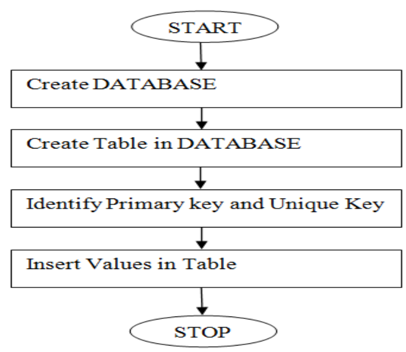

Fig.7 : Flow chart for creating database

Java is a general-purpose, high level, concurrent, class-based, object-oriented language. Here Java program is used to communicate with the database created in SQL and RFID and later transmits the data through ZIGBEE. here 1st we identify the person as authorized person with the help of RFID reader and transmits his information to PC through serial port and later communicate with database and finally transmit through Xbee transmitter to the desired Xbee receiver to perform the automation job as described. The flow chart shows the sequence of execution.

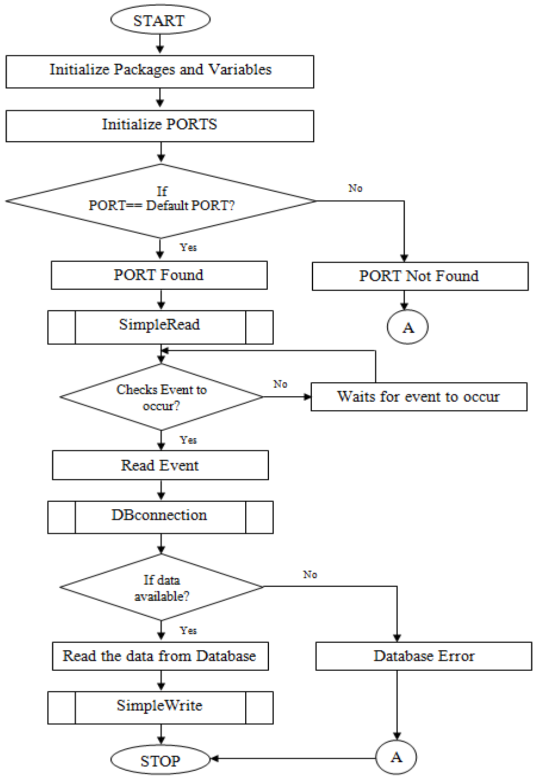

Fig. 8 : Flow chart for Access Control

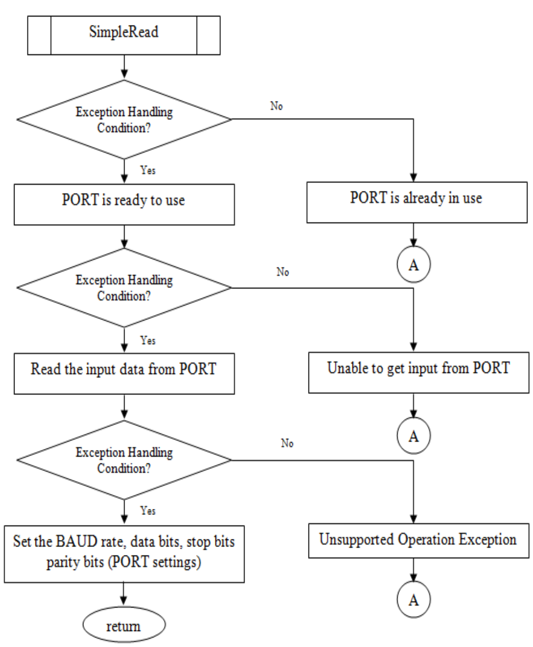

Fig. 9 : Flow chart for class SimpleRead

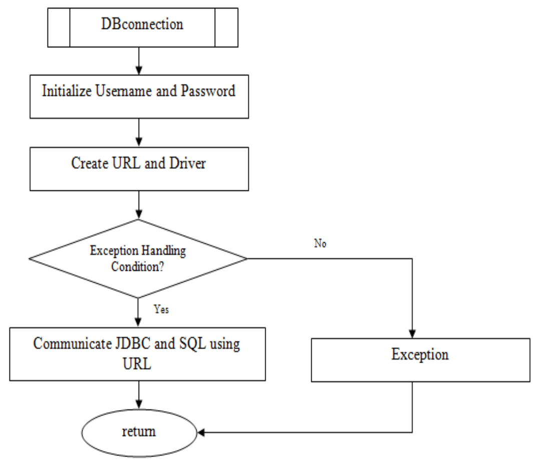

Fig. 10 : Flow chart for DBconnection

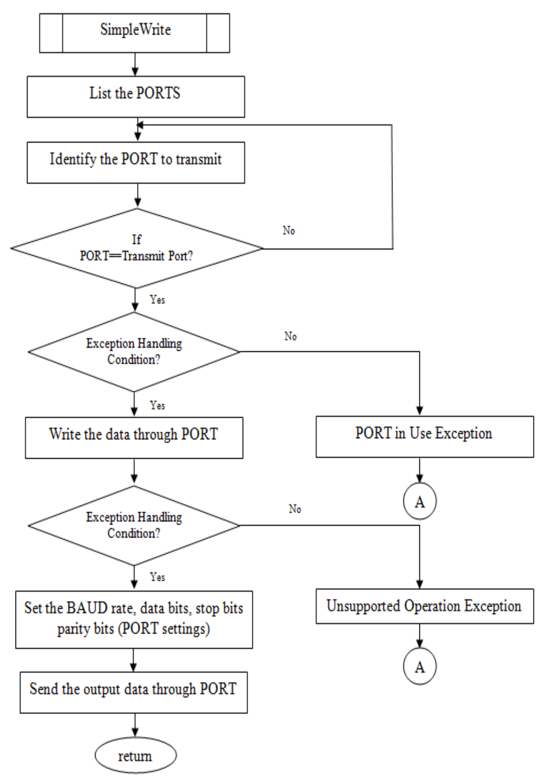

Fig. 11: Flow chart for class SimpleWrite

Embedded C is an extension for the programming language C, to support embedded processors, enabling portable and efficient application programming for embedded systems. Embedded C is written in micro controller and later used to communicate with ZigBee and Driver circuit according to RFID information received to perform the automation job.

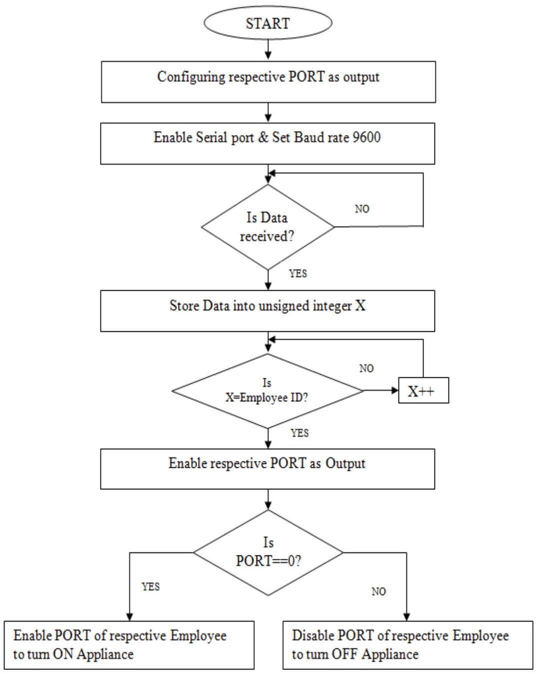

Fig. 12 : Flow chart for PIC Microcontroller

VI. RESULTS

The implementation described in the previous Section was evaluated under a office environment and it works as expected. Other equipment transmitting/ receiving in the same frequency band were operating at the same time (Wi-Fi and Bluetooth) without any sign of interference. The access control module refused entry to unauthorized users, while users with permission were granted access. The RFID reader was able to read tags. The Xbee modules successfully transmit and receive the signals. The micro controller generates signals corresponding to the on/off of lighting and other appliances when the corresponding events occurred.

VII. CONCLUSION

A smart space developed with the use of RFID technology brings numerous advantages and some of them are described in this paper in the context of an office room. The beauty of the developed system is that it provides these features quite inexpensively.

The design details of an intelligent office room that was implemented using two wireless technologies, namely wireless sensor networks and RFID systems. The pilot tests suggest that the architecture proposed in this paper works reasonably fine for controlling one Office room and a set of several interconnected rooms. The system works in tandem with RFID reader boards, ZigBee modules, control circuits and database servers. Facilities like room automation, object tracking, theft control and power conservation are some of the features that can be effectively utilized in any office environment provided by our system. The future work includes the implementation of an improvised version of this architecture and also extend this to all kinds of appliances.

REFERENCES

[1] Daniel Minoli Kazem Sohraby and Taieb Znati. Wireless Sensor Networks - Technology, Protocols and Applications. 1st. Edition, Wiley-Inter science, USA, 2007.

[2] Jose A. Gutierrez, Edgar H. Callaway Jr., and Jr. Raymond L. Barret. Low-Rate Wireless Personal Area Networks – Enabling Wireless Sensors with IEEE 802.15.4. 2nd. Edition, IEEE Press, USA, 2003.

[3] Article - “ZigBee Helps Light the Future” by David Cohen, California Eastern Laboratories Electronic Products – June 01, 2009.

[4] http://www.digi.com/products/wireless- wired-embedded-solutions/zigbee-rf-modules/zigbee-mesh-module/xbee-zb-module.

[5] Dr. Jeremy Landt, “Shrouds of Time: The history of RFID”, White Paper, AIM Inc, October 2001, URL:http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf (Accessed on 1st July, 2008).

[6] Aqeel-ur-Rehman, Abu Zafar Abbasi, Zubair A. Shaikh “Building A Smart University using RFID Technology” Department of Computer Science National University of Computer and Emerging Sciences (FAST-NU) Karachi, Pakistan-2008 International Conference on Computer Science and Software Engineering.

[7] http://ww1.microchip.com/downloads/en/devicedoc/39582b.pdf

[8] Ivan Cabrera Altamirano and Francisco Rodrıguez Henrıquez “A Scalable Intelligent Room Based on Wireless Sensor Networks and RFIDs” Department of Computer Science- 2010 7th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2010) Tuxtla Gutiérrez, Chiapas, México. September 8-10, 2010.