International Journal of Innovative Research in Electronics and Communications (IJIREC)
Volume 1, Issue 6, September 2014, PP 11-19
ISSN 2349-4042 (Print) & ISSN 2349-4050 (Online)
www.arcjournals.org

Realization of Smart Campus Security System Using Wireless Technology

Darakshan Ansari[#1], Vidya Gogate [#2]

[#]M. H. Saboo Siddik Polytechnic, Mumbai
[1]*darakshan.javed.2012@gmail.com*
[2]*vidyagogate68@gmail.com*

Abstract: *In recent days, no. of valuables owned by numerous professionals, VIP delegates and business class people (or any region of services) are increasing, valuables such as laptops, smart phones etc. Due to which theft becomes more clever& hidden. To mitigate this problem, we propose a smart campus security system based on RFID &Zigbee, which provides an effective protection on campus. RFID (radio frequency identification), reads significant data of the identity card which includes personal identity, valuables identification through radio frequency signals using advance network.*

Keywords*: FID, ZigBee, PIC, Microcontroller, TPM, SPI.*

1. INTRODUCTION

Currently there are various wireless technologies available, for instance Bluetooth, infrared (IR), Zigbee, radio frequency identification (RFID) etc. Radio frequency module is a wireless device that basically works on either 413MHZ or 315MHZ frequency [8]. Zig bee is a protocol based on open system interconnection (OSI) layer model.Based on technology and strength of RFID, we combine RFID &ZigBee to form wireless network. This method provides high efficiency & safer campus with anti-theft system. Antitheft system helps to prevent robbery, theft and accidents etc. Based on RFID &Zigbee, the intelligent campus security system detects theft in monitoring areas [8].

When the person enters into a facility/premises by any of the Gate, his identity and luggage identity is scanned through sensor and saved in a data base through wireless communication. When the person exits from any of the gate, he has to swipe his identity card and luggage identity, the system checks the identification through database, if identity is matched then a person can exit, if by any chance identity of a person or luggage didn't match, then person will not be allowed to exit from any of the gate. It can provide and highlight the appropriate situation scene in security control centre to an action, through sound & light alarm signals to enable emergency measures to be taken.

2. PROPOSED SYSTEM

The intelligent campus security system is based on wireless communication services between nodes provided by RFID tags within the building from different gates to prevent thefts & track valuables, so as to protect the property of the authorized members of the premises. The block diagram as shown in Fig. 1

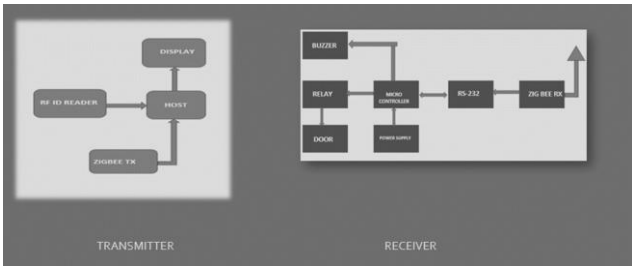

Fig. 1. *Hardware Architecture of proposed System*

Work Flow of the Proposed System can be described by the following steps:

RFID tags are inexpensive and can be reprocessed also data transmission is easy to implement at low powered .RFID tags are used to read data from user identity card and save into the server or PC nodes through RF signals[5,6]. In this data transmission & reception take place through Zig bee Protocol. Zig Bee module provides two way data transmission services and returns the corresponding control information after passing center node and PC processing, control information is sent to microcontroller through Zig bee communication module [10]. Transceiver receives RFID data that sends the information of the read tags to the microcontroller, according to RS232 protocol corresponding data will be stored in the database [3]. PC node gives the matched result by querying the registered tag information in the database and returns the corresponding results through the wireless module. When the incoming tag information does not match, PC node will give warning message, pass the warning and control message to entrance guard[4].

a) When a person enter from any one of the gate, his required identity card data and a luggage information saved in the database server through wireless module.

b) When a person wants to exit from the campus with his luggage, he has to swap his identity card and luggage identity card from the RF reader.

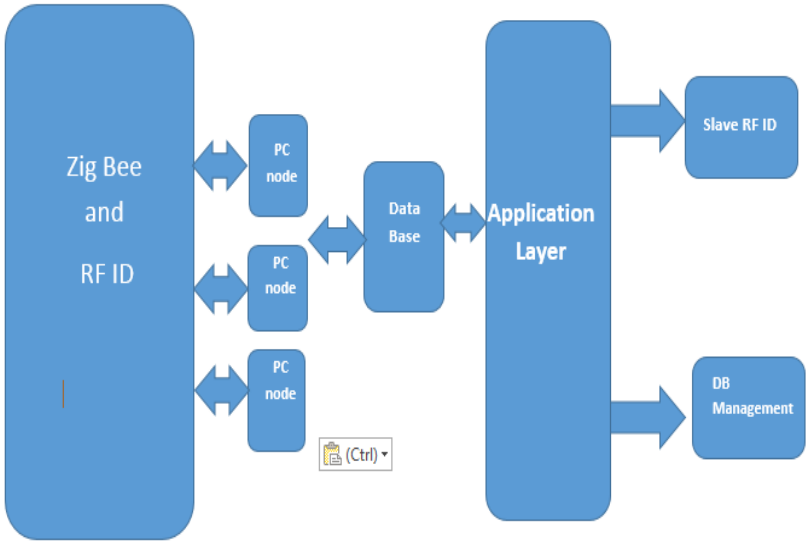

Fig 2. *Software schematic*

System algorithm

1) To get the RFID data from the upper layer, form packets, add source address, destination address, sequence number, data length, checksum to it, and then send it to the serial output module of the microcontroller.
2) The serial output module adds FLAG to the data packet, if required then go to step3.
3) Return true if receive Acknowledgement, if time extended & packet is not received then inform the upper layer that transmission is fails.

When the receiver receives the data, perform the following steps.

1) Check the data packet according to the check operation, if check result is same then proceed to the step 2 else drop the packet.
2) Check the destination node number of the data packet if its same as persons ID &luggage ID go to step 3 else drop the packet.
3) Return the corresponding acknowledgement of the data packet, determine whether its request for new packet or retransmission according to the sequence number of data packet, then send it to the upper layer for computing & handling.

3. LITERATURE SURVEY

A) PIC Microcontroller 18F4520:

Features:

PIC stands for peripheral interface controller which is an 8bit microcontroller, it has RISC architecture with some standard features such as on chip program (code) ROM, data RAM, and data EEPROM & I/O

Special Microcontroller Features

- C compiler optimized architecture
- Optional extended instruction set designed to optimize re-entrant code.

PIC microcontroller have program or code ROM with the space of 2 megabytes[15].

Data RAM [4096 bytes(4K)] (General purpose RAM) is the amount of RAM available for data manipulation (scratch pad) in addition to the special Function Registers(SFRs) space which is divided into banks of 256 bytes each.

PIC 18FXXX (F) stands for flash, the flash version is ideal for fast development because flash memory can be erased in seconds compared to the 20 min needed for the UV-EPROM version. The PIC 18 can have from 16 to 72 pins dedicated for I/O.

B) RFID (Radio Frequency Identification):

The RFID (Radio Frequency Identification-

It consists of an RFID Reader/Writer (Transceiver), an HF Tag and a Processor unit interfacing to peripherals.

HF Tags: a wide range of HF Tags are required for processing that help to decide which tag to use. In addition, the amount, type and security level of the information stored on the card determine the appropriate tag. HF Tags, made up of paper and plastic lamination. Memory sizes up to 2kBit with different security levels are available [14].

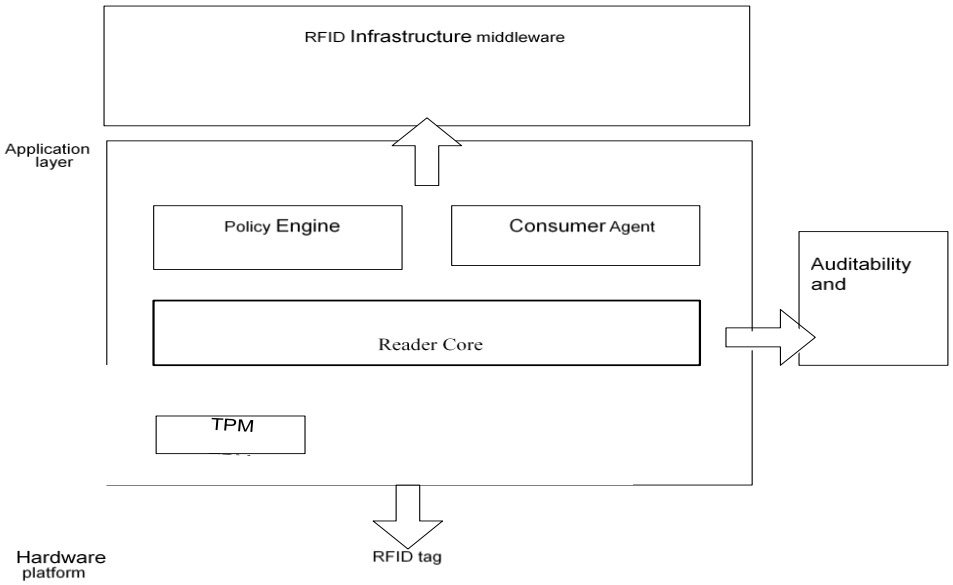

Fig 3. *Functional Block diagram of RFID*

Reader core: The reader core is defined to interface with the TPM and to make sure that the platform integrity is accurately recorded. It is also responsible for monitoring the applications that are run on top of the kernel. The reader core is also responsible for interfacing with the RFID radio interface at the operating system level.

Policy engine: The function of the policy engine is to store secrets in the policy engine. The policy engine always has an active policy set. The policy defines which tags are allowed to be passed to the RFID application and which tags have to remain private. Whenever the active policy changes the consumer agent is informed of this change and receives a description of the new policy.

Consumer Agent: The consumer agent is a logging component that allows third parties to actively monitor privacy policies. It interacts with both the policy engine and the reader core. It records the reading operations that have occurred and the policies that have been enabled. The consumer agent is also responsible for reporting the integrity of the system and can halt the system if it is compromised.

Backscatter modulation:

It is a communication method used by a passive RFID tag to send data back to the reader. By repeatedly shunting the tag coil through a transistor, the tag can cause slight fluctuations in the reader's RF carrier amplitude. The RF link work as a transformer; as the secondary winding (tag coil) is shunted, the primary winding (reader coil) experiences a momentary voltage drop. The reader must peak-detect this data at about 60 dB down (about 100 mV riding on a 100V sine wave).

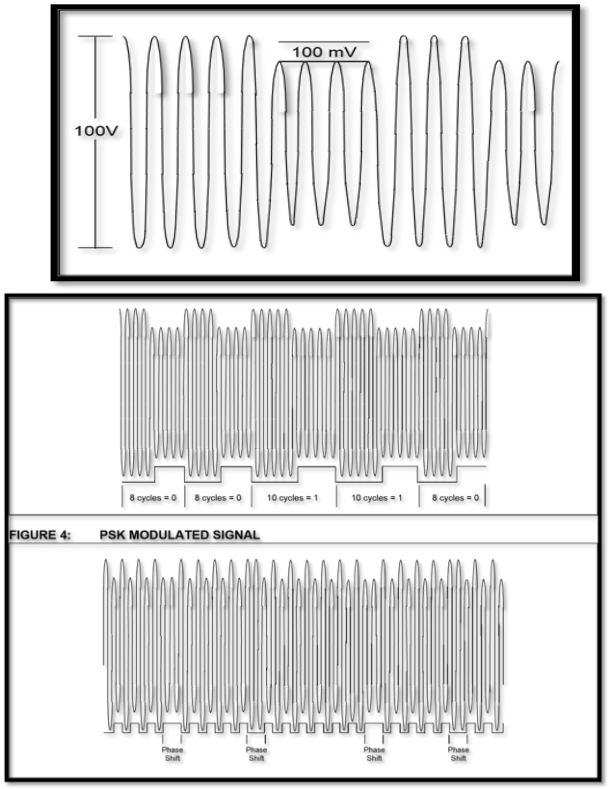

Fig 4. *modulation Technique(TI data sheet)*

RFID Reader/Writer (Transceiver): The RFID Transceiver represents the core of the RFID reader which interface to the reader's antenna, a parallel or serial communication can be used between the Processor and the Transceiver unit. The transceiver unit supports data communication levels to the MCU/I/O Interface ranging from 1.8V to 5.5V also providing a data synchronous clock. Processor: There are two types those are fixed and Mobile RFID Reader, the important factor is the power consumption of the Processor.

C) ZIGBEE Technology:

The IEEE 802.15.4 and the Zigbee Technology. The IEEE 802.15.4 is "an emerging standard that is based on the IEEE 802.15.4 and adds network construction (star networks, peer-to-peer/mesh networks, and cluster-tree networks), application services, and more."

The general block diagram of Zigbee module shown below:

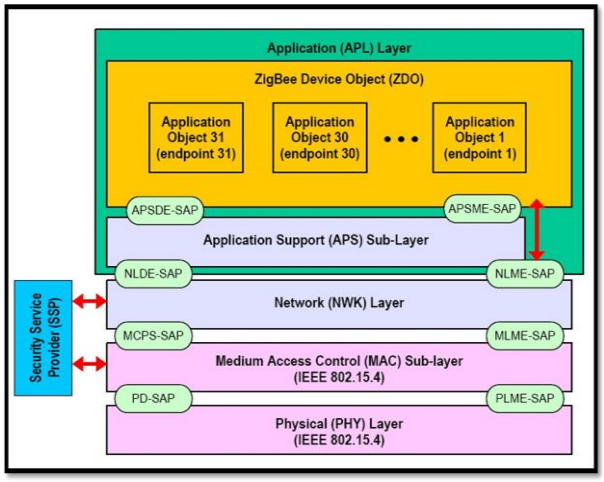

Fig 5. *Layered Architecture of ZigBee protocol[10]*

The Co-ordinator is responsible for starting a Zigbee network. Network initialization involves the following steps: 1. Search for a Radio Channel-The Co-ordinator first searches for a suitable radio channel (usually the one which has least activity). This search can be Assign PAN ID: - The Co-ordinator starts the network, assigning a PAN ID (Personal Area Network identifier) to the network. The PAN ID can be pre-determined, or can be obtained dynamically by detecting other networks operating in the same frequency channel and choosing a PAN ID that does not conflict with theirs. Start the Network: - The Co-ordinator then finishes configuring itself and starts itself in Co-ordinator mode. It is then ready to respond to queries from other devices that wish to join the network.

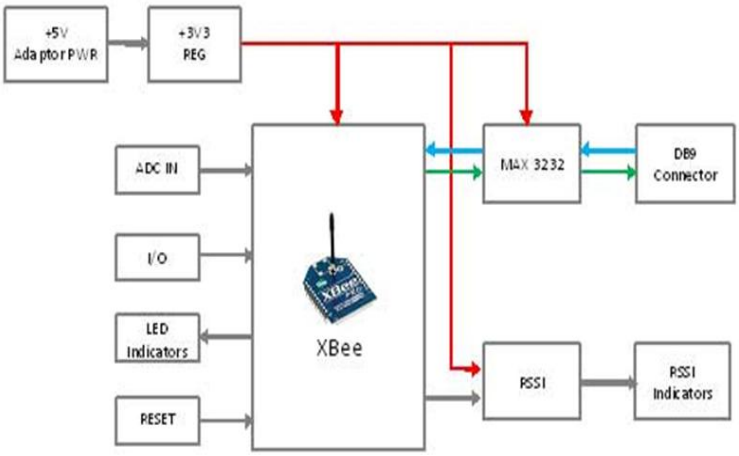

Fig. 6. *Functional Block Diagram of ZIGBEE Protocol*

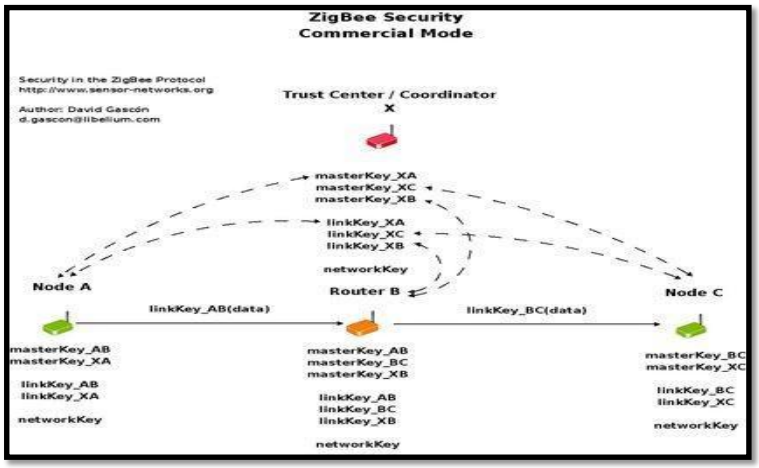

Fig 7. *Security Architecture of Zig Bee Technology*

Security Scenario in Zig bee

Zig bee implements two extra security layers on top of the 802.15.4 one: The Network and Application security layers.

There are three kinds of Keys: master, link and network keys.

- Master Keys: They are pre-installed in each node. Their function is to keep confidential the Link Keys exchange between two nodes in the Key Establishment Procedure (SKKE).
- Link Keys: They are unique between each pair of nodes. These keys are managed by the Application level. They are used to encrypt all the information between each two devices, for this reason more memory resources are needed in each device.
- Network key: It is a unique 128b key shared among all the devices in the network. It is generated by the Trust Centre and regenerated at different intervals. Each node has to get the Network Key in order to join the network. Once the trust centre decides to change the Network Key, the new one is spread through the network using the old Network Key. Once this new key is updated in a device, its Frame Counter is initialized to zero. Coordinator, however, it can be a dedicated device.

It has to authenticate and validate each device which attempts to join the network... Zig bee may secure messages transmitted over a single hop using secured MAC data frames, but for multi-hop messaging Zigbee relies upon upper layers (such as the NWK layer) for security.

The MAC layer uses the Advanced Encryption Standard (AES) as its core cryptographic algorithm and describes a variety of security suites that use the AES algorithm. These suites can protect the confidentiality, integrity, and authenticity of MAC frames. The MAC layer does the security processing, but the upper layers, which set up the keys and determine the security levels to use, control this processing. When the MAC layer transmits (receives) a frame with security enabled, it looks at the destination (source) of the frame, retrieves the key associated with that destination (source), and then uses this key to process the frame according to the security suite designated for the key being used. Each key is associated with a single security suite and the MAC frame header has a bit that specifies whether security for a frame is enabled or disabled.

Each pair of devices can have set both Network and Link Keys. In this case the Link key is always used (more security although more memory is needed). There are two kinds of security policies which the Trust Centre can follow: -Commercial mode: the Trust Centre share Master and Link Keys with any of the devices in the network. This mode requires high memory resources. This mode offers a complete centralized model for the Key Security control. - Residential mode: the Trust Centre shares just the Network Key (it is the ideal mode when embedded devices have to cope with this task due to the low resources they have). This is the mode normally chosen for the Wireless Sensor Network model.

D) Power Supply:

The external power can be DC source, voltage (+5V/, 1A output) at 230V AC input. The LM1117 Fixed +3.3V positive regulator is used to provide power to the Zigbee Modules and other peripherals.

- RESET: The Reset Switch is used to reset (re-boot) the RF module.
- Serial Port: Female DB9 connector.
- RSSI Indicators: RSSI LEDs indicate the amount of fade margin present in an active wireless link. Fade margin is defined as the difference between the incoming signal
- X-CTU Software: X-CTU is a software program used to interface with and configure RF Modules. The software application is organized into the following four tabs:
- PC Settings tab - Setup PC serial ports for interfacing with an RF module
- Range Test tab - Test the RF module's range and monitor packets sent and received
- Terminal tab - Set and read RF module parameters using AT Commands
- Modem Configuration tab - Set and read RF module

4. HARDWARE AND SOFTWARE CO-DESIGN

There are two approaches for the embedded system design: The software development life cycle ends and the life cycle for process of integrating the software into hardware begin at the time when a system is designed both cycles concurrently proceed when co-designing a time for sophisticated system. The selection of the right hardware during hardware design gives the understanding of hardware & software for sophisticated embedded system.

A platform consists of a number of units those are Processor, memory, RFID, Zig bee and their configuration.

- **Processor:** here PIC18F4520 is in used, it is 8bit processor means CPU can work on only 8bit data at a time, uses RISC architecture with flash memory so it can erased in seconds. We can configure by MPLAB having C18 compiler gives Hex then from PC, we can have PICkkit3 burning programme that will burn into the flash memory of microcontroller. Here we have also RJ45 may use for further programming modification. Memory is 16 Kbytes of Flash memory which can store up to 8,192 single-word instructions.

To initialize microcontroller by two serial ports from port i.e COM data will be transferred serially from RFID reader to the server (mainframe PC) & checks the data from database transferred whether valid or Invalid that information from server to the master Zig bee i.e. connected to the serial port 2 i.e. master Zigbee sends information to the slave zig bee those are connected to the each gate according to the date they will allow to exit with correct luggage.

- **Coding language:** microcontroller deals with database i.e. central data base to handle network base programming which should not hang in-between interconnection between our coding with data base language then put a logic of indication after checking,e.g

For Campus 1 =

{49, 65} __ [1, A]

{49, 66} __ [1, B]

{49, 67} __ [1, C]

For Campus 2 = {50, 65} __ [2, A]

{50, 66} __ [2, B]

{50, 67}__ [2, C]

How 49 & 50 comes,

For campus 1_____ 31 H _3*16+1=48+1=49

For campus 2_____32 H_ 3*16+2=48+2=50

When card swap for a individual that opens serial port and information read by the port1that port value and that value is converted into the character by a command Read char and after each increment the value of Y will be increased y=y+ x[i], serial port discard all previous information and check with the database such information is exist if it find no such data then gives Invalid data and informs serial port 2 through ZigBee not to open the gate and the person could not exists from any of the gate. Again SPI closed and timer began and takes next swapping and reads luggage ID, at least one luggage ID checks valid data from database and ZigBee allows to open the gate through microcontroller, if by any chance luggage will be more than one than it will read all luggage ID, if luggage ID matches then gives luggage OK and in message box shows valid student that Information passes to master ZigBee then will transmit it to the slave ZigBee for open or close the gate. In another condition if a person has no luggage only person ID matched then system allow it to go because luggage does not exists here.

5. RESULT AND ANALYSIS

As per our proposed system, we have three important module of devices i.e. PIC 18F4520 microcontroller, RFID 125KHZ & Zigbee standard type, all devices worked in an integrated form, firstly when a person swipe his identity card, his password is in HEX mode e.g. **FE00750D6C**,

this is an identity number which is present on card. This data is transmitted through radio frequency signal, Radio Frequency (RF) is a rate of oscillation in the range of about 3 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals. It is the use of radio signals to communicate real-time data. The hex code generally known as hex file, is a format used to store machine language code in hexadecimal form. It is widely used format to store programs to be transferred to microcontrollers, ROM and EEPROM. The compilers convert the programs written in assembly, C etc into corresponding hex files, which are dumped into the controllers using burners/programmers. The microcontroller understands machine language consisting of zeroes and ones.

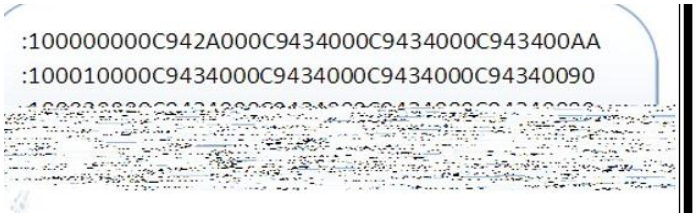

Fig 8. *code format*

This data is accessed by RF module which consist of reader core which is use to interface with the TPM and to make sure that the platform integrity is accurately recorded according to their policy engine which identifies the valid code that is already store in our TPM tool.

6. CONCLUSION

The proposed system implies campus safety & security by identifying the correct person and his own luggage to validate identity cards of person as well as for luggage. This implementation is done by newer wireless communication through RFID & ZigBee, it supports user to track valuables in real time. The system can also provide personnel tracking to support services related geographical location using client server networking method.

7. FUTURE SCOPE

In this system, there is only server for display & for connection because this system is only for the demonstration purpose, when we consider a large campus in that case then the system can be modify as a Client –Server networking. We can increase the power of Zig bee Transmitter and Receiver for advance system for large campus using pro type zig bee. This system is limited, it can be used as a dedicated network.RJ45 is connected because if we want to modify the PIC programming for future use. Our system sensor network uses middle distance RFID reader, ZigBee, RS232 & PIC18F4520 to perform small scale tracking & system verification. In order to save experimental cost, we can use simulation method to achieve large scale test & verification of our sensor network, the simulation in the experiment only replaces the process of reading the RFID tag information and PC directly simulates the actual tag data acquisition process also offers used in personnel logistics system.

REFERENCES

[1] XiLi, Tiyan shen ,Jinjie and changmin shi, A spatial Technology Approach to campus Security, October 1 2007(IEEE).

[2] Zhu Yuan-Jiao Ke-qin(Beijing university of civil Engineering Design & Realizing of the Digital Campus Security System, Beijing 100044 (IEEE 2003).

[3] Ricardo O.Michell, Hamad Rashid, Fakir dawood & Ali Alkhalidi (university of Saudi Arabia) Hajj Crowd Management & Navigation system.

[4] Li Bai-ping ,SHANG Liang ,LI Wen –Feng, Chen Lei, Research on coal mine personnel orientation rescuing system based on RFID,(IEEE 2008).

[5] Floerkemeier C, sarma s, An overview of RFID system interfaces & Reader Protocol,RFID 2008 IEEE international conference.

[6] Kaun J.H ,chang H,HO.J,A development of information protection system using system engineering & RFID Technology, system science and engineering,

[7] zhu yu yu ,wangzeng sheng,personnel orientation study based on RFID,science & Technology information ,system science & engineering 2010 international conference on IEEE 2010.(in Chinese)

[8] Chung-Hsin Liu, Jian-Yun Lo, The Study for the ZigBee with RFID Positioning System, Multimedia and Information Technology (MMIT), 2010 Second International Conference on 2010.

[9] Yu Li-e, Deng Xu-dong, The Research about the Application of RFID and 3G Technology in Cargo Transportation Security, Logistics SciTech, 2007(10) (in Chinese).

[10] Elshayeb, S.A., Bin Hasnan, K., Chua Yik Yen, RFID technology and ZigBee networking in improving supply chain traceability Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2009 IEEE International Conference.

[11] Chau-Chung Song, Yin-Chieh Hsu, Chiz-Chung Cheng, Hong-Lin Ke, Der-Cherng Liaw, Study and implementation of a networking information platform for RFID system, Industrial Technology 2008,

[12] Qian C,Ngan H,Liu Y. Cardinality Estimation for Large-scale RFID Systems[C] .Preceedings of IEEE Int'l Conf.on Perv.Comp.and Comm(PerCom). 2008:30-39.

[13] REN Xiao-Kui, LIANG Chao-Zhong, Analysis and Improvement of Anti-Collision Algorithm for RFID Syst Chung-Hsin Liu, Jian-Yun Lo, The Study for the ZigBee with RFID Positioning System, Multimedia and Information Technology (MMIT), 2010 Second International Conference on 2010. Computer Systems & Applications, 2010(2) (in Chinese).

[14] Texas Instruments Data sheet for RFID (125 KHz).

[15] Texas Instruments Data sheet for PIC 18F4520.