ISSN 2250-3153

Use of RFID for Safety at School/Hospital Campus

Sushil I. Bakhtar[1] and Prof. Ram S. Dhekekar[2]

Sant Gadge Baba Amravati University, Amravati (Maharashtra)[1]
Electronics & Telecom. Department, SSGMCE, Shegaon (Maharashtra)[2]

Abstract- With growth of technology and giant leap in the field of Radio frequency transmission, a requirement for the safety and campus security using RFID is desired. The main purpose of the campus security system is to make the campus secured in every way that is need to be done and also maintaining the discipline in the school/hospital campus. Authentication of the person entering the campus is done automatically with help of RFID system.

I. INTRODUCTION

We have seen the security personnel checking the employees' identification cards at the entrances to avoid illegal entry. The employees sign a register at the entrance before getting in. This is still being practiced in most of the companies. However, the disadvantages are that, when there is a necessity of providing control at many locations inside the company, a person at each point will not be an economical way of implementing it. Then came were the punch cards. Employees possess cards, which are punched when they enter into the building. But it had disadvantages. Workers started to practice buddy punching, for their co-workers. It is a much common sight to see a bar code reader in the companies. These are used to check with the employee's identification. The employees swipe the card in the provided slot. Then the access is given after checking the authenticity of the card. This was a substitute to the security and emerged as a new technique in access control. This acted as a starting to the automation of the access control. But, the bar code readers are contact readers where, the cards are required to touch the readers. With growth of technology and giant leap in the field of Radio frequency transmission, a requirement for the same application using RFID is desired. The term RFID (radio frequency identification) describes the use of radio frequency signals to provide automatic identification of items. RFID is a flexible technology that is convenient, easy to use, and well suited for automatic operation. It combines advantages not available with other identification technologies. RFID can be supplied as read-only or read / write, does not require contact or line-of-sight to operate, can function under a variety of environmental conditions, and provides a high level of data integrity. In addition, because the technology is difficult to counterfeit, RFID provides a high level of security. RFID is similar in concept to bar coding. Bar code systems use a reader and coded labels that are attached to an item, whereas RFID uses a reader and special RFID devices that are attached to an item. Bar code uses optical signals to transfer information from the label to the reader; RFID uses RF signals to transfer information from the RFID device to the reader.

Radio waves transfer data between an item to which an RFID device is attached and an RFID reader. The device can contain data about the item such as what the item is, what time the device traveled through a certain zone, perhaps even a parameter such as temperature. RFID devices, such as a tag or label, can be attached to virtually anything – from a vehicle to a pallet of merchandise.

II. RFID MODULE FOR SCHOOL/HOSPITAL CAMPUS

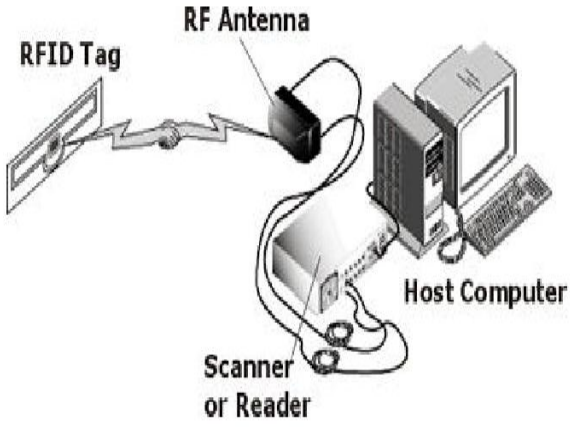

Figure 1. Typical RFID system

An RFID system typically includes the following components:
• An RFID device (transponder or tag) that contains data about an item
• An antenna used to transmit the RF signals between the reader and the RFID device
• An RF transceiver that generates the RF signals
• A reader that receives RF transmissions from an RFID device and passes the data to a host system for processing
If anyone has entered in campus then its identity is automatically recorded by RFID reader placed near main gate. Also identity and mobility in campus of each person in campus will be monitored and recorded by no. of RFID readers placed in campus and a central database station.

Every person has its permanent Tag attached to it which will be stored with the some details such as person name, mobile number, address and the gate at the campus will have the reader attached to it. When a person enters in the campus there is communication between reader and the tag which are at same frequencies, reader reads the information and feed it to the host computer.

A. Working of RFID tags

The RFID tags based on the mode of operation are classified as Active and Passive tags. The classification is done on basis of the tags ability to transmit the code embedded in it. Hence an active tag is capable of transmitting to a reader independently, whereas the passive tag needs an external excitation to transmit the code. The reader usually provides the excitation. Further each of the tags either active or passive has their own frequency of operation. We have used the active type of tag operating at a frequency of 2.4GHz in this application.

B. Tag Classes

One of the main ways of categorizing RFID tags is by their capability to read and write data. This leads to the following 4 classes. EPC global has also defined five classes

CLASS 0 – READ ONLY. – Factory programmed

These are the simplest type of tags, where the data, which is usually a simple ID number, (EPC) is written only once into the tag during manufacture. The memory is then disabled from any further updates. Class 0 is also used to define a category of tags called EAS (electronic article surveillance) or anti-theft devices, which have no ID, and only announce their presence when passing through an antenna field.

CLASS 1 – WRITE ONCE READ ONLY (WORM) – Factory or User programmed

In this case the tag is manufactured with no data written into the memory. Data can then either be written by the tag manufacturer or by the user – one time. Following this no further writes are allowed and the tag can only be read. Tags of this type usually act as simple Identifiers

CLASS 2 – READ WRITE

This is the most flexible type of tag, where users have access to read and write data into the tags memory. They are typically used as data loggers, and therefore contain more memory space than what is needed for just a simple ID number.

CLASS 3 – READ WRITE – with on board sensors

These tags contain on-board sensors for recording parameters like temperature, pressure, and motion, which can be recorded by writing into the tags memory. As sensor readings must be taken in the absence of a reader, the tags are either semi-passive or active.

CLASS 4 – READ WRITE – with integrated transmitters.

These are like miniature radio devices that can communicate with other tags and devices without the presence of a reader. This means that they are completely active with their own battery power source.

C. How tags communicate

Near and Far fields

In order to receive energy and communicate with a reader, passive tags use one of the two following methods. These are near field, which employs inductive coupling of the tag to the magnetic field circulating around the reader antenna (like a transformer), and far field, which use similar techniques to radar (backscatter reflection) by coupling with the electric field. The near field is generally used by RFID systems operating in the LF and HF frequency bands, and the far fields for longer read range UHF and microwave RFID systems.

In terms of computational power, RFID tags are quite dumb, containing only basic logic and state machines capable of decoding simple instructions. This does not mean that they are simple to design! In fact very real challenges exist such as, achieving very low power consumption, managing noisy RF signals and keeping within strict emission regulations. Other important circuits allow the chip to transfer power from the reader signal field, and convert it via a rectifier into a supply voltage. The chip clock is also normally extracted from the reader signal. Most RFID tags contain a certain amount of NVM (Non volatile M emory) like EEPROM in order to store data

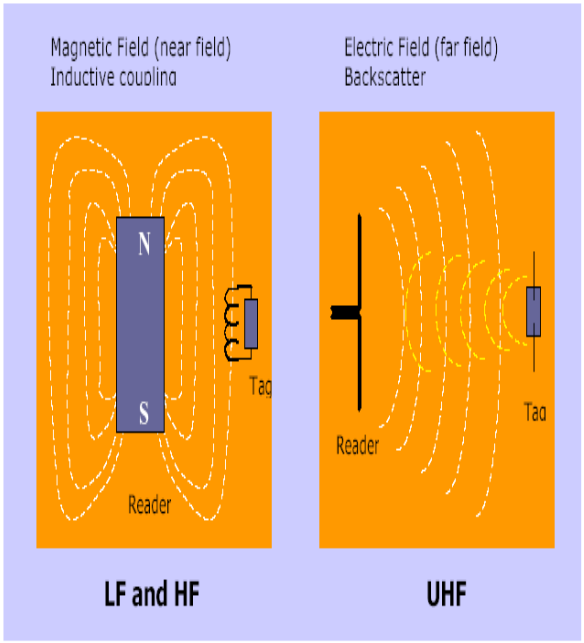

Fig. 2: How Tags Communicate

D. LF, HF Tags

Tags at these frequencies use inductive coupling between two coils (reader antenna and tag antenna) in order to supply energy to the tag and send information. The coils themselves are actually tuned LC circuits, which when set to the right frequency (ex; 13.56 MHz), will maximize the energy transfer from reader to tag. The higher the frequency the less turns required (13.56 MHz typically uses 3 to 5 turns). Communication from reader to tag occurs by the reader modulating (changing) its field amplitude in accordance with the digital information to be transmitted (base band signal). The result is the well-known technique called Amplitude modulation (AM). The tags receiver circuit is able to detect the modulated field, and decode the original information from it. However, whilst the reader has the power to transmit and modulate its field, a passive tag does not. How communication is therefore achieved back from tag to reader?

The answer lies in the inductive coupling. Just as in a transformer when the secondary coil (tag antenna) changes the load and the result is seen in the Primary (reader antenna). The tag chip accomplishes this same effect by changing its antenna impedance via an internal circuit, which is modulated at the same frequency as the reader signal. In fact it's a little more complicated than this because, if the information is contained in the same frequency as the reader, then it will be swamped by it, and not easily detected due to the weak coupling between the reader and tag. To solve this problem, the real information is often instead modulated in the side bands of a higher sub- carrier frequency, which is more easily detected by the reader

E. Anti-collision

If many tags are present then they will all reply at the same time, which at the reader end is seen as a signal collision and an indication of multiple tags. The reader manages this problem by using an anti-collision algorithm designed to allow tags to be sorted and individually selected. There are many different types of algorithms (Binary Tree, Aloha....), which are defined as part of the protocol standards. The number of tags that can be identified depends on the frequency and protocol used, and can typically range from 50 tags/s for HF and up to 200 tags/s for UHF.

Once a tag is selected, the reader is able to perform a number of operations such as read the tags identifier number, or in the case of a read/write tag write information to it. After finishing dialoging with the tag, the reader can then either remove it from the list, or put it on standby until a later time. This process continues under control of the anti collision algorithm until all tags have been selected.

III. RESULT

This system delivers the flexibility, scalability, and responsiveness that today's organizations need. It provides accurate, up-to-minute information, high- speed communication, and powerful analysis features required to make better decisions faster. The major potential comes from the much acclaimed no line of sight and simultaneous reading properties of RFID.

It is now widely recognized that real–time information will revolutionize the control and logistical organization with significant safety of campus. So we came up with many challenges to make the campus security with the help of RFID system. With the concept of on stationary transceiver kept in campus at main gate and when the person enters in the campus the stationary RF module reads the another module entered in the campus attached to the person and that module is called as the tag .

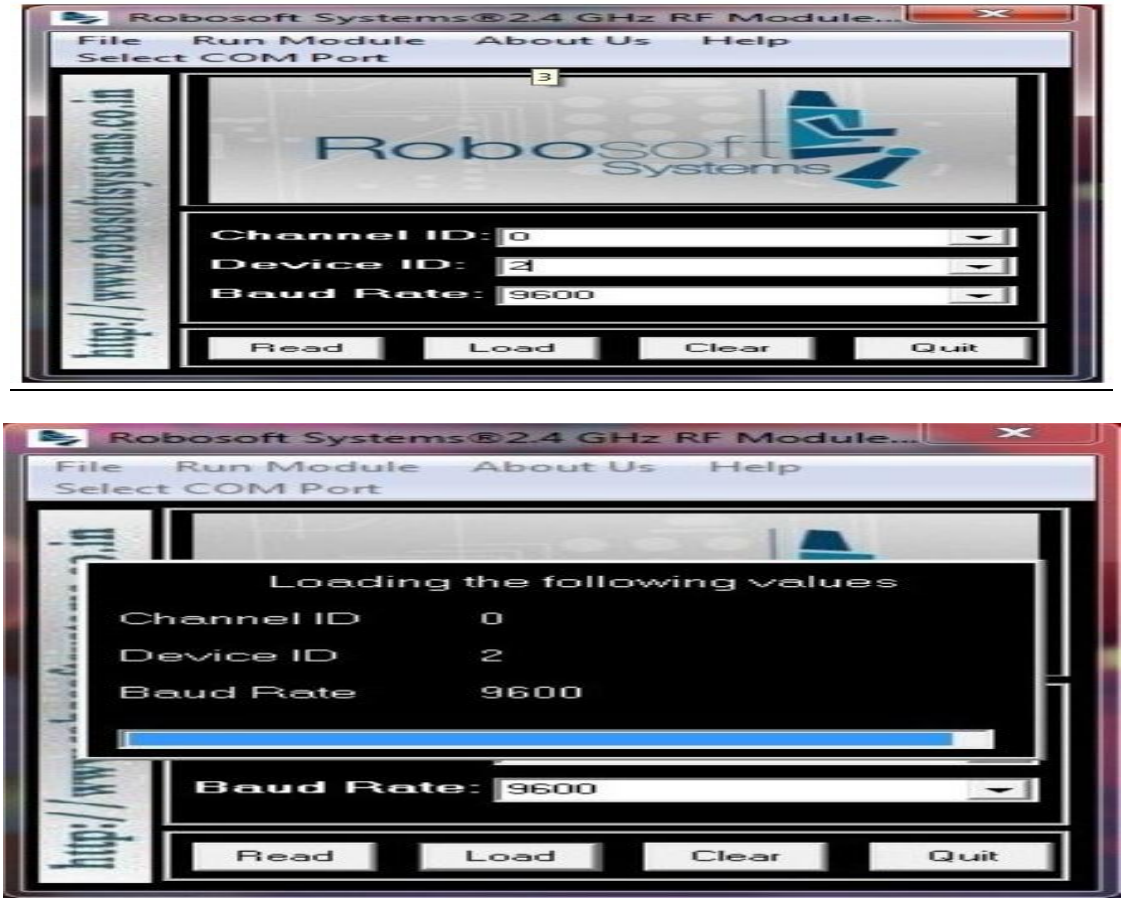

Fig. 3: Expected Results

IV. CONCLUSION

The implementation of RFID based security system is bound to increase in the future. The advantages, efficiency and reliability of the system have made it manifest itself over the existing systems. The system achieves a high level security making the incorporating school/hospital campus more secure.

Further this system is compatible for the future up gradations like a Finger print scanner, retina scanner, monitoring camera, etc. making it more versatile. With the introduction of more smart RFID devices in the near future the system is going to rule the field of access control and security.

And so on the RFID identification has much wide variety in its application

- **Security**

Access control

Counterfeiting and Theft control/prevention

- **Manufacturing and Processing**

Inventory and production process monitoring
Warehouse order fulfillment

- **Supply Chain Management**

Inventory tracking systems
Logistics management

- **Retail**

Inventory control and customer insight
Auto checkout with reverse logistics

- **Location Tracking**

Traffic movement control and parking management

REFERENCES

[1] B. Glover and H. Bhatt. RFID Essentials. O'Reilly, 2006.

[2] E.P.C. Inc. The EPC global Network: Overview of Design, Benefits and Security. EPC Global White Paper, 2004.

[3] www.laranrfid.com ("A basic introduction of RFID technology" paper by Laran)

[4] Sybase, Inc., "SYBASE RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY ARCHITECTURE"One Sybase Drive Dublin CA, 94568 USA, 2005, http://www.sybase.com/sb_content/1031464/16056_RFID_Arch_L02607_FNL3.pdf accessed on 11 February 2007.

[5] K. Finkelzeller, The RFID Handbook, 2nd ed., John Wiley & Sons, 2003.

[6] R. Want et al., "Bridging Real and Virtual Worlds with Electronic Tags," Proc. ACM SIGCHI, ACM Press, 1999, pp. 370–377.

[7] R. Want, "Enabling Ubiquitous Sensing with RFID," Computer, vol. 37, no. 4, 2004, pp. 84–86.

[8] E. Batista, "'Step Back' for Wireless ID Tech?" Wired News, 8 Apr. 2003; www.wired.com/news/wireless/0,1382,58385,00.html.R. Singel, "American Passports to Get Chipped," Wired News, 19 Oct. 2004; www.wired.com/news/privacy/0,1848,65412,00.html.

[9] A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," Proc. 8th ACM Conf. Computer and Comm. Security, ACM Press, 2003, pp. 103–111.

[10] D.W. Engels and S.E. Sarma, "The Reader Collision Problem," white paper MITAUTOID-WH-007, Auto-ID Center, Nov. 2001.

AUTHORS

First Author: Sushil I Bakhtar, PG student, Sant Gadge Baba Amravati University, Amravati.

Second Author: Prof. Ram S. Dhekekar, Ass.Prof. in department of Elec. & Telecom., SSGMCE, Shegaon(Mah)