Journal of Information & Communication Technology
Vol. 1, No. 2, (Fall 2007) 35-42

An Approach for Surveillance Using Wireless Sensor Networks (WSN)

Bilal Ahmad Khan *
Muhammad Sharif *
Mudassar Raza *
Tariq Umer *
Khalid Hussain *
Aman Ullah Khan *

COMSATS Institute of Information Technology Islamabad, Pakistan

ABSTRACT

This paper purposes a new surveillance system for an organization using wireless sensor networks and RFID. The system authenticates the authorized person of the organization using RFID (Radio Frequency Identifier) tags embedded cards and also detects the unknown person using Motion sensors. The system also alarms the presence of unknown person. The benefit of this system is to surveillance the people without using close circuit cameras.

Inspec Classification: B6250Z, B6220, D3035, E0240C

Keywords : Multiple Values, Binary Search, Complexity, Data Warehouse

1) INTRODUCTION

The wireless sensor networks technology is used in number of applications. (Key Romer, 2004). In future big companies are planning to monitor their product using WSN. RFID (wikipedia.org) is widely accepted by industries to be an emerging technology for product identification (Yi Zhi Zhao, 2006), (Dong Seong Kim, 2005). The proposed idea is to use WSN in the surveillance of an organization or building. The system is skipping the use of cameras and biometric identifiers. Proposed system is the simple use of the paired device called reader and transponder.

* Bilal Ahmad Khan : bilal_khan_5212086@hotmail.com
* Muhammad Sharif : muhammadsharifmalik@yahoo.com
* Mudassar Raza : mudassarkazmi@yahoo.com
* Khalid Hussain : khalidusmani_65@yahoo.com
* Aman Ullah Khan : auk_pk@yahoo.com
* Tariq Umer : t_umer@yahoo.com

2) EXISTING TECHNIQUES

There are different techniques for surveillance. Each technique has some advantages and drawbacks. The most used techniques in the world are.

a). Surveillance using Cameras.
b). Surveillance using biometrics.

A. Surveillance using Cameras

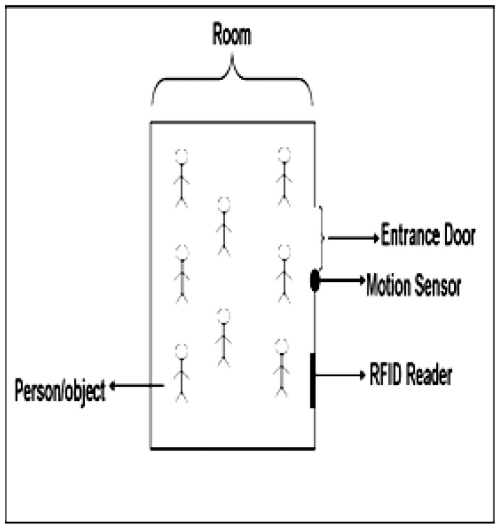
This technique just uses the cameras to do surveillance. It needs a command and control center to monitor all the activities using cameras. All the cameras are connected to the command center and send their data directly to the central location. All the activities which are happening in the organization or inside the building can be viewed live from the command center. If they found some threat then they do further action. Some newly developed techniques are distributed camera surveillance which uses an intelligent system to automatically track movements (Zen Chen).

B. Surveillance using Biometrics

This system uses the matching technique; it checks the physical characteristics of the human body. This type of system involves the image processing. It contains a database of pictures. All the entrance points or check points are installed with cameras or scanners. That takes high resolution pictures to match with the database. For example, some systems take human eyes pictures and match the iris with the database.

3) PROPOSED SYSTEM

Fig 1:
A brief view of proposed system.



The system uses transponder embedded in the objects identity card. It simply recognizes the transponder signal and then sends it to the central database server which checks for the domain of the object and take a decision from the identity embedded on the ID card. The system has two basic portions.

A) Sensors.
B) Database Server.

A. Sensors

Sensors part is one of the basic parts of the system. It allows to go any where inside the building person/object do not need to wait for the scanning, processing and then for the result. System will not ask anybody for his identity the sensor portion will recognize the object/personitself and check the domain of that room, hall or path way.(D. Patranabis)

Sensor portion has further two parts

i) Reader
ii) Transponder

i) Reader

The RFID reader portion has a motion detector which tells the reader about the presence of a person/object in the room it also tells the number of persons. Then reader starts sensing the signal emitted by the transponder's tag (Joongheon, 2005). The deployment of the readers can be varied with the nature of the deployment environment. For example if our interrogating area is highly risky then our deployment will be dense. It means density (d) is directly proportional to the risk (r).

$$d \propto r$$

The above equation shows that density is directly proportional to the risk. If we know that the interrogating area is the risky one, then we increase the density of the reader.

But density is inversely proportional to the threats (t).

$$d \propto 1/t$$

This equation shows that if we increase the density of the reader then the number of threats will be decreased.
Here system is using a motion detector as an additional component to make it more secure.

Motion Sensor

System uses a motion sensor with the reader device; it increases the security of the system (D. Patranabis). If a scenario has been taken that a person into the system without the transponder then readers sense less number of transponders; because they cannot sense the presence of an object into the room. So the motion sensor will tell the reader about the presence as well as the number of the objects. So if reader does not find the same number of transponder as number of objects then it will inform the central database server about some threat.

Collision Problem

If there are more then one transponder present in the room, there will be chance of a collision or data loss. So to minimize this risk, the system is using a new technique as written by "Tsan-Pin Wang" in his paper "Enhanced Binary Search Tree with cut-though Operation for Anti-Collision in RFID System" (Tsan-Pin Wang, 2006). The cut-through operation minimizes the search operation as early as an RFID device can be uniquely identified. This will decrease the collision problem.

Fig 2:
Example of Binary Search Tree in the reader (Tsan-Pin Wang, 2006)

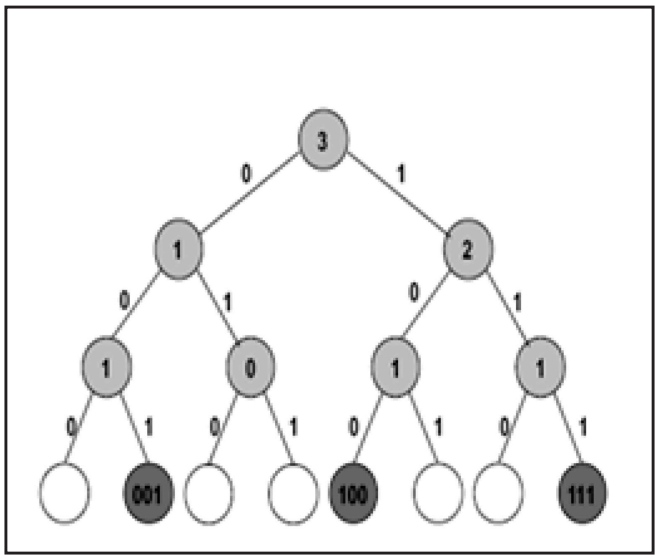
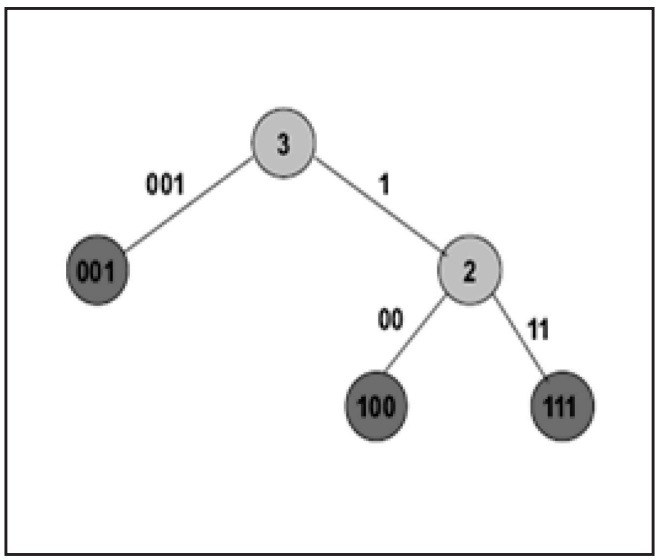


Fig 3:
Binary Search Tree with Cut-Through operation (Tsan-Pin Wang, 2006)



ii) Transponder

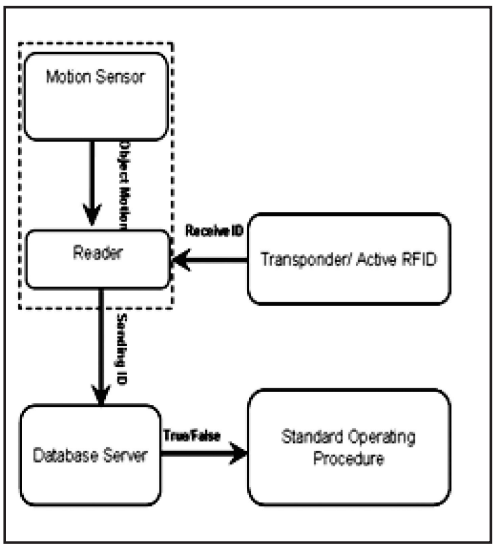
It is a transmitter, which transmit the information stored in them.(Dong Seong Kim), (J. Vazquez-Gimez, 1993). In the proposed case the information about the object will be stored in the transponder. It is a chip imbedded in the card of the object. The transponders used by the system are called as RFID.

4) PROPOSED TECHNIQUE USING ACTIVE RFID

This type of the RFID's has a capability to emit its information all the time without any outer interference (D. patranabis). They use batteries or some other mean of power. They can transmit at more distance then passive RFID. Their battery limits their life, means that they can be alive until their battery goes empty, and become alive when recharge or have power by some other mean. In this case the transponder emits the ID automatically and whenever it comes in the range of reader its information sent to the server for authentication. The use of this type of transmitter's is useful for the far away transmission. So the use can be varied among the scenario if the data have to be transmitted the far away readers or the other transmitters then we can use the active transmitter. But as far as the proposed technique is concerned the active RFID is not preferred due to following problems.

- These type of RFID's have the capability to change there information time to time. (devx.com), (A Basic Introduction to RFID).
- They are large in size due to the battery carrying capability (devx.com), (A Basic Introduction to RFID).
- Due to there long Range of transmission they can be detected by more then one reader. So conflict about location will happen in the database.

Fig 4:
System using Active RFID

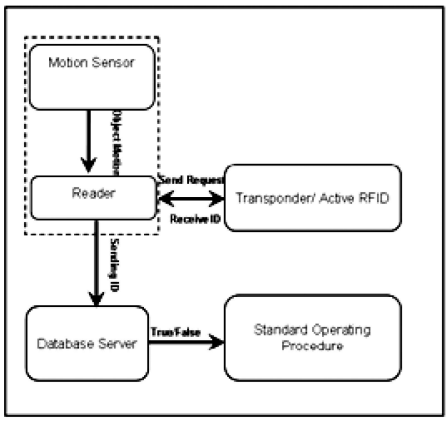


4) PROPOSED TECHNIQUE USING PASSIVE RFID

This type of RFID has long life, but its transmitting range is very short. They only transmit their information on request from the reader. This type of transponder can also be used with our system. But in the case of passive RFID reader sent a request to the transponder to send the ID in response transponder sent the information stored in it and the information is sent to the server for authentication. These types of transponders are ideal for the surveillance inside the building. They can be detected from 6 meters, (devx.com), (A Basic

Introduction to RFID), (D. Patranabis) so this range is sufficient inside the building. And their size is much smaller then active RFID transponders.

Fig 5:
System using Passive RFID

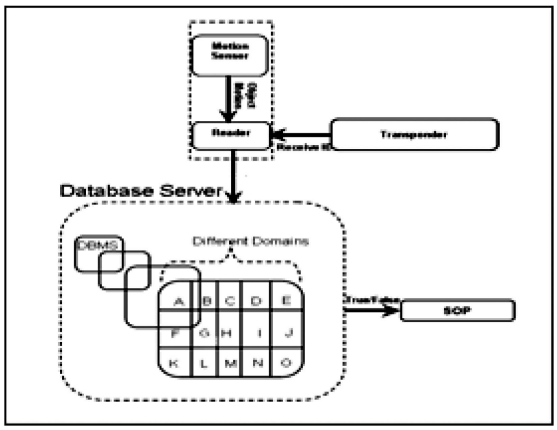


5) DATABASE SERVER

All the readers are connected with the central database server. This check for the domain of the object, if it finds some sort of threat then it follows the Standard Procedure as per organization. To understand this we take a scenario.

An object enters the room motion sensor sense the object it also tells the reader about the number of transponders present in the room. After motion detector reader read the signals and sends the information to the server which checks the object domain in the database if object is in the right domain then it makes a log file and follows the Standard Procedure as per organization. But in the case of wrong domain it also makes a log file and follow the Standard Procedure for false case. So here we have to note one thing very clearly that the designing of database system is a very careful process. Because a small mistake in the database can allow the imposters to penetrate in the organization.

FIG 6:
Different Domains of Database.



As shown in figure the database has different domains that have different set of rules for different locations. When some object come in contact with the reader. Reader sends that information to the database and it checks that ID with the same domain, where it comes from And then make a log for that event and follow the Standard Procedure for that type of case, for example if that object is not allowed to enter in that room then the alert will be sent to the surveillance officer. On the other hand if that object is allowed to enter in that room then the log file will be made only and nothing will happen.

6) PROPOSED SYSTEM V/S OLD ONE

The proposed system does the things what others cannot do. It is using the transponders which can easily locate the person in an organization or building, so by using the proposed system anyone can easily monitor the domain of the person, which cannot be done by the help of surveillance cameras. It is also being told about the person where it is in the organization at the specific time. Biometric identification system has number of steps scanning, processing and result. For this we have to stop each and every person of the organization. That waste a lot of time to identify a person. It is a very costly process because it involves heavy processing; each and every door or corridor of the organization has to be installed with the expensive scanners and cameras. Some times its results become false, for example if we are scanning the face of a person then a person can be in any mood or with any facial expression that is why results can be wrong. The proposed system needs no eyes like cameras needs no waiting time like biometrics. So we can say that proposed system is much betters then the others.

7) CONCLUSION

As proposed system has the quality of both well known surveillance or security systems named as surveillance using cameras and Biometrics security system. Proposed System is a very low cost system. As reliability of proposed system is much better than the both systems mentioned above. Due to these qualities this system can be used in many scenarios.

REFERENCES

KAY ROMER(2004), AND FRIEDEMANN MATTERN ETH ZURICH, The Design Space of Wireless Sensor Networks, in IEEE Wireless Communications, December 2004.

YI ZHI ZHAO (2006), OON PEEN GAN, Distributed Design of RFID Network for Large-Scale RFID Deoloyment. 2006 IEEE

RYO IMURA (2005), "Driving Ubiquitous Network – How Can RFID Solution meet the Customers' Expectations", 10th International Conference on Emerging Technologies and Factory Automation, Italy, 2005

DONG SEONG KIM, TAEK-HYUN SHIN, JONG SOU PARK, A Security Framework in RFID Multi-domain System.

JOONGHEON KIM (2005), WONJUN LEE, JIEUN YU, JIHOON MYUNG, EUNKYO KIM, CHOONHWA LEE, Effects of Localized Optimal Clustering for Reader Anti Collision in RFID Networks: Fairness Aspects to Readers, 2005 IEEE

TSAN-PIN WANG (2006), Enhanced Binary Search Tree with cut-though Operation for Anti Collision in RFID System, IEEE Communication Letters, VOL 10 NO 4, APRIL 2006.

J. VAZQUEZ-GIMEZ (1993), MODELLING MULTIDOMAIN SECURITY, In Proc. Of New Security Paradigms Workshop, Little Compton Thode Island, United States, Pages:167-174, 1993

An Introduction to RFID Development www.devx.com/enterprise/Article/31108

A Basic Introduction to RFID Technology and its use in the Supply Chain

ZEN CHEN, A distributed-Camera Intelligent Video Surveillance System for Tracking People and Their Activities, National Science Council.

D.PATRANABIS, Sensor and Transducers 2nd Edition, ISBN-81-203-2198-7.
Radio-frequency identification, http://en.wikipedia.org/wiki/RFID