International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN: 2349-9745
p-ISSN: 2393-8161

A Survey: SMS Sending Through RFID Sensors

Mithila Pushpendu[1]
[1]*Dept. of Research, Almix Softech, Banglore, India, Pushpendumithila.almix@gmail.com*

Abstract—This paper throws light on combined working of RFID sensors along with SMS sending technique. Paper is based how RFID sensors can sense data. Generally these data needs to be send through some wired or wireless medium, But sometime we need to send such data in groupings or indications directly from Sensors.

Keywords— RFID, Sensors, SMS

I. INTRODUCTION

This paper answers idea of working of RFID sensors with SMS architecture. Here, it is assumed that all sensors are smart sensors and they are capable enough to calculate some important data from sensed data. So, in some circumstances if we need to speed up intimation to some authority that can be done directly from sensors. Main advantage of this idea is speeding up of communication in some abnormal situations. Here, mainly three technologies are working, RFID, sensors and SMS architecture. Its application area can be identification of fast moving vehicles above certain speed, detecting some specified animals or product in factory. In these areas, we need to have quick response in short time and through this technology it can be minimized.

II. TECHNOLOGY

1. SMS Architecture

Short message service (SMS) is a globally accepted wireless service. SMS appeared on the wireless scene in 1991 in Europe. The European standard for digital wireless, now known as the Global System for Mobile Communications (GSM), included short messaging services from the outset[1]

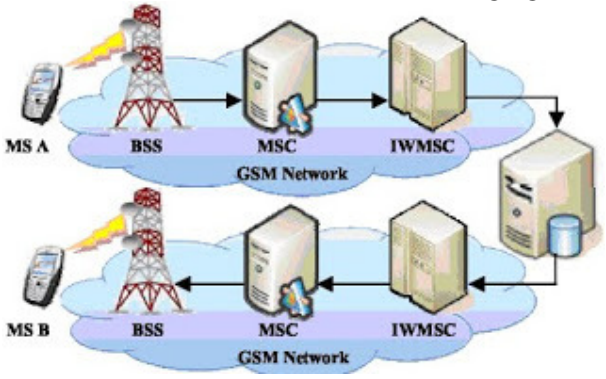

Figure 1: SMS Architecture

At the beginning, if a user sends a SMS to his buddy,the SMS first deliver from the MS which is know as Mobile Station A to SM-SC(Short Message Service Center) Via the Base Station System (BSS), and then it catch up to the Mobile Station center(MSC) and finally combine with

e-ISSN: 2349-9745
p-ISSN: 2393-8161

Interworking MSC(IW-MSC). The use of Short Message Service Center (SM-SC) to carry ahead the SMS message to the GSM network through a definite GSM-MSC called the Short Message Service gateway MSC (SMS-GMSC). The SM-SC is allowed to link with several GSM networks and to several SM-GMSCs in a GSM network. The SMS-GMSC come across the contemporary MSC of the message acceptor and then step ahead the SMS message to that Mobile Station center, pursue the Global System for Mobile Communication (GSM) roaming protocol.The MSC then Publish the SMS through the Base Station System (BSS) to the destination MSB[2][3].

2. RFID Technology

RFID transponders (tags) consist in general of:Micro chip,Antenna,Case and Battery (for active tags only)
The size of the chip depends mostly on the Antenna. Its size and form is dependent on the frequency the tag is using. The size of a tag also depends on its area of use. It can range from less than a millimeter for implants to the size of a book in container logistic. In addition to the microchip, some tags also have rewritable memory attached where the tag can store updates between reading cycles or new data like serial numbers. A RFID tag is shown in figure 1. The antenna is clearly visible. As said before the antenna has the largest impact of the size of the tag. The microchip is visible in the center of the tag, and since this is a passive tag it does not have an internal power source[4].

2.1 Energy Sources

We distinguish 3 types of RFID tags in relation to power or energy: Passive,Semi-passive,Active

Passive tags do not have an internal power source, and they therefore rely on the power induced by the reader. This means that the reader has to keep up its field until the transaction is completed. Because of the lack of a battery, these tags are the smallest and cheapest tags available; however it also restricts its reading range to a range between 2mm and a few meters. As an added benefit those tags are also suitable to be produced by printing. Furthermore their lifespan is unlimited since they do not depend on an internal power source.

The second type of tags is semi-passive tags. Those tags have an internal power source that keeps the microchip powered at all times. There are many advantages: Because the chip is always powered it can respond faster to requests, therefore increasing the number of tags that can be queried per second which is important to some applications. Furthermore, since the antenna is not required for collecting power it can be optimized for back scattering and therefore increasing the reading range. And last but not least, since the tag does not use any energy from the field the back scattered signal is stronger, increasing the range even further. Because of the last two reasons, a semi-active tag has usually a range larger than a passive tag.

The third type of tags is active tags. Like semi-active tags they contain an internal power source but they use the energy supplied for both, to power the microchip and to generate a signal on the antenna. Active tags that send signals without being queried are called beacons. An active tag's range can be tens of meters, making it ideal for locating objects or serving as landmark points. The lifetime is up to 5 years[4][5][6].

2.2 Frequency Bands

e-ISSN: 2349-9745
p-ISSN: 2393-8161

RFID tags fall into three regions in respect to frequency: Low frequency (LF, 30 - 500kHz), High frequency (HF, 10 - 15MHz), Ultra high frequency (UHF, 850 - 950MHz, 2.4 - 2.5GHz, 5.8GHz)

Low frequency tags are cheaper than any of the higher frequency tags. They are fast enough for most applications, however for larger amounts of data the time a tag has to stay in a readers range will increase. Another advantage is that low frequency tags are least affected by the presence of fluids or metal. The disadvantage of such tags is their short reading range. The most common frequencies used for low frequency tags are 125 - 134.2 kHz and 140 - 148.5 kHz.

High frequency tags have higher transmission rates and ranges but also cost more than LF tags. Smart tags are the most common member of this group and they work at 13.56MHz.

UHF tags have the highest range of all tags. It ranges from 3-6 meters for passive tags and 30+ meters for active tags. In addition the transmission rate is also very high, which allows to read a single tag in a very short time. This feature is important where tagged entities are moving with a high speed and remain only for a short time in a readers range. UHF tags are also more expensive than any other tag and are severely affected by fluids and metal. Those properties make UHF mostly useful in automated toll collection systems. Typical frequencies are 868MHz (Europe), 915MHz (USA), 950MHz (Japan), and 2.45GHz. Frequencies for LF and HF tags are license exempt and can be used worldwide; however frequencies for UHF tags differ from country to country and require a permit[7][8][9].

2.3 Standards

The wide range of possible applications requires many different types of tags, often with conflicting goals (e.g. low cost vs. security). That is reflected in the number of standards. A short list of RFID standards follows: ISO 11784, ISO 11785, ISO 14223, ISO 10536, ISO 14443, ISO 15693, ISO 18000. Note that this list is not exhaustive. Since the RFID technology is not directly Internet related it is not surprising that there are no RFCs available. The recent hype around RFID technology has resulted in an explosion in patents. Currently there are over 1800 RFID related patents issued (from 1976 to 2001) and over 5700 patents describing RFID systems or applications are backlogged[10][11].

2.4 RFID Reader

RFID reader works as a central place for the RFID system. It reads tags data through the RFID antennas at a certain frequency. Basically, the reader is an electronic apparatus which produce and accept a radio signals. The antennas contains an attached reader, the reader translates the tags radio signals through antenna, depending on the tags capacity. The readers consist of a build-in anti-collision schemes and a single reader can operate on multiple frequencies. As a result, these readers are expected to collect or write data onto tag (in case) and pass to computer systems. For this purpose readers can be connected using RS-232, RS-485, and USB cable as wired options (called serial readers) and connect to the computer system. Also can use Wi-Fi as wireless options which also known as network readers. Readers are electronic devices which can be used as standalone or be integrated with other devices and the following components/hardware into it. Power for running reader, Communication interface, Microprocessor, Channels, Controller, Receiver, Transmitter, Memory[12][13].

e-ISSN: 2349-9745
p-ISSN: 2393-8161

III. WORKING OF SYSTEM

As we have seen above that three technologies are used in this system. These systems are doing their conventional work. Here, it is assumed that RFID sensors are sensing data at site. These sensors are smart enough to carry out some simple calculations. Based on these calculations it will be decided that these data need to be send via sms or not. This process will be done periodically or on basis of when a particular need this. Whatever may the time duration, if it is found that these data needs to be send via sms then following process will be carried out.

Here, we need a device which is connected to some network and it is having capability to send a short message. Here, we can assume that a mobile device with this minimum capacity is attached between these two RFID and SMS architecture and working as a bridge between them.

If system needs to send message then data is passed to this mobile device and now it is task to that device to send sms. This will be carried out using conventional architecture of sms.

IV. CONCLUSION

It can be concluded from above discussion that this architecture can be used in mainly moving applications. When intimations needs to be send on priority basis, specifically when there is a need to minimize the time, this system can be used. This setup mainly relies on existing infrastructure. On working system we can integrate this set up as we may have RFID sensors and SMS architecture ready with us. Only mobile device need to be integrated. So, it is also easy.

REFERENCES

[1] M. Gaderi, S. Keshav. Multimedia messaging service: system description and performance analysis. IEEE Explore. Wireless Internet, 2005. Proceedings. First International Conference on 10-14 July 2005,pages 198-205.

[2] Multimedia Messaging Service: System Description and Performance Analysi Majid Ghaderi and Srinivasan Keshav School of Computer Science University of Waterloo, Waterloo.

[3] Design of Multimedia Messaging Service for Mobile Telemedicine System Andik Setyono1, Md.Jahangir Alam2, and Raed Ali Al-Saqour Faculty of Information Technology

e-ISSN: 2349-9745
p-ISSN: 2393-8161

[4] Christoph Jechlitschek. A Survey Paper on Radio Frequency IDentification (RFID) Trends, Reports on Recent Advances in Networking

[5] Jerry Landt, "Shrouds of Time": outlines history and present of RFID: http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

[6] P. F. Baude, D. A. Ender, T. W. Kelley, M. A. Haase, D. V. Muyres, and S. D. Theiss, "Organic Semiconductor RFID Transponders", Electron Devices Meeting, 2003.

[7] S. Inoue and H. Yasuura, "RFID privacy using user-controllable uniqueness", in Proc. RFID Privacy Workshop, Nov. 2003. http://www.rfidprivacy.us/2003/papers/sozo_inoue.pdf

[8] M. Feldhofer, S. Dominikus, and J. Wolkerstofer, "Strong Authentication for RFID Using the AES Algorithm", Cryptographic Hardware and Embedded Systems 2004.

[9] K. P. Fishkin, S. Roy, and B. Jiang, "Some methods for privacy in RFID communication", in Proc. 1st Eur. Workshop on Security in Ad-Hoc and Sensor Networks, 2004

[10] D. Haehnel, W. Burgard, D. Fox, K. Fishkin, and M. Philipose, "Mapping and Localization with WID Technology", International Conference on Robotics & Automation, 2004.

[11] A. Juels, "Minimalistic Cryptography for Low-Cost RFID Tags", Security in Communication Networks 2004

[12] J. Krumm, E. Eckert, W. H. Glauert, A. Ullmann, W. Fix, and W. Clemens, "A Polymer Transistor Circuit Using PDHTT", Electron Device Letters, 2004

[13] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device", in Proc. 14th USENIX Security Symp., 2005, http://rfidanalysis.org/DSTbreak.pdf

