I-Voting System Using UHF RFID Technology

Dr. Indumathi J[1], Sharmila M[2], and T Raja[3]

[1]Associate Professor, [2]Research Scholar, [3]Research Scholar

Department of Information Science and Technology, College of Engineering,

Anna University, Chennai, India

Abstract :*This paper presents i-voting system using UHF Active RFID technology. The existing system was designed around HF passive RFID technology to make e-voting stations easier to use and also exposed to several attacks are relay attacks, jamming, blocking, selective denial of service and zapping, etc. The limitations are interrogation range of RFID tags away from nominal range, no mechanical interface and increases cost and reliability. To overcome all these issues, we propose i-voting system. i-voting means digital ID with PIN codes. Digital-ID is a document, which allows identifying a person in the electronic environment and giving digital signature. Digital-ID looks like an ID card, but without a user's photo it can only be used over the Internet. By using i-voting using Active RFID, to improve the read coverage is hundreds of meters.*

Keywords: *Mobile ID, Smart Card reader, GSM*

1. Introduction

Recent research perspectives in wireless technologies are Radio Frequency Identification and Wireless Sensor Networks that have wide variety of applications such as environmental monitoring, intelligent transport vehicles, parking access control, electronic security keys, people tracking, etc. and provide unlimited future potentials. People used one of the oldest method is using paper ballots to cast their votes in an election. The touch-based electronic voting machine is introduced which is the combination of paper based voting and direct optical scanning. GSM based Electronic Voting machine is possible through embedded system. RFID based electronic voting is the system in which the reader identifies the tag and connect to the computer software. Based on the classification of tags and readers, there are advantages and disadvantages by using RFID. The advantages are no line of sight, contactless smart cards to protect personal information. The disadvantages are very expensive, security and privacy is poor because the tags is easily traced out by the readers. There are variety of readers such as one port, two port, four port, fixed RFID, Handheld RFID, Mobile RFID, USB RFID and Wireless RFID readers [1].

2. Existing System

2.1 RFID based Electronic voting

RFID enables automatic identification of physical objects through electromagnetic transmission using a radio frequency compatible integrated circuit. RFID is based on automatic identification technology consists of unique identifiers. RFID mainly consists of reader and tag. The tag classified as active, passive, semi-active and semi-passive. The tag is bidirectional device which accepts and reflects electromagnetic signal to and fro from reader. If passive tag used means, the battery charges due to reflection signal from reader. Because the passive tag has no battery [5] [4]. The reader is an interrogator which also bidirectional one. The database contains all details of candidates along with their divisions. Each polling division have local database is which contains the people information on that division and their votes. After that completion of election, the main database is updated by each division local database.

http://dx.doi.org/10.17758/R615517

The frequencies used in RFID system are low frequency, High frequency Ultra High Frequency and microwave frequency. The low frequency ranges from 100-150kHz. The high frequency range is at 15MHz.

3. Problem Statement

The low frequency range used for animal identification applications. The high frequency range used in existing system is 13.78 M Hz. The distance coverage is 1m. The high frequency range is varied for the classification of RFID tags. For three different types of tags, the range is from 11 MHz to 15 M Hz. Each tag has different bit rate, power source, memory, read range, cost and life time. The solution for this issue is i-voting system used ultra high frequency. The ultra high frequency ranges from 700-900MHz. The read range capability is approximately 3m. Each tag has different read range. The passive tag read range is approximately 2m. The active tag read coverage is around 3m. The semi-passive tag read range is less than 2m. Among these classifications active tag using UHF read coverage is around 3m. RFID attacks are zapping, jamming, blocking, denial of service and relay attacks. Among these attacks zapping is mainly affect the RF front end of RFID tags carried out by apply high power pulse apply next to the tag. This pulse permanently disabling the tags. This attack mostly affect active tags.

4. Proposed system

4.1 Methodology

Tag combines the carrier signal generated by a local oscillator and reference signal. This is the signal which enables tag to select ultra high frequency using one of the modulation techniques such as amplitude shift keying, phase shift keying and frequency shift keying depending upon application. Depending upon the transmit power, filter and amplification using modulator, the receiver sensitivity is increased. So the read coverage of the tag is improved [2] [3].

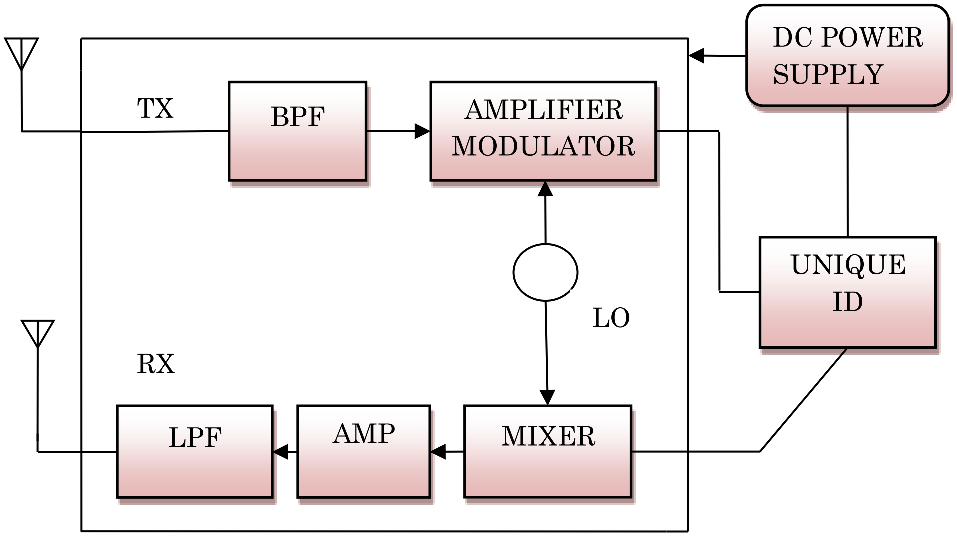

Fig.1. Block diagram of UHF Active tag

There are different ways to identify a person and to give the digital signature by means of ID card with PIN codes, Digital ID and Mobile ID. If PIN codes are lost, new ones may be requested from service points of Citizenship [6]. The assets required for I-voting using ID are Computer with Internet connection, Smart card reader and ID card software. The stages of I-voting by means of ID card are

- Voter inserts ID card into the card reader
- Opens the I-voting website

- Downloads and runs voter application
- Identifies himself/herself by entering unique ID code
- The list of candidates of the voter's electoral division shall be displayed
- Voter makes the choice
- Voter confirms his/her choice by digital signature (by entering unique ID code)
- Receives a notice that the vote has been accepted.

By means of Mobile-ID SIM card with unique codes. The assets are Computer with Internet connection and Mobile phone. There is no need to install a card reader on the computer and special software. The mobile phone with the respective SIM card performs the functions of the card and card reader simultaneously. Mobile-ID must be activated by ID card prior to use.

The stages of I-voting if mobile-ID is used:

- Voter opens the I-voting website.
- Downloads and runs voter application
- Enters his/her mobile number into the application
- Identifies himself/herself by entering in the mobile phone the mobile-ID PIN1 code (control code is sent to the mobile phone by SMS)
- Consolidated list of candidates in the electoral division of the residence of the voter shall be displayed to the voter on the computer screen
- Voter makes his/her choice with the computer
- Confirms his/her choice by digital signature, entering in the mobile phone the mobile-ID PIN2 code (control code is sent to you mobile phone by SMS)
- Receives a notice screen that the vote has been accepted.

Mobile-ID allows a person to be identified and give digital signatures but at the moment it is not possible to vote by using a mobile phone, a computer with Internet connection is also needed [6].

5. Conclusion

While it can take very long time to accept e-voting system because of technical problems. Re-voting is one of the major issue in e-voting system. Also zapping, jamming and relay attacks also defined. If properly implement the voting machine means, mitigate these issues. Non-technical error can also be eliminated. Range of passive UHF RFID systems is limited by such factors as tag characteristics, propagation environment, and RFID reader parameters. The i-voting system uses UHF Active RFID which improves the read range and also avoid zapping attacks.

6. References

[1] Carter Center, ‘Developing a Methodology for Observing Electronic Voting’, 2007, available at <http://www.cartercenter.org/documents/elec_voting_oct11_07.pdf>

[2] Organization of American States, ‘Observing the Use of Electoral Technologies’, 2010.

[3] Organization for Security and Co-operation in Europe, Office for Democratic Institutions and Human Rights, ‘In Preparation of Guidelines for the Observation of Electronic Voting’, October 2008, Pran, Vladimir and Merloe, Patrick,Monitoring Electronic Technologies in Electoral Processes’, National Democratic Institute, 2007.

[4] Vollan, Kåre, ‘Observing Electronic Voting’, Norwegian Centre for Human Rights, 2005.

[5] M. Hutter, J.-M. Schmidt, and T. Plos., "RFID and its vulnerability to faults" , in *Proceedings of the 10th international workshop on Cryptographic Hardware and Embedded Systems*, pages 363–379, Berlin, Heidelberg, 2008. Springer-Verlag.
http://dx.doi.org/10.1007/978-3-540-85053-3_23

[6] Mazidi and Mazidi, The 8051 Microcontroller and Embedded Systems, Prentice Hall, 2000.

http://dx.doi.org/10.17758/R615517