International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 4 Issue 5 || May 2015 || PP.71-79

Monitoring and Centering a Remote Discrete Using Rfid through Sim Module

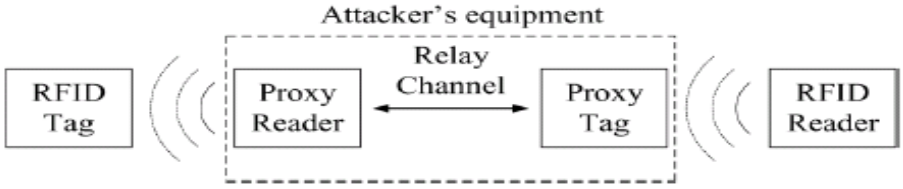
[1]K.Naga Akhilesh , [2]R.China Appala Naidu
[1,2]St Martin's Engineering College- Dhulapally Hyderabad, Telangana India -500014

Abstract: *A need for implementing and monitoring the students in a campus or university during session hours has become a priority in educational institutions in our nation. The basic emphasis is on the current location of the discrete. In this paper, we focus the presence of the candidate/student using RFID tag and sending a short message service using subscriber identity module to a registered mobile. The administrator can monitor the moments of the candidate by reading the tags with the reader. Monitoring the candidates is related to the network reliability at the readers.*

Keywords: *Discrete location, RFID Tags, RFID Readers, SIM module*

I. INTRODUCTION

The presence of a discrete within a campus is increasing the concern for the campus administrations. As significance a model being designed through a wireless communication through RFID'S. Our prototype is designed in such a way that the devices are within the communication range. The operational range of typically RFID tags used in this application is between 10cms – 15cms. For higher frequency tags there are up to 10 meters and for ultra frequency they are UHF devices. It is considered that the readers manage to communicate with the tags with the close physical proximity of the location of the reader. The aspect of this paper is the highlights of the RFID tags and the readers of a practical implementation in campus monitoring .Basically this idea is developed from the concept of distance bounding. Distance bounding protocols prevented distance fraud, mafia fraud and terrorist fraud. The reader operates on assuming that the RFID tag is in a close proximity based on the RFID system. The proxy tag doesn't need to authenticate itself to the reader as the authentication is relied on the original tag. With the help of this proxy tags when the attacker moves the valuable item it can be detected without the knowledge of mafia. A diagrammatical representation of the above practical demonstration of mafia fraud is designed below.



The SIM module here used is referred as SIM900 module which is capable to send the data in a two way direction. In one direction it sends the data to a registered mobile and in another direction it sends the data will be pooled at a server. When the data by the tag is once read by the RFID reader it keeps a track of all the tags which are passing through and sends the data to the server. Each time the administrator refreshes the website he can view the track of the tags.

In the previous system the reader can only find the tag in its physical proximity. So in a hostile environment, when the fraudulent device enters, it pretends to be the neighbour and will adversely the intended services. So due to this the administrator will not be constantly having an awareness of the devices/tags in the location. Here the manpower may be in a increasing because for each and every time the administrator wants to know the tags in his location, he need to refresh the website. There may more time complexity in tracking the tags which depends upon the network availability in the readers.
But our system does not allow a fraudulent device to be its neighbour, and tracks each and every tag in its network and intimates to the administrator through SIM module accurately. So the administrator may have a facility to be aware of the tags even when the server couldn't respond properly. The location of the tags can be accurately found out by administrator remotely if he can handle a mobile phone. The time complexity in locating the device through SIM module may be more than the data pooling from the server.

II. RESEARCH METHODOLOGY

This study is comprised of a descriptive study of research. The technique that was used under descriptive method is the normative survey approach and evaluation, which is commonly used to explore RFID tags in a certain perspective location where the tags move voluntarily. The architecture of our approach is seen below.

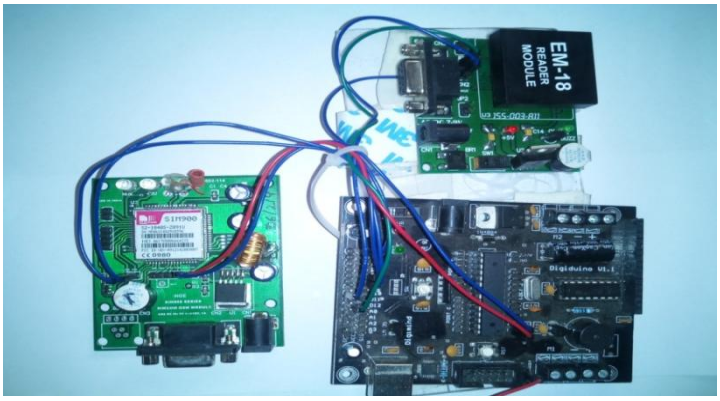


Fig1: System architectural image

RFID Reader:

Fig2: RFID reader

An RFID reader's function is based upon the RFID tags. The means of data transmission is wireless and because the distance between the tag and reader is relatively short. It contains an Radio Frequency module, which acts as both a transmitter and receiver. There will be an oscillator in this transmitter to create the carrier frequency; and also it contains a modulator which strikes data commands and also an amplifier to increase the signal for processing the tags. The receiver has a demodulator which takes the data. There will be a microprocessor which acts as the control unit and also it will store the data. This data can be sent to the network.

Frequencies

Generally between the readers and tags the data will be carried by the radio waves .This approach can be adopted to allocate frequencies depending on application. Some specific ranges are discussed here:

Low Frequency (LF) will be ranging from 125 - 135 kHz.

High Frequency (HF) will be ranging from 13.56 MHz.

Ultra High Frequency (UHF) will be ranging from 400 -1200 MHz.

The allocation of frequencies is administered by different government agencies, based on RFID applications in different countries. Since security access, asset tracking and animal identification have short reading ranges and lower system costs they are done in mostly the low frequency systems. Whereas high-frequency systems maintain long reading ranges and high reading speeds they are used for applications like railroad car tracking and automated toll collection. But it results in higher costs. Environmental conditions, generally at the higher frequencies, can also depend upon the range of communication.

DIGIDUINO:

Digiduino is basically a development hardware board which is developed to do efficient projects for most of the real-time applications. It is same as Arduino which is technically more advanced and developed. User gets a dual experience in a single hardware module because it has both the features of Arduino and Atmel AVR.

Arduino + AVR=Digiduino

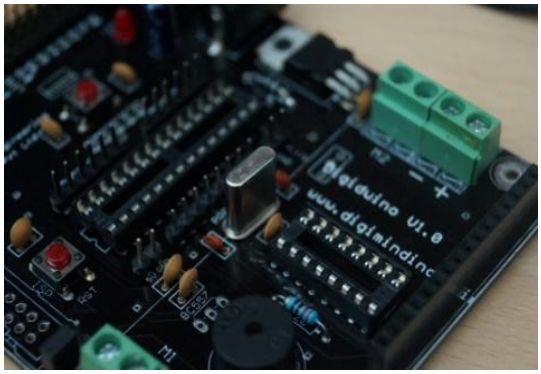
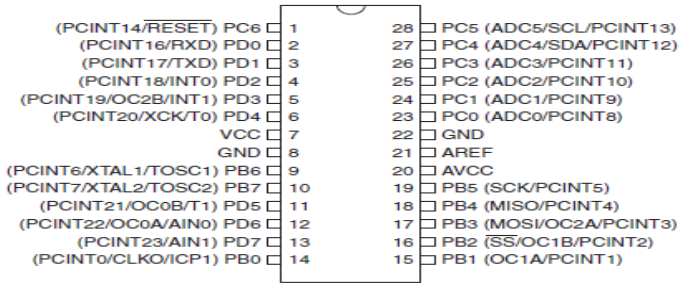


Fig3: Digiduino board

Feature	**Digiduino**
Form Factor	Average
Operating Voltage	3.5V to 5.5V
Minimum Voltage, Current & Maximum Voltage, Current	7.5V,1A – 36V,8A
Power Mode	USB, ISP, Adaptor, Battery
General Purpose Digital IO Pins	23 – AVR Operations 13 – Arduino

Pin configurations:



Specifications

- High Performance, Low Power AVR 8-Bit Microcontroller
- Advanced RISC Architecture
- High Endurance Non-volatile Memory Segments
- Temperature Measurement
- Special Microcontroller Features
- I/O and Packages
- Operating Voltage:
  – 2.7V - 5.5V for ATmega328P
- Temperature Range:
  – Automotive Temperature Range: -40°C to +125°C

Advantages:

- Uniquely designed for ease of access
- Reliable and Feasible
- Dual platform
- Open source hardware and software

SIM900 MODULE:

Fig4: SIM900 module

The SIM900 is a Quad-band GSM/GPRS solution in a SMT module which is used to develop real-time applications. SIM900 module provides GSM/GPRS 850/900/1800/1900MHz performance less power consumption. SIM900 is of size 24mm x 24mm x 3 mm, and can be used for mobile to mobile communications. There will be a powerful single-chip processor integrating AMR926EJ-S core in SIM900.This Quad - band GSM module will be approx. size of 24mmx24mmx3mm.

SIM system is assembled on SIM900 Mainframe platform. Power source, interfaces of computer, clock synchronization, and each and every module status are enabled on this mainframe. A RS-232 host interface and ADLINK GPIB interface card (IEEE-488.2) are designed on this mainframe. All commands to each and every module are routed through this mainframe host interface. Messages are transferred depending on their port number; the mainframe sends data to and from the certain destination. Two auxiliary RS-232 ports are communicated through this messaging system. Through these ports, any number of SIM900 mainframes and RS-232 instruments can be controlled from one host interface in the mainframe. In non-volatile memory of the SIM900 a 4000 byte start-up script is stored. When it is enabled, all the commands stored in this script are executed for each and every time the mainframe is turned on. This can ensure that for a desired starting configuration all the modules are automatically set. All modules can access various powers at ±5 V, ±15 V and +24 V. mainframe power supplies well regulated and filtered DC voltages which maintain stable performance.

RFID Tags:

Fig5: RFIG tag

An Radio Frequency Identification tag is a microchip which contains an antenna in a compact package. T o make a RFID tag to be attached with an object which is to be tracked this packaging is designed. The antenna receives the signals from an RFID reader and then sends the signal (like a unique serial number or other generalized information). RFID tags are very small in size from a large rice grain to a small paperback book.

Active Tag

A RFID tag is an active tag contains a battery that can be used for tag's circuitry and antenna as a power source. Some of these tags may contain rechargeable batteries others may be sealed units.

Advantages

- Depending on large frequencies it can be read remotely.
- It may contain sensors that can use electricity for power.

Disadvantages

- These tags are typically more expensive, and they need a power source.
- The tag is physically larger, which may cause limit to many real-time applications.
- The maintenance costs of these tags are greater than those of a passive.

Passive Tag

These tags do not contain a battery source. When radio waves from the reader are received by these tags, the antenna coiled within the tag forms a magnetic field. Then the tag gets power from it, boosting the circuits and sends the information encoded into the tag memory.

Disadvantages

- This type of tags can be accessible at very short distances which probably may limit the certain applications.
- It is not possible to include sensors to these tags that can use electricity for power.
- These tags remain readable even after the device to which the tag is attached is no longer being tracked for a very long time.
-

Advantages

- These tags work without a battery and much less expensive.
- These tags are smaller and may be they can be in the size of a grain of rice also.
- These tags have almost been deployed in consumer goods and other areas.

Working process:

When a tag is being swiped through the RFID reader the data will be impacted at the SIM module and it sends the data to the registered mobile and at the same time it populates the data at the server depending upon the network situation.

Propagation of data

The VCC and GND of RFID reader are connected to the VCC AND GND of digiduino board. In the same way the VCC and GND of SIM900 are connected to the VCC AND GND of digiduino board. The reader contains TX (transmission) and ports. This port is connected to D0 bit of digiduino board. The bits D4 and D5 will transmit the data which is received from the reader to the SIM module to its RX and TX data pins. The SIM module has a two way direction of transmitting the data. In one direction it transmits to a respective network through which it propagates the data to the registered mobile. In other way it sends the data to the server where the data will be populated.

III. RESULTS

On the basis of the modules used which are discussed in the above methodologies we had found out some few iterations.

Data extracted from room1:

Fig6: Message from tag1

Data extracted from room2:

Fig7: Message from tag2

Data extracted from room3:

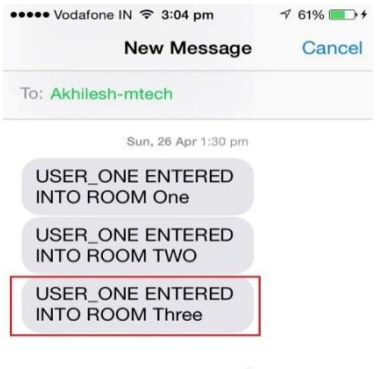


Fig8: Message from tag3

Data extracted from intruder:

Fig9: Message from intruder

Data pooled from server:

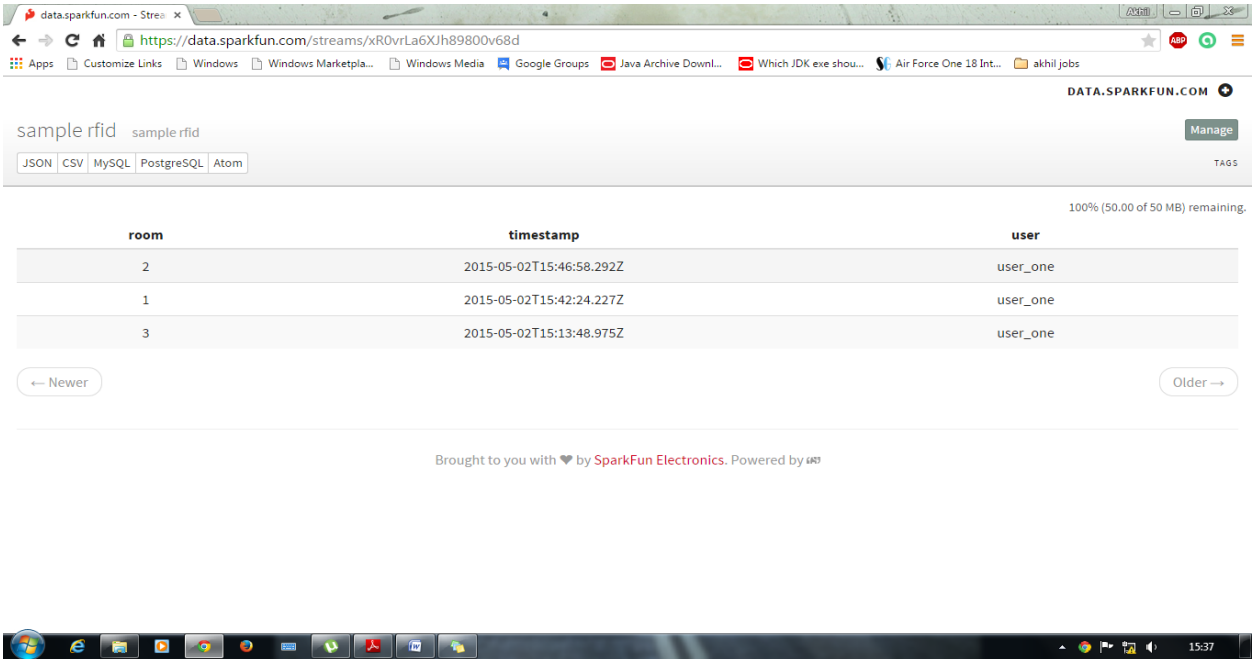


Fig10: Data at the server

This data is populated as soon as the tag reads the reader and it will be pooled at the respective server. The administrator can keep a track of discrete through this webpage.

FEW ESTIMATED GRAPHS AND TABLES:

TABLE 1: FREQUENCY V/S DATA ACCESSABILITY

Frequency	Data Accessibility
0.5	2
0.7	3
1	4

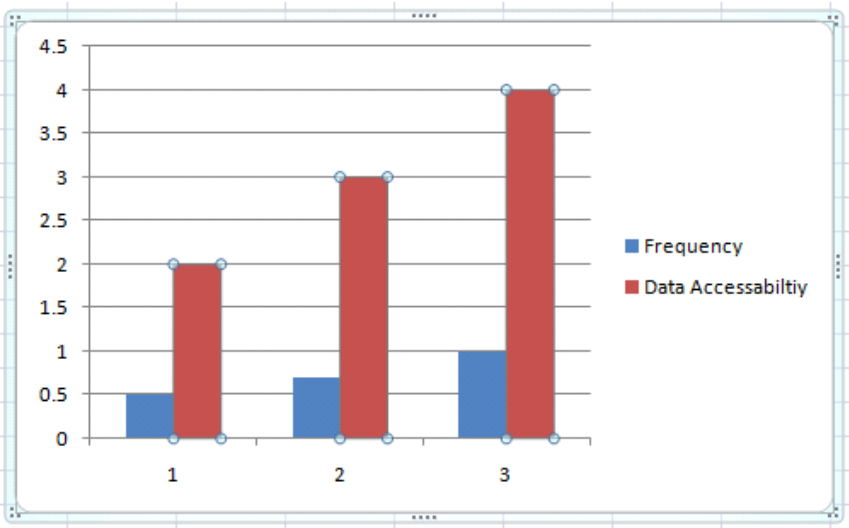


FIG 11: A GRAPH ON FREQUENCY AND DATA ACCESSIBILTIY
(LOW CONDITION)

TABLE 2:FREQUENCY V/S DATA ACCESSABILITY

Frequency	Data Accessibility
1	4
2	5
3	6

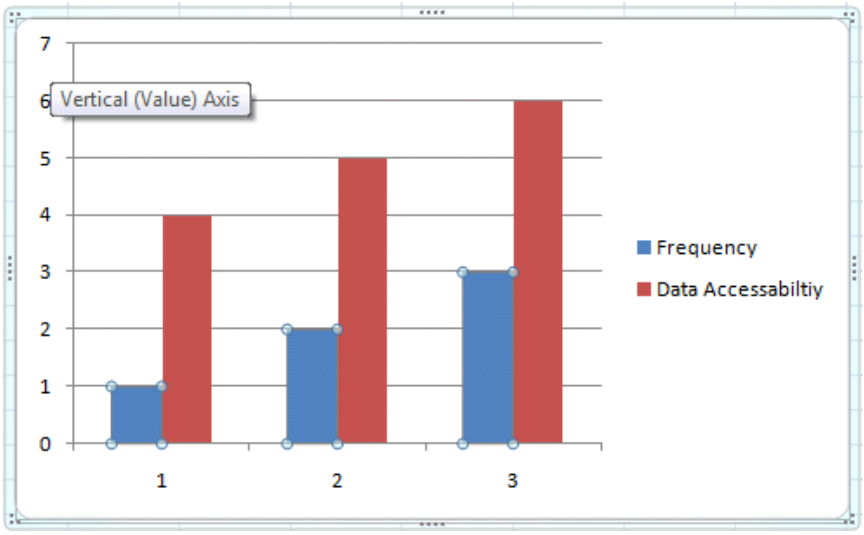


FIG 12: A GRAPH ON FREQUENCY AND DATA ACCESSIBILTIY
(MODRATE CONDITION)

TABLE 3: FREQUENCY V/S DATA ACCESSABILITY

Frequency	Data Accessibility
3	6
5	8
6	11

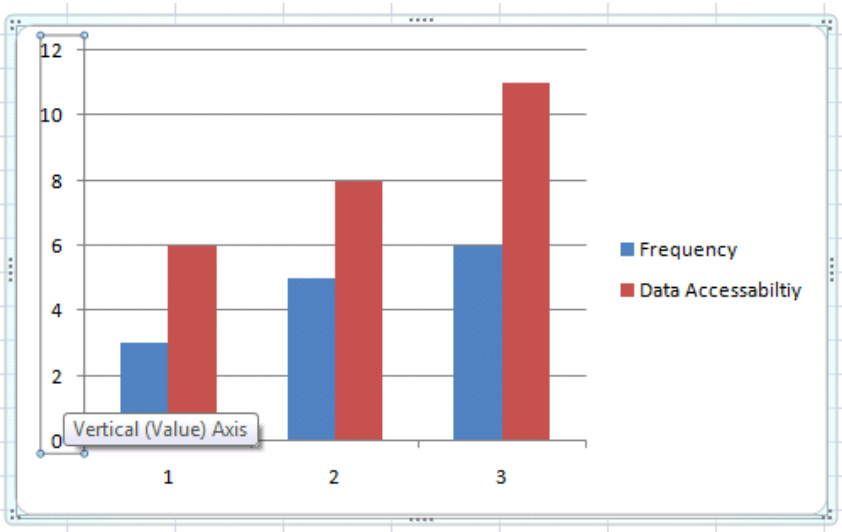


FIG 13: A GRAPH ON FREQUENCY AND DATA ACCESSIBILTIY
(HIGH CONDITION)

TABLE 4: FREQUENCY V/S DISTANCE

Frequency	Distance
1	4
3	8
9	15

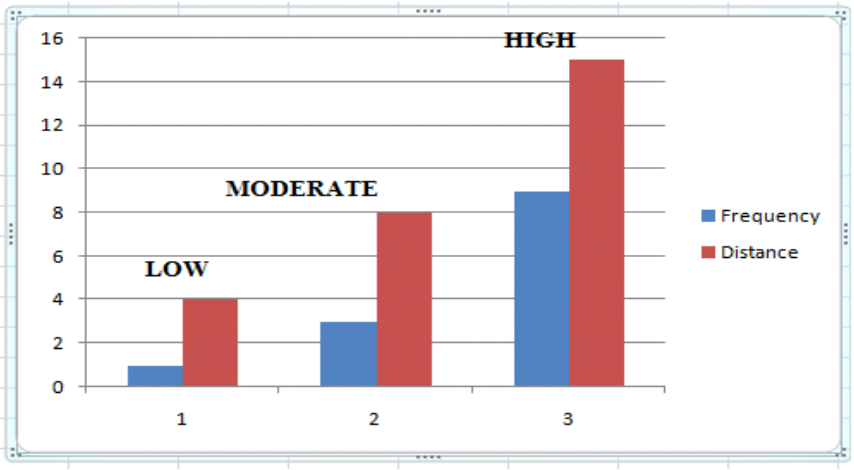


FIG 14: GRAPH ON FREQUENCY V/S DISTANCE

"WHEN THE FREQUENCY OF RFID READER IS HIGH THEN CAPABILITY TO ACCESS DATA FROM A RFID TAG AT A LONGER DISTANCE IS POSSIBLE"

IV. CONCLUSION

Since it has become more crucial and the need for adequate resources for tracking a person in a remote location, our emulation will be helpful to find track the discrete. We could provide enough resources to the tracker to get immediate response remotely. This evaluation of a sample set of protocol proposals using the above modules enhanced that the practical requirements with consideration of hardware cost, energy efficiency, and execution time are more reasonable for remote monitoring implementation. Mainly in this study we can observe that the administrator can have a track of discrete even when he is not reachable to his personal computer. So our proposed paper added a benefit to the tracker to go mobile anywhere and beware of discrete.

REFERENCES

[1]. G. P. Hancke, "RFID and Contactless Technology," in *Smart Cards Tokens, Security and Applications.*
[2]. D'Souza, M. Wei, and C. Notobartolo, "Real-time location systems for hospital emergency response,".
[3]. G. P. Hancke, "Design of a secure distance-bounding channel for RFID,".
[4]. S. Han, H.-S. Lim, and J.-M. Lee, "An efficient localization scheme for a differential-driving mobile robot based on RFID system,".
[5]. D. Lui, M.-C. Lee, and D. Wu, "A node-to-node location verification method,"
[6]. G. Avoine and A. Tchamkerten, "An efficient distance bounding RFID authentication protocol: Balancing false-acceptance rate and memory requirement,".
[7]. W. Granzer, F. Praus, andW.Kastner, "Security in building automation systems,".
[8]. Y. Wu, G. Buttazzo, E. Bini, and A. Cervin, "Parameter selection for real-time controllers in resource-constrained systems,".
[9]. N. O. Tippenhauer and S. Capkun, "ID-based secure distance bounding and localization,"