



NFC Based Vehicular Involuntary Communication System

Dipak P. Patil

Associate Professor, HOD E&TC

Sandip Institute of Engineering and Management
Nashik, India

Priyanka V. Ahire

Assistant Professor in E&TC Department

Sandip Institute of Engineering and Management
Nashik, India

Swapnil R. Kurkute

Assistant Professor in E&TC Department

Sandip Institute of Engineering and Management
Nashik, India

Pratikha D. Nandanvar

Assistant Professor in Electronics Department

Shri Ramdeobaba College of Engineering and Management
Nagpur, India

Abstract: In this paper independent model for vehicular communication is presented which is based on Near Field Communication (NFC) technology. Recent trends in the manufactures of the smart phone signify both the increasing popularity and great potential for increased use of NFC in today's society. As a result of NFC has a huge potential to simplify our everyday tasks, ranging from paying for the items and to have accessing of our office or home devices. This system proposes the design and construction of an advanced car system using NFC technology. It is going to perform various functions that will enhance the car system. The main objective of this proposed system is to develop advanced car door lock. It uses the NFC enabled mobile to access the car door lock with the help of NFC reader module. The control and communication between the user and the proposed system can be achieved through a NFC reader NFC enabled mobile. By implementing this idea it won't be easier for thief to access the door lock of car. The user could easily protect and control their car as it can be only limited to his or her NFC enabled mobile phone. It also includes the implementation of driver health monitoring system. This system makes use of Arduino along with NFC.

Keywords: Near Field Communication (NFC) technology, NFC reader module, NFC enabled mobile/tags, Arduino UNO R3.

I. INTRODUCTION

Now-days the mobile communication is the most important for all type of interactions, so it is expected that in the future most of the mobile devices will be outfitted with an NFC interface. NFC is a set of communication protocols that enable two electronic devices, one of which is portable such as smart phone, to establish a communication by bringing them within a short distance. In this era we will found that most of the vehicles are coming with most of the advancement into their system. Perhaps the scenario behind all that system is very costly, which can't be easily affordable to the ordinary vehicle user. We will also be using the term Tap and ready to go because it clearly conveys a visual image in which this technology is intended to be used. By keeping that in mind we are supposing this system to reduce the cost that is involved in developing this kind of system. The proposed system will enhance the normal vehicle with bit cost to make it advanced vehicle system.

The existing vehicles anti theft systems are of no more use now days. Already many companies and vehicle manufacturer that uses Global Positioning System based location tracking to track the stolen vehicles does not work well under indoor parking and many different areas. Most vehicles are still using the conventional alarm system which is got common and easily handled by car thief. The people little interest in the vehicle alarms since they could be falsely triggered. It's because the technology is growing very speedily so it is necessary to withstand to the new technology and make proper use of it. Even if some secure system come into the market is for high end vehicles. In ordinary vehicle it's not possible to adopt such things at

such high rate. So it's necessary to have high end technologies in small scale vehicles at efficient rate in efficient ways.

The overall system divided into four objectives

- Design and implement vehicular communication and automation system.
- Enhance the security of vehicle system.
- To adopt the new technology at efficient rate in small scale vehicles.
- Keep the track of driver health system.

II. LITERATURE REVIEW

In 2002, NFC was developed by NXP (Philips) Semiconductors and Sony. In general, because NFC is an evolution of RFID and smartcard technology, it is compatible with most surviving RFID and contactless smartcard systems, but its architecture is different in principle. While RFID and contactless smartcards have a reader/tag structure, an NFC device can be both reader and transmitter. An NFC Data Exchange Format was specified to ensure RFID tags and contactless smartcards are congenial with NFC applications. A key diagnostic of NFC is that its wireless communication interface usually has a working distance limit of about 10cm. The details of NFC can be found in ISO 18092 [1]. In 2004, The Near Field Communication (NFC) forum was formed to promote and supervise the use of the NFC technology.[10]

It was reported that as many one thousand cars were stolen monthly in Malaysia in the year 2007. The existing vehicle alarm systems are of no match to the well-equipped thievery. In the United States, there are already many transportation companies and vehicle manufacturers

industries that employ Global Positioning System (GPS) based location and tracking system combined with conventional mobile communication for stolen vehicle recovery as well as for constant monitoring of vehicle fast management. However there are situation where the GPS system cannot perform well such as at underpasses and indoor parking. Most cars or bikes are still using the conventional alarm system which is easily handled by car thief. One major problem in those car or bikes alarms is tuning and adjustment. There may be so many car alarms that are too sensitive, while the rest can withstand a main seismic disturbance without a single beep. Consequently, the public loose interest in the car alarms since they could be incorrectly triggered. Another weak point is that, it has limited capability to interact with its owner. NFC compliant electrical device NFC is a “proximity card” technology relying on the smart card standard ISO (International Standard Organization) 14443[3] and allowing wireless transactions only over a minimum distance of up to 10 centimetres [5]

The increasing computing and storage capabilities, the large number and variety of apps available on app stores and new wireless communication interfaces, such as Near Field Communication, provide many deployment possibilities for smart phones, including electronic ticketing, payment and access control. In particular, the NFC interface is a well suited for such applications due to its short minimum communication range (few centimeters) providing basic assurance of the user’s physical proximity [2].

Smart phone based immobilizer systems promise to raise the user experience by providing a variety of appealing new features and enabling flexible applications beyond what is provided nowadays by conventional transponder based immobilizer system. They do not require user to obtain a physical transponder but allow them to use their smart phones to remotely obtain electronic car keys. Moreover, access rights can be de assign to other users, bound to specific policies. In particular, self-propelling applications with a highly dynamic or large set of users, such as car sharing and fleet management, can highly benefit from smart phone based immobilizers [1].

NFC is a short range (up to 10mm) and standardized (ISO 18092)[8] wireless communication technology that adds contact less functionality to mobile devices including mobile (smart) phones and PDA’s (Personal Digital Assistants). Such devices can act both as a “contactless card” (based on its secure element reader and as a “contactless reader” and also operate in P2P mode with peer devices. These devices support various type of contactless communication standards, such as ISO 14443[9], ISO 15693 [8], FeliCa and Mifare Standard.

The technology used in NFC is compatible with existing contactless infrastructure and NFC device offers three operating modes.

a) *Reader/Writer mode*: In this mode the NFC device can read or write information such as URLs, SMS’s in a tag or smart card e.g. Smart posters applications. Here, users touch the device or a cell phone with the tag embedded in the poster, which triggers the transmission of a URL to the phone. The URL could be used to open the web browser without any human intervention.

b) *Card Emulation mode*: In this mode the NFC enabled device emulates a contactless smartcard (ISO 14443). In this case there is a secure element embedded in the device where

sensitive data can be stored in a safe place and value added services requiring a high level of security such as payment applications can be made available to the customers.

c) *Peer-to-Peer mode*: In this mode a connection is established between two NFC enabled devices and data can be exchanged between them. The NDEF (NFC Data Exchange format) is used to transmit data. This mode is standardized on ISO 18092.

III. SYSTEM MODEL

A. System Implementation

The implemented system is basically divided into two parts first NFC communication authentication and second automation. Near Field Communication is a short- rang high frequency 13.56 MHz technology that allows mobile devices to actively interact with passive objects and other active mobile devices, connecting the physical world to mobile services in ways that empower and benefit users. The automation is used to enhance the security of vehicle in terms of access to vehicle system by sensing the physical parameters of the vehicle driver carried out using an Arduino Uno R3 module. The figure shows the overall block diagram of system implementation and conceptual understanding of how the system is going to be worked out. In this diagram the system is working in the aspects of communication and automation. Communication is deployed by NFC enabled mobile and NFC reader module. The NFC enabled mobile can be replaced by Mifare cards, NFC tags or NFC enabled devices. The NFC reader module will work on to the signal which is needed to be sensed by the reader from corresponding devices. Circuit diagram was design and implemented on PCB by following and avoiding faults stated in [4]

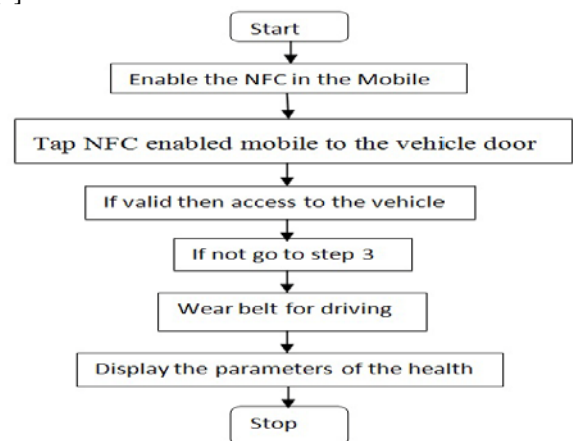


Fig. 1: System Workflow

B. Arduino-Uno

GSM Technology can be used for wireless communication [9][6] but it is a having some drawbacks so for experimentation we are going to use *Arduino*. Arduino is a hardware and software project and user community that designs and manufactures computer open-source hardware, open-source software, and microcontroller-based kits for building digital devices and interactive objects that can sense and control physical devices. These systems provide sets of digital and analog Input/output (I/O) pins that can interface to various expansion boards (termed shields) and other circuits.

C. NFC Architecture

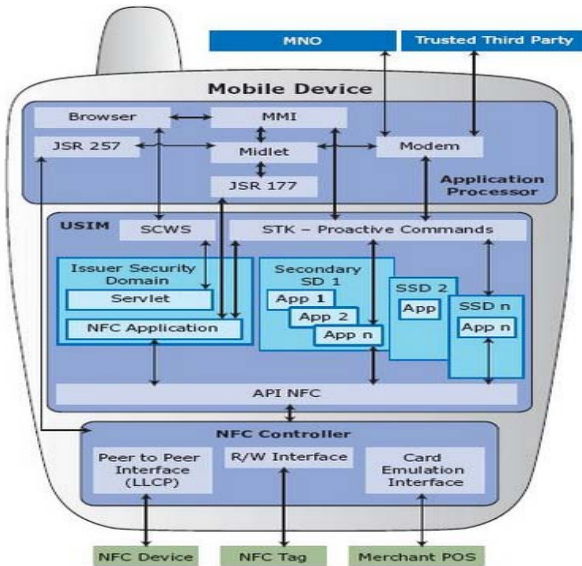


Fig. 2: Architecture of NFC integrated in a mobile device

NFC technology integrated in a mobile device consists of two integrated circuits. SE's and an NFC interface. The NFC interface is composed of a contactless; analog/digital front-end called an NFC Contactless Front-end (NFC CLF), an NFC antenna and an IC called an NFC controller to enable NFC transactions.

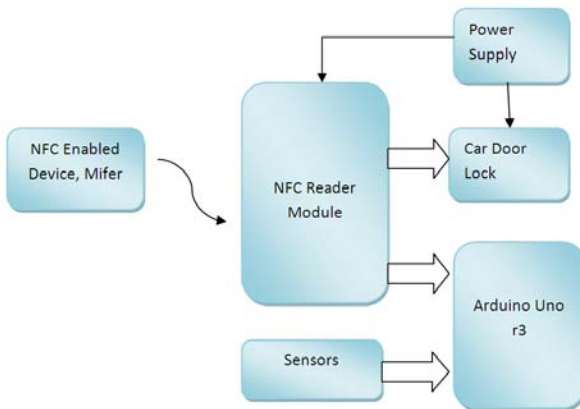


Fig. 3: NFC integrated Module

Figure 3 shows NFC integrated module with actual block representation of system implementation. The main advantage of NFC over Bluetooth is that NFC requires much low power consumption than the new Bluetooth 4.0 as well. This lower power consumption also has drawback of shorter range than Bluetooth. NFC has a range of around 10 cm while Bluetooth can transmit data up to 10 meters or more. When it comes to speed, NFC has faster connectivity. As NFC uses inductive coupling and there is no manual pairing, it takes not more than one tenth of a second for a connection between two devices. [9]

The NFC Controller is required for the analog digital conversion of the signals transferred over the proximity connection. Apart from an NFC controller, an NFC enabled mobile phone has at least one SE which is connected to the NFC controller for performing secure proximity transactions with external NFC devices (e.g. payment at POS) through Single-Wire Protocol (SWP). The SE provides a dynamic and secure environment for programs and data. The secure

element is also called as tag emulation operating mode. Host Controller Interface (HCI) creates a bridge between the NFC controller and the host controller. The host controller sets the operating modes of the NFC controller through the HCI, processes data that are sent and received, and establishes a connection between the NFC controller and the SE. Also, host controller is able to exchange data with the secure element (internal mode).

D. NFC Tag

An NFC tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product. It can store data in NDEF format. [11].The following figure illustrates the NFC Services architecture. It works on client-server architecture and has four Main components - NFC applications, NFC client, NFC server and NFC libraries.

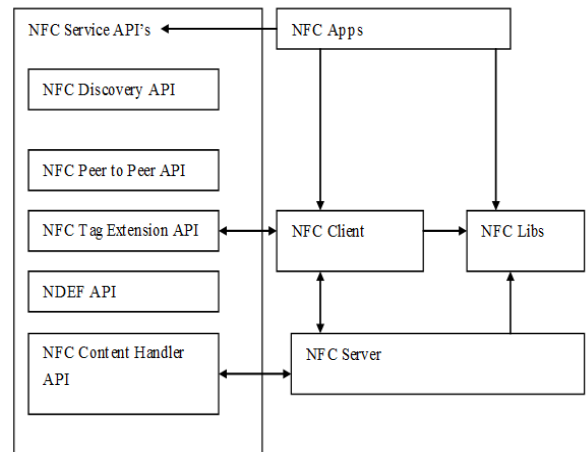


Fig. 4: Main components - NFC applications, NFC client, NFC server and NFC libraries.

E. System experimentation

For the implementation first one enable the NFC system in the mobile or electronic devices having NFC tags. NFC equipped smart phones can be paired with NFC tags which we implement on vehicle door. NFC enabled mobile tap on the vehicle door no pairing code necessary to link up, if the user is authenticated then access the vehicle otherwise it's not give the access for device. Next condition is wear the seat belt enforced to the driver. Once the car started the health parameters such as body temperature are shown on display of the vehicle.

F. System implementation

Circuit diagram was design and implemented on PCB by following and avoiding faults stated in [4]

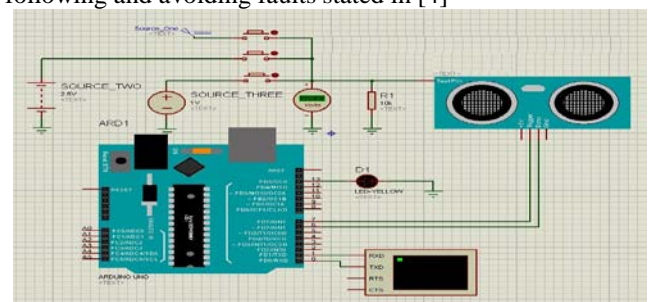
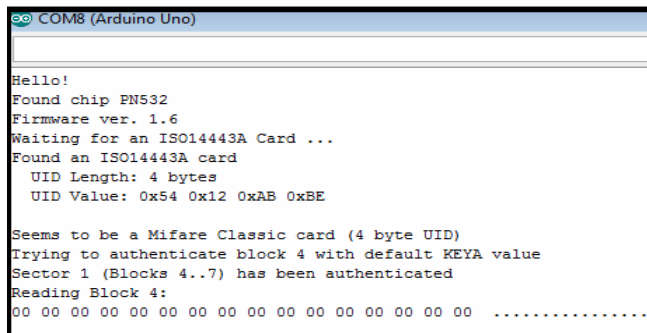


Fig 5: Simulation Arduino with sensor

Simulation can also be done using LAB VIEW software as it is also advance software with advance features [7].

IV. RESULT DISCUSSION

As user insert the card system will authenticate the card if it is authenticated the message will displayed as Found an ISO14443A card, it will also display the technical specifications of UID and authentication.



```

COM8 (Arduino Uno)
Hello!
Found chip PN532
Firmware ver. 1.6
Waiting for an ISO14443A Card ...
Found an ISO14443A card
UID Length: 4 bytes
UID Value: 0x54 0x12 0xAB 0xBE

Seems to be a Mifare Classic card (4 byte UID)
Trying to authenticate block 4 with default KEYA value
Sector 1 (Blocks 4..7) has been authenticated
Reading Block 4:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Fig 6. Output window of NFC

V. CONCLUSION

In this paper independent model for vehicular communication is presented which is based on Near Field Communication (NFC) technology. Vehicular communication and automation is basically aimed for providing the high technology solution that doesn't exist in normal vehicle system. Different types of sensors can be used by interfacing with Arduino to improve security systems. In this paper temperature and ultrasonic sensors are used for demonstration. In most of the reviews generally it is found that most of the manufacturing systems are working for providing real time security system to the vehicles. The project attempted to provide a possible explanation of the factor that triggers the theft of vehicles. It focuses on attitude towards accessing the vehicle system. It also combines the concept of communication and automation in case of vehicle system with high end technology.

VI. REFERENCES

- [1] International Organization for Standardization. Near Field Communication – Interface and Protocol (NFCIP-1).ISO/IEC 14443.2009.
- [2] Gerald Madlmayr, Josef Langer, “*Managing an NFC Ecosystem*”, IEEE 7th International Conference on Mobile Business ICMB 2008.
- [3] ISO/IEC 14443, “*Identification cards Contactless integrated circuits cards Proximity cards*”, <http://www.iso.org/>.
- [4] S. R. Kurkute, P. N. Kakrale, S. S. Kale , A. S. Kudav, “*PCB Quality Monitoring*”, International Journal of Modern Embedded System (IJMES), ISSN: 2320-9003(Online), Volume No.-5, Issue No.-1, Page No-13-16, February, 2017
- [5] ISO/IEC 15693, “*Identification cards-Contactless integrated circuits cards-Vicinity cards*”, <http://www.iso.org/>.
- [6] S. R. Kurkute, C. Medhe, A. Revgade, and A. Kshirsagar. "Automatic ration distribution system—A Review." In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on, pp. 11-13. IEEE, 2016.
- [7] S. R. Kurkute, K. P. Arbuji, C. R. Dargude, K. D. Dholi, “*Laboratory Virtual Instrument Engineering Workbench (LABVIEW)*”, International Journal of Modern Embedded System (IJMES), ISSN: 2320-9003(Online), Volume No.-5, Issue No.-1, February, 2017, Page No-17-20
- [8] Gerald Madlmayr, Josef Langer, Christian Kantner,Josef Scharinger, “*NFC Devices: Security and Privacy*” IEEE Proc. Intl. Conf. on availability, reliability and Security.2008.
- [9] V.Patil , N. Varma, S. Vinchurkar, B. Patil “*NFC Based Health Monitoring And Controlling System*” 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN) Page No-133-137
- [10] R. Marie and Marc Pasquet, “*Promising Secure Element Alternatives for NFC Technology.*” IEEE International Workshop on Near Field Communication 2009.
- [11] Roland, Michael, and Josef Langer. "Digital signature records for the NFC data exchange format." Near Field Communication (NFC), 2010 Second International Workshop on. IEEE, 2010.