Survey on NFC and RFID Technology

Naveen Kumar K, Mayank Raj, Neeraj Agarwala, Prateek Sharma, Nandhini Vineeth
Departmentof Computer Science and Engineering,
BMS College of Engineering, Bangalore,India

Abstract:
The radio frequency waves are used in communication between devices. The technologies which use the radio frequency as the medium of communication are Radio Frequency Identification (RFID) and Near Field Communication (NFC). Radio Frequency Identification technology employs a microchip called as smart tag with an antenna that broadcasts its unique 96-bit identifier and location to receivers. Near field communication is an efficient technology for communication between short ranges. It offers simple way to transfer data between electronic devices. A significant advantage of NFC is the compatibility with existing RFID infrastructures. Mobile NFC opens up new opportunities in payment and banking and various other fields. In this paper, a survey has been done on these two technologies and a comparative study is done.

IndexTerms— **Near Field Communication, Wireless Technology, OTA Technology, Advantages of NFC, RFID** *(keywords)*

INTRODUCTION

A technology that can be considered similar to NFC is **RADIO FREQUENCY IDENTIFICATION (**RFID). RFID is still in a developing phase and it is developing in terms of new applications. RFID tags are used in various applications. The use of RFID in tracking people has laid to several protests fearing its impact on people lives and privacy. There are lots of researches on RFID tags are still going on specially its integration with mobile devices. There is no proper standardization and regulation of RFID and its usage is still an open debate. The technology which is somewhat similar to RFID and is not criticized to this extent is NFC. One can expect a bright future of NFC with business opportunities and medical sciences health industries etc. With the development of more NFC enabled applications the standard and regulation is increases. The cost of designing and developing NFC system is economical.

RFID is one such technology in the field of pervasive computing [1]. RFID can read several tags simultaneously and store more data on the tag and data on the tag can be manipulated [2],[3]. Most RFID tags are passive which means they are battery less (they need external power). They can be attached to almost anything like clothes, foods, cards etc. RFID tags are mainly used for identification of physical objects and store an ID referred to as **Associate** in monitoring ELECTRONIC PRODUCT CODE (EPC). The EPC from the tag is employed to retrieve additional details concerning the object from the network information. This technique of using data from Associate in Nursing RFID tag is called "DATA-ON-NETWORK APPROACH". RFID tags comes with additional memory - Electrically Erasable Programmable Read Only Memory (EEPROM) that is utilized for storing the EPC and this approach is known as tag-on-tag approach [4]. In tag-on-tag approach, data is stored on the tag with lesser reliance on centralized network database, hence becoming a type of decentralized data storage. This section gives an introduction to the areas where the works on the NFC and RFID have been seen across

1. NEAR FIELD COMMUNICATION:

Near field communication is a technology for high frequency wireless short distance point to point communication. The operational range for NFC is less than 20cm, which is good from a security perspective, because it diminishes the threat of eves dropping. The other reasons to use NFC are the low cost of necessary components and that the connecting time is negligible. It is a small circuit attached to small antennae, capable of transmitting data to a distance of several meters. Most of the applications use NFC to retrieve some data from a passive token. The passive token could be a contact less smartcard or a key. In ticketing applications, NFC interface is used to transfer information.
Near field communication (NFC) has become one of the promising wireless technological development in the information and communication industry [1]. NFC technology is a short-range, high frequency, low bandwidth, radio technology. It allows us to transfer data within few centimeters. The integration of NFC with mobile devices offers many reliable applications such as payment, ticketing, loyalty service, identification, access control, content distribution, money transfers[5, 6, 3]. One of the major advantages of NFC is the fact that technology is compatible with the existing RFID infrastructure. NFC is build upon existing ISO standards including the ISO/IEC 1443 standard that is being used by the RFID technology. NFC operates at the 13.56 MHz radio frequency bandwidth with amplitude shift-keying modulation with data rates upto 424 kbytes/sec. In NFC there is no strict distinction between reader and transponder. A NFC capable device integrates both components: a passive transponder and an active transponder. It cannot only read and write data but can also receive and transmit data to another NFC device. IT supports three operating modes [1, 7, 8].

2. COMMUNICATION MODE:

There are three modes of communication in NFC forum:

i) Read/Write Mode: In this mode, NFC is used as a read/write tags. In this case the NFC device acts as an initiator and the passive tag is the target with the data rate being 106kbit/sec.
ii). Tag Emulation Mode: In this mode the NFC device emulates an ISO 1443 smartcard or a smartcard chip integrated in the mobile device is connected to the antennae of NFC module.
iii). Peer to Peer Mode: This mode is the classic NFC mode which allows data connection upto 424 kilobit/sec. It uses protocol (NFCIP-1) standardized in ISO 18092 and ECMA 320/340 [9].

3. OPERATION MODES OF NFC:

RF signal transmission between transmitter and receiver is the main difference between NFC and other wireless communication modes. NFC depends on magnetic coupling instead of radio waves which is used in Wi-Fi.
NFC can operate in either active or passive modes depending on the requirement.

i) ACTIVE MODE: In this mode device generates RF field to transfer data. In this situation any device can be the initiator and other will be the target. The initiator generates Radio Frequency field and other uses load modulation to transfer data. During the communication the initiator starts the communication in a particular mode at a specific speed. The target finds out the current speed and replies back to the initiator. Termination process of the communication takes place when either of the two devices is not in range [8, 9].

ii) PASSIVE MODE: This mode has benefit for battery power devices. For battery power devices, low consumption of battery is the basic priority. Thus, NFC allows devices powered with battery to operate in the passive mode. In this kind of mode, Radio-Frequency field is generated on the other side, this helps in saving the battery of the device in generating RF field [1]. In passive mode target operates continuously between H minimum and H maximum of the magnetic field [2]. The devices are not able to change the mode of communication during single transaction unless target is eliminated or de-activated [8, 9, 2].

4. THREATS TO NEAR FIELD COMMUNICATION:

NFC is the contactless token system but still, there is larger number of problems which needs to be solved. One of the fundamental issues is privacy because the tags contain sensitive information. A problem closely related to privacy is tracking, violation of location privacy. Other than privacy there are many other security issues that arise from NFC technology which are:
1. Eaves dropping threat: In this form of attack, unintended recipients are able to intercept and read messages. The range of NFC is 10 cm. They work in a close proximity. The optimal distance between the sender and receiver in order to use the RF signals is still a topic of discussion. The reason for that is huge number of parameters which determines the distance depends on the following parameters:
RF field characteristics of the given sender device.
Characteristics of the attacker's antennae.
Quality of the attacker's receiver.
Quality of the attacker's Radio Frequency signal decoder power sent out by NFC device.
Setup of location where the attack is initiated.

Furthermore, it is extremely dependent on the communication mode. That is because, it's based on active and passive mode, the transferred data is ciphered and modulated differently [8,10].
2. Data modification threats: In data modification threats, the attacker tries to modify the data instead of just accessing it. The main motive of the attacker is to disturb the communication such that the receiver is not able to understand the data sent by the other devices. In data modification, the attacker requires the receiving device to receive the valid but manipulated data. The feasibility depends on the amplitude modulation.
3. Man in the middle threats: In this threat two communicating devices are triggered by another third party device and the information is sent to this third party [8 ,10].
4. Security: There are many forms of threats which are affecting the NFC technology and needs to be removed. There are many types of security steps which can be taken in order to prevent the unauthorized access in the NFC system. This can be done by authentication and Key Generation and Pin Verification [4,11].

5. NFC APPLICATION:

NFC application has its uses in different fields: [5,7,6]
1. Service initiation category: In service initiation, NFC is as same as RFID. NFC device reads some data information from the tag and uses this information in several different ways. In this case, NFC tags acts as a transponder. This type of service is utilized in the information desk where the user touches its NFC device with the tag and retrieves the information. So basically in service initiation, there is a communication between a tag and the NFC device. These tags can be used in places like libraries, department stores etc.
2. Peer to Peer: There is a direct link between communication devices to transfer the data. If the amount of data which has to be transferred is large, the Bluetooth and Wi-Fi is used.
3. Payment and Ticketing: In this application the phone acts as an electronic wallet. We load it with virtual money which can be used for paying, travelling tickets or parking fee [5].

6. OTA(OVER THE AIR TECHNOLOGY)

Over-the-Air (OTA) technology contributes dynamic spirit of the NFC based system adaptability to flexible environments [12]. It enables loading and installation of new NFC applications on SEs - especially on UICCs - remotely, activation and deactivation of SEs, remote service management, life-cycle management of NFC applications on the SEs, and other online services. High-capacity bearers that are being used in OTA technology are very important in providing an NFC solution. For instance, several kilobytes of data needs to be transferred to the UICC based SE when downloading an application activation data or an NFC application. Using GPRS/UMTS and the BIP (Bearer Independent Protocol) protocol, applications are rapidly deployed OTA to the UICC card. Currently, OTA solutions are provided by most MNOs using their current technology infrastructure. These entities can provide OTA service independently from SE issuers or platform managers when required infrastructure is set up by other entities. One of the most appropriate cases is to use OTA solution of Trusted Service Manager as a neutral entity within the NFC Ecosystem [9].

7. ADVANTAGES OF NFC:

NFC helps to provide high level security because it establishes connection only if two devices are brought close to each other [1].

It helps us reduce the risk of swiping the card, entering password and choosing the menu, making the process more flexible.

The NFC is designed to consume less power and hence it is used in medical science.

The speed of establishing a communication link between two devices adds more advantage when compared to other devices which are not using NFC.

The other advantage of NFC is its versatility. Using NFC, one can perform multiple tasks like check out at a store, purchase and load concert tickets to their smart phones, read information from smart poster, board the subway, and many other tasks all from a single device.

The other advantage of NFC is its flexibility. Depending on the requirement the NFC can operate in passive mode as well as in active mode [7, 1].NFC provides higher data rate as compared to the RFID.Since the NFC does not require any external power source, it becomes compatible with other electronic devices.[13]

8. CHALLANGES TO NFC

NFC-based solutions that collaborates with existing contactless and smart card standards have still deficiencies.

1) NFC when combined with mobile communication has huge importance. Nevertheless, mobile NFC applications are handset specific. This restriction requires the service providers – mobile operators – to develop, test and maintain a different application for each NFC enabled device. Network related issues are also adding problem to the application. A neutral technology can be used that can hide mobile specifics in order to make NFC technology more handset independent [14].

2) The recently elaborated operating models are supporting single application business models. It means that on the chip (which stores the business application), there is only one application running, although technically it would be possible to host multiple applications, service profiles alternately. There are multiple reasons for this situation [14].

9. NFC PROTOCOLS AND STANDARD

ISO-IEC 14443 protocol:

It is one of a series of International standards defined under ISO/IEC 7810. This part of ISO / IEC 14443 describes polling for proximity card entering the field of a coupling device and a byte format or framing etc. Protocols and commands used by higher layers, by application and which are used after the initial phase are described under ISO/IEC 14443.

ISO/IEC 14443 allows operation of proximity card in the presence of other contactless cards with ISO/IEC 10536 and ISO/IEC 15693[15].

ISO 18000:

Parameters for Air Interface communications at 13.56Mhz determines physical layer, collision system and protocols for 13.56Mhz RFID systems for item identification [16].

NFC-DEP PROTOCOL

ISO 18092(NFCIP-1) or ECMA 340

This standard defines communication modes for NFCIP-1 using inductive coupling devices operating at frequency of 13, 56 MHz. It also defines the active and passive communication mode of NFCIP-1. The standard specifies the modulation schemes, coding, transfer speeds, frame format of RF interface. These devices shall have communication capability on 106/212/424 kbps and may switch to another transfer speed or remains at the same. The mode (Active or Passive) shall not be changed during one transaction until the deactivation of the target or removal of the target, even if the transfer speed of Initiator to Target and the transfer speed of

the Target to the Initiator may be different. The difference in transfer speed during one transaction can be performed by a parameter change procedure [17].

ISO 15963
This standard describes the numbering system which is used for identification of RFID'S.
The unique Id can be used
1) For traceability and quality control of the integrated circuit.
2) For traceability of RF tags from its manufacturing process.
3) For completion of reading in a multiple antenna configuration. [18]

10. RFID TECHNOLOGY:
RFID can read several tags simultaneously, store more data on the tag and data on the RFID Technology is a promising technology tag can be manipulated [12,19]. The cost of implementing RFID technology is also reducing, making [ROI] return on investment more achievable. RFID tags are used for identification of physical objects and store an id called electronics product code [EPC]. The EPC from the tag is used to retrieve more details about the physical object from the network. This system of using network is called Data on network approach.
However RFID is replacing barcode technology and has more advantage of scanning the object from a distance. It has more enhanced visibility and inventory management [20]. RFID tags have a memory capacity of 16-64 kilobytes which is much more than barcodes. Wallmart is the biggest user of RFID and it is investing to develop its application. Some security problems are there in RFID technology such as people can easily build RFID readers with lower cost and can read data from RFID chip.

11. ADVANTAGES OF RFID:
There are some advantages of RFID which cannot be neglected such as:
Reader can read and write data without direct contact.
Data from tags are accessed by radio waves.
There is no maintenance cost in RFID.
RFID is flexible and can work under any environment condition.
Read and write operation in RFID is much faster than any other technology.
RFID tags can also be used for tracking with GPRS technology.
RFID tags have a good memory capacity with 16-64 kilobytes.
They can also be integrated with other technology and a combination can be used in other high-end applications [21].

12. APPLICATION OF RFID: RFID tags are used in many applications and in various fields. It is used in numerous tasks like tracking animals, Automated checkout etc. It also provides security from piracy of video and audio disks. Another popular use of RFID is RFID BASED TOLL GATES. In this technology, RFID tags are attached to the vehicle license plate and send the information to the device equipped in the toll collecting lane. The same technology is used for tracking stolen cars by the police department.
Another popular application of RFID is animal tracking where the RFID tags are used to track the animal location. Currently, this technology has been transformed to human implantation. RFID tags based wrist bands and clothes are used to track the prisoners.
RFID tags have also their use in the health industry where the medical history of the patient is stored in the RFID tag. RFID tags are also used in airline industry to track the baggage of the passenger [22, 23].

13. SECURITY: The major security concern for the RFID is anyone can access the RFID and anyone can gather data without any prior acknowledgement. The clone of RFID tags can be generated which is a challenging problem. Criminals with RFID readers can scan digital passports to target specific nationality.[24,25]

RFID threats can be grouped in three categories which are exploits, worms, and viruses. The exploits are the normal hacking attacks that are found on internets like code insertion etc. [25] The RFID worms and virus are the copying of the original code to the new RFID tags. The main difference between the worms and the viruses is that the worms are totally dependent on the network but the virus is not.

The security steps which can be taken to secure RFID are:
1. Using the ELECTRONIC PROGRAMMABLE CODE (EPC KILL) command.
2. Use of cryptography to prevent data leakage.
3. Using tag password so that tag emit information only if it receives right password.
4. Another solution is using timer based mechanism which changes the tag password periodically. Using blocker tags can also prevent RFID threat related matters [26, 27].

I. CONCLUSION:
In this paper we have given our views on the latest emerging technology- NFC and how NFC applications will change the technology aspects which will prove beneficial to the mankind. We have also discussed about RFID, its pros and cons. The features of NFC which help in overcoming some of the shortcomings of RFID like the cost, security, health perspectives etc. are also discussed. This paper can be helpful to researchers who would like to know about the technologies NFC and RFID.

ACKNOWLEDGMENT

The work reported in this paper is supported by the college [BMSCE] through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES

[1] Hongwei Du, "NFC Technology: Today and Tomorrow", International Journal of Future Computer and Communications, Vol 2. No.4, August 2013, DOI:10.7763/IJFCC.2013.V2.183

[2] Sanjay Ahuja, Pavan Potti, "An Introduction To RFID Technology", Communications and Network, 2010, Vol. 2, No.3, pp 183-186, DOI:10.4236/cn.2010.23026.

[3] Paul Golding and Vanesa Tennant, "Evaluation of a Radio Frequency Identification (RFID) Library System: Preliminary Results", International Journal of Multimedia and Ubiquitous Engineering, 1January 2008, Vol.3, No.1, pp 1-18.

[4] Pardis Pourghomi, Muhammad QasimSaeed, Gheorghita Ghinea, "A Proposed NFC Payment Application", International Journal of Advanced Com
puter Science and Applications, 2013, Vol. 4, No. 8,pp 173-181.

[5]Vedatcoskun , keremok , Besra Ozdenizci, "A Survey on Near field communication technology", Wireless personal communications Journal, Dec 2013, Vol. 71,No.3, pp 2259-2294, DOI: 10.1007/s11277-012-0935-5.

[6]KevinCurran, Amanda Millar, Conor Mc Garvey, "Near field communication", International Journal of Electrical and Computer Engineering (IJECE), June 2012,Vol. 2,No.2, Issue.3 , pp 371-382.

[7] Ekta Desai, Mary Grace Shajan, "A review on the operating modes of near field communication", International Journal of Engineering and Advanced Technology (IJEAT) December 2012 ISSN: 2249 – 8958, Vol.2, No.2, pp 322-325.

[8] Mohamed Mostafabd Allah, "Strength And Weakness Of Near Field Communication Technology ",Global Journal of Computer Science and Technology, March 2011, Vol.11, No. 3.

[9]Rosa Iglesias, Jorge Parra,Cristina Cruces,Nuria Gomez de Segura,"Experiencing NFC-based touch for home healthcare",PETRA '09 Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments,2009,DOI:10.1145/1579114.1579141.

[10]Kevin Curran, Amanda Millar, ConorMcGarvey."near field communication", International Journal of Electrical and Computer Engineering (IJECE), June 2012, Vol.2, No.3, pp. 371-382.

[11]Menghin, M.; Druml, N.; Steger, C.; Weiss, R.; Bock, R.; Haid, J., "NFC-DynFS: A way to realize dynamic field strength scaling during communication", Near Field Communication (NFC), 2013 5th International Workshop on , Feb. 2013 ,vol.1, no.6, pp 5, DOI: 10.1109/NFC.2013.6482438.

[12] Sarita Pais, Judith Symonds,"Data Storage On A RFID Tag For A Distributed System", International Journal of UbiComp (IJU), April 2011,Vol.2, No.2, DOI:10.5121/iju.2011.2203

[13]Hussein Ahmad Al-Ofeishat, Mohammad A.A.Al Rababah, "NEAR FIELD COMMUNICATION", IJCSNS International Journal of Computer Science and Network Security, February 2012,Vol.12 No.2,pp. 93-99.

[14] Nath, F. Reynolds, and R. Want, "RFID Technology and Applications", IEEE Pervasive Computing,2006, Vol. 5,No. 1, pp 22–24.

[15]Issovits, W.; Hutter, M., "Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks," RFID-Technologies and Applications (RFID-TA), 2011 IEEE International Conference, Sept 2011, pp 335,342, 15-16 DOI: 10.1109/RFID-TA.2011.6068658

[16] Gershenfeld, Neil; Cohen, D., "Internet 0: Interdevice Internetworking - End-to-End Modulation for Embedded Networks", IEEE Circuits and Devices Magazine, Sept.-Oct. 2006 ,Vol.22, No.5, pp.48-55, DOI: 10.1109/MCD.2006.273000

[17] Hancke, G.P., "Practical attacks on proximity identification systems", IEEE Symposium on Security and Privacy, 2006 , Vol.6 No.333, pp 21-24 May 2006, DOI: 10.1109/SP.2006.30

[18] XuefeiLeng, Yuanhung Lien, Mayes, K.; Markantonakis, K. Jung-Hui Chiu, "Select-Response Grouping Proof for RFID Tags", First Asian Conference on Intelligent Information and Database Systems, ACIIDS 2009,April 2009, DOI: 10.1109/ACIIDS.2009.94

[19]Lynn A. DeNoia and Anne L. Olsen."RFID And Application Security", Department of Computer Science and Quantitative Methods Winthrop University, Rock Hill, SC 29733,2009,Vol. 41,Issue 3.

[20] Arun N. Nambiar."RFID Technology: A Review of its Applications, Proceedings of the World Congress on Engineering and Computer Science 2009, Vol II
WCECS 2009, October 20-22, 2009, San Francisco, USA.

[21]DougSerfass,KenjiYoshigoe,"Wireless Sensor Networks Using Android Virtual Devices and Near Field Communication Peer-To Peer Emulation", Proceedings of IEEE Southeastcon, 2012, March 2012, Vol.1, No.6, pp. 15-18, DOI: 10.1109/SECon.2012.6196980

[22] Paradowski, Denise; Kruger, Antonio, "Modularization of mobile shopping assistance systems," 5th International Workshop on Near Field Communication (NFC), 2013 , Vol.1, No.6, DOI: 10.1109/NFC.2013.6482444.

[23]Menghin, Druml, Steger, Weiss, Bock, Haid, "NFC-DynFS: A way to realize dynamic field strength scaling during communication", 5th International Workshop on Near Field Communication (NFC), 2013, Feb. 2013,Vol.1, No.6, DOI: 10.1109/NFC.2013.6482438.

[24] Shyamal ,Pampattiwar, " Literature Survey on NFC, Applications and Controller **",** International Journal of Scientific & Engineering Research, Feb 2012,Vol.3,Issue 2.

[25]Pardis Pourghomi Department, "Managing Near Field Communication Payment Application Through Cloud Computing", 7th International Conference for Internet Technology and Secured Transactions, 2012, pp 772-777.

[26]. Franklin T. Warren, Dr. Tabitha James, " Evaluating RFID Research a Literature Review", A Paper in Partial Fulfillment of the requirements for "Networks & Telecomm Business" 2007, pp 1-9.

[27] G.Gopichand, T. Krishna Chaitanya, R, Ravi Kumar, "Near field communication and its application in various fields",(IJETT), April 2013, Vol. 4, Issue 4.