A COMPARATIVE ANALYSIS OF VARIOUS NFC APPLICATIONS

Himen Sidhpura[1], Vishwas Banjan[2]
[1]Student, Department of Computer Science and Engineering,
[2]Student, Department of Electronics and Communication Engineering,
[1,2]Nirma University, Ahmadabad, Gujarat, India

Abstract: This paper is based on basically on different threat/vulnerabilities and complexities & challenges in various application of NFC technology in present. NFC transfer data at rate up to 420 kbits/sec in distance of 10cm or less. It operates on initiator, target and peer-peer. In this paper, we discussed about the basic of NFC and its application. We then focused in various threats/vulnerabilities, complexity/challenges in NFC. It is based on RFID. RFID transfer the data with the use the electromagnetic field. Furthermore, we have also discussed on the security analysis and future work. The paper also demonstrate the concept of Virtual NFC which reduce the connection setup time between smart phones and DTV by 60% while WIFI direct connection reduce coonection setup time by 49%.

Keywords: RFID, JIS, EMR, CE, P2P, RW, I-T,T-I

Abbreviations: Radio Frequency Identification, Japanese Industrial Standard, Electronic Medical Record, Card Emulation, Peer to Peer, Reader/Writer, Initiator-Target, Target- Initiator

I. INTRODUCTION

NFC is a technology which enables the Smartphone and other device to communicate with each other by touching then together or bring at distance of 10cm or less[24]. It works mainly on 3 device: Initiator, Target and Peer-Peer. They involves initiator and target for the communication. Initiator is responsible for the communication[25]. Initiator start the communication and energized the target when is in passive mode. Initiator generates a power for the target with help of energy component. Communication between two device are done half-duplex mode. NFC forum has defined four types of tags for transferring the data which are used on basis of speed, flexibility and security[6][18].

Table 1 : Types of Tag

	Based on	Capability	Memory
Type 1	ISO/IEC 14443A	Read and Re-Write	96 byte to 2Kbyte
Type 2	ISO/IEC 14443A	Read and Re-Write	48 byte to 2Kbyte
Type 3	(JIS) X 6319-4	Read and Re-Write	Variable upto 1Mbyte
Type 4	ISO/IEC 1443 Standard series	Read and Re-Write	Variable upto 32Kbyte

As shown in Table 1, all tags are read and re-write capability but Type 3 and Type 4 had additional capability. They can be either read & re-write or read only[11]. NFC have two communication mode: active and passive. Passive Communication take place when initiator generates carrier field and target answers it by modulating it. Active communication takes place when both initiator and target communicate alternately by generating their field. In the below Table 2 types of configuration are demonstrate between two device in which one of them can be sender and receiver.

Table 2 : Types of Configuration

Device A	Device B	Description
Active	Active	Both Device generates RF field alternatively.
Active	Passive	Device A only generates RF field
Passive	Active	Device B only generates RF field

From technical point of view, data transmission takes place with data rate of 106kbits/s, 212 kbits/s and 424kbits/s with different bit coding scheme at frequency of 13.56 MHz. NFC technology supoorts three type of Technology mentioned in Table having same frequency rate with diiferent modulation scheme, data rate and bit coding scheme.

Table 3: NFC Technology

NFC Technology	Direction	Bit Coding	Modulation	Date Rate (kbits/s)
NFC–A	I-T	Miller	100% ASK	106
	T-I	Manchester	100% ASK	106
NFC–B	I-T	NRZ-L	10% ASK	106
	T-I	NRZ-L	BPSK	106
NFC-F	I-T	Manchester	10% ASK	212/424
	T-I	Manchester	10% ASK	212/424

In the NFC, two types of coding are involved in it, Manchester coding and Miller coding to transfer the data. In the Miller coding, data transfer take place at rate of 106 kbits/sec with 100% modulation while in Manchester coding, 10% modulation is done in all other cases where Manchester coding is not used[3]. VNFC is wireless communication between smart phones and NFC equipped customer

electronics having bluetooth or WIFI module without NFC having a set of NFC enabled remote control[17]. WIFI Direct Connection Method(P2P) is a method of establishing direct peer to peer WIFI coneection between two device such as connection connection between smart phones customer electronics application such as TV, home speaker. In this method, coonection doesn't requires a wireless router. The remainder of this paper is as follow. Section II gives a background of Threats and Vulnerabilities in NFC. Section III focus on the defence against threats and vulnerabilities in NFC. Section IV discusses the various application and comparison of VNFC with wifi direct connection method. Section V shows shows some security analysis on different application of NFC. And In last conclusion remark is given.

II. THREATS & VULNERABILITIES

- Eavesdropping : It is a treat in which attacker retrieves the private data or information of user without user consent by using larger antennas then the mobile device which help the attackers to eavesdrop over the large distance[3].
- Data Corruption: In NFC, data corruption can take place if attacker focused on the transmission medium or by using malicious software running in the background of device. If attacker focused on the transmission medium then there is a chance of losing original data which may result in corruption of data stored in tag. The attacker may use valid frequencies while users communicate with each other. In this attack, original data is not corrupted but data send by the user is modified. This attack becomes a Denial of service attack[3].
- Data Modification: Data modification take place when attacker changes the actual data stored in tags.
- Data Insertion: Unwanted data inserted by attacker when two user are communicating with each other. This attack takes place when duration of communication between user is more[3].
- Man in Middle Attack: In man in middle attack, third party routes the communication between two user without knowing the two user. Instead of one to one communication it becomes third party communication.

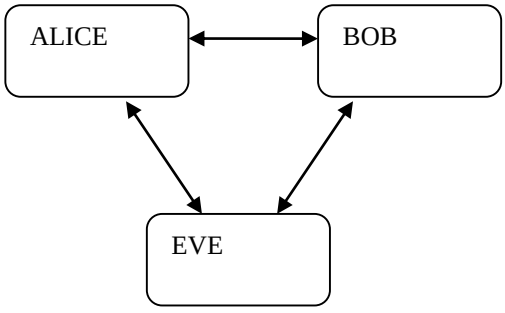

Figure 1 : Man-in-Middle Attack Setup

In Figure, man in middle attack can clearly explained. In the figure, Eve is listening to the conversation of Alice and Bob without being noticed.

III. DEFENCE

- Eavesdropping: NFC doesn't have any security against eavesdropping. This attack is overcome by only use of secure channel which is based on encryption and decryption.
- Data Corruption: These type of attack is easily detectable as change in RF field detect by the device help the user to know whether data corruption or modification is done.
- Data Modification: Data modification is protected by keeping the baud rate changing. Keeping Baud rate 106 Kbits/sec make the data modification impossible for attackers in active mode. But this may cause Eavesdropping threat [21].
- Data Insertion: This type of threat is only possible when receiver device is slow. This threat is overcome by using secure channel [19][20][21].
- Man in Middle Attack: NFC is operate in short range due to this it is practically impossible for attacker to carried out at short distance. This threat is overcome by making device in active and passive mode.
- Secure Channel: Secure channel is best approach of keeping data safe from attacker from eavesdropping, man in middle attack, data corruption and other threats.
- Diffie Hellman Key protocol used in RSA to create a secure channel. The arrangement used the scheme like AES to create proper authentication.

IV. LITERATURE SURVEY

A. Current and Future Trend In NFC

This section focus on the current and future technology in NFC. This paper demonstrate the current application which are implementated worldwide as shown in Table 3[4][22].

Table 4 :NFC Development across worldwide

Year	Country	Application based on NFC
2014	Canada	Mobile Payment Solution
2014	Spain Bankia	m-Payment Service
2013	Bulgaria	Contactless Payments with Mobile by M-Tel
2013	Sri Lanka	Fuel Card Management by Mobitel
2013	UAE	Ticketing service across Emirates metro, bus etc.

Moreover this paper focuses on the NFC development in India which are already implementated[2][4][22].

Table 5 : NFC development in India in various application

Year	Development
2014	Working on Airline Ticketing service
2014	Opening of NFC test lab by Mahindra
2013	NFC Payment service by PVR Cinema
2013	NFC couponing platform by JusTab

B. Healthcare

This section demonstrates the application of NFC in healthcare and their uses in present. In healthcare application, NFC can used store the medical related data of patient by

giving the unique NFC Tag. NFC retrieves the data from EMR system which keeps the patient record in more accurate and efficient manner. When the patient discharge from hospital, all the medical related details are updated in EMR will be synchronised and transferred back to his/her NFC tags[1][8]. When the patient changes doctor, doctor can easily retrieves the information about the patient from unique NFC tag. This unique tag is identified by National Unique Identification Number (NAUID) or Aadhar card distributed by the Govt. of India. This NFC is implementated by using NFC in writer mode operation. This technology helps both the patient and doctor[8].

Challenges & Complexities:

- Workflow of the system: Using EMR system, it helps the doctor to know the exact the problem of the patient when doesn't have proper interface with doctor[1].
- Error in documentation: Sometimes EMR system takes erroneous data. Due to point & click and drag & drop feature in EMR system promote the erroneous data.
- Interruption between doctor and patient.
- Chances of misusing the health report of the patient by authorised user of EMR system.

Future Research should address the following issue

- Privacy: The main goal in this field is to maintain the privacy of user while retrieving/retaining the data as it can be accessed by various user[1]. To solve this problem, developers should encrypt the data stored data in P2P mode and also in RW mode.
- Man in middle attack: the data can be accessed when the card is not in use. So, there are chances of misusing data.
- Authentication: There should be secure authentication should be used in financial domain. In this threat, developers should think about the security of backend and middleware system especially in application of card emulation[14].
- Accuracy in collecting data: while collecting the data, developer should design in such way that data must be stored in unique tag of user.
- Low power consumption system[1][14]

C. Monitoring Plant Information in Industries

This section demonstrate the use of NFC technology that has recently used via NFC Chip, mobile phones and PDA[5].

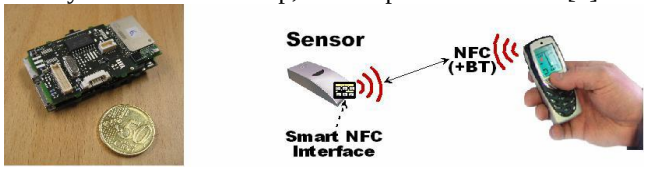

Figure 2:Smart NFC Interface Module

Complexities and Challenges:

Wireless communication brings a lot of flexibility. The proposed application should have following requirement and challenges[5]

- Harsh Environment: Environment like air consist full of small particles and temperature ranges from -10 to +50 degree Celsius, the packaging of sensor nodes should be carefully designed.
- Avoidance of Reflection: There are many surfaces where signals may be reflected and can't reach to the target. For example, concrete wall doesn't allow signal to pass through it if the signal is weak[23].
- Power consumption: Sensor should use less power and work for long period of time[12][23].
- Simple UI: Interface should designed in such a way that it should resist harsh environment and communication should also take place in outdoor condition[12].

D. Credit Transfer Among Mobile Device

This section demonstrates the transfer of credit among two smart devices. The main goal of this application is to transfer the credit using two devices. Credit Transfer is based on peer-to-peer connection mode. The System Architecture of Credit transfer is proposed in Figure . In this Figure, both the device should have NFC chip and Bluetooth adapter. Both this are used during credit transfer. First, NFC send the message to Receiver device to turn on the Bluetooth adapter. Bluetooth adapter transmit a message of credit information to the receiver device[10]. As mentioned above, this connection is possible due peer-to-peer connection offer by Google. This application is develop for android platform in the market during project development. At the moment, BlackBerry, Symbian Anna and Bada 2.0 has develop this application in their operating system. The proposed application faces significant challenges due to lack of supporting infrastructure and complex ecosystem of stakeholders[7][10].

E. Virtual NFC

This section demonstrate the wireless communication between a smart phones and DTV equipped with the NFC enabled remote control.Coomunciation is done with the help of virtual NFC between mobile device and customer electronic which have Bluetooth or WIFI module without NFC[17].

Table 6: Comparison of average connection setup time

	Connection Method	Connection Setup Time(Sec)
1 Hop Network	Normal P2P	13.84
	NFC P2P	7.12
2 Hop Network	Normal P2P	18.74
	NFC P2P	7.48

Above Table 6 shows the average connection setup time between smart phones and customer electronic application such as speaker and TV. In 1 Hop network (VNFC based), comparison of connection setup time is based on normal WIFI direct (P2P) and NFC while In 2 Hop network, it is based on normal WIFI direct and VNFC.

F. Security Analysis

This part mainly focused on the classification of attacks in

NFC. They mainly based on mode of operation, life cycle and programmability level[9].

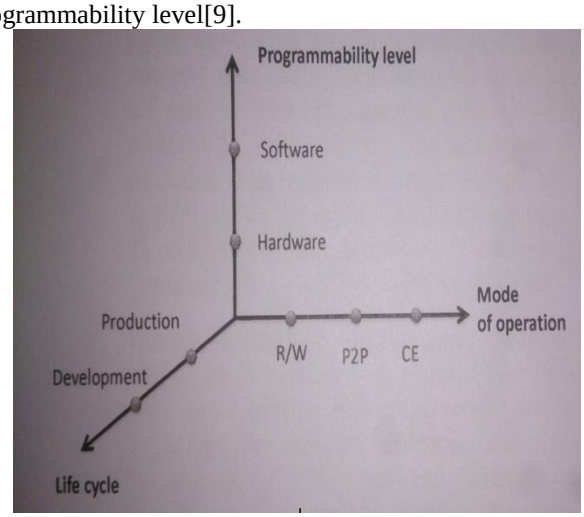

Figure 3: A multi-dimensional representation of NFC System

Figure 3 help to visualize the attacks in the three different perspectives.

Based on mode of operation:

- RW mode: In this mode, presents of two or more card in the carrier field, one of them is selected using anti-collision algorithm. Due to this any of the device can retrieve the confidential data [9].
- CE mode: This mode is mainly used in contactless payment using NFC in between two device. Attacker can retrieves the credit card information stored in the device or application [16]. In CE mode, protecting the crdit card information and having secure connection are most serious concern in CE mode.
- P2P mode: In this mode, communication is bi-directional. Due to this, there is a possibility of data interception [15].

Based on Life Cycle

- Development Phase: This attacks are mainly done during design of of NFC chips. This attack help the attacker to gain access to the information of the target in future and also it allows the attacker to create clone of chip.
- Production Phase: Attacks in this case take place through the firmware updates or software application or by extracting confidential data[16][15].

Based on Programmability Level:

Hardware Attacks: Attacks in this case take place on the NFC interface chip which are used in cellular device. This attack allow take attacker to view the transfer of data and disable transfer of data through NFC[13].

Software Attacks: This attack mostly take place in form of software/firm update on mobile device that uses NFC Application[13].

V. CONCLUSION

In this paper, we presented a comparative analysis of NFC technology in HealthCare, Industrial application and Mobile application such as credit transfer among two devices. NFC should have secure channel using encryption/decryption so that it should protect against man-in-middle attack. In HealthCare Application, NFC has great roles. With the help of NFC tags, all the information/data of patient are stored in tag and this data are easily retrieved by doctor. In this proposed application there is chance of misusing the information of patient by the attacker. In Industrial Application, NFC help us to develop Smart NFC Interface to have flexible reading of machine and sensors in Harsh Environment. In the Industries, wireless communication can be used to reduce the paper work. This can be possible with NFC. The Credit transfer is most secure application among NFC as it uses NFC to connect to device and transfer of credit takes place using Bluetooth. In the futue, the idea of VNFC will extend to use customer electronic application such as helps to transfer music play on smart phones to speaker using NFC enabled remote control. With the help of VNFC, setup time is reduce upto 54.% average.

REFERENCES

[1] Ali Alzahrani, Abdullsh Alqhtani, Haytham Elmiligi, Fayez Gebali, and Mohamed S. Yasein, "NFC Security Analysis and Vulnerabilities in Healthcare Application," , 2013.

[2] B. Benyo, B. Sodor, L. Kovacs, J. Homlok, and G. Fordos, "Security issues of Service installation on a multi appliaction NFC environment," , 2010.

[3] Naveed Ashraf Chattha, "NFC- Vulnerabilities and Defence," , 2014.

[4] Sudipts Dhar and Aniruddha Dasgupta, "NFC Technology : Current and Future Trend in India," , IEEE, 2014.

[5] Arto Ylisaukko Oja, Esko Strömmer , and Mikko Sallinen, "Application Scenario for NFC: Mobile Tool for Industrial Worker," , 2008.

[6] Muhammad Qasin Saeed and Colin D. Walter, "Off-line NFC Tag Authentication,".

[7] Pardis Pourghomi and Gheorghita Ghinea, "Managing NFC Payment Applications through Cloud," , 2012.

[8] Weider D. Yu, Hargun Hansrao, Kirandeep Dhillon, and Pradeep Desinguraj, "NFC Based m-Healthcare Application Focusing on Security, Privacy and Performance," , 2013.

[9] N Harini, M. Vahini, Sujitha Rajaram, S. Kavya, and K. Pavithra, "Vulnerability Analysis And Security System For NFC-Enabled Mobile Phones," , June 2014.

[10] David M Monteiro, Joel J.P.C Rodrigues, and Jaime Lloret, "A Secure NFC Application for Credit transfer Among Mobile Phones," IEEE, 2012.

[11] Paula Hunter Executive Director, Koichi Tagawa Chairman, and Frank Dawidowsky Secretary, "NFC Forum".

[12] Mikko Sallinen, Esko Strömmer, and Arto Ylisaukko-oja, "Application Scenario for NFC: Mobile Tool for Industrial Worker," 2008.

[13] Antonio J. Jara, Alberto F. Alcolea, Miguel A. Zamora, and Antonio F. G. Skarmeta, "Evaluation of the security capabilities on NFC-powered devices,".

[14] Akira Arutaki and Hiroshi Sakai, "Protocol

Enhancement for Near Field Communication : Future Direction and Cross-Layer Approach,".
[15] Pardis Pourghomi and Gheorghita Ghinea, "Challenges of Managing Secure Elements within the NFC Ecosystem," , 2012.
[16] Dirar Abu-Saymeh, Dhiah el Diehn I. Abou-Tair, and Ahmad Zmily, "An Application Security Framework for Near Field Communication," , 2013.
[17] Suk-Un Yoon, Shekhar Joshi, and Seung-Seop Shim, "A New Simple Wi-Fi Direct Connection Method using NFC on Remote Control and DTV," , 2014.
[18] Xiao Kun and Luo Lei, "A Novel Mobile Device NFC Stack Architecture," , 2013.
[19] Nikolaos Alexiou, Stylianos Basagiannis, and Sophia Petridou, "Security Analysis of NFC Relay Attacks using Probabilistic Model Checking," , 2014.
[20] Pascal Urien, "A Secure Cloud of Electronic Keys for NFC Locks Securely Controlled by NFC Smartphones," , 2014.
[21] Sufian Hameed, Bilal Hameed, Syed Atyab Hussain, and Khalid Waqas, "Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters," , Pakistan, 2014.
[22] Sudipta Dhar and Aniruddha Dasgupta, "NFC Technology: Current and Future Trends in India," , Kolkata, India, 2014.
[23] Ramakrishnan Ramanathan and Jahanzaib Imtiaz, "NFC in Industrial Applications for Monitoring Plant Information," , Germany, 2013.
[24] Büşra ÖZDENİZCİ, Mehmet AYDIN, Vedat COŞKUN, and Kerem OK, "NFC Research Framework: A Literature Review And Future Research Directions," , Turkey, June, 2010.
[25] Subhasini Dwivedi, Shraddha Panbude, and Rama Rao, "A Review of Applications Based on NFC Technology : A Step towards MakingUniversal NFC Receiver Using Android Device," , Mumbai, India, 2014.

