International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

A Review of Protocol Security Implementation in Near Field Communication

Prof. Rahul S. Gaikwad [1], Ms. Pranita Shankhpal[2]
Godavari Foundation’s Godavari College of Engineering,
Jalgaon, 425001, India

Abstract **- NFC (Near Field Communication) is a short-range wireless communication technology based on Radio Frequency Identification (RFID) technology. We here are presenting the idea of NFC. We have analyzed**

Research papers for formulating one final document which explains the NFC and all its components along with advantages and disadvantages it possesses. NFC is the short form of Near Field Communication which can be considered to be the higher extension of Wireless communication in the modern day world. Why should we use NFC? The answer to this question is faster data transfer rate compared to other wireless options available. The main issue that might occur though is the security of NFC. The paper also presents the scope of NFC in the near future. This paper proposes the various fields where NFC technology can be used. The most useful application is the online bill payment through your mobile. Also NFC can be used widely in the medical sector providing much more accurate results and better diagnosis. This paper thus presents the probable use of NFC in various fields and its advantages

Key Words: Near Field Communication (NFC), Security, RFID, NFC tags, etc.

1. INTRODUCTION:-

Near field communication (NFC) is a technology for contactless short-range communication. Based on the radio frequency identification (RFID), it uses magnetic field induction to enable communication between electronic devices. The number of short- range applications for NFC technology is growing continuously, appearing in all areas of life. Especially the use in conjunction with mobile phones offers great opportunities. One of the main goals of NFC technology has been to make the benefits of short-range contactless Communications available to consumers globally. NFC is estimated as Near Field Communication which was introduced in 2002 by both Sony and Philips. It allows any two devices which have NFC in them to communicate with each other when the two devices are in close proximity of about 4 cm. The main advantage of using NFC is that no communication links have to be established first due to which it is faster than the existing technologies. NFC uses two types of encoding techniques for the process of exchanging data. These two techniques are Miller Coding and Manchester Coding. Miller coding has 100 percent modulation whereas Manchester Coding has modulation ratio of 10 percent. When the baud rate is 106KB then Miller Coding has been used and in every other case Manchester Coding has been used. NFC can be used in many applications because it allows both one way and two-way communication. NFC is based completely on RFID. Each NFC device can operate in three distinctively unique modes. NFC is compatible to legacy contactless smartcard systems based on the standards ISO/IEC and Felicia. Beside that standardisation through bodies such as ISO/IEC and ECMA various data forms, normalised data’s, basic requirements, device certification. The fundamental property by which NFC works is- ‘it is all in one touch’. This means that just one touch or contact between two NFC enabled devices triggers an action in both of them. objects are embedded with NFC tags which store content like internet access address(URLs), phone numbers, SMSs and business cards. NFC works in three basic modes namely- peer-to-peer mode, reader/writer mode and card emulation modes. One of the prime reasons that a lot of research work is being carried out in the field of NFC is that our lives are more or less dependent on mobile phones and the concept of NFC is incorporated in mobile phones or smartphones. All the research carried out in this field points towards the various advantages which include faster transactions which are more reliable if certain parameters are kept in mind. The concept of NFC is still in the developing stage and has applications various different areas including Health Care, Payment, Business Transactions and in home security systems which can be extended further to regulate air conditioners and heaters.

Here are some examples of what a user can do with an NFC mobile phone in an NFC-enabled environment:

1] Download music or video from a smart poster.
2] Exchange business cards with another phone.
3] Pay bus or train fare.

4] Print an image on a printer.

5] Use a point-of- sale terminal to pay for a purchase, the same way as with a standard contactless credit card.

6] Pair two Bluetooth devices.

2. LITERATURE SURVEY:-

[1] In this paper shows the virtual view of using NFC. In the work the main aim was to point out the security issues related to NFC (Near Field Communication). Some practical solutions to these problems are also proposed in the research carried out by them. The communicating devices can be either active or passive. A communicating

device is said to be active, if it generates its own RF field, otherwise the device is known as passive. The research has been carried out by taking three applications as examples, with respect to these examples, the authors have pointed out the possible threats. The main purpose of contactless tokens is to facilitate an active NFC device to retrieve the data stored in it. However, the Ticketing/Micro Payment application is used for transactions of any kind of information which generally includes more than one interface. Whereas, device sharing application of NFC is just used to establish the link between two communicating devices because due to the small bandwidth it cannot transfer images. [2] There are some baseline payment technology introduced as,

2.1 Baseline Payment Technologies

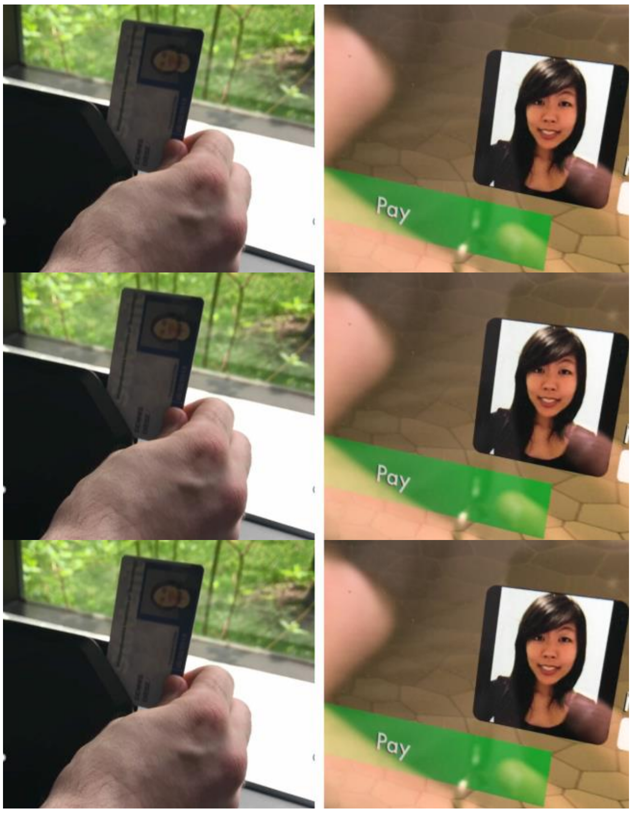
To establish a baseline, we begin with an overview of past technologies used for payment, identification, and access control and the security properties of each.

2.1.1 Magnetic Stripe Cards

Magnetic stripe cards (magstripes) were developed several decades ago [2] and have been the dominant technology used for transactions, identification, and access control since. Data on the card is organized in three tracks stored on the stripe, each with specific characteristics in terms of the information density and content it can store. The tracks encode this data by modifying the magnetism of iron-based particles [3]. However, the data is static and cannot be dynamically altered to respond to queries from a terminal (ex. even in cases of unauthorized access). As a result, magstripe cards have security analogous to handwritten notes on a sheet of paper. The static data can be written to and read from by anybody with an inexpensive ($20) skimmer. Furthermore, an adversary can write this data to a blank card and create an effective clone for slightly more ($60).

2.1.2 EMV Chip Cards

A more secure way for card-based authentication is the EMV chip, which was developed in the 2000's. EMV chip cards contain a cryptographic microprocessor that is specially designed to protect the secrets on the against unauthorized access and side channel attacks. This adds an additional layer of security through offline data authentication - a standard cryptographic check relying on public-key cryptography. The data authentication protocol is the most notable change from magstripe, as it allows the EMV chip cards to dynamically alter their responses to queries and even refuse to answer queries if they are not verified by the card issuer (ex. through offline PIN and signature verification). This provides protection against the modification or cloning of data on the EMV card. Finally, the chip itself is difficult to clone and requires expensive equipment and expertise [5] and physical possession of the card is often itself not sufficient for an adversary. However, the ID of the card doesn't change, so it is possible for a merchant, eavesdropper or malware in the terminal to track transactions made by the same card [6]. As we do not have the resources required to mount an EMV attack, we cannot perform our own analysis of EMV security.



2.2 NFC OPERATION MODES

NFC technology defines two types of devices. One is initiator device and other is target device. Initiator device is one who initiates the communication and controls the data exchanges. Target device is the device who responds to the initiator device. Active and Passive are the two operating modes of NFC [13]. In active mode, both the initiator and the target generate the RF signal on which the data is carried. In passive mode, RF signal is generated only by the initiator, and target communicates back to the initiator using a technique called load modulation. NFC uses two types of coding mechanism to transfer data, they are Manchester and Miller coding.

In addition to the two operating modes, there are three operating modes for device communication [14]. These three modes depend on the application. Figure 4 shows three operating modes of NFC technology standard. International Journal on Cybernetics & Informatics (IJCI) Vol. 4, No. 2, April 2015
137

2.2.1 Reader/Writer mode

In Reader/Writer mode of operation the application transfers data in NFC forum defined message format. In this mode the NFC enabled mobile phone can perform read/write operation on NFC tags. In Reader Mode, NFC initiator reads data from the NFC tag where as in the writer mode, initiator writes data in to the tag. It should be noted that Reader/Writer mode of communication is not secure. The applications supported by this mode are,

- Smart Poster
- Remote Marketing
- Remote Shopping
- Social Networking

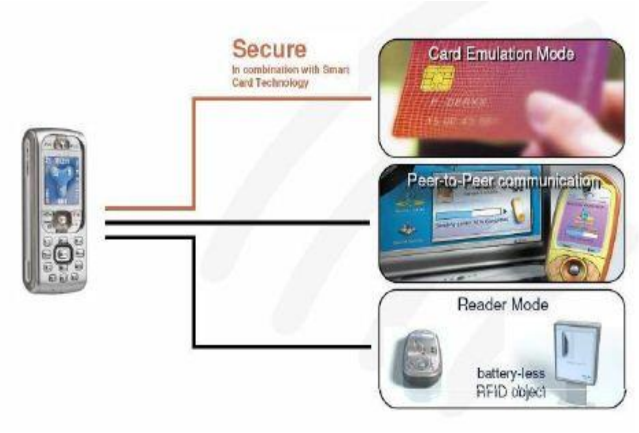

Secure
In combination with Smart Card Technology
Card Emulation Mode
Peer-to-Peer communication
Reader Mode
battery-less
RFID object

Figure 1: NFC Operating Modes

2.2.2 Card Emulation Mode

In card emulation mode, the NFC enabled mobile device acts as a contactless smart card. The examples of smart card are debit card, credit card, access cards etc. Data transfer in this mode is highly secure. This mode supports the following applications.

- Payment
- Loyalty
- Ticketing
- Access control
- Identity Services

2.2.3 Peer to Peer mode

Peer to peer mode supports link level communication. It supports two NFC enabled device to exchange information such as a text message, contact record or data of any other kind. NFCIP-1 and LLCP are the two standardized options in peer to peer mode. This mode of communication is secure. The applications supported by this mode are the following.

- Exchanging Data
- Money Transfer
- Social Networking

2.3 NFC SECURITY

2.3.1 Threats

NFC applications such as contactless money payment demand a high level of security. As NFC security has great importance, so it is to be a part of the basic NFC technology structure. Possible threats associated with NFC are explained below.

2.3.2 Eavesdropping

Eavesdropping is a common threat found in all wireless communication technologies. NFC is also a wireless communication interface between two entities [10]. They use RF signals to communicate, so any equipment with an antenna in the range can receive the signal. The attacker can extract the information from the signal transmitted through experimentation and periodic analysis processes. This is very dangerous in the case of money payments, where the users use some secret password; the eavesdropper acquires this information and can misuse it. It is very difficult to prevent eaves dropping as the attacker who uses a very precise antenna can receive the signal even if the signal strength is too weak. The only solution to eavesdropping is to use a secure channel for communication.

2.3.3 Data Corruption and Manipulation

In NFC, data is sent from sender to receiver wirelessly. There are some specific formats for data to be sent, so that the receiver accepts and decodes it [11]. The data which is not in the correct format is rejected. Data corruption and manipulation attack arises when an attacker in between corrupts or manipulates the data. The attacker may change the data format or change the contents in it, so that the data becomes useless or gets rejected as it reaches the receiver. For some coding schemes this attack is possible. The solution for this attack is to use a secure channel between the communicating parties.

2.3.4 Man- in- the Middle attack

Man in the middle attack is one step further to data corruption and manipulation attack. In this attack a third party intercepts the communication between two parties [12]. The attacker acts as a relay between the sender and receiver and forwards data (See Figure 5). The attacker can corrupt, alter, or discard the data being sent. Man in the middle attack is very difficult to achieve in NFC links and so it is not common. The solution for this attack is to use active-passive communication mode.

2.4 OVERVIEW OF NFC APPLICATIONS

This section provides an overview of NFC applications in the real world (See Figure 6) such as in retail, automotive, office, terminal, theatre/ stadium etc. NFC technology is used for the purpose of ticketing, payment, sharing (share files between phones), service discovery i.e. get information by touching smart phones etc. Some of the advantages of NFC to industrial applications are listed below [8]:

- NFC enables touch based and easy communication between two devices.
- Communication setup with NFC takes milliseconds order of time whereas for Bluetooth it is typically in seconds order.

NFC enables longer lifetime of the sensor battery in wireless sensor applications, or even battery less implementation of the sensor.

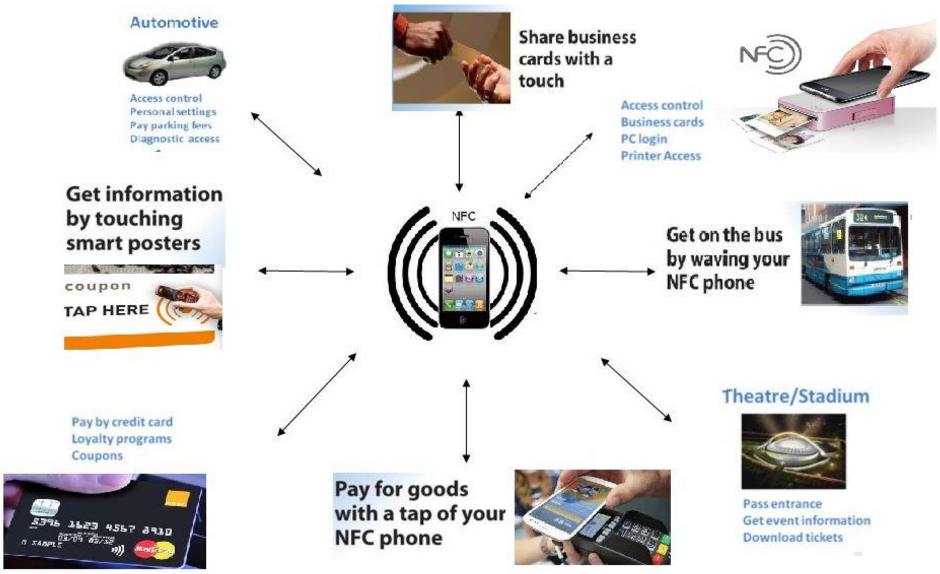


Figure 2: NFC Applications

2.4.1 NFC Ticketing

In NFC Ticketing, the user needs to carry a NFC enabled mobile phone to read and store the ticket or access code from the reader [22]. There is a ticketing sever to which a NFC reader is connected.

2.4.2 NFC Mobile Payment System

In NFC Mobile Payment System, credit card or debit card essentials of the user are stored in the secure element which is built in the OS. The merchant's NFC reader can read the essentials to transfer the money from the account to finish the payment

2.5 Advantages and Limitation of NFC:-

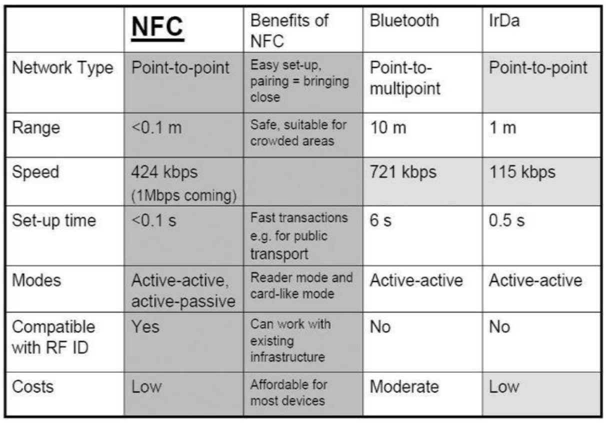
Advantages of NFC:-
1] Quicker connections.
2] Easy to use, only requires the click of a button.
3] They are compatible with existing RFID structures.
4] Cost efficient for the average customer.

Disadvantages of NFC:-
1] Only works in short ranges
2] Low data transfer rate
3] Can be costly for merchant companies to initially adopt The technologies [4].

2.6 Comparison with other Technologies:-

1)NFC and RFID Basically, the technologies Radio Frequency Identification and Near Field Communication use the same working standards. However, the essential extension of RFID is the communication mode between two active devices. In addition to contactless smart cards (ISO 14443), which only support communication between powered devices and passive tags, NFC also provides peer to-peer communication. Thus, NFC combines the feature to read out and emulate RFID tags, and furthermore, to share data between electronic devices that both have active power [8].

2)Comparison with Bluetooth and Infrared Compared to other short-range communication technologies, which have been integrated into mobile phones, NFC simplifies the way consumer devices interact with one another and obtains faster connections. The problem with infrared, the oldest wireless technology introduced in 1993, is the fact that a direct line of sight is required, which reacts sensitively to external influences such as light and reflecting objects. The significant advantage over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify the others phone, the connection between two NFC devices is established at once (<0,1s). Below figure points out these different capabilities of NFC, Bluetooth and infrared. All these protocols are point-to-point protocols. Bluetooth also supports point-to multipoint communications. With less than 10 cm, NFC has the shortest range [8]. This provides a degree of security and makes NFC suitable for crowded areas. The data transfer rate of NFC (424 kbps) is slower than Bluetooth (721 kbps), but faster than infrared (115 kbps). In contrast to Bluetooth and infrared NFC is compatible to RFID.



	NFC	Benefits of NFC	Bluetooth	IrDa
Network Type	Point-to-point	Easy set-up, pairing = bringing close	Point-to-multipoint	Point-to-point
Range	<0.1 m	Safe, suitable for crowded areas	10 m	1 m
Speed	424 kbps (1Mbps coming)		721 kbps	115 kbps
Set-up time	<0.1 s	Fast transactions e.g. for public transport	6 s	0.5 s
Modes	Active-active, active-passive	Reader mode and card-like mode	Active-active	Active-active
Compatible with RF ID	Yes	Can work with existing infrastructure	No	No
Costs	Low	Affordable for most devices	Moderate	Low

Figure 3: Comparison NFC with other Technologies.

2.7 Security Goals

1. *Confidentiality:* An adversary should not be able to view sensitive payment details (ex. card number), nor should they be able to track a user via a digital record of NFC cardless transactions.

2. *Integrity:* Transaction data should not be modified in transit between the user's phone and the merchant's payment terminal. Additionally, only a user may initiate and approve transactions, even in the case of a confidentiality breach.

3. *Availability:* The ability to perform NFC cardless payments may not be removed by persons with fewer permissions than the user (most notably the merchant).

3. CONCLUSION

In the research carried out we have tried to analyse NFC technology, its working and its advantages and disadvantages from the various research papers published related to the above topic which is Near Field Communication (NFC).). NFC has a lot many scopes in future because it makes it easier for the end users to use the technology efficiently and accurately. Though there are some security issues in the implementation to get valid data, there is research going on in various areas as how it can be implemented in fields of Health Care, Housing, making payments, institutional and educational purposes.

The corporate industries like the credit card companies are trying to merge with mobile development companies to implement the concept of NFC, so that payment can be made without having the need to carry wallets. There is a high scope in this area of technology that can bring a huge change in our day to day lives Companies like like Google and PayPal have started using this technology.

REFERENCES

[1] Gautam, Vinay, and Vivek Gautam. User Behavior Based Enhanced Protocol (UBEP) for Secure Near Field Communication.

[2] Paus, Annika. Near field communication in cell phones. Chair for Embedded Security 24 (2007).

[3] Eun, Hasoo, Hoonjung Lee, and Heekuck Oh. Conditional privacy preserving security protocol for NFC applications. Consumer Electronics, IEEE Transactions on 59.1 (2013): 153-160.

[4] Hussien, Hanady, and Hussien Aboelnaga. Design of a Secured E-voting System. Computer Applications Technology (ICCAT), 2013 International Conference on.IEEE, 2013.

[5] Roland, Michael, Josef Langer, and Josef Scharinger.Security vulnerabilities of the NDEF signature record type. Near field communication (NFC), 2011 3rd International Workshop on. IEEE, 2011.

[6] Mantoro, Teddy, and A. Milisic. Smart card authentication for Internet applications using NFC enabled phone. Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference on. IEEE, 2010.

[7] Plos, Thomas, et al. Security-enabled near-field communication tag with flexible architecture supporting asymmetric cryptography. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 21.11 (2013): 1965-1974.

[8] Gautam, Vinay, and Vivek Gautam. User Behavior Based Enhanced Protocol (UBEP) for Secure Near Field Communication.

[9] Paus, Annika. Near field communication in cell phones. Chair for Embedded Security 24 (2007).

[10] Eun, Hasoo, Hoonjung Lee, and Heekuck Oh. Conditional privacy preserving security protocol for NFC applications. Consumer Electronics, IEEE Transactions on 59.1 (2013): 153-160.

[11] Hussien, Hanady, and Hussien Aboelnaga. Design of a Secured E-voting System. Computer Applications Technology (ICCAT), 2013 International Conference on. IEEE, 2013.

[12] Roland, Michael, Josef Langer, and Josef Scharinger.Security vulnerabilities of the NDEF signature record type. Near field communication (NFC), 2011 3rd International Workshop on. IEEE, 2011.

[13] Mantoro, Teddy, and A. Milisic. Smart card authentication for Internet applications using NFC enabled phone. Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference on. IEEE, 2010.

[14] Plos, Thomas, et al. Security-enabled near-field communication tag with flexible architecture supporting asymmetric cryptography. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 21.11 (2013): 1965-1974.

[15] Konidala, Divyan M., et al. Security Framework for RFID-based Applications in Smart Home Environment. JIPS 7.1 (2011): 111-120.

[16] Haselsteiner, Ernst, and Klemens Breitfu. Security in near field communication (NFC). Workshop on RFID security. 2006.