An Overview of Near Field Communication(NFC)

BY:

Okunbor Charles, Adekunle Y.A., Adebayo Adewale, Alao O. D.,
Monday Eze, Seun Ebiesuwa.

Babcock University,
Computer Science Department, School of Computing and Engineering Sciences,
Ilishan Remo, Ogun State, Nigeria.

Abstract

Near Field Communication (NFC) is a radio frequency short range wireless communication technology used by electronic devices to communicate with other electronic NFC enabled devices in close proximity of 10cm to 20cm depending on the mode of transmission. NFC is based on and is a subset of Radio Frequency Identification (RFID) transmitting at 13.56 MHz. Devices with NFC technology have enabled users to perform contactless payments, data transfers, access digital contents, security pass/access. NFC emerged lately and a lot of research is still on going to improve this technology. This paper is an overview of NFC technology as regards data transfer, contactless transactions, mode of operation and its security.

Keywords: Near Field Communication (NFC), Radio Frequency Identification(RFID), Contactless Transactions, Data Transfer, Transmission, Security.

1.1 Introduction

Abdel-Gaber and Ali(2015) defined Near-field Communication (NFC) as a type of communication technology with short range (radiofrequency) and low power wireless for electronic devices that gives them the ability to connect and share data with other NFC enabled devices by bringing them within a close proximity. This type of transmission is also referred to as 'tap-in' or 'to tap and go'. NFC communication occurs between two active devices like smartphones, tablets, laptops having NFC technology or between an NFC device and a passive (unpowered) tag or device. With contactless transmission, users can put their device at close range or wave their smart phones over another NFC device to transmit data without the devices touching each or configuring the connection (Nearfield Communication, 2017).

The first device that initiates a communication is known as the initiator. With magnetic induction, the initiator creates a field of radio waves that the second device been targeted can detect, access and allow some volume of data to be transmitted wirelessly over a relatively short distance (NFC Forum, 2018). NFC has a coverage area of around 20 cm which is a good range when looked at from a security perspective. This short range of NFC minimizes eavesdropping and other forms of threats facing wireless technology. A good aspect of NFC is that the essential components are cheap and the quick time taken to establish a connection. Abd-Allah(2011), described NFC as a little circuit with a small antenna attached and having the ability to transmit data within a distance in response to the query of an interrogator or a reader. Contactless payment is a potential application of NFC and it is said to be the motivating force behind the development of NFC from RFID technology. Using NFC-enabled mobile phone allows secure and convenient purchases in a wide range of transactions. For example, a mobile smart phone can be used to emulate credit/debit cards and used over NFC readers/interrogators (Nagashree, Rao, &Aswini,2014).

In 2002, Philips and Sony electronics made public the collaborative intention to develop a new wireless communication technology by working together. This technology will allow user devices communicate(McHugh &Yarmey 2014). Sony and Philips in 2003 invented Near Field

Communication and ISO/IEC 18092 was adopted later that year as an interface and protocol specification for NFC's foundational functionality by the International Organization for Standardization (ISO).

Near Field Communication (NFC)Forum was established in 2004 by Nokia, Philips and Sony to promote and develop NFC technology. In 2004, NFC Forum was created but the first set of specification for NFC tags was made in 2006 by the group (Abdel-Gaberand Ali, 2015). NFC technology makes use of little objects like a sticker called tags.These tags hold data that can be captured and understood by other NFC devices like smartphones and readers/interrogators, when within range or waved over an NFC tag.NFC forum is devoted to the advancement of security, user friendliness and the acceptance of near field communication. They tutor businesses about the technology and the standards helps NFC operate between different devices. Whoever wishes to build devices that are NFC compliant must meet the standards set forth by the NFC Forum. This guarantees that NFC devices can connect and communicate with each other irrespective of the device or tag type (Near Field Communication, 2017).

According to Near Field Communication (2017), the Nokia 6131 was the first mobile cell phone with NFC technology. As the years went by, more specifications surfaced and the technology developed as well. From payment systems to sharing of files like, video, audio, contact, links and game invites between mobile smartphones and other NFC devices.The first Android NFC phone was produced in 2010 on Samsung Nexus S.

1.2 NFC Forum

In 2004, principal companies in the domain of semi-conductors, communication and electronics introduced NFC Forum as a non-profit organization. The forum aims at tutoring marketers and users about NFC so as to promote its usage. They make specifications, standards and maintain interoperability between devices and services. There are over200 universal companies partnering with them and are working towards modular NFC device architecture and much more. The members who sponsor the NFC Forum are: Intel, NXP Semiconductors, Qualcomm, Samsung, MasterCard Worldwide, NEC, Sony Corporation, Broadcom Corporation, Google Inc., STMicroelectronics, and Visa Inc. (Trivedi, 2015).

2.1 NFC Standards and Protocol

NFC is comprised of several standards and communication protocols defined by the ISO and ECMA organizations, the two major ones being ISO 14443 and ISO 18092,which are in part compatible with each other (Jakobsson, 2015).The NFC standard specifies two modes of operation and three different transfer speeds for the radio interface. An NFC device could either be active, meaning that it generates its own field or passive meaning that it relies on another device to generate a field and use load modulation to communicate (NFC Forum, 2018). The communication speeds are divided into two groups, one low speed and one highspeed. The low speed communication is done at a rate of 106 kbps and the highspeed is either 212 or 424 kbps. (ISO/IEC, 2013).

2.2 ISO 14443

The ISO 14443 standard defines the physical characteristics and transmission protocols for contactless proximity identification cards. The standard consist of four parts, each specifying a layer in the protocol stack, from the physical characteristics of the air interface to the initialization and transmission protocols(Tushie, 2012).The four parts that consist of this standard include the following;

Part	Standard	Description
1	ISO/IEC 14443-1	Explains the physical characteristics of cards
2	ISO/IEC 14443-2	Depicts the radio frequency power and signal interface. The main emphasis is on bit timings, signal waveforms and encoding used for communication. Two clearly different forms are; Type A and Type B, either form is acceptable.
3	ISO/IEC 14443-3	Describes the initialization and anti-collision provisions. This part refers to the data frames and anti-collision techniques used to discover all the cards (tags) in the electromagnetic field.
4	ISO/IEC 14443-4	Describes the transmission protocol requirements. It makes available for an optional protocol referred to as T = CL (contactless) analogous to T = 0, T= 1 protocol options used in smart cards with contacts.

Table 1.*Parts of ISO 14443 Standard*

2.3 ISO 18092

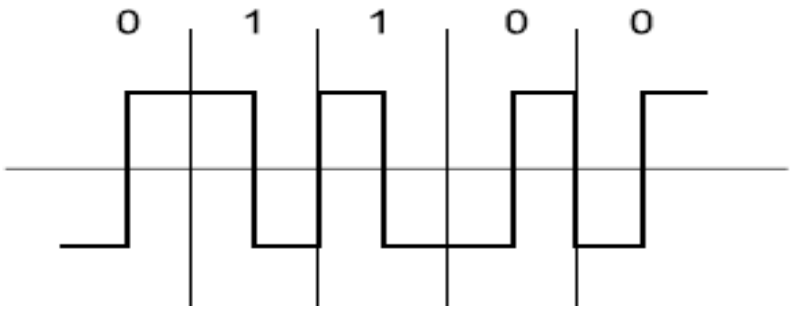
ISO 18092 is also known as NFCIP (NFC Interface & Protocol). It is the standard often referred to when talking about NFC in mobile devices (Jakobsson, 2015). As stated by NFC Forum, card emulation mode can support EMV contactless card payment application requirements for smart mobile devices as specified in EMV CCPS v2.0 and embodied by American ExpressPay 2.0, MasterCard PayPass 2.0 and Visa payWave2.1.1. Tushie (2012) stated that, there should be interoperability between NFC device and interrogator/reader (POS) operating under the ISO/IEC 18092 specification in card emulation mode.ISO/IEC 18092 also describes the process of data exchange between two devices, known as peer-to-peer mode. Examples of data that can be exchanged include; contact information, video, audio, links etc.

3.1 Modes of Communication

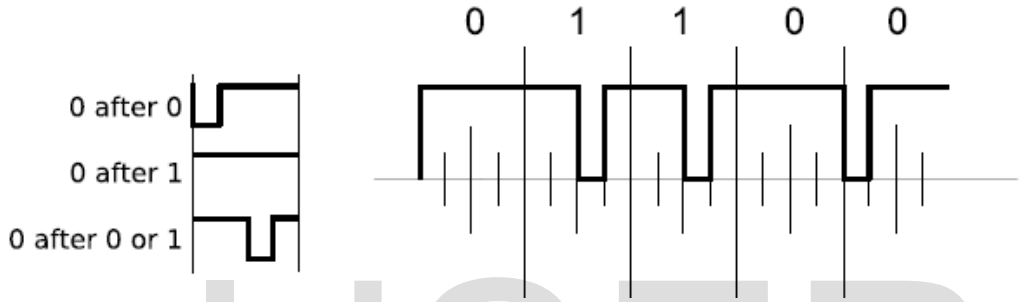
NFC communication can occur between two active (powered) devices such as cell phones or between an NFC device and a passive (unpowered) tag (Jain & Dahiya, 2015). An NFC device is said to be in active mode if the initiator and the target generate the radio frequency (RF) signal on which data is transmitted.NFC devices communicate in passive mode when the RF signal is generated only by the initiator and the target device communicates back to the initiator using a method known as load modulation (Rahul et al, 2015). Three communication configurations are possible with NFC devices, they are;

- Active – Active
- Active – Passive
- Passive – Active.

NFC configurations cannot be over-emphasized because communication and movement of data from the initiator to the target depends on the configuration of the transmitting device whether in active or passive mode. Data is transmitted using amplitude shift keying (ASK) in active mode (Castelluccia & Avoine, 2006) this implies that the base RF signal (13.56 MHz) is modulated with the data in relation to a coding format. If the baudrate is 106 kBaud, the coding scheme is the modified Miller coding. If the baudrate is greater than 106 kBaud, Manchester is coding scheme used (Abd-Allah, 2011).



Manchester code



Modified Miller code

Fig 1. *Image source: Abd-Allah, (2011).*

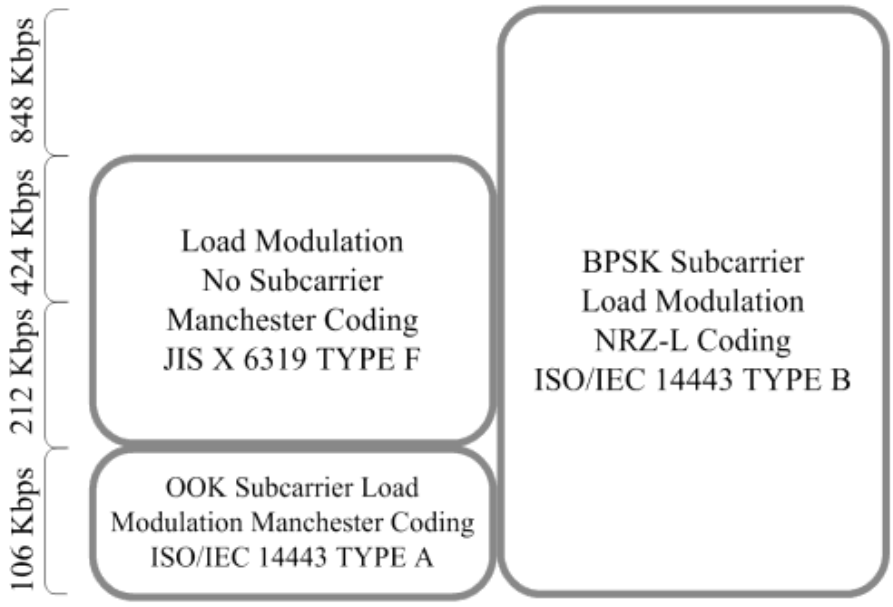
In the figure above, each and every data bit in both coding plans is sent in a fixed time slot and partitioned into two parts, called half bits. When using Miller coding, a zero is encoded with a delay in the main half piece and no interruption in the second half piece. One is encoded with no interruption in the first bit, however a delay in the second half bit. Some extra principles are used on the coding of zeros in the adjusted Miller coding. Two successive half bits would have an interruption on account of a one taken after by a zero. This can be avoided by Modified Miller coding when it encodes a zero which takes after a one directly with two half bits with no delay. The circumstance is nearly the same in Manchester coding, however contrasts by having the entire half as a delay or modulated as opposed to having a pause in the first or second half bit (Abd-Allah, 2011).

In passive mode,data is transmitted using a weak load modulation. A modulation of 10% is always used to encode data, using Manchester coding. For a 106 kBaud a subcarrier frequency is used for the modulation, for baudrates greater than 106 kBaud the base RF signal at 13.56

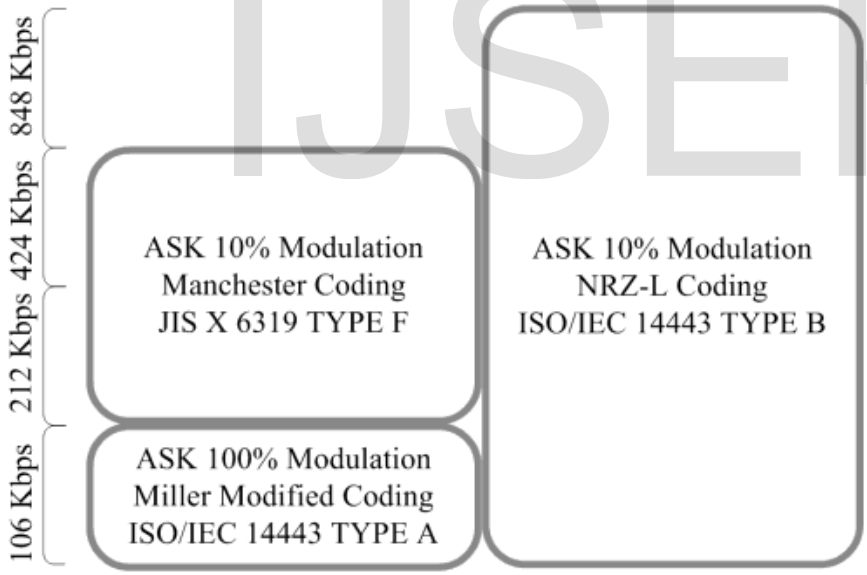
MHz. In passive mode, information is transmitted utilizing a load modulation that is weak. A modulation of 10% is always used to encode data, using Manchester coding. For a 106 kBaud a subcarrier frequency is utilized for the modulation. For baud rates larger than 106 kBaud, the base RF signal at 13.56 MHz is modulated. In active and passive mode, a device can play two roles because NFC depends on a message and answer notion, which implies that one gadget A transmits a message to another gadget B and gadget B sends back a response. It is impossible for gadget B to send any information to gadget A without first receiving some message from gadget A, to which it could respond. The gadget A that begins the information exchange by first sending a message is called initiator, the device B that receives the message and respond to it is called target (Abd-Allah, 2011).

As of today, NFC RF interface supports the transmission of data at rates of 106, 212 and 424 kbps. NFC uses different modulation schemes for data transfer like ASK (Amplitude Shift Keying) with various modulation profoundness of - 100% or 10% or load modulation and coding methods, for example, NRZ-L (Non-Return-to-Zero Level), Manchester and Modified Miller coding. According to (Coskun, Ozdenizci& Ok, 2013) the following are important when defining the modulation and coding schemes;

- the communication mode of an NFC initiator or target devices (active or passive)
- the signaling and standards used in RF interface (NFCIP-1, ISO/IEC 14443, JIS X 6319 Type F as FeliCa)
- the data transfer rate.



From Passive Device to Active Device



From Active Device to Passive Device

Figure 2.Modulation and Coding Schemes. *Image source: (Coskun, Ozdenizci& Ok, 2013).*

Abd-Allah (2011) further said that NFC transmission is not limited to a pair of NFC gadgets alone. An initiating gadget can transmit or send data to different target gadgets. In situations like this, all target gadgets are activated at the same time but before communicating information, the initiating gadget must choose a target gadget to receive the information. After a gadget is chosen

to receive the information, the information will then be disregarded by all non-chosen target gadgets. Just the chosen target gadget is permitted to reply to the received message. Hence, it is difficult to broadcast messages to more than one gadget simultaneously.

4.1 Modes of Operation

NFC devices can operate in three modes. They are;

- Reader/writer mode
- Peer-to-peer mode
- Card emulation mode

The figure below shows the three operating modes of an NFC and the services offered by these modes.

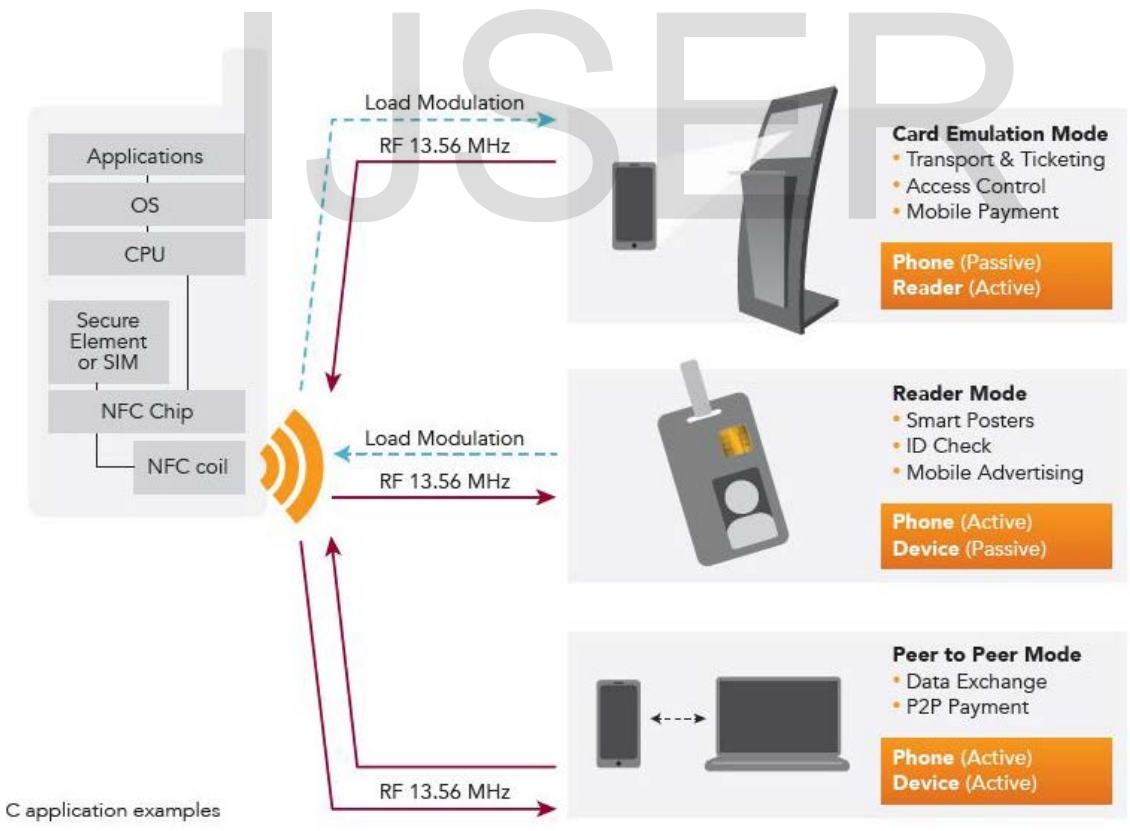
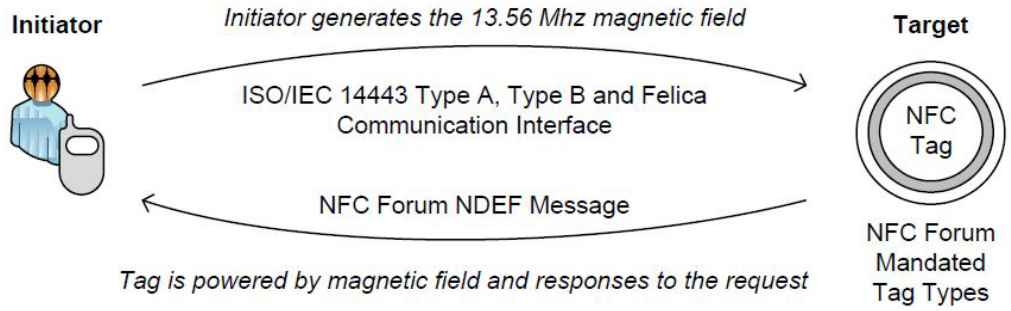


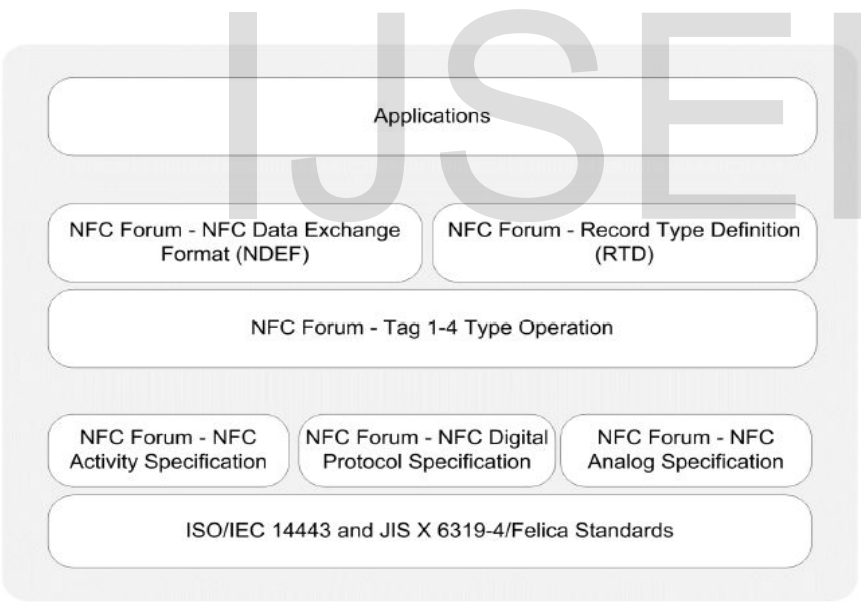
Figure 3.NFC operating modes and services offered (*Image source:Litepoint, 2016).*

4.1.1 Read/write Mode

An NFC device is said to be operating in Reader/Writer mode when it is used to read from or write to an NFC tag or NFC smart card in an NDEF message format. This is supported by the ISO 14443 standard and an extension of the Mifare and FeliCa standards (Jakobsson, 2015). NDEF (NFC Data Exchange Format, NDEF) defines the format of data to be exchanged between two active NFC and passive tag or active NFC device and active NFC device.



Reader/Writer Operating Mode

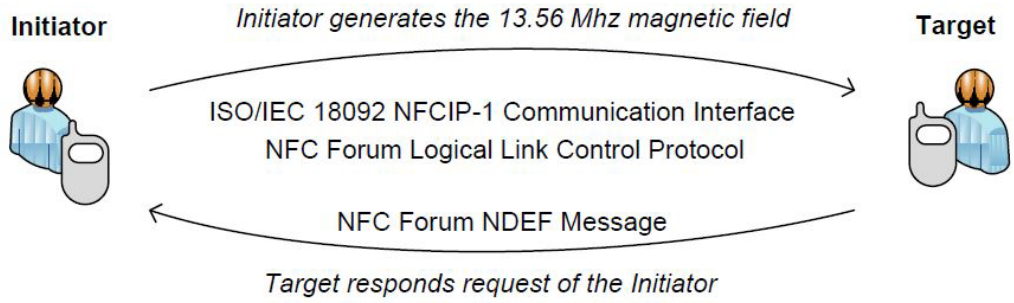


Protocol stack of reader/writer operating mode.

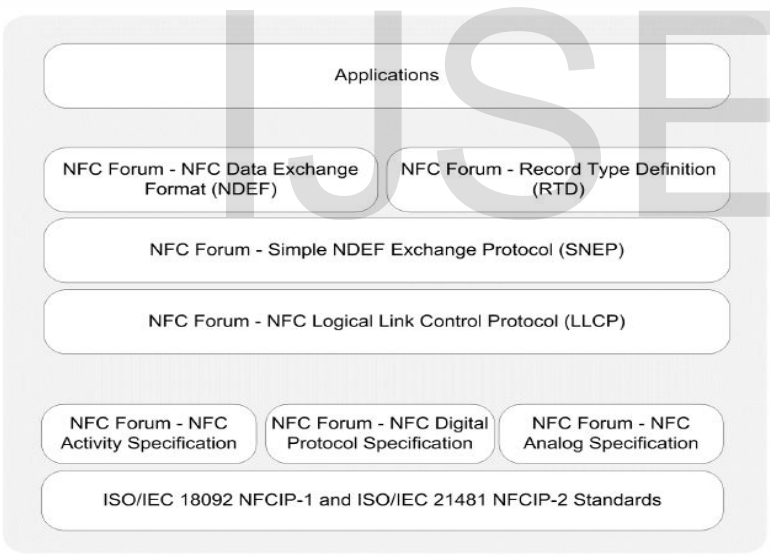
Figure 4.*Image source: Coskun, Ozdenizci and Ok (2015).*

4.1.2 Peer-to-Peer Mode

Peer-to-peer mode enables two NFC devices to share data between themselves.The data shared could be anything from digital business cards to setup parameters for Bluetooth communication. The peer-to-peer functionality is implemented through the use of the LLCP and SNEP protocols that build on top of the ISO 18092 standard (Jakobsson, 2015).



Peer-to-Peer Operating Mode



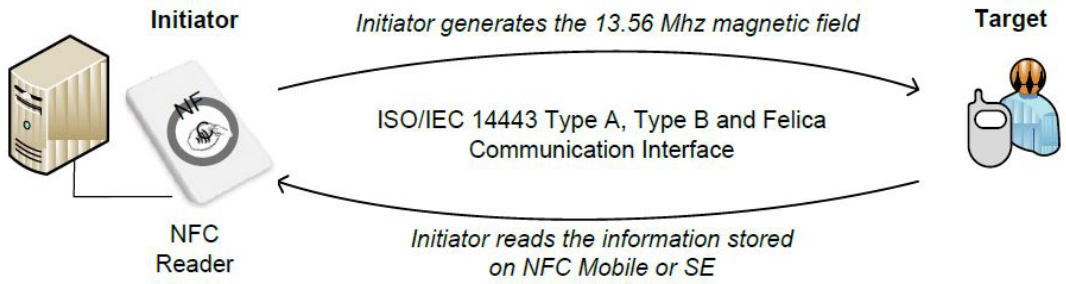
Protocol stack of peer-to-peer operating mode.

Figure 5.*Imagesource: Coskun, Ozdenizci and Ok, (2015).*

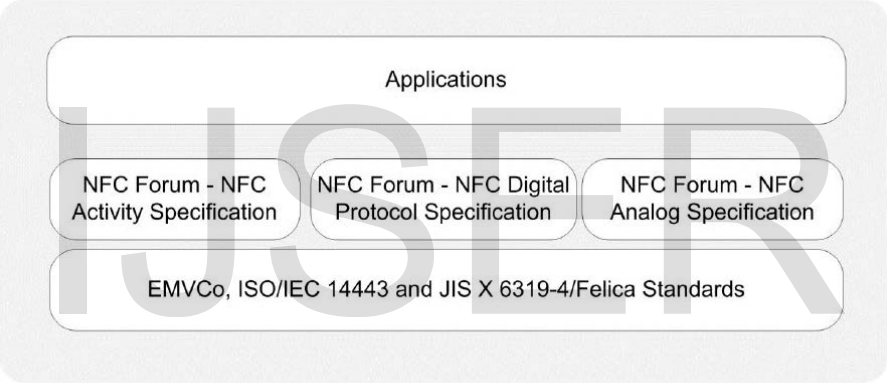
4.1.3 Card Emulation Mode

With card emulation mode, user with NFC smartphones can put their mobile device very close to an NFC reader or interrogator, in other for the smartphone to behave like a standard smart card (Coskun, Ozdenizci, Ok, 2015); This enables the NFC device to be used in contactless payment or ticketing systems without needing to change the existing infrastructure. Jakobsson, (2015)sees

the card emulation mode as a very versatile communication mode, but has a drawback in that it requires a secure element to function.



Card Emulation Operating Mode



Protocol stack of card emulation operating mode.

Figure 6.*Image source: Coskun, Ozdenizci and Ok (2015).*

4.2 Types of NFC Tags

NFC tags are a passive device that has the ability to communicate and share data with active NFC gadgets. NFC is applied in posters, security systems and other area where little measures of data needs to be transmitted and read. Four basic types of tag with 1 to 4 allocated to each having different formats and storage size. These NFC tags with different formats are based on ISO 14443 Types A, B and Sony FeliCa (Minihold, 2011).

Type 1 and 2 can hold up to 48 bytes with a data rate of 106kbps and can be extended to hold up to 2kb of information. Type 3 (FeliCa) operates at 212kbps and can hold up to 1 Mb of data. Type 4 has a data rate of 424kbps and hold 32kb of information. Type 1 and 2 are produced as

rewriteable and can be overseen by a user and set to read-only by locking it while Types 3 and 4 are configured as either rewriteable or read-only (Minihold, 2011). The table below summarizes NFC tags, data rates, memory and products compatibility.

NFC Type definition				
	Type 1	**Type 2**	**Type 3**	**Type 4**
ISO/IEC standard	14443 A	14443 A	JIS 6319-4	14443 A / B
Compatible Product	Innovision Topaz	NXP MIFARE	Sony FeliCa	NXP DESFire, SmartMX-JCOP,
Data rate	106 kb/s	106 kb/s	212, 424 kb/s	106/212/424 kb/s
Memory	96 bytes, expandable to 2 kbyte	48 bytes, expandable to 2 kbyte	Variable, max. 1Mbyte	Variable, max. 32 kbyte
Anti-collision	No	Yes	Yes	Yes

Table 2.*NFC tag types*(Minihold, 2011)

4.3 NFC and RFID Technology

The fundamental operationalbasic of Near Field Communication is rooted on RFID technology. NFC is a subset of RFID, RFID is a much wider technology (Trivedi, 2015). RFIDreaders are devices that constantly broadcast Radio Frequency (RF) signals and hangs on for atag to respond. They are also known as initiators or interrogators. Readers can be immobile (stationary) or mobile (movable). Tags are also known as transponders; they essentially consist of a microchip with an antenna. There are three types of tags:

- Passive tags
- Active tags
- Battery Assisted Passive tags

Passive tags are those tags that do not contain battery while Active tags have battery and are constantly transmitting signal. Battery Assisted Passive (BAP) tags are those tags that their batteries are activated when they sense or detect an RF field (Abdel-Gaber and Ali, 2015).

NFC tags are similar to RFID tags in design and they both use 13.56 MHz frequency. At these frequency ranges, RFID tags typically use the theory of Strongly Coupled Magnetic Resonance

which primarily depends on two proximate loop antennae that give strong electromagnetic mutual induction resonance. This effect can also be referred to as inductive coupling while in operation, other transmission frequencies are deactivated and this increases the communication speed between coupled resonances. This is only possible for loop antennae that are placed very close to each other. The strength of the initiator among other factors determines the precise coverage of the range which is only a few centimeters. This few centimeters under certain conditions can be increased to 20 centimeters. The table below shows a comparison of NFC and other similar technologies (Abdel-Gaber& Ali, 2015).

	NFC	RFID	IrDa	Bluetooth	Wi-Fi	ZigBee
International Standard	ISO 14443	-	-	IEEE 802.15.1	IEEE 802.11	IEEE 802.15.4
Set-up time	<0.1ms	<0.1ms	~ 0.5sec	~ 6sec	3-5 sec	30ms
Range	Up to 10 cm	Up to 3m	Up to 5m	Up to 30m	50-100m	10-100m
Operating Frequency	13.56 MHz	125KHz-2.5 GHz	800-900 nm	2.4 GHz	2.4 and 5 GHz	868 MHz (Europe)
Maximum Data Rate	0.42 Mb/s		20-40 and 115 kbits/s	3 and 22 Mb/s	11, 54 and 144 Mb/s	20, 40 and 250 kbits/s
Complexity	Low	Low	Low	Hi	Hi	Low
Usability	Human centric Easy, intuitive, fast	Item centric easy	Data centric easy	Data centric medium	More complex (Point to hub)	wireless mesh network
Selectivity	High, given, security	Partly given	Line of sight	Who are you?	Selective and secure	secure communications
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset	Wireless LAN connectivity, broad band access	Industrial control Home Control Building automation Smoke and intruder warning.
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed	Configuration needed	Devices can join an existing network
Cost	Low	Low-High	Low	Low	Hi	Low
Power Consumption	∞	Hours/days	days	Hours/day	Hours	Very low months/years
Directional Communication	Two way	One way	One way	Two way	Two way	Two way

Table 3: Abdel-Gaber and Ali, (2015)

4.4 NFC Security and Privacy Concerns

NFC as a technology has similar characteristics with other information systems that are subject to attacks just like other wireless forms of data communication especially when used for contactless payment purposes. The short range at which NFC transmit gives it an advantage over

many threats unlike other wireless technologies with wider range. This advantage position of NFC technology does not guaranty complete security for NFC.The following are the possible security and privacy issues facing NFC.

- **Eavesdropping**

When eavesdropped, an attacker is able to intercept and read messages. Eavesdropping is hard to avoid because transmitted signals to a recipient need to be reliably received and for this to be possible, it requires some amount of signal strength. An attacker only need a percentage of the transmission to eavesdrop (Poole, 2017).NFC communication mode is enormously affected by eavesdropping. This is so because the transmitted data on NFC tags in active and passive mode are coded and modulated differently. It is easier for an attacker to eavesdrop on data transmitted with stronger modulation. Passive devices, which does not generate its own RF field, is more difficult to attack than an active device (Abd-Allah, 2011). As discussed earlier, the short range of NFC can help minimize this type of security threat(eavesdropping) as the attacker has very short range of signals to intercept.This attack can also be avoided by establishing a secure channel using a session secret key but doing this is not an easy task to accomplish(Abd-Allah, 2011).

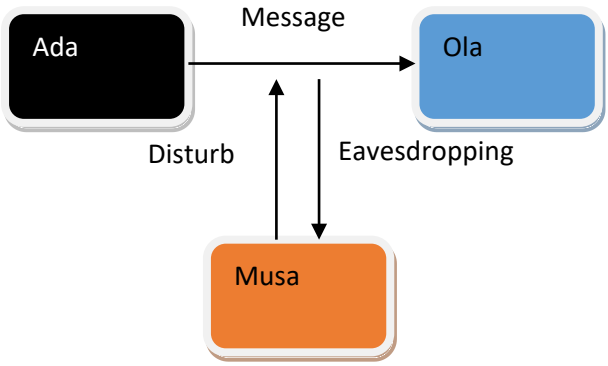


Figure 7: Eavesdropping.

- **Data Corruption and Manipulation**

This type of attack occurs when an attacker manipulates and falsify the data being transmitted to a reader or tag and as a result gets corrupted and useless on arrival to the recipient. Data

corruption can be accomplished by broadcasting valid frequencies of the data spectrum at a targeted time(Abdel-Gaber & Ali, 2015).

- **Man-in-the-Middle-Attack**

Man-in-the-Middle Attack can be described with this scenario; two parties named Ada and Ola want to talk to each other but are tricked into a three party discussion by an attacker Musa, as shown in Figure 7.Assuming Ada is communicating using active mode and Ola is in passive mode, the following situation will take place; Ada generates an RF field and transmits data to Ola. If Musa is in close proximity of the transmission, he can eavesdrop the data sent by Ada. Additionally, Musa have to actively interrupt the communication of Ada so that Ola will not receive the data. This is possible for Musa, but this can also be detected by Ada. Ada can stop the key agreement protocol if she discovers the interruption (Abd-Allah, 2011).

- **Theft**

A stolen phone can be used to make fraudulent purchases when waved over a card reader or POS. No form of encryption can stop a consumer's phone from being stolen. A thief can go ahead to download all card information from the acquired device. Theft can be avoided by using locks and multiple factor authentication system on the phone.

5.1 Conclusion

Near-field Communication (NFC) is a type of communication technology with short range (radio frequency) and low power wireless for electronic devices that gives them the ability to connect and share data with other NFC enabled devices by bringing them within a close proximity. This technology is playing an important role in today's smart world. It has proffered solution in various fields especially in the area of payments by converting them to contactless technologies. This is evident in the recent contactless payment systems used in ticketing and purchase. It has modernized and enhanced the area of security as used in access control, data collection and exchange. This paper presented an overview of NFC, its standards and protocol, communication and operation mode and its security challenges. NFC is a new technology and more work is being done by academic and industrial researchers to improve its communication mode and use.

References

Abdel-Gaber D., Ali A. (2015). Near-Field Communication Technology and Its Impact in Smart University and Digital Library: Comprehensive Study. *Journal of Library and Information Sciences*, Vol. 3, No. 2, pp. 43-77. ISSN 2374-2372

Abd-Allah M.M. (2011). Strengths and Weaknesses of Near Field Communication (NFC) Technology.*Global Journal Of Computer Science And Technology.* Volume 11 Issue Version 1.0

Coskun V., Ozdenizci B., Ok K. (2013). A survey on Near Field Communication (NFC) technology.*Wireless Personal Communications.*Volume 71 Issue 3, Pages 2259-2294

Castelluccia C., Avoine G. (2006). Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags.*Proceedings of CARDIS.* LNCS 3928, 289-299.

Coskun V., Ozdenizci B., Ok K. (2015). The Survey on Near Field Communication.*Sensors 2015*. Basel, Switzerland. ISSN 1424-8220

Jakobsson A. (2015). Secure Authentication in Near Field Communication based Access Control Systems. *School of Information and Communication Technology KTH Royal Institute of Technology*.Master of Science Thesis TRITA-ICT-EX-2015:102. Stockholm, Sweden.

Jain G., Dahiya S. (2015). NFC: Advantages, Limits And Future Scope. *International Journal on Cybernetics & Informatics*. Vol. 4, No. 4

Litepoint (2016). Test considerations for NFC enabled devices in manufacturing. Retrieved on 2nd January, 2018 from; *litepoint.com/wp-content/uploads/2016/09/NFC-Whitepaper-090116.pdf*

McHugh, S., Yarmey, K. (2012). Near Field Communication: Introduction and Implications. *Journal of Web Librarianship*, *6*, 186-207.

Minihold R. (2011).Near Field Communication (NFC) Technology and Measurements.*Rohde& Schwarz NFC technology and measure.* Retrieved on 4th January, 2018 from; https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma182/1MA182_5E_NFC_WHITE_PAPER.pdf

Nagashree R N, Rao V., Aswini N, (2014). Near Field Communication. International *Journal of Wireless and Microwave Technologies*, vol.4, no.2, pp.20-30

Near Field Communication (2017).History of Near Field Communication. Retrieved on 8th January, 2018 from; http://nearfieldcommunication.org/history-nfc.html

NFC Forum (2018). NFC Forum Specification Architecture. Retrieved on 8th January, 2018 from; https://nfc-forum.org/our-work/specifications-and-application-documents/specifications/

NFC Forum (2018). Protocol Technical Specifications. Retrieved on 8th January, 2018 from; https://nfc-forum.org/our-work/specifications-and-application documents/specifications/protocol-technical-specifications/

NFC Forum (2018). What is NFC? Retrieved on 8th January, 2018 from; https://nfc-forum.org/what-is-nfc/

Rahul A., Krishnan G., Krishnan H.U., Rao S. (2015). Near Field Communication (NFC) Technology: A Survey. *International Journal on Cybernetics &Informatics.*Vol. 4, No. 2, pp. 133-144.

Poole I. (2017). NFC Security.Retrieved on 7th January, 2018 from; http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-security.php

Tushie D. (2012).An Introduction to NFC Standards. Retrieved on 6th January, 2018 from; www.icma.com/ArticleArchives/StandardsOct12.pdf

Trivedi D. (2015).Near Field Communication.*Department of Computer Science and Engineering Institute of technology NirmaUniversity.*Master of Technology in Computer Science and Engineering. 14MCEI25.