Technical report, IDE1062, Sept 2010

A SURVEY ON NEAR FIELD COMMUNICATION IN MOBILE PHONES & PDAS

Master's Thesis in Computer Systems Engineering

IMHONTU, EROMON EMMANUEL

&

KUMAH, YAW OWUSU

School of Information Science, Computer and Electrical Engineering
Halmstad University

Touch to Share

Touch to Discover

Touch to Pay

Touch to Ticket

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

September 2010

Description of cover page picture/figure:
NFC Operating Modes (reproduced with permission of Meraj Chhaya).

Acknowledgements

We would like to express our sincere gratitude to the God Almighty for his protection & guidance in the face of hard times.

We dedicate our project work to our parents, for their prayers and immense support during this period of our studies in Sweden.

We would also like to convey our special thanks to our supervisor Urban Bilstrup, IDE-Halmstad University-for his help and guidance towards the achievement of our project goals.

IMHONTU, EROMON EMMANUEL & **KUMAH, YAW OWUSU**

Halmstad University, Sept 2010

Abstract

The last few years has witnessed a fast growth in technological advancement which has led to the development of several consumer electronic devices for different purposes or functionalities. For convenience and efficiency, there is the need to bring together all the different functionalities of these devices into a single multipurpose device such as mobile phone with the help of NFC (near field communication) technology.

The need for NFC technology in mobile devices is fast gaining popularity in some countries, especially with the successes recorded in some of the NFC pilot projects. The NFC enabled mobile device is very intuitive; works with already existing infrastructures (i.e. ISO/IEC 14443 smartcards and it readers), allows for multiple applications, has a high level of security and comes with unique and attractive features, such as the ability to serve as both reader and writer modes, etc. NFC standards are specified by NFC Forum and it has a well organised ecosystem.

This thesis is focused on the potentials of NFC and how it is used as a multipurpose device.

Contents

List of Figures & Tables

List of Acronyms and Abbreviations

NFC	Near Field Communication
RFID	Radio Frequency Identification
NXP	Next eXPerience
ISO	International Organization for Standardization
IETC	International Electro Technical Commission
RF	Radio Frequency
OCR	Optical Character Recognition
PDA	Personal Digital Assistant
UHF	Ultra high-frequency
NDEF	NFC Data Exchange Format
URL	Uniform Resource Locator
XML	Extensible Markup Language
URI	Uniform Resource Identifier
RTD	Record Type Definitions
IrDA	Infrared Data Association
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operators
TSM	Trusted Service Manager
IC	Integrated Circuit
ECMA	European Computer Manufacturers Association
UICC	Universal Integrated Circuit Card
SDK	Software Development Kits
RTD	Record Type Definitions
AEE	Application Execution Environment
SE	Secure Element
OTA	Over-the-Air
NFCIP	NFC Interface and Protocol
TEE	Trusted Execution Environment
WG	Working Group

TF	Task Force
MODEM	Modulator-Demodulator
WI FI	Wireless Fidelity
ASK	Amplitude-shift keying
POS	Point of Sale
PCB	Printed Circuit Board
POS	Point of Sale
PCB	Printed Circuit Board
P2P	Peer-to-Peer
ADSL	Asymmetric Digital Subscriber Line
SAM	Scalable ADSL Modem
AES	Advanced Encryption Standard
3DES	Triple Data Encryption Standard
UART	Universal Asynchronous Receiver/Transmitter
CRC	Cyclic Redundancy Check
SPI	Serial Peripheral Interface
I2C	Inter Integrated Circuit

1 INTRODUCTION

One of the emerging developments in the mobile communication industry is the use of cell phones for multiple applications and functions. In the last few years, different wireless technologies have been integrated into mobile phones for various functionalities and services. All these innovations have been put into mobile phones to make them friendlier and almost indispensable.

Near Field Communication (NFC) is an evolving technology with touch-based interaction, a new feature in the mobile industry. It has several new possibilities, such as travelling on the subway, unlocking the door and performing other activities by simply bringing an NFC compatible handset close to a compatible NFC reader.

NFC is a short–range radio technology based on RFID technology and allows communication between devices in close proximity. It operates in an unregulated radio frequency band of 13.56 MHZ and can interoperate with existing contactless smartcards as well as RFID standards. It has a data transfer speed of 106-424 kbps [12]. Its operating modes are based on contactless smart card standards (ISO/IEC 18092 NFC IP-1 and ISO/IEC 14443). With the use of this technology, devices such as mobile phones are designed to carry out similar functionalities such as existing contactless cards [11].

Some of the distinctive features of NFC from other existing short-range wireless communication technologies such as Bluetooth and WIFI are that, it uses a technique known as magnetic coupling, which allows a passive device to absorb energy from an active device in close proximity during inductive magnetic coupling. It also has a short transmission range of less than 10cm, which makes it very secure and protects it against attackers [1].

With the adoption of NFC technology in the mobile industry, it will be possible for anyone to depend on the mobile phone for several activities such as the payment of goods and services, event ticketing, merchandise, access to security doors, download advertisement on a smart poster to a mobile phone, etc. All these are possible with the inception of an NFC-enabled phone. NFC supports the use of mobile equipment by touch-based interactions and can be carried out basically by the user in different modes, such as Touch & Go, Touch & Confirm, Touch & Connect, Touch & Explore, thereby leading to numerous use cases in end user electronics [29].

NFC technology can also be use for embedding information into consumer products such as product information, mcoupons (mobile coupons) etc.

This technology is beginning to gain ground in Japan and South Korea, and successes have been recorded in some of the NFC pilot projects taking place in different parts of the world. Analysts are confident that NFC could emerge in the USA's markets before the end of 2010 and could rise to the peak in the next two to three years [18] [23].

In late 2002, NFC was jointly developed by NXP/Philips semiconductors, Sony and Nokia. In December that same year, the technology was adopted by the European Computer Manufacturers Association (ECMA) international [11] and was approved a year later by the International Organization for Standardization (ISO) and the International Electro Technical Commission (IETC).

1.1 Motivation

Short-range communication technologies have been very useful in the development of various applications for devices, ranging from payment of goods and services, downloading information, sharing data between two devices, etc. To reduce the inconvenience of carrying about different devices, there is the need to integrate these functionalities into a single device with multifunctional capabilities with the help of NFC-enabled mobile phones. The motivation for this survey is due to the wide usage of mobile phones as well as its interactive features, such as user interface, vibration, ringtones etc, and the multifunctional capabilities of NFC technology, which includes its interoperability with existing contactless smartcards as well as RFID. Our idea is that the integration of these two technologies (NFC and mobile phone) into a single device will make a very useful device with several possibilities

1.2 Goal

This survey is conducted on near field communication in mobile phones and PDAs. It presents an overview on how an NFC mobile device embeds various functionalities, including that of existing contactless devices, its compatibility and benefits over existing technologies used in consumer electronic devices. The goal of this thesis is to show how the use of NFC technology on mobile devices will make life better, based on qualitative comparison with existing technologies used in related consumer electronic devices and the benefits that are derived from other new possibilities that are present in NFC enabled devices.

1.3 Methodology

We will carry out a survey on NFC technology and other existing technologies that have been used over the years. A study will be carried out on the benefits of the techniques used in these technologies. A qualitative comparison with other existing technology will be made and a conclusion on why the use of NFC technology on mobile device is preferred to some other technologies. We will also look at the future of NFC in our global village and the possible areas where it is used now and where it could be used in future.

To accomplish these tasks, we will use relevant research scientific papers, articles, books and web engines to acquire relevant information for our survey. We will formulate case scenarios of the use of NFC on mobile phones based on its functionalities and draw our conclusions on its benefits over conventional methods.

2 AN OVERVIEW OF NFC AND OTHER RELATED TECHNOLOGIES

2.1 Some Common Definitions

2.1.1 Tag

A tag is a data carrier object that can be read and perhaps written on with the help of radio technology. Mainly, tags do not have their own power supply. They get powered by the generation of electromagnetic field by the reader/writer. A tag draws power from the reader, revitalizing the circuits in it. Thereafter, it sends information stored in its memory to the reader [16]. Tags that undergo this process are known as “passive” tags. When a tag comes into contact with a reader, the tag modulates the field and transmits the data. There exists varying sizes of tags for the storage of information or data. The larger the memory capacity, the longer time it takes to access information from it. Some tags are designed to contain permanent information, and cannot therefore, be modified, whereas others can be reprogrammed with new information.

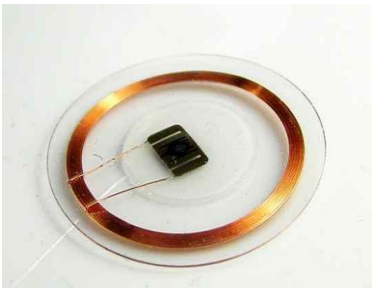


Fig.1 *An example of a passive tag [36]*

2.1.2 Contactless Card

A contactless card, as the name implies, is a contact-free card with an embedded chip containing information that can be read by a reader. Contactless cards do not require contact with the reader or either swiped in a slotted electronic device in order to obtain information contained in it. A contactless card has similar characteristics as a tag, but has a secure element inbuilt. The secure element contains sensitive information or confidential electronic data. The information embedded in the secure element is protected by means of encryption. This helps to prevent data breaches and attacks.

Fig.2 *A reader accessing information on a contactless card*

('Image courtesy of Tailwind Solutions and i4 Product Design')

2.1.3 Reader/Writer

A reader/writer is a device that is capable of reading and writing to tags as well as contactless cards. In order for a reader to communicate with passive tags and contactless cards, it creates an electromagnetic field from which the tag or contactless card gets its operating energy and subsequently modulated for data transmission to take place. RFID tags and contactless cards come in various kinds. The reader/writer is as well designed to suit dissimilar types of tags or contactless cards.

2.1.4 Radio Frequency Identification

RFID stands for "Radio Frequency Identification". RFID is a series of specifications that describes the identification via radio technology. RFID came to replace earlier used automated systems, e.g. barcode systems, optical character recognition, etc. RFID operates in different frequency, ranging from several kHz to GHz, with different transmission ranges. The two basic types are the passive (which has no power supply) and active (with own power supply) tags. Among the range of frequencies of RFID specifications, NFC uses only the frequency of 13.56 MHz with passive tags [17].

2.1.5 Contactless Card transmission

ISO 14443 is the best recognized standard for contactless card communication. It identifies two types of cards, namely: Type A and Type B. Type A contactless card was initially planned to contain just a memory card, nonetheless, modifications were made whereby a microprocessor and cryptographic card were integrated. The most widespread Type A cards found on the open market are Mifare cards. Mifare is an open architecture platform and has more than 300 million cards in the field worldwide [14]. They have a short read range and were designed initially to handle payment operations in the transportation arena. The ISO 14443 Type B contactless card was also initially proposed to be a microprocessor version of Type A, but eventually cryptographic and memory options were incorporated. Type B cards are not common in the market compared to Type A.

Fig.3 *Contactless card (Reproduced with permission of James Booker)*

2.1.6 Secure Element (SE)

This is a combination of hardware, software, interfaces and protocols that are inserted into a mobile handset in order to facilitate secure storage of information. It is made up of an

embedded processing element which guarantees that the outside communication is processed in an encrypted form and ensures that information stored is protected and made available only under certain conditions. The protected data in the secure element is transmitted in an encrypted form with the aid of NFC. Secure Element (SE) offers a secure area for the execution of the application in addition to the protection of the payment assets (e.g. payment application code, keys, etc). SE can also be involved in the authentication process, along with the storage of applications that has nothing to do with payment, but still requires a security mechanism.

2.1.7 N-Mark

N-Mark trademark, developed by NFC Forum, enables easy identification of locations where an NFC-enabled device can be used [26]. It shows spots where an NFC Forum tag and an NFC-enabled device can set up a connection. N-Mark Trademark has user guidelines that form the rules that govern the usability of N-Mark in connection with NFC Forum tags. This practice creates and guarantees a strong visual global presence and credible products in all varieties of NFC Forum tags soon to be available in the world market [26].

Fig. 4 *N-Mark Trademark* (copyright NFC forum) [26]

2.2 Some Common Automated Systems

2.2.1 Barcode

For several years, the barcode system has been in use for automated identification processes across the globe. A barcode can be simply referred to as a binary code which has a field of bars and gaps arranged in a parallel pattern. The bars and gaps are assembled to correspond to a programmed pattern and they symbolize a data element that refers to an associated symbol. The order of arrangements comprises wide and narrow bars as well as gaps which can be read numerically or alphanumerically. An optical laser is used scan across the bars and gaps to figure out the predetermined order. Below is an example of a barcode:

Fig.5 *A barcode*

2.2.2 Optical Character Recognition

The optical character recognition (OCR) was developed and first used in the 1960s. It consisted of special fonts designed in a stylized manner, in way to make it easily readable in the usual way by humans and automatically by machines. OCR came with the advantages of being able to read data visually in critical times and could contain a high density of information. OCR was used in several areas, such as registration of cheques at the banks, shops, administrative sections etc. However, OCR was considered expensive and involved complex readers in its operation.

2.2.3 Smart Card

The smart card was introduced with additional capabilities, like the ability to be reprogrammed, a larger data storage, data processing, etc as compared to the earlier mentioned technologies. A smart card is an electronic data storage system with added computing functionalities. There exist two different groups of smart cards, i.e. one with a microprocessor incorporated and the other without. The first smart cards came into being in the form of prepaid telephone cards and got underway in 1984.

Smart cards have integrated circuits which give them the ability to store data. Those that have no microprocessors are considered to play a role as memory cards. Smart cards with microprocessors can carry out extended capabilities, such as calculations of data. Information contained on a smart card can be accessed by inserting it into a reader. When a smart card is put in a reader, a galvanic connection is formed between the reader and the contact surfaces of the smart card with the help of contact springs created on the reader. Through these contact surfaces, energy and clock pulses are made available to the smart card by the reader. Data is thereby transferred in a bidirectional serial interface between the reader and the smart card. The introduction of smart cards has tremendously helped in data protection against manipulation and unauthorized access. They are easier to use, cheaper in cost and safe to use; however, the cost of maintaining the readers is expensive and its contacts are easily exposed to dirt, corrosion etc.

2.2.4 RFID Systems

Radio frequency identification (RFID) is a technology for contactless identification of transponders through a reader (interrogator) [16]. A transponder is basically a microchip connected to an antenna and a reader is an antenna able to read information from the tag. Objects can be labelled with transponders, containing a variety of data, and giving an opportunity to uniquely identify and track the objects. This is a capability that is highly desirable in many situations and this technology is expected to have a rapid growth in the future.

2.3 How RFID Technology works

The two basic components of an RFID system are the reader (interrogator) and the transponder (data-carrying device), often referred to as a “tag”. Tags come in a great range of varieties with different capabilities. They are often categorized by their power source. Active tags have an internal power source while passive tags are powered by the signals from the reader. The communication happens by the antennas emitting radio frequency fields and modulating a signal.

2.3.1 Active versus Passive Tags

The internal power source of active tags powers a transmitter that sends back a signal to the reader, thereby increasing the distance from which the tags can be read. An active tag is more expensive than a passive tag. The operating frequencies of RFID tags in three frequency ranges which are Low frequency (LF) tags (125 and 134KHz), high frequency (HF) tags (13.56 MHZ), and ultra high frequency (UHF) tags (865MHz and 950MHZ) [19].

A tag operating in the low-frequency (LF) or high-frequency (HF) bands is power-driven by a mechanism known as inductive coupling. An electromagnetic field is created between the reader and the tag, which provides a channel for communication. The tags operating in the ultra high-frequency (UHF) band are powered by propagation coupling. A tag will use the electromagnetic energy from a reader's radio-waves to send back an altered signal by changing the load on the antenna. This can be done either by changing the amplitude phase or frequency of the signal [19].

2.3.2 Frequency bands

As previously mentioned, RFID tags can operate at different frequency bands and it is argued that the operating frequency of a system should be dependent on the specific application to facilitate system performance. In real implementation of such systems, this approach alone is not practical due to regional regulations regarding available frequency bands and allowed signals.

2.4 How NFC Technology works

NFC device uses a magnetic inductive coupling to transmit energy and data from one device to the other within a close distance [1]. An NFC device that has its own internal power supply is called active while a device without internal power supply is known as passive example is smart cards. During inductive coupling passive devices absorbs energy from an active device within a required distance which allows the passive device to communicate and exchange data with the other device. An NFC device can act as passive and active device.

2.4.1 Components of an NFC chip

NFC manufacturer integrates an NFC system's antenna, analog modulator/demodulator which is use for sending and receiving signals, and digital circuitry onto a single silicon chip. Other components of the chip are RF-level detector and card-mode detector.

The RF-level detector is used to identify the presence of a nearby NFC radio field by turning it to recognize 13.56MHz signals. The card-mode detector recognizes the type of contactless technology for example Sony's FeliCa and Philip's Mifare cards.

Figure 6 shows Philips Semiconductors' PN511 near-field-communication transmission module which contains an NFC chip. Outgoing and incoming signals from other devices are processed by analog circuitry. The contactless UART element handles the technology behind the main communications .The FIFO buffer allows transfer of data between the host and contactless UART [1].

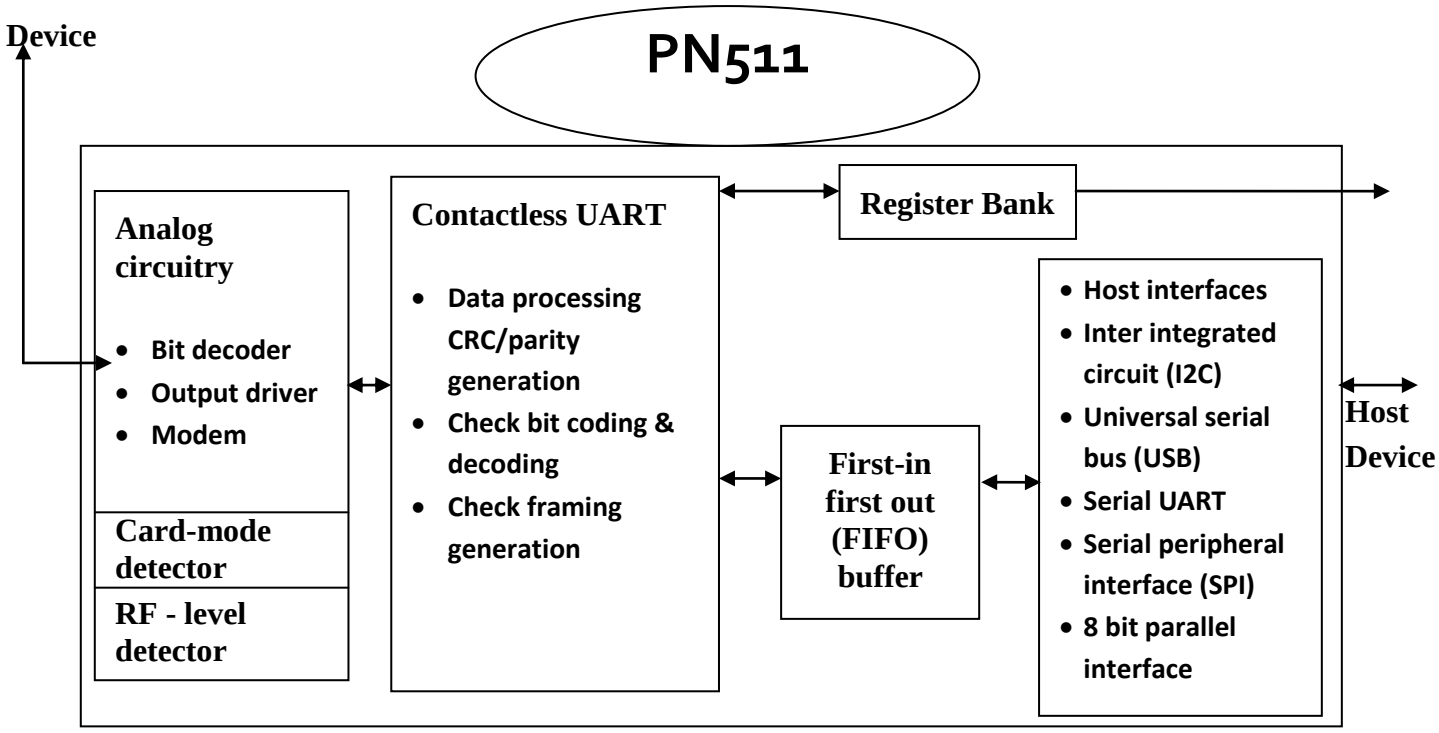


Fig.6 *Philips Semiconductors' PN511 NFC transmission module*

2.4.2 NFC Transceiver

A vital aspect of an NFC device is that it is require to act as an initiator and target at different times. However, it has just a single antenna which is designed for these purposes [38].

An NFC device initiator generates a magnetic field which is proportional to the AC current flowing through a number of turns in an inductive antenna element to produce a fixed carrier frequency of 13.56MHz. This field that is generated is used as carrier for modulated (data) signals as well as a means for conveying energy to power a passive RFID target such as transponder or tag from an NFC system if required.

NFC specification defines the functionality that describes when an NFC device is acting as an initiator (reader/writer) as well as when acting as a target (or tag).

The initiator can set up a magnetic field, H, by passing current, I, through an antenna coil with number of turns N, and radius, R, at a perpendicular distance of, x, from the centre of the antenna. This will generate a field.

$$H = \frac{I.N.R^2}{2\sqrt{(R^2 + X^2)^3}}$$

The initiator's antenna physical design governs N and R such that the produced field, H, is directly proportional to the current I

The target antenna physical design governs the number of turns, N, and areas, A, such that the voltage induced at the target antenna is directly proportional to the change in the produced magnetic field by the initiator antenna which also is dependent on the antenna coupling.

Similarly, if current flows in the target's antenna, it couples magnetic flux back to the initiator antenna. As a result, the current loading of the target's antenna transformed back to the initiator antenna [38]

What determines the degree to which two antennas are coupled is the coupling coefficient K. Where $0 \leq K \leq 1$.

2.4.3 Generating a magnetic field while acting as initiator

When NFC is acting as initiator it requires a large 13.56MHZ current to generate an NFC magnetic field, the required 13.56MHZ current is best produced using a series-resonant LC circuit.

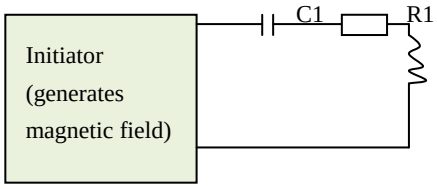


Fig.18 *Initiator driving LCR series-resonance*

2.4.4 Receiving a magnetic field while acting as a target

The strength of the receiving magnetic field varies when acting as a target. This is dependent on the initiator driving strength and the coupling coefficient. Parallel-resonant LC circuit is more appropriate to derive adequate operating voltage from an incoming magnetic field.

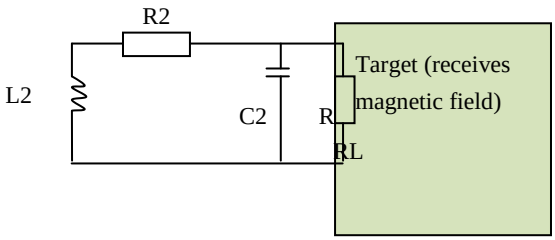


Fig.19 *Target receiving LCR parallel-resonance*

2.4.5 NFC Stamp Antenna

An NFC stamp antenna was developed by Pulse a technitrol company, the whole module has a measurement of 40×21×5mm, contains an NFC antenna which measures 15×20×5mm and supports communication at 13.56MHz. In addition to 13.56MHz frequency supported by the 15×20×5mm NFC antenna, the main module supports frequencies ranges of 824-960MHz and 1710-2170MHz for using GSM and WCDMA. [39] [40].

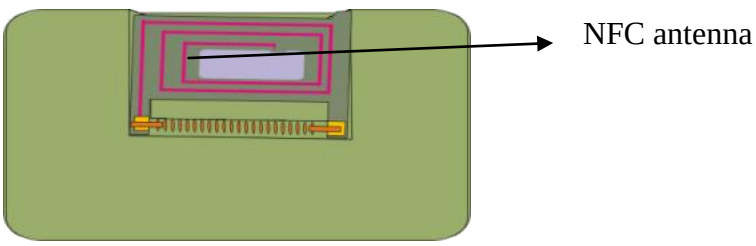


Fig.20 *NFC stamp antenna [39]*

The antenna can read tags with diameters from 15-65mm at distances from 5-20mm.

Current tag coil sizes	Reading distances with NFC Stamp antenna
15mm	5mm
42mm	7mm
65mm	7mm
44mm	22mm
47mm	22mm
86×53mm	20mm

Table 6: ***Tags and reading distances with NFC stamp antenna [39]***

The table above shows the different sizes of tags and the distances requires by an NFC stamp antenna for communication.

2.5 Operating Modes

NFC operates in three modes: reader/writer, card emulator and peer to peer mode.

2.5.1 Reader / Writer Mode

In this mode, the NFC devices are active and capable of reading a passive RFID tag. They are chiefly used for service delivery e.g. interactive advertising, accessing information and delivery of contents.

Fig.7 *NFC Reader/Writer mode (Reproduced with permission of Dawn O'Grady) [15]*

2.5.2 Card Emulator Mode

This mode allows NFC devices or handsets to act like an existing contactless card, thereby allowing external readers to access in order to communicate. They are typically employed during transactional activities, like mobile ticketing, access control, mobile payment etc.

Fig.8 *NFC Card emulation mode (Reproduced with permission of Dawn O'Grady) [15]*

2.5.3 Peer-to-Peer (P2P) Mode

This enables two NFC devices to communicate and exchange or transfer information. The devices communicating play a vital role as an initiator and target.

Fig.9 *NFC Peer-to-Peer mode (Reproduced with permission of Dawn O'Grady) [15]*

2.6 Mode Switch

In the context of mode switch, whenever an NFC device sees another device in the radio field, it initially finds out whether it is a reader/writer, contactless card, an RFID tag or another NFC device. All these are made feasible by the mode switch design. It makes sure that an NFC device enters into a status in which it is able to communicate with the other device(s) in the radio field. Additionally, it classifies the responses whenever a lot of cards are found in the radio field concurrently.

2.7 NDEF

NDEF is simply the short form for "NFC Data Exchange Format". Basically, it is a data format classified by the NFC forum in connection with the exchange of information among two devices, i.e. an NFC-enabled device and an NFC tag. It presents rules in relation to the structure of a matching message, without limiting the types of information it contains. This permits the encapsulation of a large amount of varied data, such as images, URLs or XML files. It nonetheless, does not include any NDEF transmission protocol. For this reason, the type of channel for the transmission of messages is also liberally selectable, similar to the sort of information it contains.

An NDEF message is made of a series of NDEF records. Accordingly, the actual encapsulation of the data takes place in the individual NDEF records. Defined data formats that are commonly used, e.g. Uniform Resource Identifier (URI), Smart Poster, and Text are standardized by the NFC-Forum as Record Type Definitions (RTD) to allow interoperability of products coming from different vendors [20]. The size and type of data transmitted can be recognized by means of the header. This allows a resourceful analysis of the information enclosed in the records to be carried out. With the help of the NFC Forum, a number of various types of information have been identified.

3 Overview of NFC mobile ecosystem

Before we proceed to discuss the overview of the NFC mobile ecosystem, we will, first of all, give a brief summary of how NFC in mobile phone can be used in our daily lives.

3.1 NFC Mobile Daily Usages

AREAS	USAGE OF NFC MOBILE PHONE	SERVICE INDUSTRIES
STATION AIRPORT	Get information from smart poster. Get information from information kiosk. Pay bus/taxi fare.	Mass and public transport. Advertising.
VEHICLE	Personalize seat position. Use to represent a driver's license. Pay parking fee.	Drivers and vehicle services
OFFICE	Enter/exit office. Exchange business card. Log in to PC; print using copier machine.	Security.
STORE RESTAURANT	Pay by credit card. Get loyalty point. Get and use coupon. Share information and coupon among users.	Banking Retail Credit card
THEATER STADIUM	Pass entrance. Get event information.	Entertainment
ANYWHERE	Download and personalize application. Check usage history. Download ticket. Lock phone remotely.	Any.

Table 1: ***Some Applications of NFC in our daily lives***

3.2 NFC FUNCTIONALITIES

3.2.1 Service Provisioning

Today's contactless business has this functionality and it allows a user to subscribe and get their personalized contactless cards. This functionality will go long way in expanding NFC mobile services. Both the functions to which a user subscribes and the functions of the service provisioning, preparing the personalize data are built to work with the existing infrastructure. Due to the availability of a connected network, current functionalities, such as remote user management and authentication, will surface. Service providers are responsible for this functionality. [6]

3.2.2 Mobile Network Provisioning

This is a new functionality for contactless devices. It comes with the functionalities to maintain the network infrastructure that offers data connectivity service to users, provide user authentication that ensures that only contracted users are allowed to connect to a mobile network, and also it provides care for the data connectivity service. MNOs (Mobile Network operator) or MVNO (Mobile Virtual Network Operators) offer this functionality.

3.2.3 Trusted Service Manager

Trusted Service Manager (TSM) offers a contact point between the service provider and NFC enabled mobile phones. Through TSM, a service provider can offer NFC mobile phones with remote, multi-application management functionalities. These functionalities come with the following:

- Managing and issuing a trusted execution environment.
- Assigning trusted areas within a specified service of trusted execution environment.
- Key management for a trusted execution environment.
- NFC mobile phone applications download security.
- Locking, unlocking and deleting application in accordance with users or a service provider
- Applications personalization.

Mobile network operators, service providers or third parties can perform these functionalities and all parts can be assigned by one party to another. [6]

3.3 How the NFC mobile ecosystem works

This section discusses the NFC mobile ecosystem players which are listed as users, chipset manufacturers, NFC handset manufactures, NFC component and tag manufactures.

3.3.1 Users

An NFC mobile user needs to have an agreement with the provider of an NFC mobile service before its first use. In addition to that, to make use of NFC mobile services, the user is required to subscribe to the mobile network provision service and have an NFC mobile phone as well. For plastic contactless cards, user require a different contactless card for each service, but is not so for NFC mobile phone. NFC mobile phone can embed the entire services on a single mobile phone.

3.3.2 Chipset Manufacturers

Chipset manufacturers are responsible for providing the integrated circuit component (IC) required for all NFC devices in accordance with the required technical standard (by ISO/IEC, ECMA, and NFC forum). Chipset development is carried out in agreement with handset manufacturers and service providers in order to accomplish the application requirement.

The following are components of the chipset:

- ICs for the NFC controller, which includes device driver and middleware as required in handset and reader/ writer terminal.
- ICs for trusted execution environment (UICC, Embedded, Removable for phones, and SAMs for terminals) which includes several cases of pre-personalization for the devices.

- ICs for smart tags (example, the ones in smart poster).

3.3.3 NFC Handset Manufacturer

Handset manufacturers are responsible for the design and production of NFC mobile phone in accordance with the industrial standards. They offer capabilities that help the service provider to develop applications that are suitable for users. Handset manufacturers compete to provide attractive functionalities at a minimal cost.

3.3.4 NFC Component and Tag Manufacturers

NFC component and tag manufacturers are responsible for the design and production of devices in accordance with service provider's specifications and industrial standards requirements. They reduce the implementation effort of the service providers by delivering the following features to the ecosystem.

- Secure way of satisfying customer's requirements.
  - ✓ Tamper resistivity.
  - ✓ Communication channels and content encryption.
  - ✓ Key management encryption by service provider.
- Software (such as drivers, middleware, and software development kits (SDKs)).
- Quality and interoperability management.

3.4 Factors Responsible for Building a Successful NFC Mobile Ecosystem

NFC Mobile Ecosystem is mainly targeted for contactless card businesses. In other words, it is an expansion of the current contactless ecosystem. It requires new functionalities (additional functionalities that are not in the current contactless cards business) to be more attractive and successful. This section explains the factors responsible for building a successful mobile ecosystem from the above perspective.

3.4.1 Mobile Network Operators

NFC mobile phones combine both functionalities of contactless devices and that of the mobile phone. This helps provide mobile network operators with opportunities to develop new business areas.

Because of the strong support of NFC mobile phone for multi-application capability, it makes it more convenient for the user by allowing different applications in one device and thereby increasing the number of NFC mobile service users. This is, in fact, one of the key factors. Another factor is to ensure users and services providers have a trusted, end-to-end system for their application and data which can be achieved through the TSM functionality.

However, there are several possible models showing who might provide the functionalities that make up the TSM, but the two potential candidates are the mobile network operator and service providers. Whichever model that may adopt it is imperative to clearly state the responsibilities of each ecosystem player within the specific model. The division and provision of functionalities of TSM is also a key success factor.

3.4.2 Service Provider

A contactless card service provider can only provide personalized advertisements or messages either at the point of contact, or through a different channel, like email. With an NFC mobile phone, it is possible to send a personalized message or advertisement to the same device that is hosting the contactless card anytime and anywhere [6]. This is because the NFC mobile phone is always connected to a mobile network.

Another great benefit to the service provider is in the increasing number of NFC services and the high degree of usage by adopting the multi-application capability of NFC mobile phones.

3.5 Basic recommendation to achieve a successful NFC mobile services

The below suggestions are provided for NFC mobile phones, for trusted service manager and for service provisioning.

3.5.1 Recommendation for NFC mobile phones

- The NFC mobile phone should be able to support NFC emulation mode and offer some trusted execution environment, like those in smart cards.
- It should have support for NFC peer-to-peer mode and also support exchange of data with other contactless devices and NFC mobile phones.
- It should be able to read or write to NFC tags and have support for the NFC reader/writer mode
- It should be able to exploit the user interface functionality of the phone for NFC services interactivity
- It should make use of the communication functionality of the mobile phone and offer support for the secure downloading and management of multiple trusted applications, like personalization, locking and unlocking.
- It should allow multi-issuer coexistence in trusted environment as well as support for assignment of trusted areas for a service.
- It should have the capability to communicate with other NFC devices and with existing contactless infrastructures.

3.5.2 Recommendation for NFC Trusted Service Manager

- It should have the ability to manage trusted applications on an NFC mobile phone.
- It should have the ability to authorize and securely download a trusted application to an NFC mobile phone.
- It should allow multi-issuer co-existence in a trusted execution environment and have the ability to assign a trusted area to a service
- It should have the ability to lock/unlock trusted applications.

3.5.3 Recommendation for NFC Service Provisioning

- It should have the ability to deliver the provisioning information of a trusted application to TSM.

3.6 NFC Mobile Structure

In this section, we are going to show the pieces of technology that are combined to make NFC mobile services a success. This structure describes functionalities necessary to achieve a successful end-to-end communication. The groups that are involved are: functionalities of NFC mobile phones, functionalities of the back-end server system, and functionalities of the

target with which mobile phone have communication. However, this structure is not intended to restrict the implementation, but only define functionalities.

NFC mobile back-end server system functionalities	Download	
	Provisioning	
	Personalization	
	Lock/Unlock	
	Information	
	Etc.	
NFC Mobile Phone Functionalities	AEE	Storage
		Over-the-Air (OTA)
		Execution Environment
		Phone functionality
		UI
	TEE	Secure Storage
		OTA
		Execution
	P2P	
	Reader/Writer	
	NFC Stack and Controller	
	Card Emulation	
NFC Target	PSP Devices	
	Tag	
	Reader/Writer	

Table 2: Functionalities to achieve a successful end-to-end communication

3.6.1 NFC Mobile Phone Functionalities

An NFC mobile phone should be able to make use of both the functionalities of contactless cards and that of mobile phones to realize services.

3.6.2 Application Execution Environment (AEE)

An NFC mobile phone offers NFC functionalities as well as basic mobile phone functionalities for example voice calling, packet communication, phonebook browser, mailer etc. It also offers user interface to interactively execute phone services. These collective functionalities, that are used to realize NFC mobile services, are called an "Application Execution Environment" (AEE). AEE has support for data storage and processing and the

secure execution of mobile phone services. However, the level of security might not be enough to meet the demands of all NFC service providers.

3.6.3 Trusted Execution Environment

There are some NFC services, such as payment, that demands a highly trusted environment which might not be realized by the AEE.

TEE offers secure data storage, secure management functionalities, secure execution environment etc. The secure management functionality is used to achieve over-the-air (OTA) application download and remote issuing/personalization of NFC mobile services. Though some of functionalities are also found in AEE, TEE has more security to improve the trusted NFC services [6]. There are cases where a mobile phone browser may access data stored in the TEE. This is because the TEE can open a specific interface to the AEE and allow access to TEE through the interface.

NFC mobile phones may have the capability to have more than one TEE for several reasons such as different service provider requiring separate TEEs for their application, different levels of security strategy, user control etc.

3.6.4 NFC Stacks and Controller

NFC stacks are functionalities that explore NFC potentials for communicating with NFC targets. There are three of these kinds: NFC card emulation stack, NFC reader/writer stack and the NFC peer-to-peer stack. Both AEE and TEE are capable of providing these functionalities.

3.6.5 Card Emulation Stack

The NFC emulation Stack offers NFC card emulation mode. It permits an NFC mobile phone to act like a card or tag before conventional reader/writer. With the use of this mode, existing infrastructures, such as the ones for payment and ticketing, can communicate with NFC mobile phone supporting NFC card Emulation mode.

3.6.6 Reader/Writer Stack

This offers NFC reader/writer mode. In this mode, the NFC mobile starts the communication by generating the RF field and sending the relevant command to an NFC tag, a contactless card, or an NFC device in NFC card emulation mode.

3.6.7 Peer-To-Peer Stack

NFC peer-to-peer stack offers the NFC peer-to-peer mode. In this mode, the initiator starts the peer-to-peer communication while the target responds to it. It is recommended that NFC mobile phones have the ability to be both the target and the initiator.

3.6.8 NFC Controller

The NFC controller is responsible for the handling of the physical transmission of data over the RF interface and antenna.

3.6.9 Back-End Server System Functionalities

The functionalities of back-end server system of NFC mobile phone are needed to achieve end-to-end NFC mobile services.

3.7 Common NFC functionalities

3.7.1 Download

This is a function used to securely download a mobile application to an NFC mobile phone.

3.7.2 Provision

This functionality is required to initiate a TEE and is also used to assign a trusted area within a trusted execution environment to a specific service.

3.7.3 Personalization

These functionalities are used to configure an application or user-specific data to an application. These functionalities can also be assigned to a third party by the service provider.

3.7.4 Lock/Unlock

Lock/unlock functionalities are used to lock and unlock, or delete, previously provisioned applications as requested by a user or service provider.

3.7.5 Information

These functionalities are used to receive or send information with an NFC mobile phone, e.g. a mobile phone's browser accessing web servers and its mailer receiving information by email.

4 NFC Standardization & Bodies

NFC is an International open platform standard formulated by Sony and Philips. One of the major concerns being looked at currently is the existence of an interoperable interface between NFC devices so as to increase its potency and attractiveness in a competitive global market. As a result, the standardization of NFC technology plays a key role towards the success of this evolving wireless communication technology. Based on existing technologies, standardization has been conceded in some continents such as Europe and Asia. Below are some of the standard specifications formulated by NFC Forum.

4.1 COMMON STANDARDS

4.1.1 ISO 18092 NFCIP-1

NFCIP is an acronym for NFC Interface and Protocol. It defines the fundamental capabilities, such as a scheme for bit encoding, data transfer speed, modulation, transport protocol and the frame architecture. [19]

4.1.2 ISO/IEC 15693

This identifies the surrounding area communication and stretches across considerably longer distances as compared to ISO/IEC 14443, which defines proximity communication.

4.1.3 ISO/IEC 14443

This standard specification defines the closeness in communication that exists in both type A and B contactless cards.

4.1.4 ISO/IEC 21481 NFCIP-2

This standard integrates all three standards descibed above and specifies a mechanism that holds up the coexistence of these standards as well as choosing one of the three communication modes. In order for NFC to meet the global compatibility requirements that exist among smartcards, it needs to make available all the three functions described above. For this reason, as a blend of smartcard and contactless interconnection technologies, NFC is well-suited with existing RFID-technology. This implies that it is making a great effort in providing compatibility with the numerous existing contactless smartcards and scanners across the globe.

4.2 NFC Forum

This is a non-profit making international standards organization, created on 18 March, 2004 by Sony, Nokia and NXP Semiconductors. The primary aim of NFC Forum is to promote the use of NFC short-range wireless communication technology in mobile equipment, personal computers and consumer electronics as well as educating the world about NFC technologies [20]. They support the standardization and execution of NFC technology to guarantee interoperability existing between devices and services. Over 150 affiliates have joined the NFC Forum as of September 2008 [21].

4.3 NFC Forum Organizational Chart

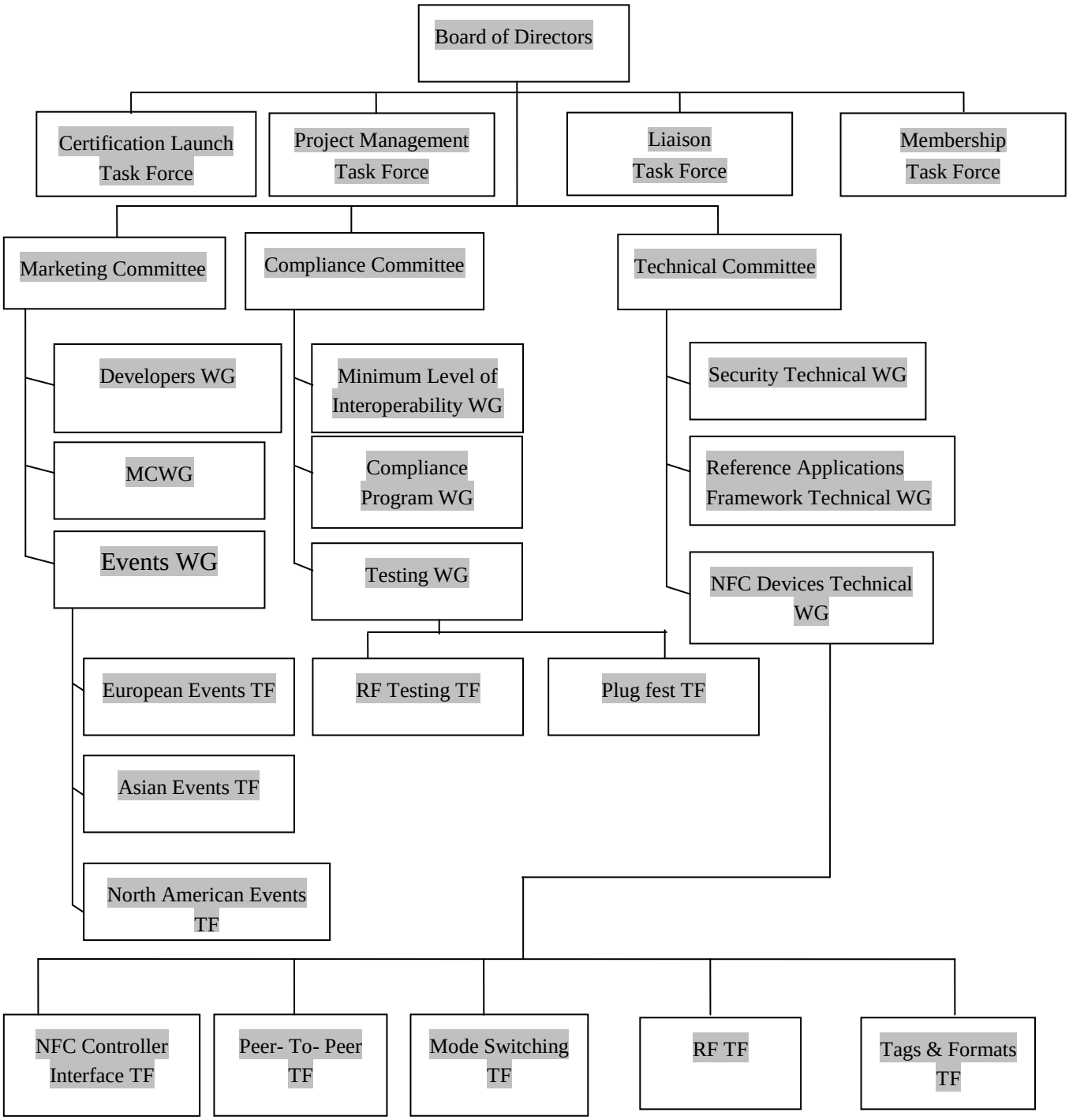


Fig.10 Organizational Structure of the NFC forum [20]

The above illustration shows an organizational chart of the NFC forum. The Board of Directors (B.O.D) represents the head of the forum. It is responsible for making decisions related to NFC technology. The BOD is made up of 13 companies. It has three (3) sub-committees under it which aids it in achieving its set goals or targets. Several groups exist in the NFC forum; they all have specified roles to play in achieving the ultimate dream of making NFC technology widely the best wireless communication technology. The working groups (WGs) are in charge of examining matters in a specified domain, the task forces (TFs)

are designated for particular issues. The Liaison TF (LTF), Certification Launch TF, Membership TF and the Project Management TF (PMTF) fall directly below the BOD. The LTF is responsible for building co-operational structures with other organizations together with the PMTF.

4.3.1 Technical Committee

The Technical Committee defines the protocols and data structures required by NFC. It has three (3) sub committees that fall under it. They contribute to the design of a strong framework for efficient and reliable communication between NFC devices. These three (3) committees are, namely, the Security Technical Working Group, NFC Devices Technical Working Group and Reference Applications Framework Technical Working Group.

(1) The Security Technical Working Group takes charge of issues or matters associated with NFC data protection and security.

(2) NFC Devices Technical Working Group defines the technical requirements for general purposes which are needed for constructing NFC devices. Five (5) sub branches, known as Task forces (TF), fall under this group. Below is the description of their respective tasks;

- *NFC Controller Interface TF* describes the technical requirements which have to do with the junction between the device host, which directs the NFC device and the NFC controller.
- *The Peer-to-Peer TF* describes the technical requirements for the logical link control protocol.
- *The Mode Switching TF* defines the technical requirements for digital protocols and other communication protocols which promote communication between NFC devices and NFC tags.
- *The RF TF* describes the technical requirements for the analog properties of the RF interface of NFC devices.
- *The Tags & Formats TF* work on the technical requirements necessary for operation of NFC tags in reader/ writer mode and the data format that exist among NFC.

(3) Defining the application framework, specifications on data format for applications, technical specifications and recommendations are various tasks carried out by the Reference Applications Framework Technical WG. All above mentioned tasks contributes to building an effective communication between NFC devices and other wireless technologies such as Bluetooth, WIFI, etc.

4.3.2 Compliance Committee

The NFC Forum's Compliance Committee, is at the moment, constructing a product certification program with a user identifiable trademark [20]. This will guarantee the NFC brand promise of compliance and interoperability. The compliance committee is generally responsible for setting up the requirements for the certification program and be aware of the inference of all NFC Forum’s requirements on the certification program. They define the range, processes and policies of the NFC Forum certification program as well as its operation rules.

This committee consists of three sub working groups (WGS): Minimum Level of Interoperability WG, Compliance Program WG and the Testing WG. They are jointly

responsible for the definition of a product certification program to give surety to interoperability of NFC devices.

- The Minimum Level of Interoperability defines the catalog of least amount of functions that a device should possess in order to guarantee its interoperability with other NFC equipments.

- The Compliance Program WG on the other hand, sets up the policies and business rules for the program certification program. They team up with the Marketing Committee, Technical Committee, and other working groups belonging to the Compliance Committee to define and administer the NFC Forum's certification program. Their primary tasks include:

- Defining the operation rules and methods for the NFC Forum certification program.
- Working in partnership with the certification authority together with the administrator to document the processes involved in the certification program.

- The Testing WG is responsible for issues related to compliance and interoperability of an NFC Forum device. NFC Test methodology, concepts and real test specifications are built and upheld by this WG. They offer assistance or directions to other technical working groups. They collaborate with the technical committee in finding solutions to probable testing inconsistencies.

4.3.3 Marketing Committee

The primary role of the Marketing Committee is to educate the public domain on the benefits of NFC wireless communication technology and the various activities undertaken by the Forum. Other activities involved in the marketing arena include setting up, upholding and improving NFC forum's website. They are responsible for press releases and play a part in exhibitions together with training companies which partake in these activities. Symbols and trade names are prepared and made available by the marketing committee. Three (3) WGs namely the Developers WG, the Marketing Communication WG and Event WG fall directly under the Marketing Committee. They work immensely to meet the targets set by the NFC Forum.

- The Developers WG offers services such as information dissemination and assistance to developers of NFC products and services. Occasionally, functions such as award presentations are organized, through which deserving and excelling developers are awarded to serve as a motivational tool.

- The Marketing Communication builds and preserves a range of NFC communication tools and materials. They are responsible for administering marketing links and brands belonging to the NFC Forum.

- The Events WG categorizes and encourages appropriate events to increase the existence of the NFC Forum. The *NFC Zone* is offered by the Events WG at important exhibitions.

5 NFC Communication Modes

An NFC platform can work in two different communication modes namely, the active and passive mode. The distinction between the two modes lies in the fact that, an active device produces its own radio frequency (RF) field during the communication process while a passive device uses inductive coupling to transmit data. For battery-powered devices, like mobile phones, it is better to act in passive mode. In contrast to the active mode, no internal power source is required. In passive mode, a device can be powered by the RF field of an active NFC device and data is transferred by means of load modulation. Hence, the protocol allows for card emulation, e.g., used for ticketing applications, even when the mobile phone is turned off.

Communication between two active devices is referred to as active communication mode, whereas the communication between an active and a passive device is called passive communication mode. With regards to the passive type of communication, the passive device serves as NFC target at all times. The active device however serves as the initiator, responsible for generating the RF field. Conversely, with active communication mode, since the RF is generated by the device itself, the functions of the initiator and the target device are firmly assigned by the device which begins the communication.

5.1 Active Mode

With NFC active communication mode, two active devices communicate with each other by means of generating RF. These devices are referred to as an initiator and a target device. Active devices have their own power supply so they do not draw energy from the field of the reader/writer. However, NFC devices that are projected to communicate totally with active devices can be equipped with smaller antennas. In the event that a device wishes to send information to another device, it produces its own radio frequency (RF) at the outset, so as to aid communication. This communication mode is typically used for devices that communicate using peer to peer (p2p) communication mode.

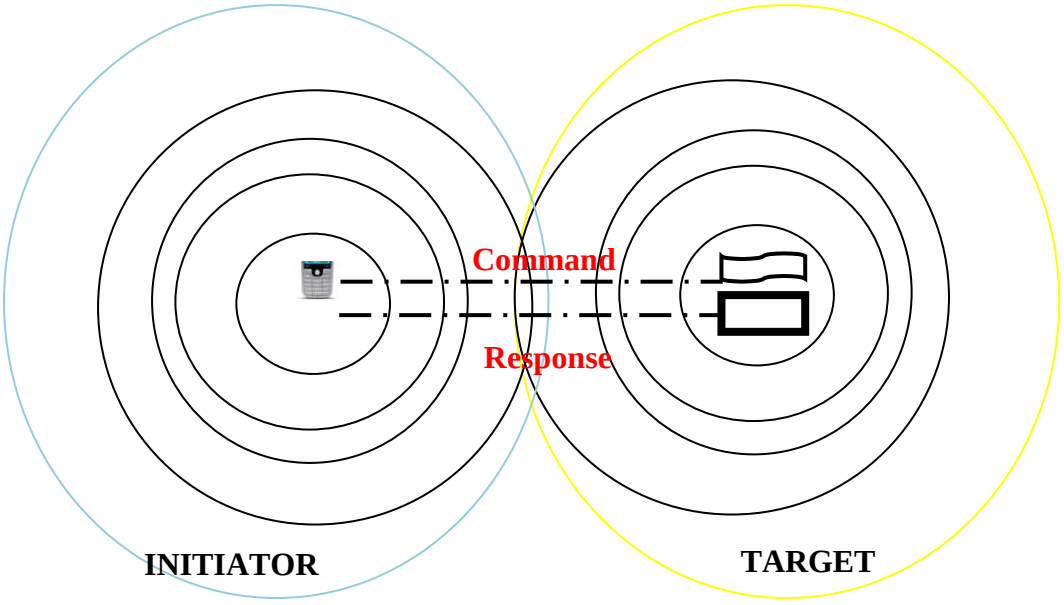
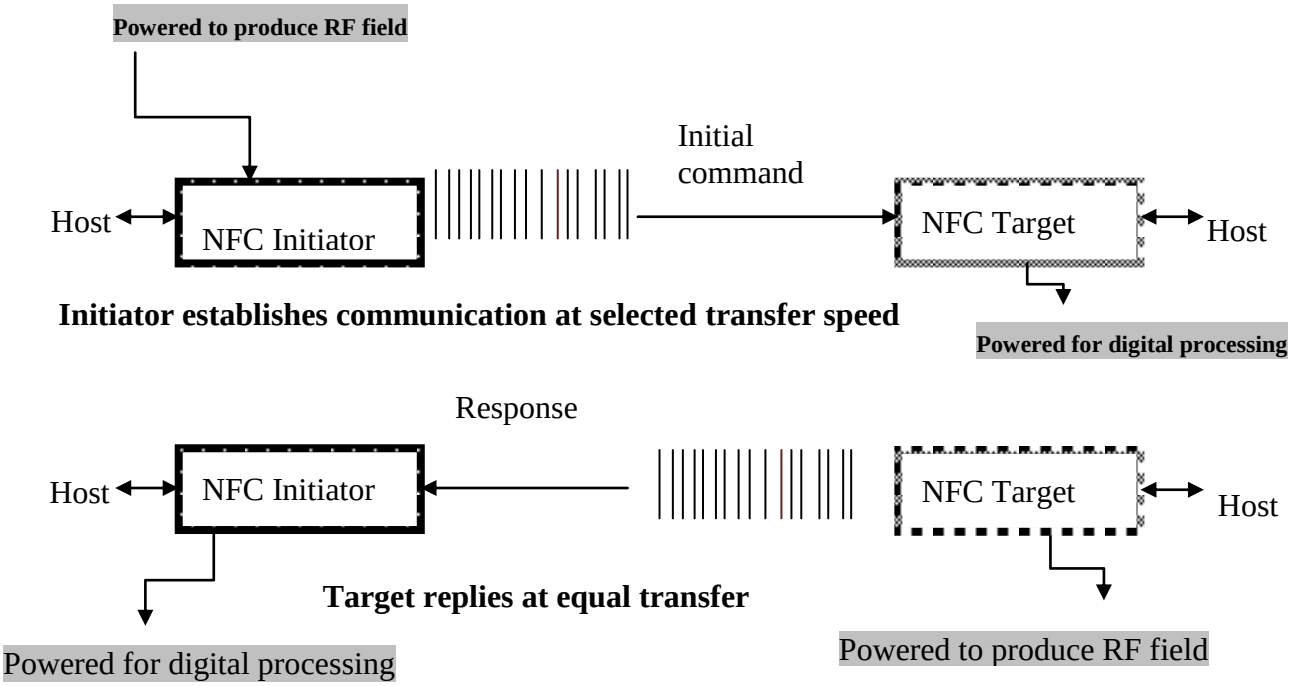


Fig.8 NFC Active mode

Active Mode

(Operating frequencies: 106 / 212 / 424 Kbit/s)



5.2 Passive Mode

In passive mode, communication takes place between an active and a passive device. However, passive devices have no direct power source (battery) thus the initiator is solely responsible for generating the RF field. In order for a passive device to read its memory, operates its own processor and memory systems, it draws the energy required from the reader/writer. This process involves a suitably large magnetic flux generated by the reader/writer. Antennas with large dimensions are required when implementing the passive mode. The area enclosed by the antenna serves as the key factor. The target device responds in a load modulation scheme. The passive mode is an extended mode for p2p and RFID communication.

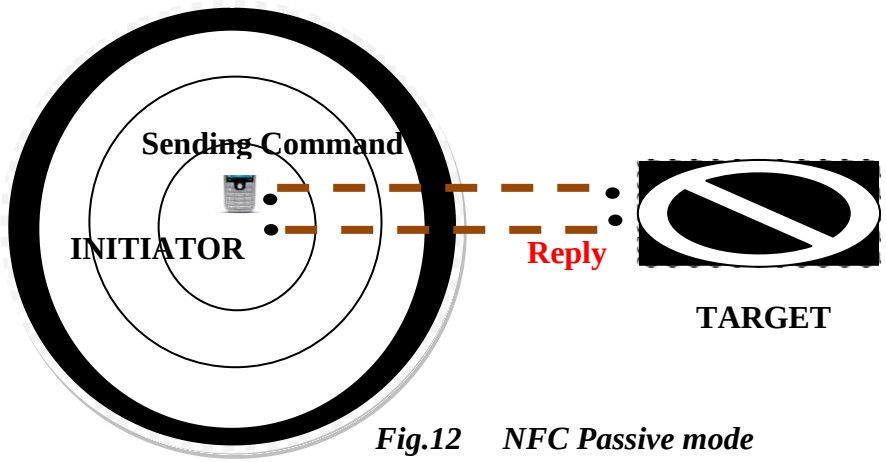
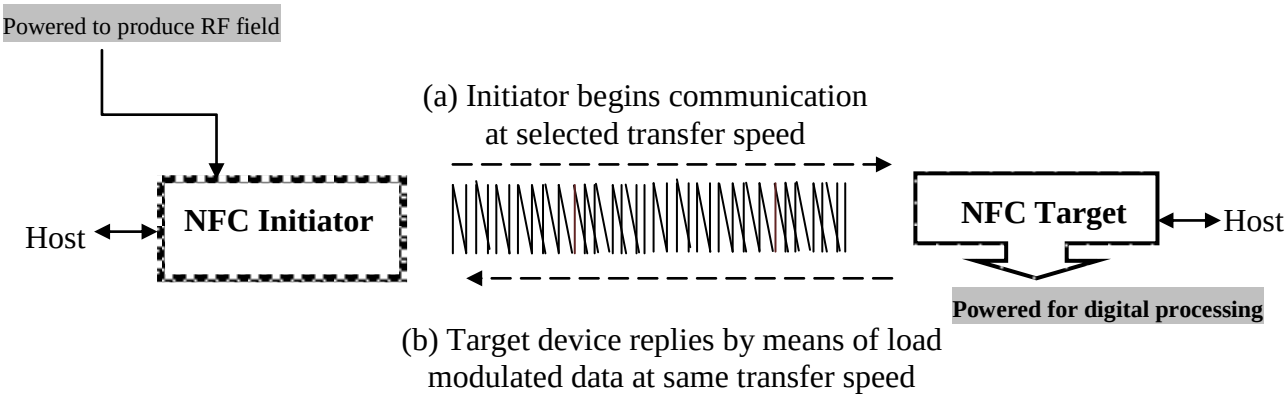


Fig.12 NFC Passive mode

Passive Mode

(Operating frequencies: 106 / 212 / 424 Kbit/s)



5.3 Initiator & Target Devices

5.3.1 NFC initiator

An initiator plays a major role in the build up of the wireless communication medium by setting up the communication channel at a preferred transfer speed. Below are other vital roles performed by the initiator;

- ability to supply power to the target devicez
- discovery of the least load modulation signal from the target for operation
- waveform measurement

5.3.2 NFC target

- determines the load modulation
- reception strength
- evaluating time required for transmission

5.4 Coding and Modulation

When information is being transmitted, it is mapped into waveforms enabling the receiver (modem) to recover it in a reliable manner. Mapping the transmitted information into waveforms is made feasible by means of coding and modulation. NFC wireless communication technology uses two different coding methods namely, the Manchester coding and modified Miller coding, for data transfer.

The difference between an active and passive device lies in the way data is broadcasted or transferred. Passive devices (e.g. contactless smartcard) employ the Manchester coding method with a modulation ratio of 10% ASK whereas active devices use the Miller coding

with 100% modulation with data rate of 106 kps and Manchester coding with a ratio of 10% and data rate larger than 106 kps. In active mode the data is transmitted using amplitude shift keying (ASK). This implies that the base RF signal is modulated with the data in relation to a coding scheme.

Transfer speeds (kbaud)	Active Device	Modulation Ratio (Active)	Passive Device	Modulation Ratio (Passive)
106	Modified Miller	100% ASK	Manchester	10% ASK
212	Manchester	10% ASK	Manchester	10% ASK
424	Manchester	10% ASK	Manchester	10% ASK

Table 3: Coding Method & Modulation ratio at different transfer speeds [13]

5.4.1 Manchester Coding

This type of bit coding splits the time needed to define the bit into two clock cycles. The first cycle represents the value of the data i.e. either 0 or 1 while the second cycle offers the timing required to change state. Also known as Phase Encoding, a Manchester code is a self clocking data encoding technique. It is inductively or capacitively coupled thus making it possible for a clock signal to be recovered from the encoded data. However it requires no direct current for its operation. A high to low shift is represented by a 1 bit, while a 0 bit stands for a low to high shift. At the midpoint of a period, transition occurs, which indicates 0 or 1. Transitions at the beginning of a period are considered as overheads and do not represent any data.

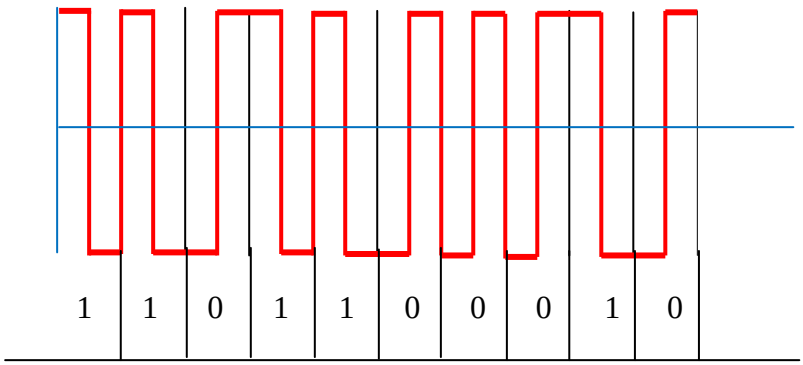


Fig.13 Illustration of Manchester code

5.4.2 Modified Miller Coding

This Modified Miller coding method converts binary data transmitted between NFC devices into two level signals, that is a “0” and “1”. It identifies one (1) and zero (0) signal by the spot where a pulse occurs during a single bit period. The signal levels are interpreted as (i) “0”

representing no change in signal level except a situation where another "0" follows it. Consequently, a transition to the other level occurs at the end of the first bit period; and (ii) when a transition occurs in the center of the bit period from one level to the other level, it is indicated by a "1". It uses half the size of the bandwidth during encoding. Miller encoding is also referred to as Delay encoding. In fig. 11, is a diagram describing the bit representation.

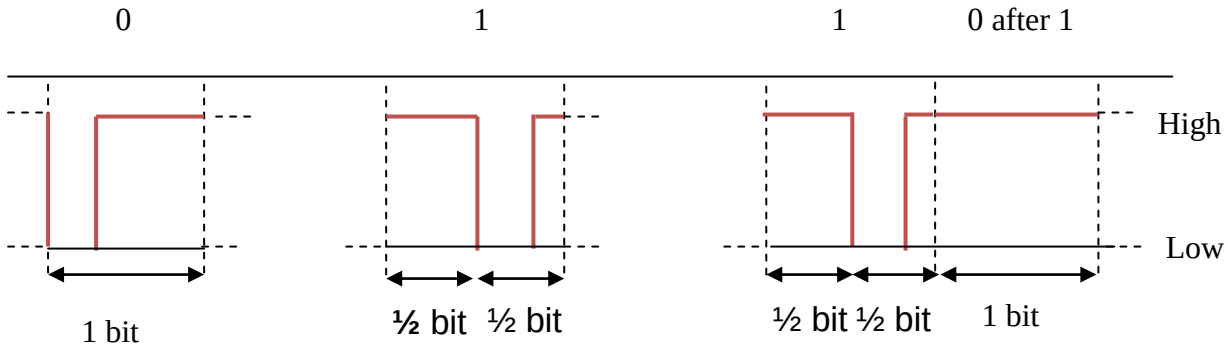


Fig.14 An example of Modified Miller coding

5.5 Channel Access Method

Carrier sense multiple access with collision avoidance (CSMA/CA) is the type of medium access method employed by NFC wireless communication technology. An initiator first verifies for an existing RF field before setting up a communication channel, likewise a target device in active mode also checks for an existing RF field before replying to instructions or commands. Devices are set to remain quiet as long as another RF field is detected, thereafter communication starts at a defined guard-time. An initiator can act together with several targets, each of which generates a random 40 bits ID at the beginning of the device selection process. The detection of target device IDs involves a well-designed process which helps prevent the occurrence of collisions when multiple targets reply concurrently [24]. Mainly, this occur when target devices respond to commands in passive mode. At the bit level, detection of collision is achievable by the use of Manchester coding, this is because collisions are discovered whenever a full bit period occurs without any transition noticed. It can only take place when a 1-bit transmitted by one target collides with a 0-bit transmitted by another target. Bits received before the occurence of collision, can be recovered and thereafter the target devices are requested to re-send data, first with the unrecovered bit. The responding targets use a mechanism called random delay to ascertain that this process does not get trapped in a forever loop.

6 NFC Targeted for Multiple Applications

In chapter three we illustrated how NFC mobile phones can be used in our day to day lives. In this chapter, we will present a brief overview of some of the areas where NFC is applicable. Applications of NFC can be divided into four (4) basic categories, namely Touch and Go, Touch and Confirm, Touch and Connect & Touch and Explore.

6.1 Touch and Go

This feature is made available in applications such as event ticketing, transport or access control. In this case, the user simply needs to bring the NFC-enabled mobile device, which stores the valid ticket or access code close to the access control reader to be granted permission. It is also applicable for data capture applications, like a smart poster (selecting a URL from a smart label on a poster or advertising new services) [31].

6.2 Touch and Confirm

It is made possible in applications such as mobile payment (m-payment), where the mobile user is required to confirm the interaction by keying in a valid password or just accepting the transacted business.

6.3 Touch and Connect

NFC-enabled devices are connected to allow a peer to peer (p2p) transfer of data. Example of such transfers can be the exchange of videos and images, business cards download/transfer of music files, etc

6.4 Touch and Explore

NFC devices may be capable of delivering several functions. The end user can explore the device's competences and thereafter determine the various functionalities and services offered by the device.

6.5 NFC targeted for mCoupons

Coupons are normally vouchers that allow a holder to be entitled to something or a discount on a product. Companies use it as a means of rewarding and establishing good customer relationship.

mCoupons are coupons that can be collected and stored on a mobile device e.g mobile phones or PDAs [7]. The purposes are the same with paper-based coupons except for the fact that, issuing and paying-in are done electronically without direct human involvement. An mCoupon is also known as mobile coupons and it different from e-coupons (electronic coupon).

An NFC-enabled issuer for example, a newspaper or an advertisement poster can issue mCoupons [7] which can be stored on an NFC -enabled mobile device to be carried to the cashier by the recipient. The significant difference between an e-coupon and mCoupon is that e-coupon systems need online access of the issuer, the recipient and the merchant while mCoupon works without online access of the recipient and the issuer but still provides protection against illegal use of persons. [7]

6.5.1 How mCoupons work

The concept behind mCoupons can best be described in figure 12 .

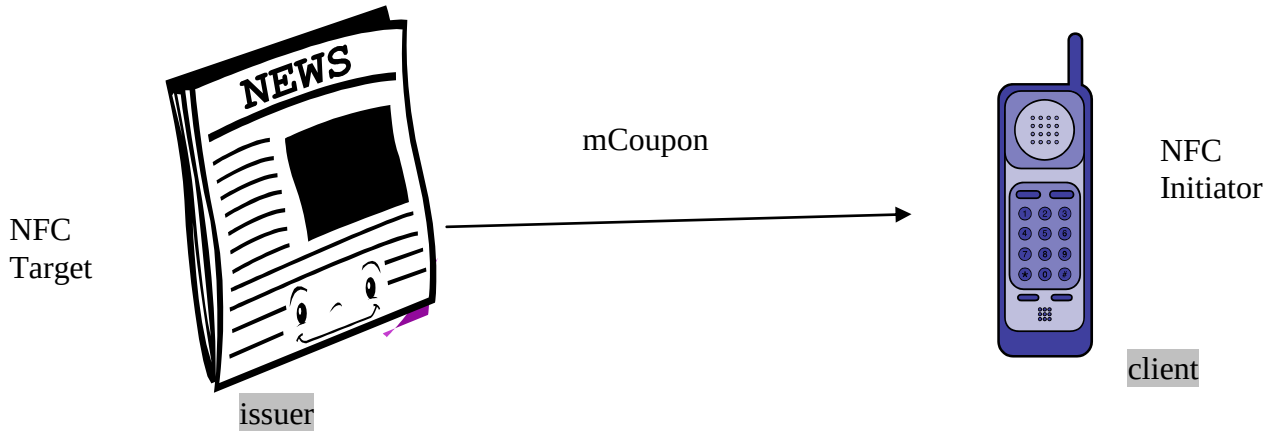


Fig.15 ***Client receiving an mCoupon***

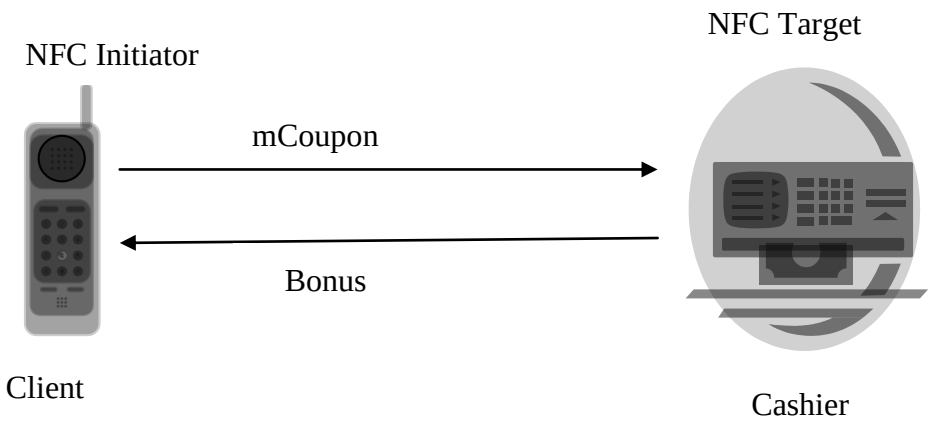


Fig.16 ***Cashing mcoupon***

In figure 12 the recipient uses a mobile phone that is equipped with an NFC interface to collect mcoupon form a newspaper advertisement which has an issuer, equipped with an NFC interface. A valid mcoupon is stored on the mobile by a touch from the client on the issuer. In figure 13 the client, takes the stored mcoupon to a cashier, which is a device also equipped with NFC interface and cash the coupon. The client gets the service product or bonus after the validity of the coupon is verified by the cashier.

To avoid illicit use of the mcoupon, the follow issues need to be considered.

Manipulation : It should not be possible to manipulate mcoupon (any form of manipulation should be invalid)

Multiple cash-in: An attacker must not be able to use the same mcoupon more than ones.

Unauthorized copying: It should not be possible for an attacker to make a valid copy of an mcoupon and cash it in.

Unauthorized Generation: It should not be possible for an attacker to issue his own mcoupons.

However some of these options could be over looked depending on what the issuer company intend to achieve from it.

6.6 NFC targeted for mobile payment service M-payment

The advent of information technology has brought about different kinds of payment services. In this section we shall consider the role of NFC-enabled mobile phone in this emerging technology.

M-payment can be defined as any payment transaction, either executed remotely or in-store, on a mobile device. In most cases a mobile phone [8].

Mobile payments are of two kinds

- Remote mobile payment
- Proximity mobile payment

Remote mobile payment may be implemented using the existing financial payment infrastructure. Example, for payment at a web merchant [9]. This section focuses on proximity mobile payment.

6.6.1 Proximity mobile payment

For example, credit or debit card version of payment application is provisioned on an NFC enabled phone which is issued by the consumer financial institution. The mobile phone uses the built-in NFC technology to communicate with the merchant contactless payment –capable POS (point-of-sale) system, just like the contactless payment card and other devices in use today [9].

Proximity mobile payment can be carried out both attended POS location and unattended location which uses the existing merchant payment infrastructure.

6.6.2 How it works

To make payment, a consumer simply need to bring the phone close to the contactless payment capable POS system and the transaction will be carried out just like in the case of credit and debit cards.

6.6.3 Mobile payment process (Steps)

Service Registration: A consumer subscribe for a payment service with a bank through certain procedure like filling of form.

Payment Request: Consumer initiates a payment to a third party in some cases the payment request is initiated by the third party [8].

Payment Authorization: Before payment can be processed the consumer has to authorize the payment.

Payment Confirmation: Payment outcome confirmation is issued to the consumer.

Payment Report: Consumer is able to view the payment that took place again and again in future.

6.7 NFC Targeted for Ticketing (Mobile Ticket)

A ticket is a paper which gives the holder the right to admission into an event, place or to travel on public transportation. For mobile ticket, it stores the ticket on an NFC device such as mobile phone,which makes the phone act like a tag. At the point of entry or wherever the ticket needs to be shown, the user places the mobile phone against the compatible reader and gets access to the event room or receives services. During this transaction, additional information or adverts can also be transferred to the user's mobile phone.

6.8 NFC Targeted for Transportation

There are two concepts used in this section. In the first concept, the NFC device which is the mobile phone, can be used to read information on the tag at a transit stop and uses the information to generate a ticket. Also, before traveling to any destination, a user can calculate the overall distance as well as road maps by just placing the mobile phone against a tag in the transit stop.

In the second concept, the user places the mobile phone against a reader in the means of transportation, such as in the train or bus and automatically sends a request to a server which identifies the mobile phone, bills and generates ticket.

6.9 NFC Targeted for Smart Poster

Information about products, links to company website and any other information such promo, can stored in a poster by placing an RFID tag on a poster which has data that are coded in accordance with the NDEF specification. Because of this, it can be read by any device such as mobile phone.

6.10 NFC Targeted for Information Transmission

This allows the user to exchange information such business cards, product information, or access information to connect Bluetooth devices or LANs. All the user need to do is to place the NFC enabled mobile phone against a tag or another NFC device and the data will be received.

6.11 NFC Targeted For Access Control

Here the mobile phone acts like the user key to allow access to buildings, offices, etc. The access control data is stored on the NFC-enabled mobile phone. The user's mobile phone is read by a compatible reader at the point of entry. There could also be other information sent to the mobile phone through the mobile phone peer-to-peer mode such as dates, and other details.

6.12 NFC Targeted for a Simple Pairing

Establishing connection between Bluetooth devices has been an uphill task till now [5]. With NFC, the complex process of searching for other devices, analyzing the profile and pairing them has been greatly facilitated by just placing NFC devices against each other and the pairing information will be exchanged, and the connection is established.

7 Threats to NFC Technology and Measures to avert them.

With the implementaion of modern techniques in the build up of wireless communication devices like NFC, several security checks have been put in place to alleviate the occurence of threats so as to promote an effective, efficient and safe communication. However these threats or attacks are inevitable but are minimised to the possible best states. Below are some possible threats NFC is likely to face as well as measures to help avert these threats.

7.1 Data Corruption

In this scenario, an attacker attempts to modify the transmitted data through the NFC interface. The attacker strives to interrupt the communication channel, consequently making it difficult for the receiver to recover the data sent by the other device in a reliable manner. Data corruption can be accomplished by broadcasting valid frequencies of the data spectrum at the appropriate period. The attacker can achieve this by computing the periods for transmission by means of in depth understanding of the modulation scheme and coding used for that specific device. This threat however does not permit the attacker to modify the actual data. Data corruption is categorised as a type of Denial of Service (DOS) attack.

Security measures

This attack can be averted by NFC devices. The reason is that, during the process of transmission of data, an NFC device should check the RF field in order to detect attacks [27]. Such attacks are detectable because the power required to distort the data is much higher than the power required by an NFC devices [27].

7.2 Modification of Data

In this case, the target device obtains some valid but manipulated data. The occurrence of this attack depends immensely on the applied strength of the amplitude modulation.This is because the decoding of the signal is different for 100% and 10% modulation ratios. With 100% modulation ratio, the decoder basically checks the two half bits to determine whether these conditions exist : RF signal on (no break) or RF signal off (break). Taking into account the 10% modulation ratio, two different signals exist, i.e 82% and a Full signal. The decoder determines both signal levels and evaluate them accordingly. In the event that they fall within the acceptable range, the signals are considered to be valid and subsequently decoded. An attacker could attempt altering the signal to represent 82%, that is , an 82% signal will emerge as a Full signal while the real Full signal appear to be 82% signal. In this scenario, the decoder translates a valid bit of the reverse value of the bit transmitted by the correct sender. The feasibility of the attack depends immensely on the active input range of the receiving device.

Security measures

There are three different methods to achieve protection against this attack. They are follows

- The use of 106 kbaud in an active mode [13]. This method makes it almost impossible for any attacker to make any modification(s) to the data transmitted through the RF link. It requires both directions in the active mode for protection against data modification. However, the major problem with this method is that it uses active mode, which is known to be vulnerable to eavesdropping.
- NFC devices have the capability to transmit and receive data simultaneously, as a result, these devices can continously check the RF field while communicating to detect collisions. Nonetheless, it can also stop data transmission when it detects an attack.

- This third method, which is effectively used in many cases of threats is putting in place a secure channel. This method is described below in section 7.6

7.3 Eavesdropping

This happens when an unauthorized user attempts to secretly listen to the signals being transmitted between two NFC devices communicating through a wireless communication channel. Communication between two NFC devices take place in close proximity. This implies that, during transmission,the devices involved are not more than 10 cm (usually less) away from each other. Due to its close proximity and low power RF field , it difficult to eavesdrop communication between NFC devices as compared to other technologies. How close an attacker requires to be in order to regain a functional RF signal depend on certain parameters. These parameters are listed below;

- Quality of the invader's receiver
- Environmental factors (noise, location, position of the invader)
- Attribute of the attacker's antenna (i.e. antenna geometry, likelihood to adjust the position in all 3 dimensions)
- Quality of the invader's RF signal decoder
- Power generated by the NFC device. etc

Furthermore, it is of great importance to know in which mode the sender of the information is operating. Whether the sending device is in the active mode (i.e generates it's own RF field) or whether it is using the RF field generated by another device (passive mode). The two communication modes apply different ways of transmitting the data and thus it becomes difficult to secretly listen to data transmitted on devices sending data in passive mode.

Security measures

It is important to note that, NFC does not provide complete protection against eavesdropping [27]. In this section we will look at two possible recommendations that can help reduce the risk of eavedropping.

Firstly, NFC devices can be operated in the passive mode to avert this attack. The passive device is difficult to eavesdrop for the reason that , data transmitted through the communication channel is sent by means of inductive coupling on the field,which is generated by the active device. According to a rule of thumb, a 10m distance is estimated for eavesdropping between active devices and 1m for passive devices [13].These are based on the NFCIP-1 standard. The same rule can be used for ISO 14443 communications standards which are closely related to the NFCIP-1 standard. For communications based on other standards like ISO 15693, eavesdropping will perhaps be possible over larger distances because it has a larger communication range defined within its standard. However, this is not so effficient when it comes to cases where applications transmit sensitive data.

The second method is more proficient and it involves establishing a secure channel (section 7.6) for an effective communication between the two devices.

7.4 Man-in-the-Middle attack

Man-In-The-Middle attack (MITM attack) is a kind of attack whereby an attacker breaks into an existing connection in attempt to intercept the exchanged data and place in false

information. It involves eavesdropping on a connection, interfering into a connection, interrupting messages, and selectively changing data.

The figure shown below illustrates a typical Man-in-the-Middle attack. Two clients (client1 and client2) communicating with one another, are trapped into another conversation by a third party (attacker). When both clients settle on a private key, which they intend using for a secure data transmission, a threat is likely to occur. This is possible because of the presence of the attacker, sitting in the middle of the exchange. The attacker can however set up a key with each client, making it possible to listen to the communication and subsequently manipulate information being passed on. This can occur at a later time, when each clients use their generated keys to establish a secure data transmission.

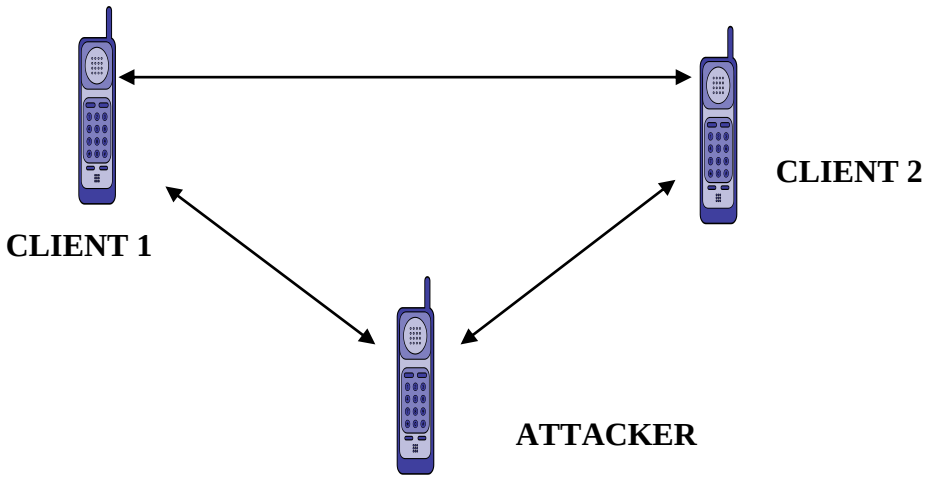


Fig.17 Man-in-the-Middle-Attack

Security measures

In a real-world scenario, man-in-the-middle-attack on an NFC link is difficult to achieve due to the proximity range required by NFC devices to communicate. However, it is strongly advised that, transmission of data between two devices should be in the active-passive mode , in this way the RF field is always generated by one of the valid device.

NFC devices have the capability to receive and transmit data at the same time. As a result, they can verify the radio frequency(RF) field and detect an occurence of collision,that is if the received signal does not agree with the transmitted signal [33].This makes it possible to notice if there are any jammings or incoherent signals.

7.5 Data Insertion

An attacker inserts messages into the data exchange between two devices. But this is only possible, in cases where the answering device needs a longer time to answer. The attacker could then send his data earlier than the valid receiver. The insertion will be successful, only, if the inserted data can be transmitted, before the original device starts with the answer. However,if both data streams overlap the data will be corrupted.

Security measures

There are three possible ways to avert this kind of problem.

The first one is a quick answering from the device that needs to respond. In this way, the attacker will not be fast enough than the answering device. In the worst case, the attacker can be as fast but this will mean that the two devices answer concurrently and that will result in data corruption.

The second method is for the answering device to listen to the channel during transmission in order to detect any possible attacker trying to insert data.

The third method is setting up a secure channel (in section 7.6) between the two communicating devices.

7.6 NFC Secure Communication Channel

One of the best techniques to use in defense against eavesdropping and other types of attack is establishing a secure channel between the two NFC devices. Securing the channel for an effective communication involves the designing of cryptograhic mechanisms that use certain protocols for key agreement and complex algorithms for encryption and data integrity. It is expected that, additional cryptography standards may come in the future, each of them identified by a Protocol Identifier (PID) [30].

A standard key agreement protocol such as Diffie-Hellmann based on Rivest, Shamir and Adleman (RSA) or Elliptic Curves [31] could be used to generate a shared secret key between two devices who have no previous knowledge of each other.

This private key can subsequently be used to obtain a symmetric key such as Advanced Encryption Standard(AES) [35] or Triple Data Encryption Standard (3DES) [34], which are used to create secure channels for effective data communication between the two devices. A high level of confidentiality, integrity, and authenticity of the transmitted data is achieved. Different modes of operation for 3DES and AES could as well be used for securing an insecure communication channel [32].

8 How NFC will make life better now and in the future

There have been constant changes in technological advancement, most of which do not come just as a result of the fact that we need a new way of doing things but as a result of human quest to make life better, easier and above all, very simple. Today, there have been constant improvements in the way we do things due to different number of consumer electronic devices that have been manufactured over the years for different purposes. With these several consumer electronic devices available, there is the need to bring all these different functionalities of these devices into a multipurpose device without having any setbacks in the networking or its functionalities

This section will focus on the benefits of NFC and areas where it has been used, how it influences our behaviour in the society, the future of NFC as a sustainable technology. A qualitative comparison with the following existing technologies would be carried out; NFC versus other Technologies, i.e. NFC & RFID Technology, NFC against Bluetooth and infra red.

8.1 Qualitative Comparison of NFC and other Short Range Technologies

In contrast to other short-range communication technologies, which have been incorporated into mobile phones or PDAs, NFC technology enables simple and safe two-way interactions between electronic devices. The pitfall for infrared has to do with its selectivity mode, i.e. a direct line of sight is essential, which responds sensitively to external factors like reflecting bodies and light. The significant advantage of NFC over Bluetooth is the shorter set-up time. It does not require manual configurations to discover the other's mobile phone, the link connecting two NFC devices is established automatically (<0.1s). NFC is based on existing RFID technology but comes along with unique functionalities such as its three (3) operating modes, namely peer-to-peer, reader/writer or card emulation mode. Table 4 shows the different capabilities exhibited by NFC, infrared, Bluetooth and RFID. NFC has the shortest range (<10cm). This gives it a high level of security and makes it appropriate and reliable for crowded places. NFC has a data transfer rate of 424 kbps, which is less than Bluetooth (721 kbps), but faster than infrared (115 kbps). NFC is compatible with RFID technology in contrast to Bluetooth and infrared.

	NFC	**Infrared**	**Bluetooth**	**RFID**
Type of Network	Point- to- point (p2p)	Point- to- point (p2p)	Point- to- point (p2p) Point- to- multipoint	Point- to- multipoint
Distance(range)	Close to 10 cm	Close to 5 m	Close to 30 m	Close to 3m
Time to setup	Less than 0.1 ms	Approximately 0.5 seconds	Approximately 6 seconds	Less than 0.1 ms
Cost of device	Low	Low	Moderate	Moderate

Usability	Human centric, simple, fast & sensitive	Data centric & simple to use	Data centric & partly easy to use	Item centric & easy
Selectivity	High, assigned with security	Line of sight (LOS)	Based on an individual	Partially assigned
Use Cases	Sharing data, payment, access granting, open service, smart poster etc	Exchange and control of data	Network for exchange of data, headset for some devices	Asset Tracking and identification
Consumer Experience	Touch & Go, Touch & Confirm, Touch & Connect, Touch & Explore	Simple	Configuration required	Obtain information

Table 4: NFC compared with IrDA & Bluetooth [25] [37]

8.2 Advantages of NFC based mobile over other smartcard

This section enumerates some of the advantages of NFC enabled mobile device has over current conventional plastic smart cards.

NFC base contactless devices	Conventional smart cards
NFC base contactless mobile device user can embed several service on a single mobile device	User requires different card for each service
NFC base contactless mobile phones combine both the functionalities of contactless cards and that of mobile phone thereby opening new business area for mobile network operators	It has just smart card functionalities
With NFC contactless mobile device such as mobile phones, it is possible to send message or advertisement to user on the same contactless device.	Different channel like email is required to send such information
NFC contactless mobile devices allow for remote user management and authentication	It does not support this functionalities for user
NFC contactless mobile device like mobile phones offers user interface functionalities for interactivity	No user interface present.
NFC contactless mobile phones support remote issuing/personalization of NFC	User requires a secure postal service to receive a smart card for each service. The

mobile service.	card can be misused if it gets to the wrong hand.
It can act as both initiator and a target	It can only be a target
Service can remotely be deactivated when the NFC contactless card is missing to avoid misuse by non contracted user.	Card can be misuse when it get to the wrong hands
All the information is embedded on the device. This makes it secure for payment because it is impossible for credit card fraud during payment such as theft of credit card number.	An attacker can misuse the card by looking at the information on it when a user is making payment or when hold it close to an attacker.

Table 5 Advantages: NFC contactless device over conventional contactless smart cards

8.3 Some benefits of NFC Technology and how it influences our society

NFC in mobile phones inherited features of already existing contactless infrastructure used by millions of people around the globe. In chapter 5, we saw some benefits of NFC and discussed on how NFC-enabled mobile phone is targeted for several applications. In this section we shall look at some of the benefits from the some perspectives.

8.3.1 Very Simple to Use

NFC enabled devices are easy to use and made accessible to each and everyone. It does not require any initial configuration by the user before it starts to communicate with either an RFID tag, an NFC active or passive device. All it requires for it to function is an RF field, where the communication takes place, together with an NFC-enabled mobile phone and RFID tags, which are positioned at vantage points.

The network pairing is without a fixed, well-defined infrastructure (Ad-hoc pairing). Exchange and storage of data is easily done automatically e.g. pictures, messages, videos etc. The program opens without human intervention thereby a minimal contact with the keypad and screen. This helps to eliminate type errors and wrong data entries by the user [29].

8.3.2 NFC Improves Communication

NFC is an effective, efficient and safe means of improving two way communications. A typical scenario is the use of NFC technology as a way by which workers communicate with each other. Workers at different locations can easily give instant feedbacks as to where they are located on the working field by simply touching an NFC tag positioned at different locations with their NFC-enabled phones. This helps to cut down time as well as improve accuracy

8.3.3 Real Time Management

In our present technological era, time is one of the most essential features required for effective communication. NFC technology will enable a number of industries to work and respond to their daily activities in real time.

A typical example is the use of NFC devices in a business working environment, where an NFC tag tapped by a mobile phone is able to send notification in couple of seconds, making it

possible for head of departments to figure out precisely where their subordinates are, and what they are doing. It allows industries to put in place a more efficient way through which staff working at remote places can report to the central office easily and quicker.

8.3.4 Security

It is difficult to intercept signals in NFC enabled devices because of its short range transmission. It is also very secure in the sense that it reduces credit card fraud because consumers do not need to give their credit card to a merchant during transaction.

8.3.5 Business

NFC enabled mobile phone has a great impact in business. For instance, using NFC in transportation ticketing can make it possible for travellers to buy ticket online and it will be provisioned over-the-air (OTA) on the NFC enabled phone [29]. By this means, the handset serves like an RFID enabled train or bus ticket. Information on train route can be accessed during a transaction and it is possible for the transit operator to send other relevant information such as new services, mcoupons, or an advertisement to a traveller's phone.

Another instance is a scenario where a customer using a cell phone to scan an NFC RFID tag, attached to a product in a shopping mall for various purposes such as, verifying the authenticity of the product, searching a lower price elsewhere within the same area, or getting more information about the product. When the consumer completes the process of reading the tag, requested product information will be downloaded from the company's website using the phone. This provides companies with data concerning the type of product, customers are interested in and the location where it can found. This statistical sale information helps companies understand customer preference.

8.3.6 Consumer Convenience

From the example of NFC transit application, illustrated in section **8.2.5**, the consumer gets other benefits apart from the possibility of conveniently buying ticket(s) online provisioned in mobile phone through a feature known as OTA. A traveller can comfortably add to, or upgrade ticket if he or she has a change in plan. Also, the traveller can get information on status updates on train routes. This helps in making better travelling plans for the day. In the second instance, a consumer can use the information from the product tag to search for better price for the same product nearby. Consumer can also check the authenticity of a product if it has an NFC RFID tag attached to it.

8.3.7 Supplier Perspective

- **Reduction in ticketing cost:** With the advent of NFC in electronic ticketing, ticket operators have witnessed a reduction cost in operation. Currently, airline operators have adopted NFC e-ticketing module because of it secure nature [28]
- **Revenue stream increase due to value added services (VAS):** With the use of NFC technology, mobile operators can expand in the revenue stream [28]. This is possible because user will have easy access to advertisement and other relevant information.

- **Implementation of rich media contents:** NFC allows users to implement sophisticated personal devices that are used only for entertainments, media sharing and storage purposes [28].

- **Easy to use:** NFC mobile technology is very convenient to use and it makes payment easier for users.

8.4 Use cases scenarios

In this section we analyze some use cases scenario of NFC enabled mobile service, how the use of NFC mobile service through NFC enabled mobile devices can be beneficial to user in each scenarios. We compare how NFC mobile phone user and non NFC mobile phone user may accomplish the same activity in these scenarios. The non NFC mobile phone user is today's consumer with conventional infrastructure while the NFC mobile phone user is consumer during when NFC compatible systems will be introduced. We also made certain assumptions based on NFC enabled mobile device functionalities.

8.4.1 Shopping At the Mall Scenario

In this scenario we assume with NFC mobile services potentials, Point-of -sales terminal will have NFC reader/writer that can read mcoupons from NFC phones. Another assumption is that goods manufacturer will provide RFID/NFC tag on some products for authentication and thirdly we assume the retailer have some utility information on NFC smart poster and provide RFID/NFC tag with audio information on products for people who are visually impaired. These assumptions are for all cases of NFC mobile phone user.

Activities	*NFC mobile phone user*	*Non NFC mobile phone user*	*Benefits from use of NFC mobiles*
Payment	Secure payment for goods and services, storing of vouchers, receipts etc by simply touching a payment terminal with an NFC phone.	Non users pays by the use of the cash system, cheques, credit/debit cards	Payment with NFC enabled phone is more secure because it provides confidentiality and integrity. Third parties are not involved in business transactions. Reduce the cost of card issuance and management
Verification	User can verify authenticity of a product that has product company's NFC tag by reading the tag with an NFC phone.	Authenticity can only be verified by careful examination.	With the use of NFC on mobile phones and PDAs, the risk of buying fake products will be reduced.
Utility	User can download mcoupon or additional information from product tag or smart poster such as product instructions, recipe etc	Consumers can only get hard copy of such information.	It may be inconveniency to carry a paper copy of these kinds of information and sometimes it can just be limited copies or even missing. An NFC phone user only requires a touch to get the information.
Aid for visually impaired	Users who are visually impaired can search for items by using their NFC phone to read tags and get feedback information in the form of audio.	There is no such possibility available for non user	This functionality enables people with disabilities to shop by themselves without seeking assistance from others.

The use of NFC on mobile phones comes with new possibilities for people with disabilities. This helps the visually impaired to shop without human aid. The user goes to the shop with an NFC enabled mobile phone, touches it on an item to find the RFID/NFC tag, thereafter the phone reads out the product information such as the name and price for the user to hear.

In the case of an NFC mobile user, he only needs to take along an NFC mobile phone when shopping as against carrying several devices such smart cards for payment and utilities

8.4.2 Travelling Case Scenario

In this section we assume NFC mobile phone user is travelling with a transport company that has NFC compatible systems.

Activities	***NFC mobile phone user***	***Non NFC mobile phone user***	***Benefits from use of NFC mobiles phones***
Ticket purchase and receipt	User can purchase a ticket with NFC phone without having to go to the ticket booth and it will be provision on the mobile phone	Payment usually requires passenger going to physical booth or buying online through internet	Purchase with NFC phone automatically provisions it on mobile phone. This enables the mobile phones to act like contactless ticket. NFC mobile phone user saves time and does not need to go print the ticket after purchase.
Travelling information details.	User can obtain latest updated information of the means of transportation and other information such maps, weather forecast by touching the NFC device in the information kiosk or through OTA during the journey	Non user of NFC phone can only see such information on the screen and might not have during the journey.	With these kinds of information on mobile device, make it easier for consumer to have full understanding of the journey before and during the journey.
Other information during the journey	Additional information can be sent to NFC phone user such as real-time local traffic information	This feature is not available without NFC compatible mobile device	This is easier for the transport company to automatically to send this information to NFC compatible phones through the help of mobile network service provider

From the above scenario, we can see how NFC mobile phones introduce additional services as compared to the conventional transportation services. New services such as, the ability to buy ticket that can be provisioned on mobile phone and used in the form of a contactless ticket, an NFC mobile phone user can also obtain information such as maps, weather forecast by simply touching the NFC device in the information kiosk. These attractive features can make travelling very convenient and cuts down delay in case of emergency. Due to the online services available on mobile phone(s), it makes it possible for transport companies to send updated information to commuters with NFC mobile phones, before, during and after the journey. This feature makes it very easy for commuters to get customer benefits such as mcoupons and stay connected with their regular transport company.

8.4.3 Business Conference Scenario

We assume organizer(s) of this conference sent an invitation that contains access control data which can be stored on an NFC enabled mobile device to all NFC mobile phone user and has a system that is compatible with contactless payment. We also assume each NFC mobile phone user has an NFC information transmission application that contains their business cards. These assumptions are for all cases of NFC mobile phone user

.Activities	NFC mobile phone user	Non NFC mobile phone user	Benefits from use of NFC mobiles phones
Information exchange	Attendee can share information such as business cards, images, contact details, etc by simply bringing their phones into close contact.	Attendee exchange information on paper.	It eases the stress of carrying several business cards. It saves time to exchange contacts which means one can get several numbers within a very short period of time by just a touch per contact. Reduce the cost of card issuance and management
Financial contribution	Contributions made during meeting sessions relating to payment can be done by just touch on a compatible reader.	A non NFC user needs to carry along cash/cards	Is more inconvenient because all you need is just your mobile phone. Risks of receiving fake currencies are avoided. Theft is also checked.
Access control	Users can access conference venue using the access control data which can be sent along with the invitation to the user phones	A cross check would have to be conducted to verify if the user is authorized to attend such meeting.	Makes it very simple for authorized attendees to gain access to the venue. Time needed to cross check long lists which could delay and interrupt meetings are controlled.
Event information	Agenda and other event details can be sent to an attendee's mobile phones.	Non user gets a printed copy of the agenda.	Any changes made in the agenda can easily be updated in attendees NFC mobile phone. It makes it easier for an attendee to easily access the web link or contact details on the event information.

This scenario shows how the use of NFC in mobile phone(s) can help achieve a well organised meeting. It ensures that only invitees have access to meeting/conferences rooms and

attendees spend lesser time exchanging contact information during the meeting .New possibilities are brought to this scenario such as the possibility for an attendee to get update information of the event and access web links directly from the event information. Also attendees do not have to worry about coming along with cash or cheque book(s) during financial contribution(s) because they can make all payments with an NFC enabled phone.

.

8.4.4 Patient in the hospital scenario

Activities	**NFC mobile phone user**	**Non NFC mobile phone user**	**Benefits from use of NFC mobiles phones**
Prescription	User can read and store prescription and dosage information from smart tag to NFC phone. E.g. name of drug, pills/dose, etc	Prescription and dosage information are read manually by the user.	This makes it possible to still have the prescription even when the prescription paper is missing. The possibilities of obtaining wrong information on drugs are reduced to minimal
Drug authentication	Authenticity of drugs can be checked by reading tags with NFC device	Authenticity of drugs is checked by careful inspection.	It reduces the risk of buying fake drugs.
Payment	User can pay for bills and services rendered by touching a payment terminal with an NFC enabled phone	Service bills are paid with cash, debit/credit cards or cheques.	Safer, convenient payment method.

Patient request	Patients with NFC mobile phones can easily keep in touch with their caretakers by touching a tag to notify that they need assistance.	Patients require alarming bells, sending a short messaging service (sms) or placing a phone call.	It helps to reduce response time to patient requests and in general increase patient's satisfaction

In this scenario the use of NFC on mobile phone helps a patient on sick bed to improve their communication with their caretakers in the form of touch based communication by touching smart tag to notify that they need assistance. There are also other benefits such as the ability to check the authenticity of drugs and ensuring that patient takes the right dosage of drug at the right time with the help of NFC mobile phone reminder functionality.

We assumed that the hospital's pharmacy has a system that can write drug prescription on RFID/NFC tag which will be attached to patent's drug in addition to the writing prescription and a payment method that is compatible with NFC technology. Also we assume drug manufacturer attached RFID/NFC tag to drug containing company's information for authentication purpose. These assumptions are for all cases of NFC mobile phone user.

8.5 NFC Technology becoming a Success

Industrial estimate propose that not less than 16% of mobile subscribers will have an NFC enabled mobile device by 2014. Presently the cost of NFC chipset is between 2 to 2.5 dollars and it has been forecasted that the cost will reduce to 1 dollar by 2013 [28]. Research has shown that Far East and Western Europe, North America and China will be at the lead in the shipment of NFC phone by 2013. Each of these regions will have an annual excess shipment of 20% [28].

In a related development, Mobilkom Austria an Austrian major mobile Network operator, has in September 2007 brought out the most extensive NFC service in the world and by 2009 it had made €50m revenue in mobile payment.

NFC technology is gradually becoming a global phenomenon as more companies are adopting this emerging technology and certain countries have already put the infrastructure in place. US, has recorded a successful mobile commerce in the NFC pilot project which involved some US payments processor. Also, Malaysia has launch Maxis Fastap NFC service.

Chinese companies Bank of communication (BoCom) China, Unicom and China UnionPay (CUP) have in June 2010 announced that they will launch an NFC payment service supporting NFC enabled handset. Meanwhile Chinese banks in conjunction with Unicom have put in place all that is needed to offer NFC services [28]

NFC service project are also going on in developing countries like Indian. In Bengaluru, pilot project called City tap and pay was started and discussions are on- going to include NFC enabled ticketing in metro project in Delhi [18].

9 Conclusions

This thesis presents a summary on how the use of NFC on mobile device allows functionalities of several consumer devices to be carried out with just a single mobile device, its benefits and additional features over related technologies. To realize these goals, we have shown how the use of NFC on mobile phone will make life better by a qualitative comparison with other existing technologies such Bluetooth, RFID, infrared. We also came up with benefits that NFC enabled mobile devices have over conventional smart cards and how it influences our society economically and technologically (i.e. its simplicity, efficient communication and security).

Finally, we demonstrated four use case scenarios of different activities and compared the conventional approaches with that of the NFC-enabled mobile phone user approach. In each scenario, we found out that, the NFC-enabled mobile user approach provides more benefits such as better and convenient payment, authenticity verification, fast and easy exchange of information, user interface screen for viewing information at convenient time as well as additional possibilities like utility features such as storage of mcoupon, product information or any other information and ability to provide audio information for user who are visually impaired as against the conventional approach.

REFERENCES

[1] Sixto Ortiz Jr. *Is Near- Field Communication Close to Success?* , IEEE Technology New, Mar 2006

[2] Jorman Ylinen, Mikko Koskela, Lari Iso-Anttila & Pekka Loula. *Near-Field Communication Network Service*: Tampere University of Technology/Pori Pohjoisranta 1128100 PORI Finland, Feb 2007

[3] Sudha Krishnamurthy, Dipanjan Chakraborty, Sandeep Jindal, Sumit Mittal, *Context – based adaptation of mobile phones using near field communication*, IEEE 1-4244-0499-1/06 2006

[4] Collin Mulliner, *Vulnerability analysis and attack on NFC-enable mobile phones*, IEEE International Conference on Availability, Reliability and Security 978-0-7695-3564-7/ 09 /2009

[5] Stollmann: *NFC Technical Overview (release r05)*, http://www.stollmann.de/en/home/

[6] *Essential for Successful NFC Mobile Ecosystem*, NFC Forum, Oct 2008

[7] Sandra Dominikus, Manfred Aigner, *Mcoupons: An Application for Near Field Communication (NFC), IEEE 21st International Conference on Advanced Information Networking and Applications Workshops* (AINAW'07) 0-7695-2847-3/07 2007

[8] Microsoft and M-com," *A white paper on mobile payment*, Sept 2009

[9] Smart Card Alliance, *Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure*, Sept 2007, http://www.smartcardalliance.org/

[10] Stefano L Ghìron, S Sposato, C M Medaglia, *A Moroni NFC Ticketing: A Prototype and Usability test of an NFC-based Virtual Ticketing Application*, IEEE First International Workshop on Near Field Communication 2009

[11] ISO/IEC 18092(ECMA-340), *Information technology – Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)*. First Edition, 2004-04-01.

[12] Ecma International, "Standard ECMA-340, *Near Field Communication Interface and Protocol (NFCIP-1)*, Dec 2004, http://www.ecma-international.org/

[13] Ernst Haselsteiner and Klemens Breitfuss, *Security in Near Field Communication (NFC)*, RFIDSec 06, 2. July 13, 2006.

[14] ISO/IEC 14443, *Identification cards - Contactless integrated circuit cards - Proximity cards*. 2001, www.iso.ch.

[15] *Near Field Solutions,* http://www.usingnfc.com/about.html

[16] Technovelgy, How RFID Works, http://www.technovelgy.com

[17] Klaus Finkenzeller, RFID Handbook: *Fundamentals and Applications in Contactless Smart Cards and Identification*, 2002.

[18] Amit Goel and Varun Uppal , Near Field Communication (NFC): Next Big Hope?, May 10, 2010

[19] RFID – journal: *The basics of RFID technology,* http://www.rfidjournal.com/

[20] NFC Forum. http://www.nfc-forum.org/

[21] http://en.wikipedia.org/wiki/Near_Field_Communication

[22] ISO/IEC 21481, *Information Technology Telecommunications and information exchange between systems Near Field Communication Interface and Protocol -2 (NFCIP-2)*. Jan 2005.

[23] Autumn C. Giusti, *NFCNews: Breaking down the business cases for NFC,* Jun 2010

[24] An RTC Group Publication, *Voice over WI-FI implementation with a single stream 802.11n*, http://rtcgroup.com/, Sept 2008

[25] C. Enrique Ortiz, *An Introduction to Near-Field Communication and the Contactless Communication API*, Jun 2008

[26] NFC Forum, *About the NFC Forum N-Mark*, http://www.nfc-forum.org

[27] Ernst Haselsteiner and Klemens Breitfuß, *Near Field Communication (NFC) Strengths and Weaknesses*, Philips Semiconductors Mikronweg 1, 8101 Gratkorn, Austriaernst

[28] Sarah Clark, *China Unicom and Bank of Communications announce commercial NFC payments launch,* Jun 25, 2010

[29] BlogNFC, *What is NFC*, http://www.blognfc.com

[30] Ecma International Standard ECMA-340, *Security Services and Protocol Cryptography Standard using ECDH and AES (NFCIP-1)* , December 2008, http://www.ecma-international.org/

[31] W.Diffie and M.E. Hellman, *New Directions in Cryptography*, IEEE Trans. on Info Theory, Vol. IT- 22, Nov. 1976, pp 644-654(Invited paper).

[32] Morris Dworkin, *Recommendation for Block Cipher Modes of Operation*, NIST Special Publication 800-38D, Nov 2007.

[33] Gauthier Van Damme, Karel Wouters, "Practical Experiences with NFC Security On Mobile Phones", 2009 https://www.cosic.esat.kuleuven.be/index.html

[34] ISO/IEC 10116*: Information technology - Security techniques - Modes of operation for an n-bit block cipher*, Feb 1, 2006 — ISO

[35] J. Nechvatal, et. al., *Report on the Development of the Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, October 2, 2000.

[36] http://www.contactless-payment.co.uk/images/Contactless-Terminal.jpg

[37] Annika Paus, *Near Field Communication in Cell phones*, 24 Jul, 2007

[38] Steve Morris & Alastair Lefley, "*A 90nm CMOS 13.56MHz NFC Transceiver" IEEE* Asian Solid State Circuits Conference Taipei, Taiwan November 16-18, 2009.

[39] Pulse *"NFC Stamp Antenna"* 2010, www.pulseeng.com/antennas

[40] Near Field Communication Stamp Antenna supports all RFID tag sizes.(Pulse's Compact NFC Stamp Antenna Enables Integration with Penta-band Antenna in Single Module). *HighBeam Research.* 11 Dec. 2010, http://www.highbeam.com