NEAR FIELD COMMUNICATIONS

Neha Katkamwar

Department of Electronics & Telecomm, Ramrao Adik Institute of Technology,
University of Mumbai, Maharashtra, (India)

ABSTRACT

Near field communication (NFC) is a set of standards for Smart Phones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few inches. Present and anticipated applications include contactless transactions, data exchange, and simplified setup of more complex communications such as Wi-Fi. Communication is also possible between an NFC device and an unpowered NFC chip, called a "tag".

NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum, which was founded in 2004 by Nokia, Philips Semiconductors (has became NXP Semiconductors since 2006) and Sony, and now has more than 160 members. The Forum also promotes NFC and certifies device compliance. It fits the criteria for being considered a personal area network.

Keywords: Near field communication, NFC Format, NFC Applications.

I INTRODUCTION

For many years, pervasive computing research has explored the potential benefits of creating a connection between the virtual world of the internet and the physical world we live in. The Near Field Communications (NFC) Standard might at last be the technology that makes these visions a ubiquitous reality. This concept is sometimes referred to as the “Internet of Things”. Evolving from a combination of contactless identification (RFID) and interconnection technologies, NFC technology bridges today’s connectivity gap. It enables the simple transfer of information -- from phone numbers to electronic transactions -- and allows people to interact with their environment without needing to navigate complicated menus or perform complex set-up procedures. The key to automation is proximate identification usually limited to about 10 centimetres.

So, just as you would walk across a room full of people to have a private conversation with someone, rather than shouting across it so that everyone could hear, Near Field Communication (NFC) uses the same principle to link electronic devices. It enables the user to exchange all kinds of information, in security, simply by bringing two devices close together. Its short-range interaction over a few centimetres greatly simplifies the whole issue of identification, as there is less confusion when devices can only "hear" their immediate neighbours.

1.1 What is NFC..??

Definition

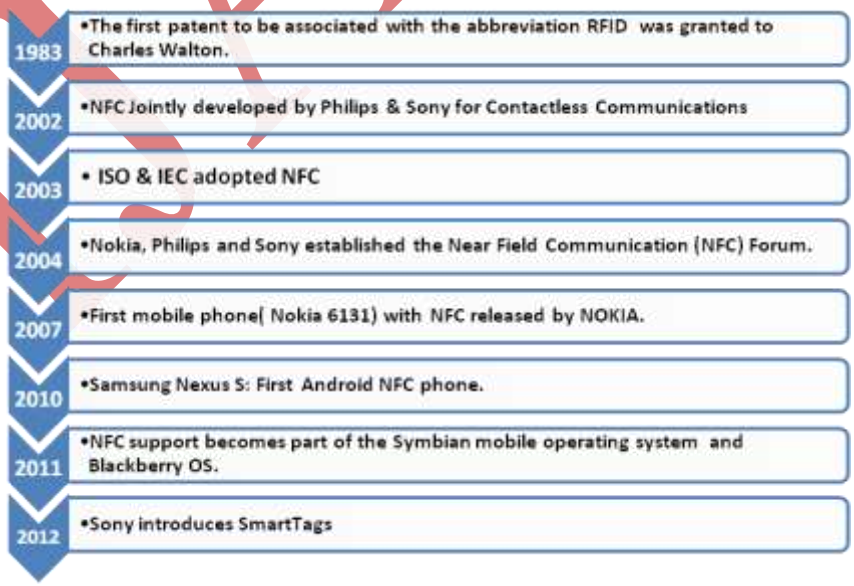
NFC is a short range and standardised (ISO 18092) wireless communication technology that adds contact less functionality to mobile devices including mobile phones and PDA's (Personal Digital Assistants). Such devices can act both as a "contactless card" based on its secure element and as a "contactless reader" and also operate in P2P mode with peer devices. These devices support various contactless communication standards, such as ISO 14443, ISO 15693, FeliCa and Mifare Standard.NFC is a form of radio-frequency identification (RFID) and it enables exchanging data without a physical contact. Important to emphasize that this technology enables a two-way communication, while earlier contactless smart cards offered only one-way communication.

NFC Reader: Usually a microcontroller-based (for example NFC enabled phones) with an integrated circuits that is capable of generating radio frequency at 13.56 MHz with other components such as encoders, decoders, antenna, comparators, and firmware designed to transmit energy to a tag and read information back from it by detecting the backscatter modulation. The reader continuously emits RF carrier signals, and keeps observing the received RF signals for data.

NFC Tag: An RFID device incorporating a silicon memory chip connecting to external antenna. Tag does not have its own power source (passive). The passive tag absorbs a small portion of the energy emitted by the reader (phone), and starts sending modulated information when sufficient energy is acquired from the RF field generated by the reader. Data modulation (modulation for 0s and 1s) is accomplished by either direct modulation or FSK or Phase modulation.

When you look for an NFC tag to buy, you will see a capacity listed. This is the amount of data that can be stored on each tag. Most tags have around one kilobyte of storage available.

1.2 History of NFC



1.3 Why NFC?

With the widespread adoption of smart devices across the global communications marketplace, powerful, easy-to-use computing is now ubiquitous. Consumers now expect that a single device can be used to access a suite of converged services that use the mobile network for communications, entertainment and increasingly, commerce. With Near Field Communication (NFC), the same mobile device becomes a platform for new applications that will massively enhance the total consumer experience using smart phones and related portable information devices.

1.4 Comparison with Existing Technologies

	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~0.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

1.5 Software

NFC tag programming app: Once you receive your tags, it's on to the programming. To do this, you will need an app on your phone. The most popular one that I have found is called NFC Task Launcher. There are a bunch of others, including NFC Writer and NFC Tag Writer. Find the one that you like the best, and go with it. Make yourself familiar with the app you chose, and then you need to decide what you want your tag to do.

1.6 Hardware: Architecture

NFC technology integrated in a mobile device consists of two integrated circuits. SE's and an NFC interface. The NFC interface is composed of a contactless; analogue/digital front-end called an NFC Contactless Front-end (NFC CLF), an NFC antenna and an IC called an NFC controller to enable NFC transactions. The NFC Controller is required for the analogue digital conversion of the signals transferred over the proximity connection. Apart from an NFC controller, an NFC enabled mobile phone has at least one SE which is connected to the NFC controller for performing secure proximity transactions with external NFC devices (e.g. payment at POS) through Single-Wire Protocol (SWP). The SE provides a dynamic and secure environment for programs and data. The secure element is also called as tag emulation operating mode. It enables secure storage of valuable and private data such as the user's credit card information, and secure execution of NFC enabled services such as contactless payments. Also, more than one SE can be directly connected to the NFC controller. The supported common interfaces between SE's and the NFC controller are the Single Wire Protocol (SWP) and the NFC Wired Interface (NFC-WI). The SE can be accessed and controlled from the host controller

internally as well as from the RF field externally. The host controller (baseband controller) is the heart of any mobile phone. Host Controller Interface (HCI) creates a bridge between the NFC controller and the host controller. The host controller sets the operating modes of the NFC controller through the HCI, processes data that are sent and received, and establishes a connection between the NFC controller and the SE. Also, host controller is able to exchange data with the secure element (internal mode e.g. for top up of money into the secure element over the air. NFC is closely related to RFID (Radio Frequency Identification). RFID is mainly used for remote tracking, tracing and identification of goods and persons without a line of sight while as NFC is used for more sophisticated and secure transactions like contactless access or payments. Both technologies have several layers and protocol concepts and are therefore open for the same attacks.

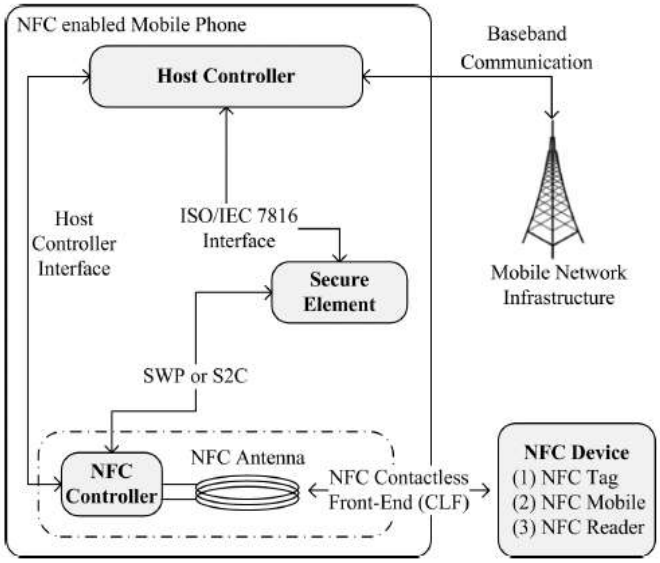


Figure 1: Architecture of NFC Integrated In a Mobile Device

1.7 Basic Functioning

1.7.1 RF Operation

A coild of wire forms an inductive circuit element, and a current in that inductor creates a magnetic field around it. When two inductors are placed very near each other, a changing magnetic field generated in one inductor induces a voltage across the other inductor. This phenomenon is called Faraday's Law and is how motors and generators work. When an alternating current circulates in a coil of wire, two types of fields are produced; radiating and non radiating. If the wire is very small compared to a wavelength, very little energy can propogate away from the inductor in the radiating field, and the movement of energy is predominently contained in the non radiating field, called the Reactive Near Field.

It is called this because unless some of the energy is taken out of the field by loading it, the energy is reabsorbed by the source instead of radiating out to the free space. It is the reactive near field, that is used by NFC. In fact, it is preferable to minimize the radiating field energy for security purposes. A way to load and thereby transmit information through the reactive near field is to place another inductor in the prosimity to the field so that the changing magnetic flux passes through the other inductor, causing a terminal voltage. The amount of coupling between two inductors that can be achieved this way is called The Mutual Inductance of the

inductor pair. Another way to look at this communication link is as to sides of a transformer, where the input of the transformer is one side of the NFC link and the output is on the other side. In order to maximize energy transfer through the inductors, they are each resonoted with a capacitor as a matching network. The capacitors and inductors form a pair of coupled resonators.

The voltage generated at the receiving resonator © changing magnetic field is used to energize the electronic cirtuits in a passive NFC tag. The energizing signal for NFC is a 13.56 MHz carrier that is allowed for transmission in all regulatory regions. The sam Erf energizing signal is also used to send the data. The amplitude of the energizing signal is modulated by the NFC reader, then the receiving circuits in the NFC tag strip off a baseband waveform that is detected and demodulated. After sending its message to the tag, the reader continues to send the RF signal without any modulations so that tag can remain ereergized and waits for a response. The tag responnds by modulating the load it presents to the reader. Since any energy transmitted to the load in the tag must be generated in the source at the reader, a change in tag load is seen as a change in current in the reader inductor. The tag data stream does this modulation by driving a circuit that switches the load across its inductor. The reader detects this change in current and as a result can demodulate the data from the tag. This method for the tag to communicate to the reader while still being energized by it is called load modulation. Care must be taken in the placement of the NFC antenna in the phone package as the magnetic field has the potential of disrupting the operation of the phone circuits, and the structure around the antenna can pull its resonant frequency.

1.7.2 Protocol

The following describes the salient features of NFC speciications ISO/IEC 18092 and ECMA-340 v2 (NFCIP-1):

1. Operation is half-duplex, one-on-one sessions with no broadcast capability.
2. Required data rates are 106, 212, and 424 in all modes. Carrier is 13.56 MHz.
3. Operating Magnetic Field strength is 1.5 A/m to 7.5 A/m. The initiator must be able to gneerate a field in this range over its product defined volume and a target must be able to operate over this range. Both devices need to have field detection with a threshold of 0.1875 A/m.
4. The initiator of the communication in any mode chooses the initial bit rate.

1.7.3 Link Level

1. All devices listen before talk for a level of 0.1875 A/m H field.
2. Application initializes initiator, determines active/passive mode, and sets two way data rate (same in both directions).
3. ID bytes are 4, 7 or 10 bytes in length.

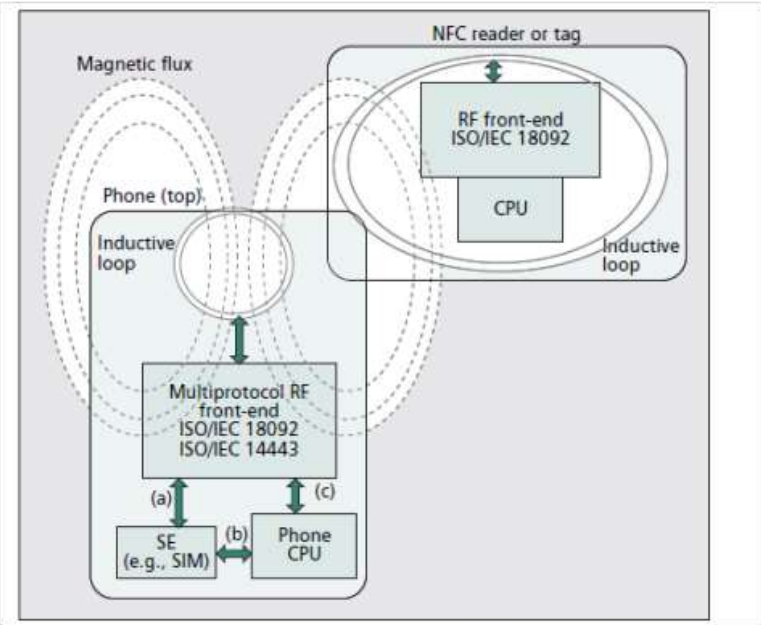


Fig 2. A high level depiction of a phone reader and a passive Tag.

Each has an inductive loop and the magnetic flux lines show how the energy is transferred. The phone is shown supporting both ISO/IEC 18092 and ISO/IEC 14443, but the tag is the former. The phone is also shown supporting a Secure Element (SE) which is where any Bank Card, Credit Card and Encryption information would stay and maybe a SIM card. The arrows indicate flow for three types of use. The path for (a) is between the NFC front and the SE so the phone is operating as a Card Emulator. Secure Financial Transactions may occur in this mode as if it were a contactless card. Path (b) would be used for when the phone needs to load the SE with a secure application or financial "Topping Up". The path in (c) would be used when the phone is operating as a reader and in peer-to-peer mode.

II TECHNICAL FEATURES

2.1 Modes of Operation

- **Reader/Writer mode**: In this mode the NFC device can read or write information such as URLs, SMS's in a tag or smart card e.g. Smart posters applications. Here, users touch the device or a cell phone with the tag embedded in the poster, which triggers the transmission of a URL to the phone. The URL could be used to open the web browser without any human intervention.
- **Card Emulation mode**: In this mode the NFC enabled device emulates a contactless smartcard (ISO 14443). In this case there is a secure element embedded in the device where sensitive data can be stored in a safe place and value added services requiring a high level of security such as payment applications can be made available to the customers.
- **Peer-to-Peer mode**: In this mode a connection is established between two NFC enabled devices and data can be exchanged between them. The NDEF (NFC Data Exchange format) is used to transmit data. This mode is standardized on ISO 18092.

2.2 NFC Signalling Technologies

Three signalling technologies exist for NFC devices to talk to each other. Offering different signalling technologies ensures the various types of near field communication technology can communicate with one another. Easy access is the key to NFC and is one of its primary benefits.

NFC-A: NFC-A corresponds with RFID Type A communication. In Type A communication, Miller encoding, also known as delay encoding, is used with amplitude modulation at 100 percent. Using this set-up, a signal sent between devices must change from 0 to 100 percent to register the difference between sending a "1" and a "0." Data is transmitted at 106 Kbps when using Type A communication.

NFC-B: Similar to NFC-A, NFC-B corresponds with RFID Type B communication. Instead of Miller encoding, Type B uses Manchester encoding. Amplitude modulation is at 10 percent, meaning a 10 percent change from 90% for low to 100% for high is used. A change from low to high represents a "0" while high to low represents a "1."

NFC-F: NFC-F refers to a faster form of RFID transmission known as FeliCa. Commonly found in Japan, FeliCa is a technology similar to NFC but faster and currently more popular. It is used for a variety of services such as subway tickets, credit card payments, and identification at office buildings and other locations with limited access.

2.3 Modes of Communication

NFC has two communicative terminals: The INITIATOR is the one who wishes to communicate and starts the communication. The TARGET receives the initiator's communication request and sends back a reply

There are two modes of communications.

- **Active Communication Mode:** Both Initiator and Target device communicate by alternately generating their own field. A device deactivates its RF field while it is waiting for data. In this mode, both devices typically need to have a power supply.
- **Passive Communication Mode:** The Initiator device provides a carrier field and the target device answers by modulating existing field. In this mode, the Target device may draw its operating power from the Initiator-provided electromagnetic field.

2.3.1 NFC Modulation & RF Signal: The RF signal format and modulation for NFC systems has been developed to ensure reliable communications while not consuming too much power. The NFC modulation format has also been chosen to cater for both active and passive modes of operation.

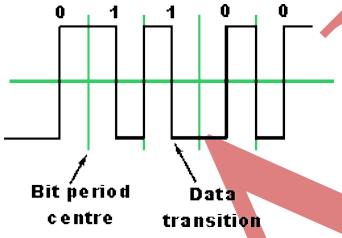
2.3.2 NFC RF signal parameters :NFC uses the global 13.56 MHz allocation as this is an unlicensed radio frequency ISM band .Using ASK - amplitude shift keying, as the format for the NFC modulation, most of the RF energy is concentrated in the allowed 14 kHz bandwidth, although the sidebands may extend out as far as ± 1.8 MHz .

2.3.3 NFC RF signal coding: NFC employs two different coding systems on the RF signal to transfer data. In most cases a level of 10% modulation is used, with a Manchester coding format. However for an active device transmitting data at 106 kbps, a modified Miller coding scheme is used with 100% modulation. In all other cases Manchester coding is used with a modulation ratio of 10%.

DATA RATE KBPS	ACTIVE DEVICE	PASSIVE DEVICE
106	Modified Miller, 100%, ASK	Manchester, 10%, ASK
212	Manchester, 10%, ASK	Manchester, 10%, ASK
424	Manchester, 10%, ASK	Manchester, 10%, ASK

2.3.4 NFC and Manchester coding: Manchester coding is used for the majority of cases for the NFC communications. The Manchester coding utilises the two different transitions that may occur at the midpoint of a period. A low-to-high transition expresses a 0 bit, whereas a high-to-low transition stands for a 1 bit.

To achieve these conditions it is sometimes necessary to have a transition at the middle of a bit period. Transitions at the beginning of period are disregarded.



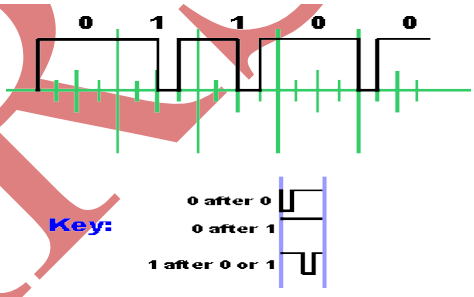


Fig. 3 Manchester coding used for NFC data transfer **Fig. 4 NFC and Modified Miller coding**

2.3.5 NFC and Modified Miller coding

The modified Miller code is a little less intuitive, but provides an efficient form of coding. It is characterised by the pauses occurring in the carrier at different positions of a period. Depending on the information to be transmitted, bits are coded as shown below. A high or "1" is always encoded inth e same way, but a low or "0" is encoded differently dependent upon what preceded it. Modified Miller coding used for NFC data transfer used for 106 kbps active device transfers

2.4 Specifications

2.4.1 Protocol Technical Specifications:

- NFC Logical Link Control Protocol (LLCP): This specification defines an OSI layer-2 protocol to support peer-to-peer communication between two NFC-enabled devices, which is essential for any NFC applications that involve bi-directional communications.

- NFC Digital Protocol Technical Specification: This specification addresses the digital protocol for NFC-enabled device communication, providing an implementation specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards.
- NFC Activity Technical Specification: The specification explains how the NFC Digital Protocol Specification can be used to set up the communication protocol with another NFC device or NFC Forum tag.
- NFC Simple NDEF Exchange Protocol (SNEP) specification: The Simple NDEF Exchange Protocol (SNEP) allows an application on an NFC-enabled device to exchange NFC Data Exchange Format (NDEF) messages with another NFC Forum device when operating in NFC Forum peer-to-peer mode..
- NFC Analogue Technical Specification: This specification addresses the analogue characteristics of the RF interface of the NFC-Enabled Device.
- NFC Controller Interface (NCI) Technical Specification: The NCI specification defines a standard interface within an NFC device between an NFC controller and the device's main application processor.

2.4.2 NFC Data Exchange Format (NDEF) Technical Specification: Specifies a common data format for NFC Forum-compliant devices and NFC Forum-compliant tags .

2.4.3 NFC Forum Tag Type Technical Specifications: The NFC Forum has mandated four tag types to be operable with NFC devices. This is the backbone of interoperability between different NFC tag providers and NFC device manufacturers to ensure a consistent user experience. The operation specifications for the NFC Forum Type 1/2/3/4 Tags provide the technical information needed to implement the reader/writer and associated control functionality of the NFC device to interact with the tags.

2.4.4 Record Type Definition Technical Specifications : Technical specifications for Record Type Definitions (RTDs) and five specific RTDs: Text, URI, Smart Poster, Signature and Generic Control.

2.4.5 Reference Application Technical Specification

- NFC Forum Connection Handover Technical Specification: This specification defines the structure and sequence of interactions that enable two NFC-enabled devices to establish a connection using other wireless communication technologies.
- Personal Health Device Communication Technical Specification: Addresses a need for an openly-defined standard for the exchange of personal health data between devices using Near Field Communication technology.

2.5 Categories

- **Touch and Go:** Applications such as access control or transport/event ticketing, where the user needs only to bring the device storing the ticket or access code close to the reader. Also, for simple data capture applications, such as picking up an Internet URL from a smart label on a poster.
- **Touch and Confirm:** Applications such as mobile payment where the user has to confirm the interaction by entering a password or just accepting the transaction.

- **Touch and Connect:** Linking two NFC-enabled devices to enable peer to peer transfer of data such as downloading music, exchanging images or synchronizing address books.
- **Touch and Explore:** NFC devices may offer more than one possible function. The consumer will be able to explore a device's capabilities to find out which functionalities and services are offered. Ex. url tags

2.6 Services

Services provided by NFC technology are as follows:

- Connectionless Transport: An unacknowledged data transmission service with minimal protocol complexity.
- Connection-oriented Transport: A data transmission service with sequenced and guaranteed delivery of service data units.
- Data link connection: A unique combination of source and destination service access point address used for numbered information transfer.
- Logical Link Control (LLC): It forms a part of the data link layer that supports the logical link control functions of one or more logical links. It includes interpreting message packets (PDUs) received on a network and generating appropriate response and acknowledgement data (PDUs).
    - Logical Link Control Protocol (LLCP): It provides a reliable communication channel between the local and the remote LLC that provides the transport for all data link connections and logical data links.
    - NFC Data Exchange Format (NDEF): It defines a message encapsulation format to exchange information, for example, between an NFC device and another NFC device or an NFC tag.
    - NFC Tag: An NFC tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product. It can store data in NDEF format. The following figure illustrates the NFC Services architecture. It works on client-server architecture and has four main components - NFC applications, NFC client, NFC server and NFC libraries:

III APPLICATIONS

Technology in the mobile industry has been moving towards integration of Near Field Communication (NFC) technology into mobile commerce. The driving force behind NFC is the public's ever increasing dependence on, and demand for smart phone functionality. This trend provides many easy ways for businesses and consumers of mobile commerce to conduct all varieties of transactions using NFC integrated on mobile devices. The many benefits and potential uses of NFC technology will continue to drive the technology and push innovation in the application fields.

A. Financial Transactions: For many people, having an ample amount of cash on hand can often be a challenge. And Rather than having to unexpectedly run to the nearest ATM, one can now use NFC technology on their mobile device to pay for things in a new ways.

B. Peer to Peer Mobile Payment: Another form of Mobile commerce that is newly available through the use of NFC technology is person to person financial exchange .The technology allows a person to send payment to another person simply by tapping NFC enabled phones together.

C. Reader/Writer mode (Use of smart tags in all applications)

D. Mobile Coupons: Instead of clipping coupons from the local newspaper, a consumer can now redeem a mobile coupon with a NFC enabled mobile device.

E. Peer to peer connection with consumer electronics: Consumer devices can be paired with mobiles just by tapping the two.

F. Healthcare: An all-purpose NFC module can easily be integrated into several medical measurement devices like blood pressure meters. After the measurement, data can be accessed simply by touching the medical measurement device with a NFC enabled mobile phone.

G. NFC in corporate / home security: simplifying everyday tasks like unlocking doors and logging in to computers

H. Transportation: A mobile device to act as a key to enter into hotel rooms and even to register a guest

I. Hotel Industry: A mobile device to act as a key to enter into hotel rooms and even to register a guest

J. Social and Entertainment: No new technology would be complete if it too didn't add its footprint to the social networking, gaming and entertainment world. Some people are dependent on social networking sites to receive information and NFC is making taking the possible avenues to make it easier for this audience to receive their information.

IV ADVANTAGES & DISADVANTAGES

Advantages	Disadvantages
1. Intuitive • Only requires swiping the NFC-enabled device • Easy to incorporate into an information system • Reduces employee training costs, reduces procedural errors, productivity 2. Versatile • Appeals to a broad range of industries • Can support any system, process, or service requiring data transfer or authentication 3. Open & Standard Based • underlying layers of follow universally implemented ISO, ECMA, and ETSI standards 4. Technology Enabling • Facilitates fast and simple setup of wireless technologies, such as Bluetooth, Wi-Fi, etc. 5. Inherently Secure • Transmissions are short range with no physical access to the store owners with your credit card information. 6. Interoperable • Works with existing contactless card technologies 7. Security ready • Has built in capabilities to support secure applications like requirement of PIN for authorization	1. High cost • Must provide all relevant members of an organization with NFC-enabled devices 2. Security risks • Losing an NFC-enabled device could mean loss of confidential business and personal information 3. Slow adoption rates • Makes business value realization difficult • Tangible and intangible benefits still only theorized and yet to be seen in real-world business applications 4. Risk of fraud • Based on integration with bankers, normally takes more time for funds to be cleared, thus risking denial of payment by banker. 5. Phone being prone to hacking • With development of software, the phones are more prone to hacking, putting all your financial data to risk. 6. Ecosystem • Multiple players & stakeholders must agree that NFC is the way of the mobile commerce future so that the entire necessary infrastructure can be put in place. 7. Incentives for adoption • Stores and merchants need adequate incentive to purchase readers, which will only occur with enough demand from customers

V SECURITY ASPECTS

There are several important areas for near field communications security. Some of the major NFC security areas are given below:

NFC security – Eavesdropping: Although near field communication is a short range technology - as the name implies - this does not make it immune to security attacks. As NFC uses radio waves to communicate, and these propagate in the vicinity of the transmitter, and not just to the wanted receiver, it is possible for unwanted users to pick up the signals.

NFC security - data corruption: This near field communications security issue is essentially a form of denial of service attack. Rather than just listening to the communications, the attacker may try to disturb the communications by sending data that may be valid, or even blocking he channel so that the legitimate data is corrupted.

NFC security - data modification: This form of NFC security issue involves the attacker aiming to arrange for the receiving device to receive data that has been manipulated in some form. This data will naturally have to be in the correct format for it to be accepted.

NFC security - man-in-the-middle: This form of NFC security issue involves a two party communication being intercepted by a third party. The third party acts as a relay, but using information received and modifying it if required to enable the attacker to achieve their aims. This must obviously be achieved without the two original parties knowing that there is an interceptor between them.

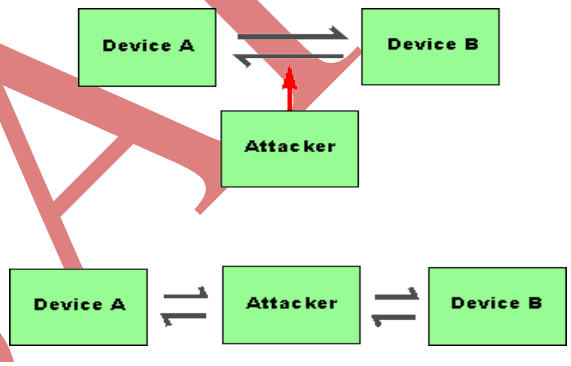


Fig. 5 NFC security - man-in-the-middle

NFC secure channel: The best approach to ensuring NFC security is to use an NFC secure channel. This means that the information is encrypted, and therefore can only be read by the intended receiver. The shared key can be used to derive a symmetric key which can then be used for the NFC secure channel. The NFC secure channel provides for confidentiality, integrity and authenticity of the data transferred between devices.

It is also easy to lose the NFC tag, and it can then be used by anyone. NFC devices should therefore be accompanied by some sort of password (pin code, cell phone password, face recognition), to ensure that no unauthorized users get access.

VI FUTURE SCOPE

Low estimates show that by 2014 over 150 million mobile devices will be NFC capable. NFC is just one of the trends that could shake up many sectors creating numerous avenues for connecting and enriching customer

relationships. Harnessing the potential of such innovations is now part and parcel of the role of brand owners and being amongst the first to identify the human potential of this technology offers huge rewards.

6.1 Future NFC Uses at Home

Currently, NFC technology has the capability to open the front door of a home simply by using the mobile phone of the homeowner. If somebody is walking up to their front door with their hands full, they could simply use their cell phone to scan the front door lock to open the door. This NFC door technology may soon be produced for the mass consumer market. NFC also has several potential uses in the kitchen beginning with the smart fridge. A refrigerator with NFC technology could make keeping track of food and drink inventories much easier for the user. A smart fridge could keep track of every item within the fridge, letting the user know when things run out or when food expires. Already, LG and Samsung have developed a refrigerator with an HD screen and Wi-Fi capabilities. NFC technology could be made compatible to those systems in the future. If user's become comfortable using NFC with their mobile payments on their phones, they would most likely be comfortable with using NFC in their homes.

6.2 Future NFC Uses in Healthcare

As **NFC** is finding its way in to almost every industry, healthcare seems to be equally competitive with huge prospects for his growing technology. NFC enabled mobile device could help the visually impaired find objects and navigate through areas conveniently. French supermarket chain, Casino is doing a pilot test on blind shoppers to understand the potential of NFC in shopping experience.

Past reports have shown that around 1% of deaths occur due to adverse drug events. If NFC could be used to maintain a database of drug compositions and doctors could access that database along with the patients past medications and allergies such accidents could be avoided [10].

Post surgery monitoring comprises a huge percentage of a total healthcare costs for a patient today. Gentag is planning to develop a low cost wireless monitoring kit which would help patients monitor their self-recovery allowing an early discharge from Hospitals and reduction in healthcare costs drastically. The kit would facilitate post surgery testing in the operated area and avoid complication by early diagnosis of any recurrence of symptoms.

6.3 NFC Enabled Advertising

NFC-enabled interactive posters could trigger content in an NFC enabled mobile app when in the vicinity.

VII CONCLUSION

Mobile handsets are the primary target for NFC and soon NFC will be implemented in most handheld devices. Even though NFC have the shortest range among radio frequency technologies but it is revolutionary due to it's security, compatibility, user friendly interface, immense applications etc

The many benefits and potential uses of NFC technology will continue to drive the technology and push innovation in the field. The keys to future success are evident in the intrinsic values provided by NFC. It is a more secure technology than RFID and Bluetooth due to its frequency and short distance specifications. Though the implementation of NFC is still in its infancy, it is evident that the future will see a proliferation in its use.

Companies will benefit from the financial success of their innovations, consumers will benefit from increased productivity, and the economy will benefit from new product growth and increased competition.

REFERENCES

[1] Ortiz, C. Enrique (2006-06). "*An Introduction to Near-Field Communication and the Contactless Communication API*". Retrieved 2008-10-24.

[2] Kasper, Timo; Dario Carluccio, Christof Paar (May 2007). "*An embedded system for practical security analysis of contactless smartcards"(*PDF). Springer LNCS (Workshop in Information Security Theory and Practices 2007, Heraklion, Crete, Greece) 4462: 150–60.

[3] Chris Foresman, "*Near Field Communications: a technology primer,"* Ars Technica (February 2011)

[4] B. Joan, (n.d.). "*Difference Between RFID and NFC,"* Difference Between. Retrieved September 26, 2011

[5] Harley Geiger, Center for Democracy and Trust, NFC Phones Raise Opportunities, Privacy And Security Issues (April 2011)

[6] 1MA182: Near Field Communication (NFC) Technology and Measurements

[7] Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)

[8] Collin Mulliner from - "*Attacking NFC Mobile Phones," 2008 and "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones*," International Conference on Availability, Reliability and Security, IEEE Computer Society, 2009.

[9] Christian Kantner, Josef Langer, Gerald Madlmayr, Josef Scharinger, *"NFC Devices: Security and Privacy,"* The Third International Conference on Availability, Reliability and Security, IEEE Computer Society, 2008

[10] R. Noor. 7 ways Near Field Communication (NFC) will revolutionize our lives.

[11] J. Titlow, "*The Future of NFC, From Mobile Wallets to Angry Birds*," Read Write Web, June 14, 2011