I.J. Wireless and Microwave Technologies, **2014, 2, 20-30**
Published Online March 2014 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2014.02.03

Available online at ***http://www.mecs-press.net/ijwmt***

Near Field Communication

Nagashree R N[a*], Vibha Rao[b], Aswini N[c]

[a]*PG student in Digital Electronics & Communication, MVJCE, Bengaluru and 560067,India.*
[b]*PG student in Digital Electronics & Communication, MVJCE, Bengaluru and 560067,India.*
[c]*Assiscant Professor in Dept of Electronics & Communication, MVJCE, Bengaluru and 560067,India.*

Abstract

Near Field Communication (NFC), an emerging short-range wireless point to point interconnection technology, with the combination of handheld electronic device has become a potential tool for the two devices to exchange various information when in close range. NFC unites various standards and proprietary technologies. This paper presents a brief introduction about the NFC and various applications and security issues.

Index Terms: Near Field Communication, Data transfer, NFC data exchange format, Communication mode, Security, applications, Advantages, disadvantages.

1. Introduction

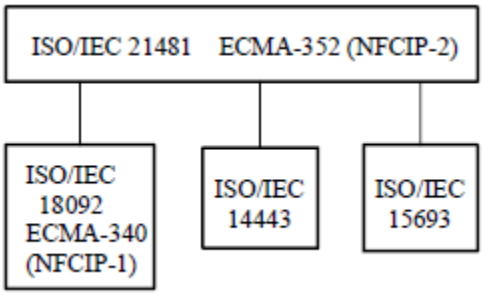
Near Field Communication (NFC), a new short-range (max. 20cm) wireless, contactless connectivity technology, evolved from a combination of earlier RFID style non-contact identification and interconnection technologies (ISO14443A/MIFARE/FeliCa). It provides a high level of comfort to user as it can communicate without any further configuration steps when two devices brought very close each other and to enjoy the privilege of accessing the content services in an intuitive way just by simply “touching” smart objects. NFC communicates based on inductive coupling. It is broadly compatible with the existing standards such as Bluetooth, Wi - Fi etc., that have been set in place. The major advantage of NFC compared to other wireless technology is its simplicity.

A potential application of NFC, contactless payment using NFC-enabled mobile phone enables secure and convenient purchases in a wide range of transactions. For example, a credit card could be integrated into a mobile phone and used over NFC. It finds a huge application in wireless sensor networks and various other fields.

* Nagashree R N. Mob.: 7259544509
E-mail address: nagashree.r.n@gmail.com

2. Features of the NFC Standard

The Near Field Communication system operating in the global 13.56MHz unlicensed radio frequency ISM band, standardized by ISO (18092), ECMA (340) and ETSI. Additionally NFC is compatible with Sony FeliCa smart card protocols and Philips' MIFARE® (ISO 14443 A).The NFC has two standards: NFCIP-1 is an NFC-specific communication mode, defined in the ECMA-340 standard. This mode is intended for peer-to-peer data communication between devices. The NFCIP-1 mode is divided into two variants: active mode and passivemode.NFCIP-2 (specified in ECMA-352) defines how to automatically select the correct operation mode when starting communications.



3. NFC Technology Data Transfer

The Near Field Communication system operating in the global 13.56MHz unlicensed radio frequency ISM band, standardized by ISO (18092), ECMA (340) and ETSI. The data transfer rate may be 106 or 212 or 424 kbps. The initial communication speed it set up by the application itself which might be later changed depending upon the communication environment and the requirements.

The NFC uses same channel to both transmit and receive, they are half duplex. They operate by using 'Listen before Talk' protocol to prevent two devices transmitting together, thus in turn avoiding the collision that would occur otherwise. In this protocol the device transmits only if they previously listen to check that no other devices are transmitting. Connection is established between two NFC enabled devices by bringing them in the close proximity of maximum of 20cm. The transmission range is so short, NFC-enabled transactions are inherently secure.

4. NFC Technology Device Types

The NFC near field communication standard defines two types of NFC device. The Initiator and Target, the initiator initiates the communication and it controls the data exchanges. Whereas the target device is the one that responds to the requests from the Initiator.

The NFC near field communication standard defines two different modes of operation:

4.1 Active mode of communication:

In this mode of communication, both the NFC enabled devices generates an RF signal on which the data is carried.

4.2 Passive mode of communication:

This is the mode of communication where only one NFC device generates an RF field. The second device is the passive device which acts as target and it uses a technique called load modulation to transfer the data back to the initiator. The passive devices do not require an internal power resource.

Generally, only two devices can communicate at the same time, but in passive communication mode the initiator is capable of communicating with several targets at the same time, which is realized by time slot method. The maximum number of time slots is limited to 16.

In addition to the NFC modes of operation, three communication modes are also defined:

- *Read / Write:*

In this mode of operation NFC allows applications to transfer data in an NDEF message format. But it should be noted that this mode is not secure. It is also necessary to note that this mode is supported the Contactless Communication API.

- *NFC card emulation:*

This NFC mode enables the NFC device to behave as a standard Smartcard. In this mode, data transfer is secure and the mode is also supported by the Contactless Communication API.

- *Peer to peer:*

A third mode within NFC is the peer to peer mode which supports device to communicate at the link-level. This mode of NFC communication is not supported by the Contactless Communication API.

5. Architecture

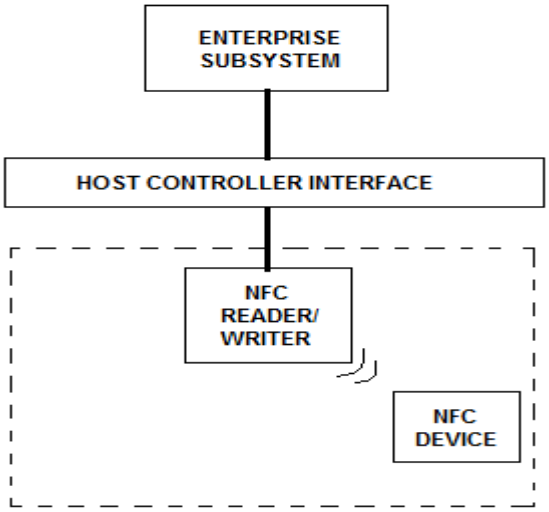


Fig 1. Architecture of Near Field Communication.

The above figure illustrates system architecture of a Near Field Communication system which has NFC system, a device that can be either active or a passive device. An active device communicates directly with each other, in an active communication mode, and/or with NFC tokens. An NFC device shall support the ISO14443 and ISO18092 standards. Here point to point communication takes place. In the above figure a NFC device, initiates the connection with the another NFC system (NFC reader/writer). This system is further connected to a Host Controller Interface (HCI), acts as an interface that enables communication between the

NFC system and Enterprise subsystem. Enterprise subsystem could be an access point, where NFC is used to pair two WLAN devices.

A NFC card mainly has two parts: a CPU and storage.CPU helps the NFC card to run some simple logic process program.

The storage can provide data storage and memory to the application. By combining these two parts make the NFC card to do all the applications of every kind of smart card. Therefore, NFC card can integrate all kinds of smart cards. Thus, just one NFC cards can helps in many applications.

In Near Field Communication, a NFC enabled device generates a low frequency radio-wave field in the13.56-MHz spectrum. When another NFC device comes within this field, magnetic inductive coupling transfers energy and data from one device to the other. A passive smart cart which has no internal power supply absorbs the energy from an active device when it gets close enough and once it gets powered up, the passive device communicates with the other device. An NFC device with an internal power supply is considered active. The ability to act as both passive and active devices makes NFC devices unique among contactless communications technologies. This enables NFC devices to function as either contactless cards or readers. Thus combination of the Near Field Communication technology and the Mobile Communication technology produce many convenient application modes, helping in the development of the smart technology.

6. NFC RF Signal Coding

The signaling format and modulation systems for NFC are chosen such that it consumes less power and ensures the reliable communications.NFC has two different coding formats on the RF signal to transfer data for both active and passive modes of operation. 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 with a level of 10% modulation is used.

Table 1. Data Rate coding type for Active and Passive Device

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

Modified Miller coding: The modified Miller code provides an efficient form of coding and it is characterized by the pauses occurring in the carrier at different positions of a period. A high or "1" is always encoded in the same way, but a low or "0" is encoded differently dependent upon what preceded it as shown below.

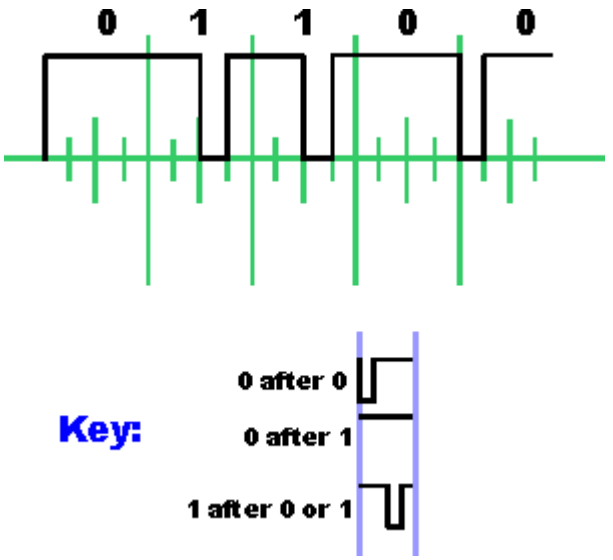


Fig 2. Modified Miller coding used for NFC.

Manchester coding: The Manchester coding utilizes the two different transitions that may occur at the midpoint of a period. Bit ’0’ is represented by a low-to-high transition, whereas bit ‘1’ is represented by a high-to-low transition. 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.

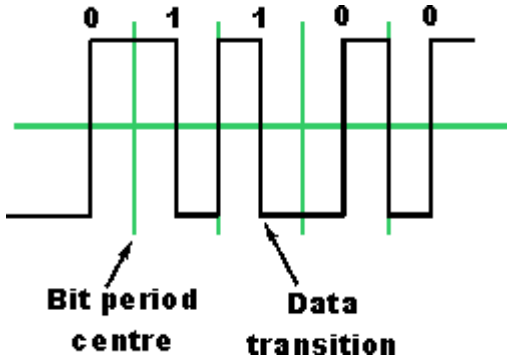


Fig 3. Manchester coding used for NFC

6.1 NFC data exchange format basics

The concept of the NFC NDEF is to be able to send data of any format over the interface while still being able to retain the air interface data format.

An NDEF message contains one or more NDEF records and the number of records that can be encapsulated into an NFC NDEF message depends upon the tag type that is being used and application.

In order for the system to know the begin and the end of the message frame, the first record in a message is marked with the Message Begin (MB) flag set and the last record in the message is marked with the Message

End (ME) flag set. The minimum message length is one record which achieved by setting both the MB and the ME flag in the same record.NFC NDEF records do not incorporate an index number directly but the index number within the message is implicitly assigned by the order in which the records occur.

The NFC Data Exchange Format (NDEF) is a specification that is used to define a message encapsulation format for the exchange of data information over an NFC link –i.e., between and two NFC devices or an NFC device and a tag. The NFC data exchange format is a binary message format that can be used to encapsulate one or more application-defined payloads which may be of a variety of types and sizes. These are combined into a single message construct. Each payload is described by a type, a length, and an optional identifier.

Each record of NFC NDEF consists of two parts:

- *Header:* The header for the NDEF exchange includes indicator for a number of elements:

a) Payload identification: It is optional field that allows the applications to identify the payload carried within an NDEF record.

b) Payload length: The payload length field is minimum of one octet long for short records but for normal records it is four octets long. The Short records are indicated by setting a value of flag bit known as the short record (SR) flag 1. Otherwise it is 0, for valid payload length.

c) Payload type: The payload type of a record indicates the kind of data being transmitted in the payload of that record. This may be used to guide the processing of the payload at the discretion of the user application. The format of the Payload Type field value is indicated using the Type Name Format field (TNF).

d) Payload: The payload can be of one of a variety of different types: URL, MIME media, or NFC specific data type. For NFC-specific data types the payload contents must be defined in an NFC Record Type Definition file, RTD.

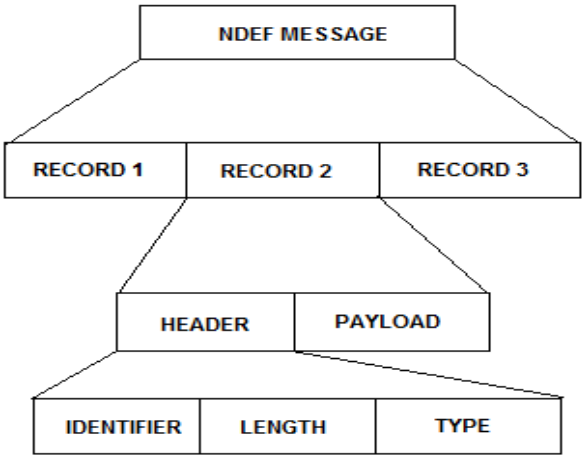


Fig 4. NFC data exchange format (NDEF) message structure

7. NFC Integrity and Security

NFC security is one of the major concerns especially with the applications for NFC being to enable contactless payments. Therefore it is essential that the basic NFC security measures to be built into the structure of NFC technology. By ensuring that the basic NFC structure is able to accommodate security measures, then the overall NFC security system is less likely to be vulnerable.

The passive attack occurs when someone eavesdrops on network traffic and as the NFC uses radio waves to communicate; it is possible for unwanted users to pick up the signals. The Passive attacks are by their very nature difficult to detect. Passive attacks on wireless networks are extremely common, almost to the point of being ubiquitous. Although the range of NFC is limited to a few centimeters, it is still possible for the attacker to retrieve usable signals up to distances, often up to 1 meter away for passive signals, and for active mode distances of up to 10 meters may be at risk. So the only real solution to prevent eavesdropping is to use a secure channel.

Once an attacker has gained sufficient information from the passive attack, the hacker can then launch an active attack against the network. 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. It is possible for NFC devices to detect this form of NFC security attack. By listening when data is transmitted they will be able to detect any attack of this form because the power required to successfully attack a system is significantly higher than that which can be detected by the NFC device transmitting the data.

The attacker might also aim to modify the data in some way. This form of attack is possible for some bits under different coding schemes. There are a number of ways to provide protection against this form of security attack. It is impossible for an attacker to modify all the data transmitted at the 106 Baud data rate in active mode. However, the best option is to use a secure channel as this provides the greatest level of NFC security.

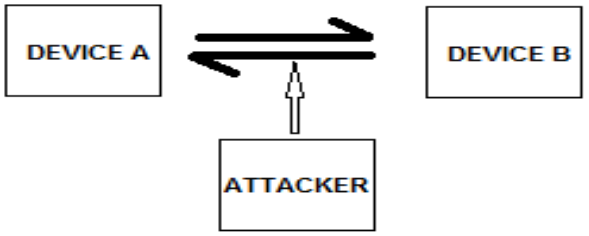


Fig 5. Attacker Aiming to Modify the Data

Man-in-the-middle attack is another form of NFC security issue that involves two party communications being intercepted by a third party. The third party uses information received and modifying it if required to enable to achieve their aims. This must obviously be achieved without the two original parties knowing that there is an interceptor between them. But practically it is not possible to do a Man-in-the-Middle-Attack on an NFC link. Anyhow it is recommended to use active-passive communication mode such that the RF field is continuously generated by one of the valid parties. Also, the active party should continuously listen to the RF filed while sending data to be able to detect any disturbances caused by a potential attacker.

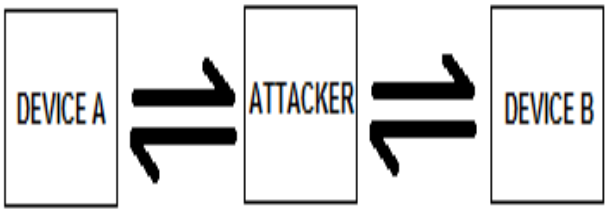


Fig 6. NFC data exchange format (NDEF) message structure

7.1 NFC secure channel

The best approach to ensuring NFC security is to use an NFC secure channel. This will protect against eavesdropping and data modification attacks. The standard key agreement protocols such as Diffe- Hellman can be used as it provides inherent protection has against man in the middle attacks and this protocol can be used in the standard non-authenticated version. The NFC secure channel also provides confidentiality, integrity and authenticity of the data transferred between devices.

8. NFC Application

Near Field Communication lends itself to a whole variety of applications, some of them are as,

8.1 Contactless Token

NFC finds contactless application in many ways which includes

- *Contactless identification* and other authentication
- *Contactless payment* which includes wide range of transactions including making service payments, downloading a movie trailer in a DVD shop, shopping from a TV at home, event ticketing from smart poster, merchandise.
- *Contactless browsing,* mainly used to municipal services, advertising and security verification. We can use SP with NFC card to get the weather forecast traffic information and other services when we move the SP over the terminal equipment provided by government.
- *Contactless connection,* it is mainly about that smart phone with NFC card can do Point-to-Point data transmission. Two SP owners can play game in a local wireless network which is near field communication technology.
- *Contactless downloads;* this includes general downloading data which provides a convenient way to get a new application based on NFC.

8.2 Medical Applications with Wireless Sensor

NFC being a high-potential technology for short-range can be applied to health monitoring systems; this is very significant, especially in long-term health monitoring and in chronic disease management by providing connectivity between health monitoring device and mobile terminals.

8.3 Security Applications

Using NFC enabled smart phones it also possible to unlock the doors of residents and hotel rooms. Therefore in future it also be enhanced for vehicle security and vehicle parking applications.

9. Comparisons of NFC and Other Wireless Technologies

NFC is a technology that is distinct from other wireless technologies, not only in the technology used, but also the applications envisaged.

9.1 Bluetooth

Although both Bluetooth and NFC can be used to transfer data, Bluetooth has been designed to transfer data over much greater distances. NFC is designed to be close proximity only. From the techno-economic viewpoint,

the advantages of NFC over alternative wireless communication technologies such as Bluetooth and IrDA are its lower price, lower power consumption and better immunity to eavesdropping. And the principal difference is the NFC uses magnetic coupling to exchange the information.

9.2 Wi-Fi / IEEE 802.11

Wi-Fi is designed for local area networks, and is not a short range peer to peer technology. Thus, NFC has a shorter transmission range and a slower data rate distinguishes it from Wi-Fi. Like Bluetooth, the principal difference between Wi–Fi and NFC is the use of magnetic coupling to exchange the information.

9.3 RFID

Although RFID is very similar to NFC in many respects, RFID is a much broader technology. NFC is a specific case which is defined by standards enabling it to be interoperable RFID and NFC are basically using the same working standards, but as the NFC standard restrict the range with use of magnetic field induction. In addition to contact less smart cards (ISO14443 [6]), which only support communication between powered devices and passive tags, NFC also provides peer - to - peer communication. NFC combines the feature to read out and emulate RFID tags and to share data between electronic devices that both have active power. A shorter transmission range and slower data rates distinguish NFC from other short-range wireless technologies such as Bluetooth, radiofrequency identification (RFID), and Wi-Fi.

10. Advantages and Disadvantages

10.1 Advantages

- *Ease of Use:*

The near field communication by it contactless payment system creates the ease of use as there is no need to carry multiple credit cards. And by loading the credit cards to phone eliminates the need of carrying each different card in the wallet.

While one can't password protect the wallet, but can password protect the smart phone. Also to access any credit card one must need PIN. Retailers no longer have physical access to the credit card information.

- *Versatility:*

NFC is adaptable for all kinds of situations like bank cards, movie passes/ tickets, bus passes etc. Therefore NFC is suited for a broad range.

- *Security:*

Near field communication users enjoys a secure communication as it transfers data over secure channels with the encryption of information.

And some of the other privilege that users enjoys are NFC allows the individuals to share the data cost-efficiently as it has the ability to transfer the files like picture or music without the carrier charges.

The close range of NFC overcomes the risk of interference when in crowded locations, which helps in smooth data sharing between the devices.

NFC consumes less power compared to Bluetooth and it does not require the setup and connection establishment with other device.

10.2 Disadvantages

- *Compatibility:*

As NFC is relatively new technology, compatibility is the main challenge it is facing because device compatibility is a key aspect to expanding its consumer base.

- *Costly:*

NFC is an expensive technology and many companies do not have the motivation to adopt this technology into the workplace as the technology they currently use may be all they need to perform efficiently. Transferring employees over to NFC compatible devices may not align with the goals of the organization.

- *Security:*

Another major risk is hacking. As mobile phone is being more developed, much like hand held computers they become more prone to viruses.

11. Conclusion

The NFC being most prominent technology for contactless system seems to be fulfilling the growing demands of mobile contact less communication. This paper discusses the concept of Near Field Communication along with its modes of communication, here we also discuss about security and integrity in which we have a list of threats has been derived and addressed. NFC by itself cannot provide protection against eavesdropping or data modifications. The only solution to achieve this is to use the secured channel over NFC. The paper also gives the comparison of NFC with other existing popular technologies. The approach of NFC can become more popular with more and more motivation and encouragement. Then the NFC technology will become important feature for mobile.

References

[1] JuergenSieck, VolodymyrBrovkov, “Near Field Communication -Research, Teachings and Training”, 2012 14th International Conference on Modelling and Simulation.
[2] ECMA, “Near Field Communication Whitepaper”, ECMA International, 2004
[3] JormaYlinen, MikkoKoskela, LariIso-Anttila and PekkaLoula, “Near Field Communication Network Services”, 2009 Third International Conference on Digital Society.
[4] Roy Want, “Near Field Communication”, PERVASIVE computing, July–September 2011.
[5] Texas Instruments “Near Field Communication”, 2013.

Authors Profile

Nagashree R N, Final Year Mtech in Digital Electronics and Enginnering at MVJ College of Engineering. Bachelor of degree was awarded in the field of Telecommunication Engineering in the year 2011 at GSSS Institute of Engineering and Technology for Women. Have teaching experience of 1 year.

Vibha Rao, Final Year Mtech in Digital Electronics and Enginnering at MVJ College of Engineering. Bachelor of degree was awarded in the field of Telecommunication Engineering in the year 2011 at GSSS Institute of Engineering and Technology for Women.

Aswini N, presently works as Assistant professor in Dept. of E&C at MVJ College of Engineering, Bangalore. She pursued her Bachelors in Applied Electronics & Instrumentation from College of Engineering, Thiruvananthapuram in 2002 and Masters in VLSI Design and Embedded systems from VTU in 2011.She has 6 years of teaching experience and her areas of interest are in Multi-core processor architectures and VLSI Design.

How to cite this paper: Nagashree R N, Vibha Rao, Aswini N,"Near Field Communication", IJWMT, vol.4, no.2, pp.20-30, 2014.DOI: 10.5815/ijwmt.2014.02.03