Mnfc-Operation Modes and Risks

Gowtham Mamidisetti, P. N. S. L. Sravani, P. Anusha

Abstract— This paper explains about MNFC(Mobile Near Field Communication) .Near Field Communication (NFC) is wireless communication technology to communicate with other NFC enabled devices . NFC builds upon Radio-Frequency Identification (RFID). In smart phones NFC created sensational things such as less time complexity for connection between the NFC enabled devices and data transfer rate is so high. The main advantage of this technology is, NFC enabled devices can work even when the devices is in switch off mode. This paper mainly focuses on different modes of operation of MNFC and their risks.

Index Terms- MNFC (Mobile Near Field Communication), NFC (Near Field Communication), RFID (Radio-Frequency Identification).

I. INTRODUCTION

MNFC is a wireless technology with NFC, we can establish connection between two Mobiles without using physical medium.NFC supports peer to peer communication and enables consumer access to aggre-gated services, anytime, anywhere, with any type consumer stationary and mobile devices.

Near Field communication technology is just like Bluetooth technology and it works more efficient than Bluetooth. It can be operated in the range of 10cm. NFC created a revolution in second generation proximity. With NFC data sharing can be done at data exchange rate 422Kb/s. NFC is designed for short distance communication, it is complementary to Bluetooth and 802.11 with their long distance capabilities. It is easy and simple connection method, no complexity in connecting devices.

Manuscript Received November, 2013.

Gowtham.Mamidisetti is an assistant Professor in Information Technology at Shri Vishnu Engineering College for Women, Bhimavaram, West Godavari Dist, and Andhra Pradesh, India.

P.N.S.L. Sravani is studying IV Btech information technology in shri Vishnu engineering college for women, Bhimavaram, West Godavari Dist, Andhra Pradesh ,India.

P.Anusha is studying IV Btech information technology in shri Vishnu engineering college for women, Bhimavaram, West Godavari Dist, and Andhra Pradesh, India.

NFC enabled devices can operate in two modes as active mode and passive mode. Passive mode is responsible for achieving significant power savings and extending the precious battery time. Devices operating in active mode can pro-vide all the power needed for communication with passive devices through their internally generated RF field. In this manner the contactless smart card are powered and ensures that data remains accessible even the NFC enabled device is switched off. NFC based communication between two devices is possible when one device acts as reader or initiator and another device as target or tag. Initiator is the one as its name specifies initiates the connection between the devices by generating RF signals. And coming to the target, it responds to the signal generated by the initiator.

INITIATOR—Initiator is an active device, which generates the radio signals to communicate with the tags/target. This is also known as Reader

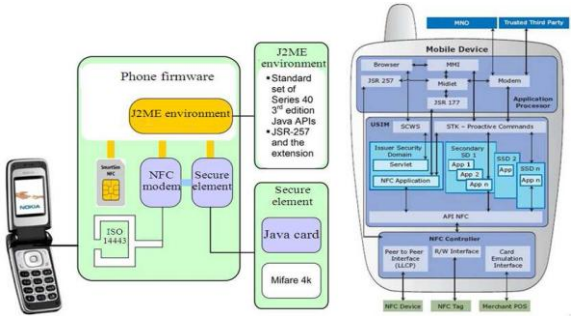
TAG—Tag is a thin device just like memory chip, it contains an antenna and small amount of memory.

COMPARISON WITH OTHER TECHNOLOGIES

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

Compared to other short-range communication technologies, which have been integrated into mobile phones, NFC simplifies the way consumer devices interact with one another and obtains faster connections. The main advantage over Blue-tooth is the shorter setup time, in less span of time NFC enabled device will connect with other, just with one touch the connection can be established. No need to search for the devices to connect with them, the connection between two NFC devices is established at once in between 0 to 1 second.

II. ARCHITECTURE OF NFC TECHNOLOGY IN A MOBILE DEVICE



a) Architecture of NFC technology in a mobile device defined by NFCF in 2011 and

(b) NFC integrated inGSMA (2011)

III. MNFC OPERATING MODES

In the context of use with mobile devices, NFC has three principal modes of operation.

1. Discovery mode
2. Transactions Mode
3. Sharing Mode

1. Discovery mode

This mode is also called as Reader writer mode. In this mode the NFC enabled devices can read and write data to the other tags. In this case both the reader/writer and the tags/target should be in NFC data format. This mode enables mobile devices to read data stored in passive RFID tags embedded in public posters, displays, and products — and to act upon that data that contains a Uniform Resource Locator (URL), which is an Internet encoding of access instructions for a file or Web address, or instruction for making a call, or the SMS instruction for sending a text message. This NFC mode also enables mobile devices to write data to some tags – notably virtual tags in other devices.

NFC requires two devices to communicate; one is NFC R/W in the format of the NFC data-exchange format (NDEF) and NFC Record-Type Definition (RTD) and the other an NFC tag. These two specifications will standardize how NFC devices operate in the R/W mode. A NFC-enabled device can access data from a RFID-enabled object, such as a "smart poster" with an embedded RFID tag that allows users to download a URL for a movie trailer.NFC tags are passive devices that can be used to communicate with active NFC devices (an active NFCR/W). Message coding format used by NFC reference applications is transmitted by NDEF. It is allows multiple NDEF messages and allows messages to be divided into chunks such as phases, stages, activities, tasks and steps.

Key risks

RISK 1: NFC tags can be susceptible to tampering. Smart posters are located in public places, where such malicious threats are possible. The tag itself is passive and can be rewritten or superimposed with different data. A poster containing malicious information could direct user to a false Web service or website and, instead of transferring the voucher to the mobile device, could misguide user to perform other, unwanted purposes. Alternatively, the repurposed tag data could include a malicious URL to instruct her mobile phone to make a mobile call or send a text message to a premium service resulting in unwanted mobile billing charges.

RISK 2: user may not have received a full understanding of what, how, why and by whom users personal information is being collected, processed, transferred or stored and how user could find out about it. If this notification were not provided, then user's actions could be lacking proper informed consent. This risk is one of most common privacy risks to consumers. Consumers can easily be subtly encouraged to act on consumer cues, without taking proper steps to understand the potential impact of their actions.

RISK 3: As with any consumer online activity, there are risks that a malicious party may use social engineering to gather user's personal information without her consent. In this case, the risk is that the service initiated with the smart poster tag could have secondary, hidden purposes to which user has not given consent. Such threats could undermine consumer trust in a digital marketplace.

RISK 4: user may have unknowingly leaned up against the smart poster with her smartphone in her hand, while talking on the phone or idly standing by. If NFC-capability in her phone is active at the same time, user may inadvertently activate the interaction contained in the smart poster passive tag.

2. Transactions Mode

This mode is also called as card emulation mode. This NFC mode enables mobile device owners to make a contactless business transaction, in the same way smart cards are used today. This mode of operation enables mobile devices to be used for identification, payment and access control applications.

NFC devices can also act as smartcard (ISO 14443) and contain a secure smartcard chip also referred as a Secure Element (SE) that operates in card emulation mode. The secure element is connected to the NFC controller for proximity transactions (contactless payments).Host controller is able to exchange data with the secure element. A NFC-enabled device emulates a contactless payment card and can be used to purchase goods and services. In this mode, the device is passive so it does not generate a RF field.

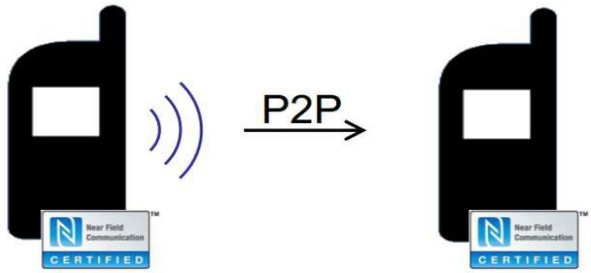
Key RISKS

RISK 1: Even with the close proximity of devices, eavesdropping security risk is possible, without detection by the legitimate owners of the devices.

RISK 2: The game store loyalty program could be used to profile user's purchasing habits, deploy that profile information for targeted advertising and shared with third-parties, without user's knowledge and consent.

RISK 3: The game store loyalty program could be the target of a data breach which could cause user to be the victim of identity theft.

3. Sharing Mode



This mode is also called as peer to peer mode. This NFC mode enables mobile devices to more easily interact with each other (i.e., each phone has to be equipped with NFC and the enabling applications) to quickly launch a mobile communications bearer for sharing data with each other, whether to exchange business cards, photos, documents or other type of personal information in "peer-to-peer" data transfers.

In this mode, two devices communicate with each other and exchange data, such as passing contact information or an electronic business card from one device to another, for example, between a NFC enabled mobile phone and a NFC-enabled PC. There are three specifications in P2P mode in order to determine the operating range of devices and testing the physical layer. Analogue Specifications defines the radio frequency characteristics of an NFC Forum device . Digital protocol specification defines the building blocks for communication. NFC Activities Specification defines the activities required to set up communication in an interoperable manner, based on the building blocks of the digital protocol specification, e.g., polling cycles, when to perform collision detection.

Key Risks

RISK 1: With the close proximity of devices, eavesdropping, while difficult, is not impossible, without being detected by the legitimate owner of the devices.

RISK 2: Sender shares malicious content instead of innocent content promised to receiver.

RISK 3: As with all sharing of any content, sender does not have any control over subsequent sharing of their content by receiver.

RISK 4: User may not be aware of which mobile application is the default handler for received content shared over a communication carrier initiated by an NFC-sharing interaction. This could lead to unforeseen storage or processing of the content.

IV. EXAMPLE SCENARIOS

1.Discovery mode

Scenario - PUBLIC POSTERS

We are now introducing the latest advancement of mobile technology by implementing the NFC (Near Field Communication) technology in the public theaters so that it will be easier to select the film of you like and can enjoy it by just tapping on The NFC (near field communication) tag. For this we just use the smart poster as the medium and improve it by advancing the implementation and name it as "NFC poster". In this NFC poster we would like to implement 3 tags behind the posters of a film .It is introduced at theaters and at public places. Now it is easier for an individual to carry his/her mo-bile and use it as a wallet. If he just sees the poster, let us sup-pose that he went to a multiplex theater and if he is not able to choose the film which he wants to go then our product comes into act, and here as said earlier we would like to implement 3 tags. First, it will be coded in such a way that if any one taps on it then the tag will send the link of the trailer of the movies and the person will be provided with a facility of watching the trailer, after that if the person likes the trailer and wishes to watch the film then he has to tap on the second tag. The second tag will be coded in such a way that he will be provided the website for booking the ticket of the film present in the poster. This implementation will reduce the human effort a lot, instead of standing in a queue for buying tickets without opening the system and waiting for the browser's response. He will just tap on it and will be

allowed to book the ticket within seconds. And the final tag is used by any individual after watching the film. If the person watches the film and if he likes it then he will provide the rating of the film by just taping on that tag. It can be easily implemented on the poster so that it will be user friendly. So here I like the advantage of the NFC tags in the public point of view. First is, NFC tag will attract the customers, making their payments as the mobile payments and the rating loyalty for the above NFC poster.

2.Transactions mode

Scenario- Ticketing / Micro Payment

In this example application, the NFC interface is used to transfer some valuable information. The ticket or the micro payment data is stored in a secure device. This could be a contactless Smart Card, but could as well be a mobile phone. When the user wants to perform a payment or use the stored ticket, the user presents the device to a reader, which checks the received information and processes the payment or accepts/rejects the ticket.

In this application example the user device must be able to perform a certain protocol with the reader. A simple read operation will not be sufficient in most cases. Also,
the user device is likely to have a second interface which is used to load money or to buy tickets. This second interface can for example be linked to the mobile phone CPU.
The ticket data could then be loaded into the mobile phone via the cellular network. In this application sometimes the term ’Secure NFC’ is used. However, this does not at all mean that the NFC link is somehow secured. In fact the name is rather misleading. The name just denotes a configuration using an NFC hardware chip in combination with a Smart Card chip. It should be called ’Secure Smart Card and NFC’, but unfortunately the shorter name is used quite often.

3.Sharing Mode

Scenario-Device pairing

In this application the two devices communicating would belong to the same group of devices. An example could be a laptop and a digital camera. The user wants to establish a Bluetooth connection between the two devices to exchange image data. The Bluetooth link is established by bringing the two devices close together and running a given protocol over NFC between the two devices. This makes it obvious for the user which two devices get actually linked and takes away the burden of navigating through menus and selecting the right devices from lists of possible communication partners.It should be noted that the NFC connection itself in this example is only used to establish the Bluetooth link. Image data is not transferred over NFC because NFC’s bandwidth is simply too small for transferring big amounts of data.

V.CONCLUSION

In this real world, technology plays a vital role as it reduces the human efforts. MNFC is one of such technologies which makes the life easier by just tapping through the NFC de-vices within short range. This type of technologies helps every-one by attracting customers in an interactive manner, mobile payments and rewarding loyalty. The implementation of NFC poster provides user with wide range of facilities like downloading teasers, reviews and movie ticket bookings and liking your favorite page in the social networking sites.

The design and deployment of NFC technology offers new conveniences and benefits to users, and represents several advances if all risks discussed in the paper are resolved.

REFERENCES

1. NFC Forum: www.nfc-forum.org.
2. NFC World: www.nfcworld.com.
3. Dr.Francesco Prato, Near Field Communication (NFC) Marketing Introduction by PHILIPS, Business Development Manager – NFC, Marketing and Sales.
4. Ben Dodson Hristo Bojinov Monica S. Lam, Touch and Run with Near Field Communication (NFC).
5. B. Joan, “Difference Between RFID and NFC,” Difference Between. Retrieved September 26, 2011, at
6. Harley Geiger, Center for Democracy and Trust, NFC Phones Raise Opportunities, Privacy And Security Issues (April 2011), at: www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues Collin Mulliner,
7. Kevin Curran, Amanda Millar, Conor Mc Garvey, Near Field Communication, International Journal of Electrical and Computer Engi-neering (IJECE) Vol.2, No.3, June 2012.
8. 8.G. Broll, S. Siorpaes, E. Rukzio, M. Paolucci, J. Hamard, M. Wagne and A. Schmidt. Supporting mobile service usage through physical mobile interaction. In In Proceedings of PerCom 2007, White Plains, pages 262–271. IEEE Computer Society, 2007.

AUTHOR PROFILE

GOWTHAM.MAMIDISETTI is an assistant Professor in Information Technology at Shri Vishnu Engineering College for Women, Bhimavaram, West Godavari Dist, Andhra Pradesh, India.

P.ANUSHA is studying IV Btech Information Technology in shri Vishnu engineering college for women, Bhimavaram, West Godavari Dist, Andhra Pradesh, India.

P.N.S.L. SRAVANI is studying IV Btech Information Technology in shri Vishnu engineering college for women, Bhimavaram, West Godavari Dist, Andhra Pradesh ,India.