ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Near Field Communication for Data Exchange

Reena Hooda
Assistant Professor, Department of Computer Science & Applications,
Indira Gandhi University Meerpur (Rewari), Haryana, India

*Abstract:*Demonetization has hastened the usage of plastic money in India in place of the paper money. One step further, with the growing population of smart phones in India, people are demanding to pay anywhere at any time.However setting up connection to the internet and sharing data is a lengthy process that is time consuming and above, connectivity is not essentially available all the time. NFC enabled devices automatically fire a command to target even to a passive device and can collect the data. Comparableto Bluetooth devices, NFC enabled devices can be tapped to each other to share information without the requirements of scanning & pairing the devices, all is done by NFC in s secure adhoc fashion. Only constraintis that the two devices must be local and data must be small. So, present paper highlighted the practicality of NFC for local communicationsand secure data exchange.

Keywords: Bluetooth, Standard, Security, Target, RFID.

1. INTRODUCTION TO NEAR FIELD COMMUNICATION

Near Field Communication (NFC) is a wireless technology developed for a local communication at small distance, created by Sony and Philips. NFC workslike a contactless smart card in which Peer to Peer network is established to exchange data and forms a PAN (Personal Area network) temporarily like adhoc network even slighter than Bluetooth. It is ECMA-340, ISO/IEC-18092 standard thatoffers a set of communication protocol allowing two devices eitherhandyor immobile passive terminal devices to communicate. Device can be a smart phone, tab and others to link over a small distance of few centimeters i.e. 4cmto 10cm at low speed connectivity.[1] One of a great facility provided through NFC is that if any of the communicating devices has the connectivity to the Internet other one can easily access the online services or information available. [1]A contactless communication is established between smart phones or tablets, contactless means just like phone contact list where you didn’t store the contact of a person, you meet him and talk to him or take his number when required without saving it, set a temporary connection and stop thereafter, similar way NFC works without any need to go through the multiple steps in setting up the connection. [2] One of the necessities of NFC is that both interactive devices must be local to share data as NFC entailsmoving or undulating the device on other. The NFC technology is now embedded in Apple’s iphone6, iphone6 plus, Apple Watch, Samsung S7edge. [5]

1.1. Applications of Near Field Communication

NFC offerssome great services; for instance, it can be used to take images with smart phone, opening the screen lock, application download &development and transferof file between devices, say mobile&computer system, entering in a parking garage, unlock car, etc. [3]simply by putting the devices together [2]. Smart phones can be waved over NFC compatible devices like tags or stickers etc. to take date information about schedules, delays, certain events advertisements, sharing games or purchasingand transferring funds without opening the wallet. NFC market is growing across the world; it is aswiftlymounting technology substituting credit cards. [3] NFC make availablevarious application software like games, photo editor, browser, accounting application, word processor, spread sheet, flight simulator or payments through NFC qualifiedgadgets. Also,NFC make it possible to share small information or data across the Systems or devices, information may contain small text files, images, clips etc. that can be accessed throughtapping the NFC enabled devices. [2]This contactlesspayment systemallows the mobile payments replacing the plastic money comprising credit /debit cards or smart cards. NFC enabled smart phones or devices can also initiate Bluetooth to perform tasks like controlling speakers, devices on office desktop or the household apparatus etc. Most striking fact is that NFC enabled devices can be represented as ids too. [2]

1.2. Historical Background

In 1903 the RFID patent was approved to Charles Walton. In December 2003, NFC was accepted as an ISO/ECC standard and ECMA standard (European Computer Manufacturing Association). In 2004, Philips, Sony and Nokia had developed NFC Forum. The primary specifications for NFC tag were given in 2006, and in 2009, NFC Forum released P2P standard to transfer contacts, URLs, initiate Bluetooth for certain tasks. In 2010 Samsung Nexus first Android NFC form launched and in 2012 NFC Smart tags were introduced by Sony Company for exchanging the different modes plus the outlines of smart phones of Sony within a closer specified range. In 2013 Visa and Samsung corporationsinitiated the development for mobile payments whereasIBM scientist formed a NFC based mobile authentications to control the frauds and enhancing the security. In November 2015, a partnership was announced by Swatch and Visa to permit NFC based financial transactions using Swatch Bellamy wristwatch, next to it Google launched Android Pay to compete Apple Pay. [2] [5]

2. FUNCTIONING OF NEAR FIELD COMMUNICATION

NFC devices canwork in an active mode, for example both devices are NFC enabled device, share data, such devices need more energy to operate so required an internal battery. [4] Devices can work in a contactless manner in the same way as smart card works. Therefore, one device must be passive like terminal to read and other card tapped to it, this time the terminal as a target must be NFC empowered to read the card or the tag. The target to which communication is required to get the data can be NFC device, empowered tags, stickers etc. and the information stored in the target/ tags can be personal data that can be the PINs or the passwords, contacts, or other card information. [4] [2] NFC worked in fashion including an initiator or the interrogator as a reader and a target as a responder for the informational. The initiator or the interrogator as an active device creates an RF filed i.e. electromagnetic energy to the passive target to empower it. Difference between active and passive tag is that active tag has a local power source such as battery whereas passive tag collects energy from neighboring RFID interrogator's radio waves those can penetrate the obstacles well.NFC device can read as well as write the data on Tag that needn't to be in the sight of the NFC device reader as communication is radio not the infrared. More technically, passive identifieris thetag thatwaits silently for a valid command and transmits information as a response to the command in a half-duplex mode because of passiveness whereas active reader or the interrogator works in a full-duplex mode. Tags normallyhaving storage capacity,are called memory between 96 to 4096 bytes. NFC Forum define 4 types of tags offering different communication speeds, configuration memory, security levels, writing facility or data holding[2].

NFC employs electromagnetic induction called Radio Frequency identification(RFID) between two loop antennas to share information within 13.56 MHZ unlicensed frequency ISM band (Industrial, Scientific, magnetic) of radio spectrum given from 3KHZ to 300 GHZ at ISO/IEC 18000-3 wireless communication having data rates between 106 and 424 kbps,reserved radio frequency excluding telecommunications. The international standard for passive RFID is anIEC 1800-3 that describe the parameters for wireless communication at 13.56 MHZ frequency meant for NFC. RFID is a method of automatic identification and data capture that apply electromagnetic fields to authenticate and trace the tags containing electronically stored information. Small RFID chips are like a rice grain embedded in the products or implanted under the skin of the animals for identification or spy. Micro chip is a set of integrated circuits using passive RFID called Passive Integrated Transponder (PIT) tag. RFID allows active devices to supply power and communicated to a passive electronic unpowered tag through radio waves. [2] The range of electromagnetic field (RF) is limited by range of ± 7 KHZ bandwidth at short distance of maximum 10 cm. The command is sent by the interrogator to tag/ target at a data rate is 423.75 kbps encoded using Phase Jitter Modulation (PJM). NFC employs 2 different coding methods to exchange data. If communicating device is in active mode that at a rate of 106 kbps, Millar coding with modulation at a rate of 100% is used, otherwise Manchester coding with 10%modulation is applied. Millar encoding or the delay encoding use half the bandwidth thanBiphasic encodes, modulated in the middle and is NRZ. Millar encoding transmissions are indicated by 180 ^{o} phase shift. Manchester encoding or the phase coding is a line code in which each data bit is either low than high or high than low so no problem of DC component.[2]

The various steps to use the NFC includethe launching of the NFC application on the phone as the first step. Then enter the password or finger print to unlock the NFC facility and tap the phone on the terminal (card reader), a connection is established by the NFC. The validation process includes a Secure Element (SE) that lies separately on chip in the phone or virtually on the cloud having complete independent authorization power therefore quite difficult to intercept. Further, SE is temper proof and secured by digital signature with well designed architecture to protect it from attacks. Once the validation process is completed, user can go for the transaction. [5]To read and write data on the tag NDEF format is used. NDEF stands for NFC data exchange format, a small binary format (bytes) used to encapsulate the text entered. A NDEF record contains MIME, typed text, URLs, Payloads andNdefMessage (byte[ ] data),constructed NDEF message by Parsing through binary data byte by byte. The basic validation requirement involvesNdefRecord() that is used to create a record having attributes named type, id and payload by following some predefined constraints like TNFEMPTY rule specify not to have type, id etc. whereas record having TNFUNKNOWN cannot have type. At minimal, one record must be available to validate the binary structure; the other validation rules may include the total length, flag etc. for the validation process [6]. A default generic package provided to the user is android.nfc.tech package that is a set of classesto help and support the user in write codes for the tags and to perform various read/ write operations on these tags. Another method is getTechList()used to definesupporting classtechnologies and offering access to the variety of the properties and input/output functions. [7]

2.1. Modes of data transmissions in Near Field Communication

NFC devices work in 3 modes, one is the reader's mode to send a command to target and read the information from it, making payments, smart money transfer and reading information from labels or smart posters, it is a one way communication where powered device (or powered terminal) read/ write to a passive NFC chip or target. In P2P adhoc mode, both devices can exchange the data in half duplex mode with slow communication, P2P makes both devices powered based on RFID [2] [4][5]. Both devices must be NFC chip embedded within and are capable to read or write data. Third is Use Card mode to communicate with higher technology like Bluetooth[4][5], having higher data rate than NFC [1].

2.2. Bluetooth vs. Near Field Communication

As compare to the Bluetooth, NFC takes less power. Secondly, to share information via Bluetooth, both devices must be paired after going through the process of scanning and permission. Further, in Bluetooth, both devices must be powered and Bluetooth enabled. Though Bluetooth can transfer a large amount of data as compare to NFC, NFC is most suitable for the small transaction, or one time communication even can work in a passive mode. Along with the data transfer, NFC provides many features like switch on the Wi-Fi, speakers, washing machine, reading information from passive labels, spy the objects without the requirement of manually paired. NFC enabled devices automatically pair by just tapping to another device.

2.3. Security in Near Field Communication

Like Bluetooth NFC devices forms a PAN provide a secure communication through cryptographic algorithms in adhoc manner. As NFC communication for data exchange is based on RFID, Felica, NDEF and ISO/IEC 1443 standard, the chances of fraud are very few due to implementation of cryptographic algorithms to encrypt the data through random key and jointly perform authentication.Felica is powered having inner battery to operate and ISO/IEC 1443 cards are contactless integrated circuit cards. NFC standards are given by GSMA group that comprises trusted service manager, single wire protocol, certification and SE as explored previously. GSMA(Global System for Mobile Communication) is an association with goal of scaling and increased interoperability for new mobile technologies covering roaming, interconnection, fraud and security, intellectual property and various other expert committees and groups. [2]From security point of view, for example transferring the funds, this NFC embedded on smart phones works well by applying passwords or finger print before proceeding for a transaction. It provides a better solution to mitigate the cards or the plastic money frauds, theft of wallet or ids. Many retailers like Target, Macys etc are NFC based contactless terminals for mobile payments. The structure of NFC is quite complex and difficult to hack thus prevent from invasion. [5] NFC are more secure than EMV or chip card payments because of the SE and requirements of tokenize card data, card information never stored directly on phone, so more secure. User can further protect their data by keeping antivirus software on smart phone or adding passwords. [3] NFC devices are full-duplex in an active mode however, NFC is not fully protected against spying and are vulnerable the threats of data alteration. SSL or different cryptographic methods can be applied to provide secure communication and data transformations to protect the this small range connectivity, however threats may arise for this local transformation of the data too as invader deliberately can still rob or modify the data even within this small range. The chances of theft are less with the passive devices as algorithms works actively on RF Field generated by active devices so requirement is to protect the active devices being scammed. Relay attacks or man in middle attack can be there in which communication between 2 parties are exchanged believing that they are directly communicating with each other. Fact is that entire communication is controlled by the attacker [2]. So embedding in smart phones or active devices can be layered against the attacks as now NFC can employ the smart applications to provide more security to data.

3. CONCLUSIONS

Like a smart card, NFC can be used as an identification proof and transfer funds plus many more facilities.However, NFC technology is not an alternate to the plastic money. You must have a smart phone having embedded NFC technology or other devicerequiring power for interaction in P2P mode to exchange the data. The advantage of NFC over plastic cards is that it doesn’t require any internet connection for authentication and information exchange. As compare to the Bluetooth, NFC works in an adhoc one time fashion, just waving over the target and communication automatically takes place albeit amount of data and data rates are too slow as compare to Bluetooth.Advantage over Bluetooth is data exchange based on RFID, SE, and NDEF, NFC provides a secure communication. By embedding in the smart phones, it can even be further protected with passwords while facilitating a wide range of applications as described in the paper. In short, communicating within a small distance for small data exchange, NFC powered us with atomicity in a robust manner and would be bone of future communication with availability of advanced versions of smart phones and information technologies.

REFERENCES

[1] Margaret Rouse( ).“Near Field Communication (NFC)”. Retrieved from:http://searchmobilecomputing.techtarget.com/definition/Near-Field-Communication

[2] Wikipedia, the free encyclopedia (2017).“Near field communication”. Retrieved from:https://en.wikipedia.org/wiki/Near_field_communication

[3] http://nearfieldcommunication.org/

[4] http://www.centrenational-rfid.com/how-nfc-works-article-133-gb-ruid-202.html

[5] Sharon Profis ( ). “Everything you need to know about NFC and mobile payments”.

[6] https://developer.android.com/guide/topics/connectivity/nfc/advanced-nfc.html

[7] https://developer.android.com/guide/topics/connectivity/nfc/hce.html