NEAR FIELD COMMUNICATION: AN OVERVIEW, SECURITY ISSUES & APPLICATIONS

DR. SANDEEP PONDE	DR. ARJITA JAIN	DR. MURLIDHAR DHANAWADE
Associate Professor,	Professor,	Professor,
NCRD's Sterling Institute of Management Studies, Nerul, Navi Mumbai.	NCRD's Sterling Institute of Management Studies, Nerul, Navi Mumbai.	NCRD's Sterling Institute of Management Studies, Nerul, Navi Mumbai.
sandeepponde@yahoomail.com	arjitajain@yahoo.com	dr.murlidhar.dhanawade@gmail.com

ABSTRACT:

Over the past century the communication & commerce industries and their underneath technologies have expand and changed most dramatically. One application of proximity mobile payment uses NFC technology. Near Filed Communication is commonly known as NFC. ***Near-field communication*** *(**NFC**) is a set of communication rules that allow two electronic devices, one of which is usually a portable device such as a Smartphone, to establish communication by bringing them close to each other. Bringing together the most recent technologies from both industries—mobile phones and e-commerce—results in a product that provides new facilities and the liberty to conduct commerce in manner that would otherwise not be possible. Near Field Communication (NFC) is one of the latest small range wireless communication technologies. NFC-empowered equipment can just be pointed or touched by the users of their devices to other NFC-empowered equipment to communicate with them. Near-Field Communication chips might replace every card in the wallet in future.*

This paper we discuss an overview of NFC System, security issues, tips for secure mobile NFC and the applications of NFC in various fields.

Keywords: *Near filed communication, Protocol, transactions, Mobile phone, wireless Communication.*

1. INTRODUCTION

Near Field Communication is undoubtedly an interesting technology that can open the way to new applications for the benefit of users and service providers. Mobile communication and computing technology has made astonishing advances since its inception in the 1980s. In reality

today mobile phone has more in common with an advanced computing platform than the simple telephone that we were using.

What Is NFC?

NFC is a latest technology developed over RFID. Near Field Communication (NFC) is a standards-based short-range wireless connectivity technology that makes life easier and more convenient for consumers around the world by making it simpler to make transactions, exchange digital content, and connect electronic devices with a touch. NFC is compatible with hundreds of millions of contactless cards and readers already deployed worldwide.

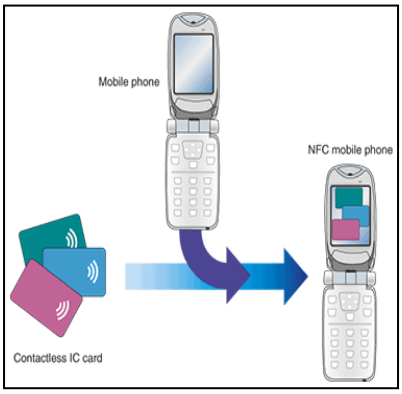

Fig.1: Concept of NFC phone

Near Field Communication technology (NFC) was *found* and *initiated* by Sony and Philips. NFC brings safe communication between electronic gadgets. Users can share business cards, make transactions, access information from a smart phone or provide credentials for access control systems with a simple touch.

NFC is an open platform technology standardized in ECMA and ISO/IEC. These standards specify the modulation schemes, coding, transfer speeds and frame format of the RF interface of NFC devices, as well as initialization schemes and conditions required for data collision control during initialization for both passive and active NFC mode. NFC works by utilizing magnetic coupling between devices Current and expected 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 develops upon RFID systems by allowing two-way communication between end points, where earlier systems such as contactless smart cards were one way only. Since unpowered NFC tags can also be read by NFC devices, it is also capable of replacing earlier one way applications. It provide seamless medium for the identification protocols that validate secure data transfer.

2. OBJECTIVE OF THE STUDY:

1. To Study the concept of Near Filed Communication technology.

2. To Study the security issues and tips for secure Near Filed Communication.

3. To Study the Applications of Near Filed Communication technology.

3. METHODOLOGY:

Writing method for this paper is qualitative. Reference sources used are different books, journals, and articles obtained from the library, as well as the resources from internet like e-book, e-journal and other supporting sites.

4. HISTORY AND BACKGROUND OF NFC

Radio Frequency Identification (RFID) is the base for Near Field Communication is a technology, An RFID system has two components, a target, which is the object to be identified, and a reader. The reader is device that power up and begin contact with a target. The reader and the target are the key components of every RFID system[2].

NFC was accredited with the standard ISO/IEC 18092 (NFC IP-1) which specifies the interface and set of regulations to be followed for simple wireless communications between devices kept near that does communication with transfer rates of 106, 212 and 424 kbps in December 2003. NFC also acquire a further internationally accredited standard ISO/IEC 21481 which meant in the future it will soon become a known technology all over the world and will have various applications in 2005. ISO standard conferred that, NFC is not encrypted which makes it compatible with previous RFID technologies.

Nokia, Philips and Sony in 2004 established the Near Field Communication (NFC) Forum with an intend to spread the knowledge about NFC technology among community and in 2006 they come up with initial specifications for NFC Tags. Nokia 6131 was the first NFC phone launch in 2006. In January 2009, NFC Forum released Peer- to- Peer standards to transfer contacts, initiate Bluetooth, etc. Samsung Nexus S: First android NFC phone shown in the year 2010Google Input –Output—HOW TO NFC demonstrates NFC to initiate a game and to share a contact, URL, app, video, etc in the year 201.NFC support becomes part of the Symbian mobile operating system with the release of Symbian Anna version in 2011.

In the year 2011 research in motion is the first company for its devices to be certified by Master Card Worldwide, the functionality of Pay Pass. Eat, a well known restaurant chain from UK and Everything Everywhere (Orange Mobile Network Operator) partner on the UK's first nationwide NFC enabled smart poster campaign in March 2012. A specially created mobile phone app is triggered when the NFC enabled mobile phone comes into contact with the smart poster. In 2012 Sony introduces the —Smart Tags, which use the NFC technology to change modes and profiles on a Sony smart phone at close range, included in the package of the Sony Xperia P Smartphone released the same year[4].

4.1. Modes of Operation in NFC:

NFC consist three operating modes: **Peer-to-Peer, Reader/Writer, and Card Emulation**.

- **Peer-to-Peer:** In this mode data transfer between two NFC enabled active devices. It is not often used because of strong competition given by other wireless technologies such as Bluetooth has more reach as compared to NFC.
- **Reader/writer:** Here data is copied is from NFC tag to cell phone or vice-versa. This is an innovative approach proposed by NFC and will become the user selling point of NFC in coming future.
- **Card-Emulation:** Here mode the data is copied from a NFC enabled mobile device to NFC Reader. The most significant feature of card emulation mode is exclusion of physical objects and proves the access control through respective user's smart phones. Thus the most used mode of NFC too.

5. SECURITY ISSUES IN MOBILE NFC:

The Near Field Communication technology (NFC) can be attacked by various ways. The various devices used for NFC communication can be manipulated physically. By the removal of a tag from the tagged article or wrapping them in metal foil in order to shield the RF signal. Another aspect is the breach of privacy. If proprietary information is stored on a tag it is vital to prevent from unauthorized read and writes access. Against an unauthorized write access read tags are safe. Attackers with the help of mobile readers and the appropriate software that enable unauthorized read and write access and reader distance is normal can attack the Rewritable tags.

Following are security issues in NFC:

1. Eavesdropping:

Eavesdropping is the number one threat to all NFC contactless payments. Here an attacker is able to use an antenna to receive the Radio Frequency signal for the wireless data transfer. Quality of the antenna and location (e.g. barriers like walls) are playing significant role in this type attack. The attacker has to be quite close in proximity, usually less than 10m for the attack to happen. However, a passive device is tough to eavesdrop as compared to an active device.

2. Data Corruption:

Data Corruption is the form of **Denial of Service (DoS) attack** where an attacker blocks the reception of the transmitted data, or disturbs the communication so that the receiver is not able to decode the data. The attacker does not need to decode the data transferred since the aim is to destroy the data transferred by intentionally transmitting radio signals to reduce the signals to random noises.

NFC device checks for Radio Frequency signal when sending data. The power to corrupt data is superior than sending the data, the sending device is able to detect the attack and stop the data transmission automatically.

3. Data Manipulation: Here an attacker intercepts and manipulates the data by modifying the binary value before sending the data back to the intended receiver.
Near Field Communication device is able to detect the increased in power that is required for the usual communication and stop the data transmission automatically.

4. Data Insertion:

Here before the answering device makes a reply an attacker inserts data into the communication channel. This takes effect only if the answering device takes a longer time to reply. If the inserted data and the data from the answering device overlap, the data will be corrupted.

5. Man-in-the-Middle-Attack:

Here an attacker acts as a middleman between two NFC devices hijacks the data without the knowledge of the two NFC devices. The attacker also reads and records or manipulates the data before sending it to the receiving device. Because of short range proximity and the detection capabilities of NFC devices, it is difficult for this attack to happen particularly when RF signals has to be aligned in an active-active communication mode.

5.1 **Tips to Secure Your Mobile NFC:**

Even though the short range communication of NFC has reduced the possibility of attacks, let's look at some tips to better secure the mobile NFC

- **Disable Mobile NFC Mode**: Disable mobile NFC service on your mobile whenever it is not in use, by doing this we can prevent any attacker from hitching your NFC signal. Always Keep the NFC service/port off, if the device is not using NFC facility.
- **Use Secure Sockets Layer (SSL) Application**: To ensure security in NFC transaction is to choose applications that use **Secure Sockets** channels i.e. Secure Sockets Layer (SSL) through the transmitted data are encrypted. It helps to defend against eavesdropping and data manipulation attacks. All the time use NFC enabled certified applications for smart phone and other devices related to payments or booking
- **Password Lock**: NFC enabled mobile device grant access to any finder to sign the phone over a card reader to make buy or transfer any delicate information. By enabling password lock on mobile device, one can it prevents the access to NFC if the device is hijacked.
- **Regular Updating the NFC Apps**: Ensure for updates from NFC device manufacturers regarding any software patches to be run. This will guarantee that NFC device being in use has right and upgraded software. Application developers and device manufacturer update their software time to time to incorporate security bugs.

6. USES AND APPLICATIONS OF NFC:

NFC technology supports the four main applications: "Sharing, Pairing, Transaction in addition to wireless charging and powering.

- **Sharing:** Sharing includes file web pages, videos and documents sharing. NFC's active communication mode permits data exchange via peer-to-peer mode communication.
- **Pairing: Pairing** is the second significant application for NFC technology. As mentioned before Bluetooth and Wi-Fi are ways of transferring information wirelessly between devices over greater distances than NFC.
- **Transaction:** Transaction is the most obvious application of the four, and a smart phone with an NFC chip could very easily be configured to work as a credit or debit card. NFC could work well for public transit passes, hotel room keycards, office building passcards and library cards.
- **Wireless charging and powering**: Wireless charging and powering is the fourth application of NFC technology. In passive communication, the magnetic field generated by the initiator device powers the target. This feature of the NFC may have big implications for application.

From above, we can sum up the main NFC applications in commerce, social networking, identity, gaming into are (Wayan, 2012; David *et al.*, 2012, Antti *et al.*, 2014)[1,4,10]:

- **Wireless payments**. The NFC devices can replace the traditional smart cards that have been used for many years in cashless payments. The little setup time for NFC devices grant mobile payments to be even smooth.
- **Smart magazines and posters / Advertising:** NFC devices can be used easily now to get more information about something in a magazine or on a poster on the street by tapping the page to get more information, or the URL to store the bookmark for later use.
- **Transit tickets**. NFC-enabled phones are simple and convenient when used in scenarios for mass transit. World Cup tickets have had embedded RFID tags since 2006.
- **Business-card exchange**. NFC devices are ideal for business-card exchanges because setup times for communication between NFC devices are very short.

- **Health Care:** FITBIT (a fitness monitoring company) has incorporated NFC for transferring details like calories burned, number of steps taken and other details from a wristband to the user's smart phone which houses a user-friendly application[7].
- **Automated Check-in system**: NFC-enabled smart phones can be used as a room key in hotels for the check-in and checkout process. Instead a person can directly enter their allotted rooms after making a booking and in return receiving a soft-key to their rooms[8].

7. CONCLUSION:

We are in this paper present and describe the Near Field Communication, Security issue & its applications. The Near Field Communication technology is based on existing RFID technology and standards. It uses magnetic field induction as a medium to establish communication between electronic devices placed closely and operating**.** It is an efficient technology for communications with short ranges Today, Near Field Communication by now begun to form the future of electronic gadgets in people's life. If the cost of chip manufacturing lower, the probability is that NFC-enabled mobile phones will become standard and their applications will become a part and parcel of life.

According to a survey[12] it is found that NFC technology was preferred by people over other technologies including Bluetooth Beacons and QR codes. NFC has also its own advantages and disadvantages. When it is compared to other technologies however presently it is not as much of popular but with the increasing android applications, shortly it will become a need. Here we are studied the security threats as well as Tips to Secure Mobile NFC.

The contactless payment standard is fully compatible with NFC. The Smart Poster concept, and peer-to-peer applications, where NFC serves as an easy to use way of opening a communication channel between devices that are physically close. In current world where digital transaction are so common it is a must application for smart phones and people need to be made aware about how it works.

REFERENCE

[1] Antti, K., Harri, K., & Eero, H. (2014). Combining the Dimensions of Written and Digital Media in a NFC-based Non-linear Adventure Game for Children, IFLA WLIC 2014 - Lyon - Libraries, Citizens, Societies: Confluence for Knowledge in Session 168 - Libraries for Children and Young Adults", In: *IFLA WLIC 2014*, 16-22 August 2014, Lyon, France.

[2] Bekir Bilginer, Paul-Luis Ljunggren "An introduction to Near Field Communication", March 201.

[3] Cameron Faulkner. "What is NFC? Everything you need to know". Techradar.com. Retrieved 30 November 2015.

[4] David, M., Joel, R., & Jaime, L. (2012). A Secure NFC Application for Credit Transfer among Mobile Phones. *Computer, Information and Telecommunication Systems (CITS) International Conference, Amman, 14-16 May 2012*, (pp. 1-5).

[5] Kevin Curran, Amanda Millar, Conor Mc Garvey, (2012) "Near Field Communication", International Journal of Electrical and Computer Engineering (IJECE), Vol.2, No.3, pp. 371-382.

[6] K.Preethi, Anjali Sinha, Nandini, (2012) "Contactless Communication through Near Field Communication", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 4, pp. 158-163.

[7] Kerem Ok, Vedat Coskun, Mehmet N. Aydin, and Busra Ozdenizci, (2010) "Current Benefits and Future Directions of NFC Services" in International Conference on Education and Management Technology (ICEMT), Cairo, Egypt, pp. 334-338.

[8] Trupti A.Bhosale and B.G.Hogade ,"Near Field Communication Technology", International Journal of Infinite Innovations in Technology, pp.3-6, vol. 1, issue 4 , ISSN:2278-9057.

[9] Wayan, S. (2012). Application of Near Field Communication Technology for Mobile Airline Ticketing. Journal of Computer Science, 8(8), 1235-1243.

[10] NFC-Forum, "Major Retail Study: Mobile Consumers Prefer NFC Technology over Competing Alternatives" February 12, 2015,[Online]. (Accessed July, 08, 2015).

[11] Near Field Communication, White Paper, Ronald Minihold, 2011

[12] https://www.makeuseof.com/tag/nfc-security-contactless-payment-issues

[13] https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/the security-issues-in-mobile-near-field-communication