NFC and Its Application to Mobile Payment: Overview and Comparison

Sunil K. Timalsina, Rabin Bhusal, and Sangman Moh
Dept. of Computer Engineering
Chosun University
Gwangju, South Korea
sunil.timalsina@gmail.com, rabin_bhusal@hotmail.com, smmoh@chosun.ac.kr

Abstract—**NFC (Near Field Communication) is a recently emerging technology for short range communications aimed to enhance existing near field technologies such as RFID (Radio Frequency Identification). In this paper, NFC is introduced in terms of operation principles and compared with the existing short range communication technologies. The NFC-enabled mobile systems are technically discussed with respect to architecture and operating modes. Then, NFC as a mobile payment solution is analyzed in terms of security and compared with other existing mobile payment solutions by observing various metrics.**

Keywords—Near field communication; personal area network; inductively coupled antenna; mobile payment; security.

I. Introduction

Near field communication (NFC) is a wireless technology operating in the short range of four to ten centimeters for communication. It is based on radio frequency identification (RFID) technology. For a communication, an NFC device generates a radio frequency in 13.56 MHz spectrum. A receiver could receive the data through the principle of *magnetic inductive coupling* if it lies in a close proximity. Transmitter and receiver are small chipsets which are able to be embedded in devices such as mobile phones, POS (Point Of Sale) terminals, cards posters and many other items.

The NFC forum (www.nfcforum.org) was formed in 2004 aimed at standardizing NFC technology. It defines NFC as: *NFC is a short-range wireless connectivity technology (also known as ISO 18092) that provides intuitive, simple, and safe communication between electronic devices*. Operating at the frequency of 13.56 MHz and limited short range communicating distance, NFC supports data rate of 106 Kbps, 212 Kbps and 424 Kbps. Therefore, NFC is suitable for transmission of short information or messages within small time interval.

In recent days, NFC technology is being widely popular among mobile phone vendors and related fields. This is because NFC is compatible with already existing popular technologies such as RFID, smartcards and contactless cards. It means that stores and systems equipped with the existing technologies should not replace their infrastructure in order to support NFC.

The incorporation of NFC into mobile devices has augmented capability of mobile phones and it is predicted to have potential to do more. This phenomenon has brought forward various works in terms of NFC transactions. At the same time, however, there are serious concerns in different terms such as privacy, user satisfaction, speed, usability, etc. Moreover, it is replacing various popular devices such as RFID tags. Hence, it is important to evaluate the performance of NFC technology and where it stands. In this paper, we have presented the brief insight to NFC technology and analyzed its performance as a mobile payment solution in terms of various factors.

The rest of the paper is organized as follows: In the following section, the principles of NFC are presented. The applications of NFC in mobile payment are discussed and compared to existing popular mobile payment solutions in Section III. Finally, the paper is concluded in Section IV.

II. NFC-enabled Mobile Systems

A. NFC Based on Magnetic Induction

NFC devices communicate through the magnetically induced signals. Therefore, during transmission, energy is coupled between transceivers instead of electromagnetic radiation as in traditional wireless communication. The magnetic induction is discussed in detail in [1-2]. The magnetic induction theory and its application to NFC are also discussed. Figure 1 shows inductively coupled NFC antennas separated by short distance usually in the units of centimeters. Within close proximity, information can be exchanged between these transceivers by magnetic induction. Equivalent circuit diagram of these antennas is shown in Figure 2. Here, our interest is on variation of power at the receiver with distance. Mathematical derivation of power at the receiver for given circuit is derived in [2], where power at the receiver can be expressed as

$$P_R(\omega) = P_T Q_T Q_R \eta_T \eta_R ({r_T}^3 \mu_0 \mu_T {r_R}^3 \mu_0 \mu_R \pi^2)/({r_T}^3 + d^2)^3, \quad (1)$$

where

This research was supported in part by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency)(NIPA-2012-H0301-12-2008).

- P_T: Transmission power,
- Q_T, Q_R: Q-factors of transmitter and receiver antenna,
- η_T, η_R: Efficiency of transmitter and receiver antenna,
- r_T, r_R : Radii of transmitter and receiver antenna coil,
- μ_0: Permeability of air (=1),
- μ_T, μ_R: Relative permeability of transmitter and receiver antenna coil core, and
- d: Distance between transmitter and receiver antenna.

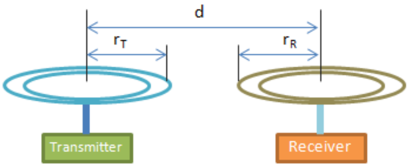

Figure 1. Inductively coupled NFC antennas.

As it can be seen from (1), power at the receiver is dependent on various factors. Therefore, varying each of the factors affects the term on the left hand side. However, for our analysis, we have tried our simulation in MATLAB based on the above expression with the parameter set as below:

- P_T: *23dbm*
- Q_T, Q_R: *48*
- η_T, η_R: *70%*
- r_T, r_R : *2.5 cm, 1.5 cm,*
- μ_T, μ_R : *1 (air-cored coils)*
- d : *0-30 cms*

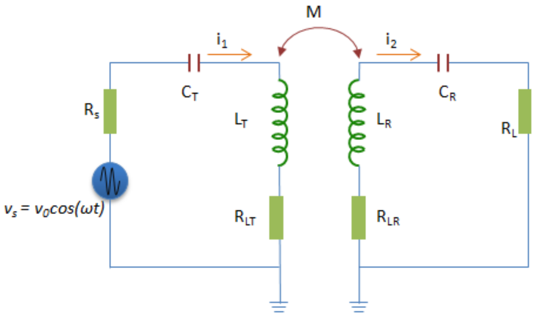

Figure 2. Equivalent circuit of inductively coupled NFC antennas in Figure 1.

Simulation result for above scenario is shown in Figure 3. As it can be seen from the plot and from power equation presented, power at the receiver decreases with the sixth power of distance. This is significant compared to traditional wireless transmission, where signal decreases with the square of the distance in free space.

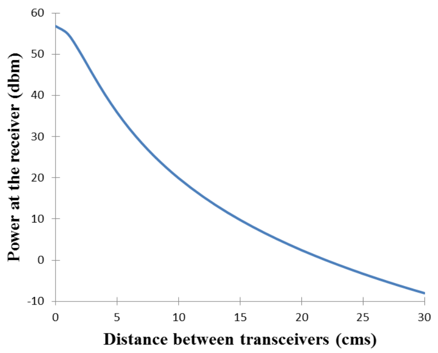

Figure 3. Power at the receiver at different distances.

Furthermore, we tried to examine variation of channel capacity in NFC with respect to distance. According to [2], channel capacity can be given by

$$C = B_f f_0 log_2(1+P_R/N), \tag{2}$$

Where, f_0 is the resonance frequency, P_R is the received signal power, N is the noise power, and B_f is the 3 dB fractional bandwidth. B_f can be approximately related with f_0 and Q-factor of circuit as in equation (3) [1].

$$B \approx 0.644 f_0/Q \tag{3}$$

Result of MATLAB simulation for channel capacity on the same environment as the previous evaluation is shown in Figure 4. We can see that as channel capacity also depends on power at the receiver and Q-factor of the transceiver antenna, degradation on its value is steep with increased distance. However, it should be noted that these results are for particular case of selected values of parameters and results may vary according to antenna configurations.

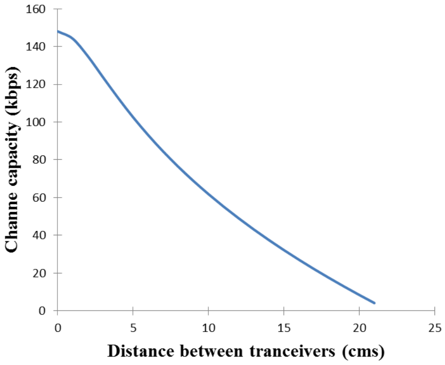

Figure 4. Channel capacity at different distances.

B. *Basic Architecture*

An NFC system basically consists of three components as shown in Figure 5. This is the typical case when an NFC phone reads an NFC tag and communicates with the backend server [3-5]. In some cases, however, an NFC tag can be another NFC phone or there would be no need to contact backend server [6-7]. In essence, an NFC mobile system consists of an NFC tag, an NFC chip embedded mobile phone and a backend server.

1) NFC tag

An NFC tag is generally embedded in items (from which it can be read) such as smart posters [3], POS, electronic devices, etc. It is a small chip usually hidden behind a sticker with NFC logo on it in order to make users aware of its existence. These tags usually contain small data based on their applications such as uniform resource identifiers (URIs), contact information, authentication credentials, valuable information, etc.

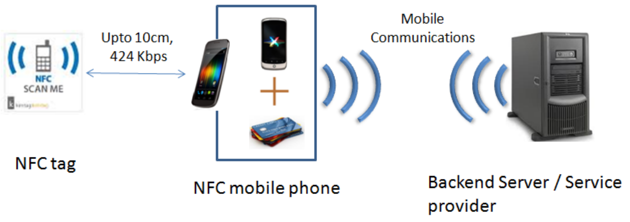

Figure 5. NFC in active/passive mode (typical example of smart poster).

2) NFC Mobile Phone

NFC chips are embedded within mobile hand-sets enabling them to read NFC tags. Mobile phone industry has shown several NFC mobile phones manufactured in last few years. It is also possible to include NFC chip within Subscriber Identity Module (SIM) card or even in micro SD cards. Therefore, hand-sets manufactured without NFC chips from industry can also be made 'NFC-equipped' by inserting NFC-SIM or NFC-micro SD cards.

The NFC phones have several applications installed to utilize NFC capabilities based on the implementation of the system. It can also emulate existing cards such as credit cards, point cards, identity cards etc to give experience of these traditional schemes within a single mobile phone. Hence, a user is give experience of having 'everything' within their mobile device.

3) Backend Server

NFC phone could communicate to the backend server through different mobile communication technology. Service provided by the backend server might vary according to applications. For an instance, it could be a simple web page for reserving movie ticket, issuing receipts, or highly secure financial transaction service. Therefore, communication between handsets and backend server needs to implement secure connection.

C. Operating Modes

Similar to RFID, NFC can also communicate on active/passive mode [8]. This means that an active NFC device is the one with power supply and generates radio field. The NFC device working on passive mode gets power supply through the active devices radiation. On the other hand, both the NFC devices can also work in active/active mode where both the devices are active devices with their own power supply. Generally, NFC can operate on three modes [3].

1) Card Emulation Mode

An NFC enabled phone acts as a tag or a kind of contactless card in card emulation mode. These tags can be read by existing traditional card readers. For an instance, it can be used as an identity card at school or office to unlock door, activate personal devices such as PC, printers, etc. Also, most common usage would be to emulate credit cards or points cards which can be used at POS terminals for payments.

2) Read/Write Mode

An NFC has a predefined data format called NDEF data format. When an NFC phone is in read/write mode, it can read from or write data to supported tag types. Particular example usage of read/write mode is to access URI from smart posters, download short manuals of electronic devices, check out bus -arrival information at bus stops, etc.

3) Peer-to-Peer Mode

The peer to peer mode adds quality functionality to NFC phones. In this mode, two NFC phones can exchange data with each other when brought to close proximity. For an example, two business partners can transfer their virtual business cards with each other by bringing their NFC-enabled phones close to each other. Another popular usage is for connection handoff to other standard technology; NFC connection can be used to set-up Bluetooth pairing or Wi-Fi setup. After successful setup, the handset can use the Bluetooth or Wi-Fi connections.

D. Comparison of NFC with Popular Personal Area Network (PAN) technologies

The NFC technology is compared with popular PAN technologies such as Bluetooth and Infrared Data Association (IrDA) technologies. Table I presents the comparison of NFC, Bluetooth version 2.1 and very fast IrDA technology.

TABLE I. COMPARISON NFC AND OTHER PAN TECHNOLOGIES

	NFC	**Bluetooth V2.1**	**IrDA**
Information transmission	Coupling of magnetic field	Electromagnetic radiation	Infrared light
Operating frequency	13.56 MHz	2.4 GHz	~ 2MHz?
Modes	Active-active, active-passive	Active-active	Active-active
Transmission range	0.04 – 0.1 m	10 – 100 m	0 – 2 m
Network type	P2P	WPAN (scatternet)	P2P
Maximum data rate	424 kbps	2.1 Mbps	16 Mbps
Setup time	< 0.1s	~6s	~0.5s
Maximum current consumption	< 15mA	< 30mA	< 5mA
Line of sight	Yes	No	Yes
Authentication and encryption	Yes	Yes	No
Cost of device	Low	Moderate	Low

III. MOBILE PAYMENT USING NFC

A. Security Issues and Considerations

NFC system consists of two communications: between NFC devices and between NFC device and backend server.

Backend server communication is done through different kinds of mobile communication technology. Security measures in these communications are discussed in literature extensively and, hence, it is out of scope of this paper. Here, we present security concerns in NFC-NFC communication. Although NFC-NFC works in very close proximity, its security can be confirmed to some extent. However, as it is a wireless technology, some security issues are inevitable [8-9].

1) Eavesdropping

Through eavesdropping, an attacker can receive the transferred information using a suitable antenna. For NFC attack, this antenna should be close enough. But, there is no solid analysis on accurate range for possible attack as it depends on attackers' antenna parameters. It is to be worth noted that NFC provides no defense mechanism against eavesdropping. In [8], it is discussed that eavesdropping in NFC is difficult if a device is working on passive mode. Hence, operating on passive mode could be one of the countermeasures against eavesdropping. However, it is not practical for an NFC device to always operate on passive mode. Therefore, eavesdropping can be avoided by establishing a secure channel between the devices.

2) Data Modification

An attacker can tamper the data using different RF field if it has enough knowledge on transmission such as operation modes, modulation technique used, etc. This attack can be further divided into following three types:

- *Data Alteration*: An attacker sends a valid but modified data to the receiver.
- *Data Insertion*: An attacker inserts its data within short interval of time before receiver answers to the transmission.
- *Data Destruction*: An attacker corrupts or blocks the transmitted data to make it unreadable by the receiver (DoS attack).

3) Relay Attack

Relay attack is also popularly known as 'man in the middle attack' in network security. Here, an attacker receives signal from transmitter and modifies or alters that data and sends it to the receiver and vice versa. Although, this is a big issue in large network security, it is very difficult or almost impossible in NFC as both transceivers can detect radio field during communication and can be aware of unknown RF field or collision.

4) Lost devices and abandoned connections

NFC-enabled mobile devices are prone to be lost. But, they contain important information such as credit card and private data. So, anyone who finds the lost hand-set can use it such as one is able to use the lost credit card. In this kind of scenario, manual security in mobile sets is the only solution such as securing hand-set access through some PIN codes or personal identification codes.

B. NFC as a Mobile Payment Solution

Most popular usage of NFC has been in mobile payment solution. NFC handsets can work in a card emulation mode. It could emulate credit cards, point cards, etc. from several vendors in a single device. This enables users from hassle free hold of their money. Even with the mobile handsets, especially smartphones, there are various applications dedicated for payments. Several banks provide SMS banking for their customers. Infrared enabled POS terminals are popular in many countries. Especially, in mobile payment solution, there has been advent of many techniques for customers. Table 2 shows comparison of NFC mobile payment solution and some other existing payment solutions.

IV. Conclusion

In this paper, we have introduced working principle of NFC and analyzed how the power at the receiver and channel capacity degrades with increased distance between transceivers. We have also discussed the different operating modes of NFC and compared NFC with the existing PAN techniques. Although there are security concerns in NFC, it is very difficult to attack as compared to other communication technologies. Among a wide range of NFC applications, mobile payment solution is one of the popular and widely exploited. We have shown that, although it is not the best solution, it improvises not only lots of perceptions in the viewpoint of users but also robustness on in the viewpoint of operation.

Acknowledgment

The authors would like to thank the anonymous referees for their helpful comments on this paper. Correspondence should be addressed to Dr. Sangman Moh (smmoh@chosun.ac.kr).

References

[1] J. I. Agbinya, N. Selvaraj, A. Ollett, S. Ibos, Y. Ooi-Sanchez, M. Brennan, and Z. Chaczko, “Size and characteristics of the ’cone of silence’ inthe near-field magnetic induction communications,” *Journal of Battlefield Technology,* Vol. 13, No. 1, Mar. 2010.

[2] J. Agbinya and M. Masihpour, “Power equations and capacity performance of magnetic induction communication systems,” *Wireless Personal Communications*, pp. 1–15. Dec. 2010.

[3] NFC Forum, “White paper on ’smart posters’,” Tech. Rep., Apr. 2011.

[4] NFC Forum, “White paper on ’essentials for successful NFC mobile ecosystem’,” Tech. Rep., Oct. 2008.

[5] NFC Forum, “White paper on ’the keys to truly interoperable communications’,” Tech. Rep., Oct. 2007.

[6] R. Steffen, J. Prei andinger, T. Scho andllermann, A. Mu andller, and I. Schnabel, “Near field communication (NFC) in an automotive environment,” *Proc. of 2010 Second International Workshop on Near Field Communication (NFC)*, pp. 15-20, Apr. 2010.

[7] C. Leong, K. Ong, K. Tan, and O. Gan, “Near field communication and bluetooth bridge system for mobile commerce,” *Proc. of 2006 IEEE International Conference on Industrial Informatics*, pp. 50-55. Aug. 2006.

[8] E. Haselsteiner and K. Breitfu, “Security in near field communication (NFC),” *Proc. of Workshop on RFID security*, 2006.

[9] C. Mulliner, “Vulnerability analysis and attacks on NFC-enabled mobile phones,” *Proc. of International Conference on Availability, Reliability and Security (ARES ’09)*, pp. 695-700, Mar. 2009.