International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-1, October 2013

Near Field Communication in Mobile Phones

Asawari Dudwadkar, Akhil Gore, Tushar Nachnani, Harshil Sabhnani

Abstract - The electronics and telecommunications industry has experienced rapid advances over the past decade. This has led to a new paradigm in the field of data transfer and wireless communication. This brings us to the current revolution the mobile industry faces in the form of NFC technology. Near Field Communication technology (NFC) is a standard for very short range communication up to a few centimetres. It finds various applications ranging from data transfer, secure identification, payments, marketing, healthcare, aviation, hospitality. NFC works at a very short range, mostly by touching the devices that employ NFC. This makes NFC a very easy and viable technology to use. This paper explains the theories behind NFC and then presents a number of compelling applications of NFC for mobile phones, while analysing the associated security threats.

Index Terms: Smartphone, NFC, NFC tags, NFC reader

I. INTRODUCTION

Near field communication (NFC) is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimeters.The number of short-range applications for NFC technology is growing continuously, appearing in all areas of life. Especially the use of NFC in conjunction with mobile phones offers great opportunities. One of the main goals of NFC technology has been to make the benefits of short-range contactless communications available to consumers globally. The existing radio frequency (RF) technology base has so far been driven by various business needs, such as logistics and item tracking. While the technology behind NFC is found in existing applications, there has been a shift in focus most notably, in how the technology is used and what it offers to consumers. With just a point or a touch, NFC enables effortless use of the devices and gadgets we use daily. Here are some examples of what a user can do with an NFC enabled mobile phone:

- Download music or video from a smart poster.
- Exchange business cards with another phone.
- Pay bus or train fare.
- Print an image on a printer.
- Use a smartphone as a ticket for boarding a flight
- Avail discounts and concessions through smart NFC posters
- Secure identification

NFC is being seen as a new paradigm for wireless data transfer.

Manuscript published on 30 October 2013.
* Correspondence Author (s)
Asawari Dudwadkar, Electronics Engineering, Assistant Professor, V.E.S Institute of Technology, Chembur, Mumbai, India.
Akhil Gore, Electronics Engineering, Student, V.E.S Institute of Technology, Chembur, Mumbai, India.
Tushar Nachnani, Electronics Engineering, Student, V.E.S Institute of Technology, Chembur, Mumbai, India.
Harshil Sabhnani, Electronics Engineering, Student, V.E.S Institute of Technology, Chembur, Mumbai, India.

It is essentially a more advanced and flexible derivative of the very popular RFID technology. We will now deal with the electrical and communication theories behind NFC to develop an understanding of NFC.

II. THEORIES AND WORKING

NFC is a technology which is very similar to RFID (Radio Frequency Identification). Just like RFID, NFC employs radio waves to communicate between devices. Generally, NFC communication consists of an active reader and a passive tag. The reader sends radio waves and reads data on the tag, the same way as RFID.

A. Data transfer through mutual induction

In order to achieve communication NFC works on the principle of mutual induction. It's the same principle that makes a transformer work. A radio frequency (RF) sine wave generated by the antenna in the reader is used to transmit energy to the tag and retrieve data from the tag. When the NFC in the reader is active, it continuously generates a periodic sine wave signal at the unregulated frequency of 13.56 MHz [3][4]. If there is any tag within the area of the magnetic flux generated by the sine wave, it gets energy from the alternating magnetic flux and changes the frequency properties of the original sine wave generated by device. The changes are detected by the reader which understands that there is a tag nearby [3].

Thus the carrier wave induces a small alternating current (AC) in the antenna of the NFC tag. Inside the integrated circuit chip, a power rectifier and regulator converts the AC to stable DC and uses it to power the chip, which immediately "wakes up" [10]. The tag antenna in turn modulates this carrier wave using Manchester Coding or Miller coding. This modulated wave is detected by the reader and gets demodulated. Modulation is done via Frequency Shift Keying, Phase Shift Keying, or Amplitude Shift Keying. This way data can be transmitted at 106 Kbps, 212 Kbps and 424 Kbps depending on the tag and the device [2][9]. NFC communication is standardised by the ECMA under the NFCIP-1 protocol. This governs the modes of operation (active & passive), modulation techniques, transfer speeds as well as initialization schemes for NFC devices [6].

B. NFC data format

Most NFC tags are passive elements which store data for the reader (for NFC enabled smart phone) in NDEF (NFC Data Exchange Format) format. When we touch our phones with any NFC enabled tags, we actually read the NDEF message through our application. The NFC Data Exchange Format (NDEF) specification defines a message encapsulation format to exchange information, e.g. between an NFC Device and another NFC Device or an NFC Tag.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

NDEF is a lightweight, binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message. An NDEF message is composed of one or more NDEF records. There can be multiple records in a NDEF message [5]. The number of records we can encapsulate in a NDEF message depends on the application and the tag type. For our analysis purposes we use only one NDEF record. This NDEF record stores the Unique Resource Identifierhttp://xyz.com
When we communicate with our NFC reader devices (smart phones) to read data froma NFC tag we read basically (for example http: //xyz. com) the following hexadecimal code [12].

03 0e d1 01 0a 55 03 6e 6f 6b 69 61 2e 63 6f 6d fe

- 03 - This is one byte that defines the type of record this is. An NDEF record is represented by the hex byte 03.[11]
- 0e - This is one byte that tells the reader how many bytes are in the payload. [11]
- d1 - NDEF records are variable length records with a common format illustrated in the figure below. In binary, d1 is 11010001.[11]

MB	ME	CF	SR	IL	TNF	TNF	TNF

Table 1 – *NFC Data Exchange Format*

In our case:

- MB = 1 (Message Begin is true means this is first record in the NDEF message).[11]
- ME = 1 (Message End, means it is last record in the NDEF message, if it is 0 that tells application that more records are ahead)[11]
- CF = 0 (means this is not a chunked message. An NDEF message can contain zero or more chunked payloads. Each chunked payload is encoded as an initial record chunk followed by zero or more middle record chunks and finally by a terminating record chunk, in our case we simplify our record as not chunked)[11]
- SR = 1 (SR stands for short record, if set, that the payload length field is a single octet. This short record layout is intended for compact encapsulation of small payloads which will fit within payload fields of size ranging between 0 to 255 octets.)[11]
- IL = 0(IL stands for identification length, if set, then the ID_LENGTH field is present in the header as a single octet. If the IL flag is zero, the ID_LENGTH field is omitted from the record header and the ID field is also omitted from the record)[11]
- TNF = 001(The TNF field value indicates the structure of the value of the TYPE field. The value 0x01 indicates that the TYPE field contains a value that follows the Record Type Definition type name format defined in the NFC Forum RTD specification [11].

The “unique resource identifier” record type enables textual URIs to be encoded in a record. The defining header, for example, “http://www.,” can also be compressed into a 1-byte field in the NDEF frame, reducing the size of the final URI text that a tag needs to store [5]. An application receiving an NDEF record with a URI type can choose to automatically pass it to an application for processing—in the examples above, a Web browser or a telnet terminal client [12].

In this way the NDEF format specifies a number of RTDs such as text, generic control, signature, smart poster which allows developers to store varied data into a NFC tag, depending on the application that employs NFC [12].

III. MODES OF COMMUNICATION

Based on how devices interact with each other, NFC supports 3 modes of communication. All the modes of communication are defined by the ECMA NFCIP-1 protocol.

- Reader / Writer Mode
- Peer to Peer Mode
- Card Emulation Mode

A. Reader / Writer Mode

This mode of communication involves a NFC device like a smart phone and a NFC tag. NFC tags have a few bytes of memory which can be written onto. The NFC enabled Smartphone writes to this NFC tag via a writing application. For writing data onto a tag, the NFC device must touch or tap the tag. In a similar way, the NFC device can even read from a tag. This can be used to perform simple operations such as toggling Wi-Fi, setting up Bluetooth or even opening an application [4][8].

B. Peer to Peer Mode

In this mode, communication takes place between two active NFC devices. This means both the devices are self-powered and do not rely on each other’s magnetic fields for power. This is the most important of all communication modes and this is where NFC differentiates itself from RFID. Using this mode 2 NFC enabled smartphones can communicate with each other. Smart phones such as Google Nexus S, Samsung Galaxy Nexus, Samsung Galaxy S 3 and a few other phones by different Original Equipment Manufacturers (OEMs) come equipped with NFC. By tapping these phones against each other data can be exchanged efficiently and with negligible time delay. The data can be a business card, a music playlist or even pictures. What data is to be sent is determined by the application [8].

C. Card Emulation Mode

This mode makes an NFC device such as a smartphone emulate a smartcard. In this mode, the device will stop emitting RF waves and become passive. If a reader is brought near this smartphone, it can read data off the phone [8].

IV.MODES OF OPERATION

Based on whether NFC uses self-powered devices or powerless devices, NFC supports 2 modes of operation –

- Passive Mode
- Active Mode

A. Passive Mode

In the passive mode, the NFC device acts as a target. All NFC tags operate in passive mode.

Passive mode is for those

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

devices which do not have their own source of power. These devices rely on the initiator (the reader or the smart phone) to get power. In the reader / writer mode, NFC tags work in the passive mode of operation [4][6][10].

B. Active Mode

This mode of operation applies to those NFC devices which have their own source of power. Smartphone and NFC readers are the examples of devices which operate in the active mode. During P2P communication, both the devices are active devices [4][10]. To ensure proper communication, NFCIP-1 defines the following protocol flow:

- All devices should stay in Target mode and not generate an RF field as default.
- A device switches to Initiator mode only if it is required by the application.
- Before activating the RF field the Initiator has to check against another active sender so no other communication is disturbed.
- If no other RF field is detected the Initiator starts communication and tells the target to use Active or Passive communication mode and sets the transmission speed. After communication, both devices switch back to Target mode and deactivate their RF fields [6].

All the above modes lead to different applications on various platforms. Applications of NFC are discussed in the next section.

V. NFC IN MOBILE PHONES

As the paper explains, NFC finds use in varied areas of our day-to-day life based on the different modes of operation offered by NFC.

NFC provides us with a "Hit and run" functionality. This means that touching a NFC tag or another NFC mobile phone with an active NFC device can invoke some functionality of the device based on the context. This feature of NFC is its most important advantage and holds a lot of scope for application development.

Analysing the many applications we came up with using NFC, we have identified three important classes of applications of NFC in mobile phones :

A. Payments

NFC was designed to interoperate with existing deployments of near-field radio technologies, including contactless payments and access to public transit systems. Moving these transactions to the phone may help reduce the number of things a person carries, but there are other more significant benefits [6].

We can improve the security of credit card transactions by moving the contactless payment to an active, programmable device by supporting one-time use credit cards. One-time use credit cards are tremendously useful for reducing credit card fraud—instead of giving a vendor our credit card numbers, we can request our bank to give us credit card numbers that can be used only once. With NFC on a phone, users can run an application that stores one-time credit card numbers securely and easily, and the application can present these one-time numbers to vendors. The phone may negotiate several one-time use numbers in advance so that payments can be made with the phone offline. With these daily tasks moved to the phone, we can further enhance the mobile experience [6][8].

Applications for payments :

Receipts, reimbursement and money management are the proposed applications. As an add-on to contactless payments, we imagine the transaction results in a receipt being sent to the user's phone. The receipt may be transmitted as part of an enhanced standard for contactless payments, or may occur as an additional transaction during the same NFC scan. The phone keeps a local database of transactions and receipt objects, and allows programmatic access to them (with appropriate security restrictions). This will enable, for example, an application for managing receipts. Another application can help manage reimbursement claims. After a few purchases, a user can send electronically mail these receipts to file a reimbursement claim. The receipt data is stored privately on the phone, and is only released at the user's discretion.

Real time Check-ins Check-in services such as Foursquare and Facebook Places have grown in popularity. Usually check-in services make use of the Global Positioning System (GPS) on a smartphone for initializing check-in. Using NFC for contextual awareness is a much lower-power solution than using GPS and is also more accurate. We also imagine dedicated NFC tags that a business may put out explicitly for making check-ins easy.

Public transportation We can improve the usability of ticketing for a public transport system by using the phone as our ticket. Scanning into the system using NFC can invoke an application. This program can provide the user with a real-time schedule, customized to their current stop, and can alert the user when their destination nears. It can also be used to purchase tickets or give information about the available credit in their account.

B. Virtual tokens

NFC can be used to replace various applications involving physical tokens: from getting a claim check for valet parking to getting loyalty cards from restaurants for attracting repeat customers. By using NFC on the phone, we do not have to worry about misplacing physical tokens; furthermore, these virtual tokens can be entered into our databases and tracked automatically.

In the following, we will describe the applications of virtual tokens.

Applications for virtual tokens :

Receipts, physical objects represented by virtual tokens: Receipts or tokens are often handed to the customers as they bring in their dry-cleaning to the cleaners, leave their car with the valet etc. Instead of pieces of papers, NFC can be used to give the customers a receipt, which they can use to claim their items upon their return. In this way, customers do not have to worry about misplacing the receipts. More importantly, customers can submit these tokens remotely over the network before they arrive in person so that these objects can be retrieved ahead of time. Here it is important that the tokens are not forgeable. These tokens can also be used as signatures from grantee to grantor. Users can sign for packages by tapping their phone to a delivery person's portable kiosk, adding improved verifiability to the system [8].

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Unification of peer generated tokens

Users cannot be expected to install separate mobile applications for each service provider they interact with. We propose the notion of a rich token manager for handling tokens. The token manager maps a service (a particular restaurant, etc.) to a token. Given a service identifier, a user will typically have at most one matching token in his database. Each token has a globally unique identifier generated by the grantor, such as a random 128-bitnumber. In addition, the token incorporates a creation timestamp and the creator's service identifier—the grantor certificate. The token will not have personal identifying information associated with it by default, although it may be reissued with additional data attached as the grantor and grantee interact over time. All token contents are signed by the grantor, and the signature is verified by the receiving party [8].

token GUID, timestamp
attribute #1, attribute #2…
grantor certificate, grantor signature

Table 2 - *Format of virtual token*

The user experience is as follows. First, the user unlocks his phone. He then touches it to the grantor's station, be it kiosk, mobile phone, or otherwise. The phone learns of the grantor by its known service name and checks the phone's database to see if the user has an existing token. If so, the token is presented to the grantor, as long as the user has allowed automatic submission. Otherwise, he is prompted to approve the action. Finally, if the user does not have an existing token, the grantor can create one. The new token will be unique and can be coupled with other personal information at the user's discretion.

C. Junctions

NFC can introduce two peers so they can interact with each other based on context, using the peer-to-peer mode of communication. By allowing peers to exchange a session-specific secret, we can enable all forms of peer-based interactions, without having to be monitored by third-party servers. We use NFC as a tool for bootstrapping multi-party applications, with the application session running over another channel. NFC can be used to exchange playlists, pictures, contact cards, etc between two smartphones. In this exchange, NFC is employed as an authenticator for boot-strapping longer range wireless technologies such a Bluetooth and Wi-Fi. Google's Android operating system for mobile phones supports data transfer via the NFC protocol through its custom application Android Beam. NFC on an Android smartphone allows the phone to read NDEF data from a tag or from another phone using Android Beam. In this way, several types of data can be exchanged with the least setup time (<0.1 sec). Junction application of NFC presents the most exciting opportunities for application developers to develop applications using the NFC API supplied by Google and by other OEMs supporting NFC such as Windows Phone and BlackBerry.

VI. SECURITY THREATS TO NFC

Despite NFC being a very close range communication protocol, it faces security threats. There are different possibilities to attack the NFC technology. On one hand, the different NFC devices may be manipulated physically. This may include the removal of a tag from the tagged item or wrapping them in metal foil in order to shield the RF signal. NFC tags could also be tampered with by illegitimately writing data onto them if they aren't read-only tags [1][7]. In this case, we want to focus on attacks with regard to the communication between two devices.

A. Man–in–the-Middle Attacks

With NFC, we must watch out for the possibility for an attacker, a third party with an active tag, to inject itself in the conversation and modify it to his advantage or destroy it using RFID jammers, possibly even without being noticed. While peer certificates can go a long way towards excluding third parties from an exchange, they will never be the complete answer as certificates can be obtained fraudulently, or perhaps with an apparent owner which appears to be legitimate, but is not (such as using a slightly misspelled version of the legitimate owner). Because of this, it is imperative that interactions be designed with multiple safeguards: verification based on cryptography, as well as user verification and common sense (e.g. when confirming a payment, there should not be two or more simultaneous payment requests from different payees, or, when payment is confirmed but the service is still unavailable, assume fraudulent use—the payment went to the wrong destination—so the user should investigate)

B. Data Insertion

This attack can only be implemented by an attacker, if there is enough time to send an inserted message before the real device starts to send its data. NFC devices are able to receive and transmit data at the same time. That means, they can check the radio frequency field and will notice the collision. If a collision occurs the data exchange would be stopped at once. In order to prevent such attacks the device should try to answer with no delay. Alternatively, again checking the RF field and also the secure channel can be used to protect against attacks [1][7].

C. Data modification

Unauthorized changing of data, which results in valid messages, is much more complicated and demands a thorough understanding. Data modification is possible only under certain conditions. In order to modify the transmitted data an intruder has to concern himself with the single bits of the RF signal. The data can be sent in different ways. The feasibility of this attack, that means if it is possible to change a bit of value 0 to 1 or the other way around, is subject to the strength of the amplitude modulation. If 100% modulation is used, it is possible to eliminate a pause of the RF signal, but not to generate a pause where no pause has been. This would demand an impracticable exact overlapping of the attackers signal with the original signal at the receiver's antenna [1][7].

VII. CONCLUSION

This paper studies NFC and proposes new applications for NFC in mobile phones, while addressing the security threats. It endeavours to show the possible benefits of NFC in our day-to-day lives.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

There are many OEMs which are bringing out NFC enabled phones and estimates suggest that around 100 million smartphones with NFC will be shipped in 2013. Indeed the possibilities will be limitless. There is an undeniable possibility that in around 2-3 years, all we may need to carry on our person is a smart phone. With this paper we have attempted to elucidate the myriad ways we can make our smartphones, smarter. Even as NFC theoretically presents compelling applications, it remains to be seen whether countries adopt this wireless protocol and upgrade their current infrastructure. Only then can we realise the vision of a fully automated, paperless future.

REFERENCES

[1]. André Filipe de AzevedoFigueiredo Cruz, "NFC And Mobile Payments Today", Universidade De LisboaFaculdade De CiênciasDepartamento De Informática.
[2]. Anokwa Y et al, "A user interaction model for NFC enabled applications", Pervasive computing and communications workshop, IEEE
[3]. Basil Rajeev, "Near field magnetic communication", Antennas and Propagation Magazine, IEEE, vol 46
[4]. ECMA, "Near field communication white paper"; "http://www.ecma-international.org/activities/Communications/tc32-tg19-2005-012.pdf"
[5]. Google Android developer forum. "NFC basics"; "http://developer.android.com/guide/topics/connectivity/nfc/nfc.html #tag-dispatch"
[6]. Hussein Ahmad Al-Ofeishat et al, "Near field communication (NFC)", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012
[7]. Infosec institute resources, "Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema"; "http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/"
[8]. Infosys, SETLabs Briefings; "http://www.infosys.com/infosys-labs/publications/Documents/winning-it.pdf#page=69"
[9]. Nasution, S.M et al, "Prototype of Train ticketing application using NFC on Android device", System Engineering and Technology International Conference
[10]. Nokia. Nokia Developer. "NFC usage and working principles" ;"http://developer.nokia.com/Community/Wiki/Inside_NFC:_Usages _and_Working_Principles"
[11]. Nokia. Nokia Developer. "Understanding NFC Data Exchange Format (NDEF) messages";"http://developer.nokia.com/Community/Wiki/Understanding_NFC_Data_Exchange_Format_(NDEF)_messages"
[12]. Want R, "Near field communication", Pervasive Computing, IEEE, vol 10.

Asawari Dudwadkar, Assistant Professor, Department of Electronics, VESIT, Mumbai Research Scholar, JJTU, Rajasthan Mrs. Asawari Dudwadkar received the Bachelor's Degree in Electronics Engineering and Master's Degree in Electronics & Telecommunication from University of Mumbai, India in 1996 and 2007 respectively. She is currently working toward the Ph.D. degree in the Department of Electronics and Communication engineering from JJT University, Rajasthan. Her main research interests include Induction Heating Applications, Inverter modeling and digital control design strategies. She has many publications to her name, some of which are:-

Mrs. Asawari Dudwadkar & Dr. Y.S Rao,"Induction Heating: An overview of Digital control Based Systems" at National conference at LT COE, Mumbai Sep 2011

Mrs. Asawari Dudwadkar & Dr. Y.S Rao (vice principal SPIT, Mumbai) Published paper in INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH , ISSN No: 2277 8179 on " Optimisation of Induction Heating system in Simulink.." for July 2013 issue.

Mrs. Asawari Dudwadkar & Dr. Y.S Rao ," Contributions to Optimization of Induction Heating System ".International Journal of Scientific and Modern Engineering (IJISME), Aug2013 , ISSN2319-6386

Akhil Gore, Akhil is a final year Bachelors of Engineering student in VESIT, Mumbai- University of Mumbai.

Tushar Nachnani, Tushar is a final year Bachelors of Engineering student in VESIT, Mumbai- University of Mumbai.

Harshil Sabhnani, Harshil is a final year Bachelors of Engineering student in VESIT, Mumbai- University of Mumbai.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)