International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Wireless Communication through Near Field & its Security

Vikas Nivrutti Dhakane[1], Gaurav Mahavir Phade[2], Sachin Dadaso Pandhare [3]

[1,2,3] Professor, Department of CSE, SMSMPITR, Akluj, , Solapur University, Maharashtra India

Abstract: ***This paper gives a complete idea about near field communication & analysis of security with respect to NFC. Near Field Communications (NFC) is a short-range wireless technology that allows mobile devices to actively interact with passive physical objects and other active mobile devices, connecting the physical world to mobile services in ways that empower and benefit users. We will also be using the term "Tap 'n Go" because it clearly conveys a visual image in which this technology is intended to be used. Near field communication is a set of principles for smart phones and alike devices to establish radio communication with each other by connecting them together or bringing them into compatibility which are usually not more than a few centimeters apart. Present and anticipated applications include contactless transactions, data exchange, and simplified setup of more complex communications such as Wi-Fi. This paper highlights the capabilities of near field communication and its potential to enhance everyday lives. It further describes how the NFC Forum works to drive NFC standardization and encourage its adoption in the market. . NFC allows for contextual application invocation (CAI)—the execution of code on the phone as a result of our environment.NFC builds upon Radio-Frequency Identification (RFID) and contactless smartcard technologies that enable stored data to be actively "read" at a distance. RFID is a powerful enabling technology that is being applied in an astonishing range of applications and uses, from supply chain management and product inventory control to identity authentication and access control.***

Keywords: CAI (Contextual Application Invocation), NFC (Near Field Communication), protocol, network, Radio-Frequency Identification (RFID), NDEF (NFC Data Exchange Format)

1. Introduction

1.1 Introduction & History of NFC

NFC is based on a communication standard that specifies how two devices establish a peer to peer network in order to exchange data. NFC uses electromagnetic radio fields to communicate. This is in contrast to Bluetooth or Wi-Fi which use radio transmissions. Near field communication (NFC) traces its roots back to radio-frequency identification (RFID). Indeed, NFC is actually a subset of RFID with a shorter communication range for security purposes. In 2004, Nokia, Sony, and Philips came together to form the NFC Forum. This group is dedicated to Promoting the security, ease of use, and popularity of near field communication. It aims to educate businesses about the

Technology and upholds standards that allow NFC to operate between different devices. Those who wish to create NFC compliant devices must meet these standards set forth by the NFC Forum. This ensures that any user with any NFC device can use it with any other NFC device or NFC tag [1].

1.2 Purpose of NFC

Near field Communication or NFC is a standard defined by the NFC Forum, a global consortium of hardware, software/application, credit card companies, banking, network providers, and others who are interested in the progression and standardization of this promising technology [4].

2. Features of NFC System

Following are some important features of Near Field Communication [6]:

- It is easy to control whether the two devices communicate by simply placing them next to each other or keeping them apart.
- This allows for the establishment of the network connection between the devices be completely automated and happen in a transparent manner.
- Another important feature of this protocol is the support for the passive mode of communication.
- The NFC devices are able to work with the smart cards and smart card readers conforming to these protocols in a flawless manner.

3. Protocols Specification

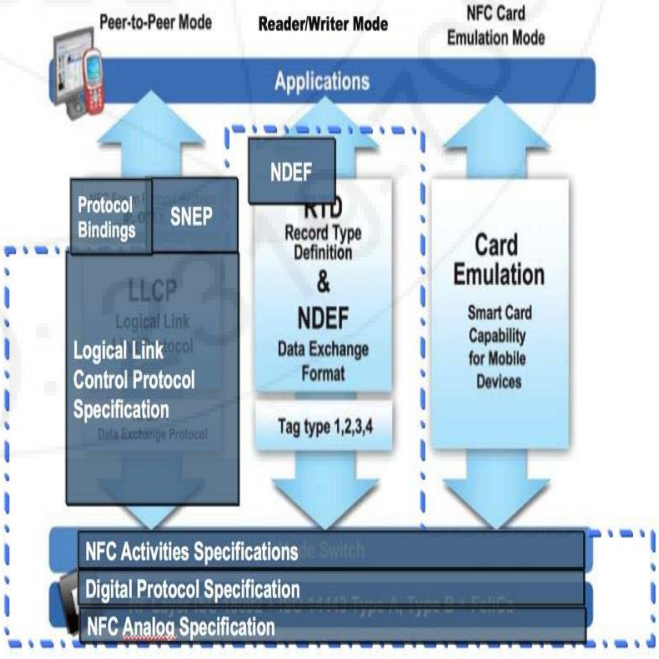

Figure 4.1: Protocol Technical Specification

3.1 NFC (LLCP) Technical Specification

Defines an OSI layer-2 protocol to support peer-to-peer communication between two NFC-enabled devices, which is essential for any NFC applications that involve bi-directional Communications. The specification defines two service types, connectionless and connection-oriented, organized into three link service classes: connectionless service only; connection-oriented service only; and both connectionless and connection-oriented service[4], [9].

3.2 NFC Digital Protocol Technical Specification

This specification addresses the digital protocol for NFC-enabled device communication, providing an implementation specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards [4], [9].

3.3 NFC Activity Technical Specification

This specification explains how the NFC Digital Protocol Specification can be used to set up the communication protocol with another NFC device or NFC Forum tag. It describes the building blocks, called Activities, for setting up the communication protocol. These Activities can be used as defined in this specification or can be modified to define other ways of setting up the communication protocol, covering the same or different use cases[4], [9].

3.4 NFC Simple NDEF Exchange Protocol (SNEP) Specification

The Simple NDEF Exchange Protocol (SNEP) allows an application on an NFC-enabled device to exchange NFC Data Exchange Format (NDEF) messages with another NFC Forum device when operating in NFC Forum peer-to-peer mode. The protocol makes use of the Logical Link Control Protocol (LLCP) connection-oriented transport mode to provide a reliable data exchange [4], [9].

3.5 NFC Analog Technical Specification

This specification addresses the analog characteristics of the RF interface of the NFC-Enabled Device. The purpose of the specification is to characterize and specify the externally observable signals for an NFC-Enabled Device without specifying the design of the antenna of an NFC-Enabled Device [4], [9].

4. NFC & Other Technologies

Bluetooth, Radio-frequency identification, QR codes the modern world is ever expanding and with it comes new technologies that change the way we communicate and interact with each other [2], [3].

Table 4.1: NFC Comparison

Features	*RFID*	*Bluetooth*	*NFC*
Security	✓	✓	✓
Short Distance	✓	✓	✓
No Authorization	✓	✖	✓
Receive & Send	✖	✓	✓
In build	✖	✓	✓
Widely Known	✓	✓	✖

5. About Near Field Communication Tags

NFC tags are programmed with just about any sort of information and then plopped into almost any product, letting you read them with a smartphone or another NFC-capable device. **NFC tags**, for example stickers or wristbands, contain small microchips with little aerials which can store a small amount of information for transfer to another **NFC** device, such as a mobile phone [8].

Figure 5.1: NFC Tags

6. Benefits & Applications

6.1. Benefits of Near Field Communication

- **Ease of Use**
  By far the most obvious benefit of near field communication and the contactless payment systems it creates is its ease of use. No need to carry multiple credit cards or dig through your wallet for the right one. No more lost movie tickets or subway passes. And finally, no more individual rewards cards from different stores to track. Instead of carrying a card for every store you shop at, load them on your phone and coupons and rewards points go straight to your account without ever digging out the card [1],[7].
- **Security**
  If your wallet is stolen, a thief has instant access to all your credit cards, debit cards, and photo IDs. Storing this information all in one place on your smartphone may sound dangerous at first, but actually provides a safer environment than your physical wallet. While you can't password protect your wallet, you *can* password protect your smartphone. No thief can use your cards if they can't unlock the phone to get at them [1], [7].
- **Versatility**
  Perhaps one of the most important aspects of near field communication technology is its versatility. Ease of use is important to convince individuals to stick with the technology, but it needs to cover a variety of uses for others to really catch NFC fever. Customers can check out at a store, purchase and load concert tickets to their smartphones, board the subway, read information from a smart poster, and many other tasks all from a single device [1],[7].

6.2. Applications of Near Field Communication

Where ever you go, you'll encounter ways to make your day easier using near field communication. Plans for the future cover shopping malls, office buildings, and even your own vehicle as potential places for near field communication to help offer quick services. Below is a list of ways everyday

people can or will be able to interact with near field communication[1], [7].

- **Commuting to the office**: During the drive to and from work, NFC can unlock your car, adjust your seats, and even admit you to the company's secure parking garage.
- **At the office:** Once you've arrived, you can gain access to your office building and clock in by swiping your smartphone or other device.
- **On the bus:** If you commute to the office, you can pay for your bus or subway pass and wave your phone to pass through the gates..
- **At the store:** On the way home from work you stop to buy groceries. Coupons and customer reward points are already pre-loaded on your smartphone and are applied to your total automatically when you check out. Payment occurs when you wave your smartphone over the card reader and you're ready to go without ever opening your wallet.
- **At a concert:** Like purchasing a bus ticket, you can purchase concert tickets and use your NFC compatible smartphone to gain access to a concert. You can also interact with smart posters at the concert for information about the band, the current schedule of events, and upcoming performances.
- **Hanging out with friends:** Finally, when you need some down time you can share games, links, and info with friends by bumping phones. NFC can establish a Bluetooth connecting between your phones for sending large amounts of data from a further distance range than NFC covers.

7. Security in NFC

Establishing a secure channel between two NFC devices is clearly the best approach to protect against eavesdropping and any kind of data modification attack. Due to the inherent protection of NFC against Man-in-the-Middle-Attacks it is rather easy and straightforward to setup a secure channel. A standard key agreement protocol like Diffie-Hellmann based on RSA or Elliptic Curves could be applied to establish a shared secret between two devices. Because Man-in-the-Middle is no threat, the standard, unauthenticated version of Diffie-Hellman works perfectly. The shared secret can then be used to derive a symmetric key like 3DES or AES, which is then used for the secure channel providing confidentiality, integrity, and authenticity of the transmitted data. Various modes of operation for 3DES and AES could be used for such a secure channel and can be found in literature [5], [6].

Security Concerns with NFC Technology

New users of near field communication, especially for payment purposes such as storing credit card information, are understandably concerned at first about the security and safety of their private information. Possible security attacks include eavesdropping, data corruption or modification, interception attacks, and physical thefts. Below we cover the risks and how NFC technology works to prevent such security breaches from occurring.

Eavesdropping is when a criminal "listens in" on an NFC transaction. The criminal does not need to pick up every single signal to gather private information. Two methods can prevent eavesdropping. First there is the range of NFC itself. Since the devices must be fairly close to send signals, the criminal has a limited range to work in for intercepting signals. Then there are secure channels. When a secure channel is established, the information is encrypted and only an authorized device can decode.

Data corruption and manipulation occur when a criminal manipulates the data being sent to a reader or interferes with the data being sent so it is corrupted and useless when it arrives. To prevent this, secure channels should be used for communication.

8. Conclusion

In this paper, we have presented our vision of how communication will change when NFC becomes commonplace.NFC will allow what we term contextual application invocations. Paper also reflect that NFC has the impending potential to make almost all wireless technologies easy enough so that everyone and even the non-technical persons can use them.

Applications can also be launched to exchange tokens, with our phones responding to the context of the token grantor. Finally, one phone may provide context to another to create a junction between them, allowing them to partake in a cross-device activity. We have implemented the Junction platform and written several applications for it, demonstrating the usefulness of programmable NFC on smart phones. This paper also concluded with wide range of application regarding NFC and its security concerns.

9. Acknowledgments

Thanks to Prof. R. R. Nimbalkar for his valuable support & guidance.

References

[1] NearFieldCommunication.org
[2] Kasper, Timo, Dario Carluccio, Christof Paar. "An Embedded system for practical security analysis of Contactless smartcards".
[3] Morris Dworkin, "Recommendation for Block Cipher Modes of Operation", NIST Special Publication 800-38A, 2001.
[4] NFC Forum (www.nfc-forum.org). Generic control record Type definition technical specification. 2007.
[5] ISO/IEC 18092(ECMA-340): Information technology – Telecommunications and information exchange between Systems - Near Field Communication - Interface and Protocol (NFCIP-1). First Edition, 2004-04-01.
[6] Ecma International: Standard ECMA-340, Near Field CommunicationInterface and Protocol (NFCIP-1), December2004,URL:http://www.ecmainternational.org/publications/standards/Ecma-340.htm.
[7] www.en.wikipedia.org/wiki/Near_Field_Communication.
[8] Ortiz, C. Enrique "An Introduction to Near-Field Communication and the Contactless Communication API", 2008-10-24.
[9] NFC protocol specification http://www.nfc-research.at

Author Profile

I received M.Tech in Information Technology from JNTU, 2014. My areas of interest are System Programming, Networking and Cloud Computing.

I received M.Tech in Information Technology from JNTU, 2014.My areas of interest are Discrete Mathematics, Database Engineering.

I received B.E in Computer Engineeringfrom Pune University in 2010. Myareas of interest are networking & Data Mining