ISSN: 2321-7782 (Online)
Volume 1, Issue 4, September 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

NFC: an overview

Sashi Suman
Student
Atria Institute of Technology
Bangalore – India

Abstract: ***Near Field Communication (NFC) is the next generation, low power wireless link, short-range communication technology, evolved from radio-frequency identification (RFID) tech that can transfer small amounts of data between two devices, held a few centimeters from each other. It has taken the network industry by storm. This technology isn't new as the concept was fore-thought. However its usage has been encouraged only in recent years, by various mobile companies.***

Keywords: Tags, Initiator, Bluetooth, Wireless, RF Field, Encryption, Data, Encryption.

I. INTRODUCTION

There was a time when we were amazed by Bluetooth and it's true that it changed the way we transfer files and information among compatible devices. No more the hassle of connecting wires and installing compatible drivers on the computer. Being Wireless, it has been a boon to the consumer and manufacturers alike. However there is the question of efficiency of this technology. Since the devices involved in Bluetooth Pairing need to activate themselves first, only then the file/information transfer occurs, this involves considerable wastage of energy; switching on one of the device and then waiting for the other and then later, switching off the Bluetooth on both the devices; this leads to wastage of the limited power in the portable devices. NFC solves this problem in a very simple way. Don't activate the connection, until both the devices are at a CLOSE proximity to each other.

The main objective of the paper is to understand the NFC technology and its benefits. The remainder of this paper is organized as follows: section 2 contains the setup and working of connection through NFC, section 3 list the usage of NFC in our daily lives, section 4 introduces the benefits, section 5 presents its security aspects, section 6 is the conclusion and section 6 list the references to this paper.

II. SETUP AND WORKING OF NFC

NFC is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. Communication between two NFC enabled handsets is started and completed with a simple proximity wave or touch of the two devices to each other. NFC operates at 13.56 MHz and at rates ranging from 106 kbit/s to 424 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target [1]. It uses magnetic induction between two loop antennas located within each other's near field, effectively forming an air-core transformer. The diagram below shows the basics of data transmission with NFC.

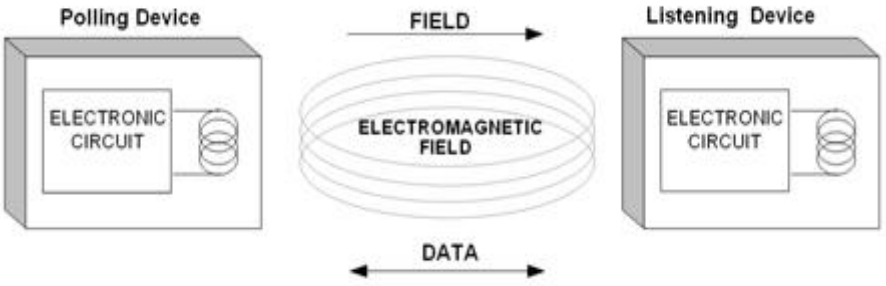

Fig. 1 Information Exchange between the devices (Image from Rohde & Schwarz's NFC white paper) [2]

The significant advantage of NFC over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify Bluetooth devices, the connection between two NFC devices is established at once (less than 1/10 second).There is two modes:

A. ***Passive communication mode:*** The initiator device provides a carrier field and the target device answers by modulating the existing field. In this mode, the target device may draw its operating power from the initiator-provided electromagnetic field, thus making the target device a transponder.

B. ***Active communication mode:*** Both initiator and target device communicate by alternately generating their own fields. A device deactivates its RF field while it is waiting for data. In this mode, both devices typically have power supplies.

NFC operates at slower speeds than Bluetooth, but consumes far less power. NFC sets up more quickly than standard Bluetooth, but has a lower transfer rate than Bluetooth low energy. Moreover, due to its shorter range, NFC provides a higher degree of security than Bluetooth and makes NFC suitable for crowded areas.

The real power of NFC relies in combining with contact less smart card infrastructure. The mobile handset user can make transactions just by touching his phone to a NFC credit card reader or ticket gate. The communication can also imply passive parts also in the form of an NFC tag, these tags gains power from the RF fields emitted by an active NFC device, for the communication.

III. Uses of RFC in Normal Life

A. ***Passive NFC tags or Contact less Smart Cards:*** This entitles the devices as passive parts, wherein the tags would remain 'inactive' until an active NFC device comes near them. Such inactive devices contain stored information, to be read by the Active devices. Passive NFC 'tags' on posters, in shops and on trains could contain a web address, a discount voucher, a map or a bus timetable that passers-by could touch their phones on to receive – or to instantly pay for absolutely anything.[3]

B. ***NFC enabled smart phones or handheld devices:*** These would entitle the 'Active' devices, which would read information from the passive NFC tags, or from other Active NFC device.

C. ***NFC enabled infrastructure/readers*:** Normally such devices are POS terminals, public transit gates, industrial equipment; the mobile handset user can make transactions just by touching his phone to a NFC credit card reader or ticket gate.

IV. KEY BENEFITS OF NFC

NFC provides a range of benefits to consumers and businesses, such as:

- ***Intuitive*:** NFC interactions require no more than a simple touch.
- ***Versatile*:** NFC is ideally suited to the broadest range of industries, environments, and uses.
- ***Open and standards-based*:** The underlying layers of NFC technology follow universally implemented ISO, ECMA, and ETSI standards.
- ***Technology-enabling*:** NFC facilitates fast and simple setup of wireless technologies, such as Bluetooth, Wi-Fi, etc.).
- ***Inherently secure*:** NFC transmissions are short range (from a touch to a few centimeters).
- ***Interoperable*:** NFC works with existing contact less card technologies.
- ***Security-ready*:** NFC has built-in capabilities to support secure applications [4].

V. 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.

A. ***Eavesdropping*:** 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 the second option is secure channels. When a secure channel is established, the information is encrypted and only an authorized device can decode it.

B. ***Data Corruption and Manipulation:*** 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.

C. ***Interception Attacks:*** Similar to data manipulation, interception attacks take this type of digital crime one step further. A person acts as a middleman between two NFC devices and receives and alters the information as it passes between them. This type of attack is difficult and less common. To prevent it, devices should be in an active-passive pairing.

D. ***Theft:*** No amount of encryption can protect a consumer from a stolen phone. If a smart phone is stolen, the thief could theoretically wave the phone over a card reader at a store to make a purchase. To avoid this, smart phone owners should be diligent about keeping tight security on their phones. By installing a password or other type of lock that appears when the smart phone screen is turned on, a thief may not be able to figure out the password and thus cannot access sensitive information on the phone [5].

While it may seem like NFC would open up a world of new security risks, it may actually be safer than a credit card. If a user loses her credit card, a criminal can read the card and find out the owner's information. If that same person loses her smart phone and has it password protected the criminal cannot access any private info. Through data encryption and secure channels, NFC technology can help consumers make purchases quickly while keeping their information safe at the safe time.

VI. Conclusion

The advantages of NFC far outweigh the limitations that we've seen till now. It's an Innovative step towards the Wireless connection establishment in our daily lives. Pairing with devices has never been so easy and efficient. Though it'd take some time before this technology gets completely absorbed in our lives, its future does appear very promising. Although it is new, the logic is sound and will remain a Guiding Beacon for generations to come.

References

1. Nosowitz, Dan (1 March 2011). "Everything You Need to Know About Near Field Communication". Popular Science Magazine. Popular Science. Retrieved 14 June 2011.
2. http://cdn.rohde-schwarz.com/dl_downloads/dl_application/application_notes/1ma182/1MA190_5E_NFC_WHITE_PAPER.pdf
3. http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410
4. http://www.nfc-forum.org/aboutnfc/
5. http://www.nearfieldcommunication.org/nfc-security.html

Author Profile

Sashi Suman, is currently studying in Atria Institute of Technology, affiliated to through VTU, Belgaum. He is pursuing his degree in Computer Science Engineering. His ambitious and helping nature has made him one of the favourite students of the department, among the lecturers and classmates alike.

