International Journal of Advance Research and Innovation
Vol. 1(2), Apr-Jun 2013, pp. 32-35
Doi: 10.51976/iiari.121308

Article Info
Received: 01 Aug 2012 | Revised Submission: 22 Aug 2013 | Accepted: 28 Aug 2013 | Available Online: 20 Sept 2013

Near Field Communication: a Review

*Navneet Verma**

ABSTRACT

The current state of the consumer electronics can be characterized by moving from a single purpose device to multifunctional devices and by moving from an isolated device to networked devices. In this last respect, it is important that people do not face the complexities of setting up network connections between devices. Cumbersome network settings can possibly be dealt with in the computer world but certainly not in the consumer electronics world.

Keywords: *Near Field Communication; NFCIP-1 Wireless Devices; Faster Protocols; Bluetooth; Wireless Ethernet; PDA.*

1.0 Introduction

Today, various public transport agencies in Europe, the United States, and Japan have piloted and implemented the use of NFC-enabled mobile phones. NFC [1][2] is used in the context of transport ticketing in gateless systems to enable a simple start-up program. Other trials have added retail contactless payment cards to the ticketing options. Multiple applications, including online payment and over-the-air ticketing, have also been enabled by the phone. The following sections give a general overview of the use of NFC technology and its application in a transport and ticketing environment.

NFC is a standards-based, short-range wireless [12][15]116] connectivity technology that enables simple and intuitive two-way interactions between electronic devices. With NFC technology, consumers can perform contactless transactions, access digital content and connect NFC-enabled devices with a single touch.

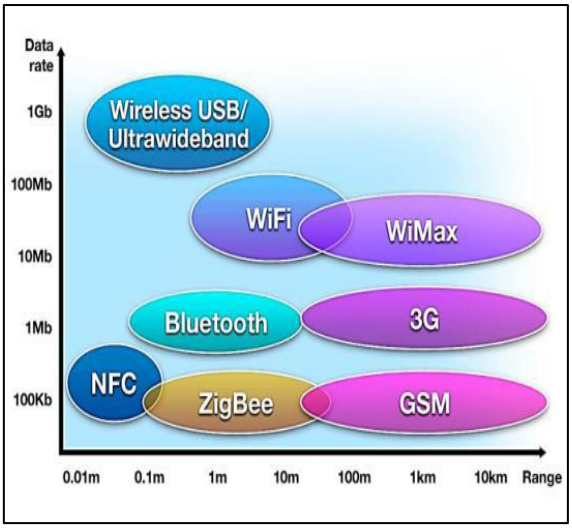
NFC simplifies setup of some longer-range wireless technologies, such as Bluetooth and Wi-Fi. It is also compatible with the global contactless standards [2][3](ISO 14443 and/or ISO 18092), which means transport agencies that have already deployed contactless programs enjoy a built-in advantage, as their equipment may readily interact with NFC enabled mobile devices and provide richer services.

The following chart shows how NFC compares in range and speed with other wireless technologies that can beused in a mobile phone.

1.1. Transfer of content

Let's say you went somewhere on a trip and you took lots of pictures with your Mobile phone or camera and you want to show them to your friends on a big screen like TV or LED.

Fig 1: NFC Compares with Other Wireless Technologies



**Corresponding Author: Department of Electronics and Communications, Shri Venkateshwara University, Gajraula, U.P, India (E-mail: navneetverma.cet@gmail.com)*

Fig 2: Take Picture

And show it on the TV by touching the "hot spot" of the TV with the Mobile Device.

Fig 2.1: Show Picture on Big Screen.

Let's take another example. If you have a PC and a mobile phone equipped with NFC, you can easily download a new game from a website directly onto this mobile phone for your kid using NFC. And this same principle will work for any sort of data transfer between two pieces of equipment when they support NFC. There is no need to set up communication manually provided that the applications are capable of handling the communication. This opens countless possibilities for content transfer and management of personal data stored within different types of consumer electronics equipment.

2.0 NFC with Other Protocols

Imagine that you would like to transfer a large amount of information between two computers – a desktop and a laptop. Let's say you want to transfer a presentation file. Using NFC may be slow and we decide to use something with more bandwidth. Let's say for this example we use Bluetooth. Now, to set up Bluetooth communication [22] between two computers we would need to set it up manually with a password to protect the communication. Using NFC [1] [2] we can set up this communication by simply touching the two computers:

Fig 3: A Set up of Communication for Other Protocols

Touch the computers at the "hot spot". They will open a connection to exchange the parameters of the Bluetooth communication and establish a secret key. The Bluetooth communication is established as a second step of this procedure without any human interference using the exchanged parameters.

Fig 3.1: A Set up of Communication for Other Protocols

Now the computers can be put away from each other but the communication continues using the session of Bluetooth that was established previously.

3.0 The Protocol

The protocol is based on a wireless interface. There are always two parties to the communication; hence the protocol is also known as peer-to-peer communication protocol. The protocol establishes wireless network connections between network appliances and consumer electronics devices.

The interfaces operate in the unregulated RF band of 13.56 MHz. This means that no restrictions are applied and no licenses are required for the use of NFC [1] [2] [3] devices in this RF band. Of course, each country imposes certain limitations on the electromagnetic emissions in this RF band. The limitations mean that in practice the distance at which the devices can connect to each other is restricted and this distance may vary from country to country. Generally speaking, we consider the operating distances of 0~20 cm.

NFC protocol [22] [26] distinguishes between the Initiator and the Target of the communication. Any device may be either an Initiator or a Target. The Initiator, as follows from the name, is the device that initiates and controls the exchange of data. The Target is the device that answers the request from the Initiator.

NFC protocol also distinguishes between two modes of operation: Active mode and Passive mode. All devices support both communication modes. The distinction is as follows:

- In the Active mode of communication both devices generate their own RF field to carry the data.
- In the Passive mode of communication only one device generates the RF field while the other device uses load modulation to transfer the data. The protocol specifies that the Initiator is the device responsible to generate the RF field.

The application sets the initial communication speed at 106, 212 or 424 Kbit/s. Subsequently the application and/or the communication environment may require speed adaptation, which can be done during communication.

NFCIP-1[5] [6] [7] [9] uses different modulation and bit encoding schemes depending on the speed. While establishing the communication, the Initiator starts the communication in a particular mode at a particular speed. The Target determines the current speed and the associated low-level protocol automatically and answers accordingly.

4.0 Conclusion

This paper presents a high level perspective on different NFC applications that can be used in the public transit industry. The Smart Card Alliance Transportation Council has prepared this white paper to foster greater understanding of NFC technology, explain its role in the transit industry.NFC technology has the potential to redefine the mobile arena by offering new opportunities for people to communicate, make purchases, and access information. However, the complexity of the NFC ecosystem and the challenges of widespread deployment have so far limited NFC deployment primarily to pilot testing.

References

[1] About nfc. (2012). Retrieved from http://www.nfc-forum.org/aboutnfc/

[2] Coskun, V., Ok, K., & Ozdenizci, B. (2012). , Near field communication from theory to practice [Kindle PC app]. Retrieved from Amazon.com

[3] Definition of: Rfid. (2012). Retrieved from http://www.pcmag.com/encyclopedia_term/0,2542,t=RFID&i=50512,00.asp

[4] Thangham, C. (2007, October 31). World's smallest and thinnest rfid tag is powder made by hitachi. Retrieved from http://digitaljournal.com/article/244321/World_s_smallest_and_thinnest_RFID_tag_is_powder_made_by_Hitachi

[5] Rfid tag characteristics. (2012). Retrieved from http://www.zebra.com/id/zebra/na/en/index/rfid/faqs/rfid_tag_characteristics.html

[6] Iso/iec 18092:2004. (n.d.) Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38578

[7] Planck, S. (2011, August 11). Nfc tag everything, respect nothing. nfc tag prices coming down to a sub 5 cent price point.

Retrieved from http://www.nfcrumors.com/08-12-2011/nfc-tag-everything-respect-nothing-nfc-tag-prices-coming-down-to-a-sub-5-cent-price-point/

[8] Wang, J. (2012, December 21). Transforming business with mobile payments Retrieved from http://www.entrepreneur.com/article/222459

[9] Duprey, R. (2011, December 27). Wall Street's best hidden stocks Retrieved from http://www.fool.com/investing/general/2011/12/27/wall-streets-best-hidden-stocks.aspx

[10] Nxpinvestors relations. (2012). Retrieved from http://investors.nxp.com/phoenix.zhtml?c=209114&p=irol-IRHome

[11] Identiveinvestors relations. (2012, April 23). Retrieved from http://www.identive-group.com/en/index.php?option=com_content&view=article&id=66&Itemid=89

[12] Nxpi. (2012). http://seekingalpha.com/symbol/nxpi?source=search_general&s=nxpi

[13] NFC Forum: www.nfc-forum.org

[14] NFC World: www.nfcworld.com

[15] NFC Nokia: http://europe.nokia.com/nfc

[16] Office of the Information and Privacy Commissioner (IPC) of Ontario, Canada: www.ipc.on.ca

[17] Privacy by Design (PhD): www.PrivacybyDesign.ca

[18] Chris Foresman, "Near Field Communications: a technology primer," ArsTechnica (February2011), at: http://arstechnica.com/gadgets/guides/2011 /02/near-field-communications-a-technology-primer.ars

[19] B. Joan, (n.d.). "Difference Between RFID and NFC," Difference Between. Retrieved 2011, at www.differencebetween.net/technology/difference-between-rfid-and-nfc/

[20] Harley Geiger, Center for Democracy and Trust, NFC Phones Raise Opportunities, Privacy and Security Issues (2011), at: www.cdt.org/blogs/ Harley-geiger/nfc-phones-raise-opportunities-privacyand-security-issues

[21] Attacking NFC Mobile Phones," 2008 at: www.mulliner.org/nfc/feed/collin_mulliner_eusecwest08attacking_nfc_phones.pdf

[22] Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones," International Conference on Availability, Reliability and Security, IEEE Computer Society, 2009, at www.mulliner.org/collin/academic/publications/vulnanalysisattacksnfcmobilephones_mulliner_2009.pdf

[23] Christian Kantner, Josef Langer, Gerald Madlmayr, Josef Scharinger, "NFC Devices: Securityand Privacy," The Third International Conference on Availability, Reliability and Security, IEEE Computer Society, 2008, at:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4529403

[24] Dr. Marnix Dekker and Dr. Giles Hogben, European Network and Information Security Agency (ENISA),

[25] Appstore security: 5 lines of defense against malware (2011), at: www.enisa.europa.eu/act/application-ecurity/smartphone-security-1/appst ore-security-5-lines-of-defenceagainst-malware

[26] Smart phones: Information security risks, opportunities and recommendations for users (2010), at www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunitiesand-recommendations-for-users