NEAR FIELD COMMUNICATION (NFC) TECHNOLOGY: A SURVEY

Anusha Rahul[1], Gokul Krishnan G[2], Unni Krishnan H[3] and Sethuraman Rao[4]

Amrita Center for Wireless Networks and Applications, Amrita Vishwa Vidyapeetham, Kollam, Kerala, India

ABSTRACT

Near Field Communication, NFC- is one of the latest short range wireless communication technologies. NFC provides safe communication between electronic gadgets. NFC-enabled devices can just be pointed or touched by the users of their devices to other NFC-enabled devices to communicate with them. With NFC technology, communication is established when an NFC-compatible device is brought within a few centimetres of another i.e. around 20 cm theoretically (4cm is practical). The immense benefit of the short transmission range is that it prevents eavesdropping on NFC-enabled dealings. NFC technology enables several innovative usage scenarios for mobile devices. NFC technology works on the basis of RFID technology which uses magnetic field induction to commence communication between electronic devices in close vicinity. NFC operates at 13.56MHz and has 424kbps maximum data transfer rate. NFC is complementary to Bluetooth and 802.11 with their long distance capabilities. In card emulation mode NFC devices can offer contactless/wireless smart card standard. This technology enables smart phones to replace traditional plastic cards for the purpose of ticketing, payment, etc. Sharing (share files between phones), service discovery i.e. get information by touching smart phones etc. are other possible applications of NFC using smart phones. This paper provides an overview of NFC technology in a detailed manner including working principle, transmission details, protocols and standards, application scenarios, future market, security standards and vendor's chipsets which are available for this standard. This comprehensive survey should serve as a useful guide for students, researchers and academicians who are interested in NFC Technology and its applications [1].

KEYWORDS

Near Field Communication, RFID

1. INTRODUCTION

Nowadays the increasing mobility of devices provided by mobile communications has become an important feature in the emerging technical world. Before the introduction of Near Field Communication (NFC) technology, the mobile phones already had several types of communication options with the external environment .When the mobile phones were introduced, the primary need was to setup voice communication, it was primarily provided by Global System for Mobiles (GSM) which has other services such as SMS, MMS and even internet access. Later Bluetooth technology was introduced that connects peripherals with computing devices including mobile phones [2]

In present days, a new communication technology known as NFC is becoming popular in mobile smart phones. This technology needs two NFC compatible devices placed very near to each other (less than 4cm) in order to communicate. NFC operates at 13.56 MHz and can transmit

information up to a maximum rate of 424 Kbits per second [3]. In an NFC communication, two devices are needed. First device is called the initiator which is an active device and is responsible for starting the communication, whereas second device is called the target and responds to the initiator's requests. The target device may be active or passive. The communication starts when the active device gets close to the target and generates a 13.56 MHz magnetic field and powers the target device [3, 4] (See Figure 1).The NFC technology works via magnetic field induction and operates on an unlicensed radio frequency band. Also it includes an embedded energy source component whereas the target can be a RFID card, tag or an NFC device which gives the reply to initiator's request [5].

The remaining part of this paper is structured as follows. Section II gives a clear idea about NFC hand over, working principle and data transmission. Section III discusses about NFC protocols and standards. Section IV discusses about the various NFC operation modes. In Section V we give an overview of NFC security including the potential threats in NFC technology and solutions. In Section VI we discuss about the worldwide NFC application. Section VII covers NFC setup and Section VIII talks about NFC vendors and manufacturers.

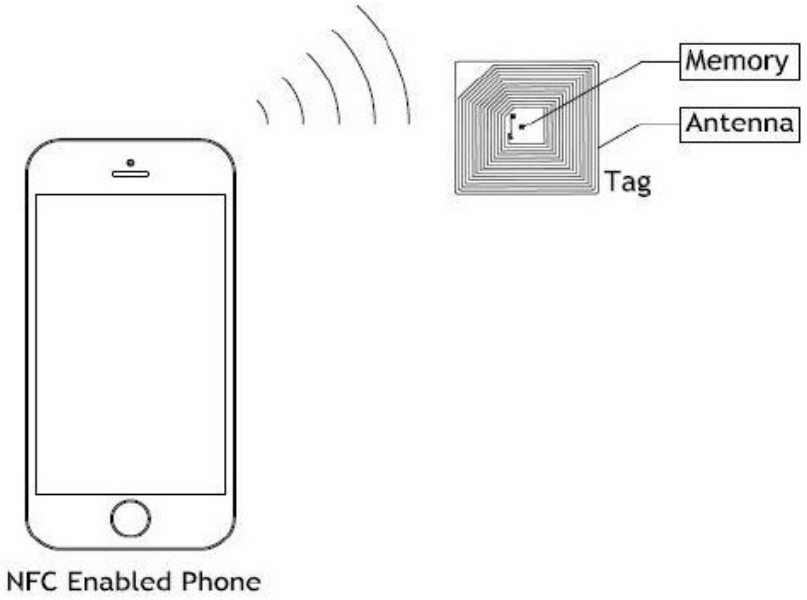

Figure 1: NFC Enabled Phone

2. NFC HANDOVER, WORKING PRINCIPLE & DATA TRANSMISSION

In NFC technology the communication is initiated with NFC but later the transmission is done by some other technologies such as Wi-Fi/Bluetooth. The two handover mechanisms specified by NFC forum are negotiated handover and static handover. In the first case, the initiator (handover requester) sends a handover request to target device (handover selector) which might support multiple carriers such as Wi-Fi/Bluetooth. Target device sends a response to the requester, i.e. initiator (see Figure 2). NFC requester device can select the best possible carrier that is compatible with both devices when it receives the response message. In static hand over method, handover selector device does not comprise an NFC Forum device but has a NFC Forum tag attached which gives memory space that can be read or written [6]. The main advantage of NFC

over Bluetooth is that it consumes far less power and doesn't require pairing but the highest data transfer rate of NFC (424 Kbit/s) is lesser than that of Bluetooth V2.1 (2.1 Mbit/s) [1].

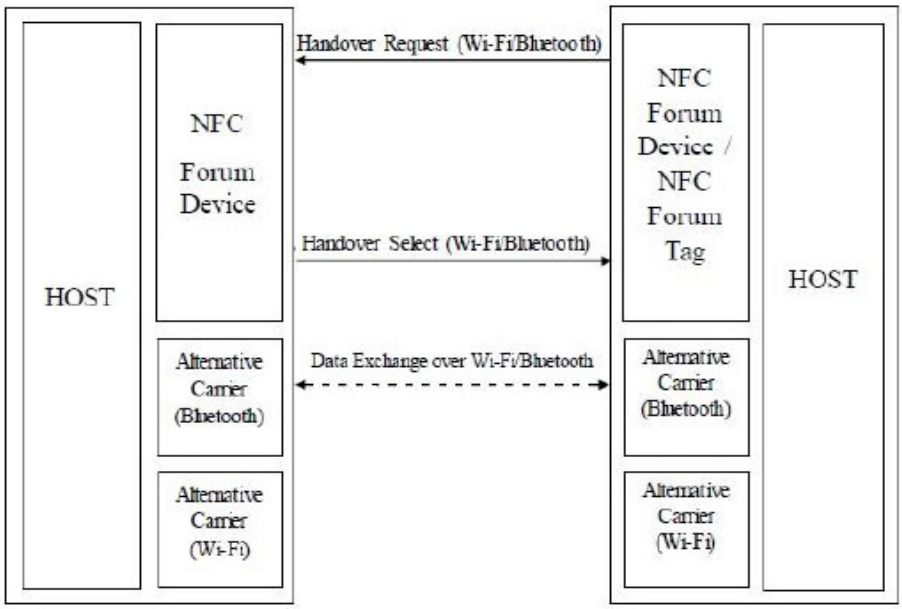

Figure 2: NFC Handover

NFC uses an inductive coupling technique comparable to the transformer principle i.e. the magnetic near-field of two conductor coils is used to pair the initiator (Polling) device and target (Listener) device (See Figure 3). In this pairing of the coils of initiator and target, a passive listening device also affects the active polling device. A variation in the impedance of the listening device results in an amplitude or phase changes to the antenna voltage of the polling device, detected by the polling device [7].

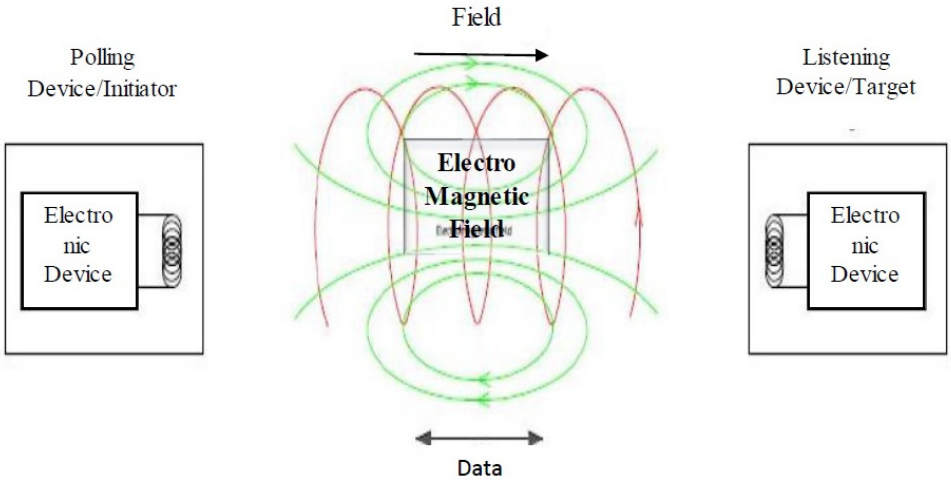

Figure 3: NFC Transmission

3. NFC PROTOCOLS AND STANDARDS

The NFC protocol needs standardization in order to be accepted by the industry for commercialization and provide for compatibility between the devices produced by different vendors. Standardization means keeping the specifications open and stable, and accessible for everyone, also facilitating the protocol analysis and device adaptation for various purposes. The standards are published by ECMA International and ETSI standards. The three standards ISO/IEC 14443 A, ISO/IEC 14443 B and JIS X6319-4 are RFID standards which have been prompted by different companies (NXP, Infineon and Sony) [4,7].

- ISO-IEC Protocol

ISO/IEC 14443 is a series of international standards used for international interchange that describes the parameters for identification cards as described in ISO/IEC 7810. It also gives a detailed information about polling for proximity cards into the field of a nearest coupling device, the initial request and reply command content, techniques to sense and communicate with one proximity card amongst several proximity cards and other parameters necessary to initialize communications between a proximity pairing device which can be the initiator or target and a proximity card. Protocols used by upper layers and by applications which are used after the primary phase is detailed in ISO/IEC 14443-4 [8].

- ISO 15963

This Standard gives information about the numbering systems that are accessible for the recognition of RF tags used for the traceability of the IC and RF tag which is used for the close evaluation in a multi-antenna configuration

- ISO 18000:

This standard has 2 mode of procedure, proposed to address diverse applications [3].

- ISO 18092(NFCIP-1) or ECMA 340

This Standard describes active and passive communication modes for NFC protocol and interface. This gives the specifications of coding, modulation schemes, frame format, transfer speeds of the RF interface, initialization schemes and surroundings required for data collision control through initialization [8].

4. NFC OPERATION MODES

NFC technology defines two types of devices. One is initiator device and other is target device. Initiator device is one who initiates the communication and controls the data exchanges. Target device is the device who responds to the initiator device. Active and Passive are the two operating modes of NFC [13]. In active mode, both the initiator and the target generate the RF signal on which the data is carried. In passive mode, RF signal is generated only by the initiator, and target communicates back to the initiator using a technique called load modulation. NFC uses two types of coding mechanism to transfer data, they are Manchester and Miller coding.
In addition to the two operating modes, there are three operating modes for device communication [14]. These three modes depend on the application. Figure 4 shows three operating modes of NFC technology standard.

4.1. Reader/Writer mode

In Reader/Writer mode of operation the application transfers data in NFC forum defined message format. In this mode the NFC enabled mobile phone can perform read/write operation on NFC tags. In Reader Mode, NFC initiator reads data from the NFC tag where as in the writer mode, initiator writes data in to the tag. It should be noted that Reader/Writer mode of communication is not secure. The applications supported by this mode are,

- Smart Poster
- Remote Marketing
- Remote Shopping
- Social Networking
- Location based services

Figure 4: NFC Operating Modes

4.2. Card Emulation Mode

In card emulation mode, the NFC enabled mobile device acts as a contactless smart card. The examples of smart card are debit card, credit card, access cards etc. Data transfer in this mode is highly secure. This mode supports the following applications.

- Payment
- Loyalty
- Ticketing
- Access control
- Identity Services

4.3. Peer to Peer mode

Peer to peer mode supports link level communication. It supports two NFC enabled device to exchange information such as a text message, contact record or data of any other kind. NFCIP-1 and LLCP are the two standardized options in peer to peer mode. This mode of communication is secure. The applications supported by this mode are the following.

- Exchanging Data
- Money Transfer
- Social Networking

5. NFC SECURITY

5.1. Threats

NFC applications such as contactless money payment demand a high level of security. As NFC security has great importance, so it is to be a part of the basic NFC technology structure. Possible threats associated with NFC are explained below.

5.2. Eavesdropping

Eavesdropping is a common threat found in all wireless communication technologies. NFC is also a wireless communication interface between two entities [10]. They use RF signals to communicate, so any equipment with an antenna in the range can receive the signal. The attacker can extract the information from the signal transmitted through experimentation and periodic analysis processes. This is very dangerous in the case of money payments, where the users use some secret password; the eavesdropper acquires this information and can misuse it. It is very difficult to prevent eaves dropping as the attacker who uses a very precise antenna can receive the signal even if the signal strength is too weak. The only solution to eavesdropping is to use a secure channel for communication.

5.3. Data Corruption and Manipulation

In NFC, data is sent from sender to receiver wirelessly. There are some specific formats for data to be sent, so that the receiver accepts and decodes it [11]. The data which is not in the correct format is rejected. Data corruption and manipulation attack arises when an attacker in between corrupts or manipulates the data. The attacker may change the data format or change the contents in it, so that the data becomes useless or gets rejected as it reaches the receiver. For some coding schemes this attack is possible. The solution for this attack is to use a secure channel between the communicating parties.

5.4. Man- in- the Middle attack

Man in the middle attack is one step further to data corruption and manipulation attack. In this attack a third party intercepts the communication between two parties [12]. The attacker acts as a relay between the sender and receiver and forwards data (See Figure 5). The attacker can corrupt, alter, or discard the data being sent. Man in the middle attack is very difficult to achieve in NFC links and so it is not common. The solution for this attack is to use active-passive communication mode.

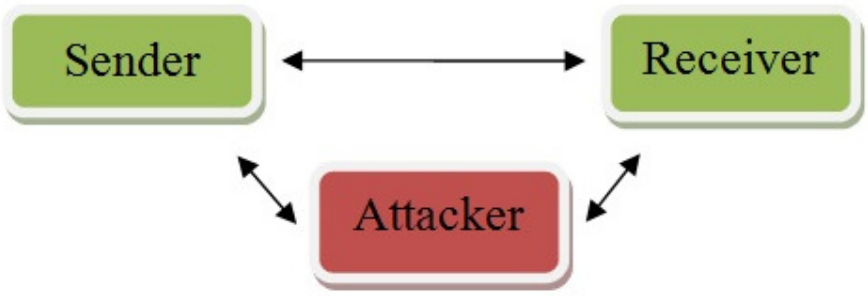

Figure 5: Man in the middle attack

5.5. NFC Worm

NFC worm attack is found in NFC enabled phones. In this the PushRegistry can be abused to intercept all URI NDEF messages. It is done by utilizing the standardized NFC Java API [21]. Push Registry helps the applications to register themselves for handling some specific data like images

5.6. Solutions

Establishing a secure channel between the sender and the receiver is the best solution for eavesdropping, data corruption and manipulation attacks. As NFC is having inherent protection against man in the middle attack, it is an easy task to setup. A shared key can be obtained between sender and receiver using Diffie –Hellman based on RSA or elliptical curve. This shared key can be used to derive a symmetric key like 3DES or AES. The symmetric key can be used to enable a secure channel between the communicating entities. NFC specific key agreement mechanism is also there, which is of less computational cost for establishing a secure channel.

6. OVERVIEW OF NFC APPLICATIONS

This section provides an overview of NFC applications in the real world (See Figure 6) such as in retail, automotive, office, terminal, theatre/ stadium etc. NFC technology is used for the purpose of ticketing, payment, sharing (share files between phones), service discovery i.e. get information by touching smart phones etc.

Some of the advantages of NFC to industrial applications are listed below [8]:

- NFC enables touch based and easy communication between two devices.
- Communication setup with NFC takes milliseconds order of time whereas for Bluetooth it is typically in seconds order.

NFC enables longer lifetime of the sensor battery in wireless sensor applications, or even battery less implementation of the sensor.

Figure 6: NFC Applications

6.1. NFC Ticketing

In NFC Ticketing, the user needs to carry a NFC enabled mobile phone to read and store the ticket or access code from the reader [22]. There is a ticketing sever to which a NFC reader is connected. The user can read the ticket from the reader and store it (See Figure 7).

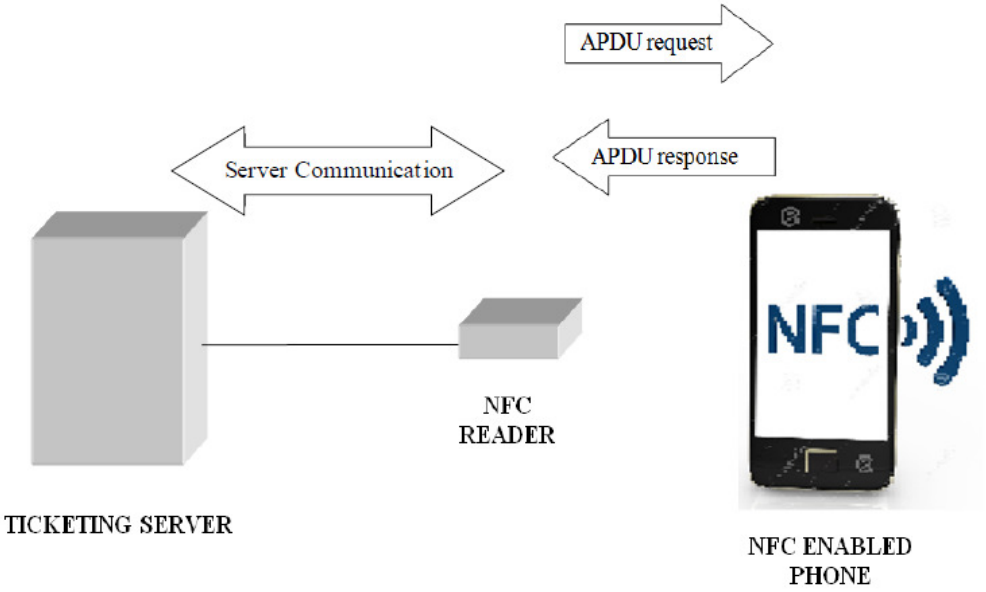

Figure 7: NFC Ticketing

6.2. NFC Mobile Payment System

In NFC Mobile Payment System, credit card or debit card essentials of the user are stored in the secure element which is built in the OS. The merchant's NFC reader can read the essentials to transfer the money from the account to finish the payment (See Figure 8).

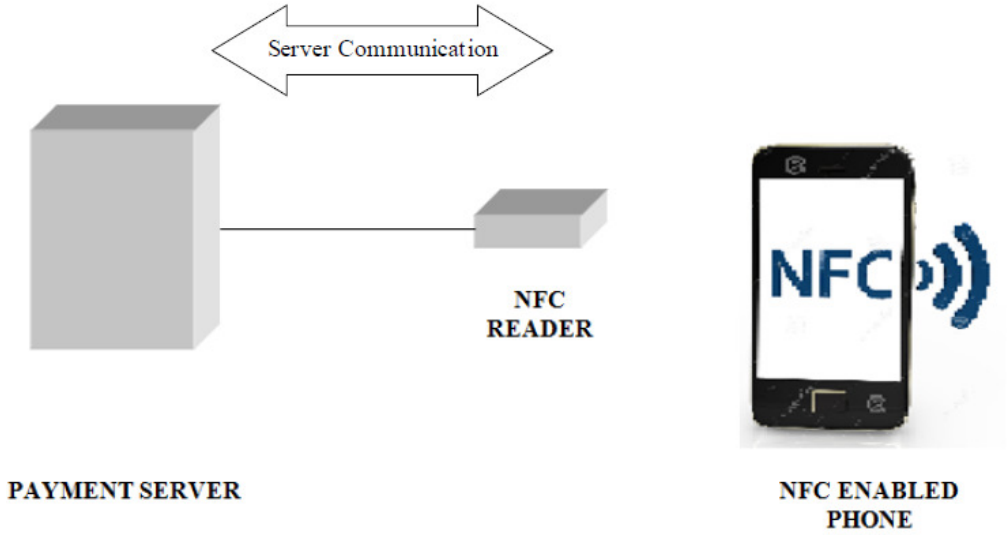

Figure 8: NFC Mobile Payment

7. NFC SETUP

Those who wish to use NFC must own an NFC compatible device or buy a SIM card or SD card with an NFC chip installed on it [20]. So with this, one can communicate with other NFC devices and tags. Most common operating systems used on NFC devices are android OS and Apple's iOS. Users can activate Google wallet that is pre - installed on NFC compatible android phones. Other android applications like PayPal's mobile app, NFC payments can be downloaded from sites like play store. Money transfer can be done by keeping two devices close to each other. Note that it is very important to make your phone protected with a password, to prevent a thief from unlocking the phone and using services such as Google Wallet to purchase items or send money from the owner's PayPal account to the thief's own account.

8. NFC VENDORS AND MANUFACTURERS

There are many vendors that have been working on NFC. Some of the names and their chipsets are given in Table I. [15], [16], [17], and [18]. This is only for understanding of companies that are manufacturing NFC chipsets and most of them are not available for retail sale.

Among these companies HTC and Xiaomi are using NFC controllers from NXP and Broadcom [15]. Except Inside secure and MediaTek chipsets, all others will support full duplex mode of communication. The prices of all chipsets are almost the same. Among them, Sony's chipset is expensive which is used in Sony's NFC one touch remote [18] and NXP's PN544 gives high level of integration and greater flexibility. Also it supports a number of RF protocols [16].

Table 1: NFC Vendors and Manufacturers

Sl No	Manufacturer / Vendor	Model	Price
1	Broadcom	BCM206794	US $18
2	NXP	PN544	US $8.68
3	NXP	NTAG203	US $8.2
4	Samsung Electronics	S3FHRN2	12.28 Euro
5	Sony	RC S330	US $28.33
6	HTC	NXP/Broadcom	
7	Xiaomi	NXP/Broadcom	
8	STMicroelectronics	ST21NFCA	NA
9	Oberthur Technologies	Dragonfly	NA
10	Qualcomm	QCA1990	NA
11	MediaTek	MT6605	NA
12	Shangai Fudan Microelectronics[17]	FM1930	NA
13	Inside secure	VaultIC 150/150D	NA

9. FUTURE DIRECTIONS OF NFC SERVICES

Many applications of NFC are the extensions to current solutions. Wireless /Contactless payment and ticketing solutions are commonly available across the world and, are compatible with NFC enabled devices. Taking these applications to an appropriately equipped mobile device will be the next step in the adoption of NFC.

New generations gadgets such as iPad, iPhone and iPod are equipped with NFC technology [19]. Recently, Microsoft announced that all Windows8 Phone devices will make use of the NFC technology. Google's Smartphone app, Google Wallet, allows users to load entire credit card information and pay with the swipe of their phone. Visa and Samsung combined to create a NFC compatible Smartphone which will carry special content that aims to make purchases at the Olympic Games faster.

10. CONCLUSION

This paper covered the entire details of Near Field Communication (NFC) technology. NFC can be combined with existing infrared, Bluetooth technologies for improving the range of NFC. NFC offers a secure and simple way for transferring data between two electronic devices. Another advantage of NFC is its compatibility with RFID technology. NFC is actually based on RFID technology. RFID uses magnetic field induction to initiate communication between electronic devices in close vicinity.NFC operates at 13.56MHz and has 424kbps maximum data transfer rate. NFC is complementary to Bluetooth and 802.11 with their long distance capabilities. This paper discussed the concepts of NFC technology in a detailed manner including working, transmission details, protocols and standards, application scenarios, future market, security standards and vendors' chipsets available for this standard.

ACKNOWLEDGEMENTS

We thank God Almighty for his grace, for giving us strength and ideas for making this work flow smoothly.

REFERENCES

[1] NFC,Wikipedia,Available: http://en.wikipedia.org/wiki/Near_field_communication
[2] Vedat Coskun, Busra Ozdenizci, Kerem," A Survey on Near Field Communication (NFC) Technology" Wireless Personal Communications Volume 71, Issue 3 , pp 2259-2294
[3] NFC-Forum, Available: http://www.nfc-forum.org
[4] Ecma International, Near Field Communication - White Paper, 2005, Ecma/TC32-TG19/2005/012, Available: http://www.ecma-international.org/
[5] Esko Strömmer,Juha Pärkkä, Arto,Ilkka\Korhonen Ylisaukkooja, "Application of Near Field Communication for Health Monitoringin Daily Life", Proceedings of the 28th IEEE EMBS Annual International Conference, February 2006.
[6] NFC handover,Available:http://developer.nokia.com/community/wiki/NFC_Handover_working_principle
[7] Rohde & Schwarz, NFC technology and measurements White Paper, June 2011.
[8] Shyamal Pampattiwar,"Literature Survey on NFC, Applications and Controller", International Journal of Scientific & Engineering Research, Volume 3, Issue 2, February-2012
[9] Future of NFC, available: http://www.nearfieldcommunicationnfc.net/nfc-future.html
[10] NFC Security Available: http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-security.php
[11] NFC Security available: http://www.nearfieldcommunication.org/nfc-security.html
[12] Ernst Haselsteiner and Klemens Breitfuß, "Security in Near Field Communication (NFC) Strengths and Weaknesses"
[13] NFC operation modes available: http:// en.wikipedia.org/wiki/Near_field_communication.
[14] Ekta Desai and Mary Grace Shajan, "A Review on the Operating Modes of Near Field Communication", In proceedings of International Journal of Engineering and Advanced Technology (IJEAT), December 2012
[15] BCM206794, Available: www.broadcom.com/products/NFC/NFCSolutions/BCM2079x-Family
[16] PN544,Available:http://www.nxp.com/documents/leaflet/75016890.pdf
[17] FM1930, Available: www.fmsh.com/xqitadmin/uploadFiles/20130529043554.pdf
[18] RC S330, Available: www.sony.net/HOME/Products/USB NFC Reader
[19] Phone list using NFC, available: www.nfcworld.com/nfc-phones-list/
[20] Setting up NFC, Available: http://www.nearfieldcommunication.org/howto-setup.html
[21] Collin Mulliner, "Vulnerability Analysis and Attacks on NFC-enables Mobile Phones" International Conference on Availability, Reliability and Security, 2009
[22] Shyamal Pampattiwar, "Literature Survey on NFC, Applications and Controller" International Journal of Scientific and Engineering Research, Volume 3, Issue 2, 2012

AUTHORS

Anusha Rahul received B. tech degree in Information technology from Mahatma Gandhi University, India in 2006.She had more than 5 years teaching experience in India and Abroad. She is now pursuing her Post Graduation in Wireless Networks and Application from Amrita University, India. Currently she is working on wireless sensor networks based project for augmenting women's safety in women's only local intracity railway carriages.

Gokul Krishnan G received B.Tech degree in Electronics and Communication Engineering from Cochin University of Science and Technology, India in 2013. He is now pursuing his Post Graduation in Wireless Networks and Applications from Amrita University, India. Currently he is working in a project which is associated with National Knowledge Network (NKN)

Unnikrishnan H received degree in Electronics and Communication Engineering from Kerala University, India in 2012. He is now doing his Post Graduation in Wireless Networks and Application from Amrita University, India. Currently he is working in a project on Overtaking assistance System related to VANET Technology.

Prof. **Sethuraman Rao** is an associate professor at Amrita Center for Wireless Networks and Applications, Amrita University, Kollam, Kerala, India. He holds a Masters degree in Computer Science and a Bachelor's degree in Mechanical Engineering from IIT Madras, India. He has over 20 years of international experience in the networking industry having held technical and management positions at Juniper Networks, Alcatel-Lucent and a few startups. His areas of interest include wired and wireless LANs, wireless security, software engineering and network management.