



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

A Survey on Smart Phones with Near Field Communication Technology

P.Akalya

PG Scholar, Dept. of Computer Technology , Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu , India

ABSTRACT: Wireless technology revolutionized the entire world. Near field communication is an emerging technology whose strength is contactless communication. NFC is a short range wireless technology that is integrated into smart phones. This technology establishes radio communication between devices at a maximum distance of around 20cm or less. The Standards of NFC includes ISO/IEC 18092 and those defined by the NFC forum, which was founded in 2004 by Nokia, Philips and Sony, and now has more than 160 members. NFC technology enables users to perform safe, contactless transactions, access digital content and connects electronic devices simply by touching or bringing devices into close proximity. It validates secure data transfer. There are two modes of operation in NFC, they are ACTIVE MODE and PASSIVE MODE. Active mode allows communication between two Powered devices. Passive mode allows communication between a powered and a non self-powered device. This paper describes about the modes of operation in NFC, applications of NFC technology in contactless payments, information sharing, health care, social networking and transportation. It further describes about the security aspects in NFC technology.

KEYWORDS: Contactless communication, Modes of operation, Applications of NFC, Security aspects in NFC.

I.INTRODUCTION

As we are living in a digital world today, most of our daily activity involves the digital technology around us. Technology in the mobile industry has been moving towards integration of Near Field Communication (NFC) technology. Evolving from the RFID (Radio Frequency Identification) Technology, NFC is a promising short range high frequency contactless communication technology that facilitates mobile phone usage of billions of people throughout the world. It is a set of standards for smart phones and similar devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than a few centimetres. It uses electromagnetic radio fields to allow two compatible devices to exchange data and share information when passes close to each other. It offers diverse services ranging from payment and loyalty applications to access keys for offices and houses. It replaces many physical applications by communicating directly without any third-party server. NFC-enabled devices can simply point or touch their making application and data usage easy and convenient. Eventually NFC technology integrates all such services into one single mobile phone and makes it a whole lot easier to perform a huge range of digitized task.

II.RELATED WORKS

In [1] author proposes a set of multiple network functions are handled in the computer world, but not in the world of electronics. Using the protocol (NFCIP-1), according to which users of electronic devices, which provide the use of secure means of communication between various devices without effort is considerable intellectual in the formation of their own network concept is simple striking: According also to communicate between two devices, and bring them together, using Protocol NFCIP-1 and the wireless network to deal with them in the peer Baland and here is the exchange of configuration data using NFC, and here you cannot continue with the devices, some of the longer and faster than protocols such as Bluetooth or wireless Ethernet (Wi-Fi).

In [2] author analyze the problems that are encountered in mobile ticketing systems where proximity technologies are used for validation and check of the e-tickets, leaving out the stage of ticket purchase, which can be done either



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

remotely or in proximity. We have identified several security issues that are common in mobile ticketing and we propose some methods to solve them. In addition, we propose a protocol to provide secure validation and check of e-tickets. The innovation of this protocol is that it provides a good level of security and it is sufficiently abstract to be independent of NFC operating mode; that is it works in classical Card Emulation mode making use of Secure Element and it is implementable in Peer-to-Peer mode too.

In [3] author proposes that how a relay attack can be implemented against systems using legitimate peer-to-peer NFC communication by developing and installing suitable MIDlets on the attacker's own NFC-enabled mobile phones. The attack does not need to access secure program memory nor use any code signing, and can use publicly available APIs. Then describes that how relay attack counter measures using device location could be used in the mobile environment. These counter measures could also be applied to prevent relay attacks on con-tactless applications using 'passive' NFC on mobile phones.

In [4] author approaches security testing of NFC-enabled mobile phones. Testing approach takes into account not only the NFC-subsystem but also software components that can be controlled through the NFC-interface. Through testing approach, we were able to identify a number of previously unknown vulnerabilities, some of which can be exploited for spoofing of tag content, an NFC-based worm, and for Denial-of-Service attacks. Further it shows that findings can be applied to real world NFC-services.

III.GENESIS

The NFC standards and protocols are based on existing radio frequency identification (RFID) standards that includes ISO/IEC 14443 and Felica. The Standards of NFC includes ISO/IEC 18092 and the standards defined by the NFC forum, which was founded in 2004 by Nokia, Sony and Philips and now has more than 160 members. The GSMA (Global System for Mobile communicating Association) has also worked to define a platform for the deployment of "GSMA NFC Standards" for mobile handsets. GSMA's attempts include Trusted Service administrator, Single wire protocol, experimenting and documentation and secure element.

In 1983, the first patent to be associated to the abbreviation of RFID was granted to Charles Walton. In 2004, Nokia, Philips and Sony established the Near Field Communication (NFC) forum. Nokia 6131 was the first NFC phone which was launched in 2006. In 2009, NFC Forum released Peer-to-Peer standards which are used to transfer contact, URL and initiate Bluetooth. In 2010, Samsung launched its first Android NFC phone Nexus S. NFC became part of the Symbian mobile operating system in 2011 with the release of Symbian Anna version. In 2012 Samsung introduced the Smart Tags and stickers, which use NFC technology to change modes and profiles on a Sony smart phone at close range, included in the Sony Xperia P. In 2013, Samsung and Visa announced major partnership to develop mobile payments.

IV.WORKING OF NFC

NFC is based on RFID technology that operates at 13.56 MHz .It uses magnetic field induction to enable communication between two electronic devices in close proximity. NFC is similar to the working inductive coupling. NFC works using magnetic induction between two loop antennas located within each other's near field.NFC includes an initiator and a target. The NFC initiator i.e. a smart phone or other NFC compatible device produces a radio frequency field that interacts with an NFC tag found in compatible card readers and smart posters. The signal creates a current flow through the NFC tag and allows the device and the tag to communicate with each other. For two devices to communicate with each other using NFC, one device must have an NFC reader/writer and the other device must have an NFC tag. For peer to peer communication using NFC, both the devices must be powered. The NFC target takes very simply forms such as tags ,key fobs ,stickers or cards that are cheaper and do not require batteries. The target tag is an integrated circuit containing data and the tag is connected to an antenna, which can be read and written using the reader. The NFC tags contain data that can be read-only but they are also rewritable. The maximum transfer bit rate of an NFC tag is 800kbps. These tags are used to store personal data such as debit and credit card information, PINs and networking contacts securely when compared to the other information.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

V. MODES OF OPERATION

There are two modes of operation in NFC technology. They are ACTIVE communication mode and PASSIVE communication mode.

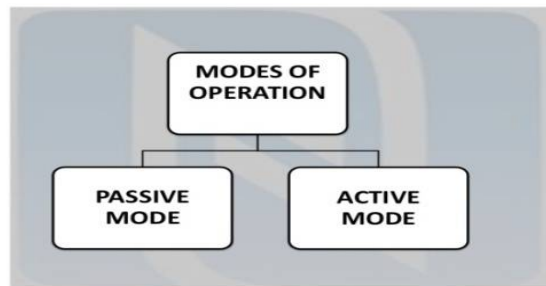


Fig 1.TWO MODES OF OPERATION

PASSIVE MODE (CARD EMULATION MODE):

The NFC device behaves like an existing contactless card conforming to one of the legacy standards. Here, the initiator device provides a carrier field and the target device answers by modulating surviving field. In this mode, the target device may draw its working control from the initiator supplied electromagnetic field. The NFC device appears to an external reader much the same as a traditional contactless smartcard. The NFC device behaves as a contactless smartcard. This enables contactless payments and ticketing by NFC enabled phones without changing the existing infrastructure.



Fig 2.PASSIVE MODE

ACTIVE MODE (READER/WRITER MODE):

The NFC device is active and reads or writes to a passive legacy RFID tag. Both initiator and target device communicate by alternately generating their own field. A device deactivates its RF field while it is waiting for data. In this mode, both the devices should have a power supply. The NFC device is capable of reading NFC Forum-managed tag types, such as a tag embedded in an NFC smart poster.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017



Fig 3.ACTIVE MODE

PEER-TO-PEER MODE:

Two NFC devices exchange information. Both devices take part in communication. The initiator device (polling device) requires less power compared to the reader/writer mode because the target (listener) uses its own power supply.

VI. COMPARISON WITH OTHER TECHNOLOGIES

NFC is compared with other technologies based on its range, usability, selectivity and consumer experience.

COMPARISON WITH OTHER TECHNOLOGIES				
	NFC	RFID	IrDa	Bluetooth
Set-up time	<0.1ms	<0.1ms	~0.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

Fig 4.COMPARISON WITH OTHER TECHNOLOGY

VII. SECURITY ASPECTS IN NFC

Security threats in current uses of NFC are well understood from similar applications in areas like content distribution, web browsing, and networking.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

- **PREVENTING UNAUTHORIZED TICKET SHARING:**
In the case of electronically presented service “tickets”, such as in public transportation or sports events without assigned seating, we have to ensure that users can not share their benefits with other parties.
- **SECURING BACKGROUND APPLICATION INVOCATION:**
The smart phone reading passive content over NFC will be a dominant mode of interaction. Several security principles underpin such operations both for the purpose of contextual application invocation. These principles derive from the analogy to browsing on the Internet and following links, we learn to be careful when navigating to unknown domains, and modern browsers offer much assistance in helping us make the correct decisions.
- **EAVESDROPPING:**
The RF signal for the wireless data transfer can be picked up with antennas. The distance from which an attacker is able to eaves drop the RF signal depends on many parameters, but it covers only a small distance.
- **LOST PROPERTY:**
Losing the NFC RFID card or the mobile phone will open access to any finder and act as a single-factor authenticating parameter. Mobile phones secured by a PIN code works as a single validating factor.

VIII. APPLICATIONS OF NFC

- **TRADE AND COMMERCE:**
A NFC device can be used for contactless payments.
- **SOCIAL NETWORKING:**
Sharing contacts, photos, videos or files etc.
- **SMARTPHONE AUTOMATION AND NFC TAGS:**
A Smart phones equipped with NFC can be paired with NFC tags or stickers which can be programmed by NFC apps to automate tasks.
- **NFC FOR BUSINESS:**
In case of business, it is used for staff communication, real time updates, improved customer service etc.
- **NFC FOR INDIVIDUALS:**
In case of individuals, it is used for information sharing, contactless payments, transportation, health care, social networking etc.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017



Fig.5.APPLICATION OF NFC

IX.ADVANTAGES OF NFC

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

1. **Adaptability:** NFC is ideally suited to the broadest range of industries and the environments.
2. **Open and Standards-based:** The fundamental layers of NFC technology follow universally implemented ISO, ECMA and ETSI standards.
3. **Technology -enabling:** NFC transmissions are secure due to short range communication.
4. **Interoperable:** NFC works with all the existing contactless technologies.
5. **Security:** NFC has a built-in capability to support secure applications.

X.FUTURE OF NFC

New generations of iPhone, iPod and iPad products would reportedly be equipped with NFC capability which would enable small-scale monetary transactions. In the future, near field communication technology has the potential to become a staple of our daily lives. NFC technology is compatible with a wide variety of devices, giving the opportunity for future growth unlimited. Already, NFC technology is beginning to be compatible with several different smart phone manufacturers allowing users to do things such as make payments or unlock their hotel room doors by simply using a smart phone. We believe NFC technology will continue to grow and become pervasive throughout our society.

XI. CONCLUSION

Mobile handsets are the major target for NFC and it will be implemented in most handheld devices. There are already smart phones on the market with NFC chips that will let you purchase items just by holding your phone near a reader at the cash register. It is not necessary to carry credit cards. Although NFC has the shortest range among radio frequency technologies, joining them with Bluetooth or infrared can rise its range of applications.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

ACKNOWLEDGEMENTS

Our sincere thanks to the experts supported this work and their valuable comments.

REFERENCES

1. Hussein Ahmad Al-Ofeishat, Mohammad A.A.Al Rababah. Near Field Communication (NFC).IJCSNS, Feb 2013
2. S. L. Ghiron, S. Sposato, C. M. Medaglia and A. Moroni. "NFC ticketing: A prototype and usability test of an nfc-based virtual ticketing application. Near Field Communication", International Workshop on, 0:45–50, 2009.
3. L. Francis, G. P. Hancke, K.Mayes and K.Markantonakis."Practical NFC Peer-to-Peer Relay Attack using Mobile Phones. In Workshop on RFID Security–RFID"Sec'10, Istanbul, Turkey, June2010.
4. C. Mulliner. "Vulnerability analysis and attacks on nfc-enabled mobile phones". Availability, Reliability and Security, International Conference on, 0:695–700, 2009.
5. A. Fressancourt, C. Herault, and E. Ptak. Nfcsocial: "Social networking in mobility through ims and nfc. Near Field Communication", International Workshop on, 0:24–29, 2009.
6. K.Preethi, Anjali Sinha, Nandini "Contactless Communication through Near Field Communication "IJARCSSE Volume 2, Issue 4, April 2012.
7. Mohamed Mostafa Abd Allah "Strengths and Weaknesses of Near Field Communication (NFC) Technology" Global Journal of Computer Science and Technology Volume 11 Issue Version 1.0 March 2011.