Overview of Near Field Communication & Secure Mobile System

Snehal H. Kuche, Ankur S. Mahalle

Abstract— Near field communication (NFC) is commonly used for Smartphone and similar devices to set up radio communication with each other by moving them together or bringing them into closeness, usually no more than a few inches. As mobile phone availability becomes being present everywhere at once around the world, the use of Mobile phone based patient terminals require an easy-to-use and able to move freely in all directions. To assemble these requirements a user interface idea based on mobile phones, social networking, social organization as well as medical sensor devices enabled with Near Field Communication. NFC is related or an acquired form of Radio Frequency Identification (RFID). Its working principal is technically based on RFID, which is closely related to Bluetooth device. Currently, it has applications mostly in the field of contactless electronic payment.

Index Terms— Frequency Identification (RFID), near field communication (NFC), Security, Radio

IJSER

1 Introduction

NEAR Field Communication (NFC) is a wireless connectivity technology and set of communication protocols that enables suitable short-range communication between electronic devices such as Smartphone. NFC protocols established a generally-supported standard and also easy to use target selection, by simply holding two or more than two devices close to each other shows in Fig1

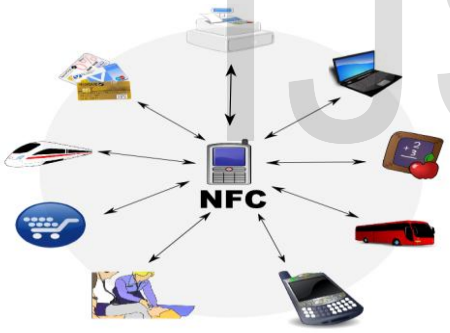


Fig.1. NFC connects different devices

NFC is the Wireless short range communication technology and low power wireless link acquired from radio-frequency identification (RFID) tech that can transfer small amounts of data between two devices. It is corresponding to Bluetooth, wifi and 802.11 with their long distance capabilities and also works in dirty environment.NFC interface can operate in two different modes: active and passive. In comes in both passive and active flavors, including Peer-to-Peer mode, exchanging information, such as business cards or contacts and Secure Element NFC where a machine recognizes a NFC phone as a bankcard.NFC builds upon RFID systems by allowing two-way communication between endpoints, where earlier systems such as contactless smart cards were one-way only. NFC has used for data transfer or 'data beaming' in applications such as smart posters or communication methods such as Wi-Fi or Wi-Max.

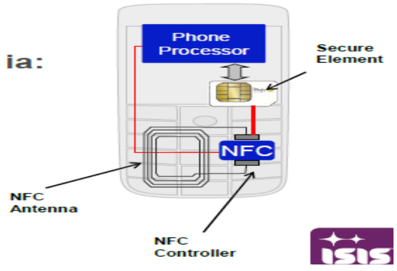


Fig.2. Secure elements of NFC

NFC phones contain special hardware- shows Fig.2.
Secure Element: Stores susceptible data (e.g. payment card information)
NFC Controller: Manages traffic and RF signals
NFC Antenna: Collects & transmits the RF
NFC devices can be used in contactless payment systems, credit cards and electronic ticket smartcards, and allow mobile payment to replace, transfer, exchange or supplement these systems.

2 Literature Review

Near Field Communication (NFC) is a wireless interface increasingly available in current and future mobile phones as well as Smartphone's. It is a short range (<10cm) wireless technology evolving from radio frequency identification (RFID). Near Field Communication is based on RFID that can transfer small amounts of data between two devices held a few centimeters from each other. The RFID reader is also called an interrogator or an initiator. It is a device that constantly propagates Radio Frequency (RF) signals and waits for a tag to response. For short range communication, RFID technology uses frequencies in the radio range of the Electromagnetic (EM) spectrum; which are in the range of 3 kHz – 300 GHz. NFC can be used in shops, bank, train station and social networking situations, such as sharing contacts, photos, videos or files, and entering multiplayer mobile games shows in Fig. 3.

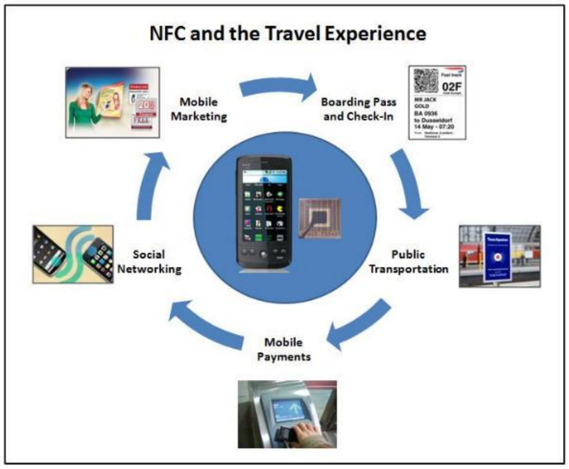
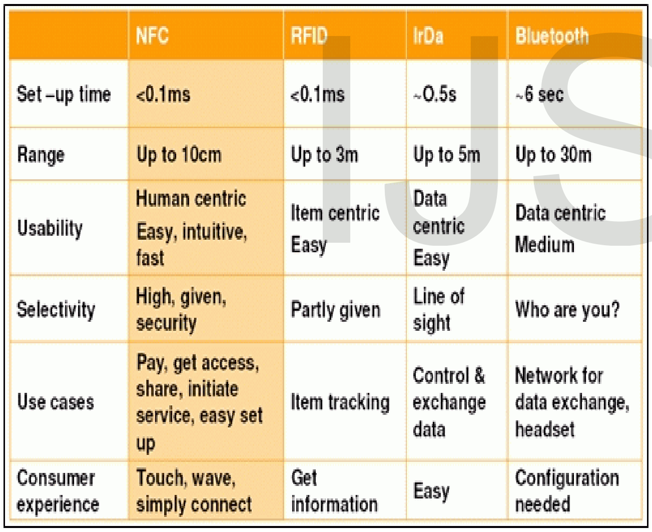


Fig. 3. NFC in Social Networking

Acting as a secure gateway to the connected world, tomorrow's NFC-enabled mobile devices will allow users to store, transfer, share and access all kinds of personal data or social data at home or on the move such as messages, pictures, MP3 files, etc.

Table 1: Comparison between NFC and 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

3 TECHNOLOGY OVERVIEW

3.1 Wireless short range communication technology

- Typical operating distance of 10 cm
- Compatible with today's field confirmed contactless MIFARE and FeliCa smart cards
- Data exchange rate today up to 424 kbit/s.
- Allows spontaneous initialization of wireless networks
- NFC is corresponding to Bluetooth and 802.11 with their long distance capabilities
- NFC also works in polluted environment
- NFC does not require line of sigh
- Easy and simple connection method
- Provides communication method to non-self powered devices.

NFC is a short-range wireless technology for distances measured in centimeters. It is optimized for spontaneous, easy and secure communications between various devices without requiring user configuration. To make two devices communicate, users simply bring them close together. The devices' NFC interfaces will automatically connect as well as configure themselves to form a peer-to-peer network. NFC can also help other wireless protocols like Bluetooth or Wireless Ethernet by exchanging arrangement of elements and session data.

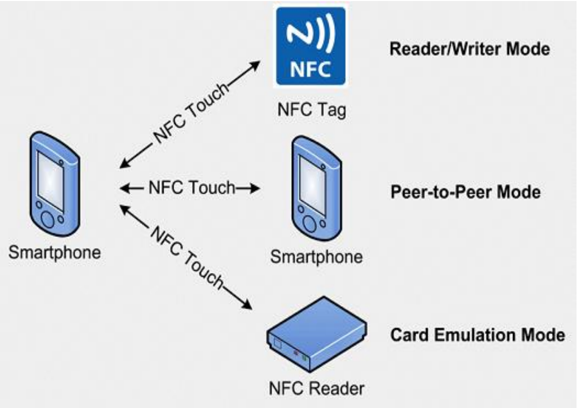


Fig.4 Wireless short range communication technology

IJSER

3.2 Communication Modes: Active and Passive

The NFC boundary can work in two different modes: active and passive. An active device generates its own radio frequency (RF) field, whereas a device in passive mode has to use inductive coupling to transmit data. For battery-powered devices, like mobile wallet, digital wallet and mobile phones, it is better to act in passive mode.Differences to the active mode, no internal power source is essential. In passive mode, not only a device can be motorized by the RF field of an active NFC device but also transfers data using load modulation. Therefore the protocol allows for card emulation, e.g., used for ticketing applications, even when the mobile phone is switch off.

3.3 Combining communications and identification Near Field Communication

NFC is a only one of its kind of wireless connectivity technology that enables convenient short-range communication between various electronic devices. It allows not only fast but also automatic set-up of wireless networks. It provides an implicit connector for accessible cellular, Bluetooth and wireless 802.11 devices. This touch-and-go convenience enables fast and easy communication between all types of user devices, which making NFC is the perfect solution for controlling and managing data in increasingly complex and connected world. NFC devices can read information from contactless cards and combines connectivity with smart card security. This makes smart cards which is the ideal solution for bringing information as well as electronic voucher into the NFC world.

4 Security Aspects

There are so many different possibilities to attack the Near Field Communication technology. On the other hand the different used devices can be forced physically. This may be the withdrawal of a tag from the tagged item or wrapping them in metal foil in order to defend the RF signal. Another feature is the infraction of privacy. For detecting errors, NFC uses the cyclic redundancy check (CRC). This method allows devices to check whether the received data has been spoiled or damaged.

4.1 Eavesdropping

Radio Frequency (RF) waves for the wireless data transfer with an antenna enables attackers to pick up the transmitted Monitoring data. When two devices connected or communicate via NFC they use RF waves to talk to each other. An attacker can use an antenna to receive the transmitted signals. Either by experimenting or by writing research the attacker can have the re-quired knowledge on how to extract the transmitted data out of the received RF signal.

4.2 Data modification

It is easy to completely destroy data by using a jammer. There is no way currently to avoid such an attack. However, if NFC devices verify the RF field while they are transfer, it is promising to detect attacks and the slightly modify it.

4.3 Data Destruction

An attacker who draw a bead on data damage intends a corruption of the communication. The outcome is that a provision is no longer available for used. Still, the attacker is not able to create a valid message. Instead of eavesdropping this is not a passive attack. There is no technique to avoid such an attack, but it is probable to detect it. NFC devices are capable to accept and broadcast data at the same time. That means, they can verify the radio frequency field and will observe the collision.

4.4 Data Insertion

This attack can only be implemented by an attacker, if there is enough time to send an inserted message before the real device starts to send his answers. If a collision occurs the data exchange would be stopped at once.

4.5 Man-in-the-Middle-Attack

In order to show that NFC is secure against a Man-in-the-Middle-Attack to survey both, the active and the passive communication mode.

4.6 Lost property

Losing the NFC RFID card or the mobile phone will open access to any finder and act as a single-factor authenticating entity. Mobile phones protected by a PIN code acts as a single authenticating factor.

4.7 Secure Element

- Java Card Operating Platform
- Secure memory
- Contact and contactless interfaces ISO7816 and Single Wire Protocol (SWP)
- Implements Global Platform Smart card specification that defines card components, command sets, transaction sequences.

5 Conclusion

In summary, Near Field Communication is a resourceful technology for communications with short ranges. It offers spontaneous and simple way to transfer data between two electronic devices. A important advantage of this technique is the compatibility with existing RFID infrastructures. Moreover, it would bring benefits to the setup of longer-range wireless technologies, such as Bluetooth. With a protected channel NFC provides confidentiality, integrity and authenticity.

References

[1] L. Francis, G. P. Hancke, K. Mayes, and K. Markantonakis, “Practical relay attack on contactless transactions by using nfc mobile phones.” IACR Cryptology ePrint Archive, vol. 2011, p. 618, 2011. [Online]. Available: http://dblp.uni-trier.de/db/journals/iacr/ iacr2011.html#FrancisHMM11

[2] ETSI TS 102 190 V1.1.1: Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1) 2003-03, URL: http://www.etsi.org.

[3] Yang, B., & Sun, J. (2011). Near field communication technology. Linkopings Universitet,

[4] Near field communication. (2012, January 28). In Wikipedia, The Free Encyclopedia. Retrieved 23:49, January 31, 2012

[5] The RFID Knowledgebase - Sample Case Studies.http://www.idtechex.com/pdfs/en/k3807f3934.pdf

[6] NFC Forum. (Feb. 03 2013). Specification overview [Online].Available at: http://www.nfcforum.org/specs/spec_dashboard/.

[7] B. Ozdenizci, K. Ok, V. Coskun, and M. Aydin, “Development of an indoor navigation system using nfc technology,” in Information and Computing (IC-IC), 2011 Fourth International Conference on, april 2011,pp. 11 –14.

IJSER