International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey on Near Field Communication in Healthcare

Prasad S. Halgaonkar[1], Nikita S. Daga[2], Dr. V. M. Wadhai[3]

[1]Reaserch Scholar, Department of Computer Science, SGBAU, Amravati, India

[2]ME Student, MITCOE, S. P. Pune University, Maharashtra, India

[3]Principal, SAE collage of Kondhwa, Pune, Maharashtra, India

Abstract: ***Near Field Communication is a short range high frequency wireless communication technology. It is based on RFID technology [1]. NFC has different types of operating modes and communication mode. NFC enabled mobile phone can be used in health care application which introduces some attacks on it. Attacks are Denial of service (DOS), phishing attack and lost property attack.***

Keywords: NFC, Operating modes, Communication modes, Tags.

1. Introduction

1.1 What is NFC?

Near Field Communication is local area wireless communication technology which allows the exchange of data between a reader and a target with recognizable distance of 10cm and operate speed between 106- 424kbps. Frequency speed of the NFC is 13.56 MHz.NFC is Based on RFID (Radio Frequency Identification) uses the magnetic field induction to enable communication between two electronic devices in close approximate. It allows bidirectional communication between NFC devices. IT provides seamless medium and open platform technology. It is not require set up by user. NFC technology makes it combine the interface of a reader and a smart card in a single device. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (**RFID**) standards. The standards include ISO/IEC 18092 and those defined by the NFC Forum, which was founded in 2004 by Nokia itself, Philips and Sony, and now has more than 160 members.

1.2 Communication Mode

In NFC, two type of communication mode: Active and Passive. NFC protocol distinguishes between the Initiator and the Target of the communication. Any device may be either an Initiator or a Target. The device that initiates and controls the exchange of data is called initiator and target is the device that answers the request from the Initiator.

a) Active Communication Mode:
Initiator and Target Device both have own power supplies and alternate generate their own RF signals on which the data is carried. It always be the same for both initiator to target and target to initiator. A device deactivates its RF field while it is waiting for data. Ex. Mobile phone, NFC reader

b) Passive Communication Mode:
Target device has no power supply of their own RF signal. They are power by the field generated by the initiator (reader). The Initiator is the device responsible to generate the RF field. The Initiator device provides a carrier field and the target device answers by modulating existing field. Ex. Tag

1.3 Operating Mode

NFC has three operating modes: peer-to-peer mode, reader/writer mode and card emulation mode. In peer-to-peer mode, NFC devices directly communicate with each other either in active or passive communication mode. In passive mode, Initiator initiates the communication by generating the RF signal, and the wait for target replies to the initiator command. It is based on ISO 18092 standards. In the active mode, the initiator and the target need to generate their RF signals. The initiator starts NFCIP-1 communication session and the target replies to the initiator command. It is not supported by the contactless communication API [2].

In reader/writer mode, NFC device acts like a normal active contactless card reader. It can then generate RF fields to communicate with contactless cards, RFID tags or NFC Forum tags. the NFC initiator reads data from the passive NFC tags and write the data into the passive NFC tag[2]. This mode is basically passive and it is based on ISO/IEC 14443 and FeliCa standards. It is supported by the contactless communication API. RW mode is used for NFC poster applications.

In card emulation mode, NFC device emulates a contactless smartcard and, thus, is able to communicate with existing RFID readers. The NFC device can be used as a contactless smart card, emulating a smart card to interact with a NFC reader [2]. The device is passive so it does not generate a RF field. NFC devices can work as a smart card, which contains a secure element (SE). The emulation can be done through two ways: either as an application, such as mobile e-payment applications, or as a SE which could be embedded in smart-phones. An NFC device can act as a tag and could be used for purchasing. It is supported by the contactless communication API.

2. Previous work

Healthcare: People continuously try to improve their quality of life and technology plays an important role in it. Such technologies like mobile devices can be use in health care application .Mobile devices are personal, always on, always with the patient and are location aware; the patient can use it for self help or to communicate with a professional and or to monitor the health of the patient. This makes the NFC enable mobile phone a much more appropriate device for remote healthcare than any other media. NFC-enable mobile phone is tap to the NFC-TAGs. NFC tags contain information about the patient, Patient has given a unique NFC-tags. By swiping the TAG with an NFC-enable phone, the patient can be identified and important information can be transmitted to the nurse however it not only provide medical professionals with information about what treatments a patient should receive, but they can also keep track of when nurses and doctors have checked in with that patient. These tags are re-usable, programmable and transmit data about the location, operation. It NFC ability to work off-line with automated recordings of visits, Visiting nurses can be monitored by having them check in and out during a patient visit. This way the execution of all planned visits can be monitored and the amount of working hours can be properly recorded.

Mobile Health Monitoring Applications: Patients are located at a distance or mobile. Small portable devices such as mobile phones equipment are used for collecting and processing health information. Transmission technologies such as NFC, Bluetooth, USB, Global System for Mobile Communication (GSM), General Packet Radio Service (GPRS) and Radio Frequency Identification (RFID) tags are used to communicate information between patients and healthcare providers[6].

Denial of Service: The only purpose of this type of attack is to interrupt the communication between NFC devices[3]. The attack is relatively simple to achieve with the appropriate hardware but difficult to prevent. Denial- of-Services attacks can be used for destroying the relationship between the NFC devices. Denial of Service (DoS) attack is possible on both the server and the tag.

Phishing: Phishing is a fraudulent attempt, usually made through email, to steal your personal information. In NFC replacing a tag on an NFC based smart poster, an attacker can deceive and force the user to visit websites with the same look and feel, but those sites are actually fake and malicious. For instance, in the case of an NFC poster, which enables customers to acquire a bus ticket by sending an SMS, it is simple for an attacker to alter the telephone number so that users are directed to a premium rate number instead. Phishing attack is possible on tag and server.

Lost property: Losing the NFC tag 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[5]. A way to defeat the lost-property threat requires an extended security concept that includes than one physically independent authentication factor. Lost property is possible on tag and NFC enables mobile phone.

3. Conclusion

Presented data provides an overview of the NFC technology, currently developed NFC applications classified into NFC modes. NFC technologies in healthcare environments have contributed to improve user's life. This is possible because, NFC is designed for intuitive, simple communication between initiator and target devices. These advantages can also be taken in many other situations for trying to make care-dependent people's life as easier as possible. Thus, in the future focus of our research will be to develop services for improving people's quality of life.

4. Acknowledgement

I have taken efforts in this literature review. However, it would not have been possible without the kind support and help of many individuals. I would like to extend my sincere thanks to all of them. I am highly indebted to ***Prof. Prasad Halgaonkar*** for her guidance and constant supervision as well as for providing necessary information regarding the project. I would like to express my gratitude towards her for her kind co-operation and encouragement which helped me in completion of this Literature review.

References

[1] Mohammed Riyazuddin, "NFC: A review of the technology, applications and security", ABI research.
[2] Ekta Desai, Mary Grace Shajan "A Review on the Operating Modes of Near Field Communication", International Journal of Engineering and Advanced Technology, December 2012
[3] CollinMulliner, "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones", International Conference on Availability, Reliability and Security2009
[4] Michael Roland, Josef Langer, Josef Scharinger, "Practical Attack Scenarios on Secure Element-enabled Mobile Devices", IEEE 4th International Workshop with Focus on Near Field Communication, 2012. IEEE DOI10.1109/NFC.2012.10
[5] Ashutosh Jaiswal , Zarina Shariff , Nilay Tambat, Akshay Mahale ,"NEAR FIELD COMMUNICATION", *Mumbai University*
[6] Ali Alzahraniy, Abdullah Alqhtaniy, Haytham Elmiligiy, Fayez Gebaliy, and Mohamed S. Yasein "NFC Security Analysis and Vulnerabilities in Healthcare Applications".

Author Profile

Prasad S. Halgaonkar is working as Assistant Professor, MITCOE, Pune, Maharashtra, India

Nikita S. Daga, ME, MITCOE, Pune, Maharashtra, India

Dr. V. M. Wadhai is Principal of SAE college of Kondhwa, Pune, Maharashtra, India