ISSN 2319 – 7757 EISSN 2319 –7765

Indian Journal of Engineering

Near field communication: programming and security

CharanPuladas, Sai Sri Lakshmi B

Dept of Electronics & Communication, Geethanjali College of Engineering & Technology, JNT University, Hyderabad, India

Corresponding author: Dept of Electronics & Communication, Geethanjali College Of Engineering &Technology,JNT University, Hyderabad, India. Mail: charan220493@gmail.com

Received 06 August; accepted 17 September; published online 15 October; printed 28 October 2013

ABSTRACT

Basically near field communication is a cousin of Bluetooth but is far more advantageous in the most peculiar forms, being said because of its very short range which is no more than a few centimetres and having a data rate of 424Kbits/sec. Near field communication or the NFC, its name itself suggest that data transfer at very close proximity. Which is one of its very key features that ensures the security of the data. NFC is standardized as ISO 18092 and uses RFID(Radio Frequency Identification) which is one very crux part of powering up the NFC tags, emulation cards or peer devices. NFC devices like smartphone's and tablets have NFC either built into its phone or on to the battery of the phone.

Keywords: RFID, Manchester coding, ASK Modulation, Baud rate, Modified miller coding, card emulator, NFC tag, eavesdropping.

To Cite This Article
CharanPuladas, Sai Sri Lakshmi B. Near field communication: programming and security, *Indian Journal of Engineering*, 2013, 5(13), 53-56

1. INTRODUCTION

NFC stands for Near Field Communication. The specification details of NFC can be found in ISO 18092. The main characteristic of NFC is that it is a wireless communication interface with a working distance limited to about 10 cm. The interface can operate in several modes. The modes are distinguished whether a device creates its own RF field or whether a device retrieves the power from the RF field generated by another device. If the device generates its own field it is called an active device, otherwise it is called a passive device. Active devices usually have a power supply,passive devices usually don't (e.g. contactless Smart Card). When two devices communicate three different configurations are possible. These are described in Table 1. These configurations are important because the way data is transmitted depends on whether the transmitting device is in active or passive mode. In active mode the data is sent using amplitude shift keying (ASK). This means the base RF signal (13,56 MHz) is modulated with the data according to a coding scheme. If the baudrate is 106 kBaud, the coding scheme is the so-called modified Miller coding. If the baudrate is greater than 106 kBaud the Manchester coding scheme is applied. In both coding schemes a single data bit is sent in a fixed time slot. This time slot is divided into two halves, called half bits. In Miller coding a zero is encoded with a pause in the first half bit and no pause in the second half bit.

A one is encoded with no pause in the first bit, but a pause in the second half bit. In the modified Miller coding some additional rules are applied on the coding of zeros. In the case of a one followed by a zero, two subsequent half bits would have a pause. Modified Miller coding avoids this by encoding a zero, which directly follows a one with two half bits with no pause.In the Manchester coding the situation is nearly the same, but instead of having a pause in the first or second half bit, the whole half bit is either a pause or modulated. Besides the coding scheme also the strength of the modulation depends on the baudrate. For 106 kBaud 100% modulation is used. This means that in a pause the RF signal is actually zero. No RF signal is sent in a pause. For baudrates greater than 106 kBaud 10% modulation ratio is used. According to the definition of this modulation ratio, this means that in a pause the RF signal is not zero, but it is about 82% of the level of a non-paused signal. This difference in the modulation strength is very important from a security point of view as we will describe later on in the security analysis.In passive mode the data is sent using a weak load modulation. The data is always encoded using Manchester coding with a modulation of 10%. For 106 kBaud a subcarrier frequency is used for the modulation, for baudrates greater than 106 kBaud the base RF signal at 13.56 MHz is modulated. Additionally to the active and passive mode, there are two different roles a device can play in NFC communication. NFC is based on a message and reply concept. This means one device A sends a message to another device B and device B sends back a reply. It is not possible for device B to send any data to device A without first receiving some message from device A, to which it could reply. The role of the device A which starts the data exchange is called initiator, the role of the other device is called target.

2. COMMUNICATING USING NFC TAGS

NFC devices use a special NFC tag, which are programmed to perform a specific operation, here being controlling any home appliance. The NFC uses RFID with which the NFC tags are powered up. The principle here is Electromagnetic Induction. It

Table 1
Communication configurations

Device A	Device B	Description
Active	Active	When a device sends data, it generates RF field and while receiving it doesn't generate RF field. Hence A and B generate RF field alternately.
Active	Passive	Device A generates RF field.
Passive	Active	Device B generates RF field.

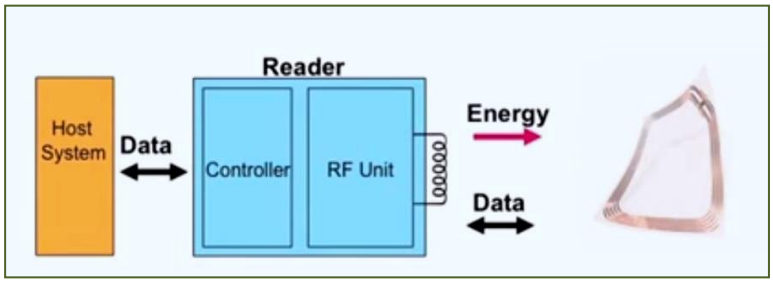

Figure 1
NFC tag with a few turn of coil

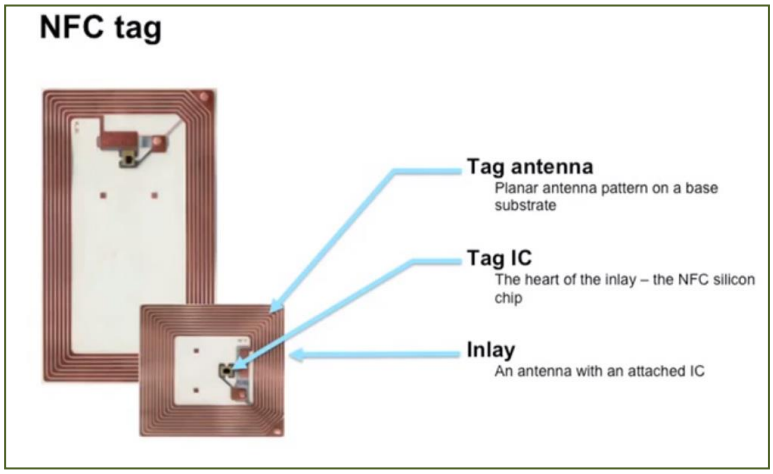

Figure 2
NFC tag performs various tasks that are programmed into it

Figure 3
Modes in NFC

works as a "Air-transformer" where the primary winding is the NFC device and secondary device is the NFC tag. The NFC tag contain a few turn of coil which pick up the magnetic lines of force when it comes in contact with the device. This is shown in Figure 1. When the power is received to the NFC tag it performs various tasks that are programmed into it. This is how a NFC tag looks like (Figure 2). The NFC tag has a EEPROM in the IC basically to potentiate the tag to read and write data in to it or from it. The picture is self-explanatory. The NFC device could be a high end smartphone like a Samsung Note2 or Google Nexus 4 or HTC one. These phones are used to write the program into the NFC tag and the program is runs whenever the smartphone that was used to write the program is brought into contact with the tag. There are different modes in NFC, which were described in Table 1. Here is picture that would help you out more in understanding the modes in NFC (Figure 3). A peer to peer communication has both device active, and the rest of the modes use a single active device.

3. PROGRAMMING OF NFC TAGS

The main advantage of NFC is that it has got a highly sophisticated programming tool kit where the user has to only select what he wants to do, the rest is done by the software. The software apps are available onplaystore. NFC Task Launcher is the best to use. These images show the NFC Task Launcher. Basically programming a NFC tag or a card emulator is a very user friendly task. Here are a few images that guide you how to program a tag.

1. Select the NFC Task Launcher (Figure 4).
2. Select the + option (Figure 5)
3. Click on New Task (Figure 6)
4. Select the type of Action that has to be performed (Figure 7).
5. Select the any of the application that is to be embedded in to the NFC tag, for instance camera (Figure 8).
6. Click on save and write, and the task of programming the NFC tag is completed when you place the NFC tag near the phone after saving (Figure 9)
7. Figure 10 show how the camera starts up when the tag is touched to the phone.

4. SECURITY

4.1. Threats (Eavesdropping)

Because NFC is a wireless communication interface it is obvious that eavesdropping is an important issue. When two devices communicate via NFC they use RF waves to talk to each other. An attacker can of course use an antenna to also receive the transmitted signals. Either by experimenting or by literature research the attacker can have the required knowledge on how to extract the transmitted data out of the received RF signal. Also the equipment required to receive the RF signal as well as the equipment to decode the RF signal must be assumed to be available to an attacker as there is no special equipment necessary. The NFC communication is usually done between two devices in close proximity.This means they are not more than 10 cm (typically less) away from each other. The main question is how close an attacker needs to be to be able to retrieve a usable RF signal. Unfortunately, there is no correct answer to this question. The reason for that is the huge number of parameters which determine the answer. For example the distance depends on the following parameters, and there are many more.

- RF filed characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case, the PCB, the environment)
- Characteristic of the attacker's antenna (i.e. antenna geometry, possibility to change the position in all 3 dimensions)
- Quality of the attacker's receiver
- Quality of the attacker's RF signal decoder
- Setup of the location where the attack is performed (e.g. barriers like walls or metal, noise floor level)
- Power sent out by the NFC device

Therefore any exact number given would only be valid for a certain set of the above given parameters and cannot be used to derive general security guidelines. Additionally, it is of major importance in which mode the sender of the data is operating.

CharanPuladas et al.
Near field communication: programming and security,
Indian journal of engineering, 2013, 5(13), 53-56,

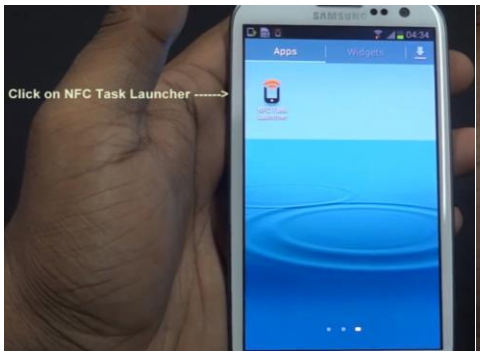

Figure 4
Select the NFC Task Launcher

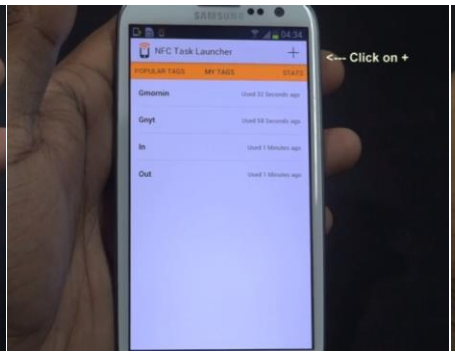

Figure 5
Select the + option

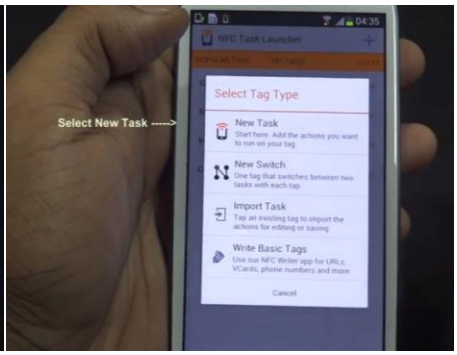

Figure 6
Click on New Task

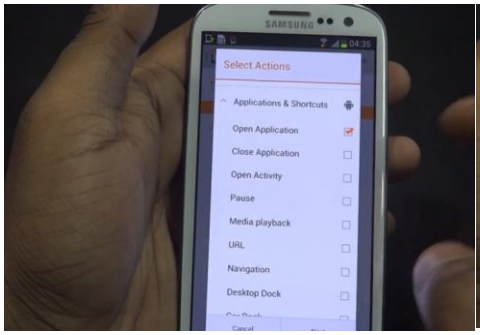

Figure 7
Select the type of Action that has to be performed

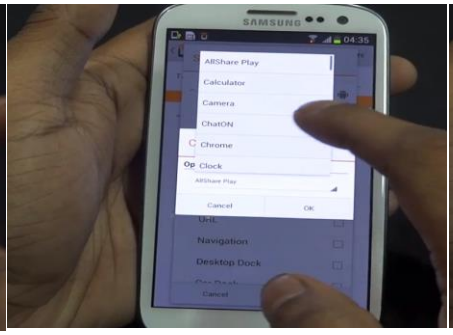

Figure 8
Select the any of the application that is to be embedded in to the NFC tag, for instance camera

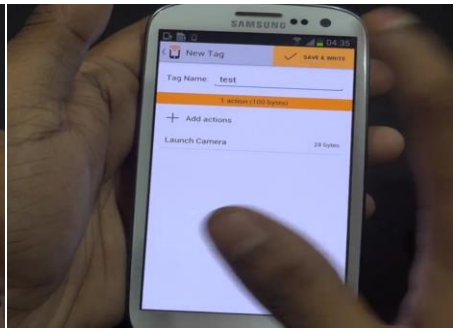

Figure 9
Click on save and write, and the task of programming the NFC tag is completed when you place the NFC tag near the phone after saving

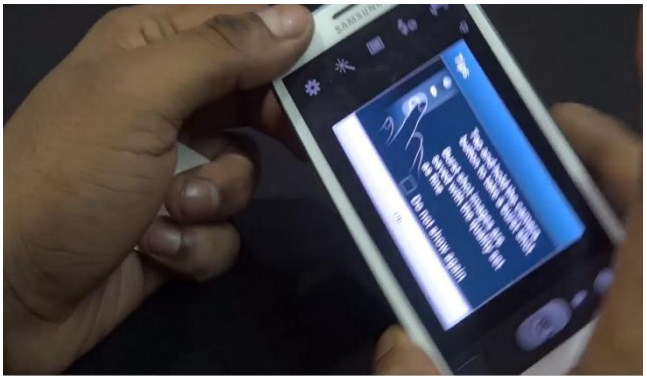

Figure 10
Shows how the camera starts up when the tag is touched to the phone

This means whether the sender is generating its own RF field (active mode) or whether the sender is using the RF field generated by another device (passive mode). Both cases use a different way of transmitting the data and it is much harder to eavesdrop on devices sending data in passive mode.In order to not leave the reader without any idea on how big the eavesdropping distances are, we give the following numbers, which as stated above are not valid in general at all, but can only serve to give a rough idea about these distances. When a device is sending data in active mode, eavesdropping can be done up to a distance of about 10 m, whereas when the sending device is in passive mode, this distance is significantly reduced to about 1 m.

4.2. Secure channel for NFC

The best method for a secure transmission of data is by using a NFC specific key agreement. It does not require any asymmetric cryptography and therefore reduces the computational requirements significantly. Theoretically, it also provides perfect security. The scheme works with 100% ASK only and it is not part of the ISO standard on NFC. The idea is that both devices, say Device A and Device B, send random data at the same time. In a setup phase the two devices synchronize on the exact timing of the bits and also on the amplitudes and phases of the RF signal. This is possible as devices can send and receive at the same time. After that synchronisation, A and B are able to send at exactly the same time with exactly the same amplitudes and phases. While sending random bits of 0 or 1, each device also listens to the RF field. When both devices send a zero, the sum signal is zero and an attacker, who is listening, would know that both devices sent a zero. This does not

CharanPuladas et al.
Near field communication: programming and security,
Indian journal of engineering, 2013, 5(13), 53-56,

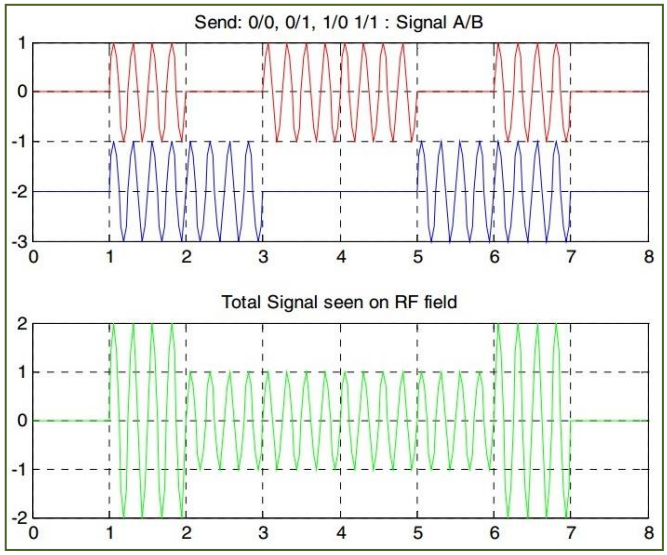

Figure 11
NFC specific key agreement

help. The same thing happens when both, A and B, send a one. The sum is the double RF signal and an attacker knows that both devices sent a one. It gets interesting once A sends a zero and B sends a one or vice versa. In this case both devices know what the other device has sent, because the devices know what they themselves have sent. However, an attacker only sees the sum RF signal and he cannot figure out which device sent the zero and which device sent the one. This idea is illustrated in Figure 11. The top graph shows the signals produced by A in red and by B in blue. A sends the four bits: 0, 0, 1, and 1. B sends the four bits: 0, 1, 0, and 1. The lower graph shows the sum signal as seen by an attacker. It shows that for the bit combinations (A sends 0, B sends 1) and (A sends 1, B sends 0) the result for the attacker is absolutely the same and the attacker cannot distinguish these two cases. The two devices now discard all bits, where both devices sent the same value and collect all bits, where the two devices sent different values. They can either collect the bits sent by A or by B. This must be agreed on start-up, but it doesn't matter. This way A and B can agree on an arbitrary long shared secret. A new bit is generated with a probability of 50%. Thus, the generation of a 128 bit shared secret would need approximately 256 bits to be transferred. At a baud rate of 106 kBaud this takes about 2.4 ms, and is therefore fast enough for all applications. The security of this protocol in practice depends on the quality of the synchronisation which is achieved between the two devices. Obviously, if an eavesdropper can distinguish data sent by A from data sent by B, the protocol is broken. The data must matchin amplitude and in phase. Once the differences between A and B are significantly below the noise level received by the eavesdropper the protocol is secure. The level of security therefore also depends on the signal quality at the receiver. The signal quality however again depends on many parameters (e.g. distance) of the eavesdropper. In practice the two devices A and B must aim at perfect synchronisation. This can only be achieved if at least one of A or B is an active device to perform this synchronization.

5. CONCLUSION

Presently there a considerable number of high-end smart phones in Indian market which have the feature of NFC, but the feature isn't used to its potential. The programming explained above is the easiest form a embedding a task into a tag or card emulator. The applications of NFC has greater scope in everyday life, mainly home-automation where different home-appliances can be controlled using a NFC device and a passive NFC tag or card emulator. Even keyless door entry system can be achieved using NFC and a NXP Lego kit.

REFERENCES

1. Castelluccia C, Avoine G. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags, *Proceedings of CARDIS 2006,* 2006 LNCS 3928, 289-299
2. Ernst Haselsteiner and KlemensBreitfuß. Strengths and weakness of NFC,*Philips Semiconductors*2009, 33, 44-56
3. ISO. Information technology - Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1), http://www.iso.org/iso/catalogue_detail.htm?csnumber=38578, Accessed on 4th September 2013
4. Klaus Finkenzeller. RFID Handbuch, *HanserVerlag*, 2002, 18, 88-97

CharanPuladas et al.
Near field communication: programming and security,
Indian journal of engineering, 2013, 5(13), 53-56,