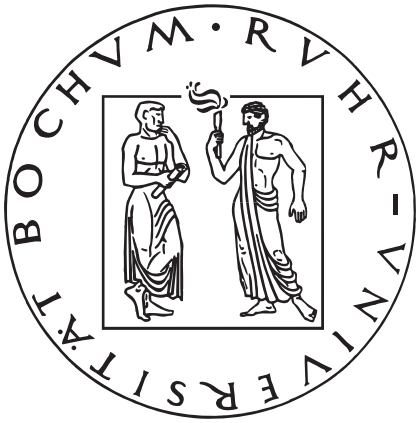
Near Field Communication in Cell Phones

Annika Paus

24.07.2007

Seminararbeit
Ruhr-Universität Bochum



Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

IPR2025-01151
Apple EX1040 Page 1

Contents

1 Introduction **1**

2 Standards and Compatibility **3**

3 Technology Overview **5**
3.1 Communication Modes: Active and Passive 5
3.2 Coding and Modulation 6
3.2.1 Manchester Code 6
3.2.2 Modified Miller Code 7
3.3 Initiator and Target 7
3.4 Collision Avoidance 7
3.5 General Protocol flow 8

4 Comparison with other Technologies **11**
4.1 NFC and RFID 11
4.2 Comparison with Bluetooth and Infrared 11

5 Security Aspects **13**
5.1 Eavesdropping 13
5.2 Data Destruction 14
5.3 Data Modification 15
5.4 Data Insertion 16
5.5 Man-in-the-Middle-Attack 16

6 Conclusion **19**

1 Introduction

Near Field Communication (NFC) is a technology for contactless short-range communication. Based on the Radio Frequency Identification (RFID), it uses magnetic field induction to enable communication between electronic devices.

The number of short-range applications for NFC technology is growing continuously, appearing in all areas of life. Especially the use in conjunction with mobile phones offers great opportunities. The main applications are:

- **payment & ticketing**
  NFC enables users to make fast and secure purchases, go shopping with electronic money, and also to buy, store and use electronic tickets, such as concert/event tickets, plane tickets, travel cards, etc.

- **electronic keys**
  For example, these can be car keys, house/office keys, etc.

- **identification**
  In addition, NFC makes it possible to use mobile phones instead of identity documents. In Japan, for example, student IDs can be stored on cell phones, which allows the students to electronically register for classes, to open locked campus doors, buy food at the school cafeteria, borrow books, and even get discounts at local movie theaters, restaurants, and shops.

- **receive and share information**
  The data stored on any tagged object (e.g. a DVD box or a poster) can be accessed by mobile phones in order to download movie trailers, street-maps, travel timetables etc.

- **set-up service**
  To avoid the complicated configuration process, NFC can be used for the set-up of other longer-range wireless technologies, such as Bluetooth or Wireless LAN.

Up to now the convenience of NFC is mostly used in Asia, for instance in Japan or South Korea, where paying with a mobile phone or a NFC-smartcard already belongs to everyday life. In September 2006, ABI research predicted that by 2011, about 30% of the mobile phones in the world (about 450 million phones) would be NFC-enabled.

In this paper we will discuss the characteristics of NFC. We start with the underlying Standards and Compatibility in Chapter 2, before we will consider the basic technology capabilities in Chapter 3. Chapter 4 deals with the correlation between NFC and RFID and confronts NFC with Bluetooth and infrared. Chapter 5 observes the Near Field Communication from the security point of view, considering different types of attack. In Chapter 6 the major results of this work are summarized.

2 Standards and Compatibility

Near Field Communication is an open platform technology, developed by Philips and Sony. NFC, described by NFCIP-1 (Near Field Communication Interface and Protocol 1), is standardized in ISO 18092 [1], ECMA 340[2] as well as in ETSI TS 102 190[3]. These standards specify the basic capabilities, such as the transfer speeds, the bit encoding schemes, modulation, the frame architecture, and the transport protocol. Furthermore, the active and passive NFC modes are described and the conditions that are required to prevent collisions during initialization.
Todays NFC devices do not only implement NFCIP-1, but also NFCIP-2, which is defined in ISO 21481 [4], ECMA 352 [5] and ETSI TS 102 312[6]. NFCIP-2 allows for selecting one of three operating modes:

- NFC data transfer (NFCIP-1),
- proximity coupling device (PCD), defined in ISO 14443 [7], and
- vicinity coupling device (VCD), defined in ISO 15693 [8].

NFC devices have to provide these three functions in order to be compatible with the main international standards for smartcard interoperability, ISO 14443 (proximity cards, e.g. Philip's Mifare), ISO 15693 (vicinity cards) and to Sonys FeliCa contactless smart card system. Hence, as a combination of smartcard and contactless interconnection technologies, NFC is compatible with today's field proven RFID-technology. That means, it is providing compatibility with the millions of contactless smartcards and scanners that already exist worldwide.

3 Technology Overview

NFC operates in the standard, globally available 13.56 MHz frequency band. Possible supported data transfer rates are 106, 212 and 424 kbps and there is potential for higher data rates. The technology has been designed for communications up to a distance of 20 cm, but typically it is used within less than 10 cm. This short range is not a disadvantage, since it aggravates eavesdropping.

3.1 Communication Modes: Active and Passive

The NFC interface can operate 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 phones, it is better to act in passive mode. In contrast to the active mode, no internal power source is required. In passive mode, a device can be powered by the RF field of an active NFC device and transfers data using load modulation. Hence, the protocol allows for card emulation, e.g., used for ticketing applications, even when the mobile phone is turned off.

This yields to two possible cases, which are described in Table 3.1. The communication between two active devices case is called *active* communication mode, whereas the communication between an active and a passive device is called **passive** communication mode.

Communication Mode	**Description**
Active	Two active devices communicate with each other. Each device has to generate its own RF field, if it wants to send data. The RF field is alternately generated by one of the two devices.
Passive	In this mode the communication takes place between an active and a passive device. The passive device has no battery and uses the RF field generated by the active device.

Table 3.1: Communication Configurations

In general, at most two devices communicate with each other at the same time. However, as defined in [2], §11.2.2.3, in passive mode the initiator (see Section

3.3) is able to communicate with multiple targets. This is realized by a time slot method, which is used to perform a Single Device Detection (SDD). The maximal number of time slots is limited to 16. A target responds in a random chosen time slot that may lead to collision with the response of another target. In order to reduce the collisions, a target may ignore a polling request set out by the initiator. If the initiator receives no response, it has to send the polling request again.

3.2 Coding and Modulation

The distinction between active and passive devices specifies the way data is transmitted. Passive devices encode data always with Manchester coding and a 10 %ASK[1]. Instead, for active devices one distinguishes between the modified Miller coding with 100% modulation if the data rate is 106 kbps, and the Manchester coding using a modulation ratio of 10% if the data rate is greater than 106 kbps. As we will discuss later the modulation ratio, defined in [1] is of high importance for the security of the NFC data transfer.

	Active Device	**Passive Device**
106 kBaud	Modified Miller, 100% ASK	Manchester, 10% ASK
212 kBaud	Manchester, 10% ASK	Manchester, 10% ASK
424 kBaud	Manchester, 10% ASK	Manchester, 10% ASK

Table 3.2: Coding and Modulation at different transfer speeds [10]

3.2.1 Manchester Code

The Manchester coding depends on two possible transitions at the midpoint of a period. A low-to-high transition expresses a 0 bit, whereas a high-to-low transition stands for a 1 bit. Consequently, in the middle of each bit period there is always a transition. Transitions at the start of a period are not considered.

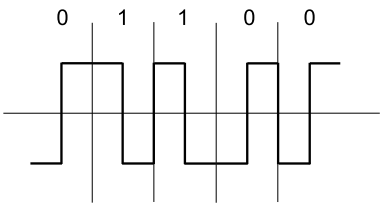


Figure 3.1: Manchester Code

[1] **Amplitude-shift keying** is a form of modulation that represents digital data as variations in the amplitude of a carrier wave [11]

3.2.2 Modified Miller Code

This line code is characterized by pauses occurring in the carrier at different positions of a period. Depending on the information to be transmitted, bits are coded as shown in Figure 3.2. While a 1 is always encoded in the same way, coding a 0 is determined on the basis of the preceded bit.

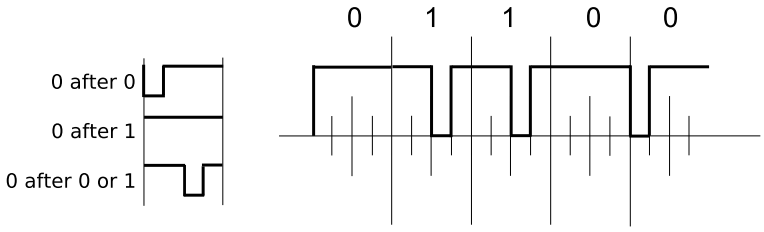


Figure 3.2: Modified Miller Code

3.3 Initiator and Target

Furthermore, it is important to observe the role allocation of initiator and target. The initiator is the one who wishes to communicate and starts the communication. The target receives the initiator's communication request and sends back a reply. This concept prevents the target from sending any data without first receiving a message. Regarding the passive communication mode, the passive device acts always as NFC target. Here the active device is the initiator, responsible for generating the radio field. In the case of an active configuration in which the RF field is alternately generated, the roles of initiator and target are strictly assigned by the one who starts the communication. By default all devices are NFC targets, and only act as NFC initiator device if it is required by the application.
In the case of two passive devices communication is not possible (see Table 3.3).

	Initiator	**Target**
Active	Possible	Possible
Passive	Not Possible	Possible

Table 3.3: Possible Combinations Active/Passive with Initiator/Target ([9])

3.4 Collision Avoidance

Usually misunderstandings are rather rare, since the devices have to be placed in direct proximity. The protocol proceeds from the principle: listen before talk.

If the initiator wants to communicate, first, it has to make sure that there is no external RF field, in order not to disturb any other NFC communication. It has to wait silently as long as another RF field is detected, before it can start the communication, after an accurately defined guard-time ([2], §11.1). If the case occurs that two or more targets answer at exactly the same time, a collision will be detected by the initiator.

3.5 General Protocol flow

As shown in Figure 3.3 the general protocol flow can be divided into the initialization and transport protocol. The initialization comprises the collision avoidance and selection of targets, where the initiator determines the communication mode (active or passive) and chooses the transfer speed.

As defined in [2], §12, the transport protocol is divided in three parts:

- *Activation of the protocol, which includes the Request for Attributes and the Parameter Selection.*
- *The data exchange protocol, and*
- *The deactivation of the protocol including the Deselection and the Release.*

During one transaction, the mode (active and passive) and the role (initiator and target) does not change until the communication is finished. Though, the data transfer speed may be changed by a parameter change procedure. For further details the reader may refer to the standards [1] or [2].

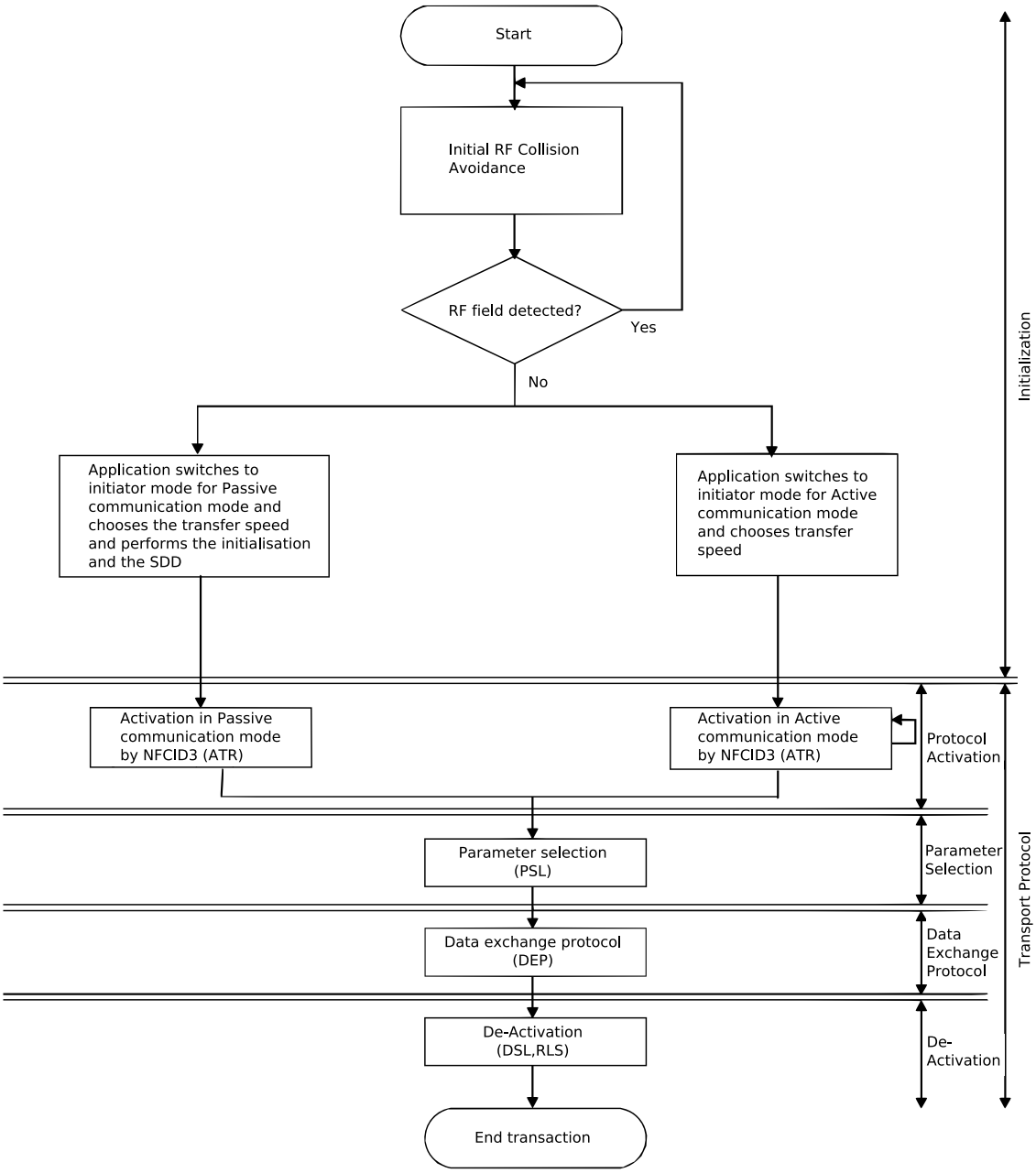


Figure 3.3: General initialization and transport protocol ([2])

4 Comparison with other Technologies

4.1 NFC and RFID

Basically, the technologies Radio Frequency Identification and Near Field Communication use the same working standards. However, the essential extension of RFID is the communication mode between two active devices. In addition to contactless smart cards (ISO 14443 [7]), which only support communication between powered devices and passive tags, NFC also provides peer-to-peer communication. Thus, NFC combines the feature to read out and emulate RFID tags, and furthermore, to share data between electronic devices that both have active power.

4.2 Comparison with Bluetooth and Infrared

Compared to other short-range communication technologies, which have been integrated into mobile phones, NFC simplifies the way consumer devices interact with one another and obtains faster connections. The problem with infrared, the oldest wireless technology introduced in 1993, is the fact that a direct line of sight is required, which reacts sensitively to external influences such as light and reflecting objects. The significant advantage over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify the other's phone, the connection between two NFC devices is established at once (<0,1s). Table 4.1 points out these different capabilities of NFC, Bluetooth and infrared. All these protocols are point-to-point protocols. Bluetooth also supports point-to-multipoint communications. With less than 10 cm, NFC has the shortest range. This provides a degree of security and makes NFC suitable for crowded areas. The data transfer rate of NFC (424 kbps) is slower than Bluetooth (721 kbps), but faster than infrared (115 kbps). In contrast to Bluetooth and infrared NFC is compatible to RFID.

	NFC	Benefits of NFC	Bluetooth	IrDa
Network Type	Point-to-point	Easy set-up, pairing = bringing close	Point-to-multipoint	Point-to-point
Range	<0.1 m	Safe, suitable for crowded areas	10 m	1 m
Speed	424 kbps (1Mbps coming)		721 kbps	115 kbps
Set-up time	<0.1 s	Fast transactions e.g. for public transport	6 s	0.5 s
Modes	Active-active, active-passive	Reader mode and card-like mode	Active-active	Active-active
Compatible with RF ID	Yes	Can work with existing infrastructure	No	No
Costs	Low	Affordable for most devices	Moderate	Low

Table 4.1: NFC compared with Bluetooth and IrDa [12]

5 Security Aspects

In this chapter, we want to analyze the security of NFC. In this context two very interesting papers have been published. In [9] Ernst Haselsteiner and Klemens Breitfuß discuss some threats and solution for the security of NFC, and also the paper "Security Aspects and Prospective Applications of RFID Systems" [13] gives some useful information.

First of all it should be mentioned that the short communication range of a few centimeters, though it requires conscious user interaction, does not really ensure secure communication.

There are different possibilities to attack the Near Field Communication technology. On the one hand the different used devices can be manipulated physically. This may be the removal of a tag from the tagged item or wrapping them in metal foil in order to shield the RF signal. Another aspect is the violation of privacy. If proprietary information is stored on a tag it is important to prevent from unauthorized read and write access. As outlined in [13] read-only tags are secure against an unauthorized write access. In the case of rewritable tags we have to assume that attackers may have mobile readers and the appropriate software which enable unauthorized read and write access if the reader distance is normal. In this work we want to focus on attacks with regard to the communication between two devices.

For detecting errors, NFC uses the cyclic redundancy check (CRC). This method allows devices to check whether the received data has been corrupted.

In the following, we will consider different possible types of attacks on the NFC communication. For most of these attacks there are countermeasures in order to avoid or at least reduce the threats.

5.1 Eavesdropping

NFC offers no protection against eavesdropping. RF waves for the wireless data transfer with an antenna enables attackers to pick up the transmitted Monitoring data. In practice a malicious person would have to keep a longer distance in order not to get noticed. The short range between initiator and target for a successful communication is no significant problem, since attackers are not bound by the same transmission limits. Consequently the maximum distance for a normal read sequence can be exceeded. The question how close an attacker has to be located to retrieve an usable RF signal is difficult to answer. As listed in [9], this is

depending on a "huge" number of parameters, such as:

- *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*

Furthermore, eavesdropping is extremely affected by the communication mode. That's because, based on the active or passive mode, the transferred data is coded and modulated differently (see Section 3.2). If data is transfered with stronger modulation it can be attacked easier. Thus, a passive device, which does not generate it's own RF field is much harder to attack, than an active device. In order to let the reader presume the risk resulting from eavesdropping, there are given rough distances in [9]: "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."

However, we assume that such attacks will occur since the required equipment is available for everyone. Equipped with such an antenna a malicious person that is able to passively monitor the RF signal may also extract the plain text. Experimenting and literature research can be used to get the necessary knowledge. Hence, the confidentiality of NFC is not guaranteed. For applications which transmit sensitive data a secure channel is the only solution.

In [14] some more detailed information of this attack are given.

5.2 Data Destruction

An attacker who aspires data destruction intends a corruption of the communication. The effect is that a service is no longer available. Still, the attacker is not able to generate a valid message. Instead of eavesdropping this is not a passive attack. This attack is relatively easy to realize. One possibility to disturb the signal is the usage of a so called RFID Jammer.

There is no way to prevent such an attack, but it is possible to detect it. NFC devices are able to receive and transmit data at the same time. That means, they can check the radio frequency field and will notice the collision.

5.3 Data Modification

Unauthorized changing of data, which results in valid messages, is much more complicated and demands a thorough understanding. As we will point out in the following, data modification is possible only under certain conditions. In order to modify the transmitted data an intruder has to concern single bits of the RF signal. As already mentioned in Section 3.2 data is send in different ways. The feasibility of this attack, that means if it is possible to change a bit of value 0 to 1 or the other way around, is subject to the strength of the amplitude modulation.

If 100% modulation is used, it is possible to eliminate a pause of the RF signal, but not to generate a pause where no pause has been. This would demand an impracticable exact overlapping of the attackers signal with the original signal at the receiver's antenna. However, Near Field Communication technology uses modulation of 100% in conjunction with the modified Miller coding which leads to 4 possible cases (see Figure 5.1). The only case, where a bit might be changed by an attacker is, where a 1 is followed by another 1. By filling the pause in two half bit of the RF signal the decoder receives the signal of the third case. Due to the agreement of the preceding bit the decoder would verify a valid one. The other three cases are not susceptible to such an attack.

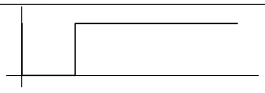
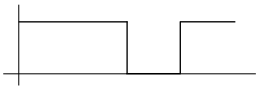
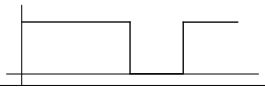
Bit x-1	Bit x		Modification of Bit x to	Feasible?
0	0		1	no
0	1		0	no
1	0		1	no
1	1		0	yes

Figure 5.1: Bit modification of the Modified Miller Code

For NFC, a modulation ratio of 10% is always used together with Manchester coding. In contrast to the 100% modulation, where really no signal is send in a pause, here within a pause the RF signal is e.g. 82% of the level of the full signal. Let's assume, an attacker may increase the existing RF signal about 18% during the whole session, without being noticed by the decoder. Then, the attacker is able to change a zero to one by increasing the RF signal during the first half of the signal period by another 18%, and also may change a bit of value one to zero by simply stopping to send anything.

Regarding the threat in summary: Except for one case, always Manchester coding with 10% ASK is used for NFC data transfer. This represents the best possible conditions for the malicious intention of modifying NFC data (compare Table 3.2). This way of transmitting the data offers a modification attack on all bits. The only exception are active devices transfering data at 106 kbps. In this case the usage of the modified Miller coding with a modulation ratio of 100% accomplishes that only certain bits can be modified.

In [9] three countermeasures are described. One possibility is the usage of the active communication mode with 106 kbps. As mentioned above this would not prevent, but at least reduce the risk of this attack. Furthermore, it is possible to let the devices check the RF field as already described in Section 5.2. Denoted as the "probably best solution" is the use of a secure channel. This would provide data integrity.

5.4 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. In order to prevent such attacks the device should try to answer with no delay. Alternatively, again checking the RF field and also the secure channel can be used to protect against attacks.

5.5 Man-in-the-Middle-Attack

In order to show that NFC is secure against a Man-in-the-Middle-Attack we have to survey both, the active and the passive communication mode. In the following we distinguish between device A and device B that are exchanging data.

In passive mode the active device (A) generates the RF field in order to send data to a passive device (B). The aim of an intruder is to intercept this message and prevent device B from receiving it. The next step would be to replace it with a different message. The first step is possible, but can be detected if device A checks the RF field while sending the message. However, the second one is practically impossible. To send a message to device B the attacker would have to generate his own RF field. Hence, the RF field of device A has to be perfectly aligned which is not practically feasible.

In contrast to the passive mode, in active mode device A switches off the RF field after sending a message. Now the attacker is confronted with another

problem. Even though he may generate an RF field, he is not able to transfer a message to device B that would not be recognized by device A, because device A is waiting for a response from device B. Thus, device A is assigned with the task to check if the received messages really come from device B.

Disregarding relay attacks, NFC provides good protection against a Man-in-the-Middle attack. This applies particularly if the passive communication mode is used and the RF field is monitored by device A.

6 Conclusion

In summary, Near Field Communication is an efficient technology for communications with short ranges. It offers an intuitive and simple way to transfer data between electronic devices. A significant advantages of this technique is the compatibility with existing RFID infrastructures. Additionally, it would bring benefits to the setup of longer-range wireless technologies, such as Bluetooth.

With regard to the security of NFC, we discussed different attacks and possible countermeasures to mitigate their impact. Despite the restriction of the range, eavesdropping or data modification attacks can be carried out. But, disregarding relay attacks, NFC provides security against Man-in-the-Middle-Attacks. In order to provide protection against these threats, the establishment of a secure channel is necessary. For this purpose simply the well known DH key agreement can be used, because Man-in-the-Middle-Attacks represent no threat. With a secure channel NFC provides confidentiality, integrity and authenticity.

Bibliography

[1] ISO/IEC 18092(ECMA-340): *Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1).* First Edition, 2004-04-01.

[2] Ecma International: *Standard ECMA-340, Near Field Communication Interface and Protocol (NFCIP-1)*, December 2004, URL: http://www.ecma-international.org/publications/standards/Ecma-340.htm.

[3] 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.

[4] ISO/IEC 21481: *Information technology Telecommunications and information exchange between systems Near Field Communication Interface and Protocol -2 (NFCIP-2).* January 2005.

[5] Ecma International: *Standard ECMA-352, Near Field Communication Interface and Protocol -2 (NFCIP-2)*, December 2003, URL: http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-352.pdf.

[6] ETSI TS 102 312, V1.1.1: *Electromagnetic compatibility and Radio spectrum Matters (ERM);Normalized Site Attenuation (NSA) and validation of a fully lined anechoic chamber up to 40 GHz* 2004-05, URL: http://www.etsi.org.

[7] ISO/IEC 14443: *Identification cards - Contactless integrated circuit cards - Proximity cards.* 2001, URL: www.iso.ch.

[8] ISO/IEC 15693: *Identification cards - Contactless integrated circuit cards - Vicinity cards.*

[9] Ernst Haselsteiner and Klemens Breitfuss: *Security in near field communication (NFC)*, Philips Semiconductors, Printed handout of Workshop on RFID Security RFIDSec 06, July 2006, URL:

http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf.

[10] Ernst Haselsteiner and Klemens Breitfuss: *Security in near field communication (NFC)*, RFIDSec 06, 2. July 13th, 2006, URL: http://events.iaik.tugraz.at/RFIDSec06/Program/slides/002%20-%20Security%20in%20NFC.ppt.

[11] Wikipedia: *Amplitude-shift-keying*, URL: http://en.wikipedia.org/wiki/Amplitude_shift_keying.

[12] Electronic Engineering Times Asia: *NFC delivers intuitive, connected consumer experience*, URL: http://www.eetasia.com/ARTICLES/2006MAY/PDF/EEOL_2006MAY01_STECH_RFD_TA.pdf?SOURCES=DOWNLOAD.

[13] Oertel, Wölk, Hilty, Köhler, Kelter, Ullmann, Wittmann: *Security Aspects and Prospective Applications of RFID Systems*, Bundesamt fr Sicherheit in der Informationstechnik, Bonn, 11. January 2005, URL: http://www.bsi.de/fachthem/rfid/RIKCHA_englisch.pdf.

[14] Gerhard P. Hancke: *A practical relay attack on ISO 14443 proximity cards.* 2005, URL: http://www.cl.cam.ac.uk/∼gh275/relay.pdf.