NEAR FIELD COMMUNICATION

**ABSTRACT**

NFC is one of the latest wireless communication technologies. As a short-range wireless connectivity technology, NFC offers safe — yet simple and intuitive — communication between electronic devices. Users of NFC-enabled devices can simply point or touch their devices to other NFC-enabled elements in the environment to communicate with them, making application and data usage easy and convenient.

With NFC technology, communication occurs when an NFC-compatible device is brought within a few centimeters of another NFC device or an NFC tag. The big advantage of the short transmission range is that it inhibits eavesdropping on NFC-enabled transactions. NFC technology opens up exciting new usage scenarios for mobile devices.

**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.

One of the main goals of NFC technology has been to make the benefits of short-range contactless communications available to consumers globally. The existing radio frequency (RF) technology base has so far been driven by various business needs, such as logistics and item tracking. While the technology behind NFC is found in existing applications, there has been a shift in focus — most notably, in how the technology is used and what it offers to consumers.

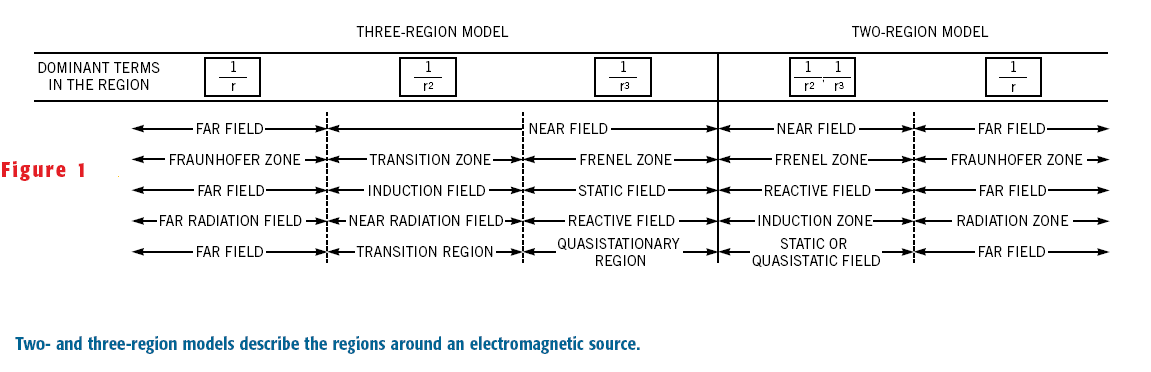
With just a point or a touch, NFC enables effortless use of the devices and gadgets we use daily. Here are some examples of what a user can do with an NFC mobile phone in an NFC-enabled environment:

* Download music or video from a smart poster.
* Exchange business cards with another phone.
* Pay bus or train fare.
* Print an image on a printer.
* Use a point-of-sale terminal to pay for a purchase, the same way as with a standard contactless credit card.
* Pair two Bluetooth devices.

An NFC-enabled phone functions much like standard contactless smart cards that are used worldwide in credit cards and in tickets for public transit systems. Once an application, such as a credit card application, has been securely provisioned to the NFC-enabled phone, the customer can pay by simply waving the phone at a point-of-sale reader. The NFC phone also offers enhanced security, enabling the user to protect the secure applications through the phone's user interface features.

**NEAR FIELD AND FAR FIELD**

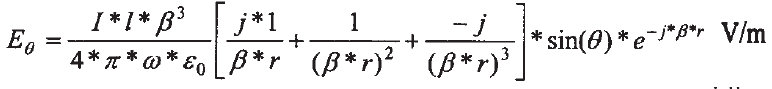
The terms “far field” and “near field” describe the fields around an antenna or, more generally, any electromagnetic-radiation source .The names imply that two regions with a boundary between them exist around an antenna. Actually, as many as three regions and two boundaries exist. These boundaries are not fixed in space. Instead, the boundaries move closer to or farther from an antenna, depending on both the radiation frequency and the amount of error an application can tolerate. To talk about these quantities, we need a way to describe these regions and boundaries. A brief scan of reference literature yields the terminology in **Figure 1**. The terms apply to the two- and three-region models.



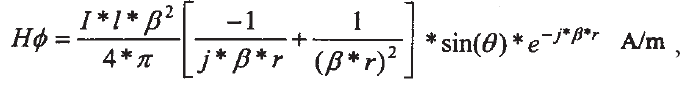
**USING AN ELEMENTAL DIPOLE’S FIELD**

Defining a near-field/far-field boundary, we use a strictly algebraic approach .We need equations that describe two important concepts: the fields from an elemental—that is, small—electric dipole antenna and from an elemental magnetic loop antenna. SK Schelkunoff derived these equations using Maxwell’s equations. We can represent an ideal electric dipole antenna by a short uniform current element of a certain length,

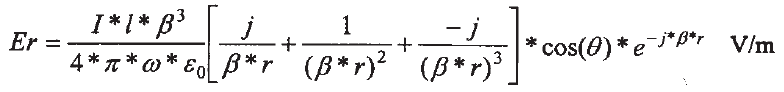
l. The fields from an electric dipole are:



(1)

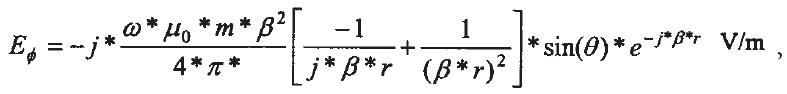


(2)

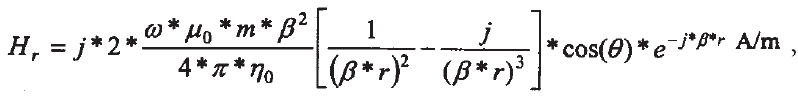


(3)

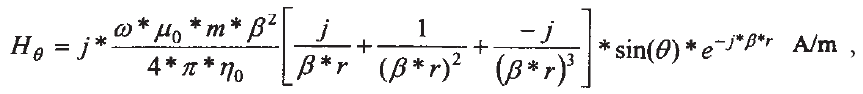
2.The fields for a magnetic dipole loop are:



(4)



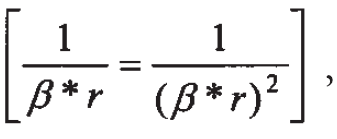
(5)



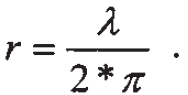
(6)

where I is the wire current in amps; l is the wire length in meters; b is the electrical length per meter of wavelength, or v/c, 2\*p/l; v is the angular frequency in radians per second, or 2\*p\*f; e0 is the permittivity of free space, or 1/36\* p\*1029 F/m;m0 is the permeability of free space, or 4\*p\*10-7 H/m; u is the angle between the zenith’s wire axis and the observation point; f is the frequency in hertz; c is the speed of light, or 3\*108m/sec; r is the distance from the source to the observation point in meters ; and h0 is the free-space impedance, or 376.7V.

**Equations 1** through **6** contain terms in 1/r, 1/r2, and 1/r3. In the near field, the 1/r3 terms dominate the **equations**. As the distance increases, the1/r3 and 1/r2 terms attenuate rapidly and, as a result, the 1/r term dominates in the far field .To define the boundary between the fields, examine the point at which the last two terms are equal. This is the point where the effect of the second term wanes and the last term begins to dominate the equations. Setting the magnitude of the terms in **Equation 2** equal to one another, along with employing some algebra ,we get r, the boundary for which we are searching:



and



Note that the **equations** define the boundary in wavelengths, implying that the boundary moves in space with the frequency of the antenna’s emissions. Judging from available literature, the distance where the 1/r and 1/r2 terms are equal is the most commonly quoted near-field/far-field boundary.

**NFC DEVICES**

**ESSENTIAL SPECIFICATIONS**

* Like [ISO 14443](http://en.wikipedia.org/wiki/ISO_14443), NFC communicates via [magnetic field](http://en.wikipedia.org/wiki/Magnetic_field) [induction](http://en.wikipedia.org/wiki/Electromagnetic_induction), where two [loop antennas](http://en.wikipedia.org/wiki/Loop_antenna) are located within each other's [near field](http://en.wikipedia.org/wiki/Near_field), effectively forming an air-core [transformer](http://en.wikipedia.org/wiki/Transformer). It operates within the globally available and unlicensed [radio frequency](http://en.wikipedia.org/wiki/Radio_frequency) [ISM band](http://en.wikipedia.org/wiki/ISM_band) of 13.56 [MHz](http://en.wikipedia.org/wiki/MHz), with a bandwidth of almost 2 MHz.
* Working distance with compact standard antennas: up to 20 cm .
* Supported data rates: 106, 212, or 424 [kbit/s](http://en.wikipedia.org/wiki/Kbit/s) .
* There are two modes:
  + Passive Communication Mode: The Initiator device provides a carrier field and the target device answers by modulating existing field. In this mode, the Target device may draw its operating power from the Initiator-provided electromagnetic field, thus making the Target device a [transponder](http://en.wikipedia.org/wiki/Transponder).
  + Active Communication Mode: 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 devices typically need to have a power supply.

|  |  |  |
| --- | --- | --- |
| [**Baud**](http://en.wikipedia.org/wiki/Baud) | **Active device** | **Passive device** |
| **424** [**kBd**](http://en.wikipedia.org/wiki/Baud) | Manchester, 10% ASK | Manchester, 10% ASK |
| **212 kBd** | Manchester, 10% ASK | Manchester, 10% ASK |
| **106 kBd** | Modified Miller,100%  ASK | Manchester, 10% ASK |
|  |  |  |

* NFC employs two different [codings](http://en.wikipedia.org/wiki/Coding) to transfer data. If an active device transfers data at 106 kbit/s, a modified [Miller coding](http://en.wikipedia.org/wiki/Miller_coding) with 100% [modulation](http://en.wikipedia.org/wiki/Modulation) is used. In all other cases [Manchester coding](http://en.wikipedia.org/wiki/Manchester_coding) is used with a modulation ratio of 10%.

NFC devices are able to receive and transmit data at the same time. Thus, they can check the radio frequency field and detect a collision if the received signal does not match with the transmitted signal**.**

**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, ECMA 340 as well as in ETSI TS 102 190. 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.

NFC devices not only implement NFCIP-1, but also NFCIP-2, which is defined in ISO 21481 , ECMA 352 and ETSI TS 102 312. NFCIP-2 allows for selecting one of three operating modes:

• NFC data transfer (NFCIP-1),

• proximity coupling device (PCD), defined in ISO 14443 , and

• vicinity coupling device (VCD), defined in ISO 15693 .

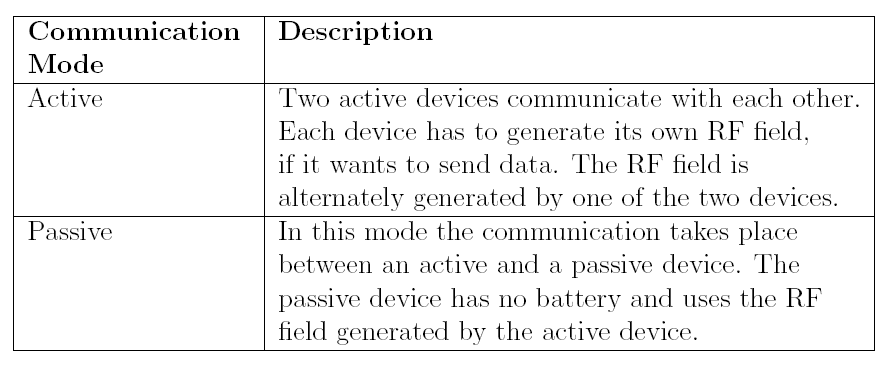
NFC devices have to provide these three functions in order to be compatible with the main international standards for smartcard interoperability, ISO 14443 (proximity cards, e.g. Philip’s Mifare ), ISO 15693 (vicinity cards) and to Sonys FeliCa contactless smart card system. Hence, as a combination of 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.

**TECHNOLOGICAL OVERVIEW**

NFC operates in the standard, globally available 13.56MHz 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.

**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 . 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 CONFIGURATION

In general, at most two devices communicate with each other at the same time. However in passive mode the initiator 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.

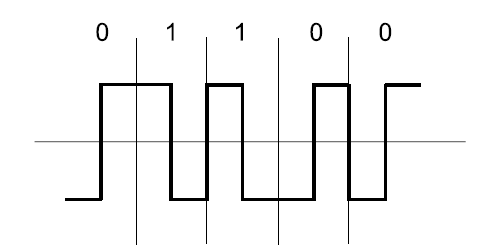
**CODING AND MODULATION**

The distinction between active and passive devices specifies the way data is transmitted. Passive devices encode data always with Manchester coding and a 10%ASK1. 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. The modulation ratio using modified Miller coding is of high importance for the security of the NFC data transfer.

**1. MANCHESTER CODE**

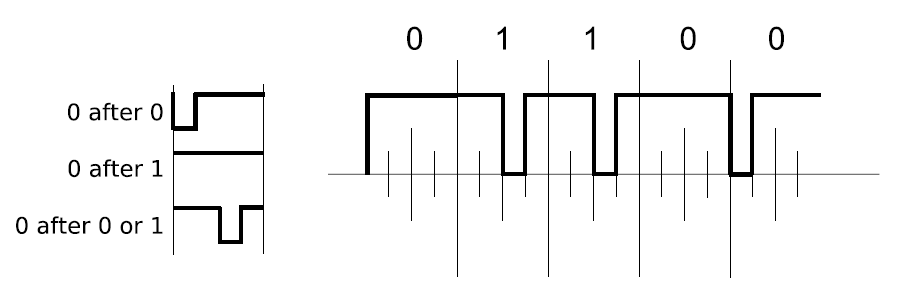
The Manchester coding depends on two possible transitions at the midpoint of a period. A low-to-high transition expresses a 0 bit, whereas a high-to-low transition stands for a 1 bit. Consequently, in the middle of each bit period there is always a transition. Transitions at the start of a period are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



MANCHESTER CODING

**2. MODIFIED MILLER CODE**

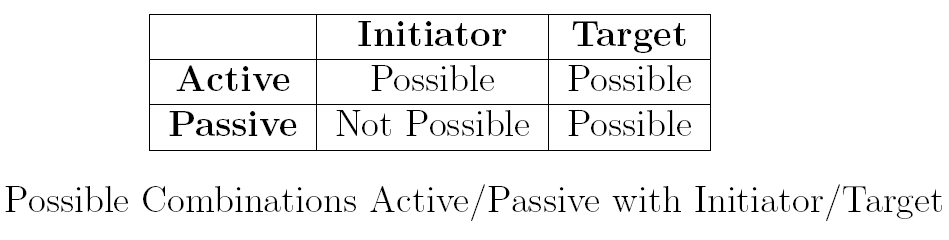
This line code is characterized by pauses occurring in the carrier at different positions of a period. Depending on the information to be transmitted, bits are coded as shown in Figure. While a 1 is always encoded in the same way, coding a 0 is determined on the basis of the preceded bit .



MODIFIED MILLER CODE

**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).



**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. If the case occurs that two or more targets answer at exactly the same time, a collision will be detected by the initiator.

**GENERAL PROTOCOL FLOW**

As shown in Figure 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.

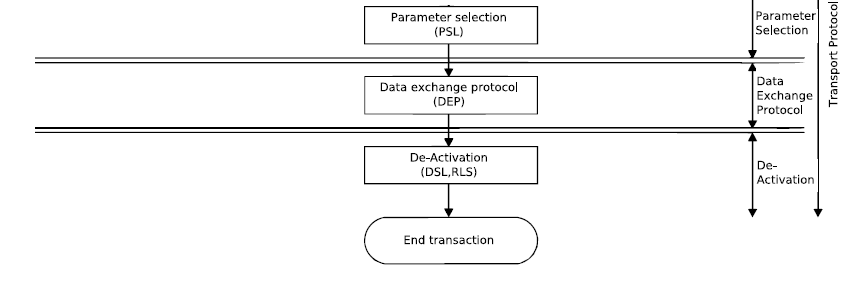
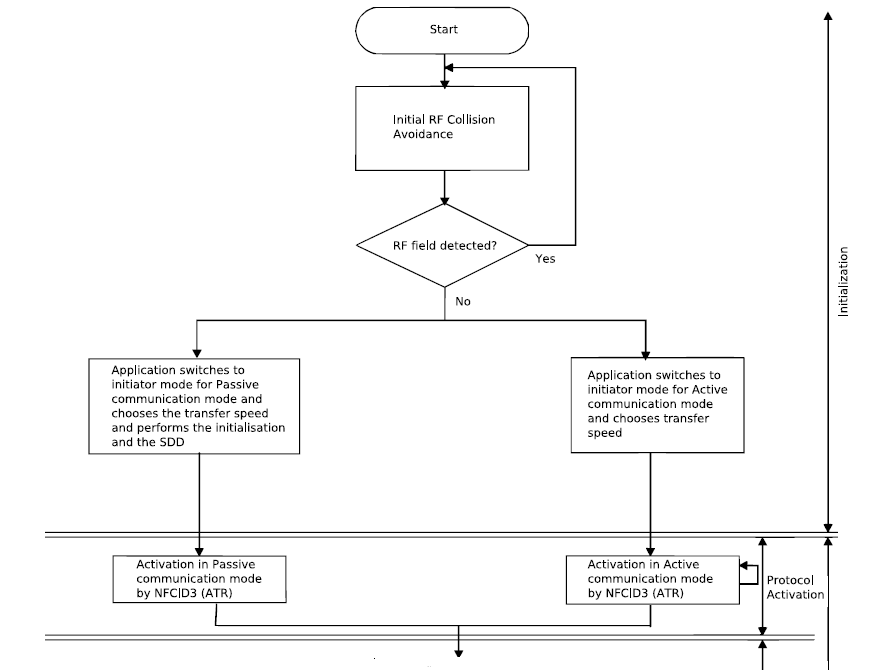
The transport protocol is divided in three parts :

• 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.

 General initialization and transport protocol

# UNIQUE FEATURES

What makes the communication between the devices so easy is that the NFC protocol provides some features not found in other general-purpose protocols.

First of all, it is a very short-range protocol. It supports communication at distances measured in centimeters . The devices have to be literally almost touched to establish the link between them. This has two important consequences:

(1) The devices can rely on the protocol to be inherently securedsince the devices must be placed very close to each other. It is easy to control whether the two devices communicate by simply placing them next to each other or keeping them apart.

(2) The procedure of establishing the protocol is inherently familiar to people: you want something to communicate – touch it. This allows for the establishment of the network connection between the devices be completely automated and happen in a transparent manner. The whole process feels then like if devices recognize each other by touch and connect to each other once touched.

Another important feature of this protocol is the support for the passive mode of communication. This is very important for the battery-powered devices since they have to place conservation of the energy as the first priority. The protocol allows such a device, like a mobile phone, to operate in a power-saving mode – the passive mode of NFC communication. This mode does not require both devices to generate the RF field and allows the complete communication to be powered from one side only. Of course, the device itself will still need to

be powered internally but it does not have to “waste” the battery on powering the RF communication interface.

Also, the protocol can be used easily in conjunction with other protocols to select devices and automate connection set-up. As was demonstrated in the examples of use above, the parameters of other wireless protocols can be exchanged allowing for automated set-up of other, longer-range, connections. The difficulty in using long-range protocols like Bluetooth or Wireless Ethernet is in selecting the correct device out of the multitude of devices in the range and providing the right parameters to the connection. Using NFC the whole procedure is simplified to a mere touch of one device to another.

**OPERATING MODES OF NFC**

NFC is a proximity coupling technology closely linked to the standard of proximity smart cards as specified in ISO 14443. NFC Devices are capable of three different operating modes:

**PEER-TO-PEER MODE (NFC):**

This mode is the *classic* NFC mode, allowing data connection for up to 424kBit/sec. The electromagnetic properties and theprotocol (NFCIP-1) is standardized in ISO 18092and ECMA 320/340.

**READER/WRITER MODE (PCD):**

NFC devices can be used as a reader/writer for tags and smart cards. In this case the NFC device acts as an initiator and the passive tag is the target. In reader/writer mode data rates of 106 kBit/sec are possible.

**TAG EMULATION MODE (PICC):**

In this mode the NFC device emulates an ISO 14443 smart card or a smart card chip integrated in the mobile devices is connected to the antenna of the NFC module. A legacy reader can’t distinguish a mobile phone operating in tag emulation mode from an ordinary smart card.

This is an advantage of NFC technology as already existing reader infrastructures do not need to be replaced. The smart card chip used for tag emulation is also referred to as secure element **COMPARISON WITH OTHER TECHNOLOGY**

**1.NFC AND RFID**

The heritage of earlier standards gives NFC compatibility benefits with existing RFID applications, such as access control or public transport ticketing – it is often possible to operate with old infrastructure, even if the RFID card is replaced with an NFC-enabled mobile phone, for example. This is possible because of NFC’s capability to emulate RFID tags (“card interface mode”). NFC hardware can include a secure element for improved security in critical applications such as payments. For example, a credit card could be integrated into a mobile phone and used over NFC. NFCIP-1 is an NFC-specific communication mode, defined in the ECMA-340 standard. This mode is intended for peer-to-peer data communication between devices. In this mode, NFC is comparable to other short-range communication technologies such as IrDA, although the physical data transfer mechanism is different.

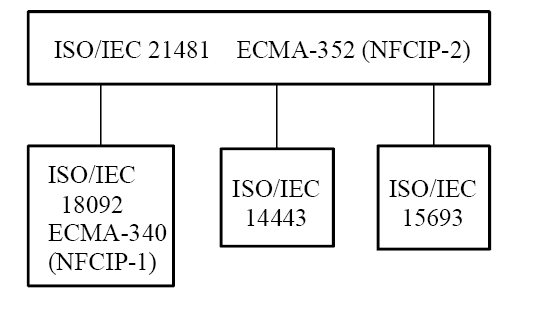
Basically, the technologies Radio Frequency Identification and Near Field Communication use the same working standards. However, the essential extension of RFID is the communication mode between two active devices. In addition to contactless smart cards (ISO 14443), which only support communication between 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.

NFCIP-1 is an NFC-specific communication mode, defined in the ECMA-340 standard. This mode is intended for peer-to-peer data communication between devices. In this mode, NFC is comparable to other short-range communication technologies such

as IrDA, although the physical data transfer mechanism is different. The NFCIP-1 mode is divided into two variants: active mode and passive mode. In active mode, both participants generate their own carrier while transmitting data. In passive mode, only the initiator generates a carrier during communications, and the target device uses load modulation when communicating back to the initiator, in a way similar to passive RFID tag behavior . This makes it possible to save power in the target device, which is a useful feature if the target device has a very restricted energy source, such as a small battery. It is possible to make a target device – such as a sensor readable over NFC – last for several years, even if operated from a small lithium coin-cell battery.

NFCIP-2 (specified in ECMA-352) defines how to automatically select the correct operation mode when starting communications. This and related standards are shown in Fig.

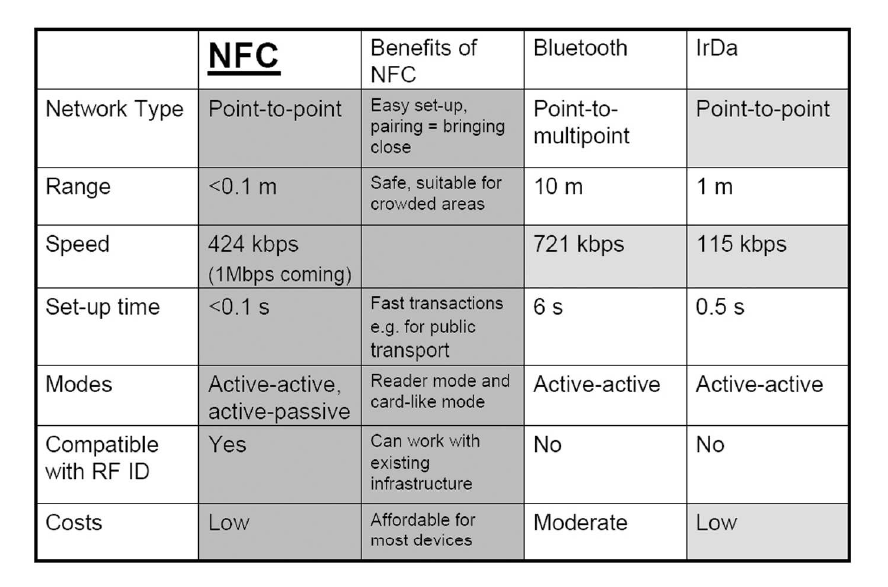


The upper layer defines the mechanism of Selecting

the communication mode on the lower layer.

**2 .COMPARISON WITH BLUETOOTH AND INFRARED**

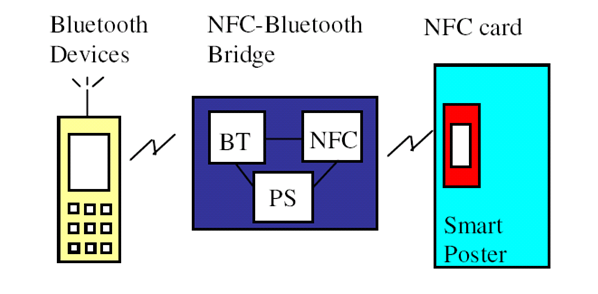
Compared to other short-range communication technologies, which have been integrated into mobile phones, NFC simplifies the way consumer devices interact with one another and obtains faster connections. The problem with infrared, the oldest wireless technology introduced in 1993, is the fact that a direct 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-uptime. Instead of performing manual configurations to identify the other’s phone, the connection between two NFC devices is established at once (<0,1s). Table 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 compared with Bluetooth and IrDa**

Near Field Communication (NFC) is an emerging wireless technology that is designed to facilitate secure, short-range communication between electronic devices such as mobile phones, personal data assistants (PDAs), computers and payment terminals. The concept is simple: in order to make two devices communicate, bring them together or make them touch. This will engage the wireless interface of the two devices and configure them to link up in a peer-to-peer network . Once the device is linked up using NFC, they can continue communication using long range and faster protocols such as Bluetooth or wireless Internet (WiFi).

**NFC-BLUETOOTH BRIDGE SYSTEM**

The system architecture of the NFC-Bluetooth Bridge System is shown in Fig. It comprises a Bluetooth enabled device, the proposed NFC-Bluetooth Bridge and an NFC card which is embedded on a smart poster.

 NFC-BLUETOOTH BRIDGE ARCHITECTURE

The NFC-Bluetooth Bridge is a separate electronic device with two different air interfaces: Bluetooth (BT) and NFC. In our prototype development, the serial NFC PN531 module from Philips Electronics was used to provide the NFC air interface, and the serial Initium Promi SD102 Bluetooth adapter was used to provide the Bluetooth air interface. Both the NFC module and the Bluetooth adapter were connected by a RS232 cable and communicated using the following RS232 protocol: 9600 baud, 8 data bits, 1 stop bit and no parity bit. The Bluetooth

adapter was configured to the discoverable and connectable mode. This mode allows the adapter to be discovered when a mobile device searches for it by the device name. Password authentication was enabled for pairing of the two Bluetooth devices.

The Bluetooth and NFC modules require a 5 VDC power supply each. A PCB (labeled as PS in Fig.) is used to share the power drawn from an external power supply to the two component modules. Driver software is needed in the mobile device to drive the NFC PN531 on the NFC-Bluetooth Bridge to react to NFC targets that are tapped between each other, and to send and receive information from it.

**SECURITY ASPECTS**

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. To analyze the security aspects of NFC two veryinteresting papers have been published. In Ernst Haselsteiner and KlemensBreitfuß discuss “some threats and solution for the security of NFC”, and also thepaper ”Security Aspects and Prospective Applications of RFID Systems” gives some useful information.

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. The 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 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.

**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. 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 . 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. 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.

**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.

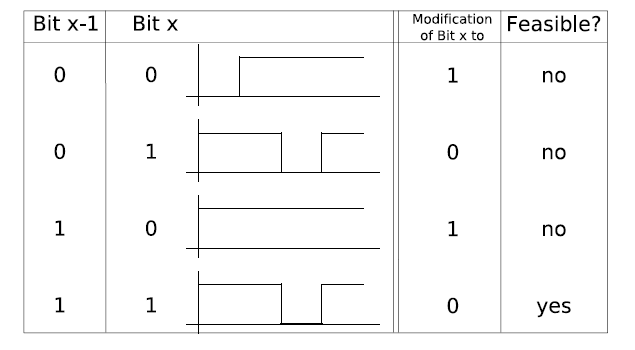
**3 DATA MODIFICATION**

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. The data can be 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). 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 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 . 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.

Three countermeasures are described here. 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. Denoted as the ”probably best solution” is the use of a secure channel. This would provide data integrity.

**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 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.

**USES AND APPLICATIONS**

NFC technology is currently mainly aimed at being used with mobile phones. There are three main use cases for NFC:

* card emulation: the NFC device behaves like an existing contactless card
* reader mode: the NFC device is active and read a passive RFID tag, for example for interactive advertising
* P2P mode: two NFC devices are communicating together and exchanging information.

Plenty of applications are possible, such as:

* Mobile ticketing in public transport — an extension of the existing contactless infrastructure.
* [Mobile payment](http://en.wikipedia.org/wiki/Mobile_payment) — the device acts as a debit/ credit payment card.
* Smart poster — the mobile phone is used to read [RFID](http://en.wikipedia.org/wiki/RFID) tags on outdoor billboards in order to get info on the move.
* Bluetooth pairing — in the future pairing of Bluetooth 2.1 devices with NFC support will be as easy as bringing them close together and accepting the pairing. The process of activating Bluetooth on both sides, searching, waiting, pairing and authorization will be replaced by a simple "touch" of the mobile phones.

**FUTURE APPLICATION**

* [Electronic ticketing](http://en.wikipedia.org/wiki/Electronic_ticket) — airline tickets, concert/event tickets, and others
* [Electronic money](http://en.wikipedia.org/wiki/Electronic_money)
* [Travel cards](http://en.wikipedia.org/wiki/Travel_card)
* [Identity documents](http://en.wikipedia.org/wiki/Identity_document)
* [Mobile commerce](http://en.wikipedia.org/wiki/Mobile_commerce)
* [Electronic keys](http://en.wikipedia.org/wiki/Remote_keyless_system) — car keys, house/office keys, hotel room keys, etc.
* NFC can be used to configure and initiate other wireless network connections such as [Bluetooth](http://en.wikipedia.org/wiki/Bluetooth) , [Wi-Fi](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup) or [Ultra-wideband](http://en.wikipedia.org/wiki/Ultra-wideband).
* NFC for Health Monitoring in Daily Life .

**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 ,Wifi .

NFC is based on existing contactless infrastructure around the world that is already in use by millions of people on a daily basis. NFC is not a fashionable nice-to-have technology, but actually a technology that makes peoples lives easier – easier to pay for goods and services, easier to use public transport, and easier to share data between devices.

BIBLIOGRAPHY

* 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.
* Ecma International: Standard ECMA-340, Near Field Communication Interface and Protocol(NFCIP-1),December2004,URL:http://www.ecma-international.org/publications/standards/Ecma-340.htm.
* José Bravo, Ramón Hervás , Gabriel Chavira From Implicit to Touching Interaction: RFID and NFC Approaches ,Sixth International Conference on the Management of Mobile Business (ICMB 2008)0-7695-2803-1/07 $25.00 © 2008 IEEE
* Anokwa, Y., et al. A User Interaction Model for NFC Enabled Applications . in *IEEE International Conference on Pervasive Computing and Communications Workshops* 2007. New York ,USA.
* A Framework for Integration of Radio Frequency Identification and RichInternet Applications
* Mikko Koskela, Jorma Ylinen and Pekka Loula *Telecommunication Research Center* Proceedings of the *ITI 2007 29th Int. Conf. on Information Technology Interfaces,* June 25-28, 2007, Cavtat , Croatia
* Near Field Communication and Bluetooth Bridge System for Mobile Commerce C.Y. Leong, K. C. Ong , K. K. Tan\*, O.P. GAN *2006 IEEE International Conference on Industrial Informatics*
* WIKIPEDIA
* [*WWW.NFCFORUM.COM*](http://WWW.NFCFORUM.COM)
* www.ecma-international.org