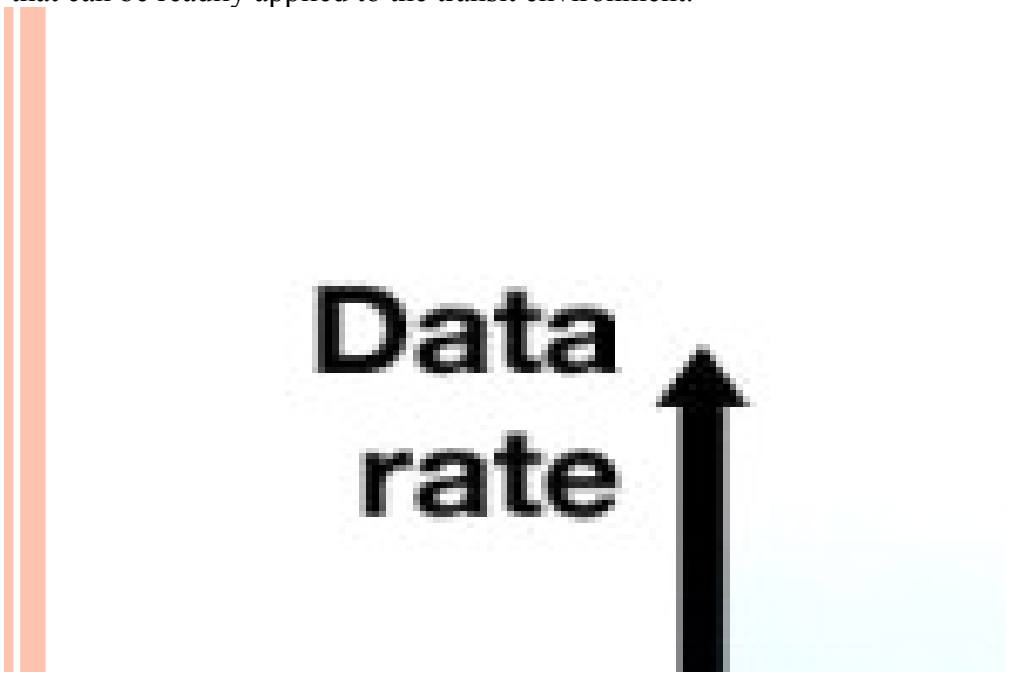
NEAR FIELD COMMUNICATION

Near field communication, or NFC, is a standards-based, short-range wireless technologies, typically requiring a distance of 4 cm or less. NFC operates at 13.56 MHz and at rates ranging from 106 kbit/s to 848 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC peer-to-peer communication is also possible, where both devices are powered. technology that enables simple and intuitive two-way interactions between electronic devices. NFC simplifies setup of some longer-range wireless technologies, such as Bluetooth and Wi-Fi. RFID reader antennas emit electromagnetic radiation (radio waves). If an RFID tag is within full wavelength of the reader, it is sometimes said to be in the "near field" (as with many RFID terms, definitions are not precise). If it is more than the distance of one full wavelength away, it is said to be in the "far field." The near field signal decays as the cube of distance from the antenna, while the far field signal decays as the square of the distance from the antenna. So passive RFID systems that rely on near-field communication (typically low- and high-frequency systems) have a shorter read range than those that use far field communication (UHF and microwave systems).

The following chart shows how NFC compares in range and speed with other wireless technologies that can be used in a mobile phone. Communication occurs when two NFC-compatible devices are brought within about four centimeters of each other. By design, NFC requires close proximity and it offers instant connectivity, which provides an intuitive consumer experience that can be readily applied to the transit environment.



Essential Specifications

- As with proximity card technology, near-field communication is mediated by magnetic induction between two loop antennas located within each other's near field, effectively forming an air-core transformer. It operates within the globally available and unlicensed radio frequency ISM band of 13.56 MHz. Most of the RF energy is concentrated in the allowed 14 kHz bandwidth range, but the full spectral envelope may be as wide as 1.8 MHz when using ASK modulation.
- Working distance with compact standard antennas: up to 20 cm
- Supported data rates: 106, 212, 424 or 848 kbit/s
- There are two modes:
    - Passive Communication Mode: The Initiator device provides a carrier field and the target device answers by modulating the 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.
    - Active Communication Mode: Both Initiator and Target device communicate by alternately generating their own fields. A device deactivates its RF field while it is waiting for data. In this mode, both devices typically have power supplies.

Baud	Active device	passive device
424 kBd	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 coding to transfer data. If an active device transfers data at 106 kbit/s, a modified Miller coding with 100% modulation is used. In all other cases 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 need to check the radio frequency field and can detect a collision if the received signal matches the transmitted signal's modulated frequency band.

Comparison with Bluetooth

	NFC	Bluetooth	Bluetooth Low Energy
RFID compatible	ISO 18000-3	active	active
Standardisation body	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Network Standard	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1
Network Type	Point-to-point	WPAN	WPAN
Cryptography	not with RFID	available	available
Range	< 0.2 m	~10 m (class 2)	~1 m (class 3)
Frequency	13.56 MHz	2.4-2.5 GHz	2.4-2.5 GHz
Bit rate	424 kbit/s	2.1 Mbit/s	~1.0 Mbit/s
Set-up time	< 0.1 s	< 6 s	< 1 s
Power consumption	< 15mA (read)	varies with class	< 15 mA (xmit)

NFC and Bluetooth are both short-range communication technologies which are integrated into mobile phones. To avoid a complicated configuration process, NFC can be used for the set-up of wireless technologies, such as Bluetooth.

NFC sets up faster than standard Bluetooth, but is not much faster than Bluetooth low energy. With NFC, instead of performing manual configurations to identify devices, the connection between two NFC devices is automatically established quickly — in less than a tenth of a second. The maximum data transfer rate of NFC (424 kbit/s) is slower than that of Bluetooth V2.1 (2.1 Mbit/s). With a maximum working distance of less than 20 cm, NFC has a shorter range, which reduces the likelihood of unwanted interception. That makes NFC particularly suitable for crowded areas where correlating a signal with its transmitting physical device (and by extension, its user) becomes difficult.

In contrast to Bluetooth, NFC is compatible with existing passive RFID (13.56 MHz ISO/IEC 18000-3) infrastructures. NFC requires comparatively low power, similar to the Bluetooth V4.0 low energy protocol. However, when NFC works with an unpowered device (e.g. on a phone that may be turned off, a contactless smart credit card, a smart poster, etc.), the NFC power consumption is greater than that of Bluetooth V4.0 Low Energy. Illumination of the passive tag needs extra power.

Uses and applications

NFC technology is intended mainly for use in mobile phones. There are currently three specific uses for NFC:

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

Plenty of applications are possible, such as:

- Mobile ticketing in public transport: an extension of the existing contactless infrastructure, such as Mobile Phone Boarding Pass.
- Mobile payment: the device acts as a debit/credit payment card.
- Smart poster: the mobile phone is used to read RFID tags on outdoor billboards.
- 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 simply bringing the mobile phones close to each other.

Other applications in the future could include:

- Electronic ticketing: airline tickets, concert/event tickets, and others
- Electronic money
- Travel cards
- Identity documents
- Mobile commerce
- Electronic keys: replacements for physical car keys, house/office keys, hotel room keys, etc.
- NFC can be used to configure and initiate other wireless network connections such as Bluetooth, Wi-Fi or Ultra-wideband.

Standardization bodies and industry projects

Standards

NFC was approved as an ISO(International Standards Organisation)/IEC(International Technical Commission) standard on December 8, 2003 and later as an ETSI (European Telecommunications Standards Institute), and ECMA (European association for standardizing information and communication systems).

NFC is an open platform technology standardized in ECMA-340 and ISO/IEC 18092. These standards specify the modulation schemes, coding, transfer speeds and frame format of the RF interface of NFC devices, as well as initialization schemes and conditions required for data

collision-control during initialization for both passive and active NFC modes. Furthermore, they also define the transport protocol, including protocol activation and data-exchange methods. The air interface for NFC is standardized in:

ISO/IEC 18092 / ECMA-340

Near Field Communication Interface and Protocol-1 (NFCIP-1)

ISO/IEC 21481 / ECMA-352

Near Field Communication Interface and Protocol-2 (NFCIP-2)

NFC incorporates a variety of existing standards including ISO/IEC 14443 both Type A and Type B, and FeliCa. NFC enabled phones work basically, at least, with existing readers. Especially in "card emulation mode" a NFC device should transmit, at a minimum, a unique ID number to an existing reader.

In addition, the NFC Forum has defined a common data format called NFC Data Exchange Format (NDEF), which can store and transport various kinds of items, ranging from any MIME-typed object to ultra-short RTD(Record Type Definition)-documents, such as URLs.

NDEF is conceptually very similar to MIME. It is a dense binary format of so-called "records", in which each record can hold a different type of object. By convention, the type of the first record defines the context of the entire message.

GSMA

The GSM Association (GSMA) is the global trade association representing 700 mobile phone operators across 218 countries of the world.

StoLPaN

StoLPaN (‘Store Logistics and Payment with NFC’) is a pan-European consortium supported by the European Commission’s Information Society Technologies program. StoLPaN will examine the as yet untapped potential for bringing together the new kind of local wireless interface, NFC and mobile communication.

NFC Forum

The NFC Forum is a non-profit industry association announced on March 18, 2004 by NXP Semiconductors, Sony and Nokia to advance the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs. The NFC Forum promotes implementation and standardization of NFC technology to ensure interoperability between devices and services. In September 2008, there were over 150 members of the NFC Forum.

Alternative Form Factors

To realize the benefits of NFC in cellphones not yet equipped with built in NFC chips a new line of complementary devices were created. MicroSD and UICC SIM cards were developed to incorporate industry standard contactless smartcard chips with ISO14443 interface, with or without built in antenna. The microSD form factor with built in antenna has the greatest potential as bridge device to shorten the time to market of contactless payment and couponing applications, while the built in NFC contollers gain enough market share.

Other standardization bodies

Other standardization bodies that are involved in NFC include:

- ETSI / SCP (Smart Card Platform) to specify the interface between the SIM card and the NFC chipset.
- Global Platform to specify a multi-application architecture of the secure element.
- EMVCo for the impacts on the EMV payment applications.

Security aspects

Although the communication range of NFC is limited to a few centimeters, NFC alone does not ensure secure communications. In 2006, Ernst Haselsteiner and Klemens Breitfuß described different possible types of attacks, and detail how to leverage NFC's resistance to Man-in-the-middle attacks to establish a specific key. Unfortunately, as this technique is not part of the ISO standard, NFC offers no protection against eavesdropping and can be vulnerable to data modifications. Applications may use higher-layer cryptographic protocols (e.g., SSL) to establish a secure channel.

Eavesdropping

The RF signal for the wireless data transfer can be picked up with antennas. The distance from which an attacker is able to eavesdrop the RF signal depends on numerous parameters, but is typically a small number of meters. Also, eavesdropping is extremely affected by the communication mode. A passive device that does not generate its own RF field is much harder to eavesdrop on than an active device. One Open source device that is able to eavesdrop on passive and active NFC communications is the Proxmark instrument.

Data modification

Data destruction is relatively easy to realize. One possibility to perturb the signal is the usage of an RFID jammer. There is no way to prevent such an attack, but if the NFC devices check the RF field while they are sending, it is possible to detect it.

Unauthorized modification of data which results in valid messages is much more complicated, and demands a thorough understanding. In order to modify the transmitted data, an intruder has to deal with the single bits of the RF signal. The feasibility of this attack, i.e., if it is possible to

change the value of a bit from 0 to 1 or the other way around, is amongst others subject to the strength of the amplitude modulation. If data is transferred with the modified Miller coding and a modulation of 100%, only certain bits can be modified. A modulation ratio of 100% makes it possible to eliminate a pause of the RF signal, but not to generate a pause where no pause has been. Thus, only a 1 which is followed by another 1 might be changed. Transmitting Manchester-encoded data with a modulation ratio of 10% permits a modification attack on all bits.

Relay attack

Because NFC devices usually include ISO/IEC 14443 protocols, the relay attacks described are also feasible on NFC. For this attack the adversary has to forward the request of the reader to the victim and relay back its answer to the reader in real time, in order to carry out a task pretending to be the owner of the victim's smart card. One of libnfc code examples demonstrates a relay attack using only two stock commercial NFC devices.

Lost property

Losing the NFC RFID card or the mobile phone will open access to any finder and act as a single-factor authenticating entity. Mobile phones protected by a PIN code acts as a single authenticating factor. A way to defeat the lost-property threat requires an extended security concept, that includes more than one physically independent authentication factor.

Walk off

Lawfully opened access to a secure NFC function or data is protected by time-out closing after a period of inactivity. Attacks may happen despite provisions to shutdown access NFC after the bearer has become inactive. The known concepts described primarily do not address the geometric distance of a fraudulent attacker using a lost communication entity against lawful access from the actual location of the registered bearer. Additional feature to cover such attack scenario dynamically shall make use of a second wireless authentication factor that remains with the bearer in case of lost NFC communicator. Relevant approaches are described as electronic leash or equivalent *wireless key*.

NFC-enabled handsets

- Nokia C7-00
- Nokia 6216 Classic (Nokia has confirmed the cancellation of this phone in February 2010)
- Nokia 6212 Classic
- Nokia 6131 NFC[1]
- Nokia 3220 + NFC Shell
- Samsung S5230 Tocco Lite/Star/Player One/Avila
- Samsung SGH-X700 NFC
- Samsung D500E
- SAGEM my700X Contactless
- LG 600V contactless
- Motorola L7 (SLVR)
- Benq T80

- Sagem Cosyphone
- Google Nexus S
- Samsung Galaxy S II
- Samsung Wave 578

References:

http://www.nfc-forum.com

http://en.wikipedia.org/wiki/Near_field_communication

http://www.ecma-international.org