**NEAR FIELD COMMUNICATION**

Near Field Communication or NFC is a short-range [high frequency](http://en.wikipedia.org/wiki/High_frequency) wireless communication technology which enables the exchange of data between devices over about a 10 centimetre (around 4 inches) distance. This was jointly developed by Philips and Sony. The technology is a simple extension of the [ISO/IEC 14443](http://en.wikipedia.org/wiki/ISO/IEC_14443) proximity-card standard ([proximity card](http://en.wikipedia.org/wiki/Proximity_card), [RFID](http://en.wikipedia.org/wiki/RFID)) that combines the interface of a smartcard and a reader into a single device. An NFC device can communicate with both existing ISO/IEC 14443 smartcards and readers, as well as with other NFC devices. NFC is primarily aimed at usage in [mobile phones](http://en.wikipedia.org/wiki/Mobile_phone). 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 frequency of 13.56 MHz. Its supported data rates are 106, 212, or 424 [Kbit/s](http://en.wikipedia.org/wiki/Kbit/s).

In NFC, communication takes place between an initiator and a target. The target responds to the initiator. The initiator performs collision detection on any targets within its field that try to respond.NFC allows communication between either two powered devices or between a powered and a non self-powered device. Hence there are 2 communication 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](http://en.wikipedia.org/wiki/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.

NFC employs two different [coding](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 need to check the radio frequency field and can detect a collision if the received signal does not match with the transmitted signal.

**Applications**

NFC technology is currently aimed mainly at being used with 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 are communicating together and exchanging information.

Some of the applications require security for controlling access to financial transactions, and some do not because they are just information gathering or transmitting of non-critical data such as camera images or loyalty card numbers. For financial transactions that require security, the NFC Initiative proposes using a trusted service manager (TSM) between the service provider and mobile network operator layers. These are third party organizations that maintain the security data, meet certain physical storage and protection requirements, and act as liaisons between the customer and the service providers.

***Available applications include:***

* 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.

#### Other applications in the future could include:

* [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): 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](http://en.wikipedia.org/wiki/Ultra-wideband).

The view of the NFC phone is that it will run multiple independent applications that would each replace a credit, debit, transportation, access, or loyalty card, an electronic wallet.

**Advantages**

The significant advantage of NFC over Bluetooth is the shorter set-up time. Instead of performing manual configurations to identify Bluetooth devices, the connection between two NFC devices is established at once (<0.1s). In contrast to Bluetooth, NFC is compatible to existing RFID structures. With less than 20 cm, NFC has a shorter range, which provides a degree of security and makes NFC suitable for crowded areas. NFC can work with an unpowered device (e.g. on a phone that may be turned off, a contactless smart credit card, a smart poster, etc.)

**Disadvantages**

* NFC offers no protection against eavesdropping and is also vulnerable to data modifications. Applications have to use higher-layer [cryptographic protocols](http://en.wikipedia.org/wiki/Cryptographic_protocol) (e.g., [SSL](http://en.wikipedia.org/wiki/Secure_Sockets_Layer)) to establish a secure channel.
* The maximum data transfer rate of NFC (424 kbit/s) is slower than Bluetooth (721 kbit/s).

**References:**

### 1. Fischer, J.; [NFC in cell phones: The new paradigm for an interactive world [Near-Field Communications]](http://ieeexplore.ieee.org/search/srchabstract.jsp?tp=&arnumber=5116794&queryText%3DNFC+IN+CELL+PHONES%3A+THE+NEW+PARADIGM+FOR+AN+INTERACTIVE+WORLD%26openedRefinements%3D*%26searchField%3DSearch+All) ,[Communications Magazine, IEEE](http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=35) 2009

**2.**NFC Forum, Essentials for Successful NFC Mobile Ecosystems, white paper October 2008

*COLLEGE OF ENGINEERING CHENGANNUR*

SEMINAR

ABSTRACT

SUBMITTED BY

Amritha Alex Panicker

Class:S7-D

Roll No: 3