NFC – Near Field Communication: What it is, Applicability, Present and Future

Abstract

The main aim of this survey is to share light on NFC, providing insight about what is known about it and its applicable suitability. It starts by accounting the development and evolution of wireless communication systems like Radio Frequency Identification (RFID) up until the appearance of Near Field Communication (NFC) (which originated directly from RFID), its impressions, practicality, security and applicatory aspects. Furthermore, the survey also focuses on some of the present and near future advantages (and disadvantages) of NFC applications, as some applications based on this technology are available presently, while some other are still under development. Finally, a theoretical device called *N-Key* is presented and discussed to better show the possibilities and commodities that NFC technology can provide.

Keywords: NFC, Near Field Communication, RFID, Radio Frequency Identification

1. Introduction

The creation and evolution of computer technology allowed its users to store and process data much faster. Subsequently, the possibility to share such data with others by creating networks of computers was soon a reality. The search for the easier way to communicate then developed and enhanced the popularity of wireless communication interfaces between computers. New technologies and wireless devices such as notebooks, smartphones, PDAs and mobile phones became part of the daily lives of people by making sure that everyday tasks were executed with a less bureaucratic and more flexible or manual communication. The amount of functions that such a device can have or run is quite diverse and appealing, but often with the need for numerous selections of items or navigation menus and submenus. The continued evolution began the spreading and consolidation of technologic contactless cards (contactless) that has been used increasingly by the transportation, retail and financial industries that quickly realised the possibility of expanding this functionality to mobile phones. These results lead to the necessity and creation of Near Field Communication. This is a relatively new technology with great potential that allows wireless communication (wireless) between two devices through one simple connection between both, without the need for the users to enter passwords, click buttons or perform some sort of action to establish the connection. Despite its short range, it opens new highways for an extensive list of applications and proposes advantages in security and operations. We must have in mind that, globally, the year 2011 was of paramount importance for NFC, which means that the technology would certainly be the focus of attention worldwide in the near future.

2. The Advent of NFC

Wireless technology networks have been around since the mid-eighties, when the development of Wireless Local Area Networks (WLAN's) from the use of different technologies such as infrared, radio and microwave radio wave scattering started. Over the years, we understood the need to create new patterns and networks and, in 1997, the Institute of Electrical and Electronics Engineers - IEEE - launched a specific standard for wireless networks called 802.11. At the same time, other standards like HiperLAN/2 and Bluetooth were created. Thereafter, a vivid interest in this market started to form, significantly increasing the number of systems with this technology and increasing the transmission rates thanks to the evolution of the protocol versions for 802.11a/b/g. Thus, the market became more attractive to invest in infrastructures. Today, and due to market needs, new models of ultrasound, optical and radiofrequency waves' wireless networks arise. Also known as Radio Frequency Identification (RFID), this type of radiofrequency allows two devices to communicate over long distances. One of them has an energy source and works actively by seeking information on another device, which does not require a power source to run itself. The evolution of RFID originated NFC (Near Field Communication) which, as its name suggests, limits the field of action of frequencies, and so one must be very close to the object so that there is data exchange. It is important to note that the data is obtained by the active source from the passive source. This means that the information that is stored in any device that uses this technology cannot be accessed by other devices. The main purpose for the creation of this technology was to transmit data more securely. NFC has gained prominence by gathering almost all models of wireless networks in the market, thus making it the most flexible and comprehensive range of communication applications. The possibility of applications for NFC is very broad due to its adaptation in many electronic devices. Faced with the scenario of technology's tremendous and fast expansion, several companies joined Sony and Philips, initially the creators of this technology, to form the NFC Forum, a selected and growing group of researchers and coordinators of NFC technology. In fact, not only the physical companies are together in this project but also their previous technologies. Almost with no external help, this important joint venture shaped and widened the scope of NFC, making it part of the framework of world renowned quality ISO standards.

3. NFC

3.1 What is NFC?

NFC, or Near Field Communication, is a technology dating back from 2005 and that aims to facilitate the communication between wireless devices, allowing the exchange of varied information between them. The condition under which this communication takes place is supervised by NFCIP - 1 (Near Field Communications Interface Protocol - 1). This protocol regulates wireless communication between electronic devices at a frequency of 13.56 MHz The main characteristic of this technology, which includes the origin of its name, is the very short distance at which data is exchanged: zero to twenty centimetres. By simply touching two devices this technology establishes a point to point communication between them, thus enabling the exchange of data. Passwords, tokens or configurations are not required, and this technology is both read/write. Communication between two NFC-compatible devices occurs when they are close to each other. The lower layers of this technology are based on standards set by organisms like ISO, ECMA, and ETSI. For maximum operating distance, NFC-based transactions are considered secure, as it provides control to whoever uses it. It is noteworthy that one of the most interesting characteristics of NFC is that it can only be used to establish the initial connection between devices, that is, to identify each one. After that, the exchange of data can be done using some other protocol like Bluetooth or Wi-Fi, which allows the connection to be maintained even if the two devices distance from one another.

Ticketing
Identification
Time & Attendance
NFC
Loyalty & Memberships
Physical Access
Cashless Payment
Transit
Secure PC Log-On

Picture 1 – Representation of NFC and its most important satellite applications. It is "a technology for high frequency wireless short-distance point-to-point communication." [Allah, 2011] This type of communication is starting to prove invaluable especially in the public and private transportation sector and that, by just clicking a button and pointing a smartphone at specific target receivers with an enhanced NFC chip, transactions are completed in a fast and safe manner.

3.1.1 Ubiquitous computing and how NFC relates to it

Mark Weiser coined the term *ubiquitous computing* in 1988, as he theorized that "The basic idea of ubiquitous computing is that computing moves outside of workstations and personal computers (PCs) and becomes pervasive in our everyday life." [Weiser, 1991] Marc Weiser envisioned more than a decade ago that, in the future, computers will be embedded into the most trivial everyday objects: clothing labels, coffee cups, light switches, pens, an advertisement on a magazine, etc., and which will be invisible to the user. In Weiser's world, we must learn to live with computers, not just interact with them, as his concept enforces the idea of people communicating with computers without the need of apparatuses such as a mouse, a keyboard, etc., but instead using natural gestures like a wrist movement. Let's observe the following illustrative scenario to better understand some of the questions involved in the defying area of research that NFC is proving to be.

A geologist from the American Institute of Geology was sent to a remote location in the western U.S. to examine the effects of a recent earthquake. Using a PC and software called MANNA that supports the activities of the geologist on any device that he uses he downloads existing maps and reports on the area in order to prepare for the visit. As the PC is not a mobile device and because the geologist must travel, the documents are transferred to a laptop and the geologist takes a plane to where the earthquake occurred. On this plane there is no supported network, so the laptop disables network connections and provides only local computation. When the geologist examines the videos of the site, the user interface toggles automatically to a black and white monitor and reduces the rate of frames per second to help conserve the battery's charge. Upon arriving at the airport, the geologist rents a car and drives to the location. He receives a message through MANNA by phone, alerting him to look at a particular location. As the cellular phone offers extremely limited screen space, the map of the region is not shown. Instead, the phone shows the geographic location, directions on how to get there and the current position (GPS) of the Geologist. A feature that allows the geologist to answer the message is also offered by the software. Arriving at the scene, the geologist uses his palmtop to take notes on the region. As the palmtop has a touch pen for interaction, interaction is not allowed by double clicking or right clicking. Furthermore, as the palmtop's screen size is also a problem, a more conservative layout is adopted to be shown to the geologist. Upon completing the investigation, the geologist prepares a presentation in two formats. First, a presentation of his journey through the site, with notes, is made to the HUD (heads up display). As the HUD has limited capacity to handle text input (it uses its own mobile device), the MANNA application offers voice-based interaction. Another presentation, more conventional, is ready to be viewed on screen. As the purpose of the presentation on the screen is not the interaction, interaction mechanisms are removed. (Eisenstein et all, 2000)

We can observe in the hypothetical scenario above that:

- Information is accessed through multiple heterogeneous devices
- The application follows the user while he's on the move
- The devices interact
- Some tasks are performed autonomously
- The panorama exchanges information with the devices and vice versa
- The MANNA application responds to the environment

Hence, instead of just playing a paramount role in ubiquitous computing, NFC technology IS ubiquitous computing. To better understand how, we then must perceive how the NFC technology works.

3.2. How does NFC Work?

NFC is a technology that was developed to enable communication between two devices. The principle is simple: one device plays the role of Initiator, accounting for the tasks of initiating communication and controlling the exchange of information. The other device plays the role of Target and it will respond to the Initiator's requests. According to the NFC Forum, the three main uses of NFC currently are sharing, synchronization and transactions. For two devices to communicate using NFC one of them must have an NFC reader/writer and the other must have an NFC tag. The tag is essentially an integrated circuit containing data, connected to an antenna, which can be read and written by the device. The NFC also has two modes of operation:

- Active Mode - In this mode, both devices generate the radiofrequency field to perform the transmission. Information is encoded using Miller code with a modulation of 100%, reaching a transmission rate of 106Kbps. The active mode is suggested for communication between devices that perform interactive actions, as in the case of payments via smartphone. In the case of Electronic Wallet, both the receiver (the equipment that is installed in an establishment) and the initiator generate magnetic fields to communicate.

- Passive Mode - In this mode, only one device generates the radiofrequency field to perform the transmission, using Manchester encoding with a modulation rate of 10%, allowing it a transmission of up to 424Kbps. The initiator provides a magnetic holder, which induces current in the antenna of the target, energizing it, and this in turn responds by modulating this field. In this case, the equipment that is generating the magnetic field will feed the electrically passive device, enabling the devices' communication. Due to this feature, it is possible to integrate the NFC device via a smartphone for example, using posters, advertisements and cards.

  Besides the action modes, NFC has three distinct modes of operation. These modes have been defined so the technology could bear a wide range of operations. These methods are:

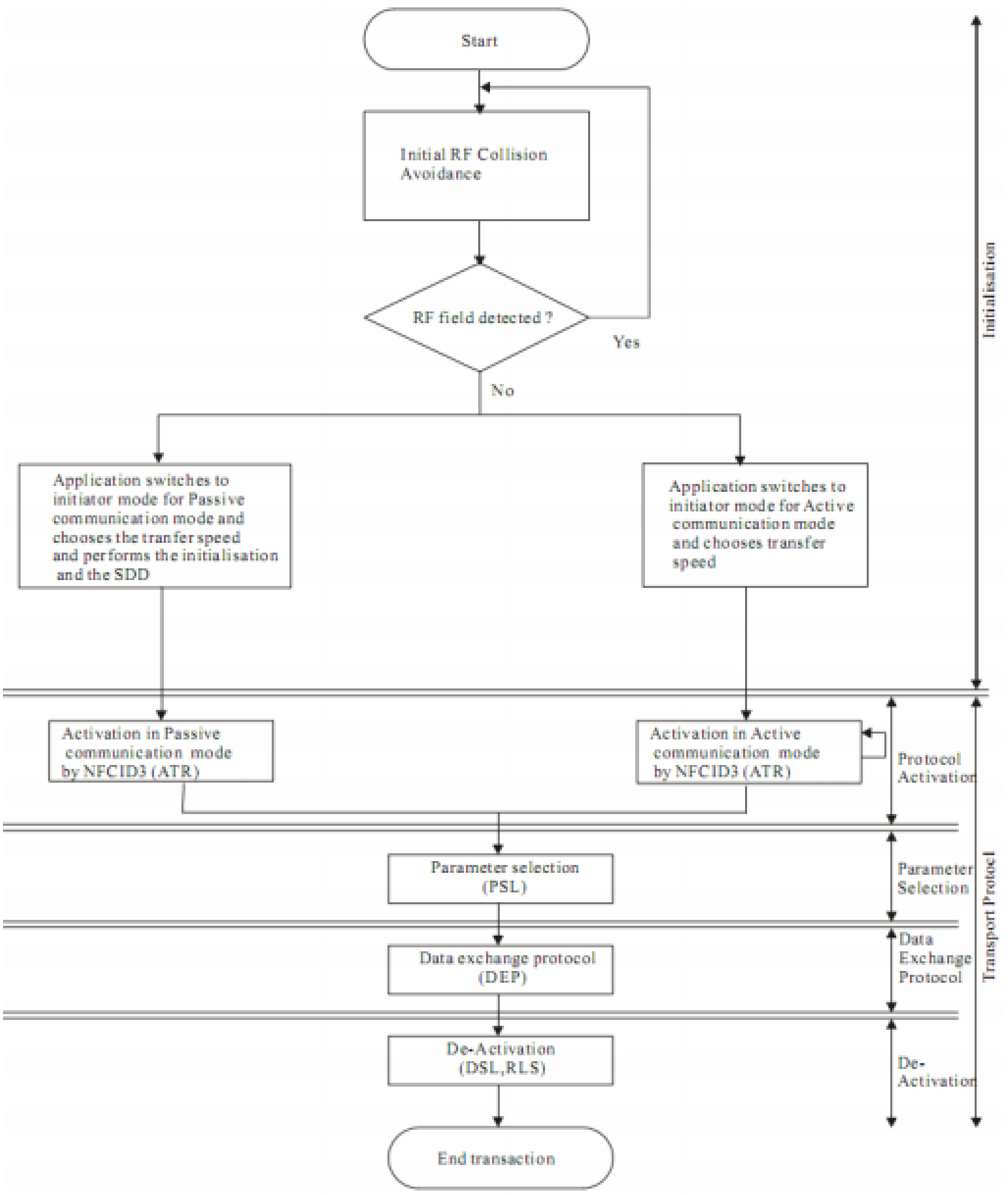
- Reading and Writing - In this mode, the NFC device can read and modify data stored in a compatible NFC in a passive way. Depending on the data stored on the tag, the NFC device performs the appropriate action without the need for any user interaction.

- Card emulation: An NFC device can also act as a smartcard, so that the reading device cannot distinguish between a smart card and the NFC device. In fact, NFC technology allows the device to be capable of storing different contactless smartcard applications in a single device.

- Peer-to-Peer: Allows two NFC devices to establish a bidirectional connection to exchange contacts, that is, each device may receive as well as send data to one another.

3.2.1. Initialization

Initially, all devices should be in target mode, that is, they should wait silently (by not emitting the RF field) for a command from an initiator. Then, the application determines which of the devices will pass to initiator mode and that it ensures that it will operate in the active or passive mode of communication at a given transmission rate (see Picture 3).

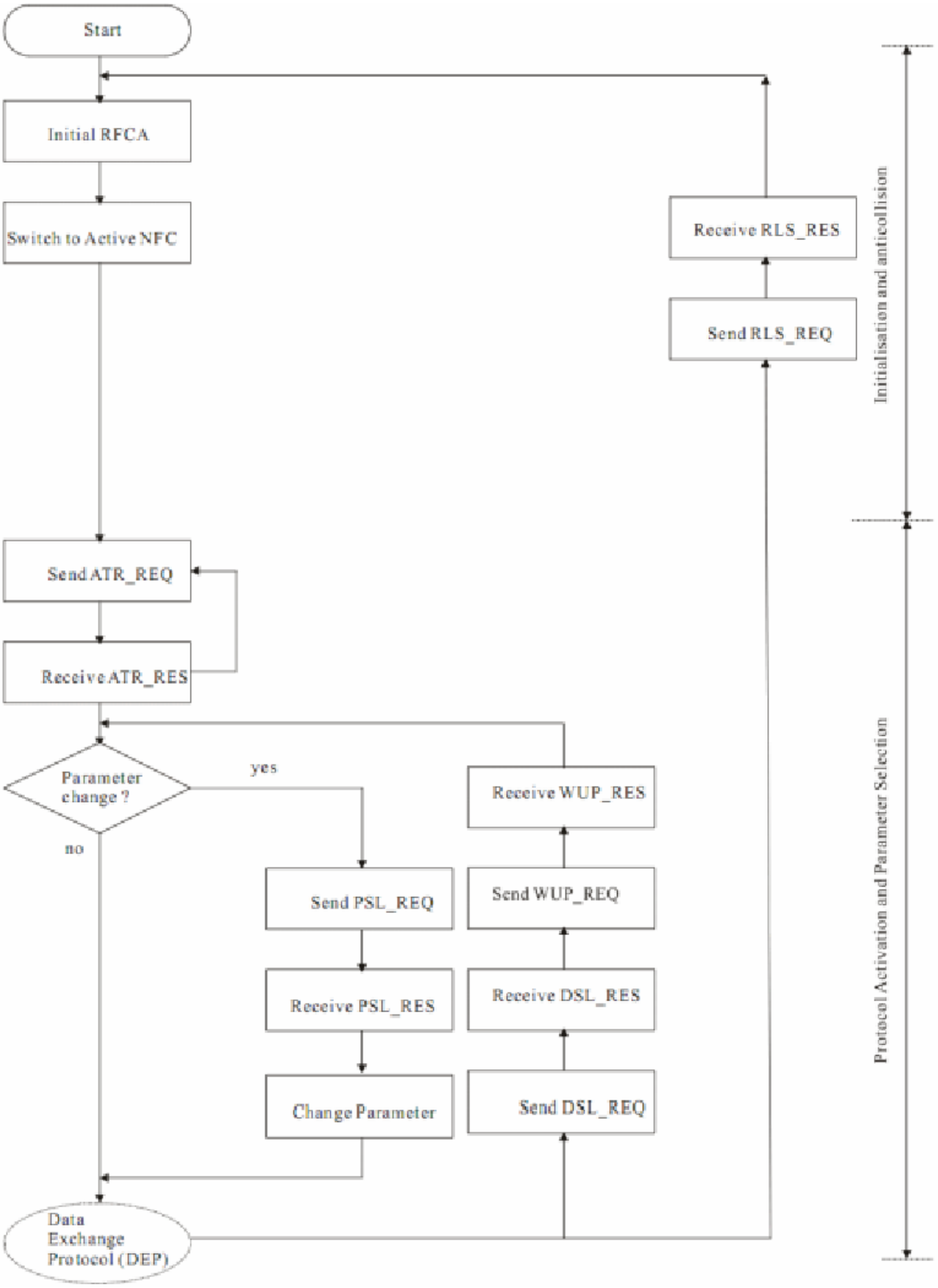

Start
Initial RF Collision Avoidance
RF field detected ?
Yes
No
Application switches to initiator mode for Passive communication mode and chooses the tranfer speed and performs the initialisation and the SDD
Application switches to initiator mode for Active communication mode and chooses transfer speed
Initialisation
Activation in Passive communication mode by NFCID3 (ATR)
Activation in Active communication mode by NFCID3 (ATR)
Protocol Activation
Parameter selection (PSL)
Parameter Selection
Data exchange protocol (DEP)
Data Exchange Protocol
Transport Protocl
De-Activation (DSL,RLS)
De-Activation
End transaction

Picture 3 – General initialization and device detection (ISO/IEC 18092)

In the next step, flux activation will begin. Flux activation differs between the passive and active modes.

3.2.2 Flux activation in the active mode of communication

In the active mode of communication (also called Active NFC), the flux (see Picture 4) starts by performing a collision avoidance step. Once the medium is free, the initiator device starts NFC's communication in active mode.



Picture 4 - Activation flux of the active mode of communication (in the initiator device's view) (ISO/IEC 18092)

The initiator must execute the collision detection algorithm to verify if there's any external RF field. If none is detected, it activates its RF field. Then, it sends an attribute request (Attribute Request - ATR_REQ) at a transmission rate that can be 106Kbps, 212Kbps or 424Kbps. The initiator then turns off its radio and waits for a response.

The parameters that are negotiated in this request are the back and forth transmission rates and they're the maximum data limit in a request.

The target that received the ATR_REQ executes the collision avoidance response algorithm (multiple targets may respond simultaneously, causing a collision). If the medium is free, the target sends the attribute response packet (Attribute Response - ATR_RES) back in the same transmission rate and turns off its radio.

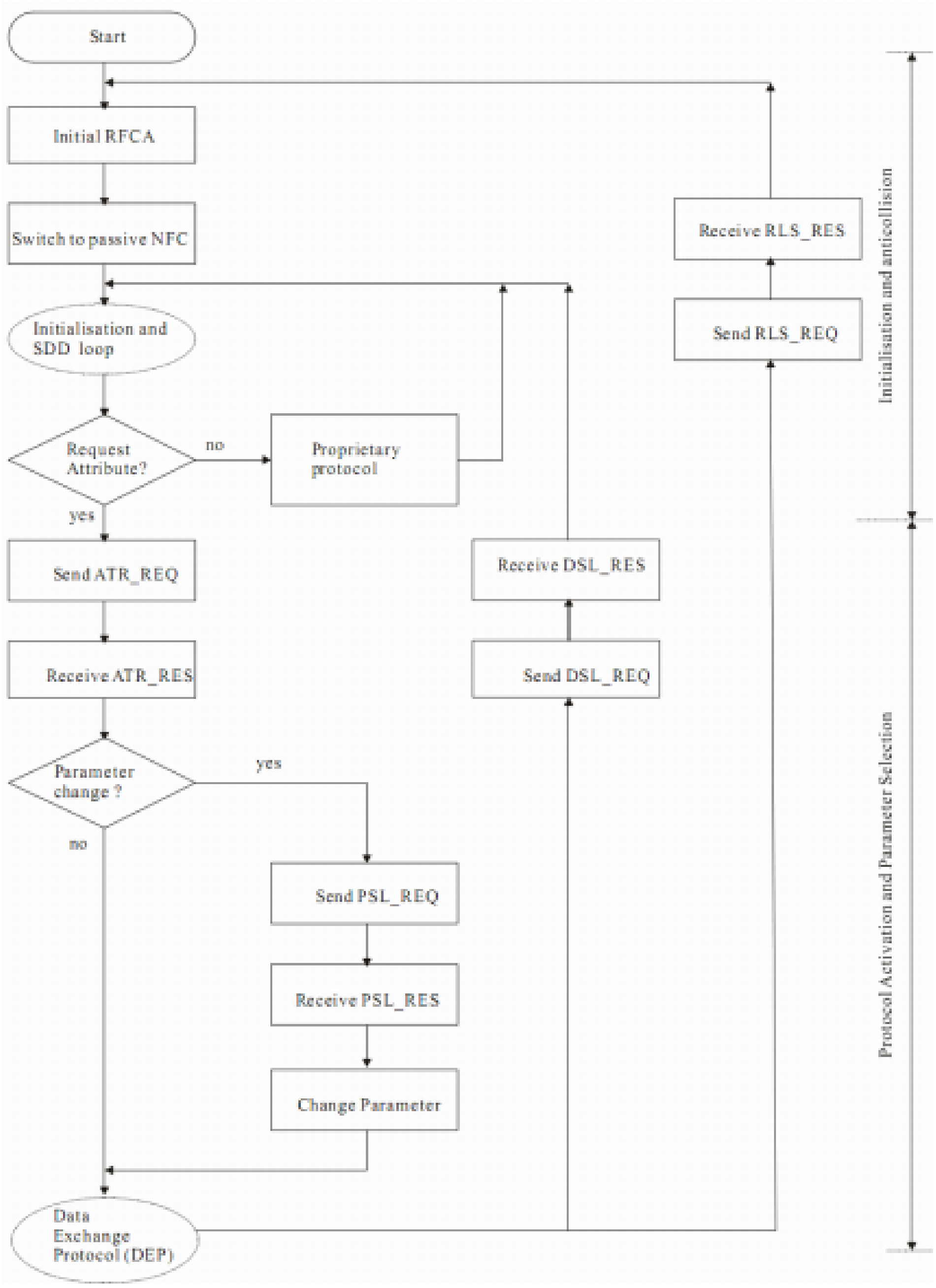
The initiator then performs collision detection. If it receives more than one answer simultaneously (collision), it resends the ATR_REQ; otherwise, it receives the response containing the parameters proposed by the target. If it's not satisfied with any parameter, it sends a parameter selection request (Parameter Selection Request - PSL_REQ) to change a parameter, and it waits for a PSL_RES response. If it's satisfied, it sends a request to start the data exchange protocol (Data Exchange Protocol Request-DEP_REQ). If all goes well, by this time the target will have an identification number (Device Identification - DID) to which the initiator will refer to henceforth.

After finishing the data exchange, the initiator may disable the exchange data protocol. When sending a deselect request (Deselect Request - DSL_REQ) to a particular target, the target sends a deselect response (Deselect Response - DSL_RES) and goes into sleep mode. In this mode, it stops responding to the data exchange protocol. To reactivate it, the initiator must send a wake up request (Wake Up Request - WUP_REQ) that contains the identification (DID) of the target. Then, the target responds with another one (Wake Up Response - WUP_RES) and goes back into activity.

The initiator may release a target with which it no longer wants to maintain any connection. To do so, it sends release request (Release Request - RLS_REQ) and waits for an acknowledgment from the target (Release Response - RLS_RES). At this time, the target loses its identification number (DID) and it becomes free to go through another initialization process.

3.2.3 Flux activation in the passive mode of communication

Much like the active mode, in the passive mode of communication (also called Passive NFC) the activation flux (see Picture 5) starts by performing a collision avoidance step. Once the medium is free, the initiator device goes into passive mode.



Picture 5 – Flux activation of the passive mode of communication (in the initiator device's view) (ISO/IEC 18092)

The next step consists of a loop in which the initialization and the discovery of a single device (Single Device Discovery - SDD) occur. This step uses different device discovery protocols, according to the transmission rate chosen by the initiator. At 106Kbps, it uses the bit collision detection protocol, while at 212 and 424Kbps it uses the time window detection protocol.

After the initialization step and discovery, the initiator checks if the target device supports the NFCIP-1 protocol. If it does, the initiator can negotiate connection parameters and then start the data exchange protocol (Data Exchange Protocol - DEP). If not, it goes back to the initiator device’s initialization and discovery step.

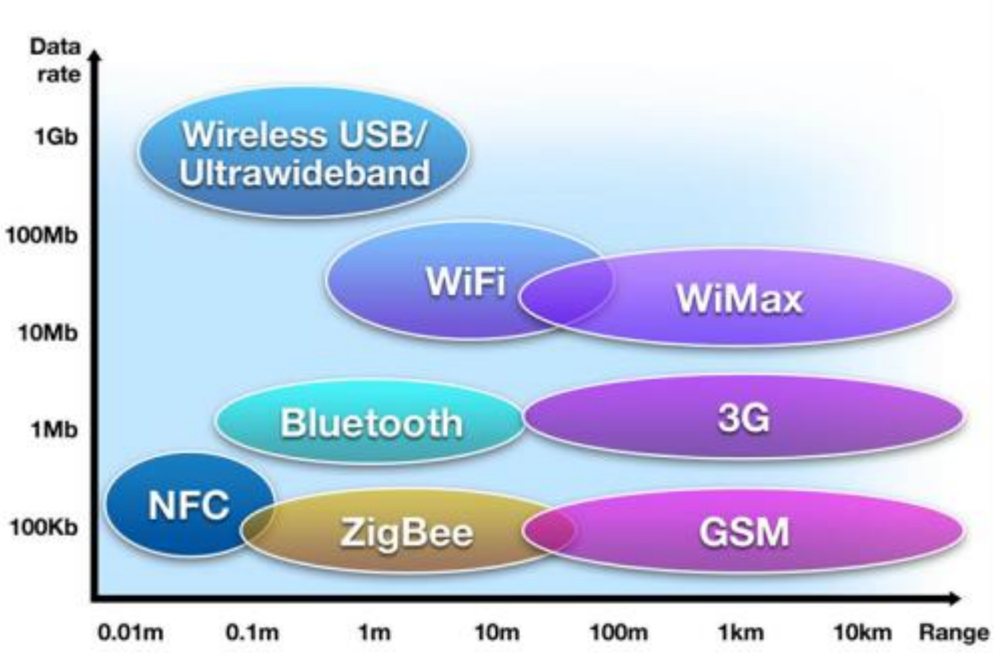
After exchanging data with a particular target, the initiator can remove a target. This target will return to a State of Dormancy and, while in this state, it will not respond to data requests. The initiator can send a request to wake it up again and return it to the State of Resolution.

The initiator can terminate the protocol for data exchange via a release request (Release Request - RLS_REQ): the initiator returns to its initial state and the targets return to the Perceptual State (a state where the target is being powered by a magnetic field and is prepared to respond to initiators looking for target devices.

3.3. NFC and other Wireless Communication Technologies

NFC is an extension of RFID, but the operating distance makes them different. Although the operating mode of both is the same, NFC works only at a distance of ~ 8 in., while RFID can operate in longer distances, particularly if the source is powered. But when compared to Bluetooth there is no difference in distance, as "NFC technology works in a similar manner to Bluetooth because the two technologies rely on close-range and secure transmission (…)" (Muriira & Kibua 2012, p.77) the latter of which is present in most mobile devices. Among these two, the major differences are:

- NFC is slower than Bluetooth;
- NFC consumes much less energy;
- The speed of the NFC's transfer rate is 424 Kbit/s while Bluetooth 2.1's can reach up to 2.1 Mbits/s;
- NFC doesn't require the pairing of the devices for communication to happen;
- Establishing a connection between NFC devices takes less than a tenth of a second;
- NFC operates in the 13.56 MHz frequency and Bluetooth between the 2.4 and the 2.5 GHz frequency;
- 8 in. is approximately the maximum distance for an NFC communication to be established, while in Bluetooth V2.1 (Class 2) the distance is 10 metres.



Picture 6 – NFC and other wireless technologies represented in their Data & Range rates.

3.4. Security

The requirement that the devices must be very close – actually, almost touching each other so that the connection is maintained - may seem disadvantageous at first glance; however, the proximity is paramount to provide one of the most important factors when it comes to technology: security; after all, there is no way to capture the transmitted data unless an ill-intentioned person is practically leaning on the victim while the transmission is being made. The security of this technology is based on three main aspects: touch, short-range and point to point connection. To initiate the communication the devices must touch, that is, for the communication to take place it is necessary to have access to the device and not just to the field of communication generated by it. Once the communication starts, and the protocol is negotiated, the communication takes place point to point. There cannot be third party equipment between the devices in this closed "network". While the communication occurs, the devices should remain generally at a distance of up to ~ 8 in. of each other, so one can "capture" the data transferred in this connection, facilitating the identification of the signal's interceptor. To deal with this, one of NFC's weapons is the SWP protocol (Single Wire Protocol). It is an interface that provides secure communication between the SIM card and the chip of the NFC device. Despite the above, security is still a concern, and for that reason we study some possible ways of attacks and how to avoid them. The principal ones are:

Eavesdropping

As Hancke (2008, p.1) states, "Eavesdropping normally occurs when the attacker intercepts communication between an RFID token and an authorized reader. The attacker does not need to power or communicate with the token, so he is able to execute the attack from a greater distance than is possible for skimming." "An attacker can execute an eavesdropping attack if he acquired a suitable antenna, an RF receiver and a method to sample and record the data. Even though I illustrated the eavesdropping attack using commercial RF equipment I also want to point out that these attacks can work outside 'laboratory conditions' with cheap and portable hardware." Because NFC is a wireless communication interface, espionage is an important concern. When two devices communicate via NFC they use RF waves to "talk" to each other. As is, NFC communication is usually made between two devices in close proximity, but the main issue is how to prevent an attacker to be able to recover a usable RF signal.

Data Corruption

Instead of just listening, the attacker can also try to modify the data that is transmitted through the NFC's interface. Data corruption can be achieved by transmitting valid frequencies of the data's spectrum at the right time. This does not allow the attacker to manipulate the actual data, but it basically acts as a denial of service.

Data Modification

It is relatively simple to perform this attack using a powerful antenna. The same causes signal interference, invalidating the data transmission. However, if the NFC equipment verifies the RF field at the time of transmission, the attack can be identified.

Data Insertion

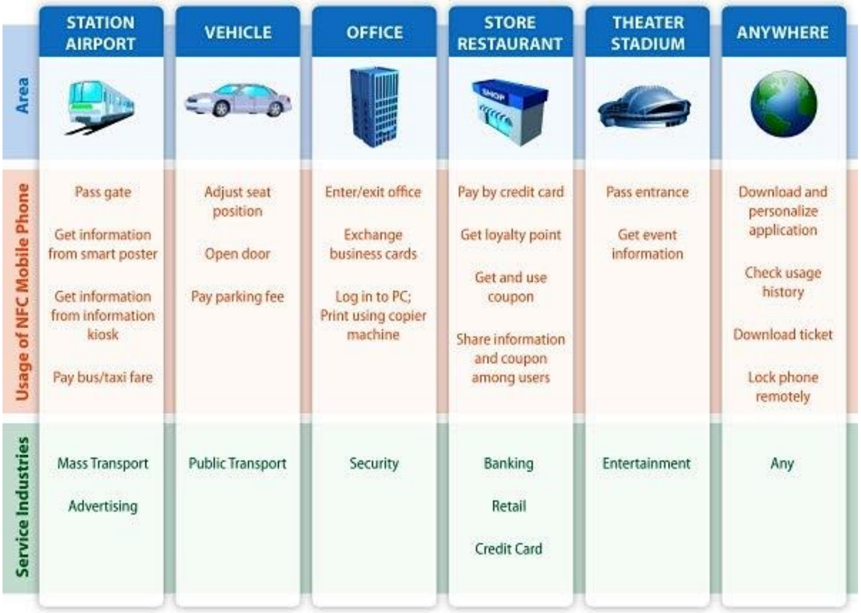
In this attack the attacker inserts messages for data exchange between two devices, but this is only possible if the responding device requires too much time to respond. The attacker can then send his data before the valid receptor. The insertion will only be successful if the inserted data can be transmitted before the original device answers. If both data streams overlap, the data will be corrupted.

Man-in-the-middle

This is a type of attack in which the data that is exchanged between two parties is somehow intercepted, recorded and possibly altered by the attacker without the victim noticing it. Paus (2007, p. 17) describes the attack by saying that "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 the active mode the 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." In normal communication, the two elements involved communicate with each other without interference through a means like a LAN, the Internet or both. During the man-in-the-middle attack communication is intercepted by the attacker and retransmitted by him discretely. The attacker can then decide to retransmit the data between the legitimate participants by altering it or by blocking parts of the information. Because the legitimate participants in the communication do not notice that the data is being tampered they treat it as valid, providing information and executing instructions ordered by the attacker. To avoid any of the setbacks exemplified above, it is more convenient to apply safety procedures in the applications, such as using encryption for transactions and authentication features.

3.5 NFC Applications

NFC is a technology that has been drawing attention in the media in recent years, mainly because of the increasingly interesting applications that use it and that, each day, demonstrate a great potential to be incorporated into our reality. This technology enables wireless short-range communication between devices and has many applications that, due to its characteristics, are primarily focused on cell phones and smartphones. With applications in several segments like electronic tickets (mobile ticketing), advertisement (smart poster), document identification, electronic keys or network configurations (Bluetooth pairing), it is the mobile payment sector - that consists in mobile payments over a mobile phone - that Near Field Communication is drawing more attention, thanks to the explosive growth of the mobile market worldwide. A mobile phone with this technology allows its user to make safe payments by only approaching the reading device of the sales point. Some people are already wagering that this technology will replace debit and credit cards like we know them today. Several examples have been applied around the world, some with the backing of major “players” in the payment segment such as MasterCard and Visa. Credit card brands, banks and telephone companies are already aware of this technology’s possibilities, and one thing is certain: in the near future, with the approach of major events like the 2014 World Cup of Football and the 2016 Olympic Games, applications using NFC will already be part of reality. As the image below clearly demonstrates, and even though NFC is in its early beginning if we think of all the possibilities it comprehends, the technology is promising in a wide array of different sectors and industries. In fact, we can easily realise that in a very short time span NFC will be adopted worldwide by every major sector as a transaction means, again due to its almost flawless security, practicality and ease of implementation or adaptation of receiver terminals. NFC users will also multiply in a very fast manner thanks to the above mentioned aspects and also because it is a very convenient method of transaction. Basically, an NFC enhanced cell phone will allow its user to acquire any sort of commodity whenever needed, be it food, transportation, leisure, health, banking, etc. without the need of extra means (credit and debit cards, plastic or paper travelling cards/tickets or money).



Area	STATION AIRPORT	VEHICLE	OFFICE	STORE RESTAURANT	THEATER STADIUM	ANYWHERE
Usage of NFC Mobile Phone	Pass gate Get information from smart poster Get information from information kiosk Pay bus/taxi fare	Adjust seat position Open door Pay parking fee	Enter/exit office Exchange business cards Log in to PC; Print using copier machine	Pay by credit card Get loyalty point Get and use coupon Share information and coupon among users	Pass entrance Get event information	Download and personalize application Check usage history Download ticket Lock phone remotely
Service Industries	Mass Transport Advertising	Public Transport	Security	Banking Retail Credit Card	Entertainment	Any

Picture 6 – The applications for NFC. Even though transportation is clearly ahead of other sectors, it’s easy to see the full capabilities of NFC in other important industries like Workforce, Food, Leisure & Entertainment and everywhere else.

3.5.1 Smart poster

A Smart Poster is a bidirectional channel between the brand or product and the consumer. The NFC tags work as printed ads displayed in public places, consisting of a small, intelligent electronic tag. By passing a smartphone with NFC on the Smart Poster, the data is transferred to the consumer’s phone. Such data may contain a plethora of information, where the only real limit is the creativity of the advertiser. This way of communicating with the consumer allows the reduction in marketing costs and the storage of large volumes of valuable data about a specific customer’s base.

3.5.2 Electronic Travel Cards (travel cards)

An NFC phone can be used as a travel card to replace travel tickets. To show a ticket, the user must touch the card reader with his phone. To use a smartphone that has NFC enabled as a travel ticket, it is necessary to implement a secure environment known as Secure Element (SE). This secure environment runs the ticket’s application, which can, for example, control the remaining number of available travels.

3.5.3 Electronic Key

This application works for hotel guests that will not have to rely on keys to get into their suites. For that they’ll just have to approach a mobile device with data transmission technology. This electronic card or key also makes it possible to skip the check-in step, giving guests the option of not having to go through the counter, allowing them to go directly to their rooms.

3.5.4 Network Configuration (Bluetooth pairing)

NFC can be used symbiotically with other technologies like Bluetooth and Wi-Fi. Because of its automatic and fast setup, these other technologies can use their link for out-of-band connection negotiations. Applications that require higher transmission rates will use this association function. For example, by approaching a phone to an NFC/Bluetooth printer, the mobile application requests an approval to establish a Bluetooth connection. The user only has to confirm with a button, and the Bluetooth connection is automatically negotiated via the NFC link. Only with a simple gesture and pressing a single button it is possible to establish a Bluetooth connection to upload photos for immediate printing.

3.5.5 Electronic Money (e-wallet, mobile payment)

This application allows the user to use a smartphone to pay bills instead of the traditional credit card, debit card or cash. The process is simple: the smartphone user approaches his phone to a receiver - it is necessary that both devices have an NFC chip - and the communication is established; the device receives the information about the process, like the total purchase price. Then, the user just has to insert a personal code on his phone and make the payment.

3.5.6 Ticketing

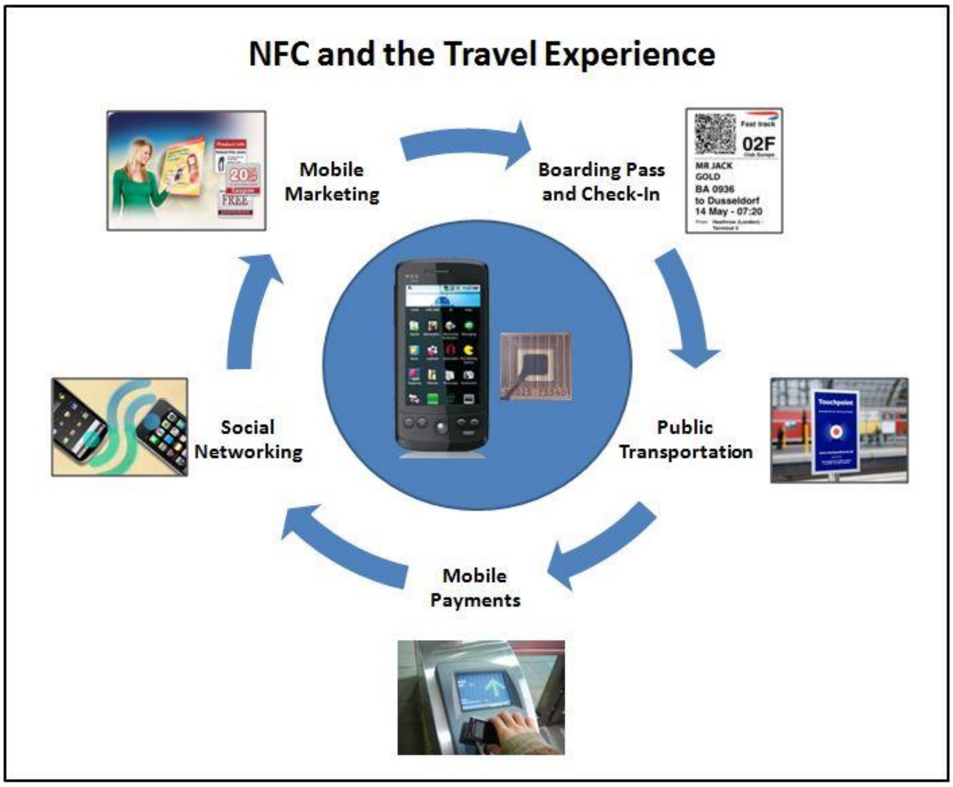
Public transportation is the leading sector in the use of NFC technology. Contactless ticketing is already being used to facilitate the use of public transportation and access controlled environments such as car parks. With NFC-enabled mobile phones, consumers can buy tickets, receive them electronically, use them for travels like “Park and Ride” and pass through special turnstiles while others keep on waiting. Besides, it’s possible to check the balance or update tickets remotely. With these as examples, one can already imagine other uses for NFC. Some other examples are:

- Identification: NFC can be used on a badge, for example, to identify the arrival of an employee to the company or its access to a particular sector;

- Virtual tour guide: if the user is in a museum, he can approach his cell phone to a nearby receiver to obtain more information about the material on display on his phone;

- Advertising: while waiting for the bus, the user can approach his cell phone to a nearby advertising poster and, by doing so, get a discount at the advertising store;

- Prices: to know the price of a product on the shelf or even more details about it, just get your cell phone close to the product to obtain the desired information.



Picture 7 – NFC and the Travel Experience cycle.

4. NFC in the United Kingdom

Even though the NFC technology is widespread mostly in Japan, it is being developed quite rapidly since 2011 in the UK, and it is possible to observe a steady crescendo of transactions related to payments made by mobile phones using this technology. One of the main objectives is to turn a mobile device into a digital wallet. Google is one of the leading companies that are investing heavily in this technology. In late 2010, the company launched its new “Nexus S” device with an embedded NFC chip, and it recently announced the launching of its mobile payment service “Google Wallet”, started as a pilot project in New York City. For that, Google arranged an agreement with MasterCard and Citigroup to facilitate mobile payments through Android. In the UK in 2012, organizations and venues such as Eat or Wembley Arena led modest trials by accepting payments via NFC-enabled phones, and even though the initial previsions were conservative as per rule, both soon realized that NFC was not just only a new and alternative payment method, but the future. However, the “ecosystem” where all elements related to mobile payment develop is still complex. There are “heavy-weight contenders” in the mobile industry with different initial interests and a great desire to lead in the mobile payment panorama. On one hand, mobile operators and credit card companies are committed to implement NFC and store user data in the device’s SIM card, so that it’s possible to access information. But the situation gets more complicated by a new element added to the list of intermediaries in the previously referred ecosystem: “vendors”. They are eager to have the means to facilitate and expedite sales, but at the same time are reluctant to invest in infrastructures such as reading points with RFID antennas for communication and identification devices with an NFC chip, uncertain if the investment is viable.

5. N-Key: One Key for A Thousand Locks

5.1 Overview

Keys are in use for the past 4000 years, and they were first made of wood and afterwards of metal, plastic, glass or alloys. Even though it's a common instrument, no one discusses or doubts its vital importance in present times: doors, ignition devices, small personal safes, bicycle locks and myriads of other devices/mechanisms that use one or more keys for varied purposes. Even though the first electronic key was introduced in 1954 (*Popular Mechanics*, August 1954, p. 94), traditional keys weren't replaced in almost 60 years, far from it: the average number of keys per person today is six.
For security reasons, each lock mechanism is unlocked with its corresponding key, so the owner of the key feels safe knowing that no one else has the exact key that opens their lock, making it an easy, inexpensive and (generally) safe way of protecting one's values. However, there are issues in this concept. A common key only serves to open and lock a single mechanism or device, for instance. On the other hand, a bundle of 4 or more keys is a common scenario that isn't practical as it has to be carried somewhere else than in one pocket, as it creates a bulge and requires some other way of carrying it (a purse or a bag, amongst others). Even though it accounts for safety, it also can be very limited and uncomfortable.

The aim of the **N-Key** is to provide a single and practical key-shaped mechanism that incorporates all of one's keys in a personal manner. Be it a car, office, house door, safe or whatever the lock, each **N-Key** will allow its user to conveniently carry it in a pocket, knowing all of his possessions are secure and offering him or her an inexpensive and user friendly experience when locking or unlocking any of the above. In fact, one will only need the key and a NFC tag reader device for each lock.

5.2 N-Key architecture

As expected, the key itself will act as the initiator device, initiating the communication and controlling the exchange of information that is transmitted by generating a magnetic field between itself and a reader tag that is connected to a door, which in turn will respond to the initiator request (passive communication). Much like the NFC reader devices that respond to a mobile phone acting as an initiator, the communication principle is the same: when the key (initiator) touches one of the locks (tag reader), it transmits encrypted information that contains a locking or unlocking command using a secure layer protocol.

The **N-Key** follows common NFC technology standards: ECMA, ISO/IEC and ETSI. The ISO/IEC18092 standard based on ECMA-340 defines the physical layer of NFC technology. This standard defines the characteristics of the RF field, the protocol and interface technology, also called NFCIP-1. The Standard ECMA-352 defines the detection mechanism and operation mode selection NFC. The safety guidelines regarding the NFCIP-1 protocol, as well as the use of encryption standards, and establishment of the secure channel, are defined in the ECMA-385 standards, also called NFC-SEC and ECMA-386 (NFC-SEC-01).

Layer (OSI model)	Protocol
Logical Link Control Sub layer (Link Layer)	LLCP
Medium Access Control Sub layer (Link Layer)	NFCIP-1
Physical Layer	

Table 1 – NFC and Stacked Layer and Protocol Architecture

That being said, each of the communication layers used between the initiator and the receiver are described below.

Logical Link Control Sub Layer

This is the upper half of the data link layer of the OSI model. Below it there's the Medium Access Control Sub layer, and below this the Physical Layer. The Logical Link Control Protocol (LLCP) provides the following services:

- Activation and deactivation of supervision connection;
- Asynchronous, balanced communication;
- Multiplexing protocol (the LLCP can accommodate multiple layer protocols at the same time);
- Connection-oriented data transmission to guarantee packet delivery through sequencing and retransmissions;
- Non-connection-oriented data transmission providing a lower overhead protocol. It can be used if the upper layer protocols provide flux control.

Medium Access Control Sub layer

This layer is implemented by the NFCIP-1 protocol, which is described in the ISO 18092 document. Its operation is described from point **3.2.1** to **3.2.3**.

Setup

Each new lock (tag reader) that is acquired needs to be connected to a computer containing the **N-Key**'s software, which will allow each new tag reader to be added to a list of existing reader devices on a database. Moreover, there's the option to personalise the device even further with biometrics (fingerprint recognition), contributing to a safer device, as it will only lock or unlock each door only after recognising one's unique fingerprint. It will also provide the user to open only the locks that are "inserted" into the key. If a key is lost, it will then be impossible to be used by someone else than its original owner.

Positive & Negative Aspects

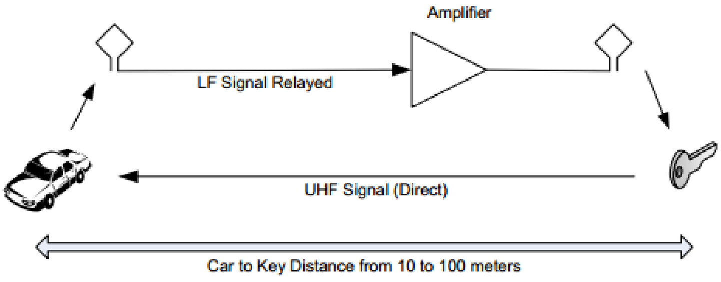
The **N-Key** has the main purpose of being able to centralise all common keys into a single key, as described in the device's Overview. While at first one can only envision positive aspects, it happens to also have minor negative issues.

Positive

- No more bulges in pockets
- No more time wasting trying to find a specific key
- Extremely assessable one-time investment
- Personalised, making it a safe device
- Easy to install
- Cheap maintenance

Negative

The sole negative aspect concerns to security regarding modern automobiles. As NFC protocols include ISO/IEC 14443 (it deals with contactless proximity cards, including radio-frequency interface and electrical interface, besides anti-collision and communication protocols. This pattern is used mostly for transportation, financial and access control ends.), it is possible to perform a Relay Attack. To perform this attack, the attacker needs to forward the reader's request to the victim's equipment and perform the opposite path in real time to the attacker's reader. This attack is similar to the man-in-the-middle (see page 16), but it is necessary to be close to the victim to better exploit this attack, and it's known as a Relay Over-Cable Attack. As Francillon et all (2010, p.5) describe, "In order to perform this attack, we used a relay composed of two loop antennas connected together with a cable that relays the LF signal between those two antennas. An optional amplifier can be placed in the middle to improve the signal power. When the loop antenna is presented close to the door handle, it captures the car beacon signal as a local magnetic field. This field excites the first antenna of the relay, which creates by induction an alternating signal at the output of the antenna. This electric signal is then transmitted over the coaxial cable and reaches the second antenna via an optional amplifier."



Picture 8 – The relay with antennas, cables and an (optional) amplifier. (Francillon et all, 2010, p.5)

However, there are several measures to combat this attack, like keeping the key inside a metallic box (creating an effective Faraday cage) or removing the battery from the key, deactivating the radio signal.

Assessment

The **N-Key** is the next logical step in admission/clearance technology, as the security and convenience it proposes is yet unheard of. Besides turning a bundle of 5 or more keys into a single key-shaped and sized device, it will make its user more relieved in terms of security.

By purchasing a single key and one lock for every door that the user wished to open, costs will also be reduced over time. As long as the system is in use, there will be no need to buy another lock due to wear and tear, nor will a key ever be trapped or stuck in a lock again. Moreover, because the locks only open with the data that is transmitted by the key (making lock picking a thing of the past) it will increment security by providing a basically impenetrable system.

Because its implementation is so easy and user-friendly, it will benefit the user each time he adds a new lock to the list, as he will only have to do as before. To remove or replace a lock will be as easy as setting it up: the user just has to delete a lock permanently in the software application and retrieve the physical lock from the door or simply move the lock from one door to another and it is done.

Even though it may some time for the common consumer to accept the idea and realise the efficiency and convenience that the **N-Key** offers, it will certainly be a winning bet in a mid-term scenario, especially if we consider that mobile NFC technology is gathering an ever growing number of users worldwide. Social acceptance is thus only but a question of time - a short one, for that matter.

6. Conclusion

Proximity communication technology has seen a healthy and fast development in recent years, including becoming increasingly more applicable in new business areas. This paper reports on one of the most promising technologies considered: NFC, focusing mainly on its concepts and its applicability. The acceptance and use of this technology is increasing, as are new applications and proposals for new business models that make use of this short distance communication. We therefore conclude that although NFC requires development and improvement, when widespread it will provide the performance of activities more efficiently, not only with regard to electronic payments but as a tool to access a plethora of activities including those that are explored herein. It's important to note that the difficulty of the availability of material on the subject raises the need of undertaking work and future projects combined with a benchmark practice in which it is possible to obtain more accurate data, especially the one regarding the consumption of this technology and the costs involved to implement it versus the profitability it purveys.

References

Allah, M. M. A. 2011, *Strengths and Weaknesses of Near Field Communication (NFC) Technology, Global Journal of Computer Science and Technology Volume 11 Issue Version 1.0 March 2011* [Pdf] Available at: http://computerresearch.org/stpr/index.php/gjcst/article/view/588/524 [Accessed July 31 2013]

Weiser, M. 1991, *The Computer for the 21st Century*, Scientific American, vol.265, no. 3,September, pp.94-104.

Eisenstein, J., Vanderdonckt, J. & Puerta, A. 2000, *Adapting to Mobile Contexts with User-Interface Modelling*. [Pdf] Available at: http://www.ximl.org/documents/XIMLMobile.pdf [Accessed July 31 2013]

Muriira, L. M. & Kibua, N., 2012. *Near Field Communication (NFC) Technology: The Future Mobile Money Service for Kenya* [Pdf] Available at: http://www.ijcir.org/volume6-number1/article8.pdf [Accessed July 25 2013]

Hancke, G. P., 2008. *Eavesdropping Attacks on High-Frequency RFID Tokens* [Pdf] Available at: http://www.rfidblog.org.uk/Hancke-RFIDsec08-Eavesdropping.pdf [Accessed July 26 2013]

Paus, A., 2007. *Near Field Communication in Cell Phones* [Pdf] Available at: http://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/near_field_communication_in_cell_phones.pdf [Accessed July 27 2013]

Popular Mechanics, August 1954, p.94. Available at: http://books.google.pt/books?id=AeADAAAAMBAJ&pg=PA94&dq=1954+Popular+Mechanics+January&hl=en&sa=X&ei=CFMiT_23OIGvgwf68vjqCA&redir_esc=y#v=onepage&q&f=true [Accessed August 05 2013]

Francillon, A., Danev, B., Capkun, S., 2010. *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars* [Pdf] Available at: http://eprint.iacr.org/2010/332.pdf [Accessed Aug 05 2013]