Near Field Communication in Mass Marketing

Deebika.D[1]

[1]Department of Computer Science & Engineering, MNM Jain Engineering College, Chennai, Tamil Nadu, India

Abstract

Near field communication (NFC) is a new secure short range wireless connectivity technology, which offers an important contribution to simplify some daily operations, such as payments, ticketing, data transfer and vouchers.

This paper is designed with the intention to help transport operators, banking /cards operators and mobile operators deploy mobile NFC solutions to enhance the efficiency and effectiveness of public transport and make payment in smart way. Any public sector such as Personal identification cards (AADHAR card) can use NFC for identification of each person using NFC tag based solution to enhance identification/verification operation even without a mobile handset. This NFC Tag could be extended for integrating all the ID proofs into a single unique Tag that provides global identification for people. This paper explores the methodologies how NFC influences various sectors of public transport and Identification.

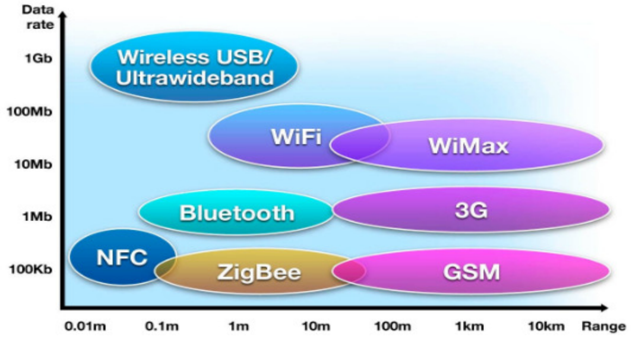
1. Introduction

NFC is a standards-based, short-range wireless connectivity technology that enables simple and intuitive two-way interactions between electronic devices. With NFC technology, consumers can perform contactless transactions, access digital content and connect NFC-enabled devices with a single touch. NFC simplifies setup of some longer-range wireless technologies, such as Bluetooth and Wi-Fi. It is also compatible with the global contactless standards (ISO 14443 and/or ISO 18092), which means transport agencies that have already deployed contactless programs enjoy a built-in advantage, as their equipment may readily interact with NFC-enabled mobile devices and provide richer services.

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

While NFC can be placed in many consumer devices, the focus of this paper is primarily on NFC in mobile phones, readers, and smart posters. However, other NFC-enabled devices, such as fobs, PDAs, PCs, readers, etc., have possible applications in the transport arena and should not be overlooked when planning a system.

Although NFC use is also beneficial for streamlining backroom operations and security, the main focus of this paper is on how implementers can improve the consumer experience.

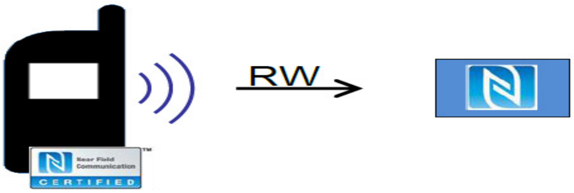


NFC Compared with Other Wireless Technologies

Developed by a global consortium, NFC is based on technology specified by numerous international standards that allows for easy transfers of information over small distances. It can turn a handset into a device for reading data attached to physical objects, be used for exchanging data between two mobile devices and be used for paying for various products, such as public transit tickets and travel cards.

As noted earlier, NFC is compatible with — and builds upon — existing RFID technologies found in millions of access, payment and identification cards — data which is accessible through an emerging RFID reader infrastructure. NFC is particularly well-suited for use in mobile devices, where its operation and behavior are controlled by the device owners.

Reader/Writer (NFC TAG)



This NFC mode enables mobile devices to read data stored in passive RFID tags embedded in public posters, displays, and products — and to act upon that data that contains a Uniform Resource Locator (URL), which is an Internet encoding of access instructions for a file or Web address, or instruction for making a call, or the SMS instruction for sending a text message. This NFC mode also enables mobile devices to write data to some tags – notably virtual tags in other devices.

Card Emulation (NFC Smart Card Emulation)

RW
Near Field Communication
CERTIFIED
Near Field Communication
CERTIFIED

When NFC card emulation is provided using a secure element, the card to be emulated is provisioned into the secure element on the device through an Android application. Then, when the user holds the device over an NFC terminal, the NFC controller in the device routes all data from the reader directly to the secure element. Figure 1 illustrates this concept.

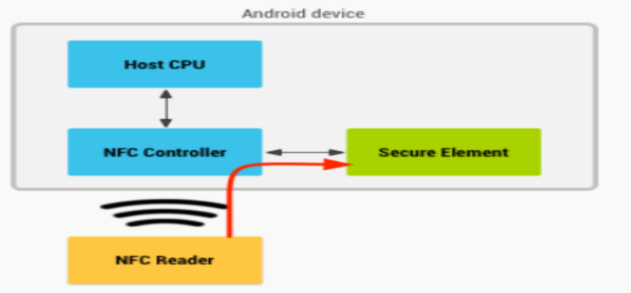
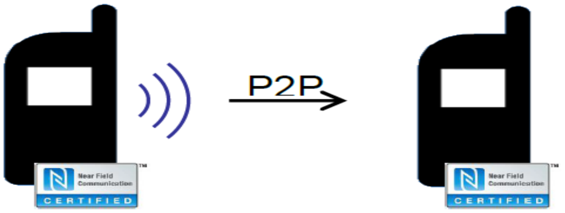


Figure 1. NFC card emulation with a secure element.

Peer to Peer (Two NFC Enabled Smart Phone)



This NFC mode enables mobile devices to more easily interact with each other (i.e., each phone has to be equipped with NFC and the enabling applications) to quickly launch a mobile communications bearer for sharing data with each other, whether to exchange business cards, photos, documents or other type of personal information in "peer-to-peer" data transfers.

Near Field Communication is a contactless radio technology that can transmit data between two devices within a few centimeters of each other. Mobile phones are increasingly being equipped with NFC capabilities, enabling an array of new digital services, such as:

- ***Ticketing*** – interactive fare media on public transport Systems-***(NFC Smart Card Emulation)***
- ***Payments*** – an alternative to cash and plastic credit cards to purchase goods and services - ***(NFC Smart Card Emulation)***
- ***Access control*** – an alternative to traditional keys and access codes -- ***(NFC Smart Card Emulation)***
- ***Couponing System*** – an interactive alternative to paper vouchers and coupons-- ***(NFC TAG)***
- ***Business Card*** – alternative to paper/ Business card. Transfer of data such as text or numbers between two NFC enabled devices. NFC tags, for example stickers or wristbands, contain small microchips with little aerials which can store a small amount of information for transfer to another NFC device, such as a mobile phone. ***(Two NFC Enabled Smart Phone)***

The Vision of Design – How mobile NFC/NFC tag could transform transport

The NFC Forum has identified three basic use cases for NFC: connection, access, and transactions. All three have application in transport. For example, an NFC-enabled phone can connect with an NFC-enabled kiosk to download a ticket, or the ticket can be sent directly to an NFC-enabled phone over the air (OTA). The phone can then tap a reader to redeem that ticket and gain access.

NFC Forum tags may be of particular interest to transport operators, as they can be embedded in posters, products, maps, etc., to provide transport service-related information. These inexpensive tags can be integrated in smart posters and can contain a variety of information or automatic links to pertinent information and transport service websites. Examples of information that can easily be accessed and activities that can be initiated by tapping a tag with an NFC-enabled phone include:

Transport timetables

- Links to an up-to-date weather report website
- Location-relevant map
- Special discounted travel offers
- Next bus arrival time
- Taxi services
- Emergency calls

- Phone-to-phone transfer of destination addresses and maps to taxi drivers.

Let's look at some ways in which NFC can improve the traveler's experience in these sample use cases taking place before, during, and after a journey.

Before the Journey

Shiva is planning a day trip to Chennai to visit some museums. he has checked the fares online with him mobile phone, purchased him train ticket, reserved her seat, and downloaded the ticket to him phone. ***(USECASE 1)****

The ticket also includes a one-day parking pass at him local station. Shiva drives to the station and taps her phone on the gate to redeem the pass(terminal reader) and enter the parking lot. ***(USECASE 2)****

Using NFC to Pay for Parking

While waiting for the train, Shiva remembers that he has a ICICI loyalty Membership card stored in him phone because he is a frequent traveler.

This enables him to touch a reader on the door to enter the executive lounge to wait for the train ***(USECASE 3)****There are smart posters (NFC Tag) on the walls of the lounge, and he taps him phone on one to download alternative return schedules in case he runs late. ***(USECASE 4)****

One of the museums he plans to visit is advertising a reduced admission fee, and he taps that poster to download the discount *coupon* and store it in him phone. ***(USECASE 5)****

He also taps to opt in to promotions from stores and restaurants in the vicinity, and he immediately receives coupons in him phone. With these waiting-room posters, the retailers have a unique opportunity to attract Shiva to their stores, and Shiva can take advantage of discounts for him favorite products and places. ***(USECASE 6)****

There's a map of Chennai on the wall, too, and he taps various spots to make sure he has directions to all the museums stored in him phone.

During the Journey

Shiva uses him phone to tap a reader, redeem her ticket, and board the train. ***(USECASE 7)**** He holds her phone out and displays him ticket and seat reservation to the conductor, who asks if he would like to purchase a newspaper for the journey. Shiva taps the conductor's handheld NFC reader with him phone to pay for the paper. ***(USECASE 8)****

A colleague he hasn't seen in some time sits down next to him. They chat and tap their NFC-enabled phones together to exchange contact information. ***(USECASE 9)****

Exchanging Information via NFC-enabled Phones

The journey ends pleasantly, and Shiva hails a taxi. He pays the driver by touching him phone to the reader in the cab and receives a virtual receipt in return, which he stores in him receipts folder in the phone. ***(USECASE 10)****

At the first museum, Shiva redeems her discount coupon when he pays her admission fee with him phone. ***(USECASE 11)****

While he is visiting the second museum, however, he receives an SMS saying her return train has been delayed. He checks the other times in the schedule he downloaded that morning in the lounge and requests a new seat reservation, which is sent to her and stored on her phone.

After the Journey

Shiva has spent a pleasant day, and the delays on him return trip was not long. He knows that each time he used him phone to pay that day, he received receipts in return. He checks him phone when he gets home and sees receipts stored for the train fare, her vending machine purchases, the taxi ride, and the museum entrance fees. He taps the phone to him NFC-enabled PC and transfers the receipts to him company expense report. (***USECASE 12)*** It is fortunate that he works for a competitive museum and can claim this trip as a business expense.

2. NFC Technology

2.1 Technical Principles and Historical Progression

NFC is a short-range wireless communication technology that is based on approved and mature standards in the field of RFID and smart cards. RFID, which has already been introduced in the 1970s, realizes automatic identification and data transfer via electromagnetic radio signals typically mymeans of an active reader that is connected to a source of energy and a passive electronic tag that is a transponder receiving its power from the reader by magnetic induction.The RFID tag normally contains an antenna for receiving and transmitting the radio signal and an integrated circuit for processing and storing information and for modulating and demodulating the signal. The RFID tag can be placed almost everywhere and is normally hidden behind existing material, like the packaging of a product, thus being invisible to the user. Those passive RFID tags without own battery usually cost between $0.1 and $1 apiece. For many business models these costs of RFID tags are still relatively large resulting to the fact that until today RFID hasn't been integrated into daily use on this scale. Also, the lack of affordable and permanently available mobile devices containing RFID readers, has led to the more or less prevalent absence and unattractiveness of the RFID technology.

In 2004, NXP Semiconductors, Sony and Nokia founded the NFC Forum in order to bring existing standards and efforts of the RFID and smart card technology together and to create a novel and innovative capability for short-range communication. Up to now, the NFC Forum counts more than 100 members and supporting companies aiming to find a worldwide standardization for the NFC.

For a long time, only a small handful of NFC mobile phones were available, mainly manufactured by Nokia, until Samsung and Google attracted a large audience when releasing the NFC supporting Nexus S phone in 2010. With the current rush on smartphones mentioned above and further successful NFC field tests in the past years, it is expected that in near future most of the top class smartphones will be equipped with NFC support.

2.2. Technical Characteristics and Operation Modes

One of the major advantages of NFC is the fact that the technology is compatible with existing RFID infrastructure, RFID tags and further contactless smart cards. NFC is built upon a subset of existing ISO standards, including the ISO/IEC 14443 standard that is being used by the RFID technology.

NFC hence operates at the unlicensed 13.56 MHz radio frequency band with amplitude shift-keying modulation allowing transfer data rates up to 424 Kbits per second. Theoretically NFC works up to a distance of 20 cm, whereas in most scenarios a working distance of about four centimeters is usual.

In contrast to conventional RFID systems, in the NFC technology there is no more strict distinction between reader and transponder. A NFC-capable device integrates both components: a passive transponder and an active reader. It can not only read and write data from or to a tag, but also receive and transmit data directly to another NFC device. Thus, NFC supports in overall three operating modes -

Reader/Writer mode, Peer-to-Peer mode, Card Emulation mode

2.3. NFC Data Exchange Format

In all modes of operation an NFC Data Exchange Format (NDEF) message is used for the transfer of data, no matter whether the communication takes places between two NFC devices or between one device and a passive NFC tag. The NFC Forum has hereby defined a universal set of rules for the data structures used for any kind of NFC communication.

A NDEF message contains one or more NDEF records that each encapsulates user data of the application layer. The NDEF record is composed of a header and a payload part containing the actual user data. Apart from an ID that uniquely identifies the record, the header most notably defines the type and therefore of the format of the record data. his could be either a MIME media type, describing a composition of e.g. images, textual content and any other types of information [4, p123], or one of the predefined NFC record type definitions (RTD). In contrast to the MIME media types, the latter specifications define not only the data structure, but also the way how the data should eventually be processed and presented on the receiving output device, i.e. the NFC handset. Amongst others, the following NFC record type definitions are possible:

The Text Record Type allows the encapsulation of basic text strings including information about the character encoding scheme and the language of the text .

The URI Record Type contains a Uniform Resource Identifier, e.g. an email address or a web address. An application receiving this NFC record can for example be adjusted to automatically process this information to a web browser application.

The Signature Record Type offers a security mechanism by providing the possibility to sign a whole NDEF message. The application receiving the signed message can then verify its integrity and authenticity by cross checking the signature with a corresponding signature approved by a Certificate Authority The issue of NFC communication security will be addressed later in this paper in more detail.

The Smart Poster Record Type provides a practical opportunity to augment physical objects, e.g. a smart advertisement poster equipped with a NFC tag, with the virtual content hence enabling the previously described concept of the ”Internet of Things’. The Smart Poster Type encapsulates multiple NDEF records containing for example a textual title record, a URI record and also a recommended action to perform when receiving that message, for example to open a certain URL with the browser or to compose a SMS message. Via a simple tap on the tagged object, a receiving NFC device can thus easily be provided with related content that is presented accordingly formatted . In the scenario of buying a concert ticket, as shown in Figure 1, most probably such Smart Poster Record Type will be used.

2.4. Connection Handover

For the transfer of huge amounts of data at high speed or over a large distance between initiator and target the described capabilities of the NFC technology might not be sufficient. In theory however, NFC also provides a mechanism for connection handover to another wireless technology with higher data rates like Wi-Fi or Bluetooth. In general, the establishment of such data communication requires a lot of configuration effort. The simple touch-and-connect principle of NFC though can be used ideally in order to exchange the required configuration parameters. Following a technical specification provided by the NFC Forum in this way the negotiation sequence for activating a new communication channel can be achieved via NFC hence enabling an easy connection handover.

2.5. Hardware Architecture of NFC-capable Phones

Before presenting several NFC application scenarios in the subsequent chapter, it will be useful to discuss the basic NFC hardware components in smartphones and their role within the NFC communication flow. This will be useful to also understand the position and attitude of the various stakeholder parties and the resulting, later discussed, conflicts between them.For NFC in mobile devices essentially four components arerequired: A Host Controller, a NFC Controller, a NFC Antenna and a Secure Element. The Host Controller acts as the heart of every mobile phone. This processor is not only necessary for executing the mobile’s operating system, but also manages the user interface and the GSM/UMTS modem and serves as Application Execution Environment (AEE). It is the gateway for the other NFC components to the mobile phone’s system itself and is therefore an essential part for integrating NFC functionality into the handset. The NFC Antenna obviously is needed for receiving and transmitting adequate radio signals. The NFC Controller modulates, demodulates and processes the signals in accordance with the mentioned NFC specifications whilst supporting all three modes of operation. Last but not least, the NFC architecture provides a Secure Element (SE) serving as Trusted Execution Environment (TEE). Many NFC systems deal with critical and sensitive data and therefore need a secure environment to store data and to execute applications being protected against manipulation and misuse. Such Secure Element can be integrated into a mobile phone in several ways.

It could either be a dedicated chip that is a fixed part of the phones hardware or it could be realized as a removable and exchangeable chip card. Maybe the most evident and reasonably way is to use the Universal Integrated Circuit Card (UICC) as Secure Element. This card is provided by the mobile network operator (MNO) to its customers anyway and does not only contain the SIM module but also a multi-functional and secure platform for various applications. When switching to a new phone, the customer can hence easily continue to use his data applications stored on ’his’ Secure Element, i.e. his UICC.

However, the UICC is released by and bound to a specific network operator making it problematic to develop UICC based NFC applications without involving the MNOs.

2.5. Comparison to Similar Technologies

Certainly, there are other technologies for wireless communication providing capabilities that are similar to the just presented RFID respectively NFC based specifications. Bluetooth is a further short-range communication technology that can also be integrated into mobile phones. It operates at a higher frequency band of 2.4 GHz, provides greater data rates up to 2 Mbit/s and is therefore more suitable for the transfer of larger amounts of data. It allows considerably higher working ranges of several meters making it on the other hand easier to undesirably intercept signals. It hence provides less security. Furthermore, NFC connections can be established at once within a fraction of a second, whereas Bluetooth usually involves further configuration settings and user interaction or device pairing. However, a new Bluetooth feature, called Bluetooth low energy (BTE), also aims to provide a more usable, low-powered technology with much faster connection setup.

Wi-Fi is another mechanism to exchange data wirelessly. It operates on the same frequencies as Bluetooth, but with higher power. This leads to more power consumption on the mobile device, but allows still higher data rates and larger working ranges of typically up to 100 meters. The connection setup is also quite complex and time consuming. Another important difference to NFC is the fact that both techniques, Wi-Fi and Bluetooth, are not able to communicate with passive, no powered devices such as passive tags.

QR codes provide capabilities that are similar to the usage of NFC tags. They represent two-dimensional optical barcodes, visualized by coded black and white patterns storing various types of data, i.e. up to several thousand characters depending on the tag's size and error correction level. Whilst generating virtually no costs, QR codes can be printed on different kinds of surfaces, typically on product packages and advertisement posters. In order to read the tag content, a camera sensor is required. In contrast to NFC tags they are thus not only more conspicuous, but also sensitive to the readers pose, lightning conditions and other disruptive conditions in the environment. QR tags are cheaper, but reading a QR tag with the built-in camera of a Smartphone is in general more cumbersome and time consuming than reading a NFC tag.

In some areas, NFC has certainly benefits compared to other technologies, but the comparison also reveals that those technologies can complement each other quite well. It is therefore likely that NFC will coexist with existing technologies like Wi-Fi and Bluetooth in future smart phones.

3. Security Concerns

As mentioned, most NFC scenarios are required to deal with sensitive data like credit card numbers, bank account details, account balances, personalized tickets or other personal data. For data storage and wireless data transfer security is therefore an essential issue. NFC thereby provides several mechanisms for security and immunity. First of all, there is obviously a certain physical security due to the touch-to-connect principle. As a matter of fact, the NFC technology only provides data transfer between two devices or between a device and a tagged object when the distance between the two items falls below a certain range. The usual transmit power of radio frequency and the receive sensitivity of NFC readers that fulfill the previously described ISO specifications are only strong enough to operate up to a range of a few centimeters. That means that e.g. at a supermarket checkout the customer needs to place his phone directly over the reading device. Data skimming, that is capturing and intercepting transferred data by a distant attacker, is hence not possible that easily. Misuse is however possible in the form of relay attacks. Such attack is basically accomplished via an attacker serving as a man-in-the-middle who is forwarding transmitted data between a reader, e.g. a reading device for NFC payments, and a target transponder, e.g. a NFC device serving as a credit card, that is actually out of the reading range. The following example illustrates The procedure: An attacker places his modified NFC phone on top of the NFC reader at the POS, e.g. at a checkout in the supermarket. The phone however forwards the data, e.g. via Bluetooth, to his distant accomplice holding another modified NFC phone. He in turn holds his phone - without attracting attention - next to a contactless NFC smart card, e.g. NFC credit card, of the attacked target person. The accomplice's phone operates as NFC reader simulating the actual reading device at the POS. The reader at the POS assumes the target person's card is close, and unknowingly debits his account.The additional data exchange and forwarding via the attacking person-in-the-middle however naturally takes some extra time. A possible countermeasure for such relay attack could for example be built upon a quite short timeout threshold that avoids transactions if the response time is too slow. The concept of Google Wallet is however also secured against such attacks as thereby a PIN has to be entered in order to activate the phone's NFC broadcast hardware and to activate the Secure Element that is storing all the sensitive data. The Wallet PIN also prevents unauthorized usage of the payment card in case the NFC phone is stolen.

On higher layers however, NFC applications can of course use industry-standard cryptographic protocols like SSL/TLS based methods to encrypt the data that is to be transferred over the air and that is stored in the Secure Element.

Other possible NFC vulnerabilities involve the manipulation of NFC tags Existing passive NFC tags, e.g. on a smart poster, could be replaced by spoofed tags such that a modified NDEF message is read by a NFC reading device.

Possible attacks could for example replace the URI record with a malicious URL, e.g. in order to make the user load a phishing website that steals the users credentials. Experiments show that one can modify the NDEF message of a smart poster such that the visualized content on the phone, e.g. the website URL, is hardly distinguishable from the original one. Furthermore, it is even possible to create a malformed NDEF message that causes the some applications to crash. This form of manipulation could be used by attackers to debase the relationship between a user and the pretended service provider.

In general, one can summarize that NFC is not more insecure than other related technologies. It offers options for encrypting data on the application layer the same way as Wi-Fi or Bluetooth, but additionally provides safety through the requirement of very close physical proximity. Compared to traditional payment methods including magnetic strip cards that can easily be skimmed or cloned, it is quite difficult to tamper NFC hardware. Beside the physiological concern of transferring money or sensitive data without wired connection over the air, the NFC technology can thoroughly be considered as secure enough for mobile ticketing and payment - at least,if the application developers make use of the provided security mechanisms. And in order to manage existent psychological discomfort, customers just need to be educated in more detail about the technology and its reliability before using it.

4. Challenges and Discussion

At present, the NFC technology has reached a level where commercial launch preparation can begin and should be established.

However, to some extent definite standards for NFC services are still missing. The lack of an ultimate conclusive strategy for the development of NFC services originates in a vital conflict between several involved key factors including mobile phone manufactures, network operators, banks and other service providers: every party indeed tries to enforce its interests and wants to play a major role in the flow of the application scenario and the associating acquisition of big money. Third-party providers, like banks and other financial institutions, want to host NFC applications in neutral space on the handset, whereas network operators of course want to charge customers for providing services hosted in secure environment on the UICC. They are also in possession of the underlying wireless network infrastructure and can thus control any SMS-based remote over-the-air management capabilities that might be used to conveniently configure or update NFC services on the handset. The mobile phone manufacturers on the other hand decide which sort of NFC hardware and which alternative forms of dedicated Secure Element chips are actually implemented in the handset. And on higher layers, of course also the phone's operating system needs to provide appropriate NFC support. Google already offers mature NFC interfaces for developers within their own Android operating system and - in partnership with several banks and the assistance of a handset manufacturer - managed to publish a fist qualified application for mobile NFC payment. Reliability and usability of NFC applications are probably the most important determinants of the user experience in everyday use of the NFC technology and therefore important keys to its success. When compared to alternative technologies,NFC offers great advantages. Essential corner stones have already been established and effectual field trials have been completed. Now, based on successful partnerships and collaborations between the mentioned stakeholders, applications with good user experience need to be published. The existence of such applications is attended by the motivation of handset manufacturers to be incentivized to the production of NFC capable smartphones. Having this accomplished, it is very likely that the NFC technology will play a big role in our future everyday life.

References

[1] G. International Telecommunication Union (ITU), "Itu internet reports2005: The internet of things, executive summary," november 2005, lastvisited on January 19th 2012. [Online]. Available: http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings summary.pdf

[2] I. C. USA, "Idc - press release: Samsung takes top spot as smartphone market grows 42.6visited on January 19th 2012. [Online].Available:http://www.idc.com/getdoc.jsp?containerId=prUS23123911

[3] ——, "Idc - press release:smartphones outstrip feature phones for firsttime in western europe as android sees strong growth in 2q11, says idc," september 2011, last visited on January 19th 2012. [Online].Availablehttp://www.idc.com/getdoc.jsp?containerId=prUK23024911