A new Approach of Touch and Run towards expediting transactions between Digital Device

Dr. Vinod L Desai
Asst. Professor, Computer Science Dept.,
Government Science College,
Sat Pipla, Opp. I.T.I., Chikhli-386521. Navsari. Gujarat.

Abstract—RFID is a wireless communication technology that is used globally for a vast number of applications such as access control, asset tracking and contactless payments. RFID was first patented in 1983 and is the precursor to NFC, the latest wireless communication technologies. As a short-range wireless connectivity technology, NFC offers safe yet simple and intuitive communication between electronic devices. The existing radio frequency (RF) technology base has so far been driven by various business needs, such as logistics and item tracking. While the technology behind NFC is found in existing applications, there has been a shift in focus most notably, in how the technology is used and what it offers to consumers. With NFC technology, communication occurs when an NFC-compatible device is brought within a few centimetres of another NFC device or an NFC tag. The big advantage of the short transmission range is that it inhibits eavesdropping on NFC enabled transactions. NFC technology opens up exciting new usage scenarios for mobile device. It uses magnetic field induction to enable communication between electronic devices in close proximity. Based on RFID technology, NFC provides a medium for the identification protocols that validate secure data transfer.

Keywords—RFID, RF, NFC, ISO, IEC, ECMA

I. INTRODUCTION

Near Field Communication (NFC) is a new, short-range wireless connectivity technology that evolved from a combination of existing contactless identification and interconnection technologies. It was jointly developed by Sony and NXP Semiconductors (formerly Philips).

NFC is designed to enable the exchange of various types of information, such as telephone numbers, pictures, MP3 files or digital authorizations between two NFC enabled devices like mobile phones, or between an NFC enabled mobile phone and a compatible RFID chip card or reader that are held close to each other. NFC is intended to be used as an access key to contents and for services such as cashless payment, ticketing and access control. NFC operates in a frequency range centered on 13.56 MHz and offers a data transmission rate of up to 424 kbit/s within a distance of approximately 10 centimeters [2].

NFC works using magnetic induction, a reader emits a small electric current which creates a magnetic field that in turn bridges the physical space between the devices. That field is received by a similar coil in the client device where it is turned back into electrical impulses to communicate data such as identification number status information or any other information. So-called ‘passive’ NFC tags use the energy from the reader to encode their response while ‘active’ or ‘peer-to-peer’ tags have their own power source and respond to the reader using their own electromagnetic fields. NFC interfaces are defined in a pair of ISO and ECMA standards. ISO/IEC 18092 / ECMA-340 defines communication modes for NFC Interface and Protocol (NFCIP) setting active and passive communications modes and relevant modulation schemes coding transfer speeds frame format collision control parameters transport protocol and more; ISO/IEC 21481 / ECMA-352 defines

NFCIP-2 which specifies communications modes to minimise interference with other contactless card devices [2][4].

To ensure interoperability between mobile phones and RFID chip cards of different manufacturers, digital protocol tests and RF measurements are required on NFC devices. The RF measurements essentially include timing measurements, the measurement of signal strength in polling mode, carrier frequency measurement, reception sensitivity in polling mode, and the measurement of load modulation (signal strength of the listener signal).

NFC is designed to support existing RFID transactions including contactless payment sand some ticketing systems, as well as being generally programmable platform. During a transaction, one party can be completely inactive, drawing power inductively from the active party. Even the active party draws little power and can be left on all the time with minimal effect on the phone’s overall power draw. Also, the nearness of NFC transactions creates the possibility of using proximity as context and triggering an appropriate action almost instantaneously. The primary driver for the adoption of NFC on cell phones is contactless payments and ticketing.NFC, in the form factor of a credit card, has been used widely in Japan and Hong Kong for many years: for public transportation, vending machines, and convenience stores.

Standards have also been created for “smart posters”;posters, signs, and magazine pages can possess cheap, embedded data tags that contain information such as details of museum exhibits, transportation schedules, discount coupons, movie clips, or links to e-commerce sites. A third important use of NFC is for making connections between electronic devices—simply touching the devices together will configure them to connect over a longer-range protocol such as Bluetooth or Wi-Fi.

II. FEATURE OF NFC

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

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

1) The devices can rely on the protocol to be inherently secured1 since the devices must be placed very close to each other. It is easy to control whether the two devices communicate by simply placing them next to each other or keeping them apart.
2) The procedure of establishing the protocol is inherently familiar to people: you want something to communicate – touch it. This allows for the establishment of the network connection between the devices be completely automated and happen in a transparent manner. The whole process feels then like if devices recognize each other by touch and connect to each other once touched.

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

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

III. THE PROTOCOL

The protocol is based on a wireless interface. There are always two parties to the communication; hence the protocol is also known as peer-to-peer communication protocol. In order to determine what sort of information is to be exchanged between devices, the NFC standard currently has three distinct modes of operation for compliant devices. Perhaps the most common use in smartphones is the peer-to-peer mode, which allows two NFC-enabled devices to exchange various pieces of information between each other. In this mode both devices switch between active, when sending data, and passive states when receiving.

Read/write mode, on the other hand, is a one way data transmission, where the active device, possibly your smartphone, links up with another device in order to read information from it. This is the mode used when you interact with an NFC advert tag.

The final mode of operation is card emulation, whereby the NFC device can be used like a smart or contactless credit card in order to make payments or tap into public transport systems.

The interfaces operate in the unregulated RF band of 13.56 MHz. This means that no restrictions are applied and no licenses are required for the use of NFC devices in this RF band. Of course, each country imposes certain limitations on the electromagnetic emissions in this RF band. The limitations mean that in practice the distance at which the devices can connect to each other is restricted and this distance may vary from country to country. Generally speaking, we consider the operating distances of 0~20 cm.

As is often the case with the devices sharing a single RF band, the communication is half-duplex. The devices implement the “listen before talk” policy – any device must first listen on the carrier and start transmitting a signal only if no other device can be detected transmitting.

NFC protocol distinguishes between the Initiator and the Target of the communication. Any device may be either an Initiator or a Target. The Initiator, as follows from the name, is the device that initiates and controls the exchange of data. The Target is the device that answers the request from the Initiator.

NFC protocol also distinguishes between two modes of operation: Active mode and Passive mode. All devices support both communication modes. The distinction is as follows:

1. In the Active mode of communication both devices generate their own RF field to carry the data.
2. In the Passive mode of communication only one device generates the RF field while the other device uses load modulation to transfer the data. The protocol specifies that the Initiator is the device responsible to generate the RF field.

The application sets the initial communication speed at 106, 212 or 424 kbit/s. Subsequently the application and/or the communication environment may require speed adaptation, which can be done during communication. NFCIP-1[4] uses different modulation and bit encoding schemes depending on the speed. While establishing the communication, the Initiator starts the communication in a particular mode at a particular speed. The Target determines the current speed and the associated low-level protocol automatically and answers accordingly. The communication is terminated either on the command from the application or when devices move out of range.

How do NFC Works?

NFC (near-field communication) allows two devices placed within a few centimeters of each other to exchange data. To materialize this to happen, both devices must be equipped with an NFC chip. In the real world, there are essentially two ways this works.

Two-way communication: This involves two devices that can both read and write to each other. For example, using NFC, you can touch two Android devices together to transfer data like contacts, links, or photos.

One-way communication: Here, a powered device (like a phone, credit card reader, or commuter card terminal) reads and writes to an NFC chip. So, when you tap your commuter card on the terminal, the NFC-powered terminal subtracts money from the balance written to the card.

IV. COMPARISON WITH OTHER TECHNOLOGIES

4.1 NFC and RFID

NFC and RFID (radio frequency identification) are sometimes used interchangeably, but NFC is really a newer version or extension of RFID. RFID waves can have very long ranges (e.g., RFID is the tech that helps highway toll readers read your car's toll pass), while NFC limits the range of communication to within 4 inches. This makes NFC perfect for more secure applications like paying for things or securely logging in at a location.

NFC also allows two-way communication, as opposed to RFID's one-way reading technology. So transferring photos or contacts between devices is a common use of NFC. However, the essential extension of RFID is the communication mode between two active devices. In addition to contactless smart cards (ISO 14443 [3]), which only support communication between powered devices and passive tags, NFC also provides peer-to-peer communication. Thus, NFC combines the feature to read out and emulate RFID tags and furthermore, to share data between electronic devices that both have active power.

4.2 Comparison with Bluetooth and Infrared

Compared to other short-range communication technologies, which have been integrated into mobile phones, NFC simplifies the way consumer devices interact with one another and obtains faster connections. The problem with infrared, the oldest wireless technology introduced in 1993, is the fact that a direct line of sight is required, which reacts sensitively to external influences such as light and reflecting objects. The significant advantage over Bluetooth is the shorter set-uptime. Instead of performing manual configurations to identify the other’s phone, the connection between two NFC devices is established at once (<0,1s). All these protocols are point-to-point protocols. Bluetooth also supports point-to multipoint communications. With less than 10 cm, NFC has the shortest range. This provides a degree of security and makes NFC suitable for crowded areas. The data transfer rate of NFC (424 kbps) is slower than Bluetooth (721 kbps),but faster than infrared (115 kbps). In contrast to Bluetooth and infrared NFC is compatible to RFID.

4.3 Comparison with Bluetooth and NFC

You might think that NFC is bit unnecessary, considering that Bluetooth has been more widely available for many years. However, there are several important technological differences between the two that gives NFC some significant benefits in certain circumstances.

The major argument in favour of NFC is that it has much lower power consumption than Bluetooth, even lower than the new Bluetooth 4.0 (aka Bluetooth low energy). This makes NFC perfect for passive devices, such as the advertising tags that we mentioned earlier, as they can operate without the need for a major power source.

However, this power saving does have some major drawbacks. Most noticeably the range of transmission is much shorter than Bluetooth. While NFC has a range of around 10cm, just a few inches, Bluetooth connections can transmit data up to 10 meters or more from the source. Another drawback is that NFC is quite a bit slower than Bluetooth, transmitting data at a maximum speed of just 424 kbit/s, compared with 2.1 Mbit/s with Bluetooth 2.1 or around 1 Mbit/s with Bluetooth Low Energy.

But NFC does have one advantage when it comes to speed, faster connectivity. Due to the use of inductive coupling, and the absence of manual pairing, it takes less than one tenth of a second to establish a connection between two devices, a speed which has only recently been matched by Bluetooth 4.0.

V. APPLICATIONS OF NFC

Many possible NFC applications are being considered. The special advantage of NFC is its straight forward mode of use. Simply touch or place a device close to something to initiate the desired service. With NFC, we can touch another phone (or any other NFC device) and we can run all kinds of applications without having to find the application of interest and painstakingly type in URLs or any other parameters. This is particularly important because we are often in a hurry on the go, which is distinctively different from how we use a PC. We are not sitting down; we do not have a keyboard; and we are always running out of time. Some typical and interesting uses of NFC are:

1. Mobile Payment

One day, we will all be paying for things with our smart phones and NFC is the ticket to that future. In light of the many recent credit card data breaches, now is an especially good time to present a solution that finally shields our wallets from theft and fraud.

Many retailers in foreign countries including Target, Macys and Walgreens already have NFC-based contactless pay terminals in place, making the transition to mobile payments easy. Phones compatible with Google Wallet can currently use these terminals, as can Apple's iPhone 6 and 6 Plus. The biggest concern around NFC payments is security, but the mobile payment structure is so complex, any hacking or intercepting would be very difficult. To understand why, here is how it works.

After launching the payment application on your phone, the phone is tapped on the credit card terminal and a connection is made using NFC. At this point, you may be asked to scan your finger or enter a passcode to approve the transaction. The transaction is then validated with a separate chip called the secure element (SE), which relays that authorization back to the NFC modem. From there, the payment finishes processing the same way it would in a traditional credit card swipe transaction.

The most important step in the mobile payment transaction is the secure element, which holds all the authorization power. Whether it's a chip in the phone, or functions virtually in the cloud, the secure element is tamper-proof and protected by a unique digital signature. As explained by Michael Armentrout of Infineon [5], which manufactures secure element chips, the architecture of the secure element is designed to be hardened against attacks on the phone.

"That includes software attacks but also hardware-based attacks where someone got your phone or SIM card, it would be extremely difficult to obtain info off of that because it's a chip that is designed to have security mechanisms that go well beyond a normal processor."

2. Paying for your parking meter, at least in some cities.
3. Getting tickets or boarding passes. Some airlines and buses are also experimenting with using NFC for boarding passes.
4. Opening doors. BMW has NFC-enabled car keys. Companies and universities are looking into or rolling out using NFC-enabled devices as security badges. To gain physical access somewhere, members need only tap their smartphones at the door.
5. Downloading information. Advertisers and marketers can use NFC chips in porters and other promotional materials so all you have to do to get more information is tap or wave your phone (easier than QR codes, perhaps).

VI. NFC STANDARDS

The NFC protocol requires standardization in order to be accepted fully by the industry and provide for compatibility between the devices produced by different manufacturers. The standardization also means keeping the specification open and accessible for everybody, facilitating the analysis of the protocol and adaptation of the devices for various needs.

The work on standardization is done within Ecma International, a standards organisation with a long history of successful projects. The standards are published by Ecma International and, consequently, become also ISO/IEC and ETSI standards. Sony Corporation and Royal Philips Electronics are the founders of this work [1][4].

Standards published as of December 2004:

- ECMA-340 “Near Field Communication – Interface and Protocol (NFCIP-1)” (ISO/IEC 18092)
- ECMA-352 “Near Field Communication Interface and Protocol – 2 (NFCIP-2)” (ISO/IEC 21481)
- ECMA-356 "NFCIP-1 - RF Interface Test Methods" (ISO/IEC 22536)
- ECMA-362 "NFCIP-1 - Protocol Test Methods" (ISO/IEC DIS 23917).

VII. SECURITY ASPECTS

It should be mentioned that the short communication range of a few centimetres, though it requires conscious user interaction, does not really ensure secure communication.

There are different possibilities to attack the Near Field Communication technology. On the one hand the different used devices can be manipulated physically. This may be the removal of a tag from the tagged item or wrapping them in metal foil in order to shield the RF signal. Another aspect is the violation of privacy.If proprietary information is stored on a tag it is important to prevent from unauthorized read and write access. The read-only tags are secure against an unauthorized write access. In the case of rewritable tags we haveto assume that attackers may have mobile readers and the appropriate software which enable unauthorized read and write access if the reader distance is normal.In this work we want to focus on attacks with regard to the communication between two devices. For detecting errors, NFC uses the cyclic redundancy check (CRC). This method allows devices to check whether the received data has been corrupted or not.

VIII. CONCLUSION

In summary, Near Field Communication is an efficient technology for communications with short ranges. NFC supports a better user experience, since one device can scan another without first launching a special application. It offers an intuitive and simple way to transferdata between electronic devices. A significant advantage of this technique is the compatibility with existing RFID infrastructures. Additionally, it would bring benefits to the setup of longer-range wireless technologies, such as Bluetooth.

With regard to the security of NFC, we discussed different attacks and possible Counter measures to mitigate their impact. Despite the restriction of the range, eavesdropping or data modification attacks can be carried out. But, disregarding relay attacks, NFC provides security against Man-in-the-Middle-Attacks. In order to provide protection against these threats, the establishment of a secure channel is necessary.

REFERENCES

[1] Ecma International: http://www.ecma-international.org

[2] www.nfc-forum.org.

[3] ISO/IEC 14443: Identification cards - Contactless integrated circuitcards - Proximity cards. 2001, URL: www.iso.ch.

[4] ISO/IEC 18092(ECMA-340): Information technology – Telecommunicationsand information exchange between systems - Near FieldCommunication - Interface and Protocol (NFCIP-1). First Edition, 2004-04-01.

[5] http://www.cnet.com