Master Project Report

NFC- An Accurate Indoor Navigation System

Submitted in partial fulfillment of the requirements for the degree of

Master of Technology

By

Arpit Jain

Roll No: 113050028

Under the guidance of
Prof. D.B. Phatak

June, 2013

Department of Computer Science and Engineering
Indian Institute of Technology, Bombay
Mumbai-400076
# Contents

1 Introduction 1
   1.1 Operating modes of NFC .......................... 1
   1.2 NFC Forum standards .................................. 2
   1.3 Uses of NFC ........................................... 2
   1.4 NFC Architecture ....................................... 3

2 Attacks on NFC 5
   2.1 Attacks .................................................. 5
      2.1.1 Relay Attack ........................................ 5
      2.1.2 Skimming and cloning attack on NFC .................. 6
      2.1.3 Orientation and problems identified .................. 6
   2.2 Security countermeasures for Relay Attack ................. 8
      2.2.1 Preventing Relay Attacks using Location Information ... 9

3 Navigation 10
   3.1 Graphing ................................................ 10
   3.2 Routing Algorithm ....................................... 10
      3.2.1 Dijsktra’s Algorithm .............................. 10
      3.2.2 Breadth First Search .............................. 11
      3.2.3 User Interface .................................. 11

4 Android APIs 13
   4.1 NFC APIs ............................................... 13
   4.2 QR code android library ................................ 13
   4.3 Osmdroid .............................................. 14

5 Problem Statement 15

6 Positioning Techniques 16

7 Tools & Technology 18
   7.1 Tools Used .............................................. 18
   7.2 Technology Used ....................................... 18

8 Implementation 19
   8.1 Referencing Methods ................................... 19
   8.2 Data Model ............................................. 19
   8.3 Functionality Specification ........................... 19
      8.3.1 Identifying Location .............................. 19
8.3.2 Shortest Route ........................................ 21
8.3.3 Other NFC tags/QR code .............................. 21
8.3.4 All Paths ................................................. 21
8.3.5 Finding Nearest Places .............................. 21
8.4 Map View .................................................. 24
8.5 NFC handling ............................................. 24
8.5.1 Creating NDEF record .............................. 24
8.5.2 Intent filter declaration ............................ 24
8.6 QR Code Handling ........................................ 25
8.7 Software architecture ................................... 27
8.8 Applications .............................................. 27
8.9 Limitations ............................................... 27
8.10 Test Results .............................................. 27

9 Conclusion & Future Work ................................ 28
  9.1 Conclusion ............................................... 28
  9.2 Future Work ........................................... 28

10 Acknowledgements ........................................ 30
## List of Figures

1.1 NDEF message and records ........................................... 2
1.2 Functional diagram of NFC architecture .......................... 3

2.1 Practical relay setup using only NFC mobile phones ............... 6
2.2 Message flow Diagram ................................................. 7

4.1 Tag Dispatch system ....................................................... 13

8.1 Interface for indoor navigation system .............................. 20
8.2 User Location inside building .......................................... 20
8.3 Illustrates User query for finding shortest path ..................... 21
8.4 Map showing Shortest path .............................................. 22
8.5 Map showing all the NFC tags/ QR code inside building ............ 22
8.6 Map showing all the path from source to destination ............... 23
8.7 User queried for nearest lab from its location ..................... 23
8.8 Map showing the path from user location to nearest lab ........... 24
8.9 Showing Map of a building ............................................. 25
8.10 Illustrating read/write operation on NFC tags ...................... 25
8.11 QR code scanner ......................................................... 26
8.12 Showing User location after QR code scanning .................... 26
Abstract

Contactless technology now a days, is widely used in security applications including identification, payment and access control. Near Field Communication (NFC) is a short range wireless technology which uses frequency of about 13.56MHz for communication between devices, not more than 10cm. It has been found that NFC is generally used for payment purposes to make it free from attacks. This report contains various attacks possible on NFC and their suggested countermeasures.

This report also presents an idea of using the short range of NFC for indoor navigation, to mitigate present indoor navigation problems. This system allows user to find out its location and to navigate within building by only touching the tags spread over the building. Using NFC has its own advantages in terms of location precision inside building, over other indoor navigational technologies like Wireless fingerprinting. This report proposed an indoor navigation system using NFC and QR code in order to increase the system usability.

Keywords: NFC, NFC-enabled phone, peer-to-peer, relay attack, transactions, countermeasures, Location based services, QR code.
Chapter 1

Introduction

NFC (near field communication) is a short range wireless technology that allows 2 devices to communicate that are held closely. NFC uses ISO 14443 standard (standard for contactless card) [10] and is compatible with existing contactless card infrastructure.

NFC operates at a frequency of 13.56 MHz and provides a transmission rate of up to 424 kbit/s within a distance of approximately 10 centimeters. NFC-capable devices can communicate in active-active (peer-to-peer) as well as active-passive in contrast to the conventional contactless technology [3]. In active mode, both initiator as well as target have their own RF field using which they can communicate. Initially, Initiator transmits an RF carrier to target, who after receiving it, acknowledges initiator. Initiator then switches the carrier signal off and then a response from target is sent to initiator. While in passive mode, the target device does not have its own RF field but is powered by the radio signals of initiator.

NFC-enabled mobile phones consists of a secure element which is responsible for storing cryptographic keys and thus providing secure environment for applications. Basically there are three ways to implement secure element (SE) in NFC. First involves the presence of an independent hardware module inside phone which act as SE. The first involves an SE that is present inside phone as an independent embedded hardware module. Second way is to implement SE within Subscriber Identity Module (SIM). While the last option is to implement SE on Secure Digital card (Secure SD).

1.1 Operating modes of NFC

There are three modes in which NFC operates:

1. Read/Write: In Read/write mode, any NFC supported tags can be read/write using NFC enabled mobile phones.

2. Peer-to-Peer: This mode supports exchange of data between two NFC-enabled devices.

3. Card Emulation: In this mode, NFC enabled mobile phone will act like a contactless card or as a tag for NFC reader.
1.2 NFC Forum standards

1. **NDEF**: NDEF forum specifies a format for message encapsulation, so that NFC device can exchange information with another NFC device or NFC tag. Its a light weight message in the form of 0/1’s, used to encapsulate payload of 1 or many application and combine it into a single message. There can be more than 1 NDEF record in an NDEF message. The payload can be of type either URL, MIME or an NFC data type provided that for any NFC data type the payload contents must be specified in an NFC Record Type Definition (RTD) file.

   During communication between NFC reader devices and NFC tag for read/write, hexa code are read. Figure[1.1] shows the NDEF message and records.

   ![NDEF message and records](image)

   **Figure 1.1**: NDEF message and records

2. **RTD(Record Type Definition)**- NFC forum defines various record formats that can be put in NDEF records. And each NFC Forum record should be defined in Record Type Definition (RTD) document. NFC has the following RTDs:

   (a) NFC Text
   (b) NFC URI
   (c) NFC Smart Poster
   (d) NFC Generic Control
   (e) NFC Signature

3. **LLCP**- NFC Forum has introduced the link-level protocol called as the Logical Link Control Protocol(LLCP) to improve the peer-to-peer mode. LLCP introduces a link-level, two-way connection, allowing send and receive of data between peers through two methods of data exchange as follows: (i).Connection-oriented transfer, in which acknowledgement data exchanges is done (ii).Connectionless transfer, where no acknowledgement of data exchange is done.

1.3 Uses of NFC

The special advantage of NFC is its straightforward mode of use, simply place a device close to tag to initiate the desired service. Some typical uses are:
1. **Service Initiation** - In this, an NFC-enabled phone touched against an NFC tag can read information such as URL, text etc, based on which an action will be defined. Example: In smart poster NFC tags have been placed containing some information in NFC data format. When an NFC-enabled phone touches a tag in the poster, it reads the information present. Depending on the information type, the phone opens web browser, or asks the user for telephone call.

2. **Ticketing** - Ticketing can be done using NFC enabled phone by touching your phone to ticket reader. Here phone works in a card emulation mode and therefore act as a card. For using NFC phone as travel ticket, secure element (SE) should be present on the phone running ticketing application.

3. **Payment** - A payment in a similar way as Ticketing can be done using NFC phone provided phone uses a secure element which runs payment application.

4. **Sharing** - Peer-to-peer communication mode allows NFC enabled mobile phones to share data. For example, NFC-enabled phones can share information of business card by sending radio signal to the other phone in the range. The information is shared in the NDEF format which is identified by both devices. Generally sharing is done through Bluetooth, NFC is only used to initiate Bluetooth.

5. **Connecting devices** - NFC device can connect with any other device without the need of any configuration or set-up. Ex: An NFC enabled phone needs to be touch in order to connect with bluetooth headset. For this bluetooth device should have NFC tag containing all the pairing information required in NDEF format.

### 1.4 NFC Architecture

This chapter includes the main components of an NFC-enabled phone platform[5], and also API’s available for communication between these components. 3 main components are as follows:

1. **Application Execution Environment (AEE)**: The general application area of the mobile phone providing data storage and processing capabilities.
2. **Trusted Execution Environment (TEE):** NFC based transaction is controlled using a secure platform for holding sensitive applications and cryptographic keys. TEE contains this secure element which is supposed to be the core of NFC system. Basically there are three ways to implement secure element (SE) in NFC. First involves the presence of an independent hardware module inside phone which act as SE. The first involves an SE that is present inside phone as an independent embedded hardware module. Second way is to implement SE within Subscriber Identity Module (SIM). While the last option is to implement SE on Secure Digital card (Secure SD).

3. **NFC Controller:** NFC controller handles the physical transmitting and receiving of data over the RF interface. Through standardized interfaces SE communicates with the external reader device, NFC controller and the applications installed on the mobile phone.
Chapter 2
Attacks on NFC

2.1 Attacks

Although NFC communication range is restricted to few centimeters, but still NFC does not ensure secure communication. There are various attacks possible over NFC like Eavesdropping, data modification, relay attack etc. The most prominent among these is the relay attack because in that attacker do not need any dedicated hardware and no special knowledge of protocols used. Unlike in Eavesdropping, we need an antenna for picking up the RF signals, the distance at which an attacker can eavesdrop RF signals depends on various parameters, but only small number of meters. In the same way, data can be destroyed using RFID jammer, however modification of data in such a way that it appears valid to the user, is difficult.

2.1.1 Relay Attack

NFC technology now a days has proven its utility in m-payment, ticketing and access control. But the ability of NFC-enabled phones to act as a token and a reader makes it an ideal platform for implementing relay attacks. In relay attack [6, 7], attacker only needs to relay the challenge and response to the legitimate token and reader respectively, without the knowledge of the data to be relayed and security protocols used. For this the attacker and his accomplice uses proxy-devices that communicate over a proxy channel, and thus requires a high-speed and reliable communication link between the two NFC mobile phones implementing the proxy-reader and proxy-token. Figure[2.1] shows practical implementation of relay attack where, a person without the knowledge of rules of chess could challenge two grand masters and play against them. It only need to forward the move received from one grand master to the other. Each grand master would think that they are playing said person, but in reality they are playing against each other.

Relay attack is able to bypass application layer security protocol even if it is based on strong cryptographic principles by simply relaying a challenge to the authenticated token, which provides him the correct response, which can be relayed back to the verifier. In this case the attacker has no need to know the details of the content he/she relays, i.e. does not need to know about the protocol, or any secret key material.
2.1.2 Skimming and cloning attack on NFC

NFC enabled mobile phone with an embedded secure element can be used as a platform for skimming and cloning attacks[4]. For developing clone, some midlet needs to be executed for unlocking of SE and once it gets unlocked, an applet will be installed on SE, GP shell. Our applet should be designed in a way to receive the communication messages exchanged and respond in a way with the messages that makes the reader feel like it is communicating with the legitimate reader. In a same way MIDLET(for skimming) can be developed and designed to establish an connection with external smart cards and exchange APDUs(Application protocol data units) with them. Figure[2.2] illustrates the static messages used to authenticate contactless card.

2.1.3 Orientation and problems identified

1. NFC enabled phones has an legitimate acceptable factor which makes them less suspicious in public, unlike custom built hardware used for skimming and cloning attacks.

2. No dedicated hardware is needed for the relay attack to perform, it is possible using unmodified NFC-enabled mobile phones, and requires an attacker to write suitable mobile platform applications using publicly available APIs.

3. Some security vulnerability are also available in NDEF, standard which NFC is using for communication. An attacker may replace tag content or even replace whole tag with the modified tag, this may result in attacks like phishing.
Figure 2.2: Message flow Diagram

TestReader

1.a. Selects $DDF_{name}$.

2.a. Selects $ADF_{AID}$ received from (1.b).

3.a. Initiates GET PROCESSING OPTIONS.

4.a. Initiates reading of application specific data or records.

5.a. Completes static identifier process and proceeds with card specific functions.

TestCard

1.b. Selects $DDF_{name}$. If successful, returns AID of $ADF_{AID}$ else, returns file not found error.

2.b. Selects $ADF_{AID}$. If successful, returns application details of the selected ADF else, returns file not found error.

3.b. Performs GET PROCESSING OPTIONS function.

4.b. Reads and returns application specific data or records.

5.b. Completes static identifier and proceeds with cardholder verification, transaction processing, etc.

Notations used:

2.2 Security countermeasures for Relay Attack

This section briefly examines security countermeasures proposed for making contactless systems resistant to relay attacks. While considering the countermeasures, user experience should also be kept in mind. We therefore do not consider countermeasures which shifts the responsibility of security to the end user, such as shielding tokens or performing a two-factor authentication using a PIN. Various countermeasures are as follows:

1. **Time Based Protocol**: This countermeasure is based on timing constraint on response, as the relayed response will lead to increase in response time in comparison to legitimate response. But it is difficult to implement in practice. Firstly, obtaining accurate transaction time information is a challenge, considering number of underlying process components adding overhead. Accurate response time would require dedicated hardware which monitors RF channel.

2. **Distance Bounding Protocol**: Based on the round trip time of challenge-response pairs, this protocol defines an upper bound for the distance between two communicating entities, and it has been proposed that these are suitable for relay-resistant RFID systems. Distance bounding is in theory the most effective countermeasure but this approach requires special communication channels to facilitate accurate and secure distance estimates, since conventional RF channels have been shown inadequate for implementation of secure distance bounding.

3. **Location Based Protocol**: Use of location information in mobile network access systems has given rise to many applications and services, the capabilities of mobile phones to deduce both absolute and relative location are not utilized for verifying the proximity of devices conducting a transaction. Reliable and accurate location information is an effective countermeasure against relay attacks, e.g. location information could be simple appended to a transaction that is then signed by the legitimate sender, and as has also been shown to enable other security services. In fact the use of location information available in the mobile environment to provide security services is not new, and could serve as an ideal countermeasure in NFC systems, which as intrinsically linked to mobile. In this section, we discuss the potential role of mobile location-based services in preventing relay attacks on transactions between NFC-enabled phones, or an NFC-enabled mobile phone and a reader with knowledge of its own location. There are various methods of retrieving the mobile location information. Some of them are as follows:

   (a) **Network Cell Broadcast**: location information can be obtained using metrics from the cell broadcast towers or base stations. These include a Cell-ID identifier associated with parameters such as Mobile Country Code (MCC), Mobile Network Code (MNC) and Location Area Code (LAC). The cell broadcast information can be retrieved by using location APIs from the mobile software platform or from the (U)SIM.

   (b) **GPS Based Location Sensing**: The Global Positioning System (GPS) is a navigational system based on earth-orbiting satellites and provides location information around the globe. GPS finds applications in many fields such as transportation, aviation and shipping. The GPS system is based on 24 satellites in six different orbital-paths. The satellites and the receivers are
synchronized with high precision clocks which is used to estimate the distance between them and the receiver.

2.2.1 Preventing Relay Attacks using Location Information

This method is based on embedding some location information and timestamp along with the message by the sender. And this message is encrypted using digital signature in order to prove that the message is constructed by the legitimate sender only. Now the receiver on the other side compares sender location and confirms its presence in close proximity. If the message is relayed by the attacker then it would get detected. The timestamp is used to prevent recording a valid transaction by an attacker and using it later for the same location.
Chapter 3

Navigation

Navigation system helps to find out the optimal route from source to destination. It is composed of graphing functionality and routing algorithm.

3.1 Graphing

This is the most important module for navigation, as with the current user location known, one cannot move to its destination until and unless some path is available to user. But since the map is in the form of geometrical images, it is difficult to find the path. Therefore, we need to first represent the map of building in a graph with nodes and edges, so that all the algorithms can be applied. A graph can be a complex system with nodes and links connected in a tree like structure. Specific positions in building is represented by nodes with some location information associated with them. Whereas the link is a line where the user can move while going from one node to another. User can move between 2 nodes only if there is a link in between. The link is associated with a cost metric representing the distance to travel through the link. The distance between 2 nodes can be found by computing the euclidean distance between their coordinates.

3.2 Routing Algorithm

Two routing algorithms used in this application. Dijsktra’s is used for finding shortest path between two locations and Breadth first search for finding all the path from source to destination. Following are the algorithms.

3.2.1 Dijsktra’s Algorithm

Dijkstra’s algorithm[9] is one of the widely used algorithm for routing, proven to find the shortest path. This algorithm is suitable for finding shortest path for a graph with single source node and one/more destination nodes. This algorithm starts from the source node and chooses the node from the source node with minimum cost. This node now become visited from the source node. Now marked this node as optimized and evaluate the cost to all the adjacent nodes. Once the algorithm reaches the destination, the optimized cost can be found out and the path can be deduced by traversing it in reverse order. The complexity of this algorithm is o(n^2), n is the total number of nodes. There are some disadvantages of this algorithm, first is the direct proportionality to the number of nodes.
Thus needs a lot of computational efforts for large graphs with large number of node. And second is its limitation to work with graphs having negative edge weight.

**Pseudo Code**

\[
\text{dist}[s] \leftarrow 0 \\
\text{for all } v \in V - s \quad \text{do } \text{dist}[v] \leftarrow \infty \\
S \leftarrow \emptyset \\
Q \leftarrow V \\
\text{while } Q \neq \emptyset \quad \text{do } u \leftarrow \text{mindistance}(Q, \text{dist}) \\
S \leftarrow S \cup u \\
\text{for all } v \in \text{neighbors } [u] \quad \text{do if } \text{dist}[v] > \text{dist}[u] + w(u, v) \\
\quad \text{then } \text{dist}[v] \leftarrow \text{dist}[u] + w(u, v) \\
\]

Dijkstra’s algorithm fit into our requirement as the graph always contains non-negative cost links. The complexity of this algorithm is also reduced to \(O(n \log n)\) by using minimum heap data structure, thus well suited for building like environment with moderate number of node.

### 3.2.2 Breadth First Search

Breadth First Search\cite{9} is a search algorithm for graph that starts with the root node and explores all the neighboring nodes. Now for all of those nodes keeps exploring the unexplored neighbor nodes until it finds the goal.

**Pseudo Code**

\[
\text{procedure BFS(Graph, source):} \\
\text{create a queue } Q \\
\text{enqueue source onto } Q \\
\text{mark source} \\
\text{while } Q \text{ is not empty: } \\
\quad \text{dequeue an item from } Q \text{ into } v \\
\quad \text{for each edge } e \text{ incident on } v \text{ in Graph: } \\
\quad \quad \text{let } w \text{ be the other end of } e \\
\quad \quad \text{if } w \text{ is not marked: } \\
\quad \quad \quad \text{mark } w \\
\quad \quad \text{enqueue } w \text{ onto } Q \\
\]

The worst case complexity of breadth-first search is found to be \(O(|E| + |V|)\) since every vertex and every edge will be explored. This algorithm has space complexity of \(O(b^d)\) where \(b\) is the branching factor and \(d\) is the depth.

### 3.2.3 User Interface

This module contains intuitive user interface, facilitating the usability of navigational system. It is composed of various activities for map display, optimal route finding, avail-
able NFC tags/ QR code and finding nearest places. This module is explained in more
details in implementation section.
Chapter 4

Android APIs

This chapter briefly describes the available APIs for NFC, QR code and OSM maps in android.

4.1 NFC APIs

This API uses a tag dispatch system which will first discover the NFC tag, scan them, and then identify the activity capable of handling it. Because if user is allowed to execute the application after discovering the NFC tags, then it will result in user to move away from tag, which results in breaking the connection. Once the tag dispatch system is done, intent is sent to interested application. Incase of more application activity chooser resolves it by allowing the user to select any activity. It does this by:

1. Scan NFC tag and finding out the MIME type that specifies data payload.
2. Encapsulating the MIME type and the payload into intent.
3. Based on intent starts an activity.

4.2 QR code android library

Zxing is an android library that helps user to scan graphical barcodes either 1-D or 2-D with camera on their android device. This program converts the scan data represented by

![Figure 4.1: Tag Dispatch system](image)
the barcode into the original data. This makes android system works almost like barcode scanner.

4.3 Osmdroid

osmdroid provides Tools / Views to interact with OpenStreetMap-Data. Osmdroid’s MapView is a replacement of Google’s MapView class. To use this library osmdroid-android.jar and its dependent files should be included into the project.
Chapter 5

Problem Statement

Initially, idea was to explore attacks on NFC and finding the countermeasures for it, to make transaction more secure. But knowing about NFC and its architecture, helps to make use of this wireless technology for a wider purpose. NFC can be used for navigation within buildings, malls, hospitals etc, where other positioning technology like GPS does not work. There are technologies like wireless fingerprinting which are widely used for indoor navigation, but with the short range of NFC(< 10cm), the precision in location achieved is about 10cm, which is one of the significant requirement in buildings. As in building, if the location precision is about 10m than it will be difficult to navigate user within building. To make it a more effective solution this application is integrated with QR code so that without NFC device user can locate itself by using camera of its device. This Application can also be combined with other web services like Local wiki, zomato etc., to avail other location based services.
Chapter 6

Positioning Techniques

This chapter describes various positioning and navigation techniques which have analyzed before this project.

1. **Satellites**: Satellite navigation system provides geo-spatial positioning with global coverage. Using altitude, latitude and longitude can lead to higher degree of accuracy can be determined. But for its functioning line of sight (LOS) is required. This restricts it to use for indoor navigation where LOS is blocked by roofs and walls. For outdoor applications GPS works like a semi-accurate global positioning and navigating system. The GPS system consists of 24 satellites equally spaced in six orbital planes 20,200 km above the Earth. In open space it accuracy lies in the range of 5-6 meters. Since LOS is blocked in an indoor environment so it cannot be used inside building.

   In order to improve the startup performance, or time-to-first-fix of a GPS satellite-based positioning system, Assisted GPS (A-GPS) is used. This system is suitable when satellite signals are unavailable or weak. Assisted GPS is primarily used in cellular phones in which cell phone provides information that helps GPS receiver.

2. **Cellular Communication Network**: Cellular Communication Network is another method for finding user location using Cell-ID. This method uses the capability of the network to find out the position of a cell phone by identifying the cell tower that the device is using at a particular time. The advantage of this method is that it is easy to implement and all mobile phone supports it. As the range of cell towers are around 35Km so the accuracy of this method is very low.

3. **WiFi**: Wi-Fi positioning system is widely used for indoor purposes where GPS is inadequate due to various causes including multi-path and signal blockage. Using the intensity of the received signals and the method of fingerprinting, positioning can be done. In this system also, signal fluctuation may lead to errors and inaccuracies in the path of the user. And this method requires the abundance of several distinguishable WLAN networks and calibration (mapping).

4. **Infrared**: Infrared wireless technology is the leading technology in the field of indoor navigation. There is a remote positioning system based on this technology in which the location of the user is determined from the unique IR signal emitted every 10 seconds by a badge. These signals are captured by sensors placed at
various location inside building and forwards this information to a server. The accuracy of this method is very high for indoor navigation but suffers from certain limitation like, sensor installation cost due to low limited range of IR and the receivers sensitivity to sunlight.
Chapter 7

Tools & Technology

7.1 Tools Used

1. **Eclipse**: Eclipse is a multi-language Integrated development environment consisting of a workspace and an plug-in system for customization. Mostly it is written in Java. It can be used to develop java applications and, through various plug-ins, application of other programming languages like Ada, C, C++, COBOL, Fortran, Haskell, JavaScript, Perl, PHP, Python can also be developed.

2. **Android SDK**: Android SDK provides the developer tools and API libraries required to build, test, and debug android apps. Generally android SDK is installed as a plugin in eclipse to provide easy coding support.

3. **JOSM**: JOSM is the ”Java OpenStreetMap Editor”, a desktop application providing an interface for building maps. This tool is linked with open street maps so maps from osm can be downloaded and changes done in them will get reflected to osm maps, and so can be accessed by everyone.

7.2 Technology Used

1. **Near Field Communication (NFC)**: NFC is a short range wireless communication technology which works at a distance less than 10cm. It allows to share small payloads of data between two Android-powered devices or a tag and NFC device. NFC uses some standard protocols for communication like NDEF for data exchange, and thus are based on existing RFID standards.

2. **QR Code**: Quick Response Codes are a type of barcode either 1-D or 2-D that can be read by smartphones or dedicated QR reading devices, that is linked with phone numbers, text, emails etc. A barcode is attached to the item and contains information about that item. Barcodes initially came for automotive industry but due to its greater storage capacity and fast readability it has become popular outside.

   A QR code consists of a square grid on a white background with full of black modules arranged, which can be read by an camera and processed through error correction method. Once the image is interpreted appropriately, data can then be find out from patterns present in both vertical components and horizontal of the image.
Chapter 8

Implementation

This chapter describes the implementation details of the demonstrator application, covering from functional specifications to android libraries used for this system.

8.1 Referencing Methods

There are two ways of associating location to an object (NFC Tags) used for identifying location of the user. Both of them are described below:

1. **ID Reference Matching** In this method a unique feature is assigned to each object, and that feature is read from the object (either NFC UID or unique QR code content), and matched against a reference model. The reference model maps unique features to links or some geo location. If match is found then the application loads the reference link/location.

2. **Explicit Link** This method uses information directly stored on object (either link or location). And accordingly the application will load that location. In our demo application we have used this reference model. Location information is stored in QR code which is retrieved by the application and the corresponding location will be displayed.

8.2 Data Model

OpenStreetMap XML is used for demonstration purpose. But because of lack of support of suitable standard for indoor geometry data storage, the current model uses only basic geometry elements (nodes and ways).

8.3 Functionality Specification

8.3.1 Identifying Location

The application displays a map showing the current location of the user in building. This can be done by either tapping NFC enabled mobile phone near the NFC tags or by capturing the QR code present outside the room. Any of the NFC tags or QR code can be used depending on what type of device is used and whether camera is allowed or not within building.
Figure 8.1: Interface for indoor navigation system

Figure 8.2: User Location inside building
8.3.2 Shortest Route

Along with the location on the map, user can also find out the shortest route from its location/or any other location to destination. The shortest path is computed using dijkstra’s algorithm. As the graph contains non-negative edges, so the path found is always the shortest one. Figure[8.2] and figure[8.3] shows the optimal path from source to destination.

8.3.3 Other NFC tags/ QR code

This feature helps user to find out the location of all the NFC tags/ QR code placed within building. Thus no need to search in entire building for finding tags. Figure[8.4] and figure[8.5] shows all the available NFC tags/Qr code in the building.

8.3.4 All Paths

Finding shortest route is always not the case, there may be situation when the user does not want the shortest route, but the one which covers some intermediate locations. This feature allows the user to find all the paths from source to destination regardless whether it is the optimal or not. Figure[8.6] shows all the paths from source to destination.

8.3.5 Finding Nearest Places

If the user wants some locations(can be lab/ washroom in our application) which are nearer to its location, then this feature helps him to navigate. This feature also uses the same dijsktra’s algorithm to find the shortest path from its location to the all the location with the same id(desired location), and the choose the shortest among them. Figure[8.7] and figure[8.8] shows the specified nearest place from the user location. in the building.
Figure 8.4: Map showing Shortest path

Figure 8.5: Map showing all the NFC tags/QR code inside building
Figure 8.6: Map showing all the path from source to destination

Figure 8.7: User queried for nearest lab from its location
8.4 Map View

Map View is created by using maps API provided by OSM which is a replacement of google map API. During the onCreate method, the map is initialized to display the standard OSM satellite/aerial map and two overlays. Figure[8.9] shows the map of test building made in osm using JOSM.

8.5 NFC handling

NFC is used for finding user location using the information stored on NFC tags. This information is further used by our application for navigation within building. NFC handling is demonstrated using two NFC mobiles in close proximity and check whether the data written on one can be read by other as shown in figure[8.9]. Using this application we can write location parameters on NFC tags and any NFC enabled mobile device can read and use it for navigation.

Permission[8] required for NFC element to access NFC hardware

< uses − permissionandroid : name = "android.permission.NFC" / >

8.5.1 Creating NDEF record

NdefRecord mineRecord = NdefRecord.createMime("application/vnd.com.example.android.beam", "Beam me up, Android".getBytes(Charset.forName("US-ASCII")));

8.5.2 Intent filter declaration

Tag dispatch system[8] scan all the specified intents filter, for finding whether any match exist for the intent recieved during tag discovery. If match found then application will
handle the intent.

```java
IntentFilter ndef = new IntentFilter(NfcAdapter.ACTION_NDEF_DISCOVERED);
try {
    ndef.addDataType("/**/");
} catch (MalformedMimeTypeException e) {
    throw new RuntimeException("fail", e);
}
intentFiltersArray = new IntentFilter[] {ndf, };
```

### 8.6 QR Code Handling

For reading QR code our application invokes an API, ZXing Barcode Scanner, via an intent[8]

```java
Intent intent = new Intent(getString(R.string.qr_scan_action));
```
intent.putExtra("SCAN_MODE", "QR_CODE_MODE");
startActivityForResult(intent, 0);

The returned intent is then resolved using the following code:

IntentResolver i = new IntentResolver(getApplicationContext(), intent);
if (i.getLocation() != null) {
    updateLocation(i.getLocation().getLon(), i.getLocation().getLat());
}

Figure 8.11: QR code scanner

Figure 8.12: Showing User location after QR code scanning
8.7 Software architecture

Our implementation will be a client-server based architecture, where server(OSM) holds the map of a building. In NFC enabled phones we have application which extracts the Tag-Id from RF tags and shows the exact position of user within that building. All the communication between mobile phone and server is done using XML. Server parsed the data to XML format and send it to device. In the mobile device the XML is parsed again to make a graph with nodes and edges. This graph helps to find the optimal route from source to destination using dijkstra’s algorithm. Once the path is known, it gets displayed on mobile phone using the location information of the nodes in the path.

The goal is to design an application which is simple to use and focus on making the application more usable. In order to keep the solution more useful QR code is also embedded in this system. Thus the mobile phones without NFC can also use their camera for knowing the position and navigate within the building.

8.8 Applications

1. This system finds its usefulness in large malls, buildings etc, where finding a place is a cumbersome task.

2. Tourist can use this system to visit monuments, palaces etc, and know about them by using the information written over NFC tags/QR code.

3. It is helpful for students to locate the allotted rooms during exams in examination centre.

8.9 Limitations

1. The system is not based on continuous navigation, user needs to go near NFC tags/QR code to know its location.

2. It works only for single floor, and thus does not consider elevators and stairs.

8.10 Test Results

Following are the test cases upon which this application working is checked.

1. NFC handling i.e write content on NFC tags and read by NFC reader.

2. QR code reader check.

3. Application capability to find shortest path and all paths from source to destination.

4. Application functionality of showing all the available NFC tags or QR code inside building.

5. Application functionality of showing specified nearest place from user location to destination.
Chapter 9

Conclusion & Future Work

9.1 Conclusion

This paper describes short range wireless technology NFC, which is being used widely for a range of applications, in contactless payment system, e-posters, Door-locking system and bluetooth and WiFi connection which makes it vulnerable to many attacks. Prominent among them are Relay attack, skimming and cloning attacks which may badly affects transactions and can make NFC enabled devices as a platform for attackers. Although, countermeasures for these attacks are available which helps in improving the utility of NFC devices in various applications.

This report also proposed a system for indoor navigation using NFC and QR-code which are capable of providing three necessary functionalities. Firstly, the device can find out its location inside building using the NFC tags/QR code available. Secondly, the optimal route to a destination can be determined. Thirdly, an user interface capable of providing the access all these features to user.

To determine the optimal path to the destination, the rooms and corridor were represented as graphical nodes and edges. Among other routing algorithms dijkstra’s was chosen because of its guarantee to provide optimal path and low complexity. And the user interface was developed using android software development kit and provides the user an interface to determine its location, optimal path to destination, available nfc tags in building and finding nearest places.

Device testing proves the accomplishment of these three objectives and an average deviation between user’s position and estimated position to be less than 10cm.

9.2 Future Work

The proposed system works only for single floor due to lack of support of indoor geometry in OSM maps. The system can be extended for multi-floor building so that the navigation is possible in entire building.

Apart from this, the application can be linked with location based services. So once you go near NFC tags/QR code your location will be determined and based on your location all the services available will be shown. Example:

**Local wiki**: Write Tag-ID in NFC tags along with location information, so that ID can also be read by the application and automatically send to server. Thus once unknown NFC tag is touched, an existing wiki-page is shown to user or If page is not there for that
tags ID, then the application will show a form in which page can be added.
Chapter 10

Acknowledgements

I would like to express my gratitude to Prof. D. B. Phatak, for his valuable guidance throughout the project. I would also like to thank Nagesh Karmali for his continuous monitoring of my work. I would also like to thank all those who are involved directly or directly with my work.
Bibliography


