|  |
| --- |
|  |
| LITERATURE REVIEW – CHEAPER EXCHANGE OF INFORMATION VIA WIRELESS TECHNOLOGY |
| AUTHOR: KAIRU JOSHUA WAMBUGU |
| REGISTRATION NUMBER: CS281-0720/2011 |
| DATE: Tuesday, 27 October 2015 |

|  |
| --- |
|  |

# ABSTRACT

This report contains three examples of open data applications. Information on the applications was found from desktop research online. The report comes to the conclusion that open data applications can really assist citizens increase the quality of their life. However, it is recommended that more open data sets be exposed since currently available sets do not cover many of the services ordinary citizens would want from open data.

# CONTENTS

[ACKNOWLEDGEMENTS 2](#_Toc423457319)

[CONTENTS 3](#_Toc423457320)

[ABSTRACT 4](#_Toc423457321)

[INTRODUCTION 5](#_Toc423457322)

[METHODOLOGY 5](#_Toc423457323)

[FINDINGS 5](#_Toc423457324)

[DISCUSSION 5](#_Toc423457325)

[1. The Web Service DontEat.At 6](#_Toc423457326)

[2. The Web Site FixMyStreet.com 7](#_Toc423457327)

[3. The National Pollutant Release Inventory(NPRI), Canada. 9](#_Toc423457328)

[CONCLUSIONS 13](#_Toc423457329)

[RECOMMENDATIONS 13](#_Toc423457330)

[REFERENCES 14](#_Toc423457331)

# 

# BACKGROUND/INTRODUCTION

As established in the Project Proposal, communication has developed a lot over the decades. Currently, cell phones work by creating a connection between two individual mobile phones. That connection is done by allowing the two devices to use their network service provider infrastructure. The use of that infrastructure is paid for by the users of the mobile phones.

The Project Proposal also established that smartphones have had a major impact on communication. They have become handheld computers. Computers can communicate with each other over both wired and wireless networks without use of third party infrastructure. Could the same be done between smartphones? This could be tested by seeing if two smartphones can be connected via wireless without a third party. Once this is established, one can try to send and receive data via this connection. Doing so will ensure that two smartphones will communicate with each other without incurring the costs of involving a third party – reducing the costs of information sharing among smartphones. The information the project will try to send and receive is audio information – thus simulating a phone call.

To achieve these goals, we need knowledge concerning wireless technologies, peer-to-peer implementations, and audio encoding and file formats.

This literature review tries to analyse the aforementioned items.

# LITERATURE REVIEW

This literature review will focus on the following items.

1. Three wireless technologies – NFC, Bluetooth, and WiFi;
2. Two peer-to-peer technologies – SMPP and WiFi Direct;
3. Two audio encoding techniques – AMR-NB and AMR-WB; and
4. Two audio file formats – MP3 and AAC.

# Wireless Technologies

A number of wireless technologies were mentioned in the project proposal. These were:

1. Near Field Communication(NFC) technology;
2. Wireless Fidelity (Wi-Fi) technology; and
3. Bluetooth technology.

These technologies will be considered to some detail below.

## Near Field Communication (NFC) technology

According to a programmer’s guide to Android (Deitel et al. 2012, p. 11), Near Field Communication, or NFC, is a short-range radio frequency (RF) wireless connectivity standard that enables communication between two devices. It can also be used between a device and a tag – which stores data that can be read by NFC-enabled devices. NFC operates within a range of a few centimetres. NFC-enabled gadgets can operate in three ways:

1. **Reader/writer** – such as when a device reads data from a tag;
2. **Peer to peer** – where devices exchange information without involving a third party server; and
3. **Card emulation** – where devices act like smart cards, accomplishing various smart card operations.

Currently, Android devices support reader/writer and peer-to-peer NFC modes.

According to the ISO NFC standard governing NFC protocols (ISO/IEC-18092, 2013), NFC devices can have one of the following roles in an NFC network:

1. Initiator – That is, the generator of the RF field in which NFC signals will be passed between the communicating devices. The Initiator is also the starter of NFC communication.
2. **Target** – which responds to Initiator commands either using RF generated by the Initiator through a method is called the load modulation scheme; or using modulation of an RF field generated by the Target itself.

The same ISO standard defines two modes the Initiator and Target devices can communicate with:

1. **Active communication mode** – in which both the Initiator and the Target devices use their own RF field to enable communication; and
2. **Passive communication mode** – where the Initiator generates the RF field and the Target responds to an Initiator command in a load modulation scheme.

NFC Targets and Initiators usually have an implementation of both the Active and Passive communication modes.

According to the aforementioned standard (ISO/IEC-18092, 2013), Transactions between NFC devices start with device initialization. Initiators select one of three bit rates (, , or bits) to start the transaction. Initiators may change the bit rate in the middle of the transaction using certain commands. However, communication modes – Active or Passive – cannot be changed during one transaction.

Figure 1 gives a simple illustration how NFC communication usually happens. The figure is a simple one and leaves out some details of what is involved during each step of NFC communication since a lot of smaller processes come into play during NFC setup and teardown. The following list touches just a few of these processes:

* **RF collision avoidance** – which checks to ensure an Initiator communicates with only one Target at a time.
* **The Single Device Detection (SDD) algorithm** – which is used by the Initiator to detect one out of several Targets in the Initiator’s RF field.
* **Active or Passive mode activation** – which is done using the Attribute Request and Attribute Response messages. (Both messages are called ATRs) Activation also involves the NFCID3 – a random ID used to finish the transport protocol activation process.
* **Parameter selection** – which is done using the Parameter Selection Request (PSL\_REQ) and Parameter Selection Response (PSL\_RES) commands.
* **Data Exchange Protocol selection** – which is done using the Data Exchange Protocol Request (DEP\_REQ) and the Data Exchange Protocol Response (DEP\_RES) commands.
* **Deselection and release** – which are done during device deactivation.

Figure - NFC Communication Procedures

Initiator

Target

Initialisation

Protocol Activation, Parameter Selection, and Data Exchange

De-Activation

## // todo

NFC range

According to an article in the April 2012 issue of the *International Journal of Advanced Research in Computer Science and Software Engineering* (Preethi, Sinha, & Varma 2012), NFC has a range of up to 10 centimetres. (This translates to roughly 4 inches)

NFC started which year

The NFC Forum, which champions NFC technology, was founded in 2004 but had to wait until 2006 before NFC tags came on the scene.

~ enabled devices

NFC-enabled devices include, but are not limited to, credit cards, smart posters, smart phones, and even on some computers.

Pros and cons

The following are two advantages of using NFC;

* NFC provides security since its range is quite small. Piggybacking – which, according to a Computer Science journal article (Arul Oli, 2013), is the situation where unauthorized devices can access a wireless network by virtue of being within the operating range of that network – is almost impossible with NFC. This is because NFC operates within a very small range. Intruders would have to be very close to the victim devices to access them via NFC.
* NFC helps make device use intuitive. In English, “communicate” can mean “get in touch.” NFC helps two devices communicate by getting in touch. The concept is thus instinctive and therefore easy to adapt to daily life.

The following are two disadvantages of NFC;

* The NFC technology is relatively new. It is not common. Anecdotally, relatively few people have NFC enabled smart phones in Kenya.
* NFC can only transfer small quantities of data. It does not work well with transfer of data in the millions of bytes. This is because NFC has a relatively small maximum transfer rate of 424 kilobits per second. (Preethi, Sinha, & Varma, 2012)

## Wireless Fidelity (Wi-Fi) technology.

// todo

Definition

Wireless Fidelity technology, commonly known as WiFi, is a communication technology known to many. A study on Wi-Fi (Song & Isaac, 2014) defines it as the IEEE 802.11x standard and a short-range wireless transmission technology. The study further tells that Wi-Fi is a brand held by the WiFi Alliance, whose purpose is to improve interoperability between wireless network products based on the IEEE 802.11 standard.

WiFi started

The concept of wireless access networks emerged in the late 1980s as a byproduct of cellular wireless technology. As the demand for cellulat aservice grew exponentially, the cost of wireless network components decreased, while the cost of setting up and maintaining conventional copper-based subscriber networks increased. (Skariah & Suriyakala, 2013) It was time for a wireless technogoloy to enter the communications foray. The initial Wi-Fi standard, 802.11, was released in 1997. It was improved to 802.11a in 1999. (Song & Isaac, 2014) From then on various enhancements have been introduced in the form of new standards such as IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n. The .11n standard is the most common nowadays. It operates within both the 2.4 GHz and 5 GHz frequency range with speeds of 400 to 600 Mbps. (Song & Isaac, 2014)

Range

A normal Wi-Fi access point (AP) has a range of around 20 metres indoors and 100 metres outdoors. (Song & Isaac, 2014) This large outdoor range can be extended further by the use of overlapping APs. (Banerji & Chowdhury, 2013)

Modes of operation

Wi-Fi operates within the unlicensed radio band between 2.4 and 5 GHz. All Wi-Fi networks use contention-based Half Duplex Time Division Duplex (TDD) techniques. TDD involves vying for shared media. All devices in a Wi-Fi network attempt to use shared media (the air) at specific time intervals. Because of this operation, Wi-Fi network devices can only send or receive data at one moment. Thus they are half duplex. The contention based nature of WiFi can cause subscriber devices far from an APto be repeatedly interrupted by closer devices. This makes services such as Voice over Internet Protocol (VoIP) or Internet Protocol Televsion (IPTV) – which depend on an essential constant Quality of Service(QoS) – difficult to maintain for more than a few devices. (Skariah & Suriyakala, 2013)

To reduce thelimitations imposed by half duplex communication, the 802.11n WiFi standard – a common Wi-FI standard – optimizes technology found in the physical and MAC layers of the Open Sysyems Interconnection(OSI) model. It does this by implementing features such as Multiple Input Multiple Output (MIMO) and MIMO-Orthogonal Frequency Division Multiplexing (MIMO-OFDM), 40 MHz channels, and short guard intervals. These combined otpimizations result in enhanced throughput of up to 600 MHz for Wi-Fi-based wireless local area networks(WLANs). (Song & Isaac, 2014)

Wi-Fi uses either Direct Sequence Spread Spectrum (DSSS) or Orthogonal Frequency Division Multiplexing (OFDM) to manage the channels allocated to it in the radio band it uses. (Skariah & Suriyakala, 2013) OFDM is the more favoured of the channel management technogolies. This is because it offeres high-speed transmission rates. OFDM takes a given frequenct domain and divides it into pthergonal sub-channels. Each sub-channel uses a sub-carrier to modulate singals, and each sub-carrier performs transmission parallel to other sub-channels. (Song & Isaac, 2014)

Speaking of channels, Wi-Fi standards define a fixed channel bandwidth of 25 MHz for 802.11b and 20 MHz for either 802.11a or g.

Skariah and Suriyakala, (Skariah & Suriyakala, 2013), say that modulation of bit streams across WiFi networks is done using some of the following metgods:

* Quadrature Phase Shift Keying. (QPSK) This is used mostly in the 802.11b standard.
* Binary Phase Shift Keying (BPSK), used by 802.11a and g.
* Quadrature Amplitude Modulation (QAM), which comes in two flavours – 16-QAM and 64-QAM – and is used by 802.11a and g.

Wi-Fi operates by having an access point (AP, also known as a hotspot) which emits Wi-Fi signals. Devices desiring to connect to a Wi-Fi network send their requests to that network’s AP. A series of handshakes takes place which mostly involve authentication. Finally, the connecting device is issued with data that will enable it to connect to the said AP.

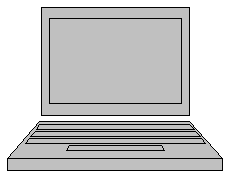
Figure 3 shows a simple example of how Wi-Fi networks can be deployed.

Table 1 shows how the five Wi-Fi standards mentioned so far – 802.11, 802.11a, 802.11b, 802.11g, and 802.11n – compare.

Enalbed devices

Various studies ( (Song & Isaac, 2014), (Skariah & Suriyakala, 2013), and (Banerji & Chowdhury, 2013) ), have found that Wi-Fi can is present in devices such as personal computers, video game consoles, smart phones, tablets, printewrs, PDAs, and routers.

Figure 3 - A simple Wi-Fi deployment



Internet



AP

|  |  |  |  |
| --- | --- | --- | --- |
| **IEEE Standard** | **Maximum Speed (Megabytes per second)** | **Frequency (GigaHertz)** | **Backward Compatible with** |
| 802.11 | 2 | 2.4 | – |
| 802.11a | 54 | 5 | – |
| 802.11b | 11 | 2.4 | – |
| 802.11g | 54 | 2.4 | 802.11b |
| 802.11n | 600 | 2.4 and 5 | 802.11a/b/g |

Table - Comparing 802.11 standards

Pros and cons

Some advantages of Wi-Fi are:

* It has the longest range of the four common wireless networks referred to here.
* Wi-Fi is a feature in almost all smart phones.

Some disadvantages of Wi-Fi are:

* Wi-Fi is inherently insecure. Because of its huge operation range, piggybacking is very possible – and piggybacking could lead to data sniffing. This could result in a breach in security.
* Wi-Fi has the highest power draw of the mentioned technologies. Some estimate Wi-Fi to use as much as 40 times more power than Bluetooth.

# Bluetooth technology

// todo

Definition

A study of Bluetooth (Singh, Sharma, & Agrawal, 2011) defined Bluetooth as a wireless communication protocol aimed at low-powered, short range applications. It was initially developed by Ericsson but is now governed by the Bluetooth Special Interest Group (SIG). Initially, it was proposed as a technology to replace cables among computer components – think of a computer’s monitor, motherboard, mouse, and keyboard working seamlessly without having to be connected via physical cabling. Bluetooth has grown past that goal – in part due to its low power consumption and potential low cost.

History

The Bluetooth we know today started in Scandinavia around 1996 when a certain Jim Kardach developed a system to allow mobile phones to communicate with computers. The name Bluetooth is based on the tenth-century Scandinavian king known in English as Harald Bluetooth. He united the whole of Denmark, achieving with the Danes what Kardach and his colleagues intended to with computers and cell phones.

According to a survey on Bluetooth security, (Ibn Minar and Tarique, 2012), Bluetooth was officially approved in the summer of 1999. Since then, the Bluetooth SIG has grown to have over 14,00 members, including some leading companies in telecommunications, computing, automotive, music, industrial automation, and network industries.

The same survey noted that Bluetooth is a combination of both hardware and software. On the one hand, the hardware is placed on a radio chip. On the other hand, the main control and security protocols have been implemented as software.

Range

Bluetooth has a range of up to around 30 metres.

Enabled devices

The previously mentioned Bluetooth study and Bluetooth security survey – (Ibn Minar and Tarique, 2012) and (Singh, Sharma, and Agrawal, 2011) respectively – mention the following as some of the gadgets in which Bluetooth technology has been implemented: mobile phones, game controllers, Personal Digital Assistants(PDAs), personal computers, laptops, keyboards, mice, printers, scanners, notebooks, palmtops, cameras, and DVD players.

Modes of operation

Figure - Bluetooth Protocol Stack

Bluetooth host security protocols

Applications

OBEX

TCP/IP

AT Commands

RFCOMM

TCS

SDP

L2CAP

HCI

LM

Baseband

Audio

Bluetooth Radio

Application specific security protocols

Security protocols on Bluetooth hardware chip

Software

Hardware

As per the previously mentioned Bluetooth security article, Bluetooth support involves both hardware and software. The hardware rides on a radio chip while software is used to implement control and security protocols. Using both hardware and software makes Bluetooth quite flexible. Over the next few paragraphs we will consider the hardware and software parts of Bluetooth.

Figure 2 shows the Bluetooth protocol stack. A protocol stack, according to the Bluetooth security study , is a combination of software and hardware implementations of the actual protocols defined in a standard as well as a definition of how devices using a certain standard should communicate with each other based on the said standard. Figure 2 has some protocols above and below a comparatively thicker line labelled HCI. HCI stands for the Host Controller Interface. All protocols above the HCI line are included in the host’s device software package. All protocols below the HCI are built into the Bluetooth microchip. The next few bullets discuss the Bluetooth protocol stack from the bottom up. They also define the abbreviations used in the figure.

* **Bluetooth radio.** It transmits data in the form of bits by using a RF. This functionality is defined in the radio layer. Bluetooth radio systems generally use the Gaussian Frequency Shift Keying (GFSK) technique to transmit and receive RFs.
* **Baseband.**  This layer does frequency hopping for interference mitigation, medium access control, and data packetformation. In addition, the Baseband layer also control link, channel, and error correction and flow control.
* **Link Manager(LM).** This layer acts as a go-between for the application and the link controller in the local Bluetooth device. Remember, the Baseband layer does link control.
* **Audio.** The audio layer is almost on the same level with the LM layer. However, Audio is separated from LM so as to avoid the overhead of upper layer protocols. This is important since the Audio layer hosts protocols used to provide real time two way voice communication. The separation of Audio from LM ensures voice communication does to experience lag due to LM protocols.
* **Logical Link Control and Adaptation Protocol(L2CAP).** This protocol is on a layer of its own. It normally resides on the host. L2CAP acts as a conduit for data on the connection link between the Baseband and host applications. L2CAP is used to ensure both connection-oriented and connection-less services. This protocol also initiates security services for any Bluetooth communication session.
* **Radio Frequency COMMunication(RFCOMM).** This is a transport protocol that is used to emulate RS-232 serial ports. It enables Bluetooth devices to connect with external gadgets such as printers and scanners.
* **Telephony Control Specification(TCS).** This protocol defines the call control signalling needed for the establishment and/or release of speech and data calls between Bluetooth devices. It also proved functionality for exchanging signalling information that is not related to ongoing calls.
* **Service Discovery Protocol(SDP).** This protocol is essential since it discovers the Bluetooth services available within the RF proximity and determines the characteristics of the available services. SDP is what allows Bluetooth devices to form ad-hoc, or peer-to-peer, networks.
* **Object EXchange Protocol(OBEX).** OBEX is used to exchange objects between Bluetooth devices. These objects include calendar notes, business cards, and data files. The exchange is done based on a client-server model.
* **Transport Control Protocol/Internet Protocol(TCP/IP).** This well-known protocol provides a reliablestream of data to Bluetooth applications from the RFCOMM layer.
* **ATtention(AT) commands.** These are not protocols as such but are a set of commands used in general telecommunications to produce commands for management of communication sessions.
* **Applications.** These are the Bluetooth applications used by end users.

Data from a sending Bluetooth device traverses the protocol stack from top to bottom – changing from intelligible information to bits. At the receiver’s end, the data traverses the protocol stack from bottom to top – changing from ones and zeros to data the end user can understand.

Bluetooth operates within the Industrial, Scientific, and Medical (ISM) RF band. This section of the electromagnetic spectrum ranges from 2,400 to 2,483.5 MHz and is divided into 79 channels, each with a bandwidth of 1 MHz. Since the ISM band is also home to other technologies such as microwaves and Wi-Fi, it is possible that Bluetooth communication may get some interference. To avoid this, Bluetooth interfaces employ frequency hopping every few seconds. This ensures that if one channel among the 79 has interference, data can be re-sent via another channel that will likely not have interference. Bluetooth uses a hopping rate of 1600 hops per second. Its developers decided to use the Frequency Hopping Spread Spectrum (FHSS) channel management technique where sender and receiver are synchronized to know which channels they will be hopping to at any given moment during their communication. FHSS leads to efficient channel use and is not affected by the distance between sender and receiver. This is unlike the other common channel management method: the Direct Sequence Spread Spectrum (DSSS) technique.

Bluetooth usually operates on a ‘master-slave’ concept. The master device works as the moderator during communication between itself and the slave as well as among slaves themselves. For devices to connect to each other, Bluetooth demands that the two share secret codes referred to as PINs. Successful PIN exchange leads to two devices being connected over Bluetooth – a process referred to as ‘pairing.’

Pros and cons

Here are two advantages of using Bluetooth:

* Bluetooth is quite flexible since it operates on both the hardware and the software level. As mentioned earlier, Bluetooth rides on a radio chip and has its control and security implemented in code.
* Bluetooth is quite common in smart phones within Kenya.

Bluetooth has some disadvantages. These include, but are not restricted to:

* The technology having a rather small range of operation. While common Bluetooth covers a larger distance than, say, NFC, it is not an ideal solution for wireless communication over 30 metres.
* Security issues since it is vulnerable to sniffing and information leaks.

Because of its proliferation and my familiarity with it, I have chosen Wi-Fi to be the technology I will implement my project with.

# Peer-To-Peer Technologies

Two peer-to-peer (P2P) technologies will be considered:

1. Short Meessage Peer to Peer (SMPP) protol; and
2. Wi-Fi Direct.

## Short Message Peer to Peer (SMPP) protocol

intro

SMPP is a Sohrt Message Service (SMS) protocol that is used to send messages over a TCP/IP connection. It is an open, industry standard protocol designed to offer a flexible data communication interface for the transfer of SMS data between a Message Centre (which acts as a store for SMSes) and a SMS application sysrem(such as a system that sends bulk SMSes to subscrivers). Examples of SMS application systems include External Short Mesaage Entities(ESMEs), Reouting Entities(REs), and Message Centres (MEs). As mentioned earlier, SMPP tranmits messages TCP/IP. The IP link used for this can either be a leased line or the Internet. Smpp has no secuirt measures specified, and this allows fast delivery of bulk SMSes. (Samanta, Mohandas, & Pais, 2012) However, this is one of its majpr drawbacks – and will be discussed a bit later.

Note: an ESME in this context of this letter refers to external sources and sinks of short messages. Such sources and sinks include Voice Proxessing Systyems, Wireless Application Protocol (WAP) Proxy Servers, or Message Handling computers. In this document, ESME excludes Short Message Entities (SMEs) – which are located within the mobile network. An example of an SME is a Mobile Statyion (MS), commonly known as a mobile phone.

SMS first appeared in Europe in 1992. It was included in Global System for Mobile (GSM) communications right from GSM’s beginning. SMS was later ported to wireless technologies such as Code Division Multiple Access(CDMA) and Time Division Multiple Access(TDMA). A standard SMS message should be a mazimum 160 characters long if each character has 7 bits ( which is suitable for encoding Latin characters such as English aphlabets); or a maximum 70 characters long if each character has 16 bits(suitable for encoding Unicode Univerdsal Character Set (UCS) 2 characters such as Chinese characters). (Samanta, Mohandas, & Pais, 2012)

Mode of op

SMS based services have proliferated in the past few years. These services include mobile banking, delivery services, airtime status checks, and mobile ticketing. Let us take an example of a SMS sent by a user enquiring after the status of their airtime balance. The user sends a message to 144.

1. User SMS: “Balance”

The SMS leaves from the MS via the GSM network to the SMS Center (SMSC). The SMSC serves as the point at which all SMSes sent in a mobile network arrive for processing. The SMSC sends SMSes using the “sotre nad forward” mechanism which involves receiving a message, storing it for some time while determining its intended recepeient, then forwarding the message to the identified recepeitn. The SMS Centere forwards the SMS to the ESME with the destination unique number “144”. At the ESME that has number “144”, the message is parsed and checked for a matching query and a response is found. This response is forwarded to the user’s MS using the path ESME to SMSC to MS. The user now knows their airtime balance. (Samanta, Mohandas, & Pais, 2012) But where is SMPP involved in this?

As mentioned in the outset, SMPP is what is used when an ESME wants to interact with the SMSC. To make ushc communication happen, an ESME first establishes a session then communication between ESME and SMSC is done over this session. This communication is performed usually over a TCP/IP or an X.25 connection. For TCP/IP, application port 2775 is the default port assigned for SMPP. (Samanta, Mohandas, & Pais, 2012)

Operations over SMPP can be categorized into four groups:

1. **Session Management:**  These operations assist in the setting up of an SMPP session between an ESME and the SMSC. Operations here also provide error handling functionalities.
2. **Message Submission:** This setr of operations allows an ESME to submit messages to the SMSC.
3. **Message Delivery:** This set of operations allows the SMSC to submit messages to an ESME. They do the inverse of the Message Submission operations.
4. **Ancillary Operations:** The operations provide a set of additional features such as cancellation queries or message replacements. (Samanta, Mohandas, & Pais, 2012)

ESMEs and SMSCs interact with each other by exchanging commands. Some of the important commands the two entities exchange with each other are:

1. *bind*. The purpose of this operation is to register an instance of an ESME with the SMSC system and request an SMPP session with the SMSC over a specified metwork connection. A secceasful bind operation allows the requesting ESME to submit messages to the SMSC and the SMSC to deliver messages to the requesting ESME. (Samanta, Mohandas, & Pais, 2012)
2. *submit­\_sm*. This operation is only used by an ESME to submit a short message to the SMSC for onward transmission to a specified SME. (SMSForum, 2002) In other words, this operation is used to transfer messages from ESME to SMSC to MS. It is most likely the operation used to transmit the user’s balance to his/her phone in the example mentioned at the outset.
3. *deliver\_sm*. This operation is used when an ESME wants to send message data to the SMSC. (Samanta, Mohandas, & Pais, 2012)
4. *data\_sm*. This operation is used to transfer data between a SMSC and an ESME. The ESME may use this operation to transfer a message to a MS. The SMSC may use this ioperatiion to transfer a MS-originated messafe to an ESME. The *data\_sm* operation is an alternative to the *submit\_sm* and *deliver\_sm* operations. (SMSForum, 2002)

figure 5, gotten froma study of SMPP secuirt flaws (Samanta, Mohandas, & Pais, 2012) illustrates how SMPP messages flow.

SMSC

MS

*SMPP*

*Wireless Network Protocol*

ESME

*bind\_tranmsitter*

*bind\_tranmsitter\_response*

*bind\_receiver*

*bind\_receiver\_response*

*submit\_sm*

*submit\_sm\_response*

*deliver\_sm*

*deliver\_sm\_response*

*submit\_sm*

*submit\_sm\_response*

Network Delivery Attempt

Acknowlegdement

Network Delivery Attempt

Acknowlegdement

Network Delivery Attempt

Acknowlegdement

*submit\_sm*

*submit \_sm\_response*

## Wi-Fi Direct

# Audio Encoding Techniques

# Audio File Formats

# RESEARCH METHODS AND DESIGN

At least three methods of research will be used in this project:

1. **Experimentation** – which will be used to test whether the project’s implementation will work on actual devices;
2. **Web Search** – where various websites will be visited to get solutions to project problems as well as get inspiration to work around implementation issues; and
3. **Interviews** – These will be done in an informal setting to acquire opinions from potential end users concerning User Interface, possible limitations, and other useful pieces of information.

A couple of the expected inputs to these research methods include:

1. For experimentation; smart phones and relevant code.
2. For web search; an internet enabled device and questions to search answers to.
3. For interviews; preparation of interview questions.

Some of the tools expected to be used in these research methods are:

1. For experimentation; smart phones, Universal Serial Bus (USB) cables, the Android Studio Integrated Development Environment (IDE), and a computer.
2. For web search; an internet enabled device and a web browser.
3. For interviews; a notebook and a pen to record interviewee responses.

The following are a number of the expected outputs from the above-mentioned research methods:

1. For experimentation; warnings, errors, and a working implementation of the project.
2. For web search; answers to the questions searched for – hopefully including snippets of code implementing those answers.
3. For interviews; various varying opinions on questions asked to interviewees.

# SCHEDULE

Below is a schedule that will serve as a guide towards the successful completion of this project.

|  |  |
| --- | --- |
| **Time** | **Proposed Activities** |
| Week starting Monday, September 14, 2015 to week starting Monday, October 26, 2015. | * Prepare the project proposal – both draft and final. * Learn to use LaTex. * Do a dummy implementation. |
| Week starting Monday, November 2, 2015 to week starting Monday, December 14, 2015. | * Come up with a detailed literature review. * Get a deeper understanding of the Android Open Source Project (AOSP)’s implementation of the Access Point Application Programming Interface (API). |
| Week starting Monday, December 21, 2015 to week starting Monday, January 11, 2016. | * Come up with designs for the application’s User Interface (UI). * Design the application’s database. * Create dummy UIs to get a feel of how the application’s UI will work. * Come up with interfaces between the UI and the application’s database. |
| Week starting Monday, January 18, 2016 to week starting Monday, February 15, 2016. | * Do a complete implementation of the project in Android. * Perform unit and system tests on the implementation. * Attempt to run the application on as many devices as possible. |

# BUDGET

I roughly estimate that I will need the following resources to achieve the desired objectives of this project:

* **10 GB worth of Safaricom data bundles.** The bundles will be used to access relevant information in the Internet.As of Sunday, 25 October 2015, Safaricom sells 3 GB worth of data for 30 days at Kshs. 1,000. 10 GB worth of data will call for the purchase of at least four sets of the 3 GB offer, resulting in 12 GB worth of data. Four sets of 3 GB bundles will cost Kshs. 4,000.

As of Sunday, 25 October 2015, the estimated amount needed for this project is Kshs. 4,000.

# OTHER INFORMATION

As of Sunday, 25 October 2015 there is no information to put in this section.

# CONCLUSION

The proposal presented above is a light one. It serves as an introduction to what this project aims to do. It is hoped that this proposal will act as a guide during the next few months and will assist in the conversion of the project idea to an actual software system.

# References

Arul Oli, V. C. (2013). Wireless Fidelity Real Time Security System. *International Journal of Computer Science Trends and Technology* *, 1* (1), 43-50.

Beck, J., & Grajeda, T. (2008). *Lowering the Boom: Critical Studies in Film Sound.* Illinois: University of Illinois Press.

Deitel, P., Deitel, H., Deitel, A., & Morgano, M. (2012). *Android for Programmers An App-Driven Approach.* Indiana: Pearsion Education, Inc.

Ibn Minar, N. B., & Tarique, M. (2012). Bluetooth Security Threats ans Solutions: A Survey. *International Journal of Distributed and Parallel Systems (IJDPS)* *, 3* (1), 127-148.

Preethi, K., A, S., & Varma, N. (2012). Contactless Communication through Near Field Communication. *International Journal of Advanced Research in Computer Science and Software Engineering* , 158-163.

Preethi, K., Sinha, A., & Varma, N. (2012, April 4). Contactless Communication through Near Field Communication. *International Journal of Advanced Research in Computer Science and Software Engineering* , 158-163.

Singh, P., Sharma, D., & Agrawal, S. (2011). A Modern Study of Bluetooth Wireless Technology. *International Journal of Computer Science, Engineering and Information Technology* *, 1* (3), 55-63.

Skariah, M., & Suriyakala, C. D. (2013). An Exploration on Wi-Fi/802.11b and WiMAX/802.16 Networks with Performance Enhancements. *International Journal of Engineering Sciences & Research Technology* *, 2* (12), 3658-3664.

Song, S., & Isaac, B. (2014). Analysis of Wi-Fi and WIMAX and Wireless Network Coexistence. *International Journal of Computer Networks & Communications (IJCNC)* *, 6* (6), 63-78.

Bluetooth Security Threats and Solutions: A Survey

# pay