DEVELOPMENT OF MULTIPLE OPERATOR ENABLED SIM CARD

Research · August 2021

DOI: 10.13140/RG.2.2.18098.94403

1 author:

Ibrahim Tijani
Federal University of Technology Minna

COVER PAGE

DEVELOPMENT OF MULTIPLE OPERATOR ENABLED

SIM CARD

BY

TIJANI, IBRAHIM ADEWALE

2012/1/42541CT

DEPARTMENT OF COMPUTER SCIENCE

FEDERAL UNIVERSITY OF TECHNOLOGY

MINNA

OCTOBER, 2017

TITLE PAGE

DEVELOPMENT OF MULTIPLE OPERATOR ENABLED SIM CARD

BY

TIJANI, IBRAHIM ADEWALE

2012/1/42541CT

PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE,

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY, FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, NIGERIA IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE

OCTOBER, 2017

DECLARATION

I hereby declare that this project titled: Development of Multiple Operator-Enabled SIM Card is a collection of my original project work and it has not been presented for any other qualification anywhere. Information from other sources (published or unpublished) has been duly acknowledged.

TIJANI, Ibrahim Adewale
2012/1/42541CT
Federal University of Technology,
Minna, Nigeria.

Signature and Date

CERTIFICATION

The project titled: Development of Multiple Operator-Enabled SIM Card by: TIJANI, Ibrahim Adewale, 2012/1/42541CT, meets the regulations governing the award of the degree of Bachelor of Technology of the Federal University of Technology, Minna and it is approved for its contribution to scientific knowledge and literary presentation.

Your Supervisor's Name	
Project Supervisor	Signature and Date
Dr. John K. Alhassan	
Head of Department	Signature and Date
External Examiner	Signature and Date

ACKNOWLEDGEMENTS

ABSTRACT

Abstract is a one paragraph summary of the whole study containing a brief introduction of the subject area, aim, methods used, data analysis, your results or/and findings, and conclusions drawn. It should not be more than 120 – 200 words. It must be single-spaced, and must not be italicized.

Introduction. Statement of the problem. Methodology, Results and recommendations

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF STUDY

The history of modern telecommunication could be dated to the discovery of the first working telegraph which was invented by Francis Ronalds in 1816 using static electricity (Ronalds, 2016). In 1860's the telegraph was used to communicate across the United States and was used during the Civil Wars. This made it the first communication device to send messages through signals almost simultaneously(MobileMarketting.am, 2017). The telegraph closed the gap of time and distance which older forms of communication could not overcome. Although this was a great achievement for the world, the telegraph still had great shortcomings. One of these shortcomings was the need for a means of sending the signal (generating and storing electricity) and receiving the signal (recording the breaks in the current). Another problem was that of mistransmission, where messages become garbled and meaningless(Tomas, 2001).

By the end 1800s, talk about a telegraph that can transmit voice began to spread and many inventions were springing up to achieve this new milestone in telecommunication. In 1876, Scottish emigrant Alexander Graham Bell was the first to be granted a United States patent for a device that produced clearly intelligible replication of the human voice (Grosvenor, Edwin, & Morgan, 1997) making them the first persons to make a successful voice call through the telephone lines. The main components of a telephone were the transmitter which a caller speaks into and a receiver for reproducing the voice in a distant location. Most telephones contain a ringer for producing sound to announce an incoming telephone call, and a dial or keypad used to enter a telephone number when initiating a call to another telephone. Until the 1970s most telephones used a rotary dial, but later in 1963 AT & T introduced the DTMF push button-dial which superseded the rotary dial. The first telephones were directly connected to each other from one customer's office or residence to another customer's location. This gave rise to landline telephone service in which each telephone is connected by a pair of dedicated wires to a local central office switching system, which developed into fully automated systems starting in the early 1900s. For greater mobility, various radio systems were developed for transmission between mobile stations on ships and automobiles in the middle 20th century. Hand-held mobile phones were introduced for personal service starting in 1973. By the late 1970s several mobile telephone networks operated around the world. In 1983, the Advanced Mobile Phone System (AMPS) was launched, offering a standardized technology providing portability for users far beyond the personal residence or office. These analog cellular systems evolved into digital networks with better security, greater capacity, better regional coverage, and lower cost. Every telephone line has specific identifying telephone number that can be called from another telephone on the network. This was possible due to the standardized international numbering system (Wikipedia, 2017b).

With the evolution of the first generation cellular analog system to second generation digital networks many systems were proposed. Most of these systems set standards that were incompatible with one another. In 1983, the European Conference of Postal and

Telecommunications Administrations (CEPT) set up the Groupe Spécial Mobile (GSM) committee with the aim of proposing a common standard for European digital cellular voice telecommunications. The first official specification for GSM was produced in 1987. By 1993, the GSM became operational in the UK with Telecom Australia becoming the first network operator to deploy a GSM network outside Europe and the first practical hand-held GSM mobile phone became available. The GSM was accepted globally with many countries switching from analog to the GSM digital technology and its users increased to millions. The GSM was not quickly accepted in Nigeria until August 2001 when it was first launched to initiate the country into the global village and since then its users have increased rapidly. According to the Nigerian Telecommunication Services Sector Report, by March of 2016, the total number of GSM subscribers was 147,398,854, an increase of 5,756,018 or 4.06% relative to March 2015.

In 1995, the European Telecommunication Standard Institute (ETSI) proposed the GSM TS.11.11 with the SIM card specification. The SIM which is a special smart card that works in the GSM network most importantly in the identification and authentication of mobile network subscriber. This is done through the profile information such as international mobile subscriber identity (IMSI), integrated circuit card identifier (ICCD) and the Authentication key (Ki) which is stored on the SIM memory(Wikipedia, 2017a). The SIM serves as data storage for storing user information such as phone contacts, messages etc. In 1991 when the SIM card was developed, it was as large as the size of a credit card. But today, there are various sizes for the SIM card ranging from the credit card size to a very small Nano SIM(Aibinu, Onumanyi, Folorunso, Ipinyomi, & Adda, 2016).

Historically, developing SIM cards was rigid and monolithic (Deville, Galland, Grimaud, & Jean, 2003) and was mainly done by commercial (operators, smart card manufacturers and specialized consultant firms) based on proprietary hardware and software solution. The smart card technology is based on standards that are created and maintained primarily by international standard organization (ISO), International Engineering consortium (IEC) in cooperation with ISO, European Telecommunication Standard Organization (ETSI), third Generation Partnership Project(3GPP) in cooperation with ETSI and Global Platform group (ETSI,2001). Development of SIM cards have gone through a series of evolutions. Today, there are tons of software, frameworks and libraries for programming a SIM which are gradually wiping out the native approach. These software use high level programming such as Gemalto suits for Java cards (a subset of java language), Globalplatform libraries and Pyscard (a python library for programming smart cards).

As the subscribers to GSM increased, the GSM traffic became congested and telecommunication infrastructure became inadequate and inefficient resulting in issues such as poor Quality of Service (QoS), poor received signal and call drops, Internet issues, lack of voice clarity, one-way speech, poor network availability and connectivity issues, pending and undelivered Short Message Service (SMS). Also, most infrastructure were situated in the urban areas leaving most rural areas with poor network services. Although the network provider and telecommunication company have attempted to solve these problems but to no avail. Solutions such as installing more base transceiver stations (BTS) has resulted in proliferation of the environment. Also, subscribers too have sorted to procure cell phones with multiple SIM cards or owning more cell phones.

In this project an attempt is made to solve these problems by developing a multiple-operator enabled SIM card. This allows subscribers to own a single SIM card with profiles of multiple mobile network operators on it which solves the problems of owning more than one cell or having a cell phone with multiple SIM cards. The various networks can be switched automatically during voice and data communication if there is a poor received signal. This ensures for seamless communication thereby increasing the quality of service to users.

1.2 PROBLEM STATEMENT

In recent years, the problem of poor communication in Nigeria has reached a peak due to many hindering factors such as poor received signals, call failure, poor QoS. These problems are as result of increase in the number of mobile subscribers in the country, coupled with the poor telecommunication infrastructure.

In an attempt to resolve these problems, mobile network providers have employed many temporary solutions such as installing more base transceiver stations in cities and rural areas where network signals are low. This solution has led to increase radioactive emission on the environment, thus leading to proliferation of the environment. The short-term solution of owing more than one phone by the subscriber has also not been an efficient work-around.

In the course of solving these problems many mobile subscribers sort to owning cell phones with more than one SIM card. Some also sort of owning more than one cell phone. The problem still persists with every other Network operator.

1.3 AIM AND OBJECTIVES

The aim of this project is to develop a Multiple Operator-Enabled SIM Card. This will be achieved by the following objectives.

1. To program a SIM with N-profile of Mobile Network.
2. To design the N-Mobile Network MOES system
3. To test and evaluate the performance of the developed N-Mobile Network MOES system.

1.4 SCOPE OF STUDY

The scope of this project is mainly on the development of a Multiple Operator-Enabled SIM CARD. This will be done with the use of Wi-Fi network as the GSM signal and ATR as the Ki key for each mobile Network. The handover decision and switching algorithm is not part of this project.

1.5 SIGNIFICANCE OF STUDY

The significance of this project cannot be overemphasized because it will result in many technological advancements. It will help in revitalizing the telecommunication company as the need for more base transceivers will be eradicated, consequently reducing the risk of environmental proliferation through radioactive emission. Also, the high cost of procuring telecommunication infrastructure such as Base transceiver station and SIM card production will be reduced. Therefore, there would be less need for an operator to separately purchase and distribute SIM cards. The obvious separation of device and service purchase might also result in an increase in the proportion of mobile phones sold through open distribution. These will lead to reduced costs of operator retail and distribution in many countries.

The users will enjoy many benefits since there is no need for them to have many phones nor will there be need for use of Multiple SIM card phones. The capability of switching between multiple network operators (MNO) without changing the SIM could increase SIM only retailing. This will ensure that price is the only differentiator for competition between mobile network operators leading to low cost of services to the subscribers. Therefore, MNO will have to find better means of gaining customers. The subscriber will have profound flexibility in selecting service e.g. choosing a cheaper package when changing from one geographical area to another. The problem of poor QoS will be eradicated, especially in voice communication as these projects give way to implementation of new and advanced technology such as automatic switching during calls between different networks which consequently will allow completion between mobile operators for better network service.

Finally, this project can enhance the adoption of embedded SIM and virtual SIMs especially in Machine-to-machine equipment where the physical SIM housing will be completely remove. This approach will lead to lowering of prices of mobile phones.

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

In this chapter, some of the concepts and technologies used in this project such as SIM Cards and their properties, Mobile Equipment, GSM technology and other Wireless Technology such as WLAN that was used to simulate MNO for authentication via SIM Cards were discussed. Authentication in the GSM network and how SIM Cards are programmed is considered. Lastly, a review of related works as regards Sim-based subscriber authentication for WLAN, subscriber authentication in cellular networks with trusted virtual SIMs is presented.

2.2 SIM CARD

SIM is an acronym for Subscriber Identity Module. SIM cards are special type of smart cards used for connecting to mobile network operators using the mobile telephony technology known as the Global System for Mobile Communication (GSM) (Edsbäcker, 2010). Smart cards are integrated circuit cards with a microprocessor embedded in them, therefore they are miniaturized computers themselves. They were developed mainly for storage, authentication and as a mechanism for access control, (Husemann, 2001). The first Smart card was invented in 1977 by Michel Ugon. Their use has grown to car fuel cards, financial debit and credit cards, authorization and access cards for television station, encrypted certificate or encryption key storing, physical company access, single sign-on. The first commercial SIM card was supplied to a Finnish Network operator in 1991 by Giesecke and Devrient. The SIM card was originally designed to work on the GSM network and was similar in size to a credit card.

According to ISO 7816-3, a SIM card like a computer has a microprocessor and a memory. The functions of these two are interrelated (NCC, 2016). The microprocessor's main function is to allow access to the memory. Another function of the processor is to protect access to memory through cryptographic functions. The SIM memory is of three different types namely, Non-volatile Memory (NVM), Read Only Memory (ROM) and Random Access Memory.

The GSM specification for SIM was made official in 1995. Recommendation GSM 02.17 splits the Mobile Station (MS) into a removable SIM containing network related subscriber information and Mobile Equipment which contains the remaining part of the Mobile Station to realize all the functions common to all subscribers of GSM. Therefore, the SIM performs two main functions: as a storage device for controlling the access to data and as a mechanism for executing algorithms in secure conditions. The main task of the SIM authentication of the subscriber's identity according to Recommendation GSM 02.09.

2.2.1 SIM CARD ARCHITECTURE

The physical architecture and function of the SIM are controlled by the ISO 7816 standards (Gielen, 2012). SIM cards like other smart cards have eight connecting pins. Six of which provide active usage while the remaining two are optional. These pins are: the VCC, Reset, Clock, Ground, VPP (or EEPROM in older cards), 2 optional USB2 and lastly the I/O pin as shown in Figure 1 and Figure 2. The VCC pin is used for applying working voltage, the SIM card operates on three voltages which are 1.8v, 3v or 5v. The Reset pin is used to reset and initiate the Answer-To-Reset (ATR) protocol. The clock provides a card clock signal, the clock rate ranges from 5 – 20Mhz. The VPP also called the EEPROM is used to supply the voltage required to program or to erase the internal non-volatile memory. The two optional USB pins are used for communication with USB devices and other purposes. The most important pin for communication is the I/O pin. This pin can be set high (H) or low (L), and by reading or changing the state of the pin at specific timings, bytes are transmitted serving as input or output for serial data (half-duplex) to the integrated circuit inside the card.(Edsbäcker,2010).

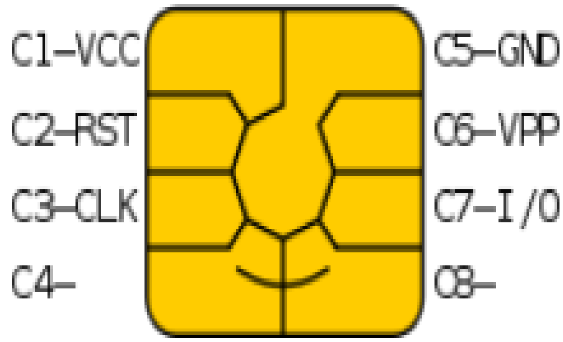


Figure 1 showing the eight connecting pins for the SIM

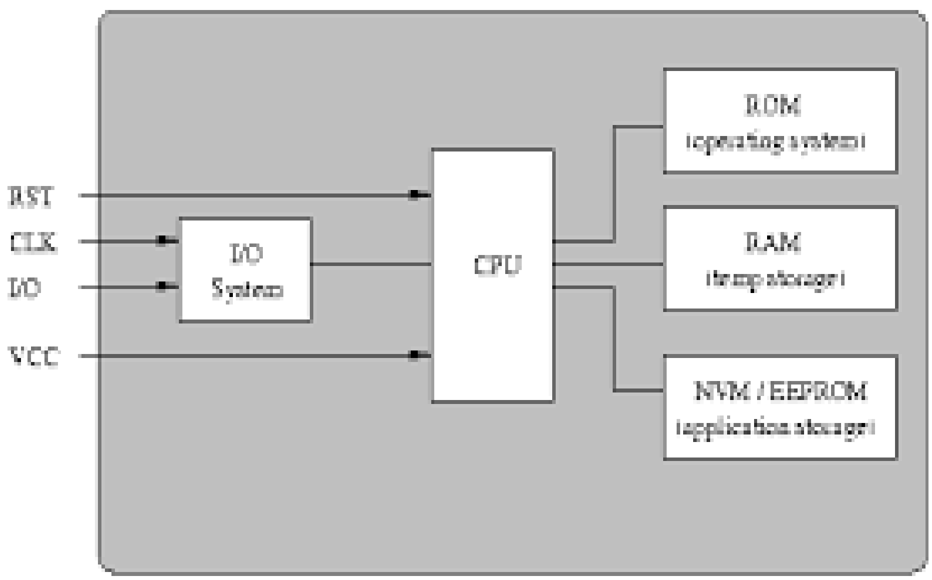


Figure 2 showing the architecture of a typical SIM

2.2.2 COMMUNICATION BETWEEN SIM AND THE MOBILE EQUIPMENT

Data communication between the SIM and the Terminal of the Mobile Equipment (ME) is done via the application protocol data unit (APDU). There are two types of APDU. They are the Command and Response APDUs. The command APDU is one sent by the ME terminal to the SIM card. The command APDU is a 4-bytes header (CLA, INS, PI and P2) which ranges from 0 bytes to 65536 bytes of data and a body.

The first field of the command APDU, the CLA field is called the class byte which has a length of 1 byte and is used to identify the type of global command issued for example it indicates whether the command is proprietary or inter-industry. The second field is the instruction code which indicates the function of the command e.g. read or write data, it also has a length of 4 bytes. The third and fourth fields are the P1 and P2 fields which indicate instruction parameters for the command e.g. offset into file at which to write the data. The body of the command APDU carries the length of data used in communication (Gielen, 2012).

On receiving command APDU the SIM responds with the response APDU. The response APDU contains only a body indicating the length of data and two status word bytes, SW1 and SW2 showing success or error in the communication. Figure 3 shows a typical communication between a SIM and ME.

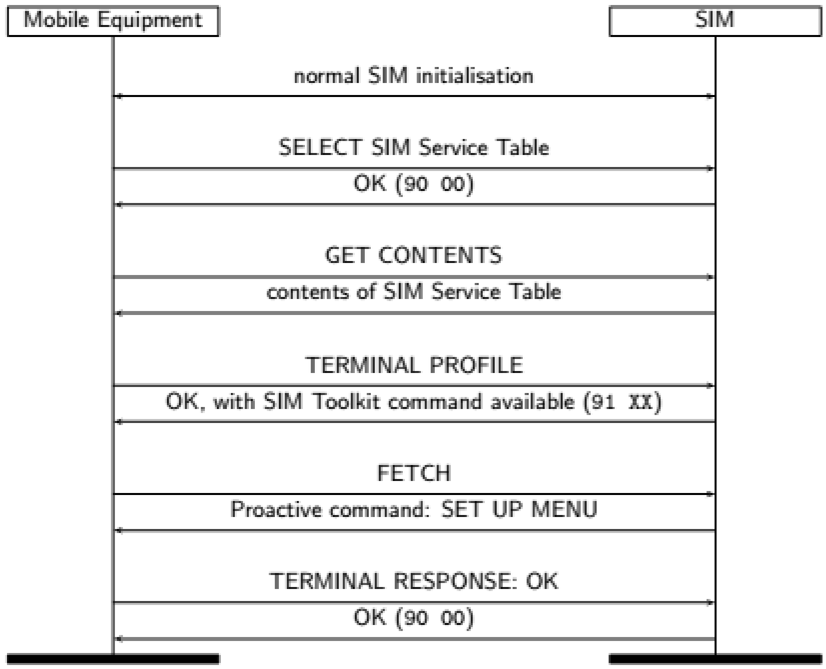


Figure 3 Typical APDU communication between SIM and ME

2.2.3 R-UIM cards

R-UIM cards contain three network applications namely GSM, SIM and USIM and can be used in all these network types. They were first released for use with CDMA2000 networks (the American 3G standard).

2.2.4 UICC cards

The Universal Integrated Circuit Card (UICC) is the smart card type which all modern SIM cards are based on. It can host all applications of section 3.2.1 and also implements Java Card. Majority of SIM cards today are based on the UICC smart card type technology. Many approaches have been used to deploy the SIM card technology. Some of these approaches are Traditional SIM card approach, Embedded Sim card and Remote Provisioning.

2.2.5 TRADITIONAL SIM CARD

Traditionally, the SIM card is a hardware that can be removed from the mobile equipment that houses it. Profiles of a network operator which has been programmed during manufacture can be stored on the SIM card. This operator profile consist of the information that helps in the identification and authentication of the mobile subscriber with the selected mobile networks. Although other profiles can exist at a time on the SIM card, only the profile of the registered network operator can be authenticated. Just like credit and debit cards, the traditional SIM card is developed on Smart Card (UICC) technology. The UICC is a physically secure computing device that can be used across multiple vertical sectors including mobile telecommunications. The UICC conforms to the specifications written and maintained by the ETSI Smart Card Platform Project.

2.2.6 EMBEDDED SIM

Some operator-locked mobile phones and Machine-to-Machine equipment that support network communication mostly have SIM cards physically integrated into them. These SIM cards cannot be removed and will remain in the device for life or until the contract between the user and operator ends.

2.2.7 REMOTE PROVISIONING

Remote Provisioning is the ability to remotely change the SIM profile on a deployed SIM without having to physically change the SIM itself. This technology can be implemented on any SIM form factor, including removable and soldered SIMs. In order to achieve this, the SIM has extra memory and is therefore capable of holding more than one operator profile (rather than only one on the traditional SIM).When a consumer purchases a service package from a specific operator, the operator profile is downloaded and saved onto the SIM memory. If a second operator package is subsequently purchased, the new operator profile is downloaded and also saved to the SIM – both operator profiles are now saved on a single SIM card and there is an ability to swap between the two installed profiles. This swap effectively mimics the actions a user would undertake when swapping the SIM card in a device.(GSMA Intelligence, 2016)

2.2.8 SOFT OR VIRTUAL SIM

According to GSM Intelligence 2016, “A Soft SIM would be a collection of software applications and data that perform all of the functionality of a SIM card but does not reside in any kind of secure data storage. Instead, it would be stored in the memory and processor of the communication device itself (i.e. there would be no SIM hardware layer)”.

As described by GSMA intelligence above, this SIM approach or technology aims to provide software-based SIM activities in such a way that all SI execution and information are made on the cell phone operating system. Although many technologies have been proposed to avail this technology, there is still speculation on the security aspect because high security will be needed to avoid tampering and duplication of data and a lot of research needs to be done to achieve such a milestone in this aspect. Many companies have started to implement this approach such as Apple Inc. and some cloud computing platforms.

2.2.9 SIM TOOLKIT APPLICATION

As discussed earlier, communication between the Sim and phone occurs using the APDU commands, this communication allows the phone to use information gotten from the SIM to connect to the required network appropriately. Although there are various types of APDU commands that can be used in communication between the SIM and the operator via the mobile phone especially in providing value added services to the subscriber. To achieve this purpose, the SIM toolkit was proposed by the ETSI in the ETSI 11.14. The standard specified a new APDU for the SIM Toolkit. The specification defines several command which include user interface commands, network and messaging commands, ME/SIM control commands, internetworking commands, timer command and commands for getting location information.(Gielen, 2012)

2.2.10 PROGRAMMING A SIM CARD

Several methods have been adopted in programming a sim card for a specific MNO. From inception SIM cards were basically developed to be used by GSM network for authentication of users with network credentials on the SIM such as the International Mobile Subscriber Identity Module (IMSI), secret key (Ki) for authentication, Ki, and ICCD.

Programming a SIM card was done natively by the MNO or the company developing the SIM card with partnership of the MNO. The programming of SIM has gradually evolved over the decade from the native method. This evolution has resulted from the popularity of high level languages which aid development of software enhancing the automation of programming process. The software include APIs, frameworks and tools which are easy to interact with even by non-programmers such as Gemalto plus IDE for Java card developer which allows programming of any smart card that supports java card, although java card can also be integrated with some other IDE such as eclipse and NetBeans. Other platforms include MOBITEL SIM TOOL KIT API (STK), PySim (a python application for Reading and writing to SIM cards) and Pyscard which is a python library for programming SIM cards.

2.3 MOBILE EQUIPMENT

Mobile Equipment (ME) are devices or hardware that are used to interface with the SIM cards. Also, it is a term used for any device that can interface or read the sim such as SIM Card reader, Mobile phone, some internet Modem etc. It is an operator independent communication device which contains the A5 algorithm. It cannot be used for GSM communication without a SIM card. It never sees the A3/8 algorithms and Ki. According to Recommendation GSM 02.17, ME consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and the SIM card. It provides the interface to the user in GSM networks. The ME also provides the receptor for SMS messages, providing capability for both voice and data use. The Figure below shows a typical example of a ME.

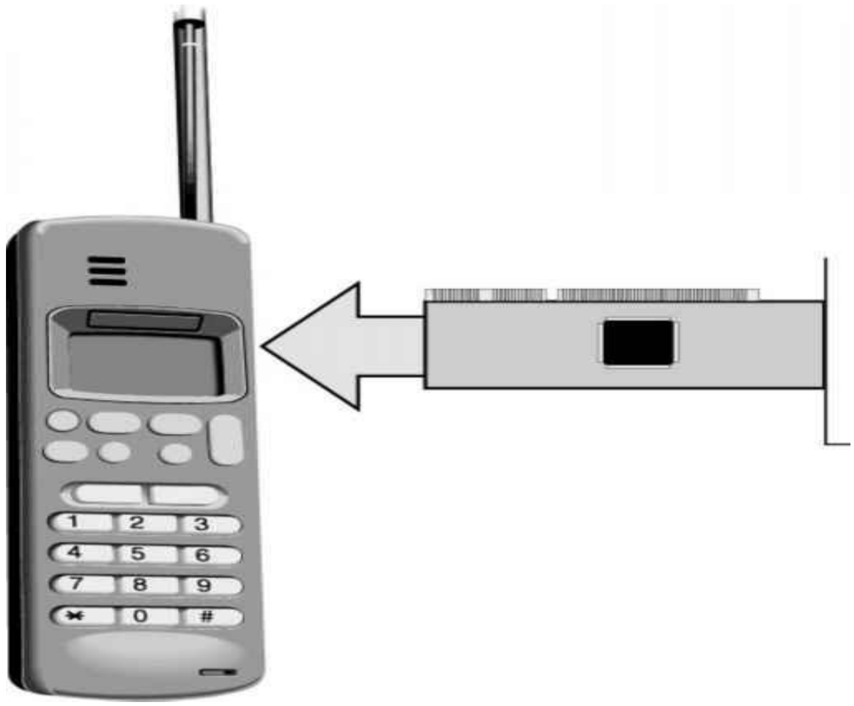


Figure 4 : A typical ME(mobile phone)

2.4 GSM

GSM is an acronym for Global System for Mobile Communication. GSM was officially announced in 1987. Then a group was set up by the European Telecommunication Standard Institute and it was named Group Special Mobile. In 1991 GSM was renamed to Global System for Mobile Communications from Group Spéciale Mobile. Although GSM was developed as a European digital communication standard to allow users to use their cellular devices seamlessly across Europe, it was later developed into a standard that would be used globally. Global System for Mobile Communications (GSM) is still the most common worldwide mobile phone standard. It uses full digital signalling in respect to its predecessors which used a mix of analogue and digital signalling and uses Time Division Multiple Access (TDMA) as a radio carrier/protocol (Rahnema, 1993).

GSM just like CDMA and D-AMPS IS-136 is part of the second generation of digital mobile phone technology. GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900MHz. It is the standard for communication for most of Asia and Europe. GSM operates on four separate frequencies: The 900MHz and 1,800MHz bands in Europe and Asia and the 850MHz and 1,900MHz (sometimes referred to as 1.9GHz) bands in North America and Latin America. GSM allows for eight simultaneous calls on the same radio frequency and uses “narrowband” TDMA, the technology that enables digital transmissions between a mobile phone and a base station. With TDMA the frequency band is divided into multiple channels which are then stacked together into a single stream, hence the term narrowband. This technology allows several callers to easily share the same channel at the same time.(Wikipedia, 2017b).

General Packet Radio Service (GPRS) added slower data bandwidth for wireless data connection data packet handling to GSM networks for consumers; it enabled things like MMS, WAP and IP. Also the new GSM EDGE technology has helped GSM speed to catch up with CDMA, although the coverage and availability of EDGE is still patchy.

The GSM, GPRS (and Edge) standards are controlled by ETSIs Smart Card Platform (SCP) committee. Promoters of these standards are the GSM Association (GSMA). The Main

Function of the GSMA is to spread GSM related technologies globally. The GSM entire architecture is divided into three subsystems: Mobile Station (MS), Base Station Subsystem (BSS) and Network Subsystem.(Aibinu et al., 2016)

2.4.1 THE MOBILE STATION

The Mobile Station (MS) consists of Mobile Equipment (ME) (e.g. mobile phone) and Subscriber Identity Module (SIM) which stores secret information like International Mobile Subscriber Identity Module (IMSI), secret key (Ki) for authentication and other user related information like certificates.

2.4.2 THE BASE STATION

The Base Station Subsystem (BSS), the radio network, controls the radio link and provides a radio interface for the rest of the network. It consists of two types of nodes: Base Station Controller (BSC) and Base Station (BS). The BS covers a specific geographical area (hexagon) which is called a cell. Each cell comprises many mobile stations. A BSC controls several base stations by managing their radio resources.

2.4.3 THE NETWORK

The BSC is connected to the Mobile Services Switching Centre (MSC) in the third part of the network NSS also called the Core Network (CN). In addition to MSC, the NSS consists of several other databases like Visitor Location Register (VLR), HLR and Gateway MSC (GMSC) which connects the GSM network to Public Switched Telephone Network (PSTN). The MSC, in cooperation with HLR and VLR, provides numerous functions including registration, authentication, location updating, handovers and call routing. The

HLR holds administrative information of subscribers registered in the GSM network with its current location. Similarly, the VLR contains only the needed administrative information of subscribers currently located/moved to its area. The Equipment Identity Register (EIR) and AuC contains a list of valid mobile equipment and subscribers' authentication information respectively.(Aibinu, Onumanyi, Folorunso, Ipinyomi, & Adda, 2016). Figure 5 summarizes the GSM architecture.

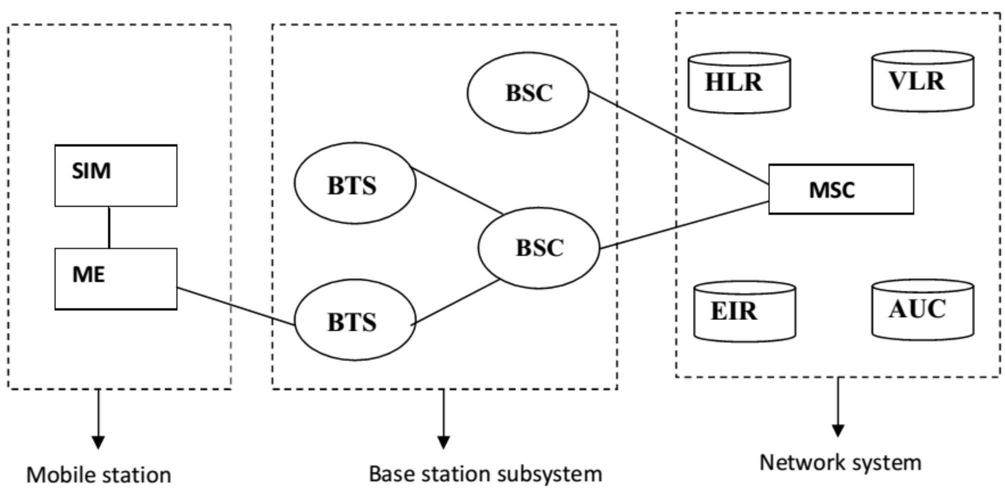


Figure 5 GSM Architecture

2.4.4 HOW AUTHENTICATION IN GSM WORKS

Authentication in a GSM network requires a SIM card containing network parameters and encryption keys at well-defined places in the file system. The file system also contains the network base applications responsible for communicating and authenticating with the operators network. Most of these parameters are defined when the SIM is manufactured because it involves root user access to the card or reside in ROM.

A Mobile Equipment (usually a phone) contacts its network. The network then contacts the home location register (HLR) for the operator in question. The HLR looks up the users account by the phone's MSISDN. The authentication key (Ki) is stored. The HLR will then generate a set of keys (based on MSISDN/IMSI and the Ki). These are sent back challenge token. The SIM card sends back its signed response to the network which verifies it with what the HLR calculated. If it is accepted the SIM generates a 64-bit session key called Kc (through the A8 algorithm). This is based on the Ki and the received challenge token. This session key is used to initialize the A5 encryption algorithm (on both sides) that is hence used during further communication. Consequently , the network verifies the ME not vice-versa, therefore, an imposter could get easily get the handset's Ki.(Aydemir & Selçuk, 2005)s

2.5 WLAN

WLAN, an acronym for wireless local area network is a network that connect two or more computers or devices within a limited geographical area such as a home, school, computer laboratory, or office building, or private work group. Only users within the local range can connect to the network. In recent years WLAN has been improved to provide a connection to the wider geographical range such as a metropolitan city.

WLANs are based on IEEE 802.11 standards which has gone through several version since its development in the 1990s. Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their customers. The W-LAN was included in the R6 release as part of the telecommunication network standard in 2004 (Wikipedia, 3GPP, 2011).

2.6 RELATED WORKS

The GSM has contributed greatly in enhancement and availability of telecommunication. Many research works have been done to improve the GSM especially in the problem of efficient handover. In 2014, Dixit and Sharma wrote a comprehensive journal on the study of handoff for enhancing communication in GSM. They explained that handoff is the mechanism for transferring ongoing calls from one cell to another. The handover needs to be done very quickly to avoid degradation of quality of service or loss of connection. Handover can be soft or hard, horizontal or vertical which can also be subdivided into intracell, intercell. The study continued by stating various reasons for handover such as avoiding call termination when moving from a cell to another, the research ends with comparing different handovers in different technologies such as GSM, CDMA, WLAN etc. (Dixit & Sharma, 2014).

Since 1995, the SIM has been a major part of the GSM without which the Mobile equipment cannot connect to GSM. In 2002, Wu, Du and Cui presented a paper on the development of a Sim card interface for general purpose. The work shows the hardware implementation, firmware implementation of a typical class A and Class B SIM. The hardware includes the power block, clock block and main block. The power uses 3.3v, the SIM clock requires 1-6Mz and the main control block is MCI14066 Motorola chip. the SIM outputs ATR at default baud rate of **f/372,** where f is the SIM clock. Consequently, The design solves the problem of power supply, initialization and data output of class A and class B SIM. This allows efficient communication with PC computers using USB (Wu, Du, & Cui, 2002).

To allow more capabilities for the SIM, the SIM application toolkit was developed. Although the SIM toolkit has enhanced the SIM greatly there are still some security risks that affect the use of SIM Toolkit. worked SIM Toolkit. He explained the various SIM Toolkit activities such as SIM Toolkit installation which involve running the SETUP MENU command, the Menu selection by the user where the Mobile Equipment will send ENVELOPE APDU to the SIM. Furthermore, SIM security tests were carried out on the SIM using the SIM tool. The Man-in-the-middle attack was carried out using eavesdropping tools such as the RebelSIM, SIMparser.pl, a perl script, SmartLogic Tool. Some SIM toolkit capabilities were shown such as User communication which involves displaying text, setting up menu, and item selection, Network communication which involves getting local information, sending short messages, setting up calls and controlling calls (Gielen ,2012).

SIM cards have been used in many applications. Tsai and Chand in 2006 worked on SIM-based Subscriber Authentication for wireless local area networks (WLAN). They implemented a system using SIM-based subscriber authentication for the WLAN environment. The system consists of three parts. The SIM Authentication Information Access Part, the Authentication information exchange and verification protocol and the GSM-MAP interface. This system has an advantage of integrating authentication mechanism of WLAN into that of GSM/GPRS network.(Tsai & Chang, 2006)

Aibinu et al., 2016 investigated on developing a system for Executed Handover of Mobile-Phone using Embedded-Multiple Operator Enabled SIM Card. The developed system acquires network parameters using an open source embedded system platform as the first stage in wireless mobile communication Handover process. The second stage involves network scanning for Handover decisions while the third stage executes the decision of the previous stage. Practical realization of these stages is achieved by the use of a five-section embedded platform, namely: The Transceiver Unit, the Micro-controller Unit, the Network Scanning Unit, Display Unit, and the Power Supply Unit. The EMOES system developed in this work uses efficient vertical-horizontal handover i.e. handover between multiple operator networks. The system ensures Seamless transfer and continuation of ongoing active sessions from one MNO to another.

Results obtained shows that the developed EMOES system is able to initiate Handover and take Handover decisions appropriately. This research will enhance quality of services of the network because users will have the ability of switching between multiple network seamlessly during voice and data communication although the use of multiple SIM ICs in the transceiver unit for each network will result to need for more power supplier from the Power supply unit.(Aibinu, Onumanyi, Folorunso, Ipinyomi, & Adda, 2016)

Aibinu et al (2016) in a research funded by the Nigerian Communication Commission (NCC) work on the development of a SIM reader and Analyser software that can read multiple SIM cards using open source hardware. The SIM card reader and analyser developed in this work has two units, a hardware unit and a software unit. The hardware unit is implemented using open source Arduino Uno board and a GSM shield that has SIM 900 integrated in it. The software unit was implemented using java fxml (a java GUI library). The hardware unit can be subdivided into the following components: The Power Supply Unit (PSU) which supplies power to the other components. The Microcontroller Unit (TMU), the SIM900A GSM Shield, Multiple-SIM Cards Driver Unit. The software reader has the following features: Automatic Connect and Disconnect feature, Send button to send command query to SIM card, an area to display information gotten from SIM query, a SIM and network information tab, capability for saving acquired information, Sim and network query parameter selection and lastly, Single and multiple sim card reading capability.

Some tests involving SIM card forensic and analysis were carried out using the developed embedded system and results were obtained from the use of the developed embedded system on three different SIM cards obtained from three different network operators in Nigeria.

The SIM reader and analyser compared to other non-open source software can read information from multiple SIM cards and can also get network details such as received signal strength and quality, and so on. This work is very useful in SIM card forensic and also in analysing different SIMs based on GSM network.(NCC, 2016)

Kasper, Kuntze and Schmidt (2008) proposes several virtual SIM (vSIM) models for authentication and enrolment of a subscriber using the Mobile Trusted Platform (MTP). The use of vSIMs pose a severe security vulnerability since software can be easily accessed compared to hardware SIMs. The research shows that use of (mobile) trust credentials in user centric scenarios by vSIM credentials or the support of online transactions are thinkable approaches. The research allows vSIM Credentials as a means for subscriber authentication since it uses Mobile Phone Work Group of the Trusted

Computing Group (TCG MPWG) technology. The TCG MPWG proposed an architecture with a high level of abstraction for trusted mobile platforms.

CHAPTER THREE

METHODOLOGY

3.1 OVERVIEWS

This chapter presents the methodology that was adopted to achieve the aim and objectives of this project. The process involves Programming a SIM with N-profile of Mobile Network and development of an N-Mobile Network MOES system. The flowchart below shows the activities of this project.

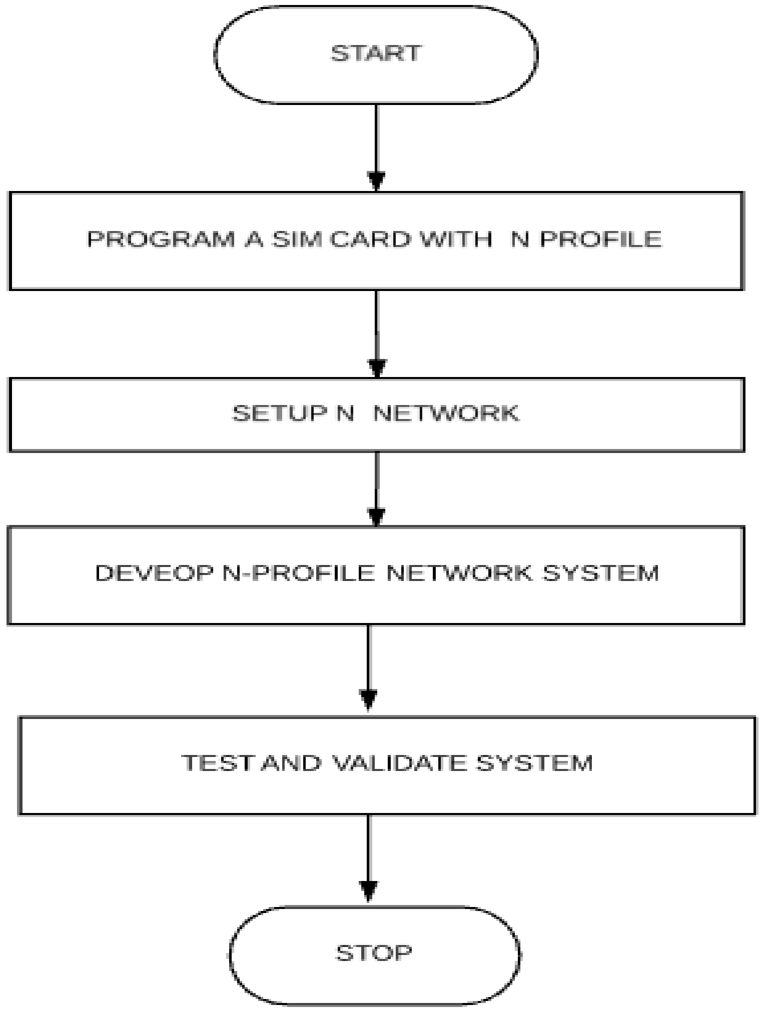


Figure 6 Flowchart of project methodology

Figure 6 shows the flowchart for the methodology employed by the project. The project starts with programming a blank sim card with four profiles representing the networks the MOES card is registered to, then the next stage is setting up a four-simulated network using Wi-Fi which MOES card will be connected to. Finally, a GUI based system is designed that checks the SIM parameters and saves the profiles to allow the SIM to automatically switch to the available networks.

3.2 PROGRAMMING A SIM

To achieve this objective, python programming language is used. This necessitates the installation of a python interpreter. A python package for SIM Card Programming Called Pyscard. The pyscard library is a python framework dedicated to building smart card applications. The package is built based on the Personal Computer Smart Card (PCSC) API wrapper also implemented in Python. The PCSC API is implemented in C. Pyscard is supported on Windows Operating System using Microsoft Smart Card Components.

The Pyscard library allows communication by interfacing with the PCSC API to access smart cards and smart card readers. The pyscard architecture is shown in Figure 7.

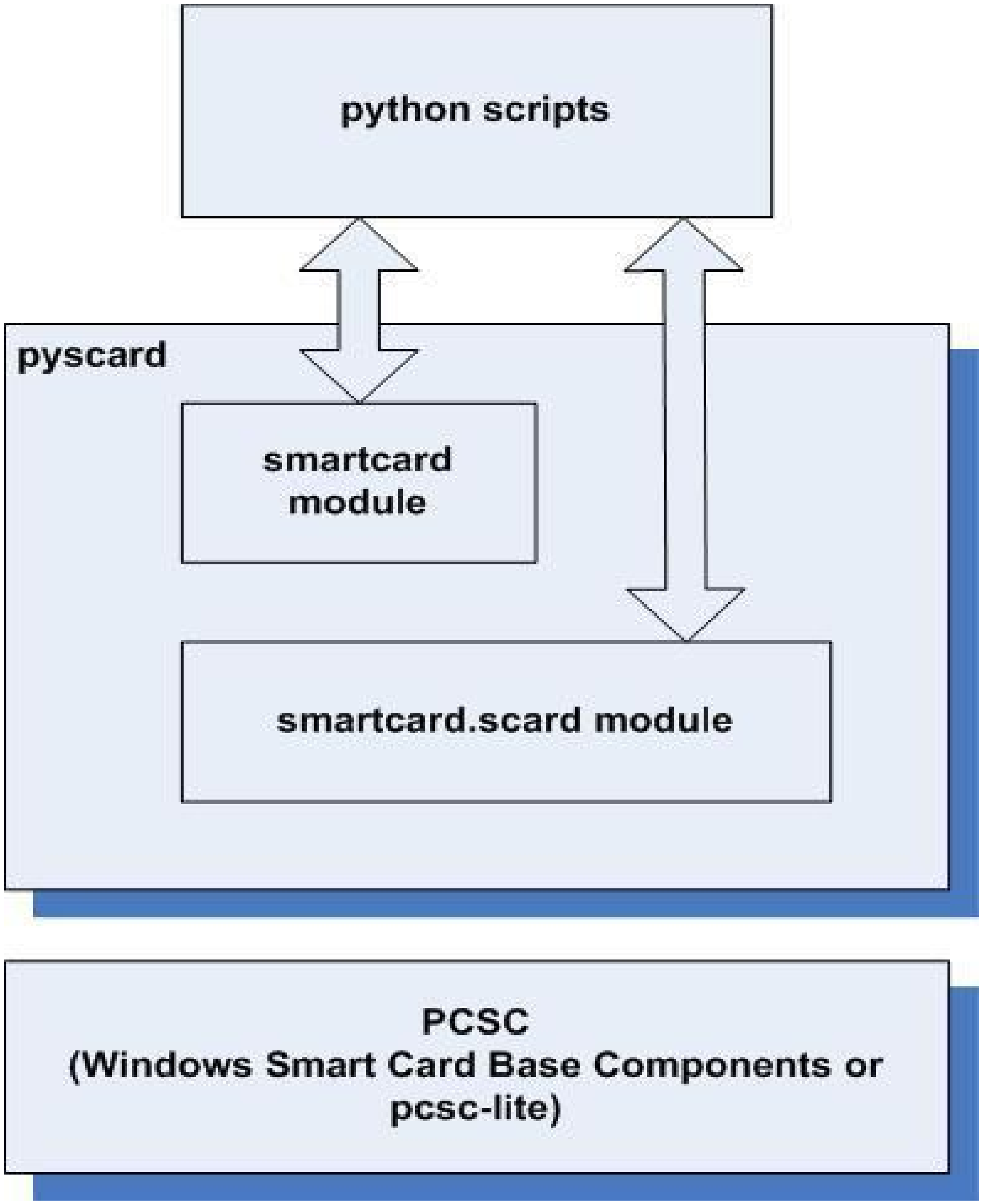


Figure 7: Pyscard Architecture

3.2.1 PROGRAMMING PARAMETERS

The following are the parameters and information used during programming of the SIM

1. Answer-to-Reset (ATR)
2. Integrated Circuit Card Identifier (ICCID)
3. Elementary(EF) file

3.2.2 SIM CARD READER:

The smart card reader is a device that allows communications between the computer and the SIM card. The smart card is connected to the serial port of the smart card and is also to the PC USB port through a USB cable. Figure 8 shows the image of the Smart card reader.

Figure 8 SMART CARD READER

3.2.3 N-PROFILES

This is achieved by having more than one batch file associated with the SIM. A batch file is a scripting file that runs in the windows DOS interpreter (Command prompt). The batch files form the N- profiles for each network to which the SIM can be connected. They contain commands that allow the PC to connect to the network's setup.

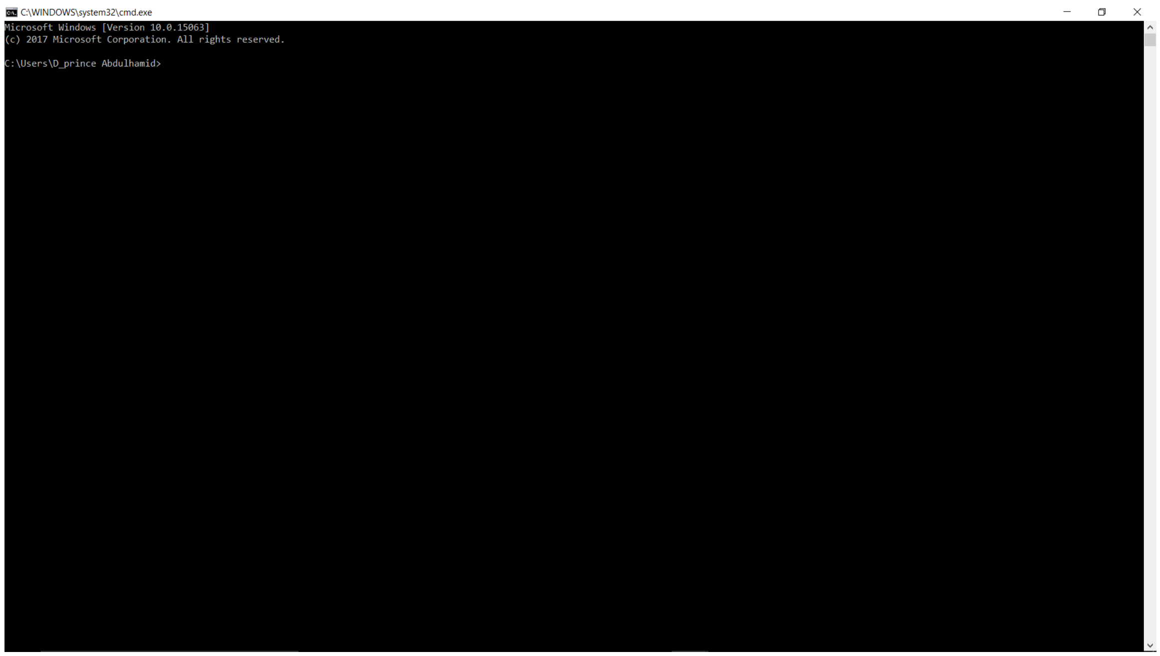


Figure 9 :Windows Dos interpreter

3.3 DEVELOPMENT OF A N-PROFILE NETWORK MOES SYSTEM

The Mobile Equipment (ME) containing the N-profile SIM signs into the N-profile network and Some APDU commands are communicated between the system and ME to verify the SIM, the network profiles are then saved and used to connect to the available network. The system switches to another network if the signal is lost or if the signal is poor. The flow of activities in the system is described by the diagram below.

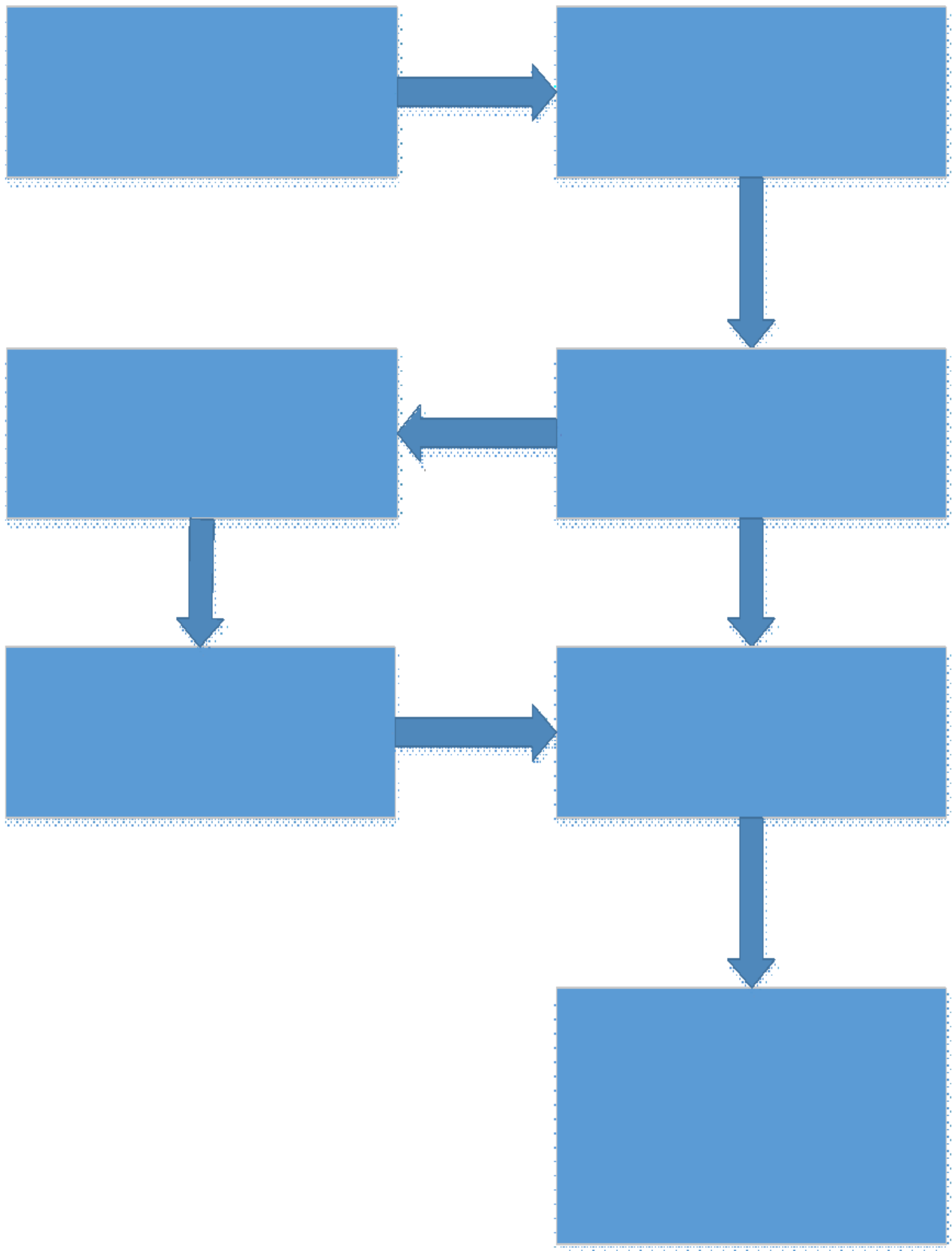


Figure 10 : process flow of the system

3.4 NETWORK SETUP

The Wi-Fi Network is used as the required GSM signal for connecting the mobile user because of the inability to set up a base station which usually requires registration of the telecommunication company which is very costly and cannot be achieved within the time frame of this project.

3.4.1 JUSTIFICATION FOR USING WIFI NETWORKS

The Wi-Fi is used in place of the GSM for the following

1. Achieving successful configuration of the GSM network requires registration.
2. GSM networks involve acquiring Base stations equipment which is rather costly and time consuming which will take longer for this project.
3. This project requires multiple networks which involve acquiring authentication key (Ki) of other network operators. This is serious constraint because network operators are unwilling to give up their Kis.
4. The Wi-Fi and the GSM both use the radio frequency although they have different frequency ranges.
5. Like the GSM, the Wi-Fi can also be used for both data and voice communication.

3.4.2 ROUTER:

Four Routers are used to set up Wi-Fi networks. The Four Wi-Fi networks are configured with the names MOES1, MOES2, MOES3 and MOES4. These networks represent the networks they can connect to using the MOES Card.

3.4.3 NETWORK SWITCHING ALGORITHM

No specific algorithm is used to switch between networks as that is beyond the scope of this project. However, a basic switching parameter is used based on the strength of the received signal and presence of a designated MOES network. This is programmed in IF and ELSE conditions which although is rather inefficient but provides a simple switching method. In this case the system will check if the current network signal is lost and switch to another MOES network available and whose signal strength is strong.

3.5 SOFTWARE INTERFACE

This is a Graphical user Interface application developed using the Kivy framework. Kivy is a python GUI library for flexible and interactive application design. The main aim of this application is to implement the N-Mobile network system and display the flow of connection activities.

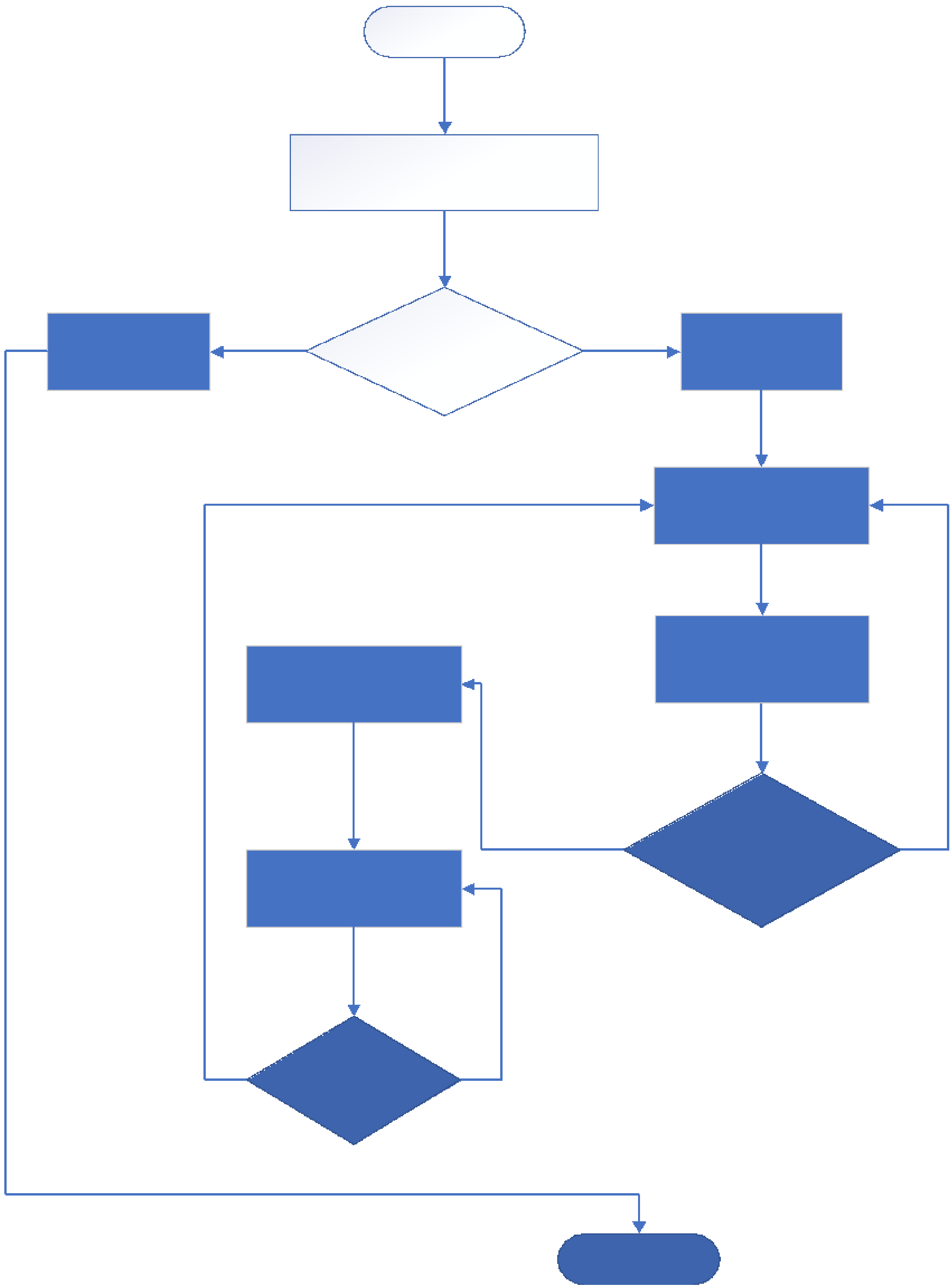


Figure 11: Flowchart of the system

The system has the following features.

1. HOME PAGE

   The home Page contain the following feature

   a. Check ATR button: This Button Sends an APDU command that is used to get ATR of the SIM inserted. The ATR of the SIM is displayed in a Label under the Button.
   b. Sign in button: This button sends a command that allows the SIM to sign in to the system. The SIM ATR is checked, if the ATR is correct i.e. it is the ATR of the MOES SIM, the SIM allowed to sign in and a new screen to check the network available.

2. CHECK NETWORK PAGE

   The check network page has the following features

   a. Check network button: This button is used to send a command that shows all the available networks in the system and their signal strengths. The strongest network is connected to.
   b. Information text area: This is a scrollable text area that shows the network information of all available networks, their status i.e. connected or not and signal strengths.
   c. Connect to network button: This button is used to connect to available network, the connection automatically switches to another network when the current network signal is lost. This is possible because the profile file of the networks has been saved in the system.

CHAPTER FOUR

IMPLEMENTATION, RESULT AND DISCUSSION

4.1 INTRODUCTION

This chapter is a comprehensive description of how the system was implemented. Detailed results of the functionality of the system obtained from simulation of the MOES network is shown. Lastly, discussion of the result from simulation is included.

4.2 CHOICE OF PROGRAMMING LANGUAGE

The python language is used extensively in the implementation of the N-profile network system. The Python Language is chosen because of its flexibility, simplicity and ability to run on multi-platforms. The python language is robust and extensible, therefore new features can be added without disrupting the structure of the language. It supports many programming paradigms such as object-oriented programming paradigm, parallel programming, procedural as well as functional programming. Object-oriented properties of python language are inheritance, Encapsulation and Polymorphism using objects and classes

4.3 SYSTEM REQUIREMENT

The requirements for the successful implementation of the system can be divided into two. They are the hardware and the software requirements.

4.3.1 HARDWARE REQUIREMENTS

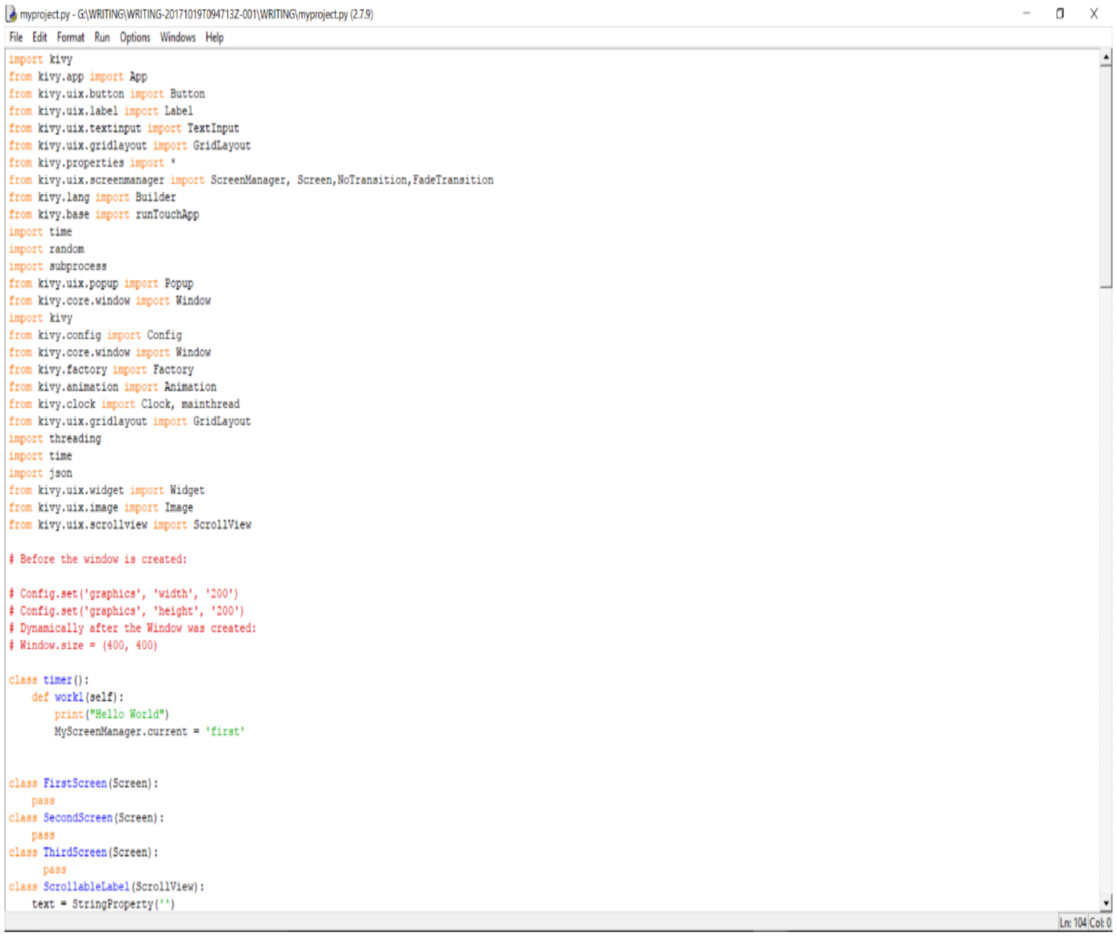
The following hardware components were used in this project are a Laptop personal computer, a SIM card, a SIM card reader and Routers. The Operating system platform used to implement are Window 10 and Windows 8(64bits) Operating systems. The

Minimum RAM used is 2GB, Processor (intel, Pentium) speed of 2.40GHz and total storage space of 500GB. The working voltage of the SIM card reader is 3v – 5v with a USB connection to the computer. Lastly, the card is a contact card that connects to the SIM card reader serially with half-duplex connection.

4.3.2 SOFTWARE REQUIREMENTS

The N-profile Network system was developed in the Python 2.7 IDLE environment which bundles basic libraries for rapid development. The python kivy library was used for the GUI design The Pyscard library was installed for python interfacing with SIM card reader to enable programming of the SIM card. The Windows Smart Card driver was also installed to allow communication between the computer and the card Reader. Windows Visual studio 2010 was also installed which is a compulsory dependency for the installation of Pyscard. The eyeshot of the start page of Python IDE used for implementation and code environment are shown below. The system requirements are categorized into two, namely functional requirement and non-functional requirement.

Figure 12: python interpreter



myproject.py - G:\WRITING\WRITING-20171019T094713Z-001\WRITING\myproject.py (2.7.9)

File Edit Format Run Options Windows Help

```
import kivy
from kivy.app import App
from kivy.uix.button import Button
from kivy.uix.label import Label
from kivy.uix.textinput import TextInput
from kivy.uix.gridlayout import GridLayout
from kivy.properties import *
from kivy.uix.screenmanager import ScreenManager, Screen,NoTransition,FadeTransition
from kivy.lang import Builder
from kivy.base import runTouchApp
import time
import random
import subprocess
from kivy.uix.popup import Popup
from kivy.core.window import Window
import kivy
from kivy.config import Config
from kivy.core.window import Window
from kivy.factory import Factory
from kivy.animation import Animation
from kivy.clock import Clock, mainthread
from kivy.uix.gridlayout import GridLayout
import threading
import time
import json
from kivy.uix.widget import Widget
from kivy.uix.image import Image
from kivy.uix.scrollview import ScrollView

# Before the window is created:

# Config.set('graphics', 'width', '200')
# Config.set('graphics', 'height', '200')
# Dynamically after the Window was created:
# Window.size = (400, 400)

class timer():
    def work1(self):
        print("Hello World")
        MyScreenManager.current = 'first'


class FirstScreen(Screen):
    pass
class SecondScreen(Screen):
    pass
class ThirdScreen(Screen):
      pass
class ScrollableLabel(ScrollView):
    text = StringProperty('')
```

Ln: 104 Col: 0

Figure 13: python code editor

4.3.2.1 FUNCTIONAL REQUIREMENT

The functional requirements of the system are;

i. The system must provide capabilities to check SIM card details.

ii. The system must allow only SIM with multiple network profile (MOES)

iii. The system must allow only SIM cards.

iv. The system must show details of the network available and their respective signal strength.

v. The system must only connect to MOES networks.

vi. The system should be able to switch between available networks when signal is low.

vii. The user should be able to view network details.

4.3.2.2 NON-FUNCTIONAL REQUIREMENT

The Non-functional Requirements of the system are;

i. The system should provide an interactive and easy-to-use interface for the user.

ii. The system should possess usability, availability, interoperability and portability.

iii. The system should provide an Error Message Box when an invalid word is entered by the user.

4.4 IMPLEMENTATION

Figure 14 is the home screen of the Graphic User Interface (GUI) of the implemented system at design period.

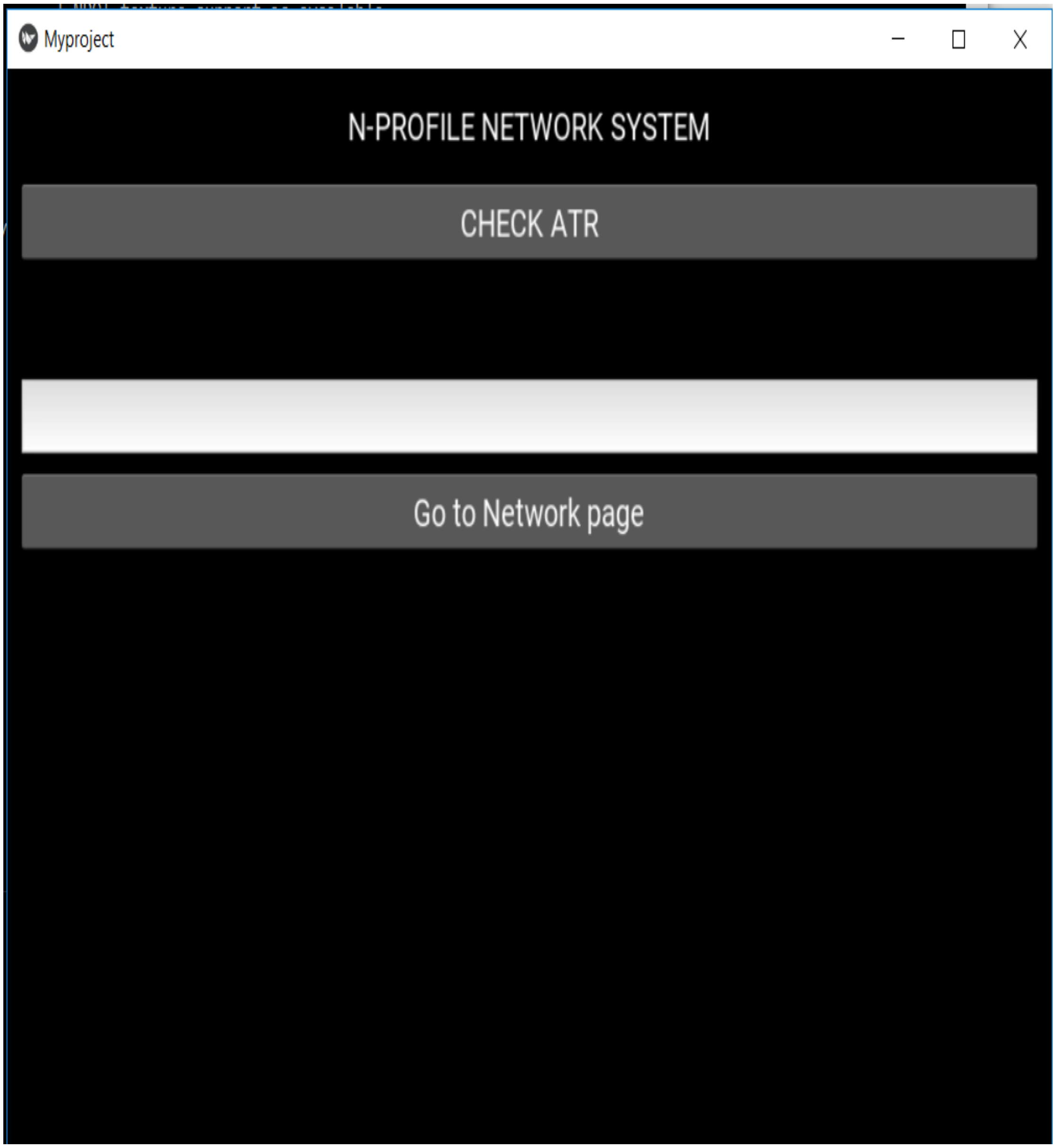


Figure 14: Home Page

It consists of a Check ATR button which when clicked the text under displays the ATR of the SIM card inserted and indicates whether the SIM is a MOES SIM or not. The Go to Network page button takes the user to the Network information page.

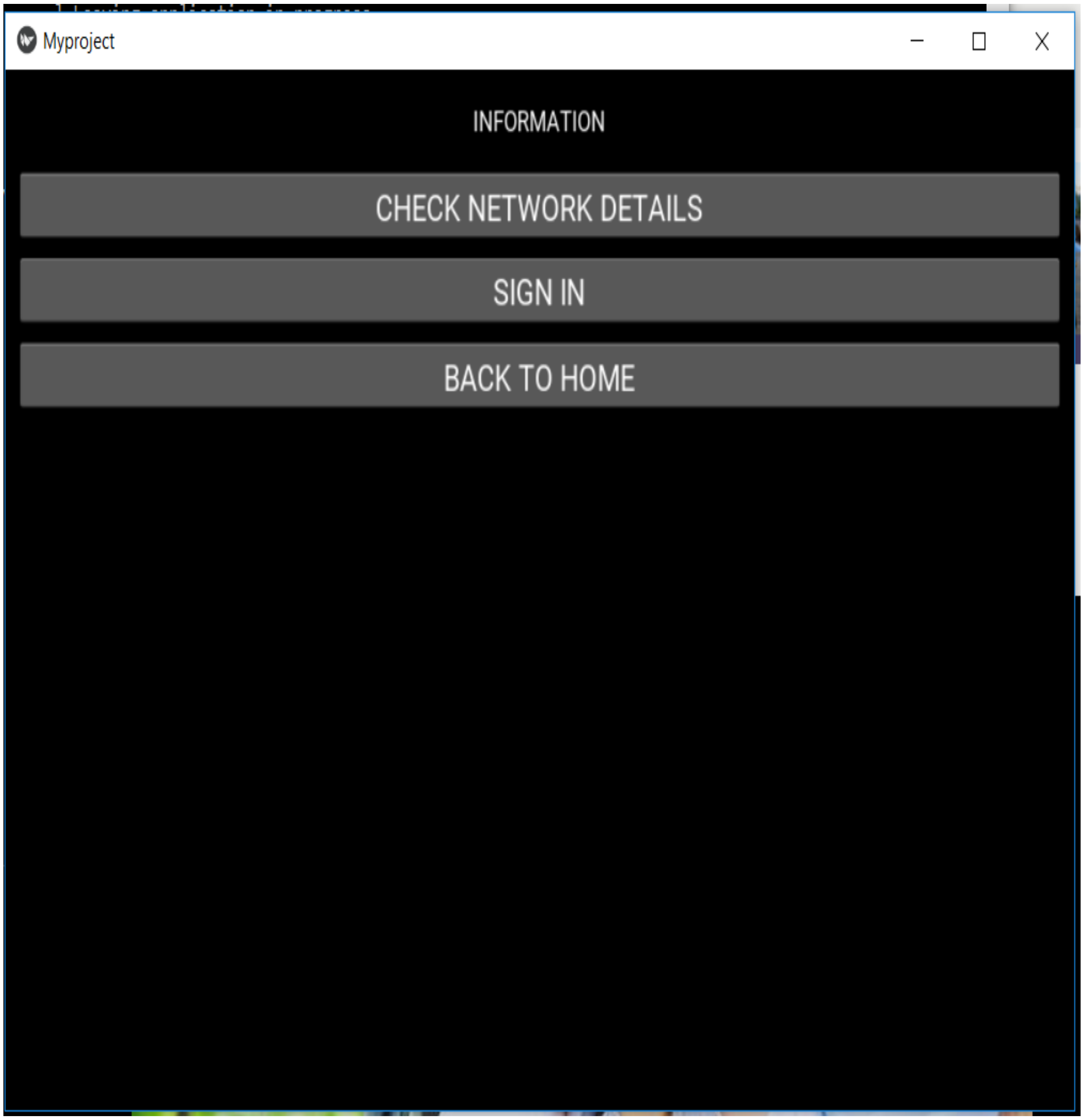


Figure 15

Figure 15 shows the network information screen. The page has a header showing the title of the page. The CHECK NETWORK DETAILS button sends the command that gets the details of all available networks and their signal strengths. The SIGN IN button opens another screen for the SIM to connect to the available network. If the SIM is not a MOES SIM, it will not be able to sign or connect to any network. The BACK TO HOME button returns the user to the Home screen. There is a scroll-text area that displays the output of the network details underneath the BACK TO HOME button. The scroll-text is automatically cleared when the CHECK NETWORK DETAILS button is pressed.

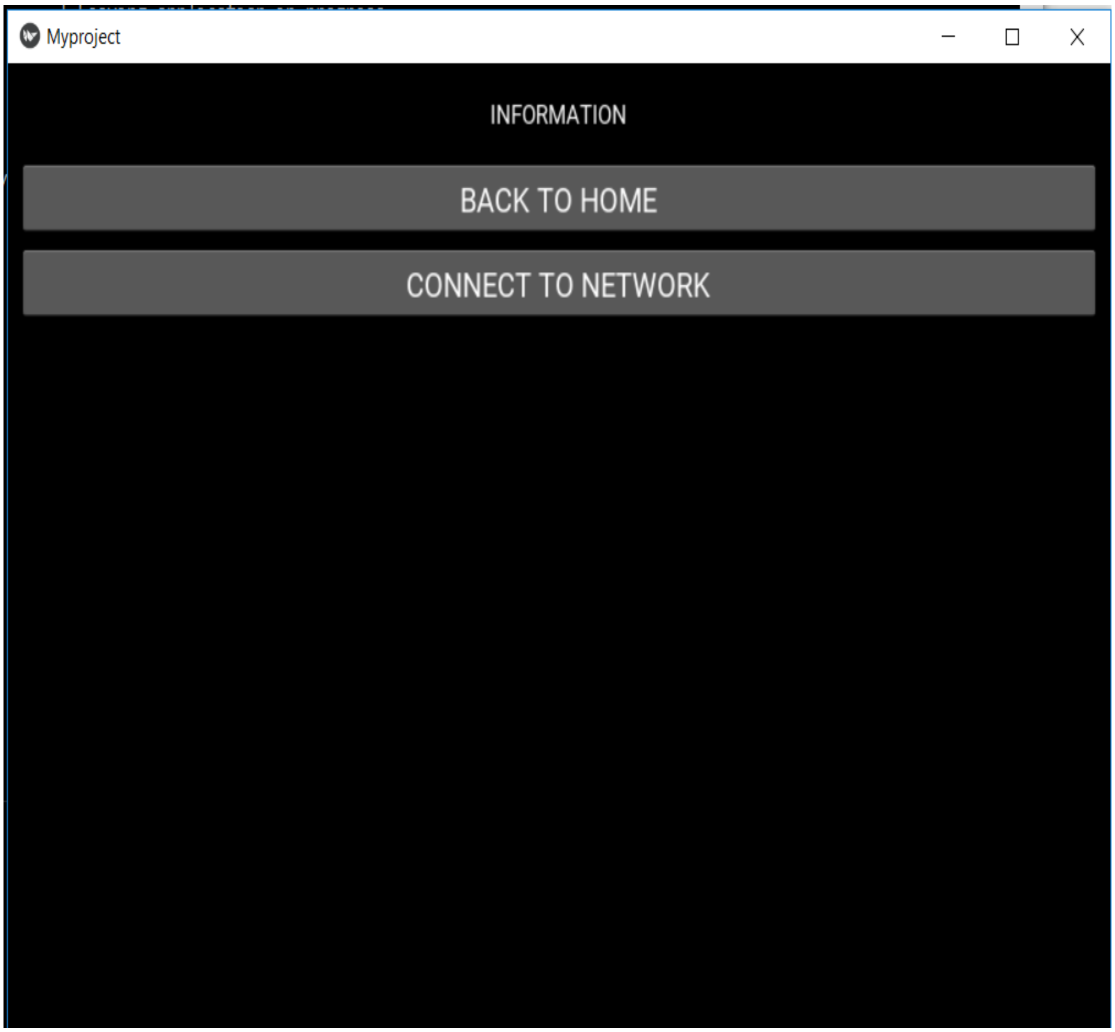


Figure 16

Figure 16 is the network connection screen. The BACK TO HOME takes the user back to the Home screen. The CONNECT TO NETWORK button connects the MOES SIM to the currently available MOES network (i.e. any available MOES NETWORK) or MOES network with the strongest received signal. There is a scroll-text area underneath the

CONNECT TO NETWORK button that shows the currently connected network. It is automatically updated when the network changes.

4.5 TESTING AND EVALUATION

The N-PROFILE system was set up to connect to four NETWORKS named MOES 1, MOES 2, MOES 3 and MOES 4 as a simulated test network for four GSM networks. The system was first tested using a SIM card from other sources (i.e. non-MOES SIM Card). Figure 17 represents the undesired output obtained.

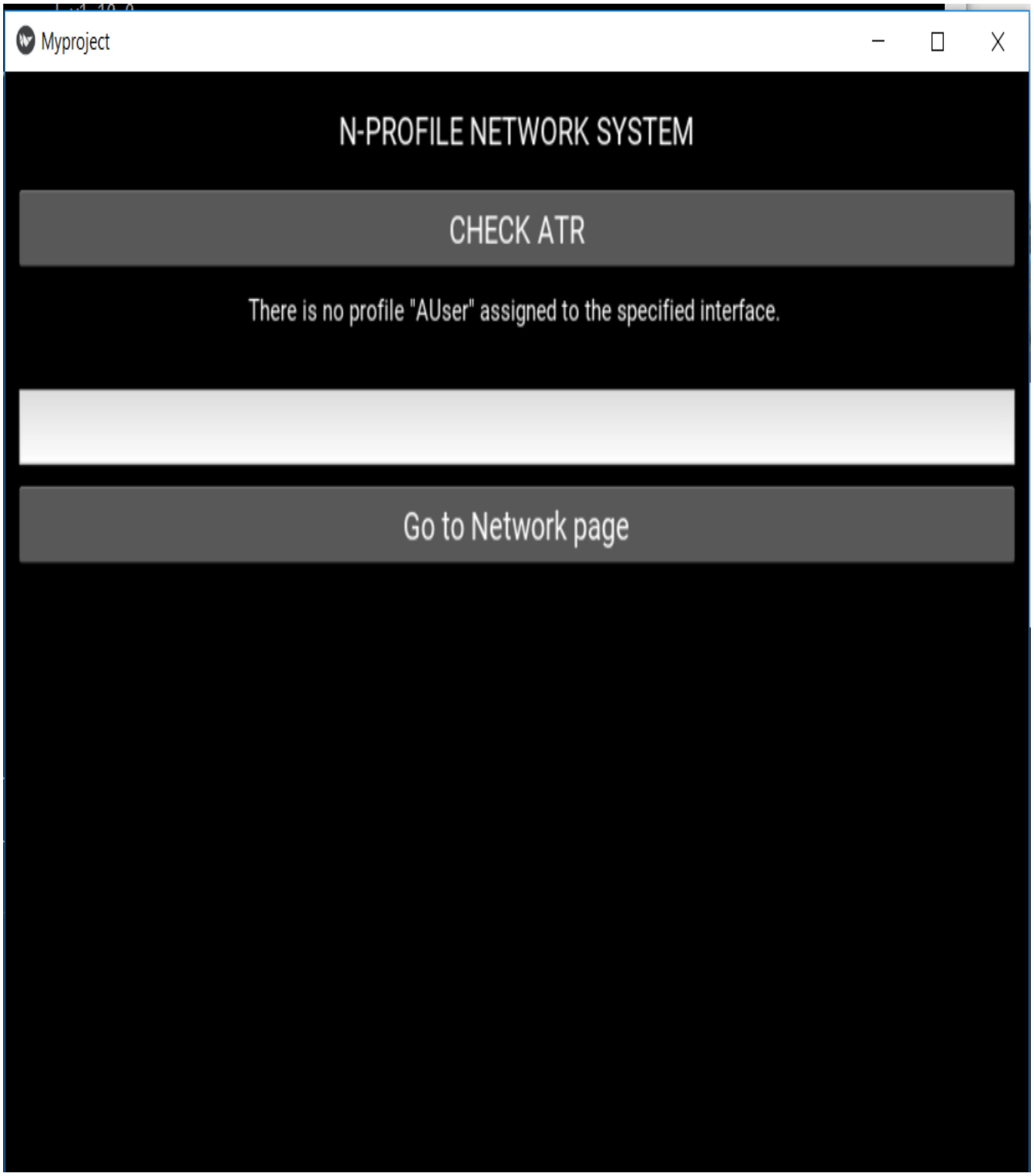


Figure 17: Checking for SIM ATR

Testing the SIM with other networks reveals the output in Figure 18

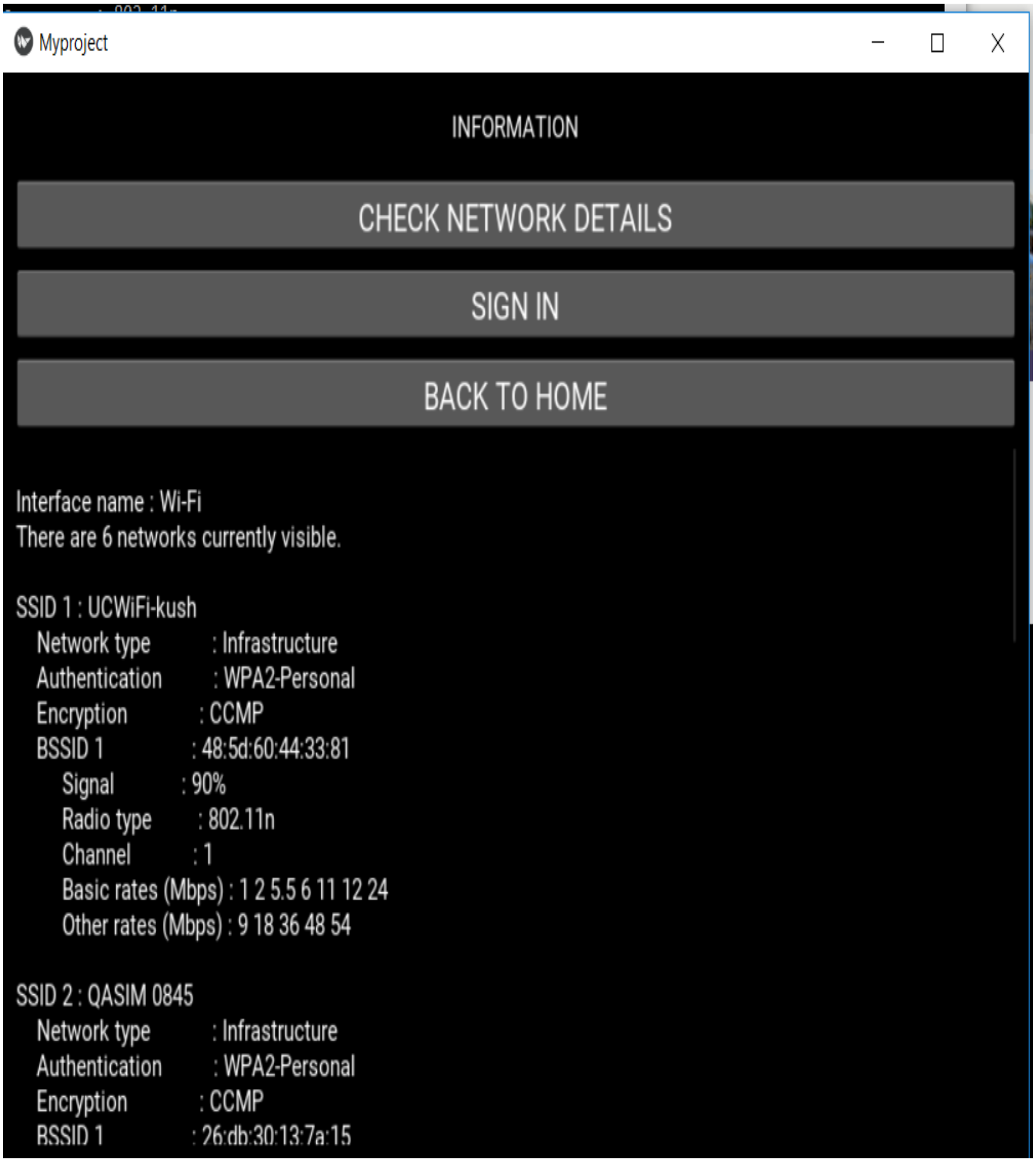


Figure 18: Getting Network details

The connection screen is not shown as the SIM is not a MOES SIM, so cannot be connected to any network.

The system was then tested using MOES SIM cards with various different signal strengths of the four MOES Networks. Figure shows the results that were derived.

4.6 DISCUSSION OF RESULT

Elaborate results obtained from the outputs in 4.5 above shows that the N-PROFILE NETWORK system has been successfully implemented. These results show that the system can detect a MOES SIM card and connect to available MOES networks. The system has a functionality of obtaining details of the MOES networks such as showing the signal strength and the currently connected networks as well as switching automatically between the available networks. Thus, the aim and objectives of this project work has been realized through the programming of a N-PROFILE Multiple Operator-Enabled SIM Card (MOES SIM card) and development of the N-PROFILE system.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 INTRODUCTION

This chapter discusses the summary, conclusion and recommendations for prospective researches that will be made to enhance the limitations of this system.

5.2 SUMMARY

This project has discussed in great detail the development of a multiple operator-enable SIM card. This project has concentrated mainly on programming a SIM card with multiple operator network profile and development of an N-Profile Network system that allows the SIM to connect to multiple networks using profiles associated with the SIM using IF THEN rule for Handover decision. The activities of this project have been sectioned into five chapters. Chapter one dealt with the introduction, problem statement, scope and limitation of the project. Chapter two gave a detailed discussion of concepts such SIM card , GSM,WLAN and a review of related studies. Chapter three described the methodology, flowchart of the system, the hardware used and the network setup. Chapter four gave a detailed and comprehensive account of the implementation, results obtained and discussion of the obtained results. Finally, in this chapter, an account of the summary, conclusion and recommendations for prospective researchers in this project is being given.

5.3 CONCLUSION

There have been various problems facing GSM telecommunication technology. Some of this problem are poor received signal strength, call drops, poor Quality of Service (QoS)s, call drops, Inter, lack of voice clarity, one way speech, poor network availability to mention a few. These problems hinder the effectiveness of GSM telecommunication. Therefore, there is a need to provide solutions to these problems. This project provides a solution to these problems by developing a multiple operator-enabled SIM card using multiple profiles saved on the SIM. The MOES SIM is further tested by the development of a N-Profile network system to evaluate the performance of the SIM in the various networks. This project is a proof of concept to the feasibility of SIM cards with multiple operator-enable networks. It shows that a GSM network system can be developed to integrate various mobile network operator profiles into a SIM card.

5.4 RECOMMENDATIONS

This project work is recommended for use in the GSM technology for seamless data and voice communication. While carrying out this project work, some limitations were discovered which were not covered. Therefore, the following suggestions are recommended for future research on this topic or related aspect of the SIM card and GSM technology.

i. Any future research on this project topic of interest should focus on the integration with the mobile phones.

ii. A researcher interested in this work can enhance it by including an efficient handover algorithm.

iii. Interested researchers should focus on using an authentication key Ki for authentication.

REFERENCES

Aibinu, A. M., Onumanyi, A. J., Folorunso, T. A., Ipinyomi, M., & Adda, A. (2016). Development of Embedded-Multiple Operators Enabled SIM (E-MOES) Card System for Mobile-Phone Initiated and Executed Handover, 20.

Aydemir, Ö., & Selçuk, A. A. (2005). A strong user authentication protocol for GSM.*Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*, *2005*, 150–153.https://doi.org/10.1109/WETICE.2005.12

Deville, D., Galland, A., Grimaud, G., & Jean, S. (2003). {Smart Card} Operating Systems: Past, Present and Future. In *USENIX/NordU*.

Dixit, A., & Sharma, S. (2014). A Study of Handoff to Enhance the (QoS) for Cell Communication in GSM & CDMA. In *IJCAT - International Journal of Computing and Technology* (Vol. 1, pp. 448–456). Retrieved from www.IJCAT.org

Edsbäcker, P. (2011). *SIM cards for cellular networks An introduction to SIM card application development*. MID SWEDEN UNIVERSITY.

Gielen, S. (2012). *SIM Toolkit In Practice*. Radboud University , Nijmegen, The Neherlands.Retrieved from https://pdfs.semanticscholar.org/47c6/3f2a6ff636dd6bc84f6a8fa4fe7e2f60db53.pdf

Grosvenor, Edwin, & Morgan, W. (1997). *Alexander Graham Bell: the life and times of the man who invented the telephone*. New York: Harry Abrams.

GSMA Intelligence. (2015). Understanding SIM evolution, (March), 1–17. Retrieved from https://www.gsmaintelligence.com/research/2015/03/understanding-sim-evolution/499/

Husemann, D. (2001). Standards in the smart card world. *Computer Networks*, *36*(4), 473–487. https://doi.org/10.1016/S1389-1286(01)00167-0

MobileMarketting.am. (2017). MobileMarketting.am. Retrieved from

MobileMarketting.com

NCC. (2016). Development of Multiple Subscribers Identity Module (SIM) cards Reader and Analyser.

Rahnema, M. (1993). Overview of the GSM System and Protocol Architecture, (April), 92–100.

Ronalds, B. . (2016). *Sir Francis Ronalds: Father of the Electric Telegraph.* London: Imperial College Press.

Tomas, N. (2001). History of the U.S. Telegraph Industry. Retrieved from http://eh.net/encyclopedia/history-of-the-u-s-telegraph-industry

Tsai, Y., & Chang, C. (2006). SIM-based Subscriber Authentication for Wireless Local Area Networks. *Computer Communications*, *vol: 29*, 1744–1753. https://doi.org/10.1016/J.COMCOM.2005.09.016

Wikipedia. (2017a). Subscriber identity Module. Retrieved from https://en.wikipedia.org/wiki/Subscriber_identity_module

Wikipedia. (2017b). Telephone. Retrieved from https://en.wikipedia.org/wiki/Telephone

Wu, P., Du, W., & Cui, H. (2002). A design of SIM card interface for general purpose. In *2002 International Conference on Communications, Circuits and Systems and West Sino Exposition, ICCCAS 2002 - Proceedings* (Vol. 2, pp. 1271–1274). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCCAS.2002.1179014