AN APPROACH TO SELECTIVELY BLOCK MOBILE PHONE COMMUNICATION WITHIN A MOBILE PHONE RESTRICTED AREA

By

Michael Agyare

(B.Sc. Telecommunications Engineering)

A thesis submitted to the Department of Electrical Engineering, Kwame Nkrumah University of Science and Technology, Kumasi in Partial fulfilment of the requirements for the award degree of

MASTER OF PHILOSOPHY IN TELECOMMUNICATION ENGINEERING

July 2019

Declaration of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma at Kwame Nkrumah University of Science and Technology, Kumasi or any other educational institution, except where due acknowledgment is made in the thesis.

…….	…….	…….
Name of Student and ID	Signature	Date

Certified by:

…….	…….	…….
Name of Supervisor	Signature	Date

Certified by:

…….	…….	…….
Name of Head of Department	Signature	Date

Abstract

The use of mobile phone jammers to discourage mobile phone usage in mobile phone restricted areas has some limitations. One major limitation is that, once the jammer is activated no mobile phone can be able to function within the restricted area. For that reason, in the case of emergencies, no mobile phone can either make or receive phone calls or perform emergency calls (police, fire and ambulance services). Works done in literature can detect and block phone calls in a certain way but depends on the mobile switching centre in order to block communication in the restricted area. Therefore, in this thesis, a selective mobile phone communication blocking system is proposed which does not depend on the mobile switching centre in order to perform blocking of communication. The proposed system seeks to allow privilege users access to communication and block non-privilege users with respect to a specific user location. Some mobile phone user locations were considered in this thesis (Hospitals, Banks and Schools). A user from a particular user location cannot enjoy the same privileges at a different location provided that user is privileged. The selective blocking nature of the system was simulated using Fuzzy Inference System (FIS) toolbox (mamdani). The inference method is based on a set of IF-THEN rules and membership functions of the input variable and output variables of the system. Users for the different locations were converted into input triangular membership functions. The output is the decision ("allow" and "not allow") for each of the inputs. S-shape and Z-shape membership functions were used as the output decision variables. The set of IF-THEN rules were used to link the input variables to the output variables. The fuzzy inference system was able to perform selective blocking of communication services for privileged and non-privileged users. The results in this work shows that when the proposed system is implemented mobile phone communication service can be prioritised to suit privilege users in specific mobile phone restricted areas.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

3G	-	Third Generation Mobile Network
ACCH	-	Associated Control Channel
ARFCN	-	Absolute Radio Frequency Channel Number
BCCH	-	Broadcast Control Channel
BCH	-	Broadcast Channel
BFSK	-	Binary Frequency Shift Keying
BJ	-	Barrage Jamming
BSC	-	Base Station Controller
BTS	-	Base Transceiver Station
CCCH	-	Common Control Channel
CDMA	-	Code Division Multiple access
CI	-	Cell Identification
CSMA	-	Carrier Sense Multiple Access
DCF	-	Distributed Coordination Function
DCS	-	Digital Cellular System
DoS	-	Denial of Service
DRTJ	-	Direct Receive & Jammers
EIR	-	Equipment Identity Registry
FCCH	-	Frequency Correction Channel
FDMA	-	Frequency Division Multiple Access
GMSK	-	Gaussian Minimum-Shift Keying
GSM	-	Global System for Mobile Communications
HLR	-	Home Location Registrar
ICD	-	Intelligent Cellular Disablers
IMSI	-	International Mobile Subscriber Identity

Kc	-	Ciphering Key
Ki	-	Authentication Key
LAC	-	Location Area Code
LTE	-	Long-Term Evolution
MCC	-	Mobile Country Code
MitM	-	Man-in-the-Middle
MNC	-	Mobile Network Code
MOC	-	Mobile Originated Call
MS	-	Mobile Station
MSC	-	Mobile Switching Centre
MSIN	-	Mobile Subscriber Identification Number
MTC	-	Mobile Terminated Call
NBN	-	Narrowband Noise Jamming
PC	-	Personal Computer
RAND	-	Random Number
SIM	-	Subscriber Identity Module
SRES	-	Signed Response
TDMA	-	Time Division Multiple Access
TIMSI	-	Temporary International Mobile Subscriber Identity
UE	-	User Equipment
UMTS	-	Universal Mobile Telecom System
USRP	-	Universal Software Radio Peripheral
VLR	-	Visiting Location Registrar

Acknowledgments

I would like to express my sincere gratitude to my supervisor Dr. Jerry John Kponyo and adviser Francis Kwabena Oduro-Gyimah for their direction and effective guidance in carrying out this research work. I would also like to thank my friends and family members who supported me through my journey especially Mr. Erasmus Agyare, Ms. Jemama Akuoko-Nketiah and Ms. Edna Owusu Boakye. Finally, Above all I thank the God ALMIGTY for His guide, protection, favour and love over my life.

Chapter 1

1.1 General Introduction

In order to influence a person's cell phone to evade undesirable calls, there is a useful device known as cell phone jammer accessible in the market. A cell phone jammer is a device utilized to deny cellular phones from getting signals from a base station. Whenever utilized, the jammer successfully debilitates cellular phones. These devices can be utilized in any location, but are located mainly in places where a phone call would be mostly disrupting on the grounds that silence is required [1]. A cell phone jammer is valuable in hospitals, banks, museums, government offices, colleges, schools, petrol pump stations, airports, meetings and seminars. After initiating a jammer, incoming calls are jammed. When the Mobile phone jammer is turned off, all mobile phones will automatically recreate connection with the base station.

Mobile phone jammer's effect can differ extensively based on reasons such as closeness to towers, indoor and outdoor sites, the existence of structures and landscape, even temperature and humidity play a part. The Output Power of the Jammer is usually stated in Watts or in some situations dBm.

To jam a cell phone, all that is needed is a device that can transmit noise on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. GSM, used in digital cellular and PC-based systems, Operates in the 900-MHz and 1800-MHz bands in Ghana and the 1900-MHz band in the United States of

America. Jammers can transmit on all communication frequencies (CDMA, GSM, DCS, and 3G). Out-of-date analog cell phones and today's digital devices cannot escape jamming [1].

1.2 Problem Statement

Due to the increasing demand for telecommunication services, mobile phones have become part of almost every human life. This allows users to make calls, text and send video messages.

However, there are some places where cell phone activities are restricted and silence is required. With this as a problem, mobile phone jammers can be used to block cell coverage or prevent cell phone users from making and receiving calls within that particular restricted area. This discourages mobile phone usage in the restricted area.

However, the use of a mobile phone jammer has some limitations. Once activated no mobile phone can be able to function within the restricted area. For that reason, in the case of emergencies, no mobile phone can either make or receive phone calls or perform emergency calls (police, fire and ambulance services) [2] [3]. There is a need for a system, which can allow some communication services for emergency communication and block others to discourage the use of mobile phones in specific restricted mobile phone areas.

Therefore, a selective mobile phone communication blocking system is proposed which can control communication services for specific mobile phone restricted areas.

1.3 Objectives of the Research

1.3.1 General Objective

The purpose of this research work is to investigate and design the possibility of having an active interception system for specific mobile phone restricted locations and allow privileged users to have access to full communication in these locations.

1.3.2 Specific Objectives

The following are the specific objectives set in order to achieve the general objective:

- To design a selective mobile phone communication blocking system.
- To develop an algorithm for the decision making of communication services for specific restricted mobile phone areas and grant privileged users access to full communication.
- To simulate the blocking nature of the system.

1.4 Justification of Research

Works in literature can all block and detect phone calls in a certain way [4] [5] [6] [7]. In connection with the problem statement of this research selective jamming approach depicted in [8] and [9], is a good approach in segregating among cell phones in a restricted area. However, these approaches did not exploit the idea of a standalone interception system, which is independent of the operator's network in other to update its identity repository, capable of functioning as a filter for connecting mobile phone users within the restricted area and the operator's network. Works in literature did not also consider a selective blocking system capable of blocking some user subscriber services with regards to a particular location and allow all users access to emergency services (police, fire, and ambulance) [10] [11] [12] [13].

It is proposed that to fully control mobile phone usage in a restricted area, an autonomous interception control system is required, which is not dependent on the operator's MSC in order to perform blocking. The system should fully control voice calls, SMS, data connection and emergency services (police, fire, and ambulance) with respect to the type of communication service restricted to a specific location.

The research seeks to design a standalone interception system with privileged user access, capable of blocking communication services with respect to a specific user location. It also seeks to allow emergency call services (police, fire, and ambulance) for all mobile phone users in the restricted area.

1.5 Research Questions and Hypothesis

In the review of literature on Active interceptors has identified a gap in literature.

Research Question

In view of this, the following research questions have been identified;

- Can an Active interception system be designed to block some user subscriber services with respect to specific user locations?
- Can an Active interception system perform selective blocking of communication?
- Can an active interception system allow all mobile phones to perform emergency calls?

Research Hypothesis

Based on the reviewed literature, the formulated hypothesis is that proposed system can perform blocking of communication services for specific mobile phone restricted areas excluding privileged users.

1.6 Scope of the Research

This study emphasises on how the proposed system will selectively block communication services in a restricted area. That is to enable eligible mobile phones users who are privileged to enjoy all or some communication services in the restricted area and block any other. The study will solely be implemented in a software environment and matlab's fuzzy inference system toolbox will be used.

Chapter 2

Literature Review

2.1 Introduction

Jamming in wireless networks is defined as the disturbance of wireless communications by reducing the signal-to-interference ratio of receiver side amid the transmission of interfering wireless signals [14]. An interceptor is a system that aids the network provider to block unwanted communications inside protected areas, according to the user identity. There are two types of interceptors; Passive and Active interceptors. The two types of interceptors will further be discussed in this chapter.

2.2 Types of Jammers

There are numerous ways a jammer may jam a network to be effective. Based on a functionality, a jammer can be termed either elementary or advanced. Proactive and reactive are the two forms of elementary jammers. The advanced jammers can be categorized as function-specific and smarthybrid [14].

2.2.1 Elementary Jammers

2.2.1.1 Proactive jamming

Proactive jammers emit jamming signals whether or not there is a data communication in a network. All other nodes on a channel are put into non-operating modes sending packets or random bits on the channel that they are working on. Nevertheless, they operate on one channel at a given time. Constant, deceptive and random are the three basic types of proactive jammers [14].

2.2.1.1.1 Constant Jammer

Constant jammer emits continuous, random bits without following the Carrier-Sense Multiple Access (CSMA) protocol [15]. According to the CSMA mechanism, a legitimate node has to sense the position of the wireless medium before transmitting. If the medium is continuously idle for a Distributed Coordination Function (DCF) Inter-frame Space (DIFS) duration, only then it is theoretical to transmit a frame. If the channel is found busy during the DIFS interval, the station should defer its transmission. A constant jammer prevents legitimate nodes from communicating with each other by causing the wireless media to be perpetually in use [15]. This form of approach is energy inefficient and easy to detect but is very easy to set up and can damage network communications to the point that no one can transmit at whatever time [14].

2.2.1.1.2 Deceptive jammer

Deceptive jammer continuously transmits regular packets [15] instead of emitting random bits (as in constant jammer). It leads on other nodes to believe that a legitimate transmission is taking office so that they remain in receiving states until the jammer is turned off or dies. Linked to a constant jammer, it is more difficult to sense a deceptive jammer because it transmits valid packets as a substitute of random bits. Comparable to the constant jammer, deceptive jammer is also energy inefficient due to the constant transmission but is very easily applied [14].

2.2.1.1.3 Random jammer

Random jammer intermittently transmits either random bits or regular packets into networks [15]. Contrary to the above two jammers, it aims at saving energy. It continuously switches between two states: sleep phase and jamming phase. It sleeps for a certain time of period and then becomes active for jamming before returning back to a sleep state. The sleeping and jamming time periods are either fixed or random. There is a tradeoff between jamming effectiveness and energy saving because it cannot jam during its sleeping period. The ratios between sleeping and jamming time can be manipulated to adjust this tradeoff between efficiency and effectiveness. [14].

2.2.1.2 Reactive jamming

Reactive jammer begins operation when a network activity is detected in a given channel [15]. As a result, reactive jammers function by compromising the reception of a message signal. In the process, both small and large sized bundles are disrupted. The reactive jammer is less energy efficient than a random jammer since it has to incessantly monitor the network while random jammer sleeps for a certain time of period and then becomes active for jamming before returning back to a sleep state. Random jammer is energy efficient because it cannot jam during its sleeping period, hence energy is saved. Nevertheless, because the packet delivery ratio (PDR) cannot be defined accurately in practice it is much more difficult to detect a reactive jammer than a proactive jammer [14].

2.2.3 Advanced Jammers

2.2.3.1 Function-specific jamming

Function-specific jamming is implemented by having a pre-determined function. In addition to being either proactive or reactive, they can either work on a single channel to conserve energy or jam multiple channels and maximize the jamming throughput irrespective of the energy usage.

Even when the jammer is jamming a single channel at a time, they are not fixed to that channel and can change their channels according to their specific functionality. [14].

2.2.3.2 Smart-hybrid jamming

They have an efficient and effective power jamming nature that is why they are called smart. The primary purpose of these jammers is to magnify their jamming effect in the network. They place sufficient energy in the right place so as to hinder the communication bandwidth for the entire network or a major part of the network, in very large networks. Each of this type of jammer can be implemented as both proactive and reactive, hence hybrid. [14].

2.3 Jamming Techniques

An attacker to can cause intentional interference in a wireless network using a jammer planted in the wireless network. A jammer can have either the same or different capabilities of legitimate nodes in the network to which they are transmitting depending upon the attack scheme used. A jammer depends on its radio transmit power, location, and influence on the network in or order to jam effectively.

2.3.1 Barrage Jamming

Barrage jamming (BJ) is the most basic of jamming and is generally defined as a jammer which transmits noise-like energy over an integral lot of the spectrum engaged by the target with 100% duty cycle in time. It is also named broadband noise jamming and is at times named full jamming. Therefore, it is non-correlated and non-protocol-aware. Game theory and information-theory have shown that barrage jamming is the best a jammer can do in the absence of the knowledge of the target signal [16].

2.3.2 Partial-band Jamming

It has been shown that jamming gains can be accomplished when jamming a single-carrier signal by not jamming the entire signal in the frequency domain, but rather jamming a fraction of the signal. This is acknowledged as partial-band jamming. It is usually debated as a non-correlated jamming attack since the jammer transmits endlessly in time. Partial band jamming is not effective against OFDM waveforms on the fact that strong forward error correction could allow the data to be restored from the unjammed subcarriers [17].

2.3.3 Narrowband noise jamming

Narrowband noise (NBN) jamming techniques place all of the jamming signal energy into a single channel. The bandwidth of this signal energy injection could be the whole width of the channel. In past systems, when the target is a digital signal, BFSK, for example, both the mark and the space tone frequencies receive jamming energy [18].

2.4 Selective jamming techniques

2.4.1 Intelligent Cellular Disablers

Intelligent Cellular Disablers (ICD) do not interfere with the frequency spectrum of an operator network like the traditional jammer do. When located in a designated quiet area, the device functions as a 'detector '. It holds a distinctive identification number for connecting with the cellular base station [19]. When an ICD device discovers the presence of a mobile phone in the quiet room, it signals the base station that the target user is in a 'quiet room; so, do not establish the communication [19]. Messages can be routed to the user's voice- mailbox if the user subscribes to a voice mail service. This operation of detection and interruption of call formation is performed during the interval normally reserved for signalling and handshaking. ICD is a passive interception system, which depends on the service provider's network to function. For the goal of having an autonomous system in the restricted area, this form of a system is not recommended.

2.4.2 Direct Receive & Transmit Jammers (DRTJ)

DRTJ functions as a portable base station, which can directly interact with a cellular network provider. This jamming system functions by using a mobile phone detector and a jamming transmitter. The jammer is usually in a receiving mode, which can detect a cell phone within its proximity [19]. Once the jammer detects a call communication setup between the mobile phone in its proximity and the operator's base station, a jamming signal from the jamming transmitter would be transmitted to disrupt the communication. Otherwise, there would be no jamming transmission [19]. This technique employs spectrum blocking and cannot distinguish between who is privileged

or not privileged. Once the spectrum is blocked no device can access the spectrum. In the case of contacting emergency services (police, fire, and ambulance) this system cannot identify emergency calls and therefore is not recommended.

2.4.3 International Mobile Subscriber Identity (IMSI) Catcher

An IMSI catcher is a simple man-in-the-middle attack device that pretends to be local cell phone tower. When close to a mobile phone, the mobile phone sees the IMSI catcher as another cell phone tower with a much stronger signal and connects to it. IMSI catcher is used for monitoring and tracks mobile phone movement within a particular area [20]. IMSI catcher does not have an identity storage of users (privileged users) and cannot perform selective blocking of communication.

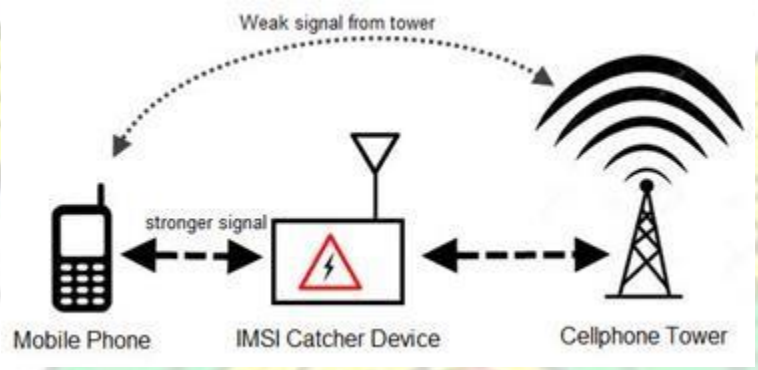

Fig. 2.1: IMSI catcher interrupting communication between a mobile phone and a cell phone tower [23]

2.5 Interception systems

An interceptor is a device that helps to block undesired communications inside protected areas, according to the user identity. There are two types of interceptors: Passive and Active interceptors.

A passive interceptor is used to monitor GSM & UMTs protocol exchange between the Base Station (BS) and the Mobile Station (MS) [5]. Passive interceptors cannot be easily detected by the mobile

phone user and forms mostly part of the operator's network [21]. Once a passive interceptor has obtained MS identities, and depending on the way, these identities are processed, two different scenarios may result: Remote Identity Scenario and Local Identity Scenario (LSI) [5]. Active interceptors are MITM (man in the middle) devices designed for cellular networks. Originally developed to steal IMSI (International Mobile Subscriber Identity) numbers from mobile phone users [22]. An active interceptors are also used to listen to voice calls, monitor text messages and capture forensic data [21]. Active interceptors can easily be detected by the mobile phone user or the network operator and does not form part of the operator's network [10]. Active interceptors do not have an identity repository and cannot perform under the 3G and 4G networks due to mutual authentication. However, ongoing work is being done to that effect [22].

2.5.1 Remote Identity Scenario (RSI)

In this scenario, MS identities are transmitted to a corresponding mobile switching centre (MSC) for blocking. It is assumed that the MSC and the interceptor are linked in a metropolitan-area network [13]. It is possible to choose a particular MSC from a group of different service providers, since the interceptor knows the carrier in which the identifier message was embedded [5]. Once the MSC knows that a particular MS is present in the monitored target area, it may block its activity during a period of time [5]. This approach requires a permanent communication between the MSC and the interceptor, which may not be available. To implement real-time blocking, the connection must also be fast and reliable hence is suitable in UMTs networks.

2.5.2 Local Identity Scenario (LSI)

In this scenario, a local jamming device is required for blocking. This device generates interferences that affect active carriers. Hence, it blocks MS activity [5]. The interceptor obtains MS identities

and checks them in a local identity repository [13]. If they are not listed there, or are not privileged, the interceptor triggers the jammer at convenient slots, blocking specific MS communications. In this case, the selective interceptor may include an RF unit that decides if an MS is located inside a target area [5]. This approach also requires communication between the MSC and the interceptor. However, it only takes place from time to time, in order to reload the identity repository. Connection speed does not compromise real-time blocking. The GSM network seems an adequate choice to implement a link between the interceptor and the MSC, since it is already present.

2.6 Related Works

J. Vales-Alonso et al. [8] proposed and built an experimental real-time GSM terminal detector [9], to be located in a cell phone restricted area. All idle terminals (mobile phones) entering the restricted area were forced to emit signalling information, which can be captured. In the following year, the group exported the idea into 3G UMTS [5] . The authors analysed detector protocol settings and response time. The system function was only to detect mobile phones entering the restricted area.

Ulrike Meyer and Susanne Wetzel presented a man-in-the-middle attack on the UMTS network. The attack allows an intruder to impersonate a valid GSM base station to a UMTS subscriber regardless of the fact that UMTS authentication and key agreement are used [6]. The study proposes how a rogue BTS can authenticate an actual UMTS e-node B and impersonate the network. The system cannot perform selective blocking of communication.

González-Castaño et al. [7] developed a real time interception systems for the GSM protocol. In their paper, they presented three interception systems for security purposes. The first one (detector) forces all MSs nearby to generate activity, which can be utilized to activate an alarm of Mobile Station (MS) presence. The second one (selective interceptor) displays information exchange between MS and BS and, in the case of MS activity:

1) Extracts messages containing MS identities

2) Checks identities in a local cache to decide if an external jamming unit should block individual calls.

The third system (enhanced selective interceptor) syndicates the previous two systems to improve blocking performance. In subsequent years, they developed an interceptor for the UMTS Terrestrial Radio Access Network. The function of this interceptor is to help the UMTS Core Network to block undesired communications inside a mobile phone restricted areas, according to user equipment (UE) identity [13]. These interceptors monitor GSM and UMTS transactions and, if necessary, block non-privileged calls using external jamming units. When these jamming units are activated over a specified spectrum, no other device can access the spectrum. The use of jamming units to block calls becomes impractical when they are to disarm mobile phones over a longer period. Their study did not exploit blocking for other communication services. Nonprivileged users cannot contact emergency services during emergency scenarios. It is proposed that all mobile phones should have admission to emergency call services in the instance of an emergency (police, fire, and ambulance). Their study was focused on only blocking voice calls. One may ask what will happen if this system is implemented in security areas where transmission of sensitive information is not allowed. For an example pictures and videos. How will data connection on mobile phones be controlled in that restricted area? This system above all depends on the MSC in order to update its user identity

repository (passive interceptor). The system is part of the operator's core network and therefore not a standalone system. To have a standalone system that can operate autonomously in a restricted area, this system is not recommended.

Song Yubo et al. paper proposed a GSM/UMTS phone number catcher over the air by man-in-themiddle attack. This project was implemented using a pseudo base station with a mobile terminal, which can transmit any frames. While the mobile terminals are trying to access the attacker's system, the phone number catcher will capture the phone numbers of these mobile terminals [4].

The phone number catcher only detects a user's phone number but cannot connect users to the operator's network to perform selective blocking of communication.

Mesud Hadžialić designed and implemented an open-source IMSI catcher using USRP device to only send malicious SMS to multiple mobile phone users [12]. This system cannot perform selective blocking of communication.

Adam Kostrzewa proposed an approach to force to connect his system to a target's cell phone [10]. The system forces to disconnect users connected to an operator's network then connect them to it as a fake BTS. The system can work for one victim at a time and cannot perform selective blocking of communication.

Kenneth van Rijsbergen designed an IMSI catcher to monitor traffic exchange between a mobile phone user and its operator using Yate BTS and blade RF [11]. The IMSI catcher can only listen to information exchange between a mobile phone and its operator and cannot perform selective blocking of communication.

2.7 GSM network overview

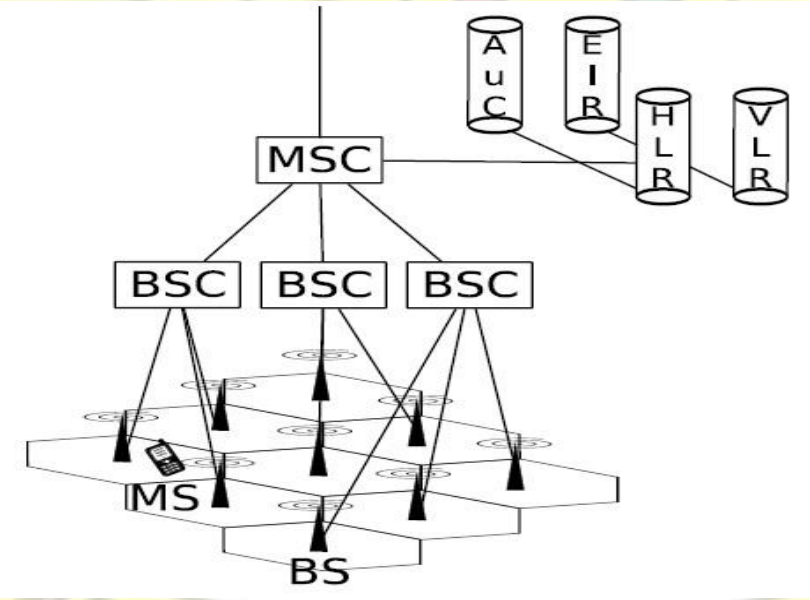

Fig. 2.2: Simplified GSM network architecture [23]

1) Mobile Stations (MS)

The Mobile Station (MS) is a device that enables a user to connect with a mobile network. It comprises two modules: Mobile Equipment (ME) and Subscribers Identity Module (SIM). The ME is a physical mobile phone. There are many frequency bands, the mobile station when connected to an operator's network uses one frequency band at a time. IMEI numbers have been designed for all mobile phone. This is assigned by the manufacturer [24].

2) Base Stations (BS)

Base Stations communicate directly with Mobile Stations. The first point of call of an MS to the GSM network is through the Base Transceiver Station (BTS). Speech encoding, encryption, multiplexing, and modulation/demodulation of the radio signals is controlled by the BTS [23] [24]

.

3) Base Station Controllers (BSC)

Multiple BS are controlled by the BSC. Allocation of radio channels, frequency management, power and signal calculation, and handovers are all managed by the BSC [24].

4) Mobile Switching Centres (MSC)

Multiple BTS are managed by the MSC. Call routing, call setup, and basic switching purposes which are controlled by the MSC. It additionally manages handovers between BSC and connection to other MSCs'.

5) Home Location Register (HLR)

Loading of phone numbers, present locations of MSs, IMSIs, roaming data are managed by HLR. The HLR is a database, which keeps track of all MSs' in the operator's network.

6) Visitor Location Register (VLR)

VLR is responsible for the location update of all network users in the network. To optimize the communication the VLA in conjunction with HLR keeps track of all network users in the network [24].

7) Authentication Centre (AuC)

In the GSM network, the Authentication Key (Ki) of each IMSI is stored by the AUC. The Random Number (RAND), Signed Response (SRES), and Ciphering Key (Kc) are generated by the AUC, which is later utilized for cryptographic operations [24].

8) Equipment Identity Register (EIR)

This supplies IMEI number of banned or stolen phones to prevent them from accessing the GSM network [23].

2.8 IMSI – TIMSI

The network operator apportions to each user with unique IMSI IDs. The SIM card keeps the ID as a 64-bit field, which is sent by MS later during call establishment. The IMSI ID is composed of 16 digits. Mobile Country Code (MCC) for Ghana is 620 [25].

Table 2.2: Various networks in Ghana and their MNC [25]

Network	MCC	MNC	Country code
Expresso Ghana Ltd	620	04	233
GloMobile	620	07	233
Milicom/Tigo	620	03	233
MTN	620	01	233
Vodafone	620	02	233
Airtel/ZAIN	620	06	233

Fig. 2.3: Composition of an IMSI number

Fig. 2.3 is an example of IMSI code structure where: 620 is the MCC code structure of Ghana,

MNC is 01 for the MTN GSM network. 0240536108 is the user subscriber number. Temporary International Mobile Subscriber Identity (TIMSI) is created periodically from the IMSI number for security purposes [24].

2.9 Mobile station registration to an operator's network

A radio interface is utilized to create a geographically limited number of radio cells by a mobile phone network. A cluster of location areas is divided into numerous cell sites. A mobile station will execute a full scan to find the available frequencies of nearby cells when it loses connection to it

operator network. The IMEI, IMSI number and a secret key kept on the SIM card are used by the MS to connect to the operator's network. The network operator will allocate a TMSI number for addressing purposes. The more frequently a network varies the TMSI it becomes difficult to trail a user [26]. The MCC, MNC, Location Area Code (LAC), and Cell ID (CI) are exclusively recognized by a cell in GSM [26]. When a Mobile Station tries to access the network, it must authenticate itself to the Base Station, although the reverse is not wanted. This procedure is outlined in Fig. 2.4 below. Foremost, the Mobile Station sends its security capabilities to the VLR (through the Base Station). This distinguishes the network what A5 encryption protocols it is capable of. The VLR then sends the Mobile Station an Identity Request command, which induces the Mobile Station to answer with its IMSI number. Now, having the IMSI, the VLR then sends an authentication parameter request to the HLR, which is sent to the AuC [27]. The AuC first produces a 128 bit random number, RAND, and calculates a 32 bit signed response SRES based on RAND and the deposited long-term secret key Ki that corresponds to the respective SIM:

$SRES = A3(RAND, Ki)$ $[VLR]$.

The AuC also generates a 64 bit session key Kc using the algorithm A8:

$Kc = A8(RAND)$ $[VLR]$

The random number RAND, signed response SRES, and session key KC is sent backwards to the VLR. Yet, only RAND is passed back to the Mobile Station. Using the secret key Ki put in storage in its SIM card, the Mobile Station can calculate:

$SRES' = A3(RAND, Ki)$ $[SIM]$

The Mobile Station, then sends SRES' back to the VLR. If SRES and SRES' do not agree, the authentication request is refused. Otherwise, it is taken and the VLR assigns the Mobile

Station a Temporary Mobile Subscriber Identity (TMSI) and tells it what cipher mode A5 to use.

The possible cipher modes include:

- A5/0
- A5/1
- A5/2
- A5/3

The TMSI is planned to increase security by dropping the number of times the IMSI is broadcasted, and serves to identify the Mobile Station in forthcoming transactions with the VLR. If any alternative other than A5/0 is chosen, the Mobile Station calculates the session key KC used in the A8 algorithm on the input RAND, as shown below. The chosen A5 algorithm is then applied to encrypt all subsequent communication between the Mobile Station and Base Station:

$CIPHER = _A 5(Kc, MESSAGE)$

The session key Kc continues to be used as long as no new authentication request is started. In practice, the same session key may stay in use for quite some time, extending to preceding calls.

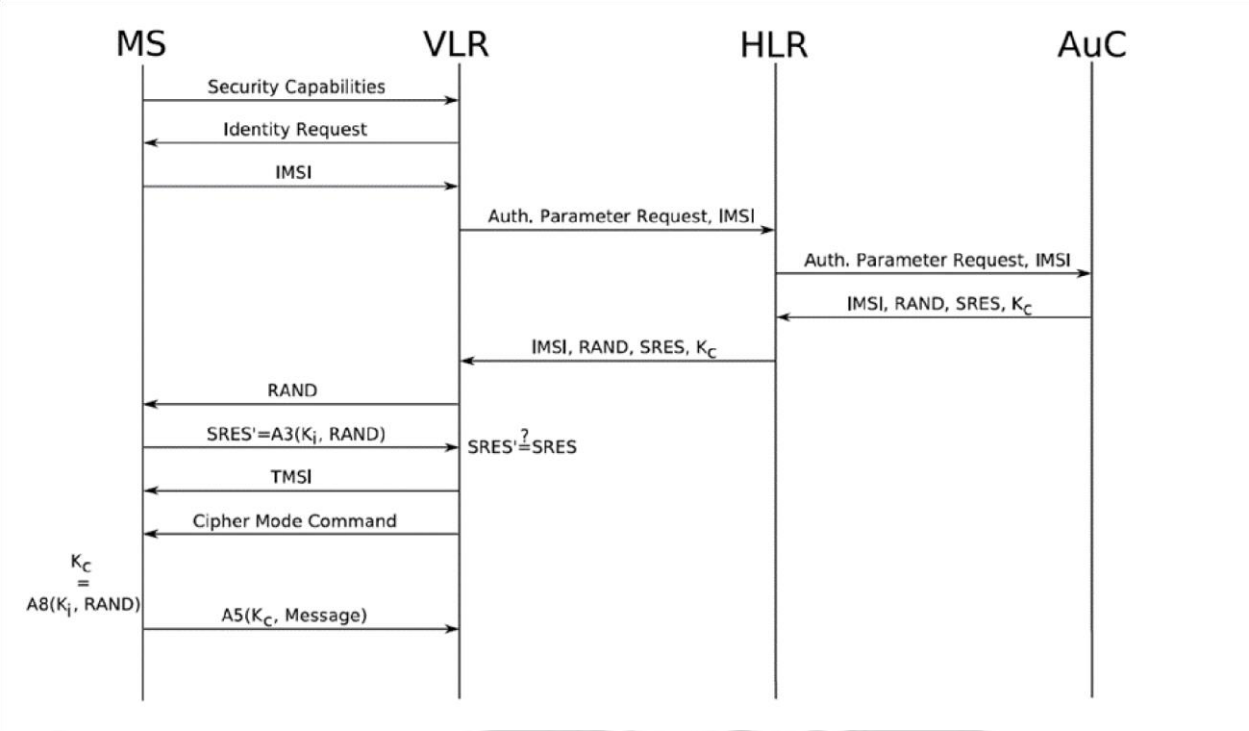

Fig. 2.4: GSM Authentication Procedure

2.10 Exploitation of Active interceptors (IMSI Catcher) on GSM Weakness

The baseband is a central element that manages all of the mobile phone's communications with cell towers owned by several carriers. The baseband turns signals received over radio waves into digital packets and passes along the ones that contain bits of audio from a call or internet data to the CPU. The baseband constantly communicates with at least one cell tower that it can communicate with, based on the list of preferred towers provided by the user's carrier and signal strength [28]. Only the mobile phone needs to authenticate to the operator's network in GSM networks, but not vice versa. This empowers an attacker to intercept a user's communication with a legitimate BTS [29]. Mutual authentication is required for UMTS networks but can be evaded using the GSM compatibility layer [30], or downgrade the communication to a 2G connection by means of jamming.

At a glance, the GSM authentication procedure has a major weakness, which is:

- The one-way authentication process requires the Mobile Station to authenticate itself to the Base Station, but does not require a Base Station to verify its identity to the Mobile Station.

2.11 Exploiting GSM Weakness to connect the proposed system to MS in MS restricted area

The aim of the thesis is to check the likelihood of selective blocking of mobile phone communication in a mobile phone restricted area. The target's mobile phone is forced to communicate with a mobile network operator through the attacker's system in the man-in-themiddle attack. The attacker will get the opportunity to listen in conversation when successful. Then full control will be gained over the connection. The target user will not realize that his connection is been tapped when this is conducted properly. Two deficiencies of the GSM security have made man in the middle attack possible. Firstly, is one-sided authentication which means a subscriber cannot validate between a genuine and rogue network. Secondly, is the limitation of the A5/2 cipher. An attacker can obtain the Kc code when an MS is communicating to a BTS [24]. Fig. 2.5 explains a typical attack scenario where four elements interact with each other. The target user – will be called "MS" later in the text. Attacker's BTS– will be called "fake BTS" later in the text. Attacker's MS – will be called "fake phone" later in the text. The real network operators BTS –will be called "actual BTS" later in the text. The first attack stage is to obtain the target's mobile phone identity. For this scenario, the MS is tricked to connect to a fake BTS station. The attacker secures the target's IMSI, which he will use to register the fake phone to the actual operator's network. In exchange will obtain a Random (RAND) number. Then target's MS will receive the RAND which

has been obtained from the actual network through the attacker's network. At this point, the target's MS will send a calculated Signed Response (SRES) to the attacker's system. MS will start encryption with the attacker's signal. The attacker will break the A5/2 cipher and obtain the Kc code. This will be sent to the actual GSM network. Within moments, all traffic conversation between the MS and the actual BTS goes through the attacker's system. Fig. 2.5 depicts the attack scenario

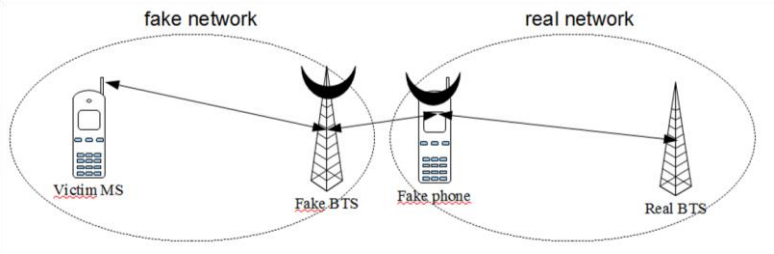

Fig. 2.5: Connecting the target user to the operator's network

This idea can be imported when implementing the proposed system. That is the proposed system should bridge the connection between the mobile phones and the operator's network in the restricted area. When mobile traffic from mobile phones in the restricted passes through the proposed system, non-privileged users can selectively be blocked according to the communication service prohibited for the restricted area.

2.12 How a mobile phone would connect to the proposed system

2.12.1 Connecting with mobile phones

There are three approaches to connect mobile phones to the proposed system. Firstly, the target user may feel reluctant to switch cells when connected to a BTS of a better signal. Target's user

can be disconnected from the original network and register to the proposed system by the use of an RF signalling channel jammer. The RF signalling channel jammer only disrupts the signalling channel of the network operator to which the target user is connected. In this case, the proposed system should make available the subsequent parameters of the actual operator's network: MCC, MNC, and network short name. The target's user will eventually drop back to a full scan mode, after an ineffective scan of the advertised neighbor frequencies. This will, therefore, give the proposed system the opportunity to connect with the target's phone.

Secondly, to increase signal quality, avoid radio interference, and thus trigger the mobile provider's own radio quality monitoring system, an attacker has to use an unused frequency (i.e. ARFCN, Absolute Radio Frequency Channel Number) for its IMSI Catcher. A relatively safe choice for a frequency are unallocated radio channels (e.g. guard channels between different operators or reserved channels for testing). However, it is less likely to lure a mobile phone onto this channel, as the phone (MS) will preferably only look on the advertised neighbour frequencies [26].

The third method is to use an advertised frequency that is actually not being used or is not receivable in the specific restricted geographical area under attack [26]. Typically, an attacker will introduce a new cell ID (preferable including a new LAC) previously unused in the specific geographical region for two reasons: First, to not provoke an accidental protocol mismatch when the MS should receive the corresponding genuine BS by accident. Secondly, to provoke a Location Update Request from the phone to be able to lure it in the fake cell.

2.12.2 Involuntary BTS selection Scenario

The BTS will send a neighbour list over an unencrypted connection when the mobile phone connects to the BTS. BTSs in the near location contains this list of frequencies. The BTS with the best signal strength will be selected based on the information presented to the mobile phone. The target's mobile phone may not recognize the fake BTS when is switched on. This may be because the target's mobile phone may be connected to other BTSs'. The fake BTS may send a signal, which will be stronger than any of the BTSs' to the closest location knowing the frequencies of those BTSs' [24]. This signal should be send on the frequency of the base station with the weakest one. The mobile phone will change its BTS automatically when the received signal is stronger than that signal of the existing connection. When the mobile phone is in the standby mode and no live communication is taking place this condition should work. The exemplary scenario is depicted in Fig. 2.6. In this scenario, the MS is connected at the beginning to the BTS 1. MS knows about the nearest BTS stations, particularly: BTS 2, BTS 3, and BTS 4. The attacker will check the frequency channel of each BTS available. After, when he switches on his fake BTS it will start to send a signal on the same channel as the BTS 4, which was resulted during the attacker's measurement of the worst signal quality. The MS will notice that the quality of the signal from BTS 4 has improved and will switch onto it. Therefore, in this way the victim's MS has been lured to connect to the attacker's fake BTS.

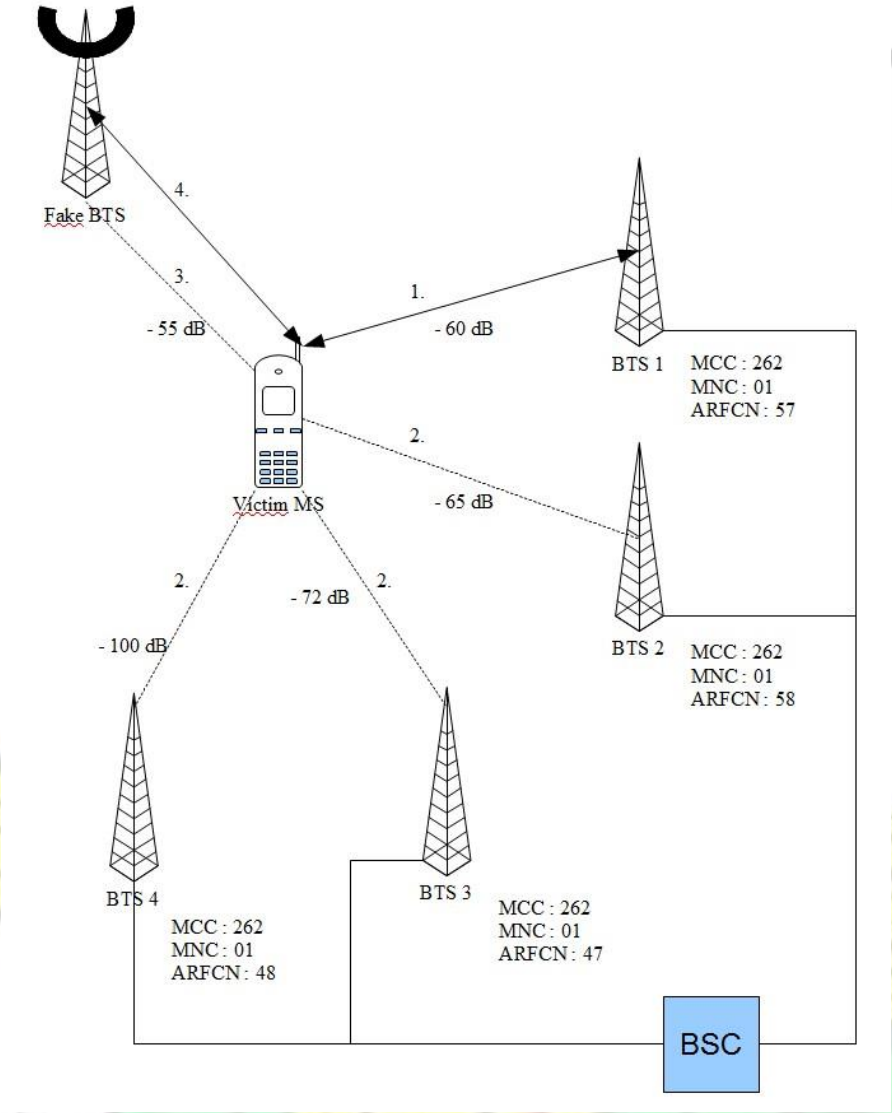

Fig. 2.6: Involuntary BTS selection scenario [31]

2.13 Encryption

IMSI Catchers are likely to disable encryption (set cipher mode A5/0) in order to ease monitoring. However, current state-of-the-art attacks on GSM A5/1 and A5/2 cipher allow for a timely decryption and key recovery. GSM Association found some flaws in the A5/2 cipher [26]. By means of rainbow tables, the stronger variant A5/1 is also prone to attacks. These are publicly

available [26]. Helpfully, the modern A5/3 and A5/4 ciphers are effective [32]. However, this encryption will force attackers to downgrade the encryption to a lower encryption for the man in the middle attack especially IMSI Catchers. The identified attacks on A5/3 are not yet realistic [33] [34] [35].

2.14 How the proposed system connects mobile phones to the operator's network

The proposed system will forward calls, data, SMS and emergency calls to the PSTN network. There are multiple ways to achieve this. The simplest solution is to use another SIM card and a MS to relay calls into the mobile network. However, from the networks point of view these calls will be made under another identity. The proposed system will most likely disable caller ID presentation to not immediately alarm the recipient. In this setup, the proposed system will not be able to handle any incoming calls for the surveyed station. Another setup could route these calls directly into a SS7 phone exchange network. Telecom operators usually trust their wholesale- and exchange partners with provider grade connections to set legitimate caller IDs. An attacker with access to such an interface could also spoof caller ID for outgoing phone calls and text messages. However, it is unlikely that the attacker can also manipulate the routing of incoming calls. A third setup option (a full MITM attack) could facilitate a more advanced GSM frame relaying setup where data is handed over to the original network as if it where send by the victims phone.

Chapter 3

Research and Methodology

3.1 Conceptual Framework of the Proposed System

The proposed system will be evaluated by simulation using fuzzy inference system toolbox integrated in matlab. The fuzzy inference system will simulate the decision making process of the proposed system. The proposed system acts as a filter, which determines what service (call, SMS, data and emergency calls) a mobile is allowed to enjoy in the restricted area. Fig. 3.1 shows the system model. Within the identity storage and decision-making unit, is a register, which contains specific mobile phone locations and their permitted communication services. The identity storage and decision-making unit also contain user identity storage for privileged users for each location. That is for every restricted location there are privileged users. The system will grant mobile phones access to communication-based on the type of communication service allowed for the specific location. Special numbers have been allocated to each specific location (museum (2), hospital (3), banks (4), and school (5)). These numbers indicate the location setting of the system. Privileged users for each specific location is given a special tag number 1 and non-privileged users are automatically tagged the value number of the specific location, which they are connected. The mobile phone detection and identity capture unit is responsible for capturing a user's IMSI number and connecting users to the system. If a mobile phone user is granted access, the user's IMSI number will be imprinted on the clone mobile phone. Then connected to the operator's network. When the communication is established between the clone mobile phone and the operator's network, then the communication bridge forwards the communication from the clone mobile phone and the operator network to the user in the restricted area. This forwarding by the communication bridge is done

through the mobile phone detection and identity capture unit. This form of communication can be established for both GSM and UMTS networks.

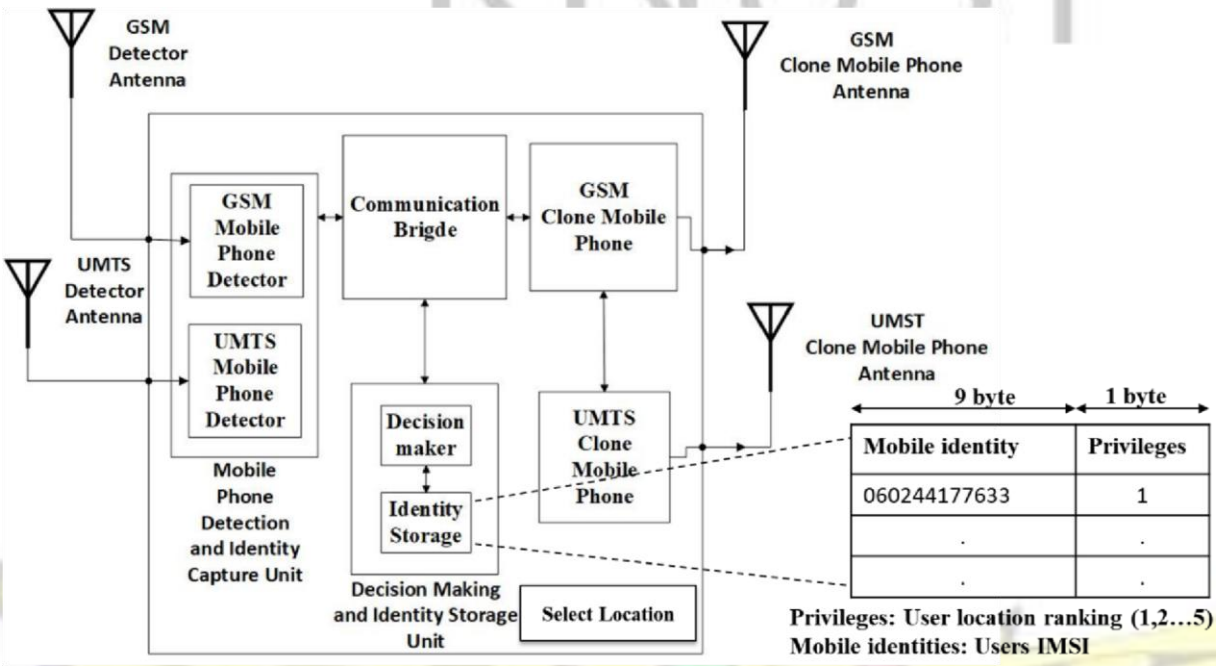

Fig. 3.1: A selective mobile phone communication blocking system (Source: Field work)

3.2 Fuzzy Inference Systems

Expert systems are computer programs, designed to make available some of the skills of an expert to non-experts. Expert systems function by acquiring knowledge from rules and fact in its database. The fuzzy inference system is a computer program, which employs rule-based systems. It uses ifthen rules (if the data meets certain particular conditions, then take appropriate actions) represent expert reasoning. The fuzzy inference system (FIS) incorporates the skills of an expert in solving in its domain. The use of fuzzy inference system can be characterized to accept numbers as input, and then translates the numbers into linguistic terms such as high, medium and low (fuzzification). Rules then map the input linguistic onto another linguistic term unknown as output. The output

linguistic terms are translated into output numbers (defuzzification). The proposed system can be modelled into an expert system using fuzzy inference system where specific restricted mobile phone locations are tagged some numbers and are characterised as input to the inference system. The rules will be characterised by the communication services allowed or restricted for these locations. The decision output will be the type of communication service allowed or restricted for those specific locations.

3.3 Operation of the Fuzzy Inference System

There are two types of FIS: Mamdani-type and Sugeno-type. The main difference between both the types is the way in which crisp output is generated from fuzzy inputs. Mamdani-type FIS uses the technique of defuzzification of a fuzzy output, while Sugeno-type uses the weighted average to find crisp output. Hence, Mamdani FIS has output membership functions while Sugeno FIS has no output membership function. Mamdani is widely used because it allows describing the expertise, more human like manner. Therefore, the type of FIS used in this thesis is the Mamdanitype. Fuzzy inference system is based on a set of IF-THEN rules and Membership Functions (MFs) of variables for a particular system to be modelled. In general, FIS has several principles. Real input values are given to the antecedent part of the rules (fuzzification), the degrees of truth of the antecedents are calculated and imposed onto the consequent of the rules (inference), the obtained outputs of the fired rules are merged (composition) and, finally, the result is given back to the crisp domain (defuzzification), in order to enable a precise actuation in the actual system. The operation of the process is described in Fig. 3.2.

In fig. 3.2,x represents the input (crisp) value, μ(x) represents the fuzzified output value, and μ(u) represents the result of inference operation and u represent the final output value. The definite (crisp) data in the input of the classifier is converted by the fuzzifier unit into linguistic variables. The fuzzy knowledge unit consists of two subsystems: (i) database and (ii) rule base. The database subunit defines the system's variables using fuzzy set, whiles the rule base subunit also performs an inspection of rules essential to obtain the actual output. Inference unit does the thinking and performs inference on the fuzzy rules. The Defuzzifier unit then converts the fuzzy values acquired from the inference unit into numerical (crisp) values. These numerical values are the final results from the inference system and are understandable by the user.

3.4 Definition of rules

The main goal of fuzzy inference system is to represent an input space to an output space, and the key mechanism for causing this is the list of 'IFTHEN' statements, which are known as rules. The

rules are the inputs for constructing the FIS.

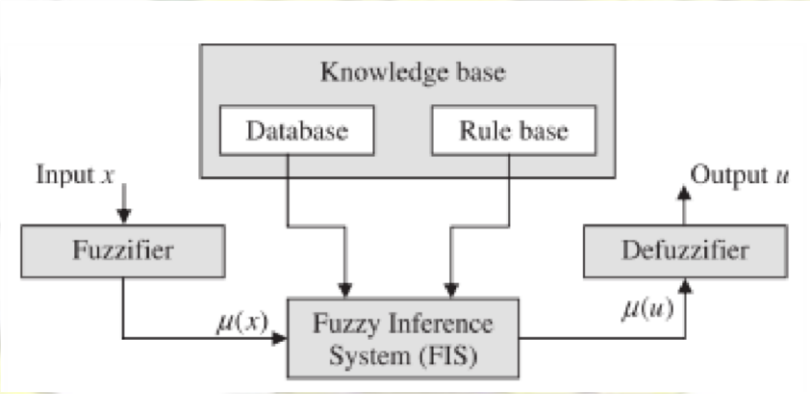

Fig. 3.2: Fuzzy logic classifier

3.5 Fuzzifier Unit

Measurements of input variables are performed by the fuzzifier unit. The crisp input measurement with arithmetic values are changed into Fuzzy measurements and all input variables are measured.

This translation is accomplished using membership functions. From set theory, a crisp set is a set, which holds solid definition of its bounds. For an instance, a set (A) can be made up of real numbers larger than 10, which can be expressed equally as,

$$A = \{x | x > 10\}$$

Any number that is more than 10 cannot be a member of the set since the boundary has been perfectly defined. Because of the precise decision given it can be understood that a particular number is either a member or not a member of the set.

Fig. 3.3: Fuzzy Inference process

In the fundamental concepts of human reasoning, many situations may be found when human thoughts are abstract and imprecise. There is also no precise boundary for decision-making. Sensors for controlling room temperature is an instance. The sensor can be fixed to a specific value, such as 70 degrees, as a high temperature for a given room. When the temperature of the room measures 69.5 degrees, it will read not hot. When imported into the human concepts, there will be no difference in temperature between 69.5-degree and 70-degree. The degree of abstractness can be perfected using fuzzy set, which is not limited in terms of its crisp boundary.

The following is a set of ordered pairs defined by a Fuzzy set as A in x:

$$A = \{(x, \mu A(x)) | x \in X\}$$

Where μA is termed as a membership function for the Fuzzy set A. A membership function must satisfy the condition of variation between 0 and 1. The membership function maps each element of X to a membership value between 0 and 1. The collection of the object X is denoted as the universe of the disclosure. Continuous or discrete objects together form the universe of the disclosure. If the universe of discourse X is a continuous space, they may be segmented into several fuzzy sets and referenced according to linguistic terms, such as ”large,” ”medium, ” or ”low.” These values are called linguistic values or linguistic labels.

Fuzzy Sets member variables are determined by the membership function against the degree of truth for a user input value. A membership function (MF) can be defined as a curve that defines how each point in the input space is mapped to a membership value (or degree of membership) between 0 and 1. The input space is sometimes referred to as the universe of discourse. Membership functions can possess the form of a triangular, trapezoidal, Gaussian, bell-shaped and sigmoidal. The choice of a membership function is based on the shape of a curve that can be defined as a function to suit the point of view of simplicity, convenience, speed, and efficiency. The simplest membership functions are formed using straight lines. Of these, the simplest is the triangular membership function, which will be considered as the input membership function to the fuzzy inference system of this thesis. This is because the apex point of the triangular membership function is able to map single input values to a membership value between 0 and 1.

3.6 Knowledge Base

The knowledge base is a fuzzy reasoning process, which involves linguistic control of rules. The fuzzy controller works together with the data and the rules concurrently to regulate the output after

receiving an input from the user. The data provide the information for the linguistic control rules, and the rule base specifies the control goals. The rule base contains a set of if-then rules. The rules are generated in many ways, depending upon the problem domain. Rules can be formed in a combination of user experience, expert's domain knowledge, modelling the action of the operator, process observation, and gradual learning, etc.

3.7 Inference Engine

The fuzzy inference Engine is the heart of the fuzzy controller, which performs control functions. To obtain the results the inference engine works with the linguistic variable. "Mobile Stations" may be considered as input linguistic variables to the fuzzy system. "very high", "high", "medium", "low" and " very low" are the expressed linguistic terms which quantify the input values of the inference system. The rules map the fuzzy inputs to fuzzy outputs through the inference engine when the linguistic variables and their values are defined. User inputs are triggered by the inference engine base on if-then rules. If x is A, then y is B, where A and B are linguistic values defined by Fuzzy Sets on X and Y, respectively. "x is A" is the antecedent, or premise, while "y is B" is the consequent, or conclusion. In this way, all input variables are converted into linguistic variables, and Inference Engine evaluates the value within the set of ifthen rules. Then, a result is obtained with the linguistic variables in Fuzzyfied form.

3.8 Defuzzification of fuzzy inputs

Defuzzification is the process of converting output-defuzzified values into crisp values. The inference engine rule-generation process is similar to the defuzzification process, which consists of

scale mapping factors. Membership functions are also used by the deffuzzifier to produce the actual output. There are several defuzzification techniques, such as Centroid, Bisector, Middle of Maximum (MOM), Smallest of Maximum (SOM), and the Largest of Maximum and so on. In this thesis, the Mamdani fuzzy logic model is used. To achieve accurate output decision results Middle of Maximum (MOM) method is used for defuzzification in this work. The Middle of Maximum method measures the central tendency of output-defuzzified values and gives an approximated crisp output value for an input crisp value.

3.9 Input variable

3.9.1 Triangular Membership Function

The triangular membership function is a collection of three points forming a triangle. The triangular membership function is defined by a lesser boundary 'a', higher boundary 'b', and a value m, where $a < m < b$.

$$\mu_{\mathrm{A}}(X) = \begin{cases} 0, & X \le a \\ \frac{x-a}{m-a}, & a < X \le m \\ \frac{b-x}{b-m}, & m < X \le b \\ 0, & X \ge b \end{cases} \quad \ldots\ldots\ldots\ldots\ldots (1)\ [36]$$

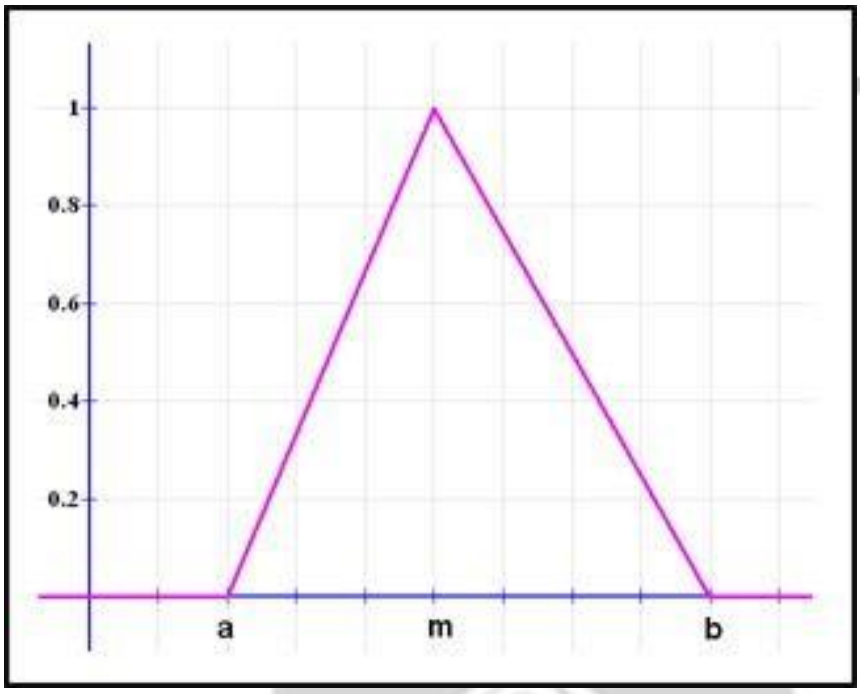

Fig. 3.4: A graphical representation of the lesser boundary a, the higher boundary b, and the value m

Fig. 3.4 defines a triangular membership function. A triangle has three vertexes, two vertexes that can form the base of the triangle and an apex point or vertex. In Fig. 3.4, point base 'a' and 'b' form the lower and upper limit of the triangular membership function. The lower and upper limits define span base of the triangular membership function. The vertical axis defines the height of the triangle with a minimum height of 0 and a maximum height of 1. For in this work maximum height is preferred to attain sufficient results. The apex holds the value m of the triangular membership function. In this work, the value m holds the value of the numbers tagged to the various user classes in Table 3.1.

Illustrated in Fig. 3.5 is an example from equation (1) where $a = 3$ and $b = 8$. This defines the lesser and higher limits respectively of the triangular membership function. The height of the triangle is 1. The value of the triangular function is $m = 6$. Therefore, $m = 6$ can represent a user location or user class ranking tagged number 6.

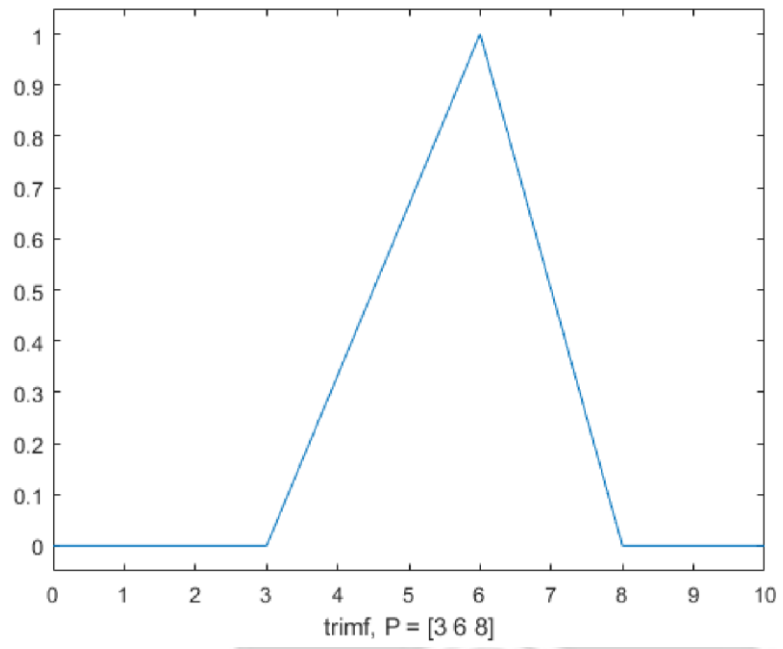

Fig. 3.5: A graphical example of a triangular membership function with defined values

3.10 Output Variables

Considering that a truth-degree is the degree of a proposition being true, while a flexible proposition is always true with a certain degree, and the range of truth-degrees is [0, 1]. The "true" in truth-degreed logic should not refer only to absolute truth, i.e., truth-degree 1, but should be

"truth with a certain degree with infimum 0", i.e., truth-degree >0. With this under- standing, the validity of an argument form in truth-degreed logic can be defined [37]. In order to facilitate description, the "true" can collectively be defined with a certain degree with infimum 0, i.e., the truth-degree >0, to be degree-true. In dual, the "false" can be called with a certain degree with supremum 1, i.e., the truth-degree <1, to be degree-false. Although degree-true inference is a kind

of reasoning method, it is only suitable to such unconventional sentences as “if x is A to a certain degree, then y is B to a certain degree” whose meanings are ambiguous, and since the scope of >0 is too large, the conclusions obtained are also not precision. And, those flexible propositions involved in usual arguments are all the flexible propositions whose meanings are unambiguous such as “if x is A, then y is B”. From the logical semantics of the propositions [37], the truthdegrees of this kind of flexible propositions are all >0.5. This is to say, in usual arguments, whether the truth-degrees of premise >0.5 (but not merely >0) is should to be considered. Thus, the condition “truth-degree >0” in the definition of degree-valid argument form appears too broad and not practical. Actually, although a truth-degree of >0 is true to a certain degree, a truth-degree of >0.5 is more tending toward true. And from the complement law of truth-degrees, the truth-degrees of <0.5 are more tending toward false, as to truth-degree 0.5 is just “half true and half false”. In order to facilitate description, truth-degrees of >0.5 can collectively be called to be near-true and truth-degrees of <0.5 can also collectively be called to be near-false. Thus, 0.5 is just located in the intermediate between near-true and near-false, which is a watershed between near-true and near-false. On the other hand, [37] that the truth-degree of a degree-true tautology actually is always ≥0.5 and the truth-degree of a degree-false tautology is then always ≤0.5. Therefore, in this thesis, the degree of truth for an argument to be “true” can be specified in the range of values from 0.5 to 1 and the degree of truth for an argument to be “false” can be specified in the range of values from 0 to 0.4. In addition, the decision for the degree of truth for an argument to be “true” is defined as “Allow” and degree of truth for an argument to be “false” is defined as “Not Allowed”. These decisions are what will be used further in this work to either grant a user access communication or not in the restricted area.

In order to specify or define these degrees of truth the Z-Shape membership function and S-Shape membership function will be used. The Z-Shape membership function and the S-Shape membership function will be used to define the decision output of the fuzzy inference system. The Z-Shape membership function is a curve, which decreases from 1 to 0 on the y-axis with parameters "a" and "b" on the x-axis. This can be seen in the example depicted in fig. 3.6. The parameter "a" and "b" of the Z-Shape membership function in equation (2) will be used to define the degree of truth for "false" i.e. from 0 to 0.4 respectively since "near-false" was earlier defined as <0.5 between 0 and 1. The S-Shape membership function is a curve, which increases from 0 to

1 on the y-axis with parameters "a" and "b" on the x-axis. This can also be seen in the example depicted in fig. 3.7. The parameter "a" and "b" of the S-Shape membership function in equation

(3) will be used to define the degree of truth for "True" i.e. from 0.5 to 1 respectively since "neartrue" was earlier defined as >0.5 between 0 and 1.

3.10.1 Z-Shape Membership Function

The parameters 'a' and 'b' located at the extremes of the sloped portion of the curve in Fig. 3.6 is given by $f\ (x, a, b)$. The Z-shape in Fig. 3.6 is named because of the spline-based function of x.

In this work, the Z-Shape Membership Function is used to define a decision state of "not allowed" where there is a fall in the curve from one to zero on the vertical axis. This can be seen in the example illustrated in Fig. 3.6.

$$f(x;a,b)=\begin{cases}1, & x\le a\\ 1-2\left(\frac{x-a}{b-a}\right)^2, & a\le x\le \frac{a+b}{2}\\ 2\left(\frac{x-b}{b-a}\right)^2, & \frac{a+b}{2}\le x\le b\\ 0, & x\ge b\end{cases}\quad\ldots\ldots\ldots\ldots\ldots\ldots (2)\ [38]$$

When $a=3$ and $b=7$ are inserted into the above equation (2) and x defined by a range of values 1 to 10, Fig. 3.6 shows the results in a graphical form. The lowest point of the curve is defined as 'b' and the highest point as 'a'. It can be seen that the curve falls from 1 to 0 on the y-axis which can signify a negative response in decision making. Therefore, this membership function can be used to define a decision making the state of "not allowed" in this work.

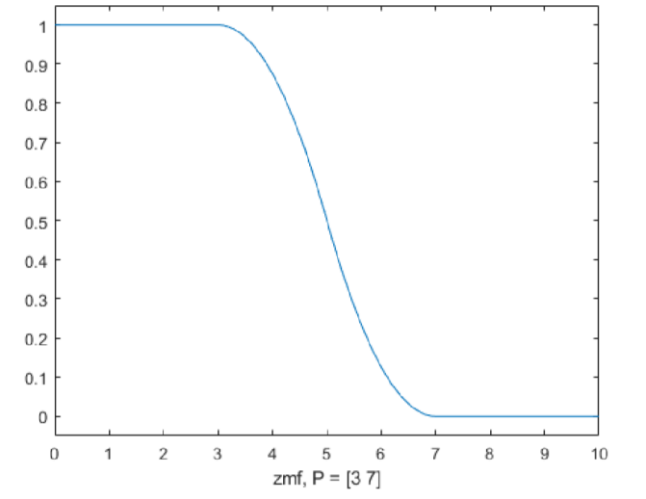

Fig. 3.6: A graphical example of a Z-Shape Membership Function with defined values

3.10.2 S-Shape Membership Function

The spline-based curve in Fig. 3.7 is a mapping on the vector x. The $f\ (x, a, b)$ plots the parameters 'a' and 'b' at the extremes of the sloped portion of the curve. It is termed for its S-shape. The S-Shape Membership Function is used to define a decision state of "allowed" where there is a rise in the curve from 0 to 1 on the vertical axis. This can be seen in the example illustrated in Fig. 3.7.

$$f(x;a,b)=\begin{cases}0, & x\le a\\ 2\left(\frac{x-a}{b-a}\right)^2, & a\le x\le\frac{a+b}{2}\\ 1-2\left(\frac{x-b}{b-a}\right)^2, & \frac{a+b}{2}\le x\le b\\ 1, & x\ge b\end{cases}\quad\ldots\ldots\ldots\ldots\ldots\ldots\ (3)\ [39]$$

When $a=1$ and $b=8$ are inserted into the above equation (3) and x defined by a range of values 1 to 10, Fig. 3.7 shows the results in a graphical form. The lowest point of the curve is defined as a and the highest point as 'b'. it can be seen that the curve rises from 0 to 1 which can signify a rise in decision making. Against the vertical axis, the curve rises from 0 to 1. Therefore, this membership function can be used to define a decision making the state of "allowed" in this work.

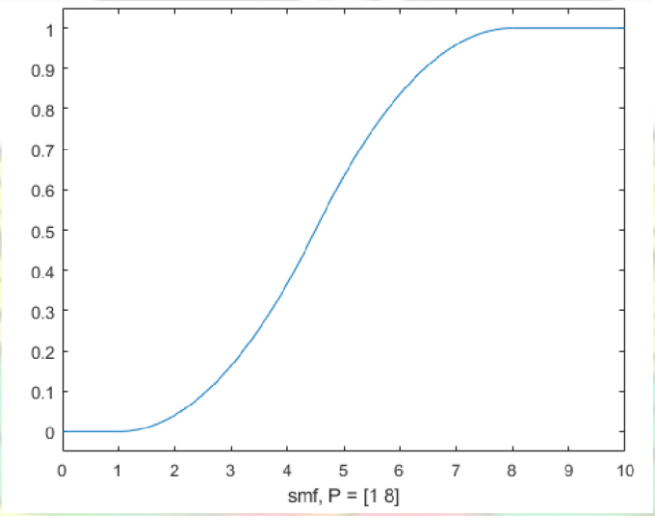

Fig. 3.7: A graphical example of an S-Shape Membership Function with defined values

3.11 Formulation of Simulation Parameters

Table 3.1: Decision table of services for eligible mobile stations

User Location	User Types	FIS Input Definition	User Class Ranking	Call Decision	SMS Decision	Data Decision	Emergency Call Decision
Hospitals	Privileged	Very High	1H	Allow	Allow	Allow	Allow

	Non-Privileged	High	2	Not Allowed	Not Allowed	Not Allowed	Not Allowed
Banks	Privileged	Very High	1B	Allow	Allow	Allow	Allow
	Non-Privileged	Medium	3	Not Allowed	Not Allowed	Not Allowed	Not Allowed
Schools	Privileged	Very High	1S	Allow	Allow	Allow	Allow
	Non-Privileged	Low	4	Not Allowed	Not Allowed	Not Allowed	Not Allowed

For the purpose of demonstration to test the decision making process of the FIS for the proposed system, table 3.1 was considered. Table 3.1 shows some mobile phone user locations with the services that they are restricted or allowed to enjoy. These locations are Hospitals, Banks, and Schools. Non-Privileged mobile phone users in these locations are not eligible to access any mobile phone communication as seen in table 3.1. Privileged users can be very important users in the restricted area. Therefore, privileged mobile phone users are eligible to perform all communication services with no restrictions as also indicated in table 3.1. User locations were converted into fuzzy logic using input triangular membership functions which are defined as follows; non-privileged mobile phone users for hospitals were defined as “High” with an input value of 2, non-privileged mobile phone users for banks were defined as “Medium” with an input value of 3 and nonprivileged mobile phone users for Schools were defined as “Low” with an input value of 4.

Privileged users in all locations were defined as “Very high” with an input value of 1. 1H, 1B and 1S represent privileged users in Hospitals, Banks and Schools respectively. This distinguishes privileged users among all the specified locations so that a privileged user from one location may not enjoy the same privileges elsewhere while he is not privilege there. However, all the allocations

assigned for privileged users in all the locations have an input value of 1 to the inference system. This is because all privileged users in all the specified locations enjoy the same benefit. The input values or user class ranking are the crisp inputs to the fuzzy inference system.

3.12 Simulation Setup

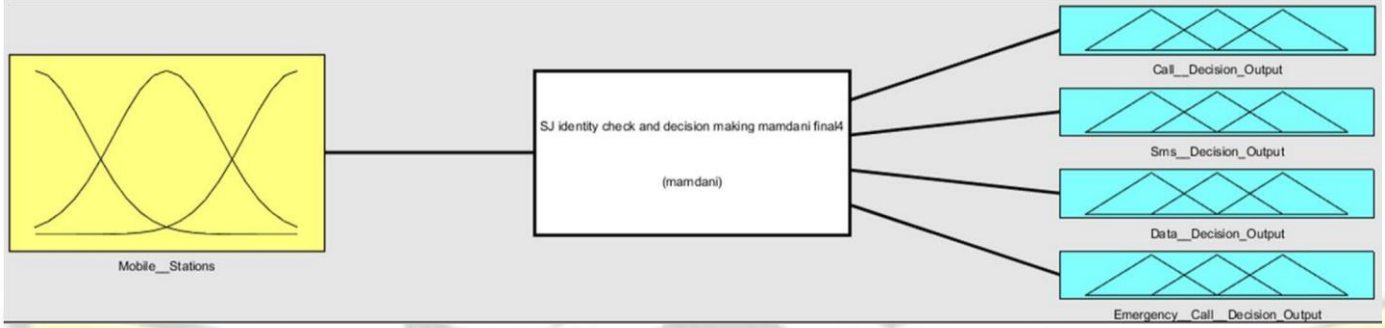

Fig. 3.8: Fuzzy Inference System for the Selective Blocking System

Fig. 3.8 shows a Fuzzy Inference System for the Selective Blocking System with one input and four outputs. In the fuzzification process, the first approach is to fuzzify the input variable and then, after defuzzify the output variables. The process involves the transformation of the crisp input values into fuzzy sets and fuzzy sets back into crisp output values. The input variable, mobile station contains the five membership functions of user locations as seen from Table 3.1. Each triangular membership function converts the assigned crisp input value of a user location into fuzzy values. The fuzzy output is defuzzified using z-shape and s-shape membership functions. The output defuzzied values are converted back into crisp output values (0 and 1). These crisp output values can be interpreted as “not allowed” and “allow” respectively. The decision making process of the FIS can be implemented using an OpenBTS, advanced IMSI catcher and software defined radio (SDR).

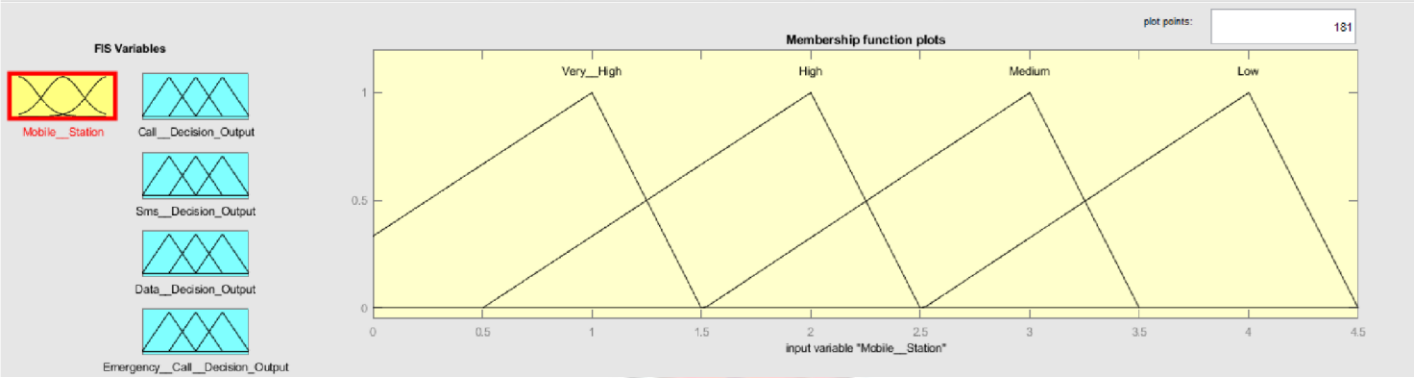

Fig. 3.9: Triangular Membership Function for Input Variable Mobile Stations

Fig. 3.9 shows the converted crisp input values of specific user locations into fuzzy values by triangular membership functions.

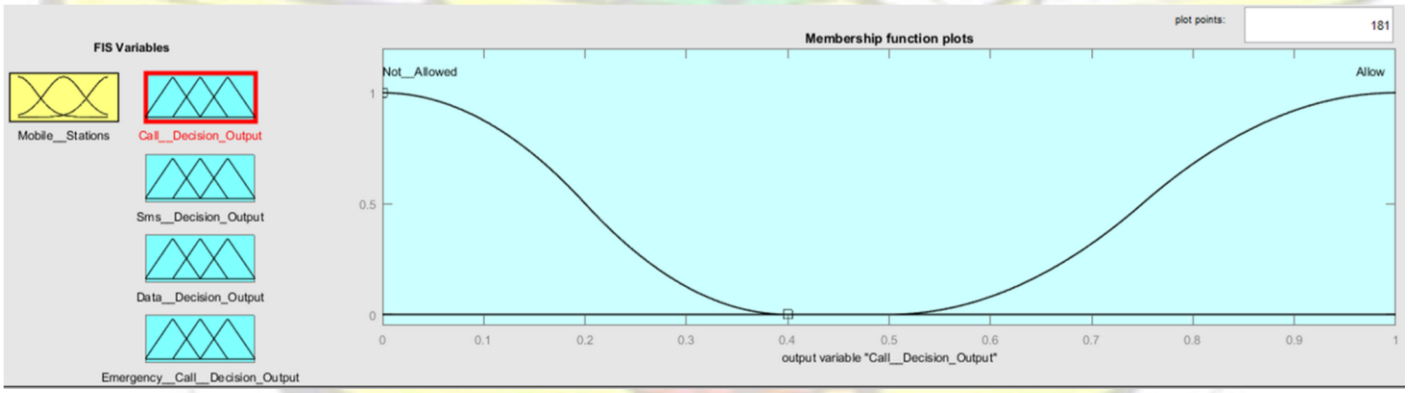

Fig. 3.10: Z-shape & S-shape membership functions for Output Variable Call Decision

Fig. 3.10 shows the Z-shape & S-shape membership functions for the Output Variable Call Decision. The Z-shape & S-shape membership functions were used to classify the defuzzified range of values between 0 and 1 into “Allow” and “Not Allowed”. Therefore, the range of values from 0 to 0.4 is classified as “Not Allowed” and between 0.5 to 1 is classified as “Allow”.

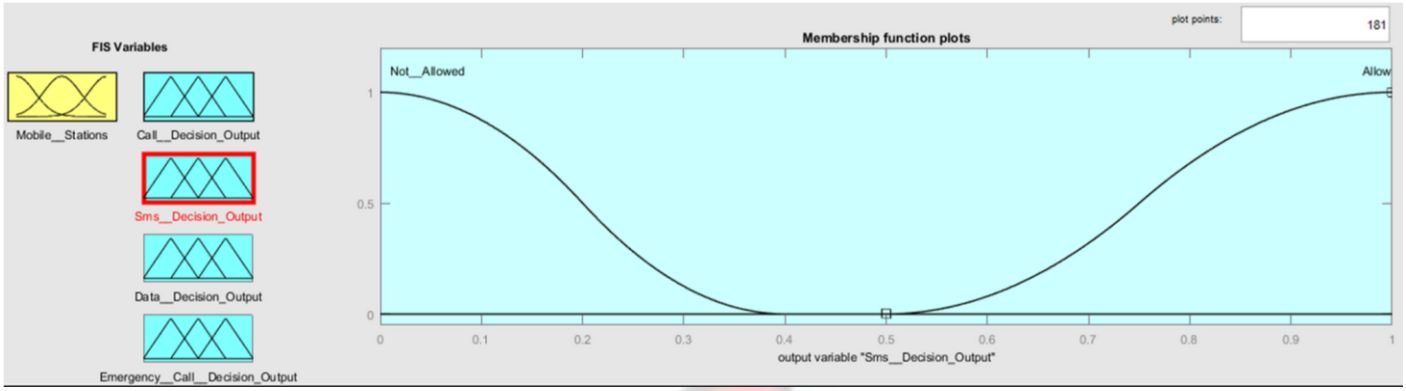

Fig. 3.11: Z-shape & S-shape membership functions for Output Variable SMS Decision

Fig. 3.11 shows Z-shape & S-shape membership functions for the Output Variable SMS Decision. The Z-shape & S-shape membership functions were used to classify the defuzzified range of values between 0 and 1 into “Allow” and “Not Allowed”. Therefore, the range of values from 0 to 0.4 is classified as “Not Allowed” and between 0.5 to 1 is classified as “Allow”.

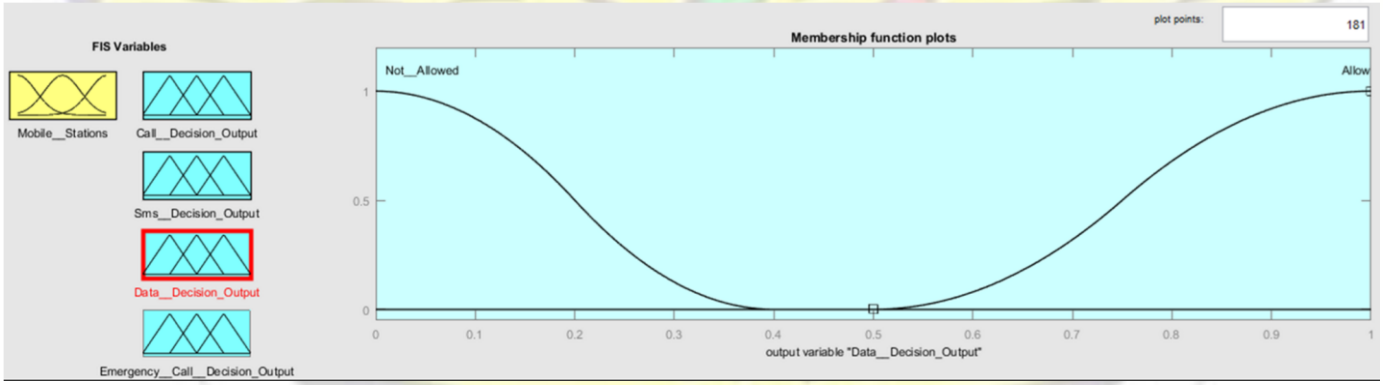

Fig. 3.12: Z-shape & S-shape membership functions for Output Variable Data Decision

Fig. 3.12 shows Z-shape & S-shape membership functions for the Output Variable Data Decision. The Z-shape & S-shape membership functions were used to classify the defuzzified range of values between 0 and 1 into “Allow” and “Not Allowed”. Therefore, the range of values from 0 to 0.4 is classified as “Not Allowed” and between 0.5 to 1 is classified as “Allow”.

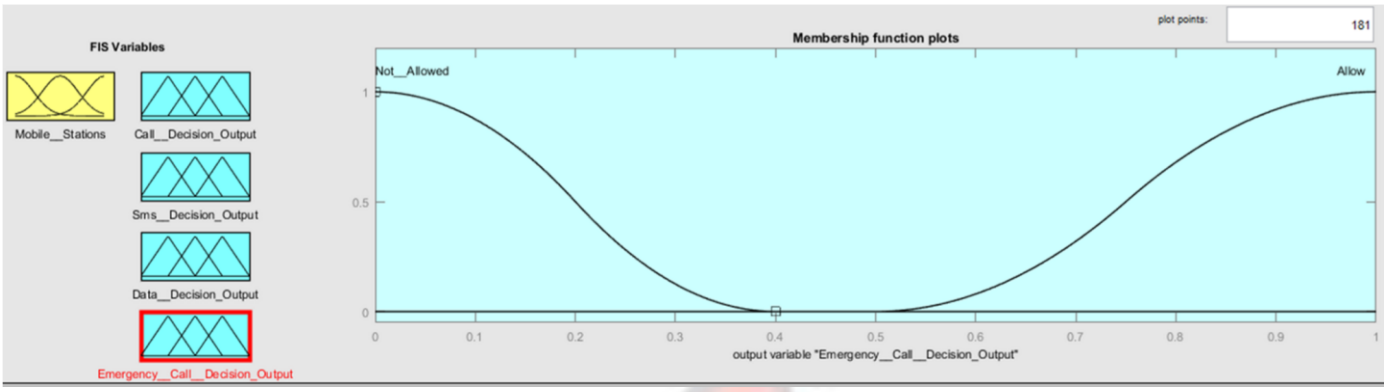

Fig. 3.13: Z-shape & S-shape membership functions for Output Variable Emergency Call Decision

Fig. 3.13 shows Z-shape & S-shape membership functions for the Output Variable Emergency Call Decision. The Z-shape & S-shape membership functions were used to classify the defuzzified range of values between 0 and 1 into “Allow” and “Not Allowed”. Therefore, the range of values from 0 to 0.4 is classified as “Not Allowed” and between 0.5 to 1 is classified as “Allow”.

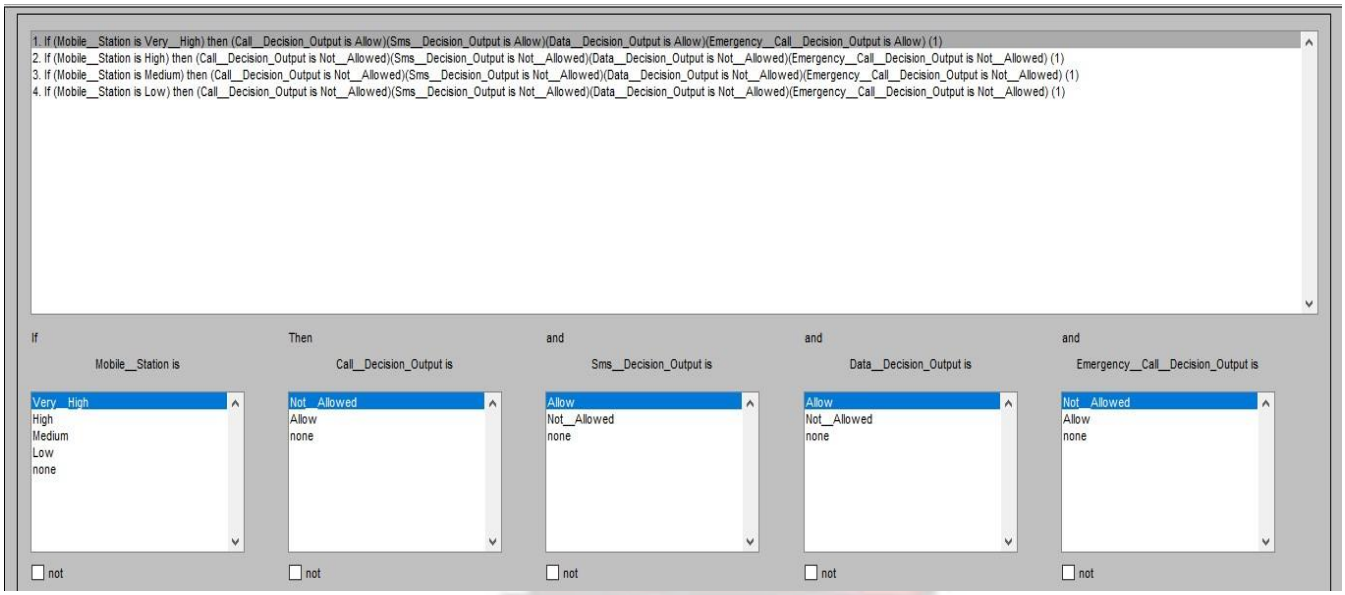

Fig. 3.14: Rule Editor for Decision Making

Based on the descriptions of the input and output variables defined with the FIS toolbox, the Rule Editor allows for the construction of rule statements based on the algorithm section 3.13, by clicking on and selecting one item in each input variable box, one item in each output box, and one connection item. Choosing none as one of the variable qualities will exclude that variable from a given rule. Choosing not under any variable name will negate the associated quality. Rules may be changed, deleted, or added, by clicking on the appropriate button.

3.13 Flow-chart for the decision making of the system

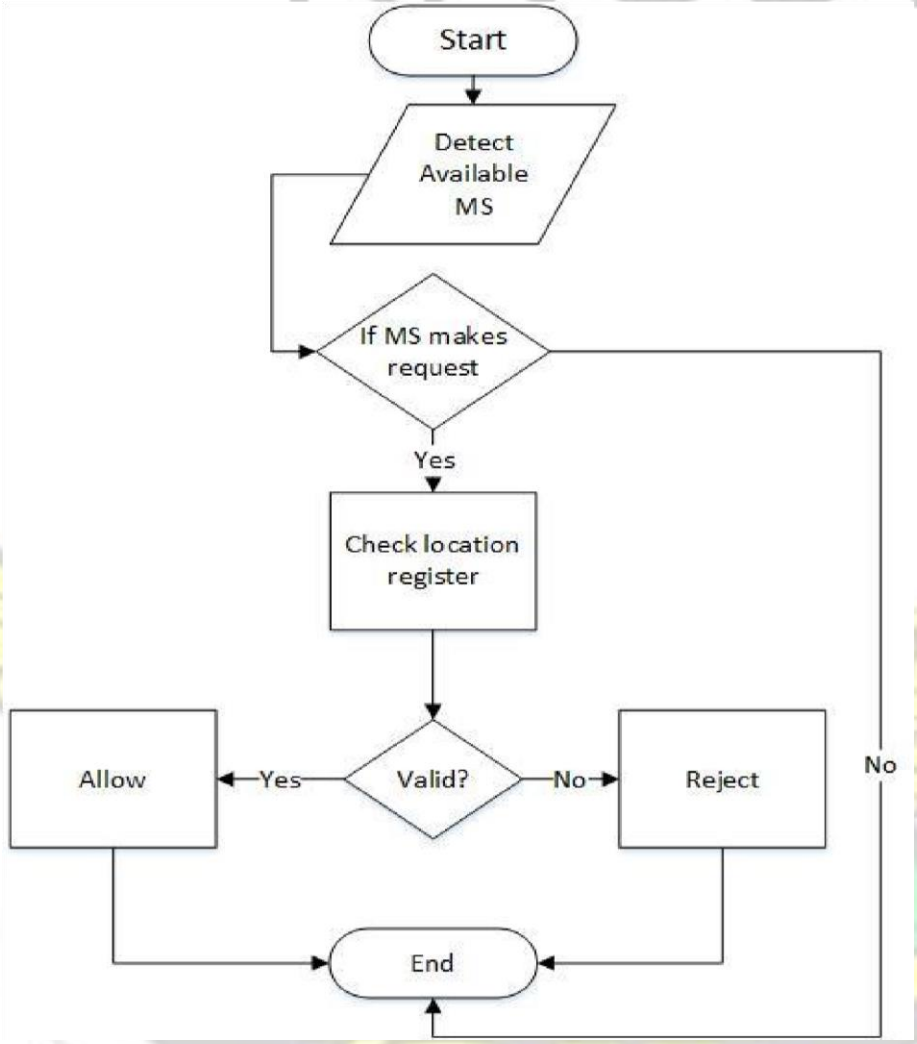

Fig. 3.15: Flow chart of selective blocking decision algorithm

Chapter 4

Results and Analysis

4.1 Description of the Decision Rule Plots

The Rule Viewer shows one calculation at a time and in great detail. In this sense, it presents a sort of micro view of the fuzzy inference system for each input value and its corresponding output values. Input and output membership functions for each rule is displayed by the rule viewer. Fig. 4.3 shows a view of 29 plots nested in it and also shows the decision outputs for an input value detected. Each rule represent an input action. The top of Fig. 4.3 the antecedent and consequent of the first rule, which is displayed as five plots. Individual columns represent a variable and every single rule is a row of plots. On the left side of each row is displayed the rule numbers. On the top side of each column is displayed the name of each variable. The first column of plots (the five yellow plots) show the membership functions referenced by the antecedent or the if-part of each rule. The first variable is denoted as "Mobile Stations" and it indicates the input value to the inference system. With every input value gives different plots of output values which corresponds to the decision making for that input value. The membership functions referenced by the consequent is displayed in blue plots. The second to the last variable is denoted as follows respectively; "Call Decision Output", "SMS Decision Output", "Data Decision Output", and "Emergency Call Decision Output". These variables indicate the output decision values of inputs to the inference system. The aggregated weighted decision for the given inference system is represented by sixth plots in the second to last columns. The input values determine the decision output for the system. The defuzzified output value is displayed as a bold red vertical line on this plot. The red thin line found in the first column is the index line. The index line always compares two triangles when an

input is made and chooses the most shaded triangle. This allows the FIS to know which rule is to fired. To change the input values, the index line was glided and output values were generated. The user class rankings from table 3.1 were the input values to the inference system. These rankings as stated represent the various classification of users seen in table 3.1.

4.2 Decision Rule for Privileged Users in All Locations

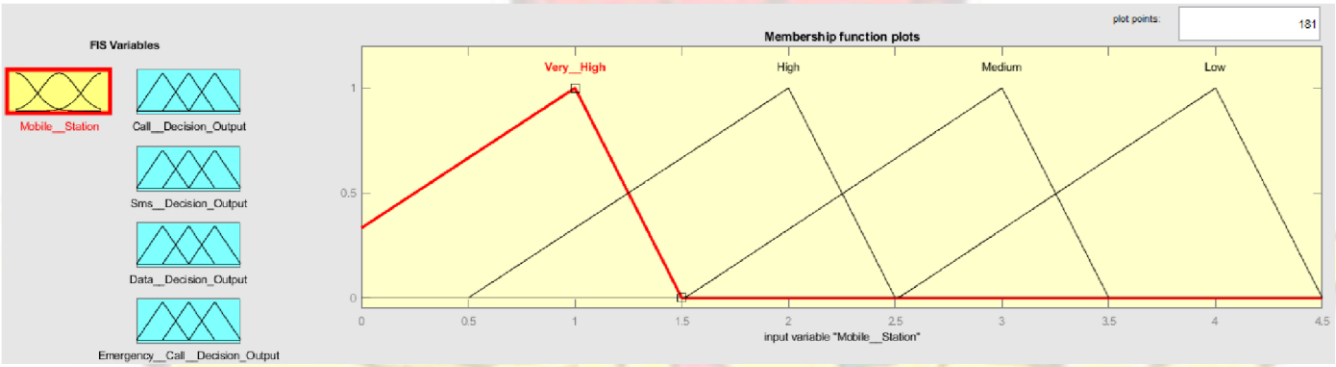

Fig. 4.1: "Very High" as input for privileged users

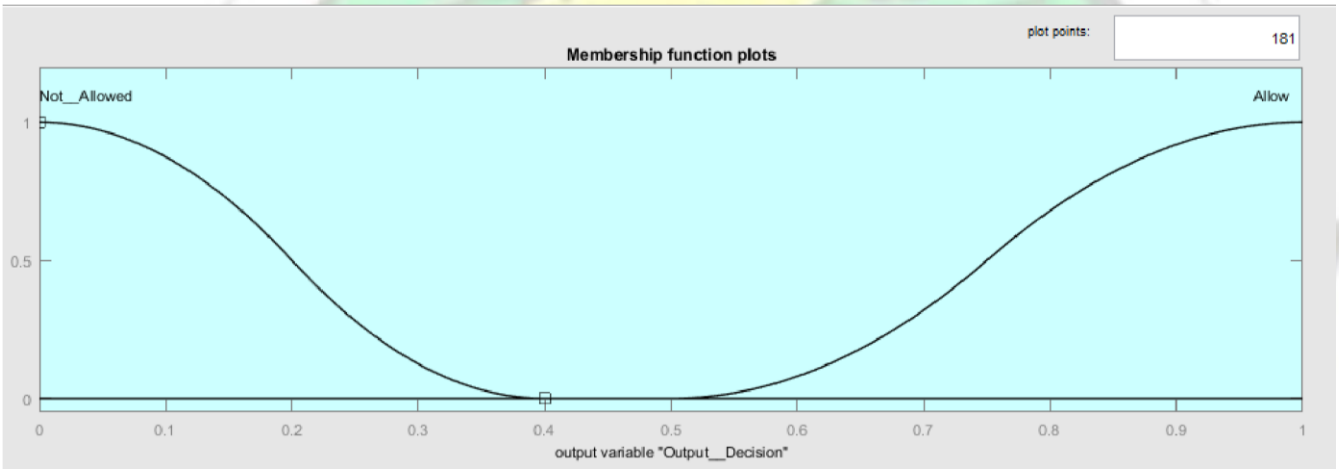

Fig. 4.2: Output decision for a communication service

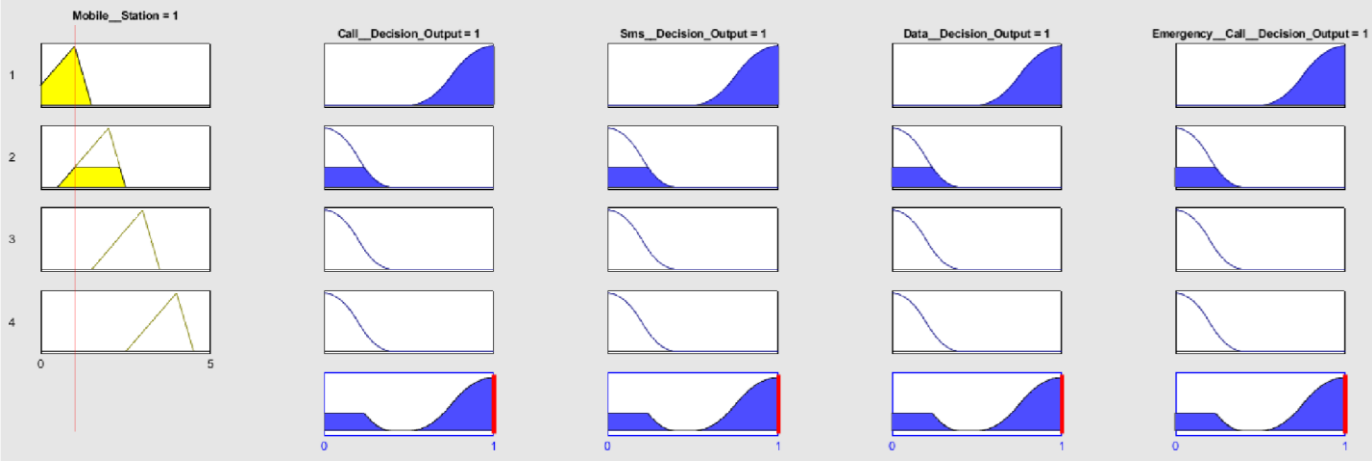

Fig. 4.3: Defuzzified decision rule for privileged users in all locations

The crisp input value of 1 for privileged users is fuzzified by the triangular membership function into fuzzy values and is denoted as “Very High” as seen in Fig. 4.1. This reads as “Mobile Station =1”, where 1 is the crisp input value and “Mobile station” is the input variable. Using the rule interface in Fig. 3.14, the defuzzified classification range for “allow” and “not allowed” in Fig. 4.2, the crisp input denoted as “Very High” and the decision table in Table 3.1 results in Fig. 4.3. When Table 3.1 is compared to Fig. 4.3, it can be shown that the following are the decision output values of communication services made for privileged users in all the locations; call decision output = 1, SMS decision output = 1, data decision output = 1, emergency call decision output = 1. The decision output value for a communication service can also be termed as the crisp output value. As seen in fig. 4.3 the sixth plot in column two to column five represents the aggregated weighted decision value for a service. That is the decision value is either 0 or 1 which means to allow or not allow. The results in Fig. 4.3 confirms that privileged mobile phone users are allowed access to all communication services.

4.3 Decision rule for Users at Hospitals

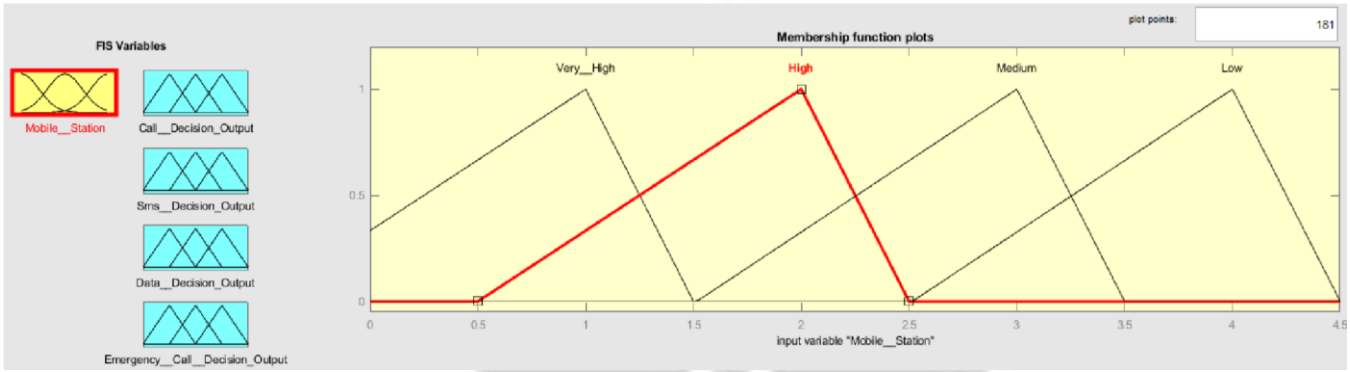

Fig. 4.4: "High" as input for Hospital users

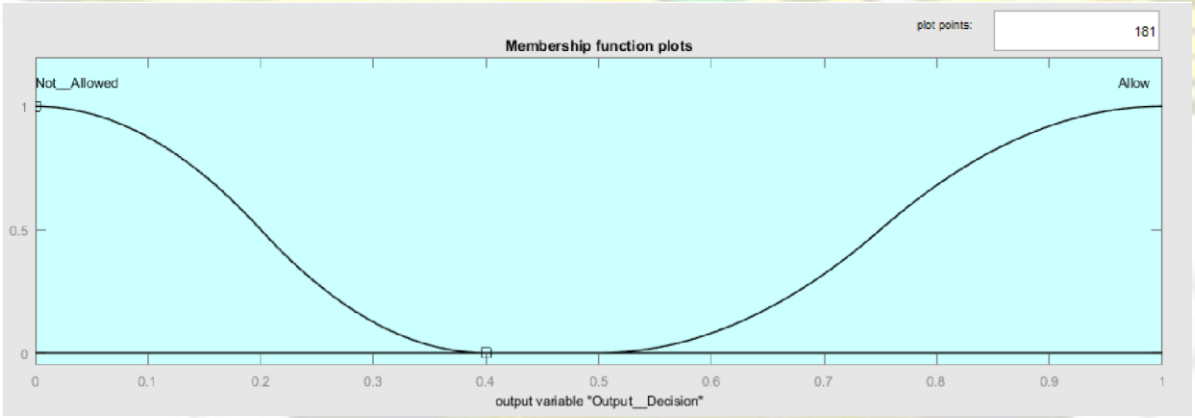

Fig. 4.5: Output decision for a communication service

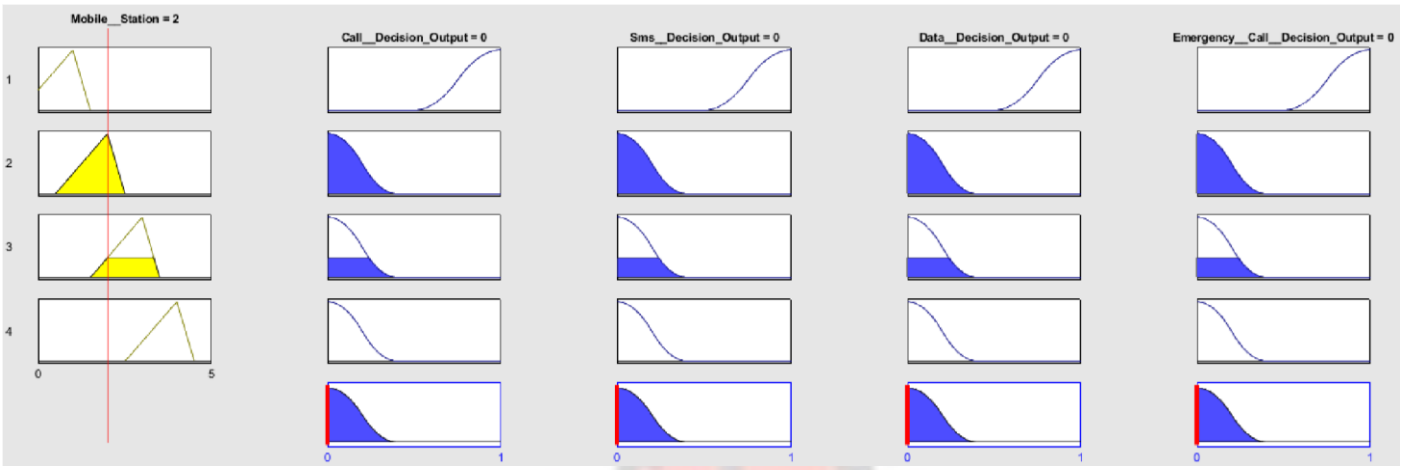

Fig. 4.6: Defuzzified decision rule for Hospitals

The crisp input value of 2 for users at Hospitals is fuzzified by the triangular membership function into fuzzy values and is denoted as “High” as seen in Fig. 4.4. This reads as “Mobile Station =2”, where 2 is the crisp input value. Using the rule interface in Fig. 3.14, the defuzzified classification range for “allow” and “not allowed” in Fig. 4.5, the crisp input denoted as “High” and the decision table in Table 3.1 results in Fig. 4.6. When Table 3.1 is compared to Fig. 4.6, the following are the crisp output values for users at Hospitals; call decision output = 0, SMS decision output = 0, data decision output = 0, emergency call decision output = 0. The results in Fig. 4.6 confirms the services restricted for non-privilege users for Hospitals.

4.4 Decision rule for Users at Banks

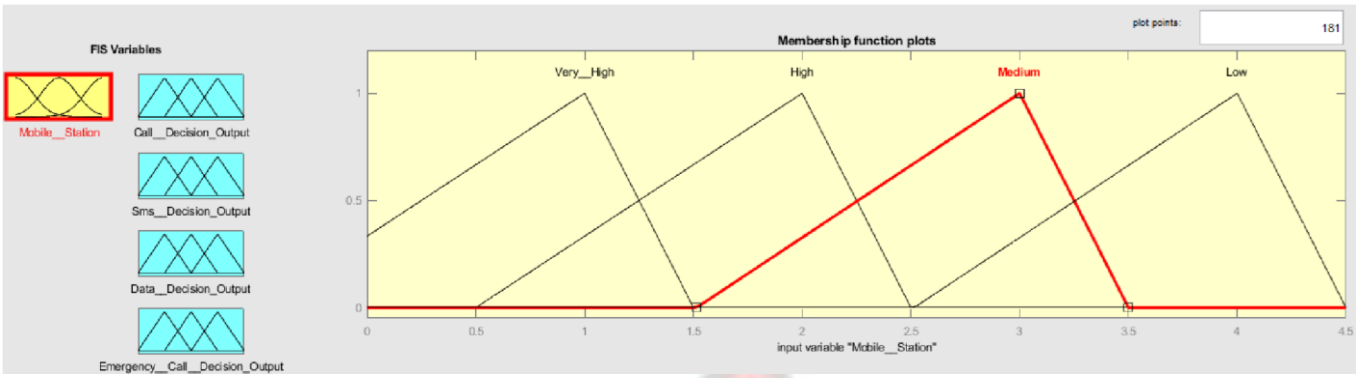

Fig. 4.7: “Medium” as input for Bank users

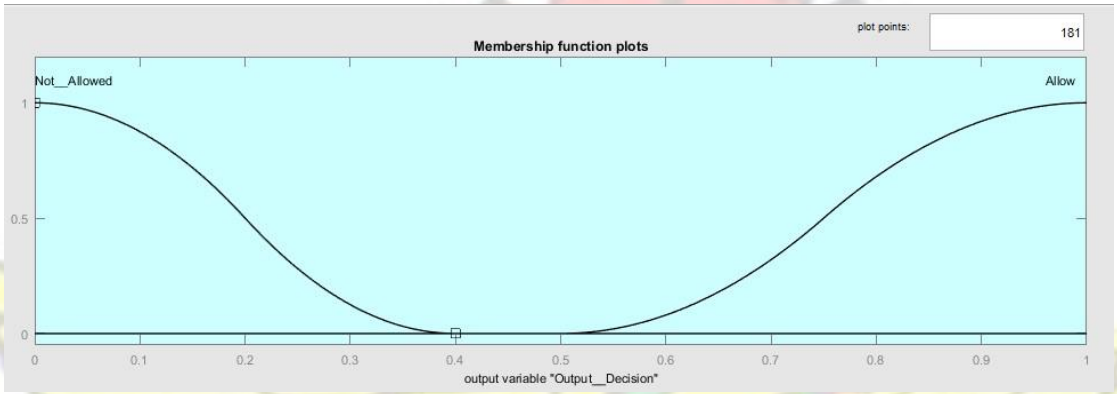

Fig. 4.8: Output decision for a communication service

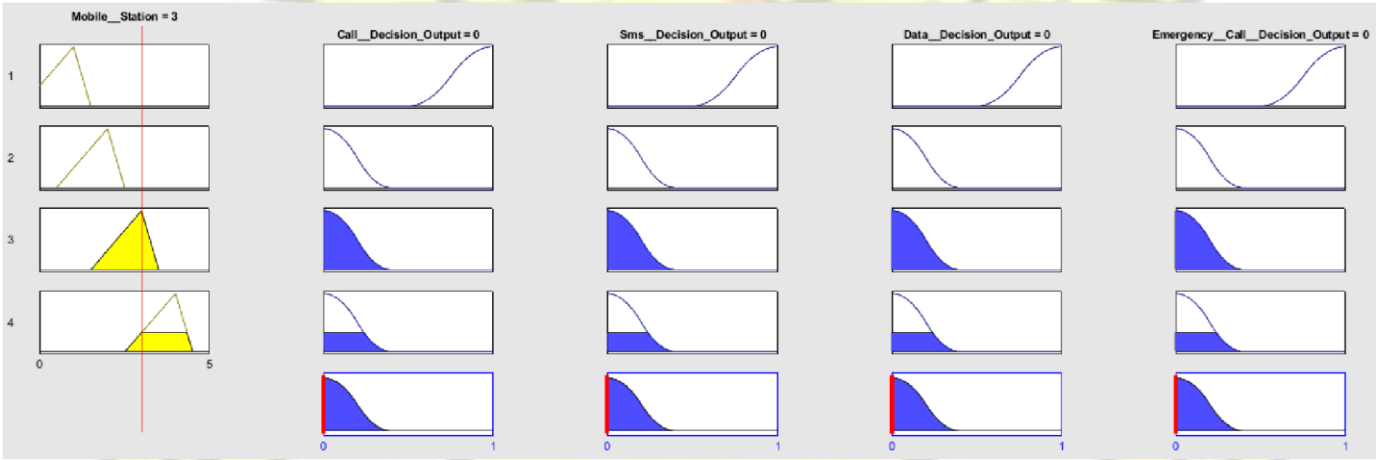

Fig. 4.9: Defuzzified decision rule for Banks

The crisp input value of 3 for users at Banks is fuzzified by the triangular membership function into fuzzy values and is denoted as “Medium” as seen in Fig. 4.7. This reads as “Mobile Station =3”, where 3 is the crisp input value. Using the rule interface in Fig. 3.14, the defuzzified classification range for “allow” and “not allowed” in Fig. 4.8, the crisp input denoted as “Medium” and the decision table in Table 3.1 results in Fig. 4.9. When Table 3.1 is compared to Fig. 4.9, communication services not permitted for Bank users results in the following; call decision output = 0, SMS decision output = 0, data decision output = 0, emergency call decision output = 0. The result in Fig. 4.9 confirms the services restricted for non-privilege users for Banks.

.

4.5 Decision rule for Users at Schools

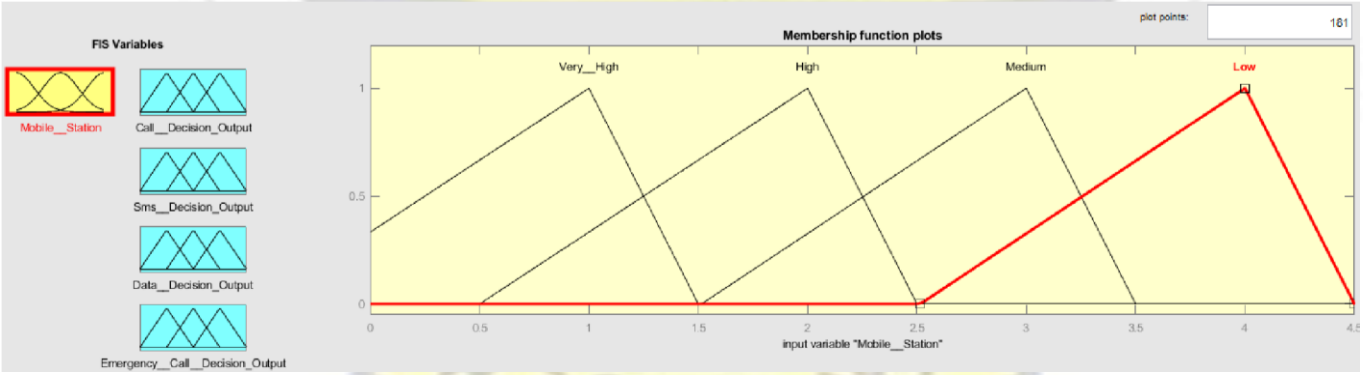

Fig. 4.10: “Low” as input for School users

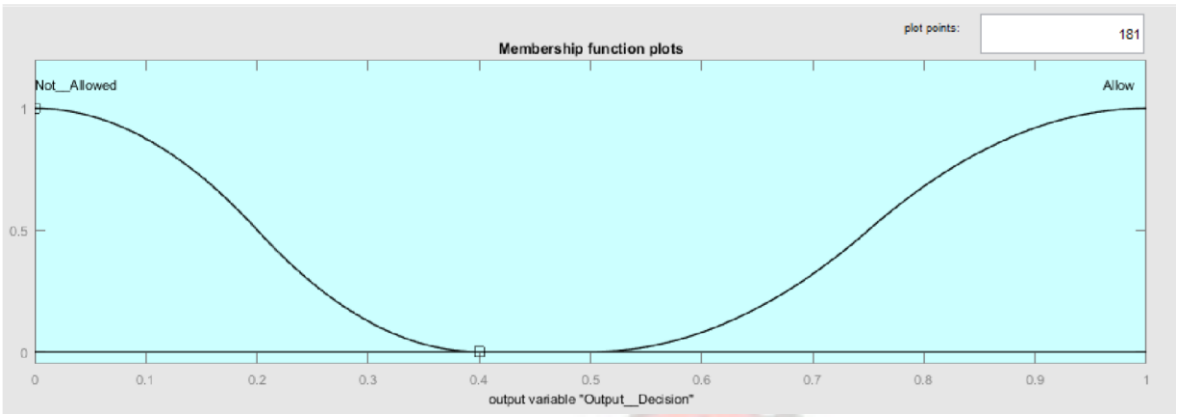

Fig. 4.11: Output decision for a communication service

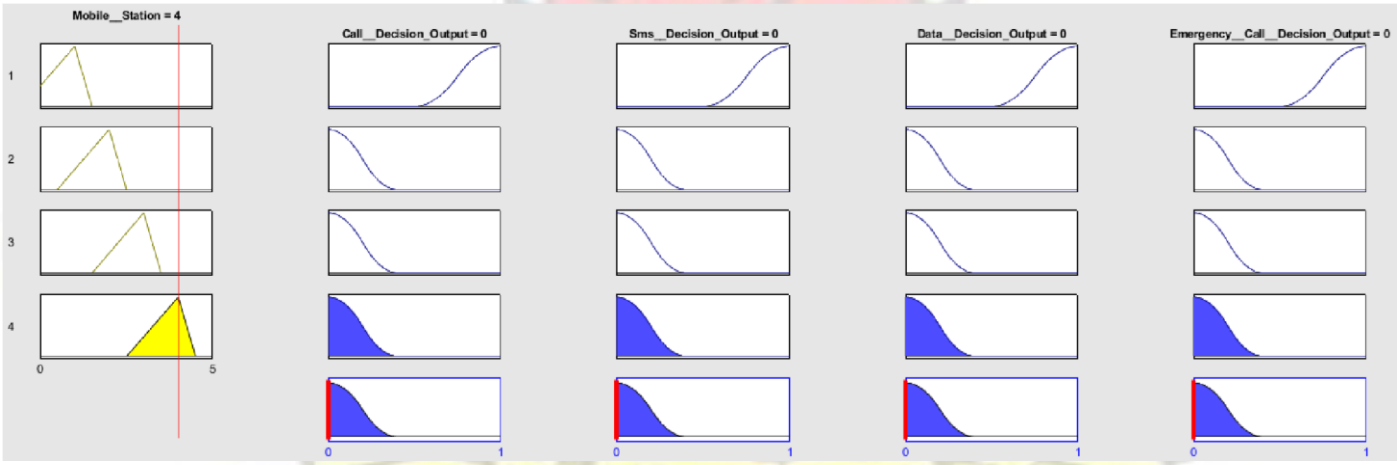

Fig. 4.12: Defuzzified decision rule for Schools

The crisp input value of 4 for users at School is fuzzified by the triangular membership function into fuzzy values and is denoted as “Low” as seen in Fig. 4.10. This reads as “Mobile Station =4”, where 4 is the crisp input value. Using the rule interface in Fig. 3.14, the defuzzified classification range for “allow” and “not allowed” in Fig. 4.11, the crisp input denoted as “Low” and the decision table in Table 3.1 results in Fig. 4.12. When Table 3.1 is compared to Fig. 4.12, the following decision output for communication services result; call decision output = 0, SMS decision output = 0, data decision output = 0, emergency call decision output = 0. The result in Fig. 4.12 confirms the services restricted for non-privilege users for Schools.

Chapter 5

Conclusion and Recommendation

5.1 Conclusion

In this research, a selective mobile phone communication blocking system was designed. A flow chart algorithm for the decision making of communication services for privilege and non-privilege mobile phone users was also designed. The selective blocking nature of the system was implemented using Matlab's Fuzzy Inference System toolbox. The Mamdani type was used. The fuzzy inference technique was based on a set of IF-THEN rules and membership functions of the input and output variables of the system. Crisp input values were converted into fuzzy values and mapped onto defuzzied fuzzy values by the rule function of the inference system. The defuzzfied values were converted back into crisp output values termed as decision output values. Nonprivileged users for hospitals, banks, and schools were successfully blocked by the Fuzzy Inference System. Privileged users in all the locations were given access to full communication with no restriction. A privileged user from a particular user location cannot enjoy the same privileges at a different location. The results from the Fuzzy Inference System shows that when the system is implemented mobile phone communication service can be prioritised to suit privilege users in specific mobile phone restricted areas. Since the proposed system has to connect to the operator's network in order to allow communication in the restricted area, it is dependent on the operator's network but not for blocking of communication.

5.2 Recommendation

This study is proposing a selective mobile phone communications blocking system to be implemented in specific mobile phone restricted areas. The adoption of the design will control and optimise mobile phone usage in the restricted zones. It is recommended that future works should look at building a prototype of the system to test the system's effectiveness.

References

[1] S. Gupta, "Cell Phone Jammer," Amity University Rajasthan, 2011.

[2] I. Torres, "Bank Bans Cell Phones," Schneier on Security, 4 August 2006. [Online]. Available: https://www.schneier.com/blog/archives/2006/08/bank_bans_cell.html. [Accessed 27 July 2018].

[3] A. Burgess and S. Derbyshire, "Use of mobile phones in hospitals," 1 october 2006 Oct 1. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1601977/. [Accessed 27 July 2018].

[4] S. Yubo, Z. Kan, Y. Bingxin and C. Xi, "A GSM/UMTS Selective Jamming System," *2010 International Conference on Multimedia Information Networking and Security*, 2010.

[5] J. Vales-Alonso, F. J. González-Castaño, J. M. Pousada-Carballo and F. and Isasi de Vicente, "Real-Time 3G UMTS Terminal Detection," *IEEE Communications Letters*, vol. VI, no. 3, March 2002.

[6] M. Ulrike and S. Wetzel, "A Man-in-the-Middle Attack on UMTS," Philadelphia, 2004.

[7] F. J. González Castaño, J. Vales Alonso, J. M. Pousada Carballo, F. Isasi de Vicente and M. J. Fernández Iglesias, "Real-Time Interception Systems for the GSM Protocol," *IEEE Transactions on Vehicular Technology*, vol. 51, no. 5, pp. 904-914, 2002.

[8] J. Vales-Alonso, F. Isasi de Vicente, F. J. González-Castaño and J. M. Pousada-Carballo, "Real-Time Detector of GSM Terminals," *IEEE Communications Letters*, vol. V, no. 6, June 2001.

[9] J. Vales-Alonso, F. J. González-Castaño and J. M. Pousada-Carballo, "Experimental RealTime Detector of GSM Terminals," *IEEE Communications Letters*, vol. VII, no. 3, March 2003.

[10] A. Kostrzewa, "Development of a man in the middle attack on the GSM Um-Interface," Berlin, 2011.

[11] K. van Rijsbergen, "The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF," 2016.

[12] M. Hadžialić, M. Škrbić, K. Huseinović, I. Kočan, J. Mušović, A. Hebibović and L. Kasumagić, "An approach to analyze security of GSM network," Belgrade, 2014.

[13] J. Vales-Alonso, F. J. Gonzalez-Castano and F. Gil-Castineira, "Selective interceptors for the UMTS Terrestrial Radio Access Network," 2004.

[14] "Jamming and Anti-jamming Techniques in Wireless Networks: A Survey," in *Int. J. Ad Hoc and Ubiquitous Computing*.

[15] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks.," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2005.

[16] T. Basar, "The gaussian test channel with an intelligent jamming," *IEEE Transactions on Information Theory,* vol. 29, no. 1, pp. 152-157, 1983.

[17] M. Lichtman, J. D. Poston, A. SaiDhiraj, C. Shahriar, T. C. Clancy, R. M. Buehrer and J. H. Reed, "A Communications Jamming Taxonomy," *IEEE Security & Privacy,* vol. 14, no. 1, pp. 47-54, 2016.

[18] R. Poisel, "Jamming Techniques," in *Modern Communications Jamming Principles and Techniques*, London, Artech House, 2011, p. 477.

[19] C. S. Kumar, M. Ganesh, M. Manu and H. Srinivas, "Cell Phone Jammer With Prescheduled Time Duration," Visvesvaraya Technological University, 2013.

[20] Trisha, "IMSI Catchers and How to Circumvent Them," TrishTech, 10 February 2015. [Online]. Available: http://www.trishtech.com/2015/02/imsi-catchers-and-how-tocircumvent-them/. [Accessed 6 April 2017].

[21] Thespyphone.com, "Passive GSM Interceptor," Thespyphone.com, 2019. [Online]. Available: https://www.thespyphone.com/passive-gsm-interceptor/. [Accessed 10 Febuary 2019].

[22] F. J. a. B. Rainer., "Method for identifying a mobile phone user or for eavesdropping on outgoing calls," 2000.

[23] D. Strobel, "IMSI Catcher," Ruhr-Universit¨at Bochum, 2007.

[24] A. Kostrzewa, "Development of a man in the middle attack on the GSM Um-Interface," Technische Universität Berlin, Berlin, 2011.

[25] SMScarrier.eu, "Mobile Country Codes (MCC) and Mobile Network Codes (MNC)," 2013. [Online]. Available: http://mcc-mnc.com/. [Accessed 2 September 2017].

[26] A. Dabrowski, M. Mulazzani, N. Pianta, E. Weippl and T. Klepp, "IMSI-catch me if you can: IMSI-catcher-catchers," *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014.

[27] D. Strobel, "IMSI Catcher," Ruhr-Universit¨at Bochum, 2007.

[28] J. Hernandez, "How IMSI Catchers Work," 16 December 2015. [Online]. Available: https://www.nstarpost.com/news/how-imsi-catchers-work/. [Accessed 6 April 2017].

[29] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani and E. Weippl, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," *ACSAC '14 Proceedings of the 30th Annual Computer Security Applications Conference*, pp. 246-255, 2014.

[30] U. Meyer and S. Wetzel, "A man-in-the-middle attack," *3rd ACM workshop on Wireless security*, pp. 90-97, 2005.

[31] D. Wehrle, "Master-arbeit zum thema: Open source imsi-catcher," Albert-LudwigUniversitat Freiburg, 2009.

[32] "GSM security map," [Online]. Available: . http://gsmmap.org/.

[33] E. Biham, O. Dunkelman and N. Keller, "A related-key rectangle attack on the full KASUMI," *Advances in Cryptology - ASIACRYPT 2005*, vol. 3788, pp. 443-461, 2005.

[34] O. Dunkelman, N. Keller and A. Shamir, "A practical-time attack on the A5/3 cryptosystem used in third generation gsm telephony," 2010.

[35] U. Kuhn, "Cryptanalysis of reduced-round MISTY," *In Advances in Cryptology - EUROCRYPT*, pp. 325-339, 2001.

[36] MathWorks, "Triangular-shaped membership function," 2018. [Online]. Available: https://www.mathworks.com/help/fuzzy/trimf.html. [Accessed 3 February 2018].

[37] S. Lian, Principles of Imprecise-Information Processing, Singapore: Springer, 2016.

[38] MathWorks, "Z-shaped membership function," 2018. [Online]. Available: https://www.mathworks.com/help/fuzzy/zmf.html. [Accessed 3 February 2018].

[39] MathWorks, "S-shaped membership function," 2018. [Online]. Available: https://www.mathworks.com/help/fuzzy/smf.html. [Accessed 3 February 2018].

[40] J. Ooi, "IMSI Catchers and Mobile Security," University of Pennsylvania, Pennsylvania, 2015.

[41] J. Eberspocher, H. J. Vogel, C. Bettstetter and C. Hartmann, "Gsm architecture, protocols and services," Wiley, 2009.

[42] K. Zhou, A. Hu and Y. Song, "A No-jamming Selective Interception System of the GSM Terminals," Southeast University, Nanjing, 2010.

[43] T. W. Z. Y. W. T. Xu W, "The feasibility of launching and detecting jamming attacks in wireless networks.," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2005.