GSM Technology & Its Application in Bangladesh

A Thesis submitted

by

Tanzana Rahman
(ID # 02201114)

Under the supervision
of

Ms. Sadia Hamid Kazi

May 3, 2007

Declaration

This is to certify that this project is my original work. No part of this work has been submitted elsewhere partially or fully for the award of any other degree or diploma. Any material reproduced in this project has been properly acknowledged.

Student's Name & Signature

.....

Tanzana Rahman

Certification Of Approval

The thesis titled **"GSM Technology & its application in Bangladesh"** has been submitted to the following respected faculty of BRAC University for the fulfillment of the course CSE 400 on May 3, 2007 by the following student and has been accepted as satisfactory.

Tanzana Rahman
(ID # 02201114)

_____

Ms. Sadia Hamid Kazi
Faculty
Computer Science & Engineering Department
BRAC University

Acknowledgement

First and for most I would like to thank my supervisor, Ms. Sadia Hamid Kazi for all the freedom and guidance she provided me in every possible way through this exertion. I discussed every single difficulty I had in my working period. Her profound knowledge, keen interest, patience, and the constant support have served as the impetus for me to carry out the task. She arranged all the facilities and necessary supports, which were indispensable for my thesis. I am grateful to her for the priceless advices she gave me generously, which led to the improvement of this thesis.

Finally, I also thank my family and all my friends, especially those, who supported me with their valuable suggestions and encouragements.

Thank you Almighty *Allah* for enabling me to do this work; for You are all. Please help me to stay true to my beliefs and myself. Please help me give back to all those who have given me so much...

Contents at a Glance

List of Figures

List of Tables

Thesis Topic Selection in Pre-thesis Semester

Semester: Spring Year: 2007

Student's Name: Tanzana Rahman

Student's ID: 02201114

Supervisor's Name: Ms. Sadia Hamid Kazi

Thesis Title: GSM Technology & its application in Bangladesh

Thesis Abstract:

My thesis gives an overview about the GSM technology and its application in Bangladesh. GSM Technology is the most popular standard for mobile phones in the world. It allows the network operators to offer roaming services, which means that the subscribers can use their phones in many parts of the world

This paper would describe how this GSM technology is being used worldwide and also how the telecom companies in our country are using it.

Supervisor

Chairperson
Department of
Computer Science &
Engineering

Chapter 1

Introduction

1.1 What is GSM?

GSM (Global System for Mobile communications), which originally stood for **Groupe Speciale Mobile**, the CEPT committee, which began the GSM standardization process. It is the most popular standard for mobile phones in the world. GSM service is used by over 2 billion people across more than 212 countries and territories. The ubiquity of the GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world.

From the point of view of the consumers, the key advantage of GSM systems has been higher digital voice quality and low cost alternatives to making calls such as text messaging. The advantage for network operators has been the ability to deploy equipment from different vendors because the open standard allows easy inter-operability. Like other cellular standards GSM also allows network operators to offer roaming services, which means that subscribers can use their phones all over the world.

As the GSM standard continued to develop, it retained backward compatibility with the original GSM phones. For example, packet data capabilities were added in the Release ‘97 version of the standard, by means of GPRS. Higher speed data transmission has also been introduced with EDGE in the Release '99 version of the standard.

GSM is an open, digital cellular technology used for transmitting mobile voice and data services. GSM differs significantly from its predecessors in that both signaling and speech channels are Digital call quality, which means that it is considered as a *second generation* (2G) mobile phone system. This fact has also meant that data communication was built into the system from the Third Generation Partnership Project (3GPP). This 2G digital technology was originally developed for Europe, which now has in excess of 71 per cent of the world

market. Initially GSM was developed for operation in the 900MHz band and subsequently modified for the 850, 1800 and 1900MHz bands.

GSM differs from the first generation wireless systems because it uses digital technology and time division multiple access transmission methods. GSM is a circuit-switched system that divides each 200kHz channel into eight 25kHz time-slots. GSM operates in the 900MHz and 1.8GHz bands in Europe and the 1.9GHz and 850MHz bands in the US. The 850MHz band is also used for GSM and 3GSM in Australia, Canada and many South American countries. GSM supports data transfer speeds of up to 9.6 kbit/s, allowing the transmission of basic data services such as SMS (Short Message Service). Another major benefit is its international roaming capability, allowing users to access the same services when traveling abroad as at home. This gives consumers seamless and same number connectivity in more than 210 countries. GSM satellite roaming has also extended service access to areas where terrestrial coverage is not available.

1.2 History of GSM

Date	**Activity**
1992-1985	• Conference Europeenne des Postes et Telecomunication (CEPT) begin specifying a European digital telecommunications standard in the 900 MHz frequency band. This standard later became known as Global System for Mobile communication (GSM)
1986	• Field tests held in Paris to select which digital transmission technology to use either Time Division Multiple Access (TDMA) or Frequency Division Multiple access.
1987	• A combination of TDMA and FDMA selected as the transmission technology for GSM. • Operators from 12 countries sign a Memorandum of Understanding (MoU) committing to introduce GSM by 1991.
1988	• CEPT begins producing GSM specifications for a phased implementation. • Another five countries sign the MoU.
1989	• European Telecommunication Standards Institute (ETSI) takes over responsibility for GSM specification.
1990	• Phase 1 specification frozen to allow manufacturers to develop network equipment.
1991	• The GSM 1800 standard was released. • An addendum was added to the MoU allowing countries outside CEPT to sign.
1992	• Phase 1 specifications are completed. • First commercial Phase 1 GSM networks launched. • First international roaming agreement between Telecom Finland and Vodaphone in UK.
1993	• Australia becomes the first non-European country to sign the MoU. • The MoU now had a total of 70 signatories. The GSM networks launched in Norway, Austria, Ireland, Hong Kong and Australia. • The number of GSM subscribers reaches one million.

	• The first commercial DCS 1800 system is launched in the UK.
1994	• The MoU now has over100 signatories covering 60 countries. • More GSM networks are launched. • The total number of GSM subscribers exceeded 3 million.
1995	• The specification for the Personal Communications Services (PCS) developed in the U.S.A. this version of GSM operates at 1900 MHz. • GSM growth trends continue steadily through 1995, with the number of GSM subscribers increasing at the rate of 10,000 per day and rising. • In April 1995, there are 188 members of the MoU from 69 countries.
1996	• The first GSM 1900 systems become available. These comply with the PCS 1900 standard.
1998	• The MoU has a total of 253 members in over 100 countries and there are over 70 million GSM subscribers world-wide. GSM subscribers account for 31% of the world's mobile market.
1999	• GSM networks now exist in over 179 countries.
2002	• Functionality of GSM extended to incorporate EDGE, AMR, and support for flexible positioning services.
2003	• Total number of subscribers expected to soar to over 1 billion.

Table 1.1 GSM Milestones

1.3 GSM Logo

Figure 1.1 GSM Logo

Chapter 2

GSM Services

GSM services are a standard collection of applications and features available to mobile phone subscribers all over the world. The GSM standards are defined by the 3GPP collaboration and implemented in hardware and software by equipment manufacturers and mobile phone operators. The common standard makes it possible to use the same phones with different companies' services, or even roam into different countries. GSM is the world's most dominant mobile phone standard.

The design of the service is moderately complex because it must be able to locate a moving phone anywhere in the world, and accommodate the relatively short battery life, limited input/output capabilities, and weak radio transmitters on mobile devices

2.1 Data transmission

The Public Switched Telephone Network (PSTN) is essentially a collection of interconnected systems for taking an *audio* signal from one place and delivering it to another. Older analogue phone networks simply converted sound waves into electrical pulses and back again. The modern phone system digitally encodes audio signals so that they can be combined and transmitted long distances over fiber optic cables and other means, without losing signal quality in the process. When someone uses a computer with a traditional modem, they are encoding a (relatively slow) data stream into a series of audio chirps, which are then relayed by the PSTN in the same way as regular voice calls. This means that computer data is being encoded as phone audio, which is then being re-encoded as phone system data, and then back to phone quality audio, which is finally converted back to computer data at the destination.

GSM voice calls are essentially an extension of the PSTN, dealing only with audio signals. Behind the scenes, we know these audio channels happen to be transmitted as digital radio signals.

The GSM standard also provides separate facilities for transmitting digital data *directly*, without any of the inefficient conversions back and forth to audio form. This allows a mobile "phone" to act like any other computer on the Internet, sending and receiving data via the Internet Protocol or X.25.

The mobile may also be connected to a desktop computer, laptop, or PDA, for use as a network interface. (Like a modem or Ethernet card, but using a GSM-compatible data protocol instead of a PSTN-compatible audio channel or an ethernet link to transmit data.) Newer GSM phones can be controlled by a standardised Hayes AT command set through a serial cable or a wireless link (using IrDA or Bluetooth). The AT commands can control anything from ring tones to data compression algorithms.In addition to general Internet access, other special services may be provided by the mobile phone operator, such as SMS.

2.2 ACCESSING A GSM NETWORK

In order to gain access to GSM services, a user needs three things:

1. A subscription with a mobile phone operator.

2. A mobile phone, which is GSM compliant and operates at the same frequency as the operator.

3. A SIM card, which is issued by the operator once the subscription is granted. The SIM card comes pre-programmed with the subscriber's

phone "identity" and will be used to store personal information (like contact numbers of friends and family).

After subscribers sign up, information about their phone's identity and what services they are allowed to access are stored in a "SIM record" in the *Home Location Register* (HLR). The *Home Location Register* is a database maintained by the "home" phone company for all of its subscribers.

Once the SIM card is loaded into the phone and it is powered on, it will search for the nearest mobile phone mast, also called a Base Transceiver Station or BTS. If a mast can be successfully contacted, then there is said to be coverage in the area.

Stationary phones are always connected to the same part of the phone network, but mobile phones can "visit" any part of the network, whether across town or in another country via a foreign provider. Each geographic area has a database called the *Visitors Location Register* (VLR) which contains details of all the local mobiles. Whenever a phone attaches, or visits, a new area, the *Visitors Location Register* must contact the Home Location Register.

The *Visitors Location Register* will tell the *Home Location Register* where the phone is connected to the network (which VLR), and will ask it for a copy of the SIM record (which includes, for example, what services the phone is allowed to access). The current cellular location of the phone (i.e. which BTS it is at) is entered into the VLR record and will be used during a process called paging when the GSM network wishes to locate the mobile phone.

Every SIM card contains a secret key, called the Ki, which it uses to prove its identity to the phone network (to prevent theft of services) upon first contact. The network does this by consulting the Authentication Center of the "home" phone company, which also has a copy of the secret key.

Every phone contains a unique identifier (different from the phone number, which is associated at the HLR with the removable SIM card), called the International Mobile Equipment Identity (IMEI). When a phone contacts the network, its IMEI is supposed to be checked against the global *Equipment Identity Register* to locate stolen phones and facilitate monitoring.

2.3 Voice Services

2.3.1 How outgoing calls are made from a mobile

Once a mobile phone has successfully attached to a GSM network as described above, calls may be made from the phone to any other phone on the global Public Switched Telephone Network assuming the subscriber has an arrangement with their "home" phone company to allow the call.

The user dials the telephone number, presses the *send* or *talk* key, and the mobile phone sends a call setup request message to the mobile phone network via the mobile phone mast (BTS) it is in contact with.

The element in the mobile phone network that handles the call request is the Visited Mobile Switching Center (Visited MSC). The MSC will check against the subscriber's temporary record held in the Visitor Location Register to see if the outgoing call is allowed. If so, the MSC then routes the call in the same way that a telephone exchange does in a fixed network.

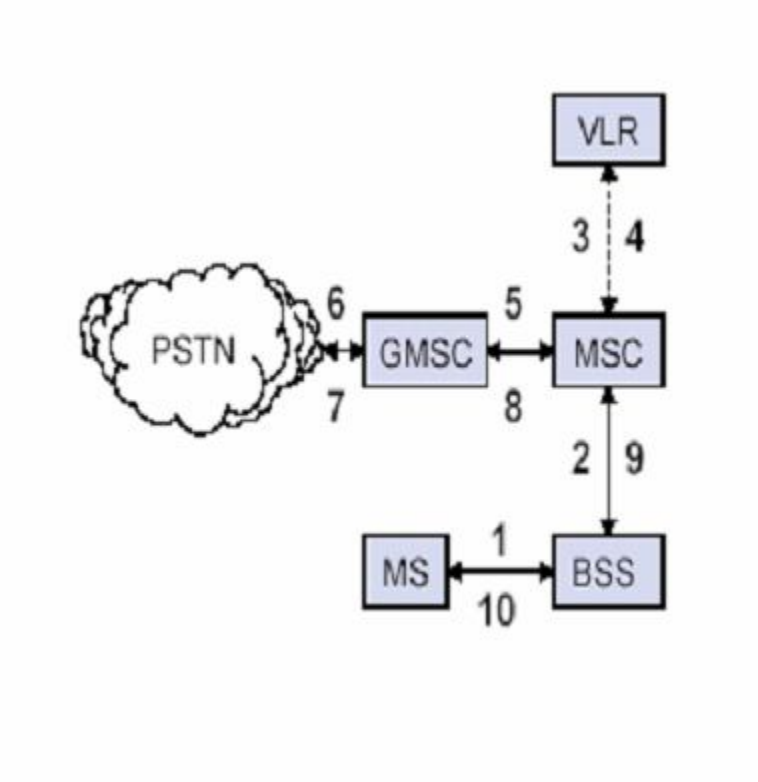

Figure 2.1 GSM Outgoing Calls

If the subscriber is on a *Pay As You Go* tariff, then an additional check is made to see if the subscriber has enough credit to proceed. If not, the call is rejected. If the call is allowed to continue, then it is continually monitored and the appropriate amount is decremented from the subscriber's account. When the credit reaches zero, the call is cut off by the network. The systems that monitor and provide the prepaid services are not part of the GSM standard services, but instead an example of intelligent network services that a mobile phone operator may decide to implement in addition to the standard GSM ones.

2.3.2 How incoming calls are made to a mobile

Step One: Contact the Gateway MSC

When someone places a call to a mobile phone, they dial the telephone number (also called a MSISDN) associated with the phone user and the call is routed to the mobile phone operator's Gateway Mobile Switching Centre. The Gateway MSC, as the name suggests, acts as the "entrance" from exterior portions of the Public Switched Telephone Network onto the provider's network.
As noted above, the phone is free to roam anywhere in the operator's network or on the networks of roaming partners, including in other countries. So the first job of the Gateway MSC is to determine the current location of the mobile phone in order to connect the call. It does this by consulting the Home Location Register (HLR), which, as described above, knows which Visitor Location Register (VLR) the phone is associated with, if any.

Step Two: Determine how to route the call

When the HLR receives this query message, it determines whether the call should be routed to another number (called divert), or if it is to be routed directly to the mobile.

- If the owner of the phone has previously requested that all incoming calls be diverted to another number, known as the Call Forward Unconditional (CFU) Number, then this number is stored in the Home Location Register. If that is the case, then the CFU number is returned to the Gateway MSC for immediate routing to that destination.

- If the mobile phone is not currently associated with a Visited Location Register (because the phone has been turned off or is not in range) then the Home Location Register returns a number known as the Call Forward Not Reachable (CFNRc) number to the Gateway MSC, and the call is forwarded there. Many operators may set this value automatically to the

phone's voice mail number, so that callers may leave a message. The mobile phone may sometimes override the default setting.

- Finally, if the Home Location Register knows that the phone is in the jurisdiction of a particular Visited Location Register, then it will request a temporary number (called an MSRN) from that VLR. This number is relayed to the Gateway MSC, which uses it to route the call to another Mobile Switching Center, called the Visiting MSC.

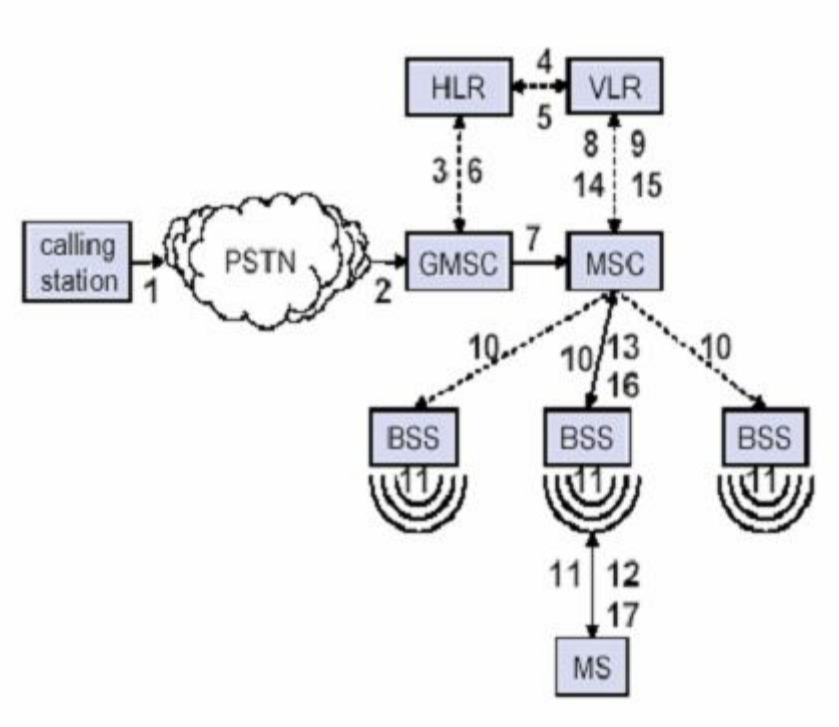

Figure 2.2 GSM Outgoing Calls

<u>Step Three</u>: Ringing the phone

When the call is received by the Visiting MSC, the MSRN is used to find the phone's record in the Visited Location Register. This record identifies the phone's location area. Paging occurs to all mobile phone masts in that area. When the subscriber's mobile responds, the exact location of the mobile is returned to the Visited MSC. The VMSC then forwards the call to the appropriate phone mast,

and the phone rings. If the subscriber answers, a speech path is created through the Visiting MSC and Gateway MSC back to the network of the person making the call, and a normal telephone call follows.

It is also possible that the phone call is not answered. If the subscriber is busy on another call (and call waiting is not being used) the Visited MSC routes the call to a pre-determined Call Forward Busy (CFB) number. Similarly, if the subscriber does not answer the call after a period of time (typically 30 seconds) then the Visited MSC routes the call to a pre-determined Call Forward No Reply (CFNRy) number. Once again, the operator may decide to set this value by default to the voice mail of the mobile so that callers can leave a message.

2.4 Data Services

2.4.1 Short message services

The GSM standards first defined the structure of a Short Message, and provide a means of transmitting messages between mobile devices and Short Message Service Centers via the Short Message Service (SMS). SMS messages may be carried between phones and SMSCs by any of the circuit-switched or packet-switched methods described above or, more typically, by the MAP protocol through the SS7 signaling channel used for call setup.
SMSCs can be thought of as central routing hubs for Short Messages. Many mobile service operators use their SMSCs as gateways to external systems, including the Internet, incoming SMS news feeds, and each other (often using the *de facto* SMPP standard).

The SMS standard is also used outside of the GSM system; see the main article for details

2.4.2 Multimedia services

There are two modes of delivery in MMS: *immediate* or *deferred*:

- **Immediate delivery:** When the MMS client on the mobile phone receives the MMS notification, it then immediately (without user intervention or knowledge) retrieves the MMS message from the Multimedia Messaging Service Center (MMSC) that sent the notification. After retrieval, the subscriber is alerted to the presence of a newly arrived MMS message.

- **Deferred delivery:** The MMS client alerts the subscriber that an MMS message is available, and allows the subscriber to choose if and when to retrieve the MMS message.

As with the MMS submission, the MMS retrieval request, whether immediate or deferred, occurs with an HTTP request. The MMSC responds by transmitting the MMS message in an HTTP response to the MMS client, after which the subscriber is finally alerted that the MMS message is available.
The essential difference between immediate and deferred delivery is that the former hides the network latencies from the subscriber, while the latter does not. Immediate or deferred delivery are handset dependent modes, which means that the handset manufacturer can provide the handset in one mode or the other or let the user decide his preference.

Chapter 3

GSM SUBSCRIBERS

Since GSM provides a common standard, cellular subscribers can use their telephones over the entire GSM service area, which includes all the countries around the world where the GSM system is used.

In addition, GSM provides user services such as high-speed data communication, facsimile, Short Message Service (SMS) and Intelligent Network (IN) services such as Mobile Virtual private Networks (MVPNs). The GSM technical specifications are also designed to work with other standards as standard interfaces are guaranteed.

3.1 Subscriber Statistics

3.1.1 Subscribers by Users

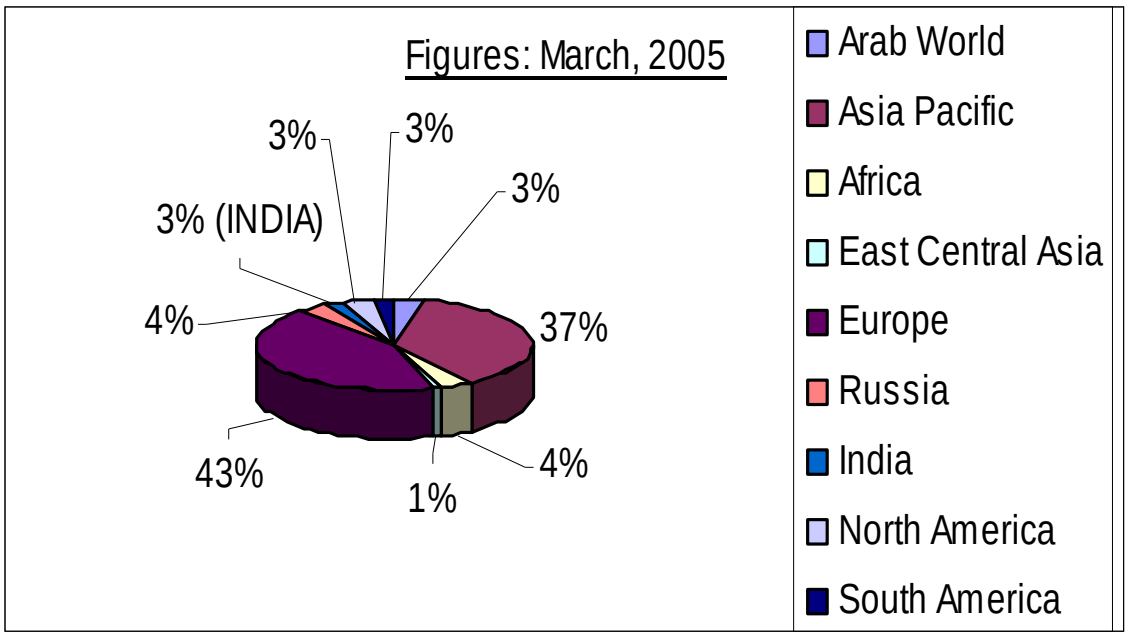

Figure 3.1 GSM Users (by number of subscribers)

The global numbers for GSM subscription are well past 1.5 billion, and adding all the other cellular technologies we have two billions. These Subscriber Statistics demonstrate the numbers of people using GSM at different frequencies, and in different global regions. It demonstrates phenomenal customer growth running at twice the industry's predicted level.

3.1.2 Subscribers by technology:

	Jan03	Apr03	July03	Oct03	Jan04	Feb04	Mar04
GSM 800	0.0014	0.0026	0.059	0.509	0.981	1.1	1.2
GSM 8/19	-	-	-	8.5	15.5	16.3	17.1
GSM 900	401.1	426.2	446.8	311.1	317.4	323.4	328.9
GSM 1800	94.1	98.3	100.7	105.4	114.7	117.3	120.2
GSM 1900	22.5	24.6	28.8	25.1	28.2	29.3	31.0
GSM 900/1800	288.1	298.1	318.7	484.3	529.5	536.9	548.4
GSM 9/18/19	-	0.025	0.0574	0.09	0.121	0.0132	0.0144
GSM 900/1900	0.0193	0.0233	0.0187	0.02	0.104	0.0114	0.0123
Total GSM Subscribers	**805.8**	**847.3**	**895.2**	**935.2**	**1006.5**	**1024.3**	**1046.8**

Table 3.1 Subscribers by technology (Source: EMC World Cellular Database)

(Source: EMC World Cellular Database)

3.1.3 Subscribers for all Mobile Technologies:

	Jan03	Apr03	July03	Oct03	Jan04	Feb04	Mar04
GSM	805.8	847.3	895.2	935.2	1006.5	1024.3	1046.8
W-CDMA	0.159	0.455	1.4	1.9	3.0	3.4	4.3
CDMA	148.3	157.9	162.3	174.1	190.2	194.4	199.1
PDC	60.3	61.7	62.3	62.5	62.0	62.2	62.4
US TDMA	108.4	110.4	112.2	109.2	109.4	110.2	111.2
Total Digital Subscribers	1123.7	1177.7	1232.8	1278.8	1388.0	1411.6	1440.0
Total Analogue Subscribers	28.1	25.1	23.2	20.7	19.0	18.3	16.5
Total Wireless Subscribers	1151.8	1202.8	1256.0	1299.5	1407.0	1429.9	1456.5

Table 3.2 Subscribers for all Mobile Technologies

(Source: EMC World Cellular Database)

3.1.4 Subscribers Regional Breakdown:

	Jan03	Apr03	Jul03	Oct03	Jan04	Feb04	Mar04
Total	**805.8**	**847.3**	**895.2**	**935.2**	**1006.5**	**1024.3**	**1047.0**
Arab World	24.9	26.8	29.2	31.9	34.8	35.6	36.4
Asia Pacific	306.5	325.9	345.3	357.5	375.2	381.2	389.2
Africa	25.8	27.8	30.4	29.6	36.7	37.9	39.2
East Central Asia	6.8	7.3	7.8	8.8	11.0	11.3	11.7
Europe	387.4	397.9	406.1	416.3	433.9	437.9	442.3
Russia	16.1	18.1	25.0	29.5	35.3	36.9	40.2
India	11.2	13.5	15.9	19.1	22.9	23.9	24.8
North America	19.3	21.0	24.2	27.9	33.7	34.8	36.1
South America	7.8	9.0	11.3	14.6	23.0	24.8	27.1

Table 3.3 Subscribers Regional Breakdown

(Source: EMC World Cellular Database)

- All figures are in Millions.

- These statistics are based on estimates and actuals are therefore subject to change.

Chapter 4

GSM Specifications

GSM was designed to be platform-independent. The GSM specifications do not specify the actual hardware requirements, but instead specify the network functions and the interfaces in detail. This allows hardware designers to be creative in how they provide the actual functionality, but at the same time makes it possible for operators to buy equipment from different suppliers.

The GSM recommendations consist of twelve series listed in the table below. Each series was written by different working parties and a number of expert groups. A permanent nucleus was established order to coordinate the working parties and to manage the editing of the recommendations. All these groups were organized by European Telecommunications Standards Institute (ETSI).

Series	**Content**
01	General
02	Services aspects
03	Network aspects
04	MS – BSS interface and protocol
05	Physical layer on the radio path
06	Speech coding specifications
07	Terminal adaptor for MS
08	BSS – MSC interface
09	Network interworking
10	Service interworking
11	Equipment and type approval specifications

12	Operation and maintenance

Table 4.1: GSM Recommendations

4.1 GSM Phases

In the late 1980's, the groups involved in developing the GSM standard realized that within the given time-frame they could not complete the specifications for the entire range of GSM services and features originally planned. Because of this, it was decided that GSM would be released in phases with phase 1 consisting of a limited set of services and features. Each new phase builds on the services offered by existing phases.

- GSM Phase 1 features
- GSM Phase 2 features
- GSM Phase 2+ features

4.1.1 Phase 1 features

Phase 1 contains the most common services including:

- Call Forwarding
- All Calls
- No Answer
- Engaged
- Unreachable
- Call Barring
- Outgoing - Bar certain outgoing calls
- Incoming - Bar certain incoming calls
- Global roaming - Visit any other country with GSM and a roaming agreement and use your phone and existing number

Phase 1 also incorporated features such as Ciphering and Subscribers Identity Module (SIM) cards. Phase 1 specifications were then closed and cannot be modified.

4.1.2 GSM Phase 2 features

Additional features wee introduced in GSM phase2 included:

- SMS - Short Message Service - Allows you to send text messages too and from phones
- Multi Party Calling - Talk to five other parties as well as yourself at the same time
- Call Holding - Place a call on Hold
- Call Waiting - Notifies you of another call whilst on a call
- Mobile Data Services - Allows handsets to communicate with computers
- Mobile Fax Service - Allows handsets to send, retrieve and receive faxes
- Calling Line Identity Service - This facility allows you to see the telephone number of the incoming caller on our handset before answering
- Advice of Charge - Allows you to keep track of call costs
- Cell Broadcast - Allows you to subscribe to local news channels
- Mobile Terminating Fax - Another number you are issued with that receives faxes that you can then download to the nearest fax machine.

4.1.3 GSM Phase 2 + features

The standardization groups have already defined the next phase, 2+. This program covers multiple subscriber numbers and a variety of business oriented features. Some of the enhancements offered by Phase 2+ include:

- Available by 1998
- Upgrade and improvements to existing services
- Majority of the upgrade concerns data transmission, including bearer services and packet switched data at 64 kbit/s and above

- DECT access to GSM
- PMR/Public Access Mobile Radio (PAMR)-like capabilities
- GSM in the local loop
- Virtual Private Networks
- Packet Radio
- SIM enhancements
- Premium rate services
- Enhanced Data-over-GSM Speeds

4.2 GSM Network components

The GSM network is divided into four systems. Each system is comprises a number of functional units or individual components of the mobile network. The systems are:

- Subscriber Equipment (SE)
- Switching System (SS)
- Base Station System (BBS)
- The Operation and Support System (OSS)

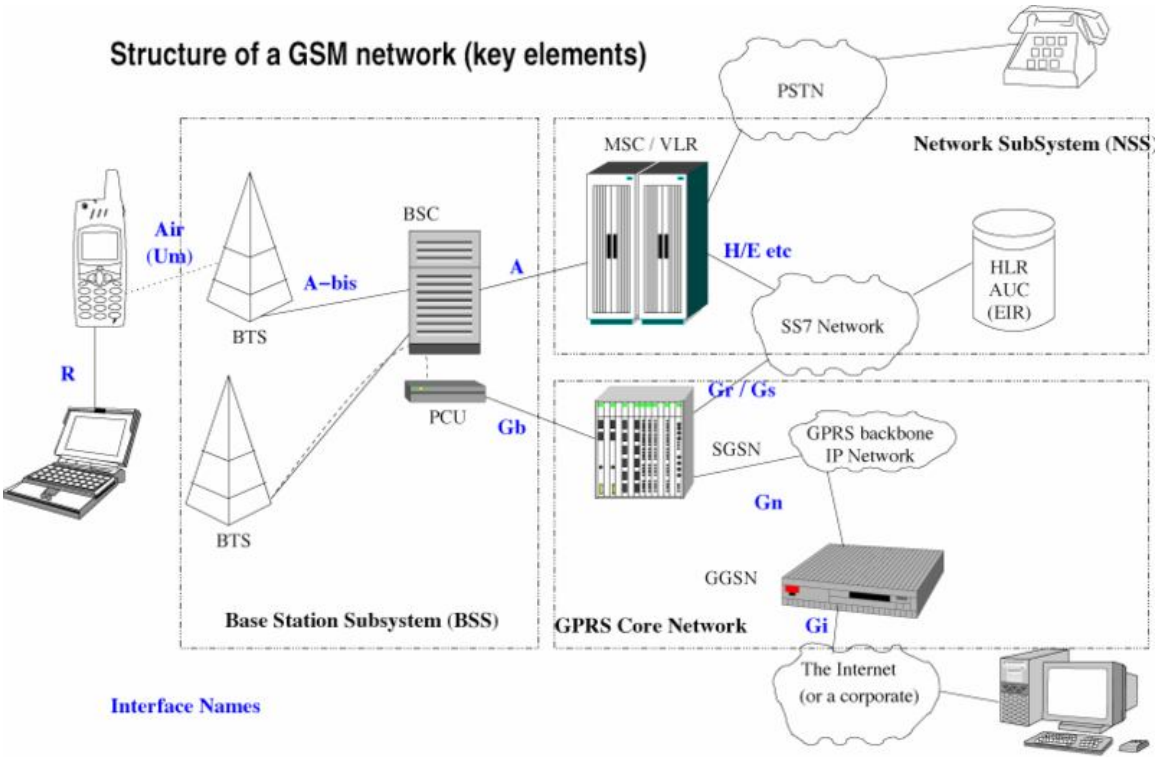

Figure 4.1 Structure of a GSM Network

The system consists of:

Subscriber Equipment (SE)

- Mobile Station (MS) - The mobile telephone

The Switching System (SS)

- Home Location Register (HLR) - A database which stores data about GSM subscribers, including the Individual Subscriber Authentication Key (Ki) for each Subscriber Identity Module (SIM).

- Mobile Services Switching Center (MSC) - The network element which performs the telephony switching functions of the GSM network. The MSC

is responsible for toll ticketing, network interfacing, common channel signaling.

- Visitor Location Register (VLR) - A database which stores temporary information about roaming GSM subscribers.

- Authentication Center (AUC) - A database which contains the International Mobile Subscriber Identity (IMSI) the Subscriber Authentication key (Ki), and the defined algorithms for encryption.

- Equipment Identity Register (EIR) - A database which contains information about the identity of mobile equipment in order to prevent calls from stolen, unauthorized, or defective mobile stations.

The Base Station System (BSS)

- Base Station Controller (BSC) - The network element which provides all the control functions and physical links between the MSC and BTS. The BSC provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in Base Transceiver Stations.
- Base Transceiver Station (BTS) - The network element which handles the radio interface to the mobile station. The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network.

The Operation and Support System (OSS)

- Message Center (MXE) - A network element which provides Short Message Service (SMS), voice mail, fax mail, email, and paging.

- Mobile Service Node (MSN) - A network element which provides mobile intelligent network (IN) services.

- Gateway Mobile Services Switching Center (GMSC) - A network element used to interconnect two GSM networks.

- GSM Interworking Unit (GIWU) - The network element which interfaces to various data networks.

4.3 Geographical network structure

Every telephone network needs a specific structure to route incoming calls to the correct exchange and then on to the subscriber. In a mobile network, this structure is very important because the subscribers move through the network; these structures are used to monitor their location.

4.3.1 Cell

A cell is the basic of a cellular system and is defined as the area of radio coverage given by one BS antenna system. Each cell is assigned a unique number called Cell Global Identity (CGI). In a complete network covering an entire country, the number of cells can be quite high.

4.3.2 Location Area (LA)

A location Area (LA) is defined as a group of cells. Within the network a subscriber's location is linked to the LA in whish they are currently located. The identity of the current LA is stored in the VLR.

When an MS crosses the boundary between two cells belonging to different LA's, it must report its new LA to the network. If it crosses a cell boundary within a LA, it does not report its new cell location to the network. When there is a call for an MS, a paging message is broadcast within all the cells belonging to the relevant LA.

4.3.3 MSC Service Area

An MSC service area is made up of a number of Las and represents the geographical part of the network controlled by one MSC. In order to be able to route a call to an MS, the subscriber's MSC service area is also recorded and monitored. The subscriber's MSC service area is stored in the HLR.

4.3.4 PLMN Service Area

A Public Land Mobile Network (PLMN) service area is the entire set of cells served by one network operator and is defined as the area in which an operator offers radio coverage and access to its network. In any one country there may be several PLMN service areas, one for each mobile operator's network.

4.3.5 Service Area

The GSM service area is the entire geographical area in which a subscriber can gain access to a GSM network. The GSM service area increases as more operators sign contracts agreeing to work together. Currently, the GSM service area spans dozens of countries across the world from Ireland to Australia, South Africa and the Americas.

International roaming is the term applied when an MS moves from one PLMN to another when abroad.

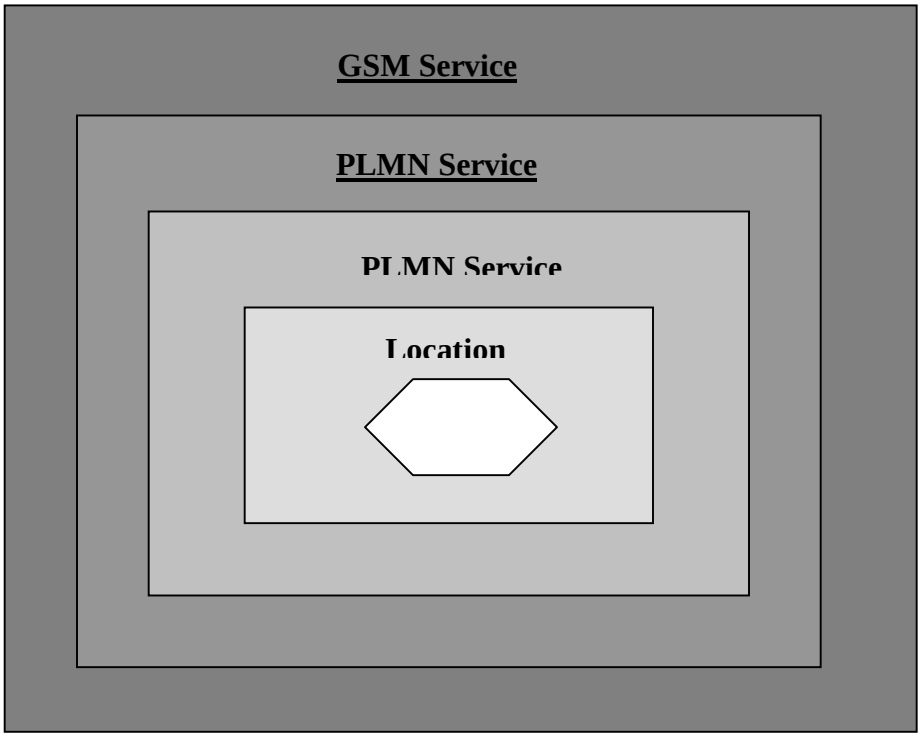

Figure 4.2 Relation between areas in GSM

4.4 GSM Frequency Bands

There are eight frequency bands defined in 3GPP TS 05.05:

1. Standard or primary GSM 900 Band, P GSM
2. GSM 450 Band
3. GSM 480 Band
4. GSM 850 Band
5. Extended GSM 900 Band, E GSM
6. Railways GSM 900 Band, R GSM
7. DCS 1 800 Band
8. PCS 1 900 Band

Though GSM has grown worldwide, it has expanded to operate at for main frequency bands: 900, 1800, 1900 and 800.

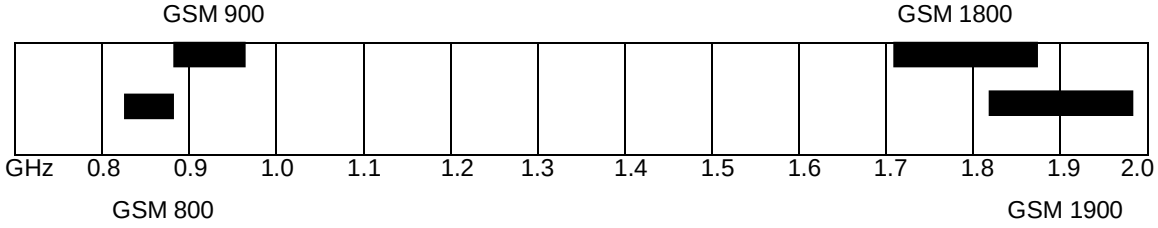

Figure 4.3 GSM Frequency Bands

System	Band	Uplink	Downlink	Channel Number
GSM 400	450	450.4 - 457.6	460.4 - 467.6	259 - 293
GSM 400	480	478.8 - 486.0	488.8 - 496.0	306 - 340
GSM 850	850	824.0 - 849.0	869.0 - 894.0	128 - 251
GSM 900 (P-GSM)	900	890.0 - 915.0	935.0 - 960.0	1 - 124
GSM 900 (E-GSM)	900	880.0 - 915.0	925.0 - 960.0	975 - 1023, (0, 1-124)
GSM-R (R-GSM)	900	876.0 - 880.0	921.0 - 925.0	955 - 973
DCS 1800	1800	1710.0 - 1785.0	1805.0 - 1880.0	512 - 885
PCS 1900	1900	1850.0 - 1910.0	1930.0 - 1990.0	512 - 810

Table 4.2 GSM Frequency Bands

Note: The table shows the extents of the band and not center frequency.

4.4.1 GSM-900

GSM-900 and GSM-1800 are used in most parts of the world: Europe, Middle East, Africa and most of Asia.

GSM-900 uses 890 - 915 MHz to send information from the Mobile Station to the Base Transceiver Station (uplink) and 935 - 960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used.

In some countries the GSM-900 band has been extended to cover a larger frequency range. This 'extended GSM', E-GSM, uses frequency range 880 - 915 MHz (uplink) and 925 - 960 MHz (downlink), adding 50 channels (channel numbers 975 to 1023 and 0) to the original GSM-900 band. The GSM specifications also describe 'railways GSM', GSM-R, which uses frequency range 876 - 915 MHz (uplink) and 921 - 960 MHz (downlink). Channel numbers 955 to 1023. GSM-R provides additional channels and specialized services for use by railway personnel.

All these variants are included in the GSM-900 specification.

4.4.2 GSM-1800

GSM-1800 uses 1710 - 1785 MHz to send information from the Mobile Station to the Base Transceiver Station (uplink) and 1805 - 1880 MHz for the other direction (downlink), providing 374 channels (channel numbers 512 to 885). Duplex spacing is 95 MHz.

GSM-1800 is also called PCS in Hong Kong and the United Kingdom. Most of the GSM operators in India use the 900 MHz band. Operators like, Airtel, Idea, and some others, use 900MHz in rural areas as well as in urban areas, where as hutch uses 1800 MHz everywhere except in its bpl network

4.4.3 GSM-850

GSM-850 and GSM-1900 are used in the United States, Canada, and many other countries in the Americas. GSM-850 is also sometimes erroneously called GSM-800.

In Australia, GSM 850 is the frequency allocated to Telstra's NextG Network, which was switched on in October 2006. The NextG Network is a step up from the 3G Network and is available at faster speeds Australia wide compared to the 3G Network, which is limited to only major population centers.

GSM-850 uses 824 - 849 MHz to send information from the Mobile Station to the Base Transceiver Station (uplink) and 869 - 894 MHz for the other direction (downlink). Channel numbers 128 to 251.

Cellular is the term used to describe the 850 MHz band, as the original analog cellular mobile communication system was allocated in this spectrum. Providers commonly operate in one or both frequency ranges.

4.4.4 GSM-1900

GSM-850 and GSM-1900 are used in the United States, Canada and many other countries in the Americas.

GSM-1900 uses 1850 - 1910 MHz to send information from the Mobile Station to the Base Transceiver Station (uplink) and 1930 - 1990 MHz for the other direction (downlink). Channel numbers 512 to 810.
PCS is an initialization for Personal Communications Service and merely represents the original name in North America for the 1900 MHz band.

4.4.5 GSM-400

Another less common GSM version is GSM-400. It uses the same frequency as and can co-exist with old analog NMT systems. NMT is a first generation 1G) mobile phone system which was primarily used in Nordic countries, Eastern Europe and Russia prior to the introduction of GSM. It operates in either 450.4 - 457.6 MHz paired with 460.4 - 467.6 MHz (channel numbers 259 to 293), or 478.8 - 486 MHz paired with 488.8 - 496 MHz (channel numbers 306 to 340). There is currently one GSM-400 network in Tanzania.

4.5 Frequency Concepts

System	GSM 800	P-GSM 900	E-GSM 900	GSM 1800	GSM 1900
Frequencies (MHz)					
• **Uplink**	**824-849**	**890-915**	**880-915**	**1710-1785**	**1850-1910**
• **Downlink**	**869-894**	**935-960**	**925-960**	**1805-1880**	**1930-1990**
Wavelength	**37.5 cm**	**~33 cm**	**~33 cm**	**~17 cm**	**~16cm**

Bandwidth	**25 MHz**	**25 MHz**	**35 MHz**	**75 MHz**	**60 MHz**
Duplex Distance	**45 MHz**	**45 MHz**	**45 MHz**	**95 MHz**	**80 MHz**
Carrier Separation	**200 kHz**	**200kHz**	**200 kHz**	**200 kHz**	**200 kHz**
Radio Channels	**125**	**125**	**175**	**375**	**300**
Transmission Rate	**270 kbits/s**	**270 kbits/s**	**270 kbits/s**	**270 kbits/s**	**270 kbits/s**

Table 4.3 Frequency concepts

Every GSM network uses one channel as a guard channel, which reduces the number of channels available for traffic by one. This is used to separate GSM frequencies from the frequencies of neighboring application, e.g. 889 MHz. In this way extra protection and quality for GSM calls is ensured.

Chapter 5

The Technology

5.1 3GSM

3GSM is the latest addition to the GSM family, which enables the provision of mobile multimedia services such as music, TV and video, rich entertainment content and Internet access. The technology on which 3GSM services are delivered is based on a GSM network enhanced with a Wideband-CDMA (W-CDMA) air interface – which is an over-the-air transmission element. Global operators have developed 3GSM as an open standard with the Third Generation Partnership Project (3GPP) standards organization.

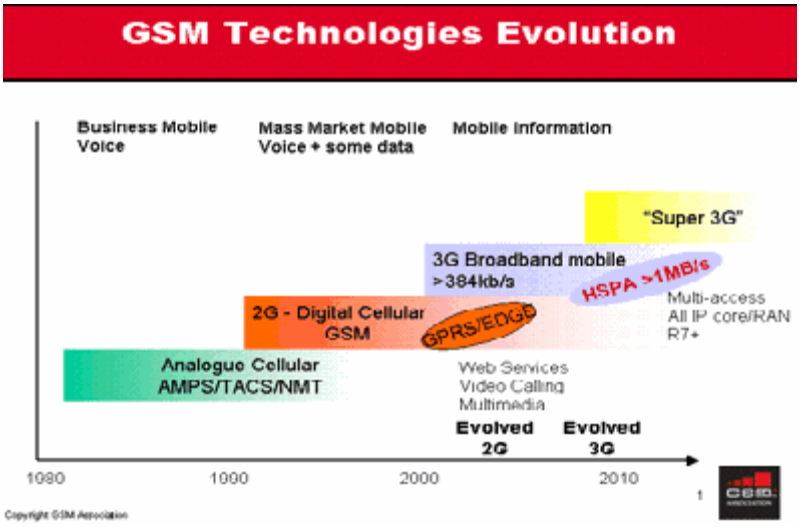

Figure 5.1 GSM Technologies Evolution

5.1.1 What is 3GSM?

Third generation (3G) is the generic term used for the next generation of mobile communications systems. These have been created to support the effective delivery of a range of multimedia services. In addition, they provide more efficient systems for the over-the-air transmission of existing services, such as voice, text and data that are available today.

Developed by the global GSM community as its chosen path for 3G evolution, UMTS is one of the International Telecommunications Union's (ITU's) family of third-generation mobile communications systems. UMTS uses a W-CDMA air interface, which lead some to refer to the technology as simply W-CDMA, creating confusion in the marketplace.

To alleviate this confusion and to highlight the backward compatibility of the system with second generation GSM, the GSM Association now refers to the range of high-speed multimedia services that can be delivered to users via mobile networks using UMTS/W-CDMA systems such as 3GSM, rather than simply the air interface technology.

The global 3G Partnership Project (3GPP), a collaboration of telecommunications standards bodies, is the organization through which much of the technical specifications are devised. The GSM Association is a market representation Partner of the 3GPP; as such it provides the 3GPP with market advice and a consensus view of market requirements from the operator community.

In summary, the GSM Association's vision of 3GSM is based on today's GSM standard, but evolved, extended and enhanced to include an additional radio air interface, better suited for high speed and multimedia data services. This system will enable users of current second generation GSM wireless networks to migrate easily to the new third generation services, with minimal disruption.

5.1.2 Data speeds and services enabled by 3GSM

The use of the W-CDMA air interface significantly increases the data transfer rate of GSM networks, offering average downlink rates of around 300 kbit/s.

TV and video on demand, high-speed multimedia data services and mobile Internet access are just a few of the offerings available to users. 3GSM expands the potential for content-rich information and communication services, as well as providing enhanced capacity for traditional voice services. 3GSM bridges the gap between the wireless world and the computing/Internet world, creating the possibility of seamless inter-operation between the two.

One of the most important characteristics of 3GSM is that it has been developed to be backward compatible with GSM systems, which have been deployed by 680 operators in more than 200 countries and territories. This interoperability of systems and services will ensure the continuation of the worldwide roaming experience users have enjoyed with GSM

The look and feel of 3GSM phones are now being dictated by functionality demands rather than technical constraints. For example, to support new Internet and multi-media services, larger, more convenient viewing screens are offered. As a result, the variation of form factors offered is likely to increase significantly and handsets could vary from wristwatch style 'simple' telephones to mini PC-type personal digital assistants (PDAs) for web-browsing usage.

5.2 GPRS

GPRS (General Packet Radio Service) is the world's most ubiquitous wireless data service, available now with almost every GSM network. GPRS is a connectivity solution based on Internet Protocols that supports a wide range of enterprise and consumer applications. With throughput rates of up to 40 kbit/s, users have a similar access speed to a dial-up modem, but with the convenience of being able to connect from anywhere. GPRS customers enjoy advanced, feature-rich data services such as color Internet browsing, e-mail on the move, and powerful visual communications such as video streaming, multimedia messages and location-based services.

For operators, the adoption of GPRS is a fast and cost-effective strategy that not only supports the real first wave of mobile Internet services, but also represents a big step towards 3GSM (or wideband-CDMA) networks and services.

5.2.1 GPRS Class Types

The class of the device determines the speed at which GPRS can be used.

For example, the majority of GPRS terminals will be able to download data at speeds of up to 24Kbps (kilobytes per second). At the higher end, speeds are theoretically possible up to 171.2 kbit/sec when 8 slots are assigned at the same time to a single user, in reality 40-50Kbps.

PC cards capable of GPRS will send data up to speeds of 48Kbps.

Compare this to current data speeds available:

Type	Uplink (Sending)	Downlink (Receiving)
GPRS	14 kbps	28-64 kbps
GSM CSD	9.6-14 kbps	9.6-14 kbps
HSCSD	28 kbps	28 kbps
Dial-UP	56 kbps	56 kbps
ISDN Standard	64 kbps	64 kbps
ADSL	256 kbps	512 kbps
Broadband	2 Mbps	2 Mbps

Table 5.1 GPRS Class Types

5.2.2 GPRS Multislot Classes

Multislot classes are product dependant, and determine the maximum achievable data rates in both the uplink and downlink directions. Written as (for example) 3+1 or 2+2, the first number indicates the amount of downlink timeslots (what the mobile phone is able to receive from the network). The second number indicates the amount of uplink timeslots (how many timeslots the mobile phone is able to transmit).

The active slots determine the total number of slots the GPRS device can use simultaneously for both uplink and downlink communications.

Class A, Class B & Class C

The class indicates the mobile phone capabilities.

Class A - Class A mobile phones can be connected to both GPRS and GSM services simultaneously.

Multislot Class	Downlink Slots	Uplink Slots	Active Slots
1	1	1	2
2	2	1	3
3	2	2	3
4	3	1	4
5	2	2	4
6	3	2	4
7	3	3	4
8	4	1	5
9	3	2	5
10	4	2	5
11	4	3	5
12	4	4	5

Table 5.2 GPRS Multislot Classes

Class B - Class B mobile phones can be attached to both GPRS and GSM services, using one service at a time. Class B enables making or receiving a voice call, or sending/receiving an SMS during a GPRS connection. During voice calls or SMS, GPRS services are suspended and then resumed automatically after the call or SMS session has ended.

Class C - Class C mobile phones are attached to either GPRS or GSM voice service. You need to switch manually between services.

5.3 EDGE

Further enhancements to GSM networks are provided by Enhanced Data rates for GSM Evolution (EDGE) technology. EDGE provides up to three times the data capacity of GPRS. Using EDGE, operators can handle three times more subscribers than GPRS; triple their data rate per subscriber, or add extra capacity to their voice communications. EDGE uses the same TDMA (Time Division Multiple Access) frame structure, logic channel and 200kHz carrier bandwidth as today's GSM networks, which allows it to be overlaid directly onto an existing GSM network. For many existing GSM/GPRS networks, EDGE is a simple software-upgrade.

EDGE allows the delivery of advanced mobile services such as the downloading of video and music clips, full multimedia messaging, high-speed colour Internet access and e-mail on the move.

Due to the very small incremental cost of including EDGE capability in GSM network deployment, virtually all new GSM infrastructure deployments are also EDGE capable and nearly all new mid- to high-level GSM devices also include EDGE radio technology. The Global mobile Suppliers Association (GSA) states that, as of November 2006, there were 156 commercial GSM/EDGE networks in 92 countries, out of a total of 213 GSM/EDGE deployments in 118 countries.

Chapter 6

GSM Security

Security in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the International Mobile Subscriber Identity (IMSI). This information, along with the individual subscriber authentication key (Ki), constitutes sensitive identification credentials analogous to the Electronic Serial Number (ESN) in analog systems such as AMPS and TACS. The design of the GSM authentication and encryption schemes is such that this sensitive information is never transmitted over the radio channel. Rather, a challenge-response mechanism is used to perform authentication. The actual conversations are encrypted using a temporary, randomly generated ciphering key (Kc). The MS identifies itself by means of the Temporary Mobile Subscriber Identity (TMSI), which is issued by the network and may be changed periodically (i.e. during hand-offs) for additional security.

The security mechanisms of GSM are implemented in three different system elements; the Subscriber Identity Module (SIM), the GSM handset or MS, and the GSM network. The SIM contains the IMSI, the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN). The GSM handset contains the ciphering algorithm (A5). The encryption algorithms (A3, A5, A8) are present in the GSM network as well. The Authentication Center (AUC), part of the Operation and Maintenance Subsystem (OMS) of the GSM network, consists of a database of identification and authentication information for subscribers. This information consists of the IMSI, the TMSI, the Location Area Identity (LAI), and the individual subscriber authentication key (Ki) for each user. In order for the authentication and security

mechanisms to function, all three elements (SIM, handset, and GSM network) are required. This distribution of security credentials and encryption algorithms provides an additional measure of security both in ensuring the privacy of cellular telephone conversations and in the prevention of cellular telephone fraud.

Figure 6.1 demonstrates the distribution of security information among the three system elements, the SIM, the MS, and the GSM network. Within the GSM network, the security information is further distributed among the authentication center (AUC), the home location register (HLR) and the visitor location register (VLR). The AUC is responsible for generating the sets of RAND, SRES, and Kc which are stored in the HLR and VLR for subsequent use in the authentication and encryption processes.

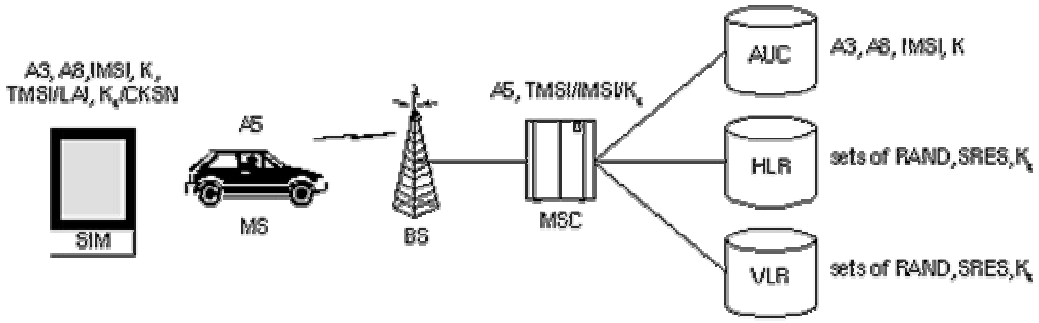

Figure 6.1 Distribution of Security Features in the GSM Network

6.1 Authentication

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit random number (RAND) is sent to the MS. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the signed response (SRES) from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber. Note that the individual subscriber authentication key (Ki) is never transmitted over the radio channel. It is present in

the subscriber's SIM, as well as the AUC, HLR, and VLR databases as previously described. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure indicated to the MS. Figure 6.2 shown below illustrates the authentication mechanism.

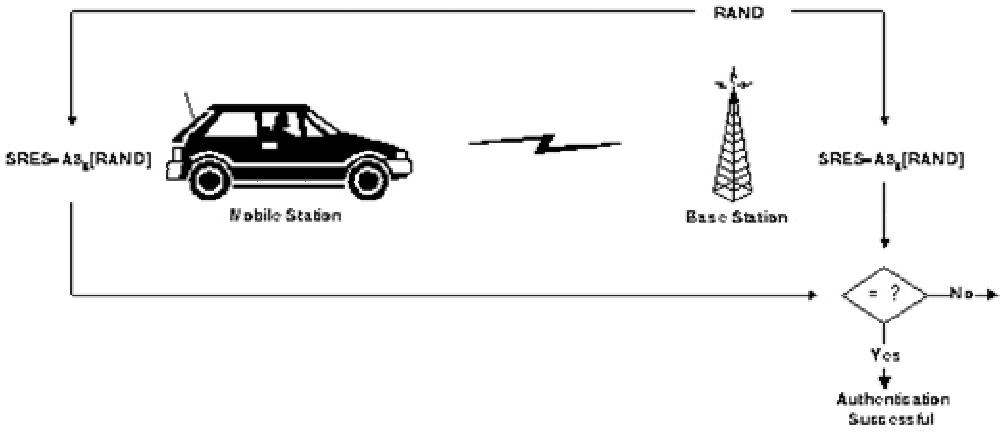

Figure 6.2 GSM Authentication Mechanism

The calculation of the signed response is processed within the SIM. This provides enhanced security, because the confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.

6.2 Signaling and Data Confidentiality

The SIM contains the ciphering key generating algorithm (A8) which is used to produce the 64-bit ciphering key (Kc). The ciphering key is computed by applying the same random number (RAND) used in the authentication process to the ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki). As will be shown in later sections, the ciphering key (Kc) is used to encrypt and decrypt the data between the MS and BS. An additional level of security is provided by having the means to change the ciphering key,

making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required by network design and security considerations. Figure 6.3 below shows the calculation of the ciphering key (Kc).

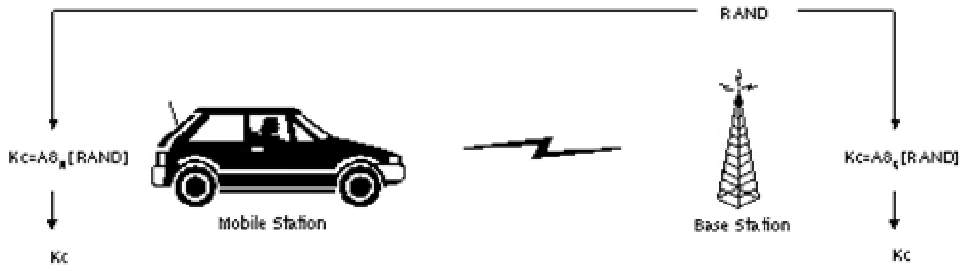

Figure 6.3 Ciphering Key Generation Mechanism

In a similar manner to the authentication process, the computation of the ciphering key (Kc) takes place internally within the SIM. Therefore sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.

Encrypted voice and data communications between the MS and the network is accomplished through use of the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc). Figure 6.4 below demonstrates the encryption mechanism.

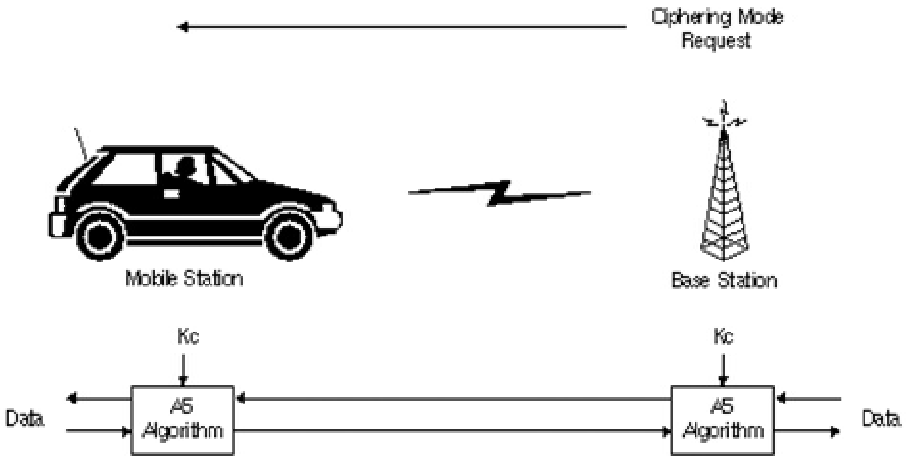

Figure 6.4 Ciphering Mode Initiation Mechanism

4.3 Subscriber Identity Confidentiality

To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. The TMSI is sent to the mobile station after the authentication and encryption procedures have taken place. The mobile station responds by confirming reception of the TMSI. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI. The TMSI allocation/reallocation process is shown in Figure 6.5 below.

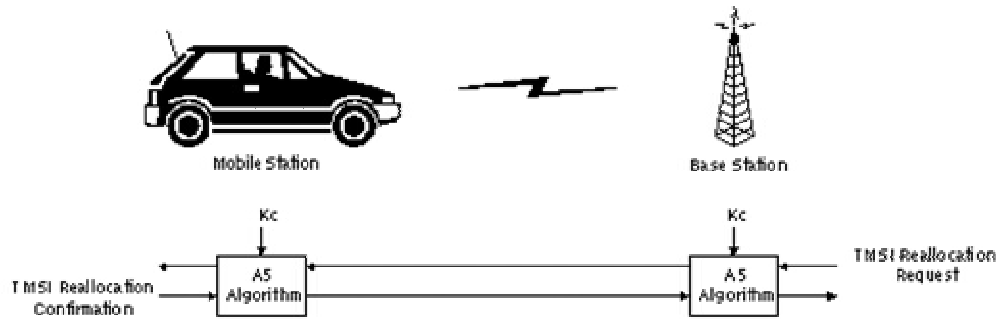

Figure 6.5 TMSK Reallocation Mechanism

Chapter 7

GSM in Bangladesh

7.1 The Providers

Among the six mobile phone companies in Bangladesh, five of them are using the GSM technology. The companies are:

1. GrameenPhone Ltd.
2. Sheba Telecom (Pvt.) Ltd. (Banglalink)
3. Teletalk Bangladesh Ltd
4. TM International (Bangladesh) Ltd (AKTEL)
5. Warid Telecom International Ltd

7.1.1 GrameenPhone

Network Information

Operator Name:	GrameenPhone Ltd
Network Name:	Grameenphone
Technology:	GSM 900
Network Status:	Live March 1997
Web Site:	www.grameenphone.com

Table 7.1 Network Information of GrameenPhone

Coverage Map

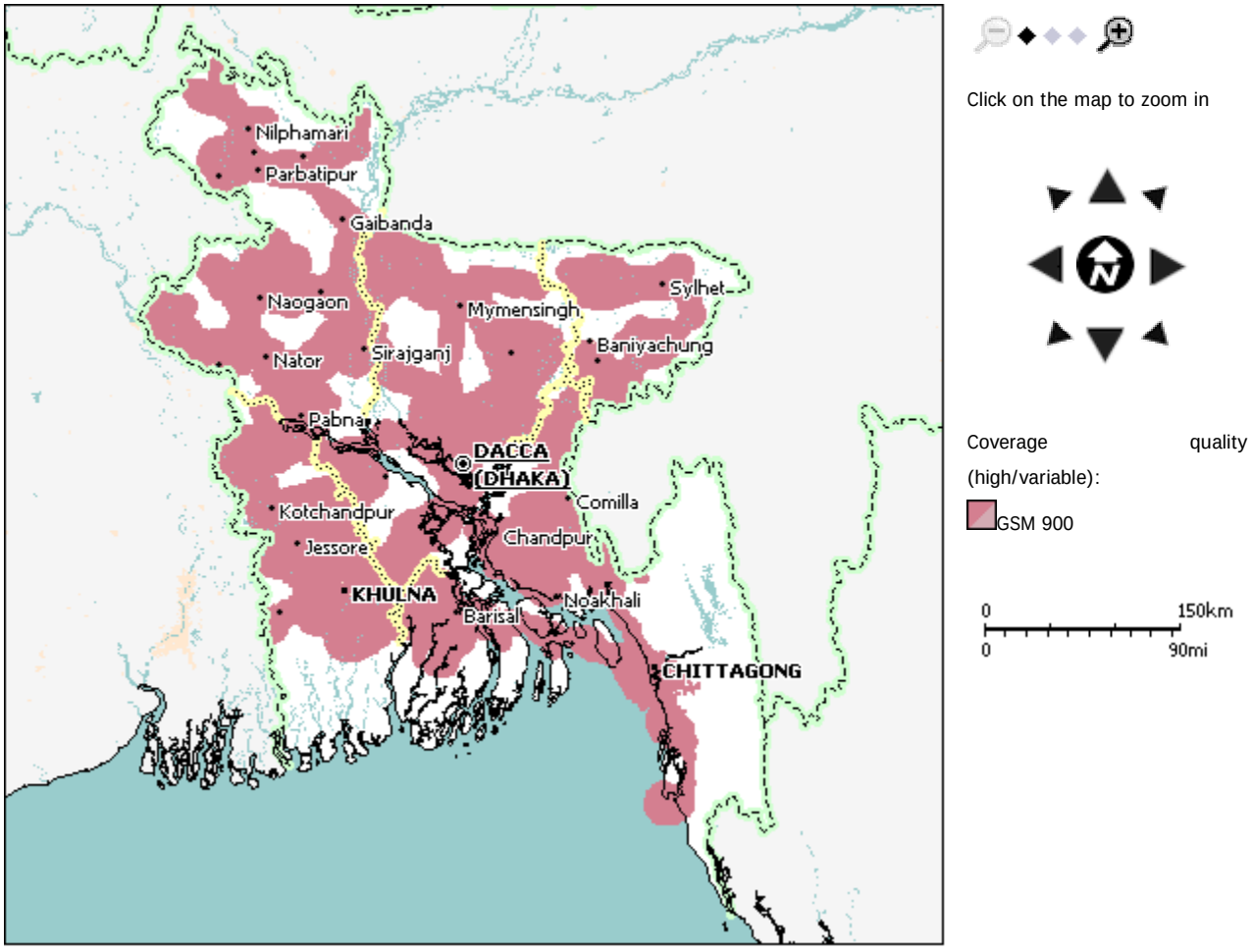

Figure 7.1 Coverage Map of GrameenPhone

7.1.2 Banglalink

Network Information:

Operator Name:	Sheba Telecom (Pvt.) Ltd.
Network Name:	Banglalink
Technology:	GSM 900
Network Status:	Live September 1998
Web Site:	www.banglalinkgsm.com

Table 7.2 Network Information of Banglalink

Coverage Map

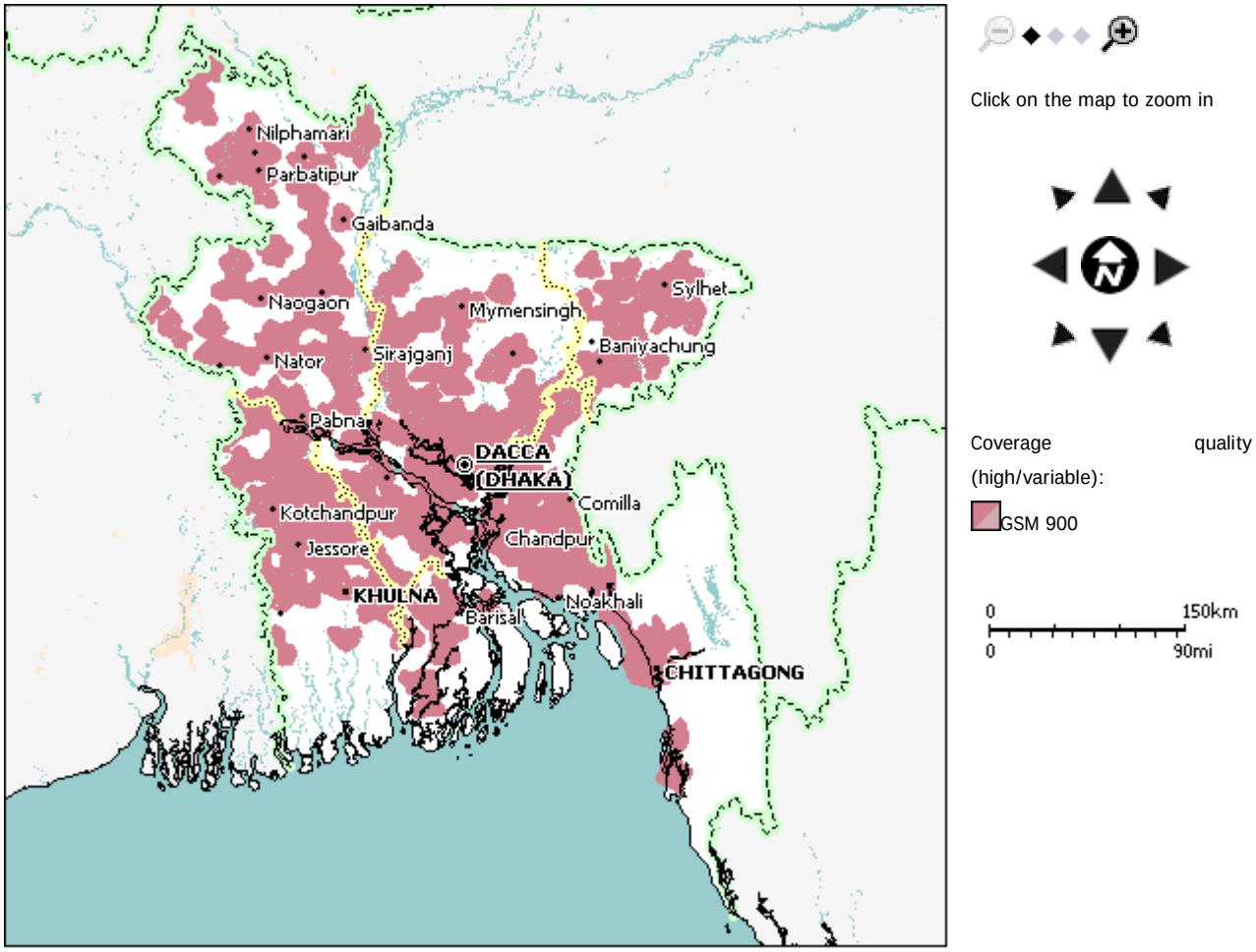

Figure 7.2 Coverage Map of Banglalink

7.1.3 Teletalk

Network Information

Operator Name:	Teletalk Bangladesh Ltd
Network Name:	Teletalk
Technology:	GSM 900
Network Status:	Live December 2004
Web Site:	www.bttb.gov.bd

Table 7.3 Network Information of TeleTalk

7.1.4 AKTEL

Network Information

Operator Name:	TM International (Bangladesh) Ltd
Network Name:	AKTEL
Technology:	GSM 900
Network Status:	Live October 1997
Web Site:	www.aktel.com

Table 7.4 Network Information of Aktel

Coverage Map

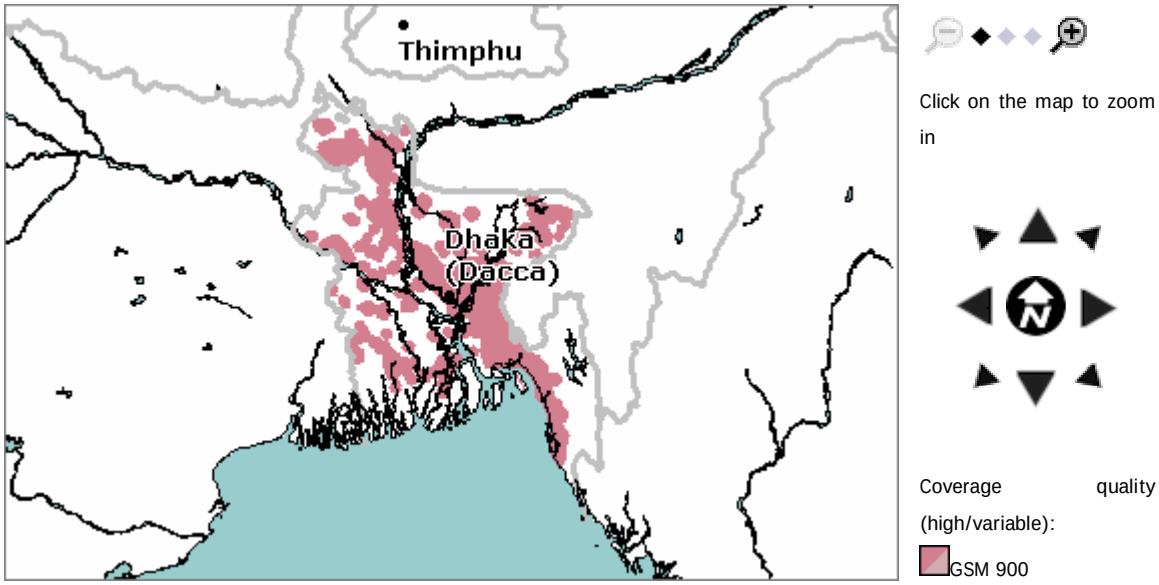

Figure 7.3 Coverage Map of Aktel

7.1.5 Warid

Network Information

Operator Name:	Warid Telecom International Ltd
Network Name:	Warid Telecom
Technology:	GSM 1800
Network Status:	Planned September 2006
Web Site:	www.waridtel.com

Table 7.5 Network Information of Warid

Chapter 8

Conclusion and Future Works

In this thesis paper, I have tried to give an overview of the GSM technology as well as its application in Bangladesh. As with any overview, this small paper cannot cover every aspect. There are many details missing. I believe, however, that I gave the general scenario of GSM and the philosophy behind its design and applications.

The security mechanisms specified in the GSM standard make it the most secure cellular telecommunications system available. The use of authentication, encryption, and temporary identification numbers ensures the privacy and anonymity of the system's users, as well as safeguarding the system against fraudulent use. Even GSM systems with the A5/2 encryption algorithm, or even with no encryption are inherently more secure than analog systems due to their use of speech coding, digital modulation, and TDMA channel access

Though GSM is a very complex standard and I guess that is the price paid to achieve the level of integrated service and quality offered to the telecommunication system.

References

Books:

[1] Jan a. Audestad. Network aspects of the GSM system. In EUROCON 88, June 1988.

[2] David M Balston. The pan-European cellular technology. In R.C.V. Macario, editor, *Personal and Mobile Radio Systems.* Peter Peregrinus, London, 1991.

[3] M. Bezler et al. GSM station system. *Electrical Communication*, 2nd Quarter 1993.

[4] C. Dechaux and R. Scheller. What are GSM and DCS. *Electrical Communication*, 2nd Quarter 1993.

[5] John Scourias, *Overview of the Global System for Mobile Communications*.

[6] Student Text EN/LZT 123 3321 R4A,*GSM System Survey,* Ericsson

Websites:

[1] http://www.gsmworld.com/

[2] http://en.wikipedia.org/wiki/GSM

[3] http://www.gsm-security.net/

[4] https://styx.uwaterloo.ca/~jscouria/GSM/gsmreport.html#1