The Libyan Academy

Tripoli - Libya

School of Applied Sciences and Engineering

Department of Electrical and Computer Engineering

Monitoring a Place and Controlling a System Remotely via GSM/ UMTS Networks

By : Ramadan Almakhzoom Baga

A Dissertation Submitted to the Department of Electrical and Computer Engineering in conformity with the Department Requirements as partial fulfillment for the Degree of Master of Engineering Science

Supervised by: Prof. Marai Mohamed Abosetta

April , 2014

Acknowledgment

My sincerest appreciation to my supervisor Professor Marrai M. Abosetta for his suggestions, corrections , continuous guidance and all that he has done to success in this dissertation .

To my patient wife and cheerful kids ,who give a taste to my life. Also I would like to thank all friends who encourage and support me to accomplish this work .

Abstract

It is very desirable to monitor a place (as a store) regarding smoke or fire and controlling that by doing the appropriate action remotely . The problem is how to get an alarm and video image showing that fire or smoke from the camera which is monitoring that place and how to activate a Fire extinguishing system while you are so far from that place . The existing infrastructure of mobile network which supports the third generation can be used to carry the alarm and the video image from the monitored place to user's mobile at anywhere to take the appropriate action and carry the control signals from the user's mobile to the monitored place . A system has been designed and implemented to monitor a designated place and related system has been activated appropriately through GSM/3G network .

Table of contents

Chapter 4: Apparatus and Devices

Chapter 5: Experimental Work and Results

List of figures

List of Acronyms

AuC : Authentication Center

BS : Base Stations

BSC : Base Station Controllers

BSS: Base Station Subsystem

BTS : base transceiver stations

BRAN: Broadband Radio Access Network

CAMEL : Customized Application for Mobile network Enhanced Logic

CDMA : Code Division Multiple Access

CGI: Cell Global Identity

CBC: Charge Back Center

CN: Core Network

CS : Circuit-Switched

CSE : CAMEL Service Environment

CUG: Closed User Group

EDGE : Enhanced Data rates for GSM Evolution

EIR : Equipment Identity Register

ETSI : European Telecommunications Standards Institute

FDD : Frequency Division Duplex

FDMA : Frequency Division Multiple Access

GMSC: Gateway Mobile services Switching Center

GGSN: Gateway GPRS Support Node

GSM : Global System for Mobile communication

GIWU: GSM interworking unit

GRAN : GSM Radio Access Network

GPRS: General Packet Radio Service

HLR: Home Location Register

HSCSD : High Speed Circuit Switched Data

HSPSD : High Speed Packet Switched Data

IMEI : International Mobile Equipment Identities

IWF : Interworking functions

IMSI: International Mobile Subscriber Identity

ITU : International Telecommunications Union

ITU-R : ITU Telecommunications Radio Sector

ITU-T : ITU Telecommunications Standardization Sector

LMSI : Local Mobile Station Identity

LA : Location Areas

LSA : Local Service Area

LAI : Location Area Identity

LCS : Location Services

MXE : Message Center

MS : Mobile Station

MSC : Mobile Services Switching Center

MSISDN: Mobile Station International ISDN

MSN : Mobile Service Node

MSRN: Mobile Station Roaming Number

NAM : Network Access Mode

NSS : Network Switching Subsystem

O&M : Operation and Maintenance

OMC : Operations and Maintenance Center

OSS: Operation and Support System

PIN : Personal Identifier Number

PLMN: Public Land Mobile Network

PS: Packet Switched

PSTN : Public Switching Telephone Network

RNC : Radio Network Controller

SGSN : Serving GPRS Support Node

SIM : Subscriber Identity Module

SMS : Short messaging Service

SMS SC: SMS Serving Center

SS : Switching System

TDD :Time Division Duplex

TDMA : Time Division Multiple Access

TMSI : Temporary Mobile Station Identity

TRAU : Transcoder and Adaptation Unit

UE: User Equipment

UMTS : Universal Mobile Telecommunications System

USIM : Universal Subscriber Identity Module

USRAN : UMTS Satellite Radio Access Network

UTRAN: UMTS Terrestrial Radio Access Network

VLR: Visitor Location Register

WCDMA : Wideband Code Division Multiple Access

WLAN : Wireless Local Area Network

CHAPTER 1

Introduction

Introduction

1.1-Introduction

Mobile communication is the most important technology in the telecommunication industry because of its great features like providing access to users at anytime and anywhere in the world. Communication everywhere, with everybody, and at any time was the dream and goal of researchers, engineers and users, since the advent of the first wireless communication systems.

Many evolutions in the technology as digitalization of communication systems, enormous progress in microelectronics, computers and software technology, the invention of efficient algorithms and procedures for compression, security and processing of all kinds of signals, as well as the development of flexible communication protocols have all helped to reach that goal. Today, technologies are available that enable the realization of high-performance and cost-effective communication systems for many application areas.

Using current wireless communication systems, the most popular of which are GSM (Global System for Mobile Communication) and UMTS (Universal Mobile Telecommunication System) , it is possible to not only roam within a network, but also between different networks.

Mobility which enables users to move and roam so freely are : terminal mobility and personal mobility. In the case of terminal mobility, the subscribers are connected to the network in a wireless way and can move with their terminal freely, even during a call is taking a place . The degree of mobility depends on the type of mobile radio network .

The users identify themselves , by using a chip card, at the place where they are currently staying and have access to the network . This identification is done by a worldwide unique and uniform addressing system which is an important requirement for personal mobility. In the mobile communication systems ,terminal mobility is the predominant issue mobile technology contains the essential intelligent functions for the support of personal mobility, especially with regards to user identification and authentication , and for the localization and administration of mobile users. GSM was used almost exclusively for speech communication and for Short Message Service

(SMS). In the mean time, additional data services have been realized, most notably the High Speed Circuit Switched Data (HSCSD) and the General Packet Radio Service (GPRS), which enable improved data rate performance by allowing for more than one GSM timeslot to be used by a terminal for a service at a time. The driving factor for new (and higher bandwidth) data services obviously is wireless access to the Internet. These additions are already working towards closing the gap between wireless and fixed networks. A further step was the introduction of third-generation (3G) mobile communication networks. The 3G networks, known as the Universal Mobile Telecommunication System (UMTS) in Europe and as the International Mobile Telecommunication System 2000 (IMT- 2000) worldwide, UMTS networks have more capabilities to provide video calls , web browsing , video conferencing and much more applications . Thanks to multi-mode terminals, which can handle both standards (GSM and UMTS), wireless network users usually do not even realize which technology they are currently using while making a call or using other wireless services. Regarding the relevance of GSM technology, it is important to note that most network providers who have implemented UMTS are using basically the same fixed backbone infrastructure architecture as used for GSM and GPRS together.

1.2- Aim of Dissertation

The objective of the work is to design and implement a system that can monitor a remote place regarding a fire and activate the appropriate system (extinguishing system) by using a mobile phone through GSM/UMTS networks as the place of interest is within the coverage area of the those mobile networks . The process is activated by sending a wireless signal from the sensor (smoke sensor) , when it senses a smoke , to the 3G camera which is loaded with a USIM card and located around , the camera will send a smoke alarm message and establish a video call to the predefined user mobile through the UMTS network . By receiving the video call , the user will do the appropriate action which is the activation of the extinguishing system . This action will be done by sending SMS (with specific text) to the number of the SIM card which is located in the control device (GSM-SMS communicator) at the monitored place through the GSM network .

Also one can dial in the 3G camera to have live video audio, live call, to take photo and record video on the 3G camera .

1.3- Outlines of Dissertation

The structure of the dissertation is classified into six chapters as follows:

Chapter 1 "Introduction" Presents an introduction to this work and what the goal of this dissertation is .

Chapter 2 "Wireless Technology" Introduces the concept of wireless technology , how can it be classified , and what are the advantages and disadvantages of wireless technology.

Chapter 3 "Mobile Networking Technology" Explains the mobile networking technology : multiple access , channel structure and network structure in GSM and UMTS systems

Chapter 4 "Apparatus and Devices" Presents the elements that are used in this work as smoke sensor , 3G security camera and GSM-SMS communicator and their features .

Chapter 5 "Experimental Work and Results" Demonstrates the actual work of this dissertation and how the elements are used in the presence of GSM and UMTS coverage .

Chapter 6 "Conclusions and Recommendations" Concludes with a summary of the contributions made in this dissertation .

CHAPTER 2

Wireless Technology

Wireless Technology

2.1- Introduction

Wireless telecommunications, is the transfer of information (audio, video, text, etc..) between two or more points that are physically not connected through wire lines . Distances can be short, as a few meters as in television remote control; or long ranging from thousands to millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of wireless technology include GPS units, garage door openers , wireless computer mice, keyboards and headsets, satellite television and cordless telephones.

Wireless is very feasible in long range communications when the implementation of the wires are impossible or impractical . The term is commonly used in the telecommunications industry to refer to telecommunications systems (e.g. radio transmitters and receivers, remote controls, computer networks, network terminals, etc.) which use some form of energy (e.g. radio frequency (RF), infrared light, laser light, visible light, acoustic energy, etc.) to transfer information without the use of wires. Information is transferred in this manner over both short and long distances .

Wireless technology has become the most exciting area in telecommunication and networking . The rapid growth of mobile telephone use, various satellite services, and the wireless Internet are generating tremendous changes in telecommunications and networking . Wireless is convenient and often less expensive to deploy than fixed service, but wireless is not perfect. There are limitations , and difficulties that may ultimately prevent wireless technologies from reaching their full potential. Regardless of the design of the transmission system, there will be errors ,resulting in the change of one or more bits in a transmitted frame.

wireless communications methods and services have been enthusiastically adopted by people throughout the world , the mobile radio communications industry has grown by orders of magnitude ,fueled by digital and RF circuit fabrication improvements ,new large-scale circuit integration , and other miniaturization technologies which make portable radio equipment smaller , cheaper ,and more reliable . Digital switching techniques have facilitated the large scale deployment of affordable , easy-to-use radio communication networks Wireless communication is the fastest-growing part of the very dynamic field of electronic communication.

2.2-History of Wireless Telecommunication :

In order to understand the present state of the art, a brief glimpse of the past will be useful. Present-day systems have evolved from their predecessors. Similarly, future systems can be expected that will be developed from current ones.

-The Beginning Wireless telecommunication began only a little later than the wired variety. Morse's telegraph (1837) and Bell's telephone (1876) were soon followed by Hertz's first experiments with radio (1887). Hertz's system was a laboratory curiosity, but Marconi communicated across the English Channel in 1899 and across the Atlantic Ocean in 1901. These successes led to the widespread use of radio for ship-to-ship and ship-to-shore communication using Morse code.

Early wireless systems used crude, though often quite powerful, spark gap transmitters, were suitable only for radiotelegraphy. The invention of the triode vacuum tube by De Forest in 1906 allowed for the modulation of a continuous-wave signal and made voice transmission practical.

Reginald Fessenden made the first public broadcast of voice and music in late 1906. Commercial radio broadcasting in both the United States and Canada began in 1920. Early radio transmitters were too cumbersome to be installed in vehicles.

The first mobile radio systems, for police departments, were one-way, with only a receiver in the police car. The first such system to be considered practical was installed in Detroit in 1928. Two-way police radio, with the equipment occupying most of the car trunk, began in the mid-1930s. Amplitude modulation (AM) was used until the late 1930s, when frequency modulation (FM) began to displace it.

World War II provided a major incentive for the development of mobile and portable radio systems, including two-way systems known as “ walkie talkies ” that could be carried in the field and might be considered the distant ancestors of today’s cell phones. FM proved its advantages over AM in the war.

Soon after the end of World War II, two systems were developed that presaged modern wireless communication. AT&T introduced its Improved Mobile Telephone Service **(IMTS)** in 1946, featuring automatic connection of mobile subscribers to the public switched telephone network **(PSTN)**. This was an expensive service with limited capacity, but it did allow true mobile telephone service. In 1947, the American government set up the Citizens’ Band **(CB) radio** service. Initially it used frequencies near 460 MHz, but in that respect it was ahead of its time, since equipment for the UHF range was prohibitively expensive. Frequencies in the 27-MHz band were allocated in 1958, and CB radio immediately became very popular. The service was short range, had no connection to the PSTN, and offered users no privacy, but it was cheap and easy to set up. Another appearing appliance has become ubiquitous: the cordless phone. Usually intended for very short-range communication within a dwelling and its grounds, the system certainly lacks range and drama, but it does have connectivity with the PSTN. Most cordless phones use analog FM in the 46- and 49-MHz bands, but some of the latest models are digital and operate at either 900 MHz or 2.4 GHz. Cordless phones are cheap and simple to use, but their range is limited and, except for the digital models, they offer little privacy.

Pagers were introduced in 1962. The first models merely signaled the user to find a telephone and call a prearranged number. More recent models can deliver an alphanumeric message and even carry a reply. Though relatively limited in function, pagers remain very popular due to their low cost and small size.

-The Cellular Revolution :

The world’s first cellular radio service was installed in Japan in 1979, followed in 1983 by North American services. Cellular systems are quite different from previous radio telephone services such as IMTS. In that, instead of using a single powerful transmitter located on a tall tower for wide coverage, Many small cells are used so that frequencies can be reused at short distances. Of course, a portable or mobile telephone may move from one cell to another cell during the course of a conversation. In fact, this **handoff** may occur several times during a conversation. Theoretically at least, the number of users in a cellular system can be increased indefinitely, simply by making the cells smaller. The first cellular systems used analog FM transmission, but digital modulation schemes, which provide greater privacy and can use bandwidth more efficiently, are used in all the new systems. These personal communication systems (**PCS)** usually operate in a higher frequency range (about 1.9 GHz compared with 800 MHz for North American cellular service) . Current cellular systems are optimized for voice ,SMS ,data ,video calls and even web browsing .

2.3- Classification of wireless systems :

The wireless systems can be classified into different segments according to the following criteria :

- **Applications:** wireless applications include voice, Internet access, web browsing, paging and short messaging, subscriber information services, file transfer, and video teleconferencing.
- **Systems :**wireless systems include cellular telephone systems, wireless LANs, wide-area wireless data systems, microwave and radio systems and satellite systems .
- **Coverage regions :**include in building, campus, city, regional, and global.

The question of how best to characterize wireless communications along these various segments has resulted in considerable fragmentation in the industry, as evidenced by the many different wireless products, standards, and services being offered or proposed. One reason for this fragmentation is that different wireless applications have different requirements. Voice systems have relatively low rate requirements (around 20 Kbps) and can tolerate a fairly high probability of bit error (bit error rates, or BERs, of round 10^{-3}), but the total delay must be less than 100 msec or it becomes noticeable to the end user. On the other hand, data systems typically require much higher data rates (1-100 Mbps) and very small BERs (the target BER is 10^{-8} and all bits received in error must be retransmitted) but do not have a fixed delay requirement. Real-time video systems have high data rate requirements coupled with the same delay constraints as voice systems, while paging and short messaging have very low data rate requirements and no delay constraints. These diverse requirements for different applications make it difficult to build one wireless system that can satisfy all these requirements simultaneously. Therefore, at least in the near future, wireless systems will continue to be fragmented, with different protocols tailored to support the requirements of different applications.

2.4– Advantages and Disadvantages of wireless technology :

Any technology has advantages and disadvantages according to their use , features , cost and some other parameters , wireless technology has advantages and disadvantages as :

2.4.1- Advantages of wireless technology :

The hard-wiring drawbacks has led many to seek a longer range and more flexible alternative in wireless networks. the wireless networks have more advantages over the wired networks :

- **Convenience:**
  The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (a home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.
- **Mobility:**
  With the emergence of public wireless networks, users can access the internet even outside their normal work environment or even while they are in movement
- **Productivity :**
  Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as their work can be accomplished from any convenient location .

- **Deployment:**

  Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building). It is Faster to build wireless network than the fixed. Also Ideal for the non-reachable places such as across river or mountain or rural area .

- **Expandability:**

  Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.

- **Cost:**

  Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables. Implementation cost is cheaper than wired network.

2.4.2- Disadvantages of wireless technology :

For a given networking situation, wireless may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology **:**

- **Speed:**

  The speed on most wireless networks (typically 1-54 Mbps) is far slower than even the slowest common wired networks (100Mbps up to several Gbps). However, Due to its Low speed compared to wired network , in specialized environments, the throughput of a wired network might be necessary **.**

- **Security:**

  To combat this consideration, wireless networks may choose to utilize some of the various encryption technologies available. Some of the more commonly utilized encryption methods, however, are known to have weaknesses that a dedicated adversary can compromise. Less secure because hacker's laptop can act as Access Point. If you connected to their laptop, they'll read all your information (username, password.etc..).

- **Complexity :**

  The communication systems in wireless networks is more complex than the wire communications , More complex to configure than wired network.

- **Reliability:**

  Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects that are beyond the control of the network administrator. Affected by surrounding. e.g: obstacles ,multi path fading, interference , attenuation , and can be affected by noise and distortion more than the wired . Limitation of the radio spectrum available make the wireless systems are constrained to operate in a fixed BW to support an increasing number of users over time .

CHAPTER 3

Mobile Networking Technology

Mobile Networking Technology

3.1- Evolution of mobile networks:

Due to the services provided by the mobile networks and the demand of improving those services , mobile networks are evolved rapidly in networks design , techniques , number of users , speed of data ,types of services and many others , figure 3.1 shows the evolution along years .

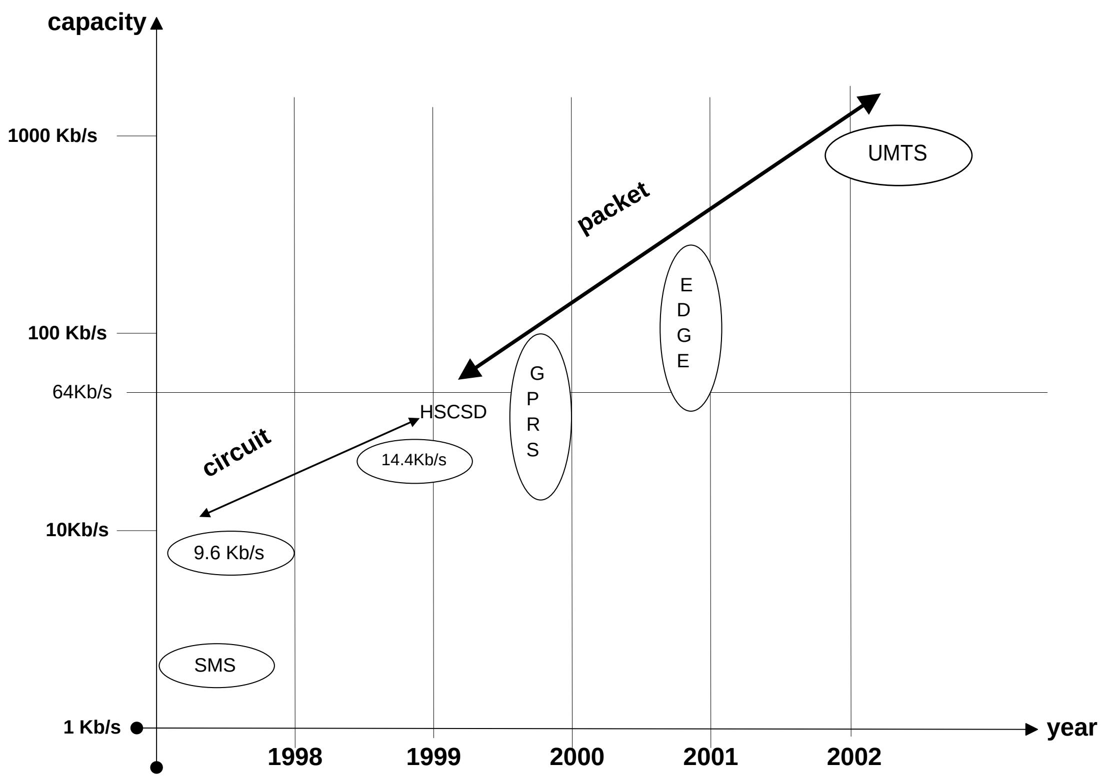


Figure 3.1- Evolution of mobile networks

The evolutions in brief from first generation of mobile networks to the next generations as :

- **First generation (1G) :**

It is the first generation cellular network that existed in 1980s . it transfers only voice in analog , it has limitations because there are no encryption , the sound quality is poor .

- **Second Generation (2G) :**

  It is the first digital cellular systems launched early 1990s . Low bit rate data services were supported as well as the traditional speech service, the speed of transfer is at 9.6 Kbps , the traffic is digitally encrypted .Compared to first-generation systems, second-generation (2G) systems use digital multiple access technology, such as TDMA and CDMA , higher spectrum efficiency, better data services, and more advanced roaming is offered.

- **2.5Generation :**

  It is launched in 1997 , General Packet Radio Service (GPRS) technique which provides IP-based packet data transmission up to 114 kbps and uses 8 time slots ,provides “always on” Internet access and the Multimedia Messaging Service (MMS) whereby users can send rich text, audio, video messages to each other .

- **2.75 Generation :**

  GPRS networks evolved to EDGE (Enhanced Data – rates for GSM Evolution) networks with the introduction of 8PSK encoding , used in 2003 , the transfer speed increased up to 384 Kbps .

- **Third Generation (3G) :**

  It is the third generation of mobile telecommunication , it allows simultaneous use of speech and data services and offers data rates up to 2 Mbps which provide services like video calls , mobile TV , mobile internet and downloading .

3.2-Global System for Mobile Communication (GSM)

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz . many countries outside of Europe joined the GSM partnership.

3.2.1- Important events of GSM :

Many of important events have been done for the GSM system as shown in table (3.1) .

Table (3.1) : events of GSM system [**27**]

Years	Events
1982	CEPT establishes a GSM group in order to develop the standards for a pan-European cellular mobile system.
1985	A list of recommendations to be generated by the group is accepted.
1986	Field tests are performed to test the different radio techniques proposed for the air interface.
1987	Time Division Multiple Access (TDMA) is chosen as the access method (with Frequency Division Multiple Access [FDMA]). The initial Memorandum of Understanding (MoU) is signed by telecommunication operators representing 12 countries.
1988	GSM system is validated.
1989	The responsibility of the GSM specifications is passed to the European Telecommunications Standards Institute (ETSI).
1990	Phase 1 of the GSM specifications is delivered.
1991	Commercial launch of the GSM service occurs. The DCS1800 specifications are finalized.
1992	The addition of the countries that signed the GSM Memorandum of Understanding takes place. Coverage spreads to larger cities and airports.
1993	Coverage of main roads' GSM services starts outside Europe.
1994	Data transmission capabilities launched. The number of networks rises to 69 in 43 countries by the end of 1994.
1995	Phase 2 of the GSM specifications occurs. Coverage is extended to rural areas.
1996	June: 133 network in 81 countries operational.

3.2.2-Multiple access and channel structure in GSM :

GSM uses a combination of both FDMA and TDMA techniques. In FDMA technique , two frequency bands (FDD) are used , one for uplink (from MS to BS) and the other for downlink (from BS to MS). The upper frequency band is used for downlink that is to overcome the attenuation by increasing the transmitted power by the Base Station . There is a frequency band (BW duplex) separates the upper link from the downlink . The FDMA involves the division by frequency of the system bandwidth into 125subbands (carriers), each with a bandwidth of 200 kHz . the last subband is used as a Guard band (Bg) to avoid interference with the neighbor system frequencies , so the number of channels N can be found according to the following equation :

$$N = \frac{Bsys - Bg}{Bc} \quad \text{..................................} \quad (3.1) \quad [26]$$

Where : N= Number of channels .

$Bsys$= the system bandwidth .

Bg= the guard band .

Bc= channel bandwidth (in GSM 200 KHz) .

Different systems of GSM and UMTS , their frequency bands and bandwidths are shown in table (3.2) .

Table (3.2) GSM/UMTS frequencies and bandwidths [26]

System	System BW		BW duplex	Channel BW
P-GSM 900	25MHz	890-915 MHz : Uplink 935-960 MHz : Downlink	45 MHz	200KHz
GSM- 1800	75MHz	1710-1785 MHz : Uplink 1805-1880 MHz : Downlink	95 MHz	200KHz
GSM- 1900	60MHZ	1850-1910 MHz : Uplink 1930-1990 MHz : Downlink	80 MHz	200KHz
UMTS	60MHz	1920-1980 MHz : Uplink 2110-2170 MHz : Downlink	190 MHz	5MHz

The carriers are then divided in time, using a TDMA scheme. The fundamental unit of time is called a 'burst period' or Time slot , and it lasts for approximately 0.577ms . Eight of these burst periods are grouped into what is known as a TDMA frame. This lasts for approximately (8* 0.577ms) 4.615 ms, and forms the basic unit for the definition of logical channels. One physical channel is one burst period allocated in each TDMA frame. In simplified terms, the base station transmits two types of channel; traffic and control. Accordingly the channel structure is organized into two different types of frame, one for the traffic on the main traffic carrier frequency and the other for the control on the beacon frequency. The frames are grouped together to form multiframes, and in this way it is possible to establish a time schedule for their operation so the network can be synchronized.

The traffic channel frames are organized into multiframes consisting of twenty-six frames and taking120 ms, and control channel multiframes that comprise fifty-one frames and occupy 235.4 ms. In a traffic multiframe, twenty-four frames are used for traffic. These are numbered 0 to 11 and13 to 24. One of the remaining frames is then used to accommodate the Slow Associated Control Channel (SACCH) , the remaining frame remaining free. The actual position used alternates between positions 12 and 25.

Multiframes are then constructed into superframes taking 6.12 seconds. These consist of fifty-one traffic multiframes or twenty-six control multiframes. Above this 2048 superframes are grouped to form one hyperframe, which repeats every 3 hours, 28 minutes and 53.76 seconds ,GSM frame organization structure is illustrated in Figure 3.2.

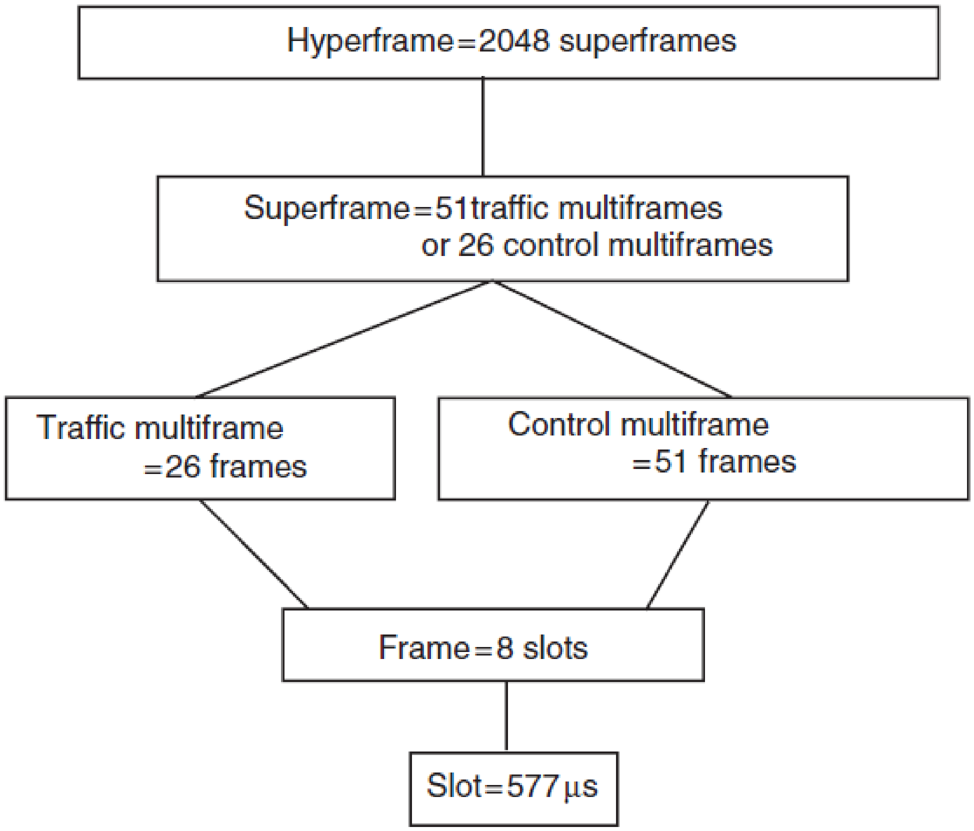


Figure 3.2 GSM frame organization structure.[20]

3.2.3-Channels :

The channels in GSM systems are divided into two types : control channels and traffic channels .

i- Control channels :

There are variety of different control channels that are used to provide the required functionality to enable the mobiles and the BTS to communicate, set up and manage the calls. There are a number of channels, and they can be split into groups, namely broadcast channels for initial synchronization, common control channels for initiating calls, and dedicated control channels to manage calls. They include the following :

1- Broadcast channels:

- Frequency Correction Channel (FCCH) : This is effectively a series of 148 zeros sent as the first logical channel in the control sequence. As the burst is all zeros, this equates in

GMSK to a sine wave at a frequency of approximately 67 kHz. The mobile finds this and adjusts its own frequency to be that of the network.

- Synchronization Channel (SCH) : This is transmitted in time slot zero in the frame following FCCH. It contains extended training sequences to allow the mobile to gain exact synchronization with the network. Also contained within the sequence are the BTS identification and the current frame location in relation to the hyperframe.
- Broadcast Control Channel (BCCH) : This channel is continually broadcast on the downlink, by the BTS. It contains information including base station identity, frequency allocations, and frequency-hopping sequences that are needed by the mobiles to set up and receive calls. One broadcast control channel segment occupies four frames per multiframe.

2- Common control channels:

- Paging Channel (PCH): This channel is used to 'page' or call the mobile to let it know that there is an incoming call. The location registers are able to identify the relevant cell for the mobile, and a request is sent out for a particular mobile (on the paging channel that all mobiles monitor periodically) to inform the mobile that there is an incoming call.
- Random Access Channel (RACH). This performs an equivalent function to that of the paging channel, except that it is used when a mobile initiates a call. Accordingly, it is located within the uplink from the mobile to the BTS. As the name implies, the channel is accessed randomly as required by the mobile. As any mobile communicating with the BTS can access this channel, there is the possibility that two mobiles will interfere with one another. To overcome this problem, the BTS sends an acknowledgement to the mobile once it has correctly accepted the access. If this does not occur, the mobile waits a random amount of time before re-accessing via the RACH. On acceptance of the access the BTS directs the mobile to the Slow Dedicated Control Channel SDCCH, a two-way channel where the call can be set up.
- Access Grant Channel (AGCH) : This channel is used to set up a call once a mobile has been paged on the paging channel or random access channel. It directs the mobile to another control channel, typically the Slow Dedicated Control Channel (SDCCH), where the call set up is progressed.

3- Dedicated control channels:

- Standalone Dedicated Control Channel (SDCCH) : This channel is used for messaging along with the companion SACCH in order to relay signalling information. The channel takes four bursts in each multiframe for each mobile that is active on the BTS, which is just sufficient to enable timely transmission of the relevant data.
- Slow Associated Control Channel (SACCH). This channel is used to relay a variety of information. On the downlink from the BTS to the mobile, this includes broadcast messages which give the beacon frequencies of neighbouring cells, power control information, and timing advance. For the uplink it includes the measurement report, which gives the strength measurements from signals received from neighbouring cell beacon transmissions, acknowledgement for the power control and acknowledgement for the timing advance.
- Fast Associated Control Channel (FACCH). This channel is used to send urgent messages that are normally unscheduled. As the SACCH may take seconds to transfer, this may not be swift enough for many functions. In order to achieve much faster data transfer, the messages are sent in place of speech data for short periods of time. Additionally, it comes free when a TCH is activated, so part way through a call set-up signalling will move to FACCH, not because it needs to be fast or is unscheduled, but because it is an available and efficient resource. It is referred to as 'fast' because it can carry up to fifty messages per second against four per second for SDCCH. It is often possible to take up to about one in six of the traffic or speech frames without loss of quality, although there is some degradation. When a frame of speech data is lost as a result of the presence of an FACCH frame being sent, the same action is taken as when data is lost due to poor signal or channel conditions. Here, the receiving end replaces the lost speech data with a repeat of the previous sound. In this way the listener hears a persistence of the sound rather than a silence or click, and in this way the missing data are masked sufficiently. As the number of frames that are used by the FACCH increases, the degradation of the speech deteriorates. This happens in a non-linear fashion as the number of frames increases.

  It is necessary that the receiver knows whether a frame is traffic (i.e. speech or FACCH) so that the data can be used correctly. To achieve this, the data are marked in each burst using two flag bits. These are set to 0 for user or speech data and to 1 for FACCH data. Two data bits are required because it is possible that the FACCH and speech data may be interleaved where the data is spread between adjacent bursts, and only half the data may be speech and half FACCH.

ii- Traffic channels :

As the name implies, the Traffic Channel (TCH) is used to carry the voice information for the call. There are three basic types of traffic channel: full-rate, half-rate and eighth-rate. A full-rate traffic channel (TCH/F) occupies a complete slot per frame, whereas a half-rate traffic channel (TCH/H)occupies only every other burst of a time slot. The eighth-rate traffic is used only on the SDCCH for the exchange of call set-up or the short message service (SMS). There are eight different time slots that are allocated, a mobile on the network normally transmitting during one of them. Similarly, the BTS transmits to a particular mobile during one burst. In some special instances, such as sending high data rates, it is possible for a mobile to be allocated more than one burst period. Also, when transmitting speech using a half-rate vocoder the mobile may use only one in sixteen burst periods. The burst periods are allocated numbers 0 to 7. The system is also organized so that equivalent bursts in the uplink and downlink do not occur at the same time as shown in Figure 3.3. In this way the mobile does not transmit and receive simultaneously, thereby simplifying the radio transmitter receiver circuitry considerably. Therefore, when the BTS is transmitting slot 0 it is receiving slot 5 – i.e. the mobile allocated to slot 5 is transmitting.

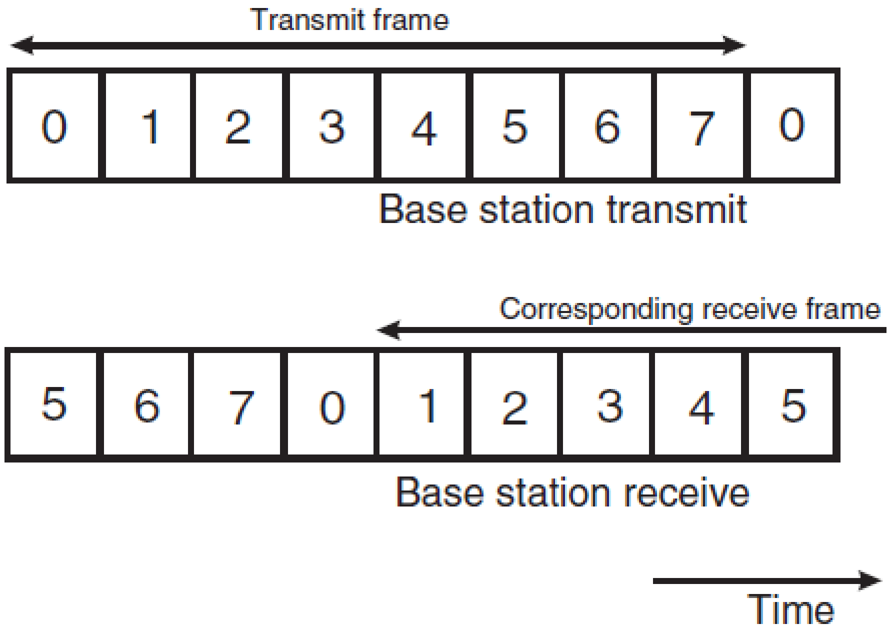


Figure 3.3 Time offsets on corresponding frames for uplink and downlink.[20]

The channel is made up of a variety of different types of data, which are grouped together logically into 'bit fields'. These bit fields include the initial tail bits, training sequences, flag bit final bits and the data payload, and there is also a guard time between bursts to or from different mobiles. The first 3 bits within any burst are set aside to enable the transmitter power to increase to the required level. This is required because it is not possible for the transmitter to turn on instantly. Also, if it were to come on prematurely to be ready for its burst, then it would interfere with the end of the transmission from the previous mobile.

Following the initial tail bits, a flag is sent followed by a section of data consisting of 57 bits, and it is normally digitized voice. On some occasions this may be replaced by signalling, where a channel called the FACCH is incorporated. The type of data, whether digitized voice or FACCH, is indicated by the flag. In the centre of the burst there is a group of data 26 bits long, called the training sequence ormidamble. This is used as a timing reference and as an adaptive equalizer training pattern. There are eight patterns (chosen to be as orthogonal as possible) used within GSM, each 26 bits long, and the same one is used in all eight time slots. Different patterns are used in cells to ensure that only the signal from the required BTS is recognized. With the movement of mobiles, signals vary considerably, and it is possible that the signal from a nearby cell may be received suddenly. The use of the training patterns enables the mobile to detect this.

The data, usually from the voice encoding, need to be split to fit the data structure. The speech is broken into blocks of 20 ms, and this is processed by the speech coder to give 260 bits to represent the speech. These are ordered and divided into two groups. For full-rate speech, one group of182 bits is passed through error correction and results in a string of 382 bits. The less critical group of 78 bits is just summed with the error-corrected data to yield 482 bits. These are diagonally interleaved to form 57 bits per time slot, the exact size of the data length in the data slots, two per burst. As a result, the 20-ms sample of speech is sent over eight timeslots over the air. A further flag and section of 57 bits of data follow. Finally there are three final tail bits where the transmitter ramps down its power, and this is followed by a guard period to separate this burst from the next. The guard period is equivalent to 8.25 bits. Figure 3.4 shows the Bursts of the GSM TDMA procedure.[20][23]

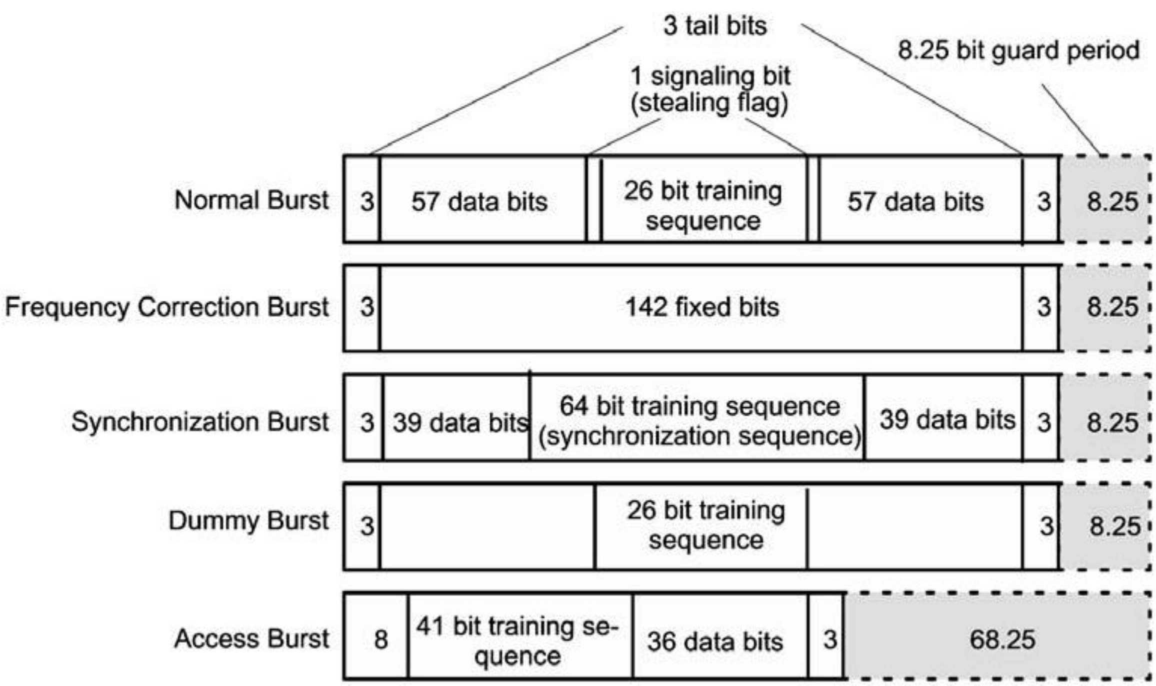


Figure 3.4 Bursts of the GSM TDMA procedure.[23]

3.2.4- GSM Network Structure :

A GSM network consists of several functional entities whose functions and interfaces are defined. The GSM network can be divided into the following broad parts :

- The Network Switching Subsystem (NSS)
- The Base Station Subsystem (BSS)
- The Operation Support Subsystem(OSS)
- The Mobile Station(MS)

The simple architecture diagram of GSM Network is shown in figure 3.5 .

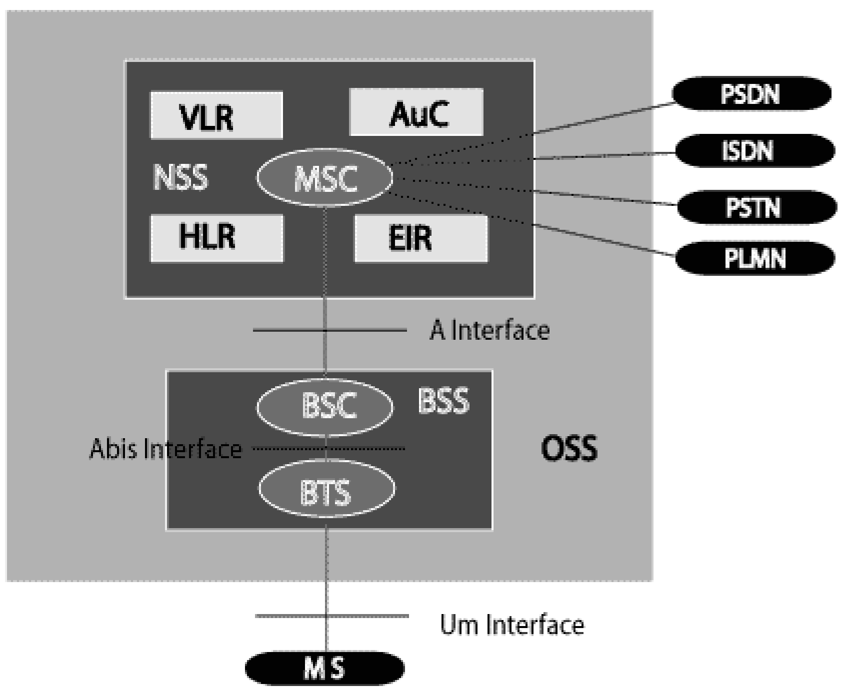


Figure 3.5- architecture diagram of GSM Network . .[27]

The added components of the GSM architecture include the functions of the databases and messaging systems:

- Home Location Register (HLR)
- Visitor Location Register (VLR)

- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- SMS Serving Center (SMS SC)
- Gateway MSC (GMSC)
- Chargeback Center (CBC)
- Transcoder and Adaptation Unit (TRAU)

The diagram of GSM Network along with added elements is shown in figure 3.6 .

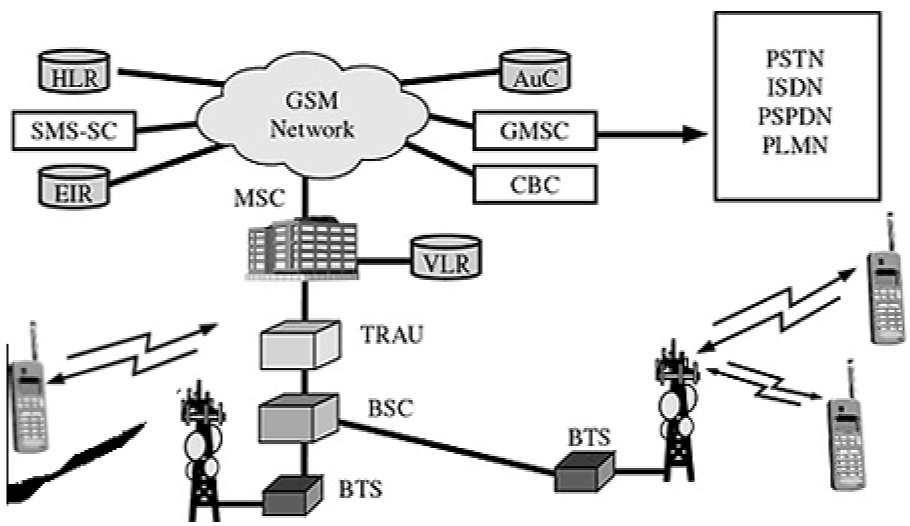


Figure 3.6- GSM Network along with added elements.[27]

i- Network Switching Subsystem (NSS) :

The Network Switching Subsystem (NSS) is responsible for performing call processing and subscriber-related functions. The Network Switching Subsystem includes the following functional units:

- **Mobile services Switching Center (MSC) :**

The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others . The Mobile services Switching Center (MSC) communicates with the BSS across the A interface.

- **Home Location Register (HLR) :**

  The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription from one of the PCS operators, it is registered in the HLR of that operator.

- **Visitor Location Register (VLR) :**

  The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

- **Authentication Center (AUC) :**

  A unit called the AUC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The AUC protects network operators from different types of fraud found in today's cellular world.

- **Equipment Identity Register (EIR) :**

  The EIR is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized, or defective mobile stations. The AUC and EIR are implemented as stand-alone nodes or as a combined AUC/EIR node.

ii- Base Station Subsystem (BSS) :

All radio-related functions are performed in the BSS, which consists of base station controllers (BSCs) and the base transceiver stations (BTSs).

- **Base Station Controller (BSC) :**

  The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC.

- **Base Transceiver station (BTS) :**

  The BTS handles the radio interface to the mobile station. The BTS and the MS communicate across the Um interface, also known as the air interface or radio link . The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTSs are controlled by a BSC.

iii- Operation and Support System (OSS):

The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS). The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations.

iv- Mobile Station (MS)

A Mobile Station consists of two main elements such as :

• The mobile equipment or terminal.

• The Subscriber Identity Module (SIM).

These main two types will be described briefly in the following points **:**

- **Terminal:**

The development of the mobile telephone has been characterized by two dominant trends: size reduction and increased intelligence. Both trends have the same origins, namely the endeavor to make components ever smaller and more advanced and the constant development and refinement of the design. Also, the mobile telephone has already passed three initial phases: the car-mounted model, the portable model and the current pocket model. In digital networks, the mobile assists in the handover process by continuously measuring base station signal strength and then reporting the measured values to the network. A mobile telephone has a number of facilities. The most common are:

- Alphanumeric display
- Memory for many abbreviated numbers
- Signal strength indicator
- Battery indicator
- Electronic lock

There are different types of terminals distinguished principally by their power and application:

- The fixed terminals are the ones installed in cars. Their maximum allowed output power is 20 W.
- The (GSM) portable terminals can also be installed in vehicles. Their maximum allowed output power is 8W.
- The handhelds terminals have experienced the biggest success thanks to their weight and volume, which are continuously decreasing. These terminals can emit up to 2 W. The evolution of technologies allows decreasing the maximum allowed power to 0.8 W

- **SIM card :**

  The SIM shown in figure 3.7 is a smart card that identifies the terminal. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. Without the SIM card, the terminal is not operational. By inserting the SIM card into another GSM cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services.

The SIM card is protected by a four-digit Personal Identification Number (PIN). In order to identify the subscriber to the system, the SIM card contains some parameters of the user such as its International Mobile Subscriber Identity (IMSI), identifying the subscriber, a secret key for authentication, and other user information. Another advantage of the SIM card is the mobility of the users. In fact, the only element that personalizes a terminal is the SIM card. Therefore, the user can have access to its subscribed services in any terminal using its SIM card.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The IMEI and the IMSI are independent, thereby providing personal mobility.

Figure 3.7- SIM card

v- Additional Functional Elements:

- **Message Center (MXE) :**The MXE is a node that provides integrated voice, fax, and data messaging. Specifically, the MXE handles short message service, cell broadcast, voice mail, fax mail, email, and notification.

- **Mobile Service Node (MSN) :**The MSN is the node that handles the mobile intelligent network (IN) services.
- **Gateway Mobile Services Switching Center (GMSC):**A gateway is a node used to interconnect two networks. The gateway is often implemented in an MSC. The MSC is then referred to as the GMSC.
- **GSM Inter Working Unit (GIWU) :**
  The GIWU consists of both hardware and software that provides an interface to various networks for data communications. Through the GIWU, users can alternate between speech and data during the same call. The GIWU hardware equipment is physically located at the MSC/VLR.

3.2.5- GSM Network Areas

The GSM network is made up of geographic areas as shown in figure 3.8 . these areas include cells, location areas (LAs), MSC/VLR service areas, and public land mobile network (PLMN) areas.

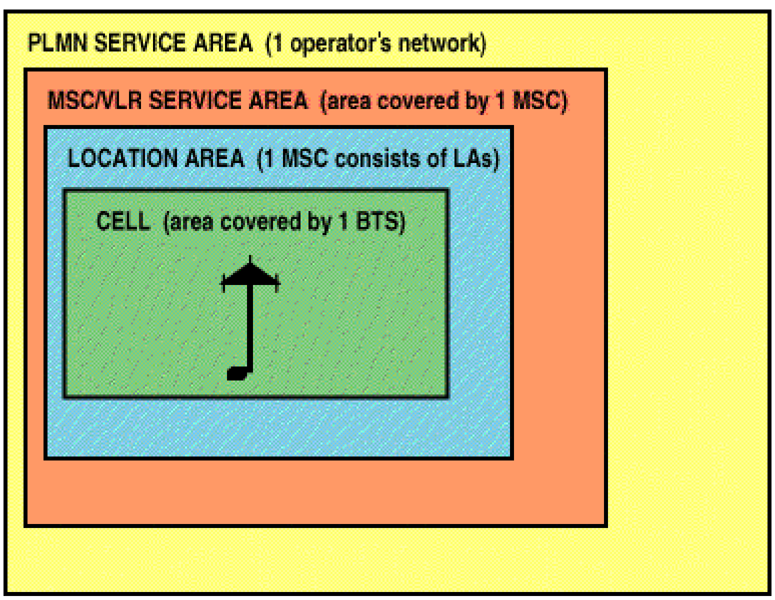


Figure 3.8- Network Areas.[28]

- **Cell:** Cell is the basic service area given radio coverage by one base transceiver station. one BTS covers one cell. The GSM network identifies each cell via the cell global identity (CGI) number assigned to each cell. that uniquely identifies the cell.
- **Location Area :** A group of cells form a Location Area as in figure 3.9. This is the area that is paged when a subscriber gets an incoming call. Each Location Area is assigned a Location Area Identity (LAI). Each Location Area is served by one or more BSCs.

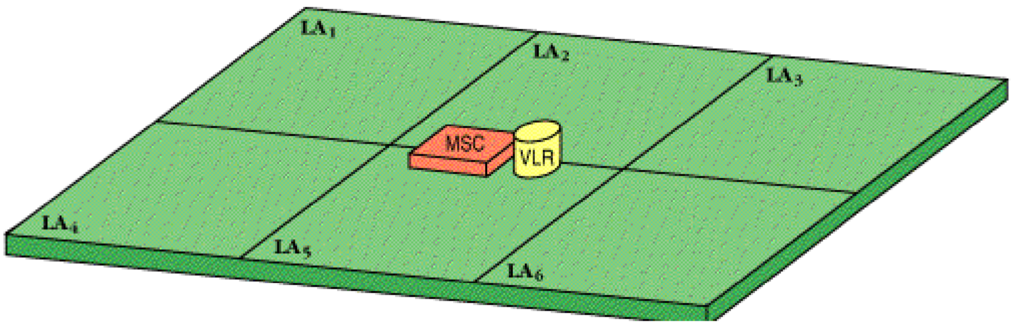


Figure 3.9- Location Areas.[28]

- **MSC/VLR Service Area :**Figure 3.10 shows MSC/VLR service area which represents the part of the GSM network that is covered by one MSC and which is reachable, as it is registered in the VLR of the MSC .

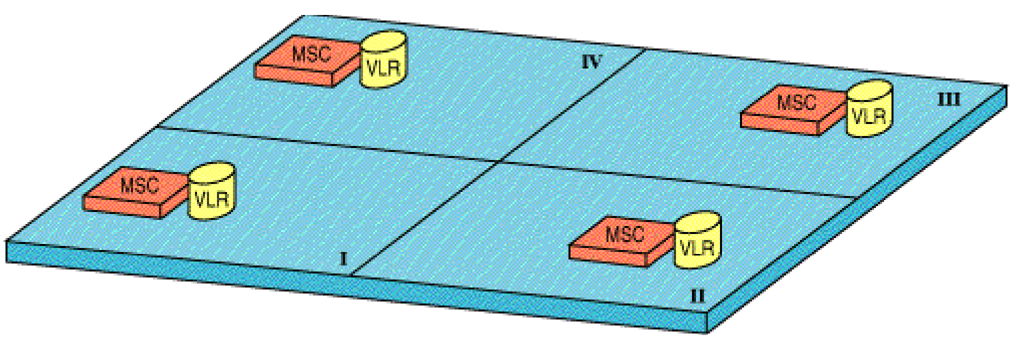


Figure 3.10- MSC/VLR Service Areas.[28]

- **PLMN :**The PLMN service area , shown in figure 3.11 , is an area served by one network operator . A PLMN can contain one or more MSCs. **.[27]**

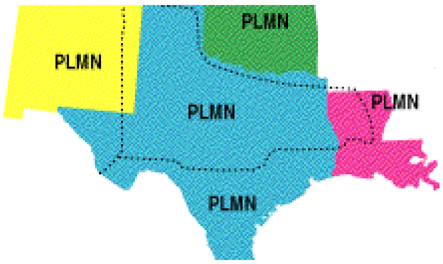


Figure 3.11- PLMN Network Areas.[28]

3.3- Universal Mobile Telecommunication System(UMTS) :

The Universal Mobile Telecommunication System (UMTS) is a third generation (3G) mobile communications system that provides a range of broadband services to the world of wireless and mobile communications. The UMTS delivers low-cost, mobile communications at data rates of up to 2 Mbps. It preserves the global roaming capability of second generation GSM/GPRS networks and provides new enhanced capabilities. The UMTS is designed to deliver pictures, graphics, video communications, and other multimedia information, as well as voice and data, to mobile wireless subscribers.

The UMTS takes a phased approach toward an all-IP network by extending second generation (2G)GSM/GPRS networks and using Wide-band Code Division Multiple Access (CDMA) technology.

3.3.1-UMTS access technology :

IMT-2000 ,the "umbrella specification" of all 3G systems, was accepted by the International Telecommunication Union(ITU) In its November 1999 meeting in Helsinki as IMT-2000 compatible :

- IMT Direct Spread (IMT-DS; also known as UTRA FDD).
- IMT Multicarrier (IMT-MC; also known as CDMA2000) .
- IMT Time Code (IMT-TC; also known as UTRA-TDD/TD-SCDMA "narrowband TDD");
- IMT Single Carrier (IMT-SC; also known as UWC-136) .
- IMT Frequency Time (IMT-FT; also known as DECT).

The IMT-2000 is not actually a single radio interface specification but a family of specifications that technically do not have much in common. IMT-DS and IMT-TC proposals are both being developed by 3GPP consortium. IMT-MC is adopted by another industry consortium, 3GPP2. The most important IMT-2000 system is IMT-DS, followed by IMT-MC.

The IMT-DS access technology used in UMTS is a Wideband – CDMA which is based on the Direct Sequence (DS) Spread Spectrum principle . Direct Sequence makes reference to the usage of a special code to separate the signals . Spread Spectrum means that because of the special signal processing method of CDMA , the original information signal is spread in the frequency domain within the wider frequency range of the W-CDMA channel .In W-CDMA systems , users belonging to a cell are separated by codes .Another characteristic of W-CDMA is that the users share the complete frequency spectrum of 5 MHz per UMTS channel all the time during their communication .In general , in CDMA systems , the way the uplink and downlink connections are separated is referred either by FDD or TDD modes .

For the UMTS public mode (W_CDMA) , the choice has been the FDD mode ,which uses different frequencies for both uplink and downlink (the mobile transmits in one frequency and receives in another) . FDD is used for large outdoor cells because it can support more users than TDD mode . TDD uses the same frequency but different time slot for each type o connection (UL , DL) and W-CDMA in TDD mode is intended to provide private indoor low –range communications .

In practice , an operator needs 2 to 3 channels (2x5x2 or 2x5x3 MHz) to be able to build a high speed , high capacity network , probably using a layering approach , such as the so called Hierarchical cell structure (HCS) scenarios , using different carriers or micro-cells and macro-cells . About the code usage , CDMA requires two kinds of codes of its operation :channelization (spreading) code and scrambling code . The usage of these codes depends on the direction of the communication (uplink or downlink). The purpose of the channelization (spreading) codes in both UL and DL directions is to separate channels from a single transmitter , whereas the purpose of the scrambling codes is to separate transmitters (also applied to both UL and DL directions)

The main difference in the frequency domain between both kinds of codes is that the scrambling codes do not modify the bandwidth of the information signal , whereas the channelization codes do .

- **Channelization (Spreading) codes**

In UL direction (UE transmits and Node B receives) , channelization codes are used to separate physical data and control channels from the same terminal . In DL (Node B transmits and UE receives) , channelization codes are used to separate connections to different users within one cell . once a channelization code is applied to the information signal , the bandwidth of the information signal changes (in frequency domain) to a higher bandwidth , in other words spread over the UMTS bandwidth channel "spread spectrum" .

In time domain , the effect is the change of rate of the information signal . To distinguish from the information rate , 3GPP calls the rate of the channelization code as the chip rate , although physically the chips are also bits (although of higher frequency than the data or information bits). Therefore , after the channelization code is applied to the information signal , the result is a signal with a bit rate equal to the chip rate (the reference chip rate in UMTS is fixed to 3.84 Mc/s , and varying the number of chips per information bit, different user speeds can be obtained). Figure 3.12 clarifies the effects of the channelization code in both frequency and time domain .

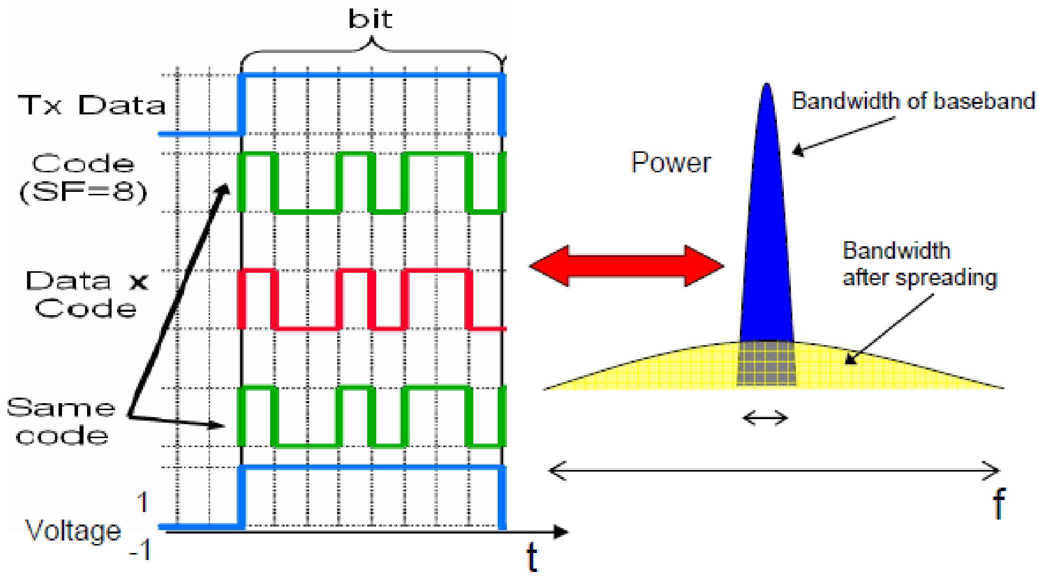


Figure 3.12 effects of the channelization code in frequency and time domain.[30]

The codes used for the channelization operations must have a special property called orthogonality . Orthogonal code means that the inner product of the code with the codes from the other user (called cross- correlation property) or the product of the code with a shifted version of the code itself (called auto-correlation) has to be as small as possible .These codes are also known as OVSF (Orthogonal Variable Spreading Factor) codes .

For orthogonality to work , the signals must be properly synchronized in time . This is had into account in CDMA capacity equations with the so-called orthogonality factor , which is a factor that varies between 0(full orthogonality, no interference) and 1 (no orthogonality , full interference).

The number of chips used for each data bit known as the **spreading factor(SF) .** Also ,in the frequency domain , SF=W/R , where W=Bandwidth of the spread signal Hz and R= Bandwidth of baseband data Hz .

In time domain:

SF = Chip Rate / Data Rate coded channel

In frequency domain :

SF=W / R

Where Data Rate coded channel means that this data rate has into account the overhead introduced by coding techniques and it doesn't corresponds directly to the information rate (unless the coding factor is 1).

- **Scrambling codes**

Scrambling codes separate different mobiles (in uplink) and different Node-B cells/sectors (in downlink). This is a code that does not affect the transmission bandwidth which was already transformed by the usage of the channelization code. The codes used for scrambling codes are known as Gold codes and there are two versions (long and short) depending on the features of the terminal/Node B either one or another version is used.

In Uplink, the number of codes available is in the order of millions of codes (that guarantees no code shortage when trying to separate the transmitting users), but in Downlink this number is limited to 512; otherwise the cell-search procedure shouldn’t be possible to solve in a reasonable time.

Finally, in the reception side the same transmitter’s channelization code is applied and that allows the receiver to reconstruct the original transmitted signal. W-CDMA also involves a certain degree of security, in the sense that without the transmitter’s channelization code available, it is almost impossible to reconstruct the original signal, thus preventing tampering attacks in the air interface.

The following schematic (figure 3.13) illustrates in a simple way the process of transmission and reception in UMTS involving all the elements mentioned.

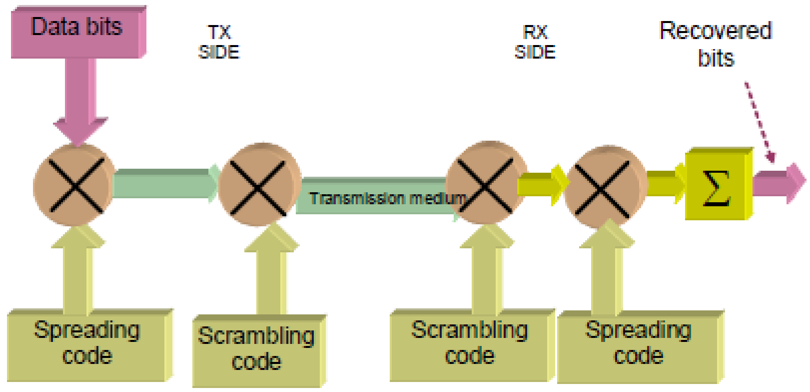


Figure 3.13 - Simplified Transmission and Reception process in UMTS.[30]

3.3.2- Channels:

There are three separate channel concepts in the UTRAN: logical, transport, and physical channels , Figure 3.14 shows these concepts .

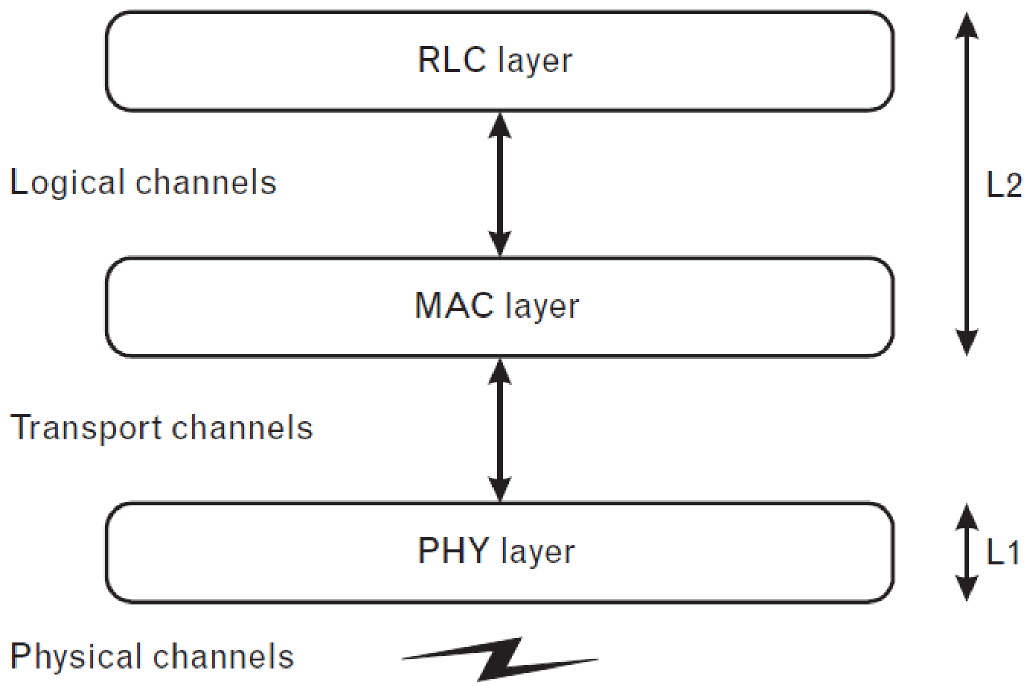


Figure 3.14 Channel concepts.[24]

Logical channels define what type of data is transferred. These channels define the data-transfer services offered by the MAC layer; that is, the concept of logical channels is used in the interface above the MAC.

Transport channels define how and with which type of characteristics the data is transferred by the physical layer. These channels are used in the interface between the MAC and the PHY layers. The transport channel is a new concept if WCDMA is compared to the GSM system.

Physical channels define the exact physical characteristics of the radio channels. These are the channels used below the PHY layer; that is, in the radio interface.

i- Logical Channels

Logical channels are not actually a layer 1 concept, but logically, they exist in the interface between the MAC and the RLC protocol layers; that is, clearly within layer 2.

Logical channels can be divided into control channels and traffic channels.

A control channel can be either common or dedicated. A common channel is a point-to-multipoint channel; that is, common to all users in a cell, and a dedicated channel is a point-to-point channel; that is, used by only one user. Control channels transfer Control plane (C-plane) information and traffic channels User plane (U-plane) information.

1- The logical control channels are:

- Broadcast control channel (BCCH) : Downlink common channel; Broadcasts system and cell-specific information.
- Paging control channel (PCCH) : Downlink channel; Transfers paging information and some other notifications.
- Dedicated control channel (DCCH) : Bidirectional point-to-point channel; Transfers dedicated control information.
- Common control channel (CCCH) : Bidirectional point-to-multipoint channel; Transfers control information.
- Shared channel control channel (SHCCH) : Bidirectional; Transfers control information for uplink and downlink shared channels; Only in TDD mode.

2- The logical traffic channels are:

• Dedicated traffic channel (DTCH) : Bidirectional point-to-point channel; Transfers user information .

• Common traffic channel (CTCH) : Downlink point-to-multipoint channel; Transfers dedicated user information for a group of users.

ii- Transport Channels

The transport channels define how and with which type of characteristics the data is transferred by the physical layer. Transport channels are divided into common channels and dedicated channels. They are all unidirectional.

1- Common transport channels include:

• Broadcast channel (BCH) : A downlink channel for broadcast of system and cell-specific information.

•Paging channel (PCH) : A downlink channel used for transmission of paging and notification messages; Transmission associated with transmission of paging indication PICH physical channel.

• Random access channel (RACH) : A contention-based uplink channel , Used for initial access or non-real-time dedicated control or traffic data; A limited-size data field.

• Common packet channel (CPCH) : A contention-based channel used for transmission of bursty data traffic; An uplink channel; Only in FDD mode.

• Forward access channel (FACH) : A common downlink channel; May carry small amounts of user data.

• Downlink shared channel (DSCH) : A downlink channel shared by several UEs; Used for dedicated control or traffic data; Associated with a DCH (does not exist alone).

• High-speed downlink shared channel (HS-DSCH) : A downlink channel shared by several UEs; Optimized for very high speed data transfer; Employs efficient link adaptation scheme; Very quick rate changes (HSDPA frame is only 2 ms versus 10ms of other channels); Associated with a DCH, and up to 4 HS-SCCHs (does not exist alone); Available only from Release 5 onward.

• Uplink shared channel (USCH) : An uplink channel shared by several UEs; Carries dedicated control or traffic data; Only in TDD mode.

2- The only dedicated transport channel type is:

• Dedicated channel (DCH) : For one UE only; Either uplink or downlink.

iii- Physical Channels :

There are two ways to use the allotted spectrum in UTRAN. In frequency-division duplex (FDD) mode, both the uplink and downlink bands have their own frequency channels. In time-division duplex (TDD) mode, there is only one frequency channel, which is then dynamically time-divided for both uplink and downlink slots. It seems that the FDD mode will be the more preferred technology choice by the operators, and the TDD mode is the less used choice. TDD is also given smaller frequency allocations. In practice, the FDD mode will be given the symmetric part of the UMTS spectrum allocation, and TDD will get the asymmetric "leftovers."Depending on the operating mode, the physical channels will be somewhat different.

1- FDD Physical Channels : The physical channels in the FDD mode are described below:

- Downlink

• Synchronization channel (SCH) : They are two subchannels, the primary and secondary SCH, transmitted only during the first 256 chips of each time slot .Used for cell search

• Common pilot channel (CPICH) : Uses a fixed rate of 30 Kbps and carries a predefined bit sequence; They are two types: primary and secondary CPICH .

-Primary CPICH (P-CPICH) : is the phase reference for SCH, primary CCPCH, AICH, and PICH, and the default reference for other downlink physical channels;

-Secondary CPICH (S-SPICH): may be the reference for the downlink DPCH, and for the associated PDSCH. The presence of S-CPICH in a cell is optional.

• Primary common control physical channel (P-CCPCH) : Uses a fixed rate of 30 Kbps , Carries BCH ,and not transmitted during the first 256 chips of each time slot.

• Secondary common control physical channel (S-CCPCH) : It uses a variable rate and carries FACH and PCH . FACH and PCH can be mapped to the same or separate channels, Transmitted only when there is data available.

• Physical downlink shared channel (PDSCH) : Carries DSCH (downlink shared channel);Always associated with a downlink DPCH, which carriers its control information.

• Paging indicator channel (PICH) : Carries page indicators to indicate the presence of a page message on the PCH.

- Acquisition indicator channel (AICH) : Carries acquisition indicators (= signatures for the random access procedure).
- CPCH Access preamble acquisition indicator channel (AP-AICH) : Carries AP acquisition indicators of the associated CPCH.
- CPCH status indicator channel (CSICH) : Carries CPCH status information.
- CPCH Collision-detection/channel-assignment indicator channel(CD/CA-ICH):

  Carries CD (collision detection) indicators only if the CA(channel assignment) is not active, or both CD indicators and CA indicators at the same time if the CA is active.

  The three previous channels are control channels for uplink PCPCH. If CPCH functionality is not supported by the network, then these channels do not exist.
- High-speed physical downlink shared channel (HS-PDSCH) :

  Carries HS-DSCH; Can employ either QPSK or 16 QAM modulation; A HS-PDSCH frame is 2 ms, consisting of 3 time slots; Uses always the spreading factor of 16; One UE may receive several HS-PDSCH simultaneously.
- Shared control channel for HS-DSCH (HS-SCCH) :

  Carries downlink signaling related to HS-DSCH transmission; Indicates when there is data to be received on HS-DSCH for this UE; A fixed rate channel (SF = 128, i.e., 60 kbps);There can be up to 4 HS-SCCHs a UE has to monitor.

- **Downlink and Uplink**

  - Dedicated physical data channel (DPDCH) : Carries DCH (dedicated channel);Carries data generated at layer 2 and above.
  - Dedicated physical control channel (DPCCH) : Carries control information generated at layer 1. In the uplink these two channels are I/Q code multiplexed, but in the downlink they are time multiplexed. Sometimes the DPDCH and DPCCH together is an entity known as a dedicated physical channel(DPCH).

- **Uplink**

  - Physical random access channel (PRACH) : Carries RACH; Uses slotted ALOHA technique with fast acquisition indicators.
  - Physical common packet channel (PCPCH) : Carries CPCH (common packet channel);Uses DSMA-CD technique with fast acquisition indication.

- Uplink dedicated control channel for HS-DSCH (HS-DPCCH) : Carries HSDPA feedback information (HARQ acknowledgements and channel quality indications);Multiplexed with a DPCCH .[24]

3.3.3- UMTS Network Structure :

Figure 3.15 depicts the UMTS architecture at the very highest level.

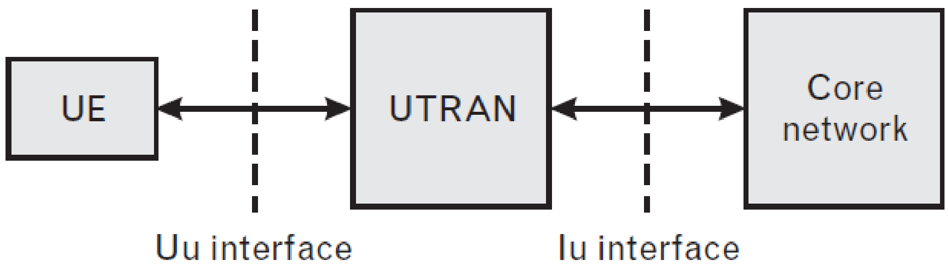


Figure 3.15- High-level UMTS architecture.[24]

The interfaces between the UE and the UTRAN (Uu interface) and between the UTRAN and the CN (Iu interface) are open multivendor interfaces.

Figure 3.16 gives a much more detailed description of the UMTS architecture.

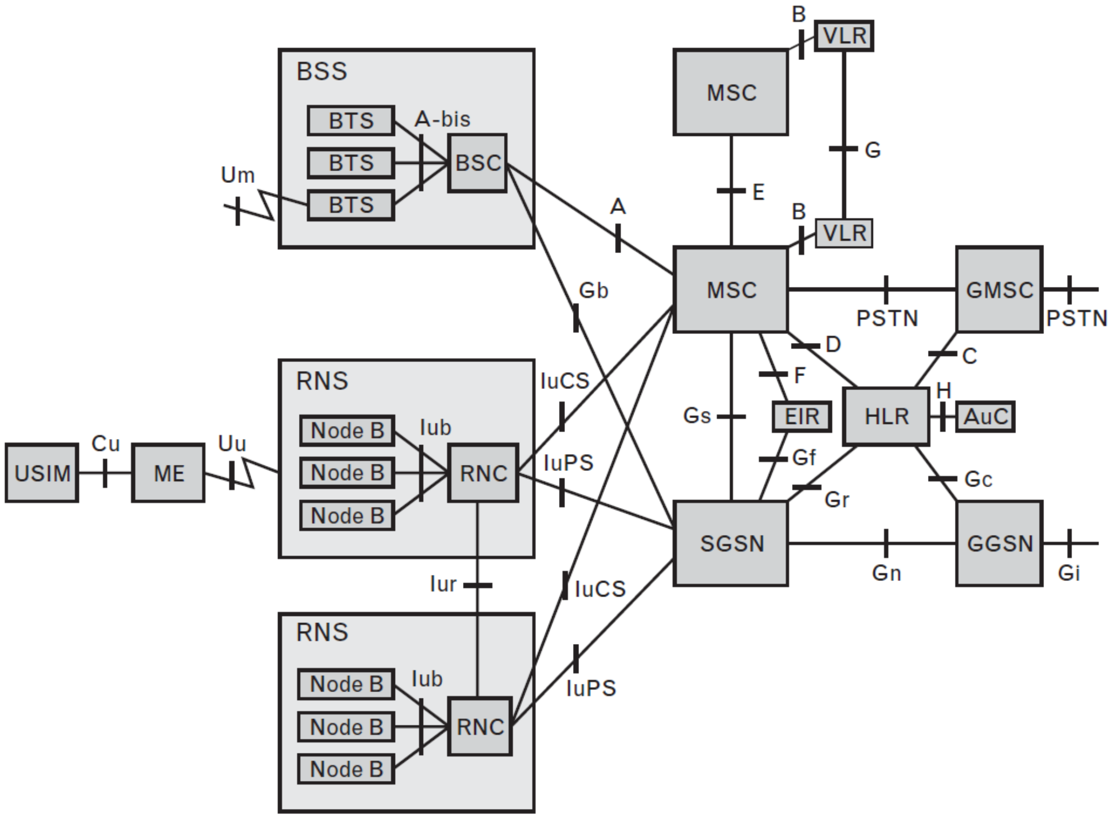


Figure 3.16- UMTS network elements and interfaces .[24]

the core network portion is the same as in the old GSM + GPRS core network combination. The same core network entities may serve both the UTRAN and (GRAN) GSM radio access networks. GSM's radio access network entities (the BSS) are included in the drawing to clarify the relationship of these two technologies. They are likely to linger in the networks to support traditional circuit-switched speech services.

The entities in this figure are briefly described in the following paragraphs. the core network is logically divided into two domains: circuit-switched (CS) and packet switched (PS). The CS-domain handles circuit-switched connections, and the PS-domain handles the packet transfer. CS core network is built around MSCs, and PS core network around SGSNs. Note that the various core network registers are common for both domains, although VLR is typically employed by CS-domain only.[24]

i- Core Network :

The core network consists of the following elements :

- **Mobile Switching Center**

  The mobile switching center (MSC) is the centerpiece of the circuit-switched core network. The same MSC can be used to serve both the GSM-BSS and the UTRAN connections . A GSM-MSC must be upgraded to meet the 3G requirements, but the same MSC can be used to serve both access networks. In addition to the radio access networks, it has interfaces to the fixed PSTN network, other MSCs, the packet-switched network (Serving GPRS Support Node : SGSN), and various core network registers (HLR, EIR, AuC). Physically, the VLR is implemented in connection with the MSC, so the interface between them (the B interface) exists only logically. Several BSSs can be connected to a MSC. The number and the size of MSCs also vary; a small operator may only have one small MSC, but once the number of subscribers increases, several large MSCs may be needed. The functions of an MSC include the following :

• Paging.
• Coordination of call setup from all MSs in the MSC's jurisdiction.
• Dynamic allocation of resources.
• Location registration.
• Interworking functions (IWFs) with other type of networks.
• Handover management (especially the complex inter-MSC handovers).
• Billing of subscribers (not the actual billing, but collecting the data for the billing center).
• Encryption parameter management.
• Signaling exchange between different interfaces.
• Frequency allocation management in the whole MSC area.
• Echo canceller operation and control.

The MSC terminates the MM and CM protocols of the air interface protocol stack, so the MSC has to manage these protocols, or delegate some responsibilities to other core network elements.

- **Visitor Location Register :**

The visitor location register (VLR) contains information about the mobile stations roaming in this MSC area. It is also possible that one VLR handles the visitor register of several MSC areas. Note that a VLR contains information from all active subscribers in its area, even from those to whom this network is their home network, so the name VLR is misleading as most entries in that register are not visitors, but users in their own home network. The VLR contains pretty much the same information as the home location register (HLR), the difference being that the information in the VLR is there temporarily, whereas the HLR is a site for permanent information storage. When a user makes a subscription, the subscriber's data is added to his home Location Register HLR. From there it is copied to the VLR the user is currently registered with. When a user registers with another network, the subscriber data is removed from the old VLR and copied to the new VLR. The VLR contains such data that the normal call setup procedures can be handled without consulting the HLR. This is important especially if the user is roaming abroad, and the signaling connection to the home network is expensive.

A VLR subscriber data entry includes the following information:

- International mobile subscriber identity (IMSI) .
- Mobile station international ISDN number (MSISDN) .
- Mobile station roaming number (MSRN) .
- Temporary mobile station identity (TMSI), if applicable .
- Local mobile station identity (LMSI), if used .
- Location area where the mobile station has been registered .
- Identity of the SGSN where the MS has been registered .
- Last known location and the initial location of the MS.

In addition, there can be lots of optional data, depending on what features the network supports [e.g., CAMEL or local service area (LSA)]. The VLR may also contain supplementary service parameters. The procedures the VLR has to perform include the following:

- Authentication procedures with the HLR and the AuC .
- Cipher key management and retrieval from the home HLR/AuC.

• Allocation of new TMSI numbers .

• Tracking of the state of all MSs in its area .

• Paging procedure support (retrieval of the TMSI and the current location area).

- **Home Location Register :**

  The HLR contains the permanent subscriber data register. Each subscriber information profile is stored in only one HLR. The HLR can be implemented in the same equipment as the MSC/VLR, but the usual arrangement is to have the MSC/VLR as one unit, and the HLR/AuC/EIR combination as another unit. One PLMN can have several HLRs. The subscriber information is entered into the HLR when the user makes a subscription. There are two kinds of information in an HLR register entry, permanent and temporary. The permanent data never change, unless the subscription parameters are changed. An example of this is the user who adds some supplementary services to his/her subscription. The temporary data contain things like the current (VLR) address and ciphering information, which can change quite often, even from call to call. Temporary data are also sometimes conditional; that is, it is not always there. A subscriber data entry can be accessed by either IMSI or MSISDN. The permanent data in the HLR include among others:

• International mobile subscriber number (IMSI), which identifies the subscriber (or actually his or her SIM card) unambiguously .

• MSISDN [the directory number of the MS(e.g.+218–1234–654321)].

• MS category information .

• Possible roaming restrictions .

• Closed user group (CUG) membership data.

• Supplementary services parameters.

• Authentication key.

• Network access mode (NAM), which determines whether the user can access the GPRS networks, non-GPRS networks, or both.

In addition, if GPRS is supported, PDP addresses are included. Again, there may be lots of other entries, depending on what features the network supports. The temporary data include the following:

• Local mobile station identity (LMSI).

• Triplet vector; that is, three authentication and ciphering parameters:

1- random number (RAND) .

2- signed response (SRES) .

3- ciphering key (Kc) .

• Quintuplet vector; that is, five authentication and ciphering parameters:

1- random challenge (RAND) .

2- expected response (XRES) .

3- cipher key (CK) .

4- integrity key (IK) .

5- authentication token (AUTN) .

• MSC number.

• VLR number (the identity of the currently registered VLR).

In addition, if GPRS is supported, SGSN and GGSN numbers (SS7 addresses) are included. the subscriber data registers can contain a lot of information (dozens of different entries). The HLR also forwards the charging information to the billing center.

- **Equipment Identity Register :**

The equipment identity register (EIR) stores the international mobile equipment identities (IMEIs) used in the system. An EIR may contain three separate lists:

1. *White list:* The IMEIs of the equipment known to be in good order;

2. *Black list:* The IMEIs of any equipment reported to be stolen;

3. *Gray list:* The IMEIs of the equipment known to contain problems (such as faulty software) that are not fatal enough to justify barring them.

At a minimum an EIR must contain a white list. It is unfortunate that the black list and the checks against it are not mandatory, as stolen mobile phones can now be used in some networks that have a weaker security policy. And it is even more unfortunate that changing the IMEI code of a handset is not yet illegal in many countries. Typically a

PLMN has only one EIR, which then interconnects to all HLRs in the network. Note that EIR handles IMEI values, not IMSIs or any other identities. The IMEI is (or should be) a unique identity of a mobile handset assigned when it is manufactured.

- **Authentication Center :**

  The authentication center (AuC) is associated with an HLR. The AuC stores the subscriber authentication key, Ki, and the corresponding IMSI. These are permanent data entered at subscription time. The Ki key is used to generate an authentication parameter triplet (Kc, SRES, RAND) during the authentication procedure. Parameter Kc is also used in encryption algorithms. An AuC physically always exists with an HLR. The MAP interface between them (the H interface) has not been standardized.

- **Gateway MSC :**

  The Gateway MSC (GMSC) is an MSC that is located between the PSTN and the other MSCs in the network. Its function is to route the incoming calls to the appropriate MSCs by first interrogating the appropriate HLR. If the operator allows the outside networks to access its HLRs, then a dedicated GMSC is not necessary as the other networks can route the calls to the right MSC by themselves. In practice it is also possible that all MSCs are also GMSCs in a PLMN.

- **Serving GPRS Support Node :**

  The serving GPRS support node (SGSN) is the central element in the packet-switched network. It contains two types of information:

  • Subscription information:
  - IMSI.
  - Temporary identities.
  - PDP addresses.

  • Location information:
  - The cell or the routing area where the MS is registered.
  - VLR number.
  - GGSN address of each GGSN for which an active PDP context exists.

The SGSN connects to the UTRAN via the IuPS interface and to the BSS via the Gb interface. It also has interfaces to many other network elements as seen in Figure 3.16.

- **Gateway GPRS Support Node :**

  The gateway GPRS support node (GGSN) corresponds to the GMSC in the circuit-switched network. Whereas the GMSC only routes the incoming traffic, however, the GGSN must also route the outgoing traffic. It has to maintain the following data:

  • Subscription information:
  - IMSI.
  - PDP addresses.

  • Location information:
  - The SGSN address of the SGSN where the MS is registered. The GGSN receives this information from the HLR and from the SGSN .

ii- UMTS Terrestrial Radio Access Network :

The UTRAN is the new radio access network designed especially for UMTS. Its boundaries are the Iu interface to the core network and the Uu interface (radio interface) to user equipment (UE).The UTRAN is just one realization of the GRAN concept. The other possible implementations in the future may include, for example, the Broadband Radio Access Network (BRAN) and the UMTS Satellite Radio Access Network (USRAN). The UTRAN consists of radio network controllers (RNCs) and Node Bs (base stations). Together, these entities form a radio network subsystem (RNS) as in figure 3.17.

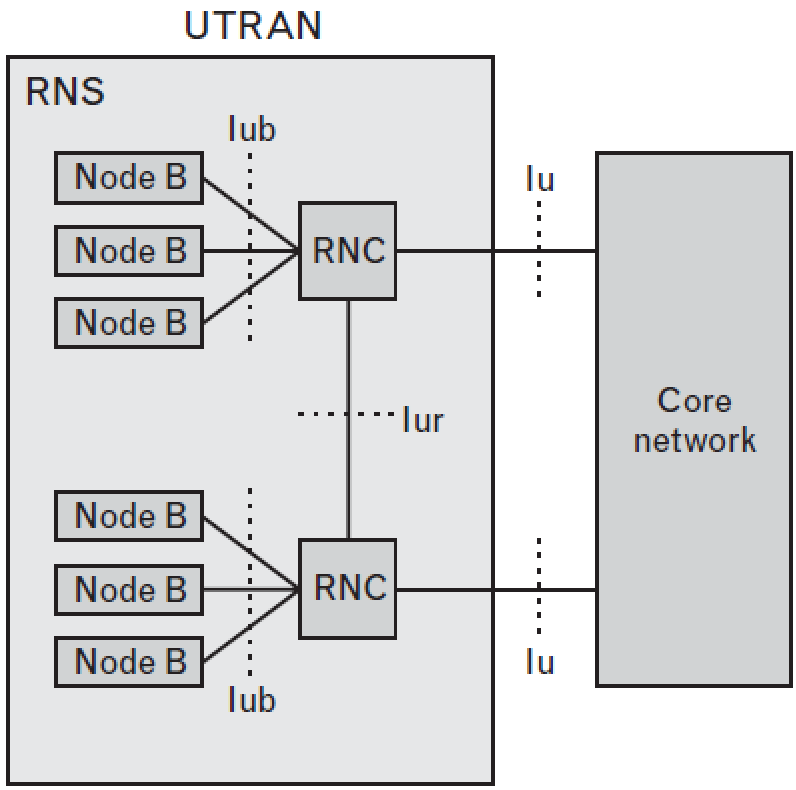


Figure 3.17- UTRAN components and interfaces.[24]

The internal interfaces of the UTRAN include the Iub and Iur. The Iub connects a Node B to the RNC and the Iur is a link between two RNCs.

- **Radio Network Controller :**

The RNC controls one or more Node Bs. It may be connected via the Iu interface to an MSC (IuCS) or to an SGSN (IuPS). The interface between RNCs (Iur) is a logical interface, and a direct physical connection doesn't necessarily exist. An RNC is comparable to a BSC in GSM networks.

Functions that are performed by the RNC include the following:

• Iub transport resources management;

• Control of Node B logical operation and maintenance (O&M) resources;

• System information management and scheduling of system information;

• Traffic management of common channels;

• Macro diversity combining/splitting of data streams transferred over
several Node Bs;
• Modifications to active sets; that is, soft handover;
• Allocation of DL channelization codes;
• Uplink outer loop power control;
• DL power control;
• Admission control;
• Reporting management;
• Traffic management of shared channels.

- **Node B :**

Node B is the UMTS equivalent of a base station transceiver. It may support one or more cells, although in general the specifications only talk about one cell per Node B. The term *Node B* is generally used as a logical concept. When physical entities are referred to, then the term *base station* is often used instead.

Functions that are performed by a Node B include the following:
• Node B logical O&M implementation;
• Mapping of Node B logical resources onto hardware resources;
• Transmitting of system information messages according to scheduling parameters given by the RNC;
• Macro diversity combining/splitting of data streams internal to Node B;
• Uplink inner loop power control (in FDD mode);
•Reporting of uplink interference measurements and DL power information.

In addition, because Node B also contains the air interface physical layer, it has to perform the following functions related to it :
•Macro diversity distribution/combining and soft handover execution;
•Error detection on transport channels and indication to higher layers;
• FEC encoding/decoding of transport channels;
• Multiplexing of transport channels and demultiplexing of CCTrCHs;
• Rate matching;
• Mapping of CCTrCHs on physical channels;

- Power weighting and combining of physical channels;
- Modulation and spreading/demodulation and dispreading of physical channels;
- Frequency and time synchronization;
- Radio measurements and indication to higher layers;
- Inner loop power control;
- RF processing.

Network manufacturers are also offering solutions where the same physical base station equipment will offer both the GSM and the WCDMA transmitter/receiver capability (i.e., they are combined GSM-BTS and WCDMA-Node Bs).[24]

3.3.4- 3G Applications:

Everybody involved in 3G businesses should understand that it is not the technology people are buying and consuming, but the services and content. There has already been one notable failure in 2G, when WAP was marketed as a technology, but nobody told the customers what they could do with WAP. GPRS has also had a slow adoption process because there have not been enough GPRS-specific services on offer. This shows that customers are not eager to adopt new technologies, but they are looking for new services. I-mode is actually based on a relatively slow transmission technology, but provides great services.

- **Voice :**

Voice is and remains the most important type of application in mobile telecommunications. However, it will increasingly be combined with other forms of communication to form multimedia communication. Even the pure voice service can provide new possibilities for applications. It is already possible to set up multipoint conference calls, but this has not been widely exploited. And voice mail will be an attractive alternative for text-based mail systems, such as e-mail or SMS. It is also known that the increased usage of other applications also increases voice usage.

ETSI has also specified the advanced speech call items (ASCI) features for GSM. These features are services that are accessible only to a closed user group. The most important features of ASCI include the following:

• Voice broadcast service (VBS): the capacity for a single mobile to talk to a group of mobiles;

• Voice group call service (VGCS): the capacity for a group of mobiles to talk to each other

• Enhanced multilevel priority and preemption (EMLPP): The fact that urgent calls can preempt less urgent calls.

In 3GPP networks voice will be transferred in IP packets once the network becomes and all-IP network. This scheme is known as Voice over IP(VoIP). Actually VoIP is not an improvement as such for voice transfer. It is a mechanism that forces voice services into a packet-switched network not optimized to handle them; this had to be accomplished so that packet switched IP could be used everywhere.

- **Messaging**

Messaging services is an important application segment. The success of SMS messaging shows that there is a marketplace for services like these. SMS messages are a convenient way to send notes to other people. They do not interrupt the other person's tasks like phone calls do. They are eventually delivered even if the other person is not available because the phone is turned off or the subscriber is outside the network's coverage area. They do not require any interaction by the receiving person. The basic text-based SMS will also be available in 3G, but the faster data rates of the new system make it possible to send much more than plain text in these messages. There is a new concept developed based on the notion of an enhanced SMS concept. This is called the multimedia messaging service(MMS).This concept translates into a non-real-time messaging service that can deliver several multimedia components, such as text, images, voice ,and video. An MMS message can contain more than one component; these components are then combined in the user interface to produce a multimedia presentation. A simple MMS application could be an electronic picture postcard. Other MMS examples include electronic newspapers, news, traffic information, maps and driving instructions, music on demand, advertisements, and on-line shopping. E-mail is probably a very safe bet when predicting 3G applications. E-mail is widely used in the Internet and increasingly in mobile terminals. The GSM specification also includes a provision for SMS cell broadcast (SMS-CB) service. This is a service where SMS messages are broadcast to all mobile stations in an area (one cell or a set of cells). An enhanced version of this service, called the cell broadcast service (CBS) will be used in UMTS networks. CBS can deliver much longer text messages than the GSMSMS-CB service. A CBS message has a maximum size of 1,395 characters.

- **Internet Access**

  Internet access is an almost mandatory application for 3G mobile terminals. Over the last decade the Internet has grown to be a very important communication medium, and it continues to grow rapidly. A communication medium as important as the Internet must be included in a3G application portfolio. Fortunately, this access will be relatively easy to implement in a 3G terminal. The 3GPP is specifying an all-IP network, which means that Internet protocols could be used all the way down to the terminal level. A mobile terminal would be an Internet node, just like any PC, with its own IP address number.

- **Location-Based Applications**

  The UTRAN system will contain several methods to determine the UE's location. This makes it possible to provide a totally new class of applications to mobile phone users: applications that use the knowledge of the mobile user's location. The location data itself can be useful information for the user. The mobile terminal can inform a lost user about his or her location. In practice, the plain coordinates as such do not help much; they must be accompanied by some additional information, like the local map or instructions about how to get to a desired location from the current position. It is easy for the operator to provide the user with a local digital map, even if the user is lost, because his location is known to the operator. The map could even be sponsored by a local business, which could advertise itself in the map.

  If the location of a mobile terminal is known, then it is possible to send it location-specific information, like advertisements, special offers, or traffic information. A mobile user could send a query requesting information about nearby bookshops, and the network could provide this information right away from its yellow pages directory as it knows the location of the requesting terminal. Tracking is already used in the trucking business and with some parcel services. At the moment it is mostly done via satellites, but once UMTS networks gain wider coverage, tracking could be done in some applications also via

UMTS. One new application could be the tracking of stolen cars. If a car includes a 3G chip, it can be tracked by the UMTS network as long as it stays within the coverage area. User's movements can also be tracked, even without his knowledge. If the UE has a GPS positioning capability, the operator could even determine the speed of the user's car. This would be very convenient for law enforcement agencies as there would be no need for special speed radars anymore and they could send an instant speeding ticket via the user's 3G device.

- **Games**

  Games will be another major application segment in 3G. Most people do not admit that they like playing computer games, but despite this, the games are still selling extremely well. In practice, most usage and revenue come from entertainment. Currently, the games some mobile terminals contain are pretty simple. The small displays and limited input devices severely restrict the applications. With bigger displays, more powerful processors, and (possibly) special 3G game terminals, most of these limiting factors will disappear. Compared to desktop PCs, mobile terminals are always lag behind in screen resolution, processor speed, and sound quality. Thus, the wireless industry has to find applications that will exploit the special characteristics of the mobile communication environment. Game applications should be downloadable from the operator or from a gaming content provider. This way the operator can get additional revenue from gaming through commissions, and customers can try new games if they have grown tired of their old games. The games should preferably be built on some common platform, such as WGE or Java, so that they would be easily portable to various mobile terminals. The importance of games in mobile terminals should not be underestimated. A large segment of customers will choose their mobile terminals based on the recreational services they can provide.

- **Advertising**

  Generally, it is not a very good idea to send an advertisement to all subscribers in the network. Most subscribers are probably not at all interested in a certain advertisement and will regard it as junk mail. This will only irritate the customers, and they may change their operator because of this practice. Moreover, sending large amounts of advertisements will use a lot of capacity; thus, it is expensive. The operator should therefore build an accurate user profile database and send the advertisement to only those customers who are most likely to be interested in it. For example, if a customer has bought several books using his mobile device, it is probable that he is interested in receiving information on book sales or new books on the same subject . It must be possible for a user to reject all advertising. On the other hand, the operator can make the reception of advertisements more attractive, for example, by lowering the subscription charges. Note that the operator can put a nice price tag on this kind of targeted advertising. For example, an ink-jet cartridge shop would pay a lot for an advertising campaign that is directed to3G customers that bought an ink-jet printer about six months earlier. [24]

CHAPTER 4

Apparatus and Devices

Apparatus and Devices

4.1- Introduction :

This work which has been done requires some apparatus and devices in order to accomplish this mission , These apparatus that are used in this work such as a wireless smoke sensor , 3G security camera , GSM-SMS communicator which are described below .

4.2- Smoke sensor:

Smoke alarm sensor is a device that used to sense the smoke in the area of interest , It is triggered when detects smoke . everything preventing the smoke from reaching the sensor obstructs an early alarm . The smoke alarm operates according to the scattered light principle . A light source and a photocell are arranged so as to ensure that normally no light strikes the photocell . the light source is activated in short intervals . If the concentration of smoke particles in the enclosure reaches a certain level ,the light is reflected and reaches the photocell ,this will set off operation of the smoke sensor .

photoelectric smoke alarm

- Power supply DC 9 V
- Red LED indicate alarm
- Test button simulates smoke used to check the performance of the smoke sensor .
- High sensitivity
- Built in sounder
- Working on 315 MHz

4.3- 3G security camera:

The 3G security camera work in three different tasks , working as a camera to video or capture an image of the place to be monitored , working as a receiver to the smoke sensor signal and as a mobile user terminal . So ,the camera contains a receiver of a 315 MHz and contains transceivers of 1800 MHz ,1900MHz of GSM/UMTS systems respectively . By using this high-tech wireless equipment (3G security camera) shown in figure 4.1 , it is possible to detect anywhere at any time by dialing video calls with 3G mobile phone . It is also compatible with normal 315 MHz or 433 MHz wireless sensors . A 3G card (W-CDMA) is needed to run the 3G camera system. When the wireless sensor such as door sensor , motion detector or smoke sensor ,as in this work, is triggered ,the 3G camera will dial out the pre-set phone numbers to have a video call so that live video of what's happening can be seen. During the video call , it is possible to record the video on the 3G camera or on the mobile . Max 15 wireless alarm sensors can be added to the system. Also the 3G camera can be dialed to start video call even if there is no alarm call from the 3G camera.

Figure 4.1 3G security camera.[Appendix A]

Features of 3G security camera :

This product uses USIM card, and supports WCDMA 3G network . Built-in 300K pixel CMOS camera and infrared light, and supports punctual wireless video surveillance for all day . Built-in Passive Infrared Detection, It automatic detect after setting defense. Built-in MIC and speaker, enables two-way video intercom and on-site talking function . Remote control by mobile message, which is confidential and safe . Supports SMS alarm, video call alarm, and voice call alarm . Alarming process automatic record into T-Flash card . Can preset 11 mobile numbers that would receive alarms . With remote controller to control setting defense, Cancel defense or emergency alarming . Built-in Replaceable lithium battery (Nokia BP-6M battery 1200mAh) to ensure that the camera work normally when the power cut.

4.4- GSM-SMS communicator :

The GSM-SMS communicator device used in this work is shown in figure 4.2 .

Figure 4.2- GSM-SMS communicator .[Appendix B]

GSM-SMS Communicator is powered by adapter 220V/9-12V/500mA , loaded with SIM card, and connected to antenna .

It works with all GSM operators, GSM network 850/900/1800/1900 MHz and it is designed for:

1. Switch On and Off circuit closer of an electrical consumer via 3 current relays. The control of these 3 relays is realized by sending SMS (with specific text) or ringing to the GSM communicator.

a) When ringing from phone number , it can:

- Restart an electrical consumer;
- Realized audio connection.

b) Sending SMS with text “on:1 (off:1)” for control of the first relay, “on:2 (off:2)” for the second relay and text “on:3 (off:3)” for the third relay.

2. Receiving information in case of activation of one or more sensors, the GSM-SMS Communicator dial to the one of the predefined phone numbers and :

a) Send SMS with specific text.

b) Ring shortly to this number

c) Ring for long time unless someone picks up the phone.

Features:

- GSM-SMS Communicator works with professional GSM module allowing to work with all GSM operators.
- Power supply from distribution 12V or alternative from main power supply (12V adapter
- 3 inputs for switching contacts. 1 and 2 works when is short circuit at input and the 3rd is working with current.
- The communicator dispose with 3 relays for switching electrical consumers with max. power 220V/ 2A.

12V Out is for supplying small-outputs with max. power 12V/250mA.

- It dispose with internal microphone;
- Preprogramming software via PC with USB cable.
- Switching on and off relays with SMS or ringing
- Information for activation of sensors via SMS or ringing

- Possibility for checking moment positions of relays and sensors via SMS.

LEDs indications :

- Red LED:

1- lightening : communicator is not ready yet. It is starting.

2- flashing : ready.

- Blue LED:

1- flashing fast : searching GSM network

2- flashing slow: GSM network working

- Green LED:

1- lightening : working properly.

Schematics and parameters of Inputs/Outputs:

Inputs 1 and 2 (D1&D2) as in figure 4.3 ,are for plug in all sorts of sensors. They are activating with close circuit. When they are activated the GSM-SMS Communicator send SMS or ringing to defined GSM number.

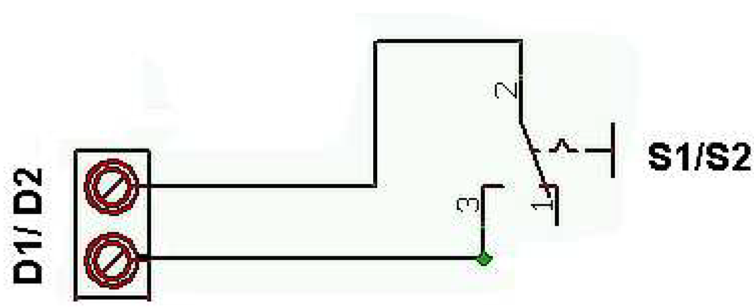


Figure 4.3- Schematics of input 1 and 2 connection.[Appendix B]

Input 3 , figure 4.4 , works as same as 1 and 2 but it is activating with current. Users can use output 12V to supply non-electrical sensors.

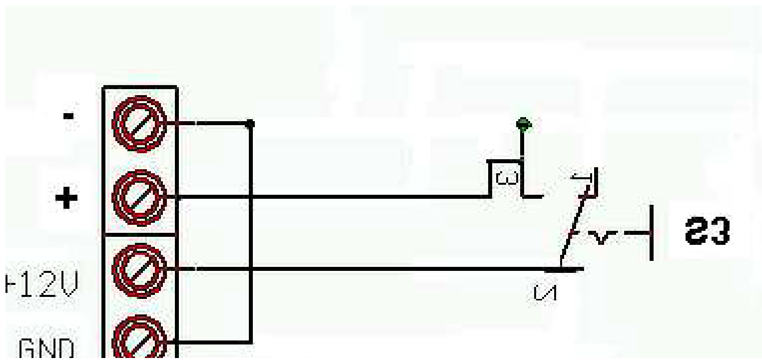


Figure 4.4- Schematic of input 3 connection.[Appendix B]

Galvanically separated switching contacts 230V/ 2A (K1, K2 and K3). Each relay has 3 pins. 1- normally On, 2- middle point, 3- normally Off. Connecting the GSM-SMS communicator device with the consumer to be controlled remotely is done as in figure 4.5 .

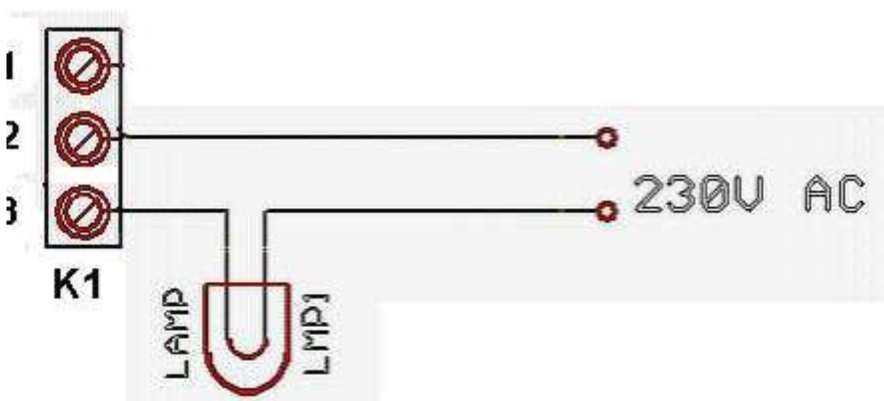


Figure 4.5- Schematics of relay connection with consumer.[Appendix B]

- **Making audio connection:**

Outs for Microphone and Speakers can be used for making audio connection between GSM-SMS Communicator and an ordinary GSM. If a user ring to the communicator and an audio connection is On, what’s happening in the place can be hear where the communicator is.

3.4- Mobile station :

Mobile station consists of SIM card and the mobile phone set . Any mobile phone compatible with WCDMA can see the monitoring area by receiving the video call from the camera or dialing video call to the camera . Any mobile phone with SMS function can control the remote camera with SMS command , also this mobile phone can deal with the GSM-SMS communicator.

3.5- Availability of GSM and 3G networks :

The area where these systems assigned to be used should be covered by GSM and 3G networks, otherwise this task will not be successfully done . To register onto the 3G network (in the network menu, dual network (3G or UMTS and GSM) is selected when the phone is set for manual network search. If the phone has been set for automatic network selection, whenever it is within a 3G network coverage, It will automatically register to the 3G network.

CHAPTER 5

Experimental Work and Results

Experimental Work and Results

5.1- Introduction :

This dissertation is aimed to get the benefits of the existence of the networks and their infrastructure of GSM and UMTS systems in the area , rather than just using these networks in voice communications or even specified data (such as SMS) or video calls , they can be used for private applications as in this dissertation ,the 3G network is used to monitor the place and the GSM network is to activate or control the remote system.

5.2- Experiment No 1: Monitoring the place

Before putting the 3G camera ,used in this experiment , in work it is necessary to configure it in a specified way to meet the needed requirements .

5.2.1- Configuration of the 3G camera :

To configure the camera , it is needed to follow specified steps as follows :

i- Activating the camera and defining the master :

When first time using the remote camera, it is needed to set the master number to activate the camera . the master has the authority to configure , control the camera , and receives alarm message when the camera is triggered .Master sends the following SMS command to the camera :

#master#

the camera replies : “ **Welcome to use remote camera, the password is xxxx**”. At this moment, the telephone has been set as an authorized master number .

when analyzing the security of this procedure , it is worth mentioning that this type of camera is designed to suit wireless applications , and once a master user is defined , it is secure that no other unspecified users will be permitted to deal with the camera .

ii- Adding alternative users :

Because many other predefined mobile telephone numbers are needed as an alternatives to the master number to get the indications of the smoke (SMS and video call) when the master number is unavailable , so some other telephone numbers have been added to the camera as an alternative normal users , that is done as follows：

The master sends the following SMS to store the user's member's mobile phone number into the camera.

#adduser#092xxxxxxx#

After successfully set ， the camera will reply ： "**The user number 092xxxxxxx has been successfully added** " . Only the master is authorized to add users . Maximum 10 user's numbers can be defined**.**

This is one of reliabilities of this system to make sure that the alarm will be submitted to one of the users who are responsible of the situation . As a part of discussing these advantages of the camera , any user other than those defined will be rejected when trying to make a call with the camera . Also the camera has a UPS system, that when the mains AC supply is turned off , the camera will be fed by an internal battery and it will send SMS to the mobile user " **AC power shut off** " .

iii- Configuring wireless sensor :

Any 315MHz wireless sensor, such as infrared motion detector, wireless door magnet, wireless smoke sensor etc, can be used and set as an alarm sensor of the camera. In this work , smoke wireless sensor is defined to the camera as follows : Power on the wireless sensor. The following SMS command has been sent to the camera by the master (it can be by a normal user) , and the camera entered into the state to add new wireless sensors:

#add sensor#smokesensor#

After receiving the SMS command, the camera sent back SMS "**Waiting to load sensor, make the sensor work immediately**" . Then the sensor is triggered to send signal immediately , the camera exited the learning status, and replied " **Adding sensor successfully** ". Max 15 wireless sensors can be added to the camera.

Configuring the smoke sensor is a kind of defining the code (encryption) between the sensor and the camera to ensure that no other signals with same frequency can effect or trigger the camera .

The communication between the smoke sensor and the 3G camera is a wireless application, it is one way communication system , where the transmitter is located in the smoke sensor , while the receiver is located in the camera. although this frequency , 315 MHz, is not in the ISM bands , it does not need any license because it is used as a personal network and it covers a short distance (e.g. in the same room) .

iv- Activating Infrared light :

In order to make the camera work even in full darkness , night shoot is activated by activating Infrared light **,** Infrared light enables the camera to have a real time video clearly in dark night . Camera can control the infrared light automatically. A SMS has been sent to turn on the infrared light . **#ir#1#**

After successful set, it replied "**Infrared light turns on** " .

v- Image parameter setting and volume adjustment :

Master and normal users can activate the real-time video by making a video call to the camera ; meanwhile, the mobile phone can be used to control the video image by setting the image brightness, focus, direction and volume. The operation definition of the correspondent key in video call as follows :

"1" Zoom in

"2" Zoom out

"3" brightness increase

"4" brightness decrease

"5" Image direction

"*"volume up

"#" volume down

A wider range of camera coverage is possible by obtaining better zooming and coverage using multiple camera system , though it is not in the scope of this work.

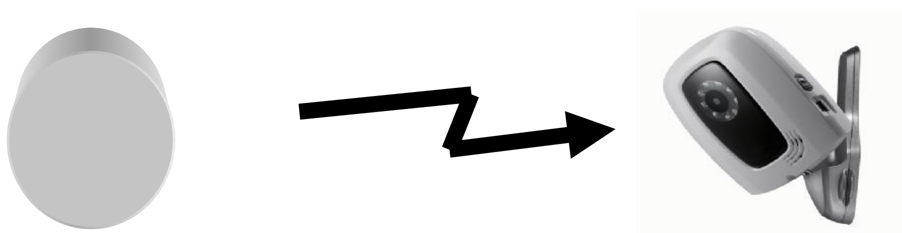
5.2.2- Actual experiment using 3G camera to monitor a place regarding a fire or smoke:

The following image , figure 5.1, is captured from the experiment that has been done to fulfill the task of monitoring a place regarding a fire or smoke.

Figure 5.1- Devices used in experiment 1 .

The place to be monitored by the camera should be covered by the 3G network ,otherwise it is not possible to get a video call from the camera to view the monitored place , but only voice call can be established.

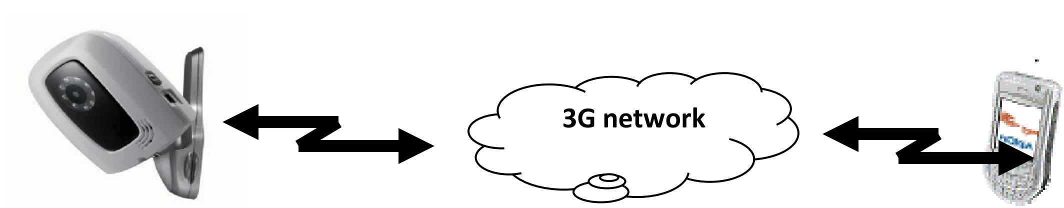
The smoke sensor and the 3G camera are located in appropriate places in the store to cover the area as much as possible. When a smoke has been created , for the sake of the experiment , in the store to be monitored ,the smoke sensor sensed the smoke and is activated . once the sensor is activated, three actions took place : sound , flashing of the LED and a signal of 315 MHz has been sent to the area around the place of interest, including the camera as in figure 5.2. This ,315 MHz , is an appropriate frequency to be used in this scenario , because the distance between the smoke sensor and the camera shouldn't be long . if long distances are needed , other frequencies can be used to carry the sensor signal to the communicator (3G camera) such as 443 MHz and 868 MHz which can go for longer distances up to 100 and 300 meters respectively .



Smoke sensor **315MHz signal** **3G camera**

Figure 5.2- The connection of the smoke sensor to the 3G camera .

the 3G camera which is located around receives that 315 MHz signal and is triggered , then it sent SMS message informing the predefined mobile user that there is a smoke alarm in the monitored place " **smoke sensor alarm** " , and the other important action done by the camera is making a video call to that user to see what is going on in the place as in figure 5.3 . If the 3G network is not available , the camera will use the GSM network and make a voice call to the mobile user .



3G camera **Mobile user**

Figure 5.3-Communication between the 3G camera and the mobile user

5.2.3- Another application of the 3G security camera :

The 3G security camera can be used for many other applications such as a motion detection application . To activate any application of the camera , special procedures need to be done .

Activation of the motion detection :

Motion detection is movement recognition technology by comparing the difference between the previous image and the later image. Motion detection works only when the camera is in Set Defense status and the motion detection function is open. The motion detection function is only used in quiet place where there is no continuous motion , such as quiet room or warehouse. It mustn't face to shaking tree or other moving things, otherwise it will continuously get the difference between the previous image and the later image which will activate the camera to send alarm message and making a video call to the predefined mobile , and that may lead to destroy the camera.

To activate the motion detection application , Master or normal users send the following SMS command to the 3G camera:

Open motion detection:

#motion#1#

After successful set, it will reply **"motion detection open"**

When this application is not needed , it can be deactivated by sending SMS to the camera

Close motion detection:

#motion#0#

After successful set, it will reply **"Motion detection closed"**

According to the place to be monitored , motion detection sensitivity is adjusted .

Motion detection sensitivity :

#grade#(0-4) #

The sensitivity grade can be 0,1, 2, 3, 4, the larger the number, the stronger the sensitivity. In grade 2, the camera can detect human body motion .

After successfully set, the camera will reply: **"Motion detection sensitivity set successfully."**, if wrong parameter, it will reply **"Wrong parameter, please check and try again"**

5.3-Experiment No. 2 :Activation of the remote platform

Following to the previous experiment ,and when the view of the monitored place is obtained , an action has been taken to control the situation (responding answer). In this experiment ,GSM and SMS network mobile systems have been used for the purpose of communication and fire extinguishing control respectively

The GSM-SMS communicator used is described in the previous chapter , it is configured to fulfill the required needs .

5.3.1- Configurations of GSM-SMS Communicator :

Drivers are installed on the computer ,used in the configuration of the GSM-SMS Communicator. At the first time connecting GSM-SMS Communicator to the computer, Windows asked for drivers. All the driver files are copied to the computer. the GSM-SMS Communicator is powered on and Connected to the computer via USB cable . The file GSM_Communicator_config.cfg is opened and the deserve changes are made, The file is saved from menu – File-> Save. then the program is closed. The file GSM_Communicator_config.bat is started to program the Communicator. Then after every line in the opened windows there is OK which means that everything is OK , After completion of the programming , The antenna is plugged in and SIM card is loaded into the communicator . The power is restarted and communicator is ready to work.

The following statements are the settings done for the file saved in the GSM-SMS communicator :

#contains the phone numbers which can control this device. All other numbers will be skipped.

SET-PLIST:0,00218928830421

SET-PLIST:1,00218926781435

SET-PLIST:2,0000000000

SET-PLIST:3,0000000000

SET-PLIST:4,0000000000

SET-PLIST:5,0000000000

SET-PLIST:6,0000000000

SET-PLIST:7,0000000000

SET-PLIST:8,0000000000

SET-PLIST:9,0000000000

#Contains the numbers which receive info when one or more sensors are activating

SET-ALIST:0, 00218928830421

SET-ALIST:1,00218926781435

SET-ALIST:2,0000000000

SET-ALIST:3,0000000000

SET-ALIST:4,0000000000

SET-ALIST:5,0000000000

SET-ALIST:6,0000000000

SET-ALIST:7,0000000000

SET-ALIST:8,0000000000

SET-ALIST:9,0000000000

#Occasion at incoming ringing

#0 - nothing / 1- refuse the call and restart 1st relay / 2-answer the call/

SET-ATAM:2

#Occasion at activating of sensor (0-only click, 1-SMS, 2-ringing, 3-SMS+ring,#4-click to ALL, 5-SMS to all, 6-SMS to ALL+ ring to 1st)

SET-SSMS:6

#Sensors time. Put the request time for activating the sensor in seconds. It can be from 0 to 60 sec.

SET-STIME:1,2

SET-STIME:2,2

SET-STIME:3,2

#names of sensors. here you can name every one sensor individually.

#when you receive SMS you can see which sensor is activated

SET-SNAME:1,Sensor1

SET-SNAME:2,Sensor2

SET-SNAME:3,Sensor3

#Put the SMS text here at activated sensor. It can't be more than 30 symbols

SET-SMSTXT:Activated sensor:

#Automatically or manually deleting of SMS. 0-manually; 1-automatecally

SET-SMSDEL:1

SET-END

5.3.2- Description of settings which are done on the file :

1- List #1 with authorized numbers which can control the device. All phone numbers which is not in that list can't control it. Their calls will be skipped. The list can contain up to 10 phone numbers which must be written in international format:

SET-PLIST:<n>,00218xxxxxxxxx , <n> = from 0 to 9

2- List #2 with all phone numbers which will receive a SMS or a call when one sensor is activated. One or more phone numbers will receive SMS or ringing when one of the sensors is activated depend on setting - SET-SSMS . The list contain up to 10 phone numbers which must be written in international format:

SET-ALIST:<n>,00218xxxxxxxxx , <n> = from 0 to 9

3- Events at activating sensor (all cases are related with phone numbers in list #2)

SET-SSMS:<n><n> - mode

If n=0 the Communicator ring shortly to the first number in List #2

If n=1 the Communicator send SMS to the first number in List #2

If n=2 the Communicator ring continuously to the first number in List #2

If n=3 the Communicator first send SMS to the first number in List #2 and after that ring continuously to that number

If n=4 the Communicator ring shortly one by one to all phone numbers in List #2

If n=5 the Communicator send SMS to all phone numbers in List #2

If n=6 the Communicator send SMS to all phone numbers in List #2 and after that ring continuously to the first number in List #2

4- Setting the time for activating of sensors. When one sensor is activated , the Communicator wait to expire that time to see if the sensor is still activated and if it is, Communicator send SMS or ring to one number. If sensor is activated for very short time (less than the defined time) the communicator will not send SMS or ring.

SET-STIME:<n>,<sec>where:<n> = 1,2 or 3 (this is the number of sensors) <sec> = the time in seconds (from 0 to 60) for activating the sensors.

5- Set the unique name to any one sensor. The name is written after the comma :

SET-SNAME:1,Sensor1

SET-SNAME:2,Sensor2

SET-SNAME:3,Sensor3

6-Set the text in SMS which the communicator will send you

SET-SMSTXT: Activated sensor:

Example: If "Activated sensor:" is written in the option SET-SMSTXT and in option SET-SNAME: "Sensor1" is written , when a sensor is activated, SMS with text: "Activated sensor: Sensor1" is received .

7- Events at incoming call

SET-ATAM:<n><n> - mode: If n=0 – nothing will happen .

If n=1 – the relay №1 will be restarting for 5 sec. (switch on and after 5 sec will be switch off) . If n=2 – the communicator make audio connection between GSM and the Communicator .

8- Switch On/Off relays with SMS.

If you want to switch relays with SMS you have to write SMS with text: '**On:1**' or '**Off:1**' for switching first relay , '**On:2**' or '**Off:2**' for the second relay and text '**On:3**' or '**Off:3**' for the third relay. If you write "**?**" at the end of the SMS you will receive SMS with the condition of all sensors and relays. If you want to check their conditions you can send a SMS only with text "**?**".

9- Manually or automatically deleting of received SMS in the SIM card in the Communicator. **SET-SMSDEL:<n>**<n> - mode

If n=0 all SMS will remain in the SIM card until someone delete them. When the SIM card contains more than 20 SMS in it, its Memory is low and the Communicator will send you warning

SMS to delete them. You can delete them with sending a SMS with text “DELETE”. If you don't delete them on time the memory will be fill in 100% and the communicator will stop receiving SMS. This will make it to work not properly. If n=1 the communicator will delete every SMS which will receive after reading and executing it. In that case the SIM memory will be always empty and the communicator will work properly.

5.3.3- Activating the fire extinguishing system :

The following image (figure 5.4) is captured from the experiment that has been done to fulfill the task of activating the fire extinguishing system .

Figure 5.4- Devices used in experiment 2 .

After finishing the configuration of the GSM-SMS communicator , It is located at the monitored place and connected to the controlled fire extinguishing system which is used to extinguish the fire through the appropriate relay .Figure 5.5 shows the interconnection between the GSM-SMS communicator ,the extinguishing system and the mobile user . In this experiment , the activation has been simulated by starting on a fan . Normally the extinguishing system can be divided into three parts , each part covers a specified area , and connected to one of the three relays at the GSM-SMS communicator K1 , K2 and K3 to specify that only the appropriate extinguishing system part will be used in the deserved area .

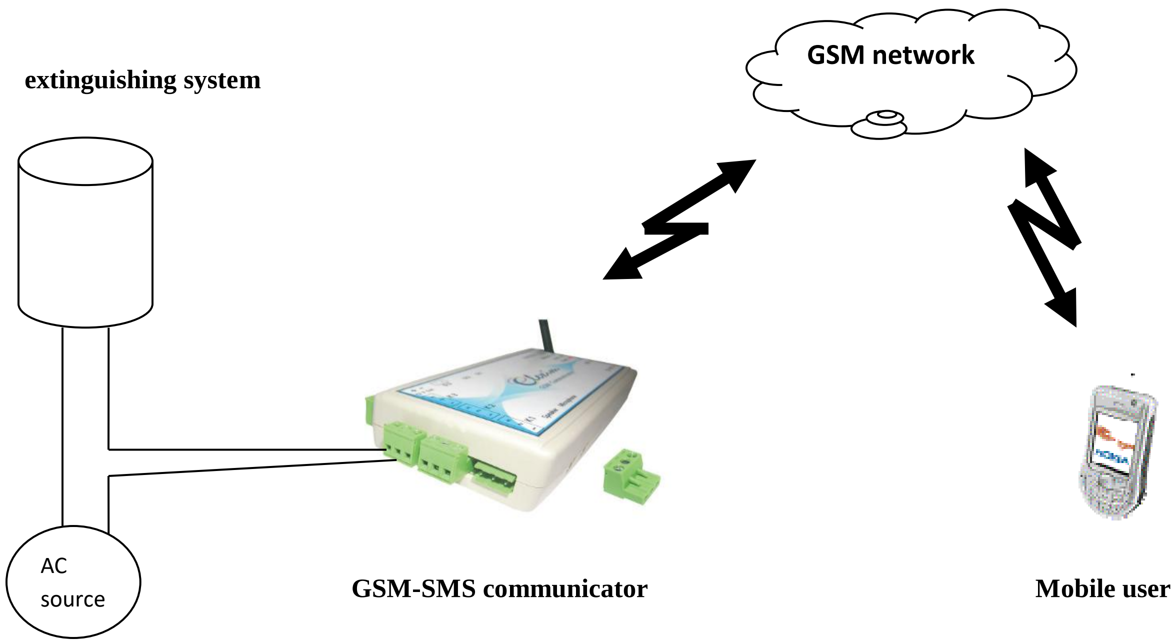


Figure 5.5- The interconnection of the GSM-SMS communicator

The GSM-SMS communicator will control the power supply of the extinguishing system through the appropriate relay K as in figure **5.6**.

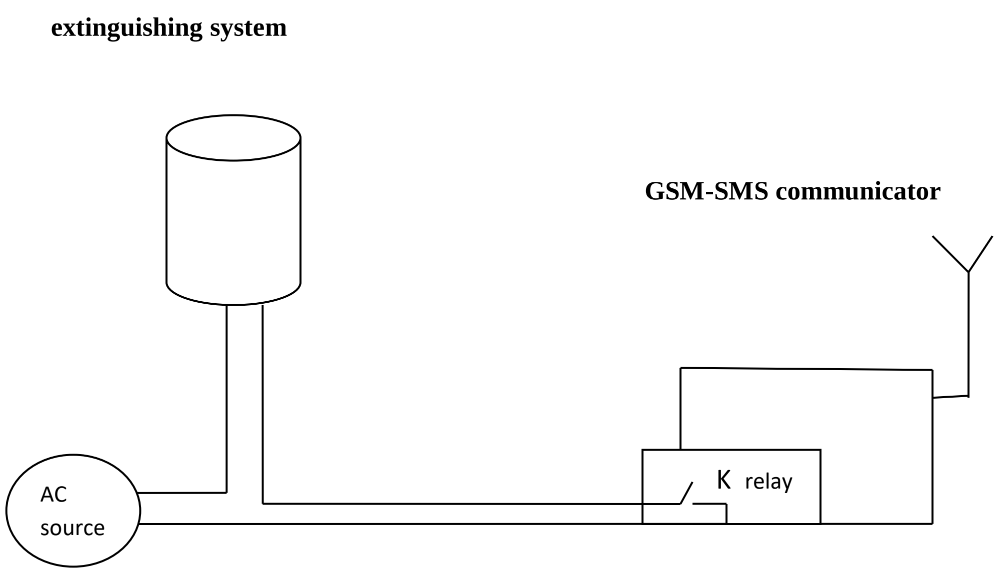


Figure 5.6- Switching on the extinguishing system

When a fire is discovered , by using the mobile , where ever the mobile user is , SMS is sent to the GSM-SMS communicator with text "**On:1" , "On:2" or "On:3"** to activate the first ,second or third part of the extinguishing system by connecting them to the power source through the relays K1,K2 or K3 respectively .

CHAPTER 6

Conclusions and Recommendations

Conclusions and Recommendations

6.1- Conclusion :

Based on the results undertaken in this work , The following conclusion can be withdrawn :

- The use of public wireless networks (such as GSM and UMTS) is feasible to conduct remote monitoring scenario , The mobility that offered by those networks provides more flexibility to accomplish a private application such as monitoring shops or stores against thefts or fire , and also to activate remote systems such as water pumps , air conditioning or any other systems or appliances while moving and not stuck in a fixed place or so far from the place of interest .
- Available technology has been used to verify the actual experimental work, and cases of smoke and motion detection have been targeted and achieved .
- Remote activation of usable detection , processing and transmission devices and apparatus has been experimented and tested .
- Payback action has been also tested as respond to a fire case by achieving remotely an extinguishing system .

6.2- Recommendations :

1- A more sophisticated system to monitor multiple points or places by enhanced voice and video .

2- Improvement of video quality ; one suggestion is suppression of voice before loaded on the channel .

REFERENCES

[**1**] Simon Haykin **, Communication Systems ,** Forth Edition **,** John Wiley & Sons, Inc., 2001 **.**

[**2**] Ian Glover , Peter Grant , **Digital Communications** , TJ International Ltd, Padstow , Cornwall , 2000

[**3**] Robert G. Winch , **Telecommunication Transmission Systems** , Second Edition , McGraw-Hill Companies Inc , 1998

[**4**] J.Dunlop and D.G. Smith **, Telecommunication Engineering ,** Third Edition , Chapman & Hall , 1994 .

[**5**] Gérard Barué , **Microwave Engineering Land & Space Radio Communications ,** John Wiley & Sons, Inc. 2008

[**6**] Roger L. Freeman , **Radio System Design for telecommunications ,** Third Edition **,** John Wiley & Sons, Inc. , 2007 .

[**7**] Antti V. Ra¨isa¨nen , Arto Lehto and Artech **, Radio Engineering for Wireless Communication and Sensor Applications ,** Artech House, Inc. **,** 2003 **.**

[**8**] Thomas A. Milligan **, Modern Antenna Design ,** Second Edition , John Wiley & Sons, Inc , **2005** .

[**9**] **Fundamentals of Wireless Communications & CDMA ,** Student Guide CDMA-050 80-13127-1 X6 January 24, 2000 .

[**10**] Bernard Sklar , **Digital Communications: Fundamentals and Applications ,** Second Edition ,Prentice Hall P T R,

[**11**] Andrea Goldsmith **, Wireless Communications ,**Cambridge University Press , 2005 .

[**12**] H.Vincent , Gregory W. Wornell , **Wireless Communications : Signal processing perspectives ,**Prentice Hall PTR , 1998

[**13**] Norihiko Morinaga ,Ryujikohno and Seiichi Sampei , **Wireless Communication Technologies : New Multimedia Systems ,** Kluwer Academic Publishers , 2002 .

[**14**] Harry R. Anderson, **Fixed Broadband Wireless System Design,** John Wiley & Sons Ltd, 2003.

[**15**] Simon Haykin and Michael Moher , **Modern Wireless Communications,** Pearson Prentice Hall , 2005 .

[**16**] Bosco Leung , **VLSI for Wireless Communication ,** Prentice Hall

[**17**] K. Fazel and S. Kaiser , **Multi-Carrier and Spread Spectrum Systems ,** Second Edition , John Wiley & Sons, Ltd , 2008 .

[**18**] William Webb, **Understanding Cellular Radio ,** Artech House, Inc. , 1998 .

[**19**] Eberhard Brunner **, cellular communication tutorial ,** Am Westpark 1-3 81373 Munich Germany

[**20**] Ian Poole **, Cellular Communications Explained From Basics to 3G ,** first edition , Linacre House, 2006 .

[**21**] Gordon L. Stüber , **Principles of Mobile Communication ,** Second Edition , Kluwer Academic Publishers , 2002 .

[**22**] Jochen H. Schiller **, Mobile Communications ,** Second Edition **,** Pearson Education Limited , 2003 .

[**23**] Jörg Eberspächer , Hans-Jörg Vögel , Christian Bettstetter , Christian Hartmann , **GSM – Architecture, Protocols and Services ,** Third Edition , John Wiley & Sons, Ltd , 2009 .

[**24**] Juha Korhonen **, Introduction to 3G Mobile Communications ,**Second Edition **,** ARTECH HOUSE, INC. , 2003 .

[**25**] **IEEE communications Magazine ,**September 2009 , vol. 47, No. 9

[26] الدكتور هشام عرودكي , **" اسس و مبادئ "** **نظم الاتصالات الخلوية** , الطبعة الاولى , مكتبة الاسد , 2013

[27] **http//www.tutorialspoint.com/gsm/gsm_architecture.htm 18/11/2012**

[28] **http//www.gsmfavorites.com/documents/introduction/mobile/ 22/11/2012**

[29] **http:// www.maketecheasier.com/the-evolution-of-cellular-network/ 20/8/2012**

[30] **http:// Nashville.dyndns.org.800/wirelessDownloads/UMTS-WCDM/ 10/5/2014**

Appendices

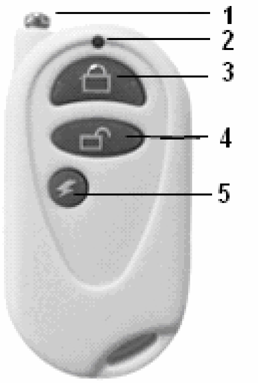
APPENDEX A

3G REMOTE CAMERA

Difference authority between Master and normal users:

User Type Function		Administrator	Normal users
Change user list		Yes	No
Automatic Alarm	Receive SMS	Yes	No
	Receive voice alarm calling	Yes	Yes
	Receive video alarm calling	Yes	Yes
Dial the phone number	Monitor by dialing voice call	Yes	Yes
	Monitor by dialing video call	Yes	Yes
Send SMS command		Yes	Yes
Add, modify ,delete sensor		Yes	Yes
Check status and obtain command help		Yes	Yes
Change password		Yes	No
System Recovery		Yes	No

Remote control illustration



Picture 2: Remote control Instructions

1. Antenna 2.Indicator light
3. Arming key 4. Disarming Key 5. Emergency key

Indicator light Status Instruction:

Color	**Action**	**Status**
Red LED	Flash slowly	Searching the network.
	Flash quickly	Sensor alarming.
	Continuously on	Not installed SIM card, or the remote camera damaged.
Green LED	Continuously on	Arming, Open the auto-alarm function.
	Flash slowly	Disarming. Close the Green auto-alarm function.
	Flash quickly	Processing data.
Orange	Flash	Wait to load remote control.

.

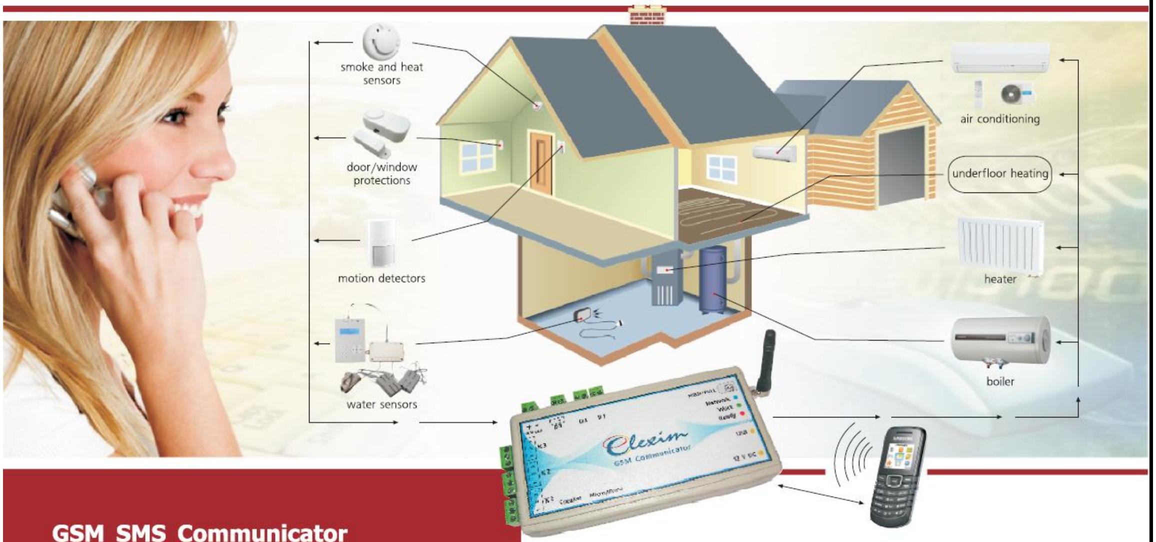
Main Technical Parameters :

Power adaptor	**Input:**100V～240V/50Hz **Output:** 5.5V DC
Work temperature	-10℃～+45℃
Store temperature	-20℃～+60℃
Relative Humidity	10-90%，without condensation
Working frequency:	HSDPA/UMTS 850/1900/2100 MHz EDGE/GPRS/GSM 850/900/1800/1900 MHz
Wireless sensor receiving code	ASK
Wireless sensor receiving frequency	315/433 MHz
Wireless sensor baud rate	500-2500 bps
Max wireless sensor	15 unites
Effective distance of the wireless remote control	100 Meters (wide area)
video format	3GP
Camera pixel	300K pixel
Camera Shooting angel	60 degree (horizontally) , 60 degree (vertically
Best shooting distance in night	≤6 meter
Lithium battery	800mAh
Battery standby time	24 hours（ close the infrared light) Affected by network

APPENDEX B

GSM SMS Communicator

System for remote control and security



GSM SMS Communicator
is highly professional and intelligent system with digital control.

Thanks to that system you can receive information of changes in the status of your secure or conditioning systems, rooms, etc.

Remote control of electrical devices, manufacturing process machines, communication equipments and etc.

Realize audio connection.

It work with SIM card supported by all GSM operators.

GUARANTEE 2 YEARS

Made in Bugaria

MAIN FEATURES

- Notify with SMS or ringing when one or more sensors is activated.
- Remotely control of electrical devices, air-conditions and etc. using SMS.
- Audio connection via embedded microphone or with external headphones.
- Checkup the status of sensors and relays using SMS.
- Access only from authorized numbers.
- LED indications.
- Easily tunes through USB cable.

* all functions and adjustments can be seen in Users manual guides on our web site ww.elexim.com

www.elexim.com

Sofia 1113, Blvd. Tsarigradsko Shose 7-th km Num 133, BIC IZOT, office 314, tel. +359 2 971 8880, 971 8881; +359 896757070
e-mail:office@elexim.com

I. Protection

Without additional security system

Sensors are directly connected to the GSM-SMS Communicator. When one of them is activated, the communicator dial one predefined number or send and SMS to that number with special text with the reason for that activation.

Add to existing secure system

If your alarm system is activated, GSM-SMS Communicator ring or send and SMS with proper text to one predefined number.

If you accept that calling you can hear what is going on in the room where the communicator is.

If you send and SMS you can swich on/off electrical devices in this room.

II. Remotely control and monitoring

Turn on/off of electrical devices such as air-conditions, lightening and irrigation systems and etc. via embedded relays.

Receive information with SMS or ringing when one or more sensor (for temperature, moisture etc.) is activated.

III. Conversation

Outgoing call:

When one of the sensors is activated the communicator dial one number and establish audio connection with external microphone and headphones.

Incoming call:

When you dial to SIM card placed in the GSM–SMS communicator you can hear via embedded microphone. If you attach sound or light signaling which inform you that incoming call exist, with external headphones you can talk.

TECHNICAL PARAMETERS

General

- 3 sensors
- 3 relays
- imbedded microphone
- jacs for external microphone and headphones

GSM network

- 900/1800 Hz
- SIM Card – 3 V, Plug-in

Antennas

- SMA connector
- Short – 5 cm, or long – 20 cm with 3 m cable

Consumption

- Stand by – 80 mA
- Max consumption – 450 mA
- Power supply – 12V/0.5 A
- Dimension – 170/80/30 mm
- Interface – USB v.1.0 type B connector
- Operating temperature – 0 ÷ 45°C

www.elexim.com

Sofia 1113, Blvd. Tsarigradsko Shose 7-th km Num 133, BIC IZOT, office 314, tel. +359 2 971 8880, 971 8881; +359 896757070
e-mail:office@elexim.com