International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 4, Issue 3 (March 2015), PP.22-31

An Investigation on Standards and Applications of Signalling System No.7

Adnan Affandi[1], Mubashshir Husain [2]
&Mohammed Ali Omar Batouk[3]
Professor, Dept., of Elect.& Comp. Eng., Faculty of Eng. King Abdul Aziz University Jeddah, KSA[1]
Lecturer, Dept., of Elect.& Comp. Eng., Faculty of Eng. King Abdul Aziz University Jeddah, KSA[2]
M.Sc.(Student), Dept., of Elect.& Comp. Eng., King Abdul-Aziz University Jeddah, KSA[3]

Abstract:- Signaling system 7 (SS7) is the standard communication system that has been used to control public telephone networks since 1980s. Also to control the GSM network (for related and not related circuit signal), SS7 technology later offers advanced intelligent network features.SS7 network are now interconnecting with and operating on Internet data network (SS7 over IP). Based on signaling system- No.7 , a device named REMOTE CONTROL OBSERVER has been developed. The purpose of this device is to start, switch off, open, lock, break down and display the location of the vehicle on the electronic map which is fixed inside it; also it enables the Security Department to locate the place and direction of vehicle inside the GSM Network. The device is consists of a screen (displays the electronic map), and a box consists of a device similar to the cellular phone (with few differences) , batteries and electronic circuit used to break down the electrical circuit of the vehicle ,where the device is subscribed with the GSM Network. The main advantage of this device is to use the available technologies and applications with adding and amending some of the programs and tasks for cellular phone and using the data base of the Home Location Register (HLR) and Visitor Location Register (VLR) by connecting a terminal to enable the user to search for any vehicle.

Keywords:- GSM, SS7 ,etc.

I. INTRODUCTION

Signaling may be described as interchange of information between different functional parts of a telecommunication system. The main purpose for using signaling in modern telecom networks is to transfer control information between different network nodes.

Signaling System #7 is a protocol developed for the implementation of Communications between entities existing within a network to provide the instructors. It is a standard, universally accepted way to transfer information between compatible switching offices following packet-data switching conventions. The SS7 network is a self healing network that maximizes its efficiency and effectiveness by using redundant nodes and links.The information transferred through the SS7 network may be categorized as one of the following:

• Information concerning the set-up and tear-down of calls (call processing for cellular or wire line)
• Information concerning inquires to databases (data base queries such as credit card validations. 800 translations, etc.)
• Information used to maintain the integrity of the SS7 network (Network Management and maintenance)

1.1 Call processing

The most common application of SS7 signaling is Call Processing which entails the transfer, between switches, of all information concerning the processing of the call. This includes the called and calling subscriber data. The charge number, call initiation and termination information, call hand-off information (intersystem when necessary). Etc.(Protocol: is a set of conventions governing the treatment and especially the formatting of data in an electronic communications system).

1.2 Database Queries

Another application supported by SS7 signaling is the Database Query or interrogations directed to the various databases that exist within the network, e.g. HLR. VLR. EIR. AC. Etc (Discussed later). This signaling includes not only the interrogations, but also the return results to these interrogations, or queries.

HLR Home Location Register
VLR Visitor Location Register
EIR Equipment Identity Register
AC Authentication Center

1.3 Network Management

The third application is that of Network Management. This includes all signaling relating to the status of entities and routes through the network. These messages are used by the network to inform all participating nodes of any changes in the availability of a specific destination.

II. OSI AND SIGNALING SYSTEM NO.7 (SS7)

A first specification of SS 7 (Signaling System no.7) was published as early as 1980 in the CCITTs Yellow book, the same year as ISO presented the OSI model. The Signaling System No. 7, which is a type of packet switched data communication, was also structured in a modular way, very similar to the OSI model, but with 4 levels instead of 7 layers.The three lowest levels form a message transfer part, MTP, and the fourth level contains the user parts .Thus, the SS7 is not wholly compatible with OSI. One big difference between the first version of SS7 and the OSI model is the communication process in the network.

The OSI model describes a connection-oriented exchange of data. The communication process then comprises three stages: setting up the connection, data transfer and disconnection.

MTP provides only connectionless transport service (only data transfer phase), which is a faster way of transmitting data in small amounts. In order to meet the need for extended services in certain applications, SCCP (Signaling Connection Control Part) was added in the Red Book of CCITT (recommendations of 1984).

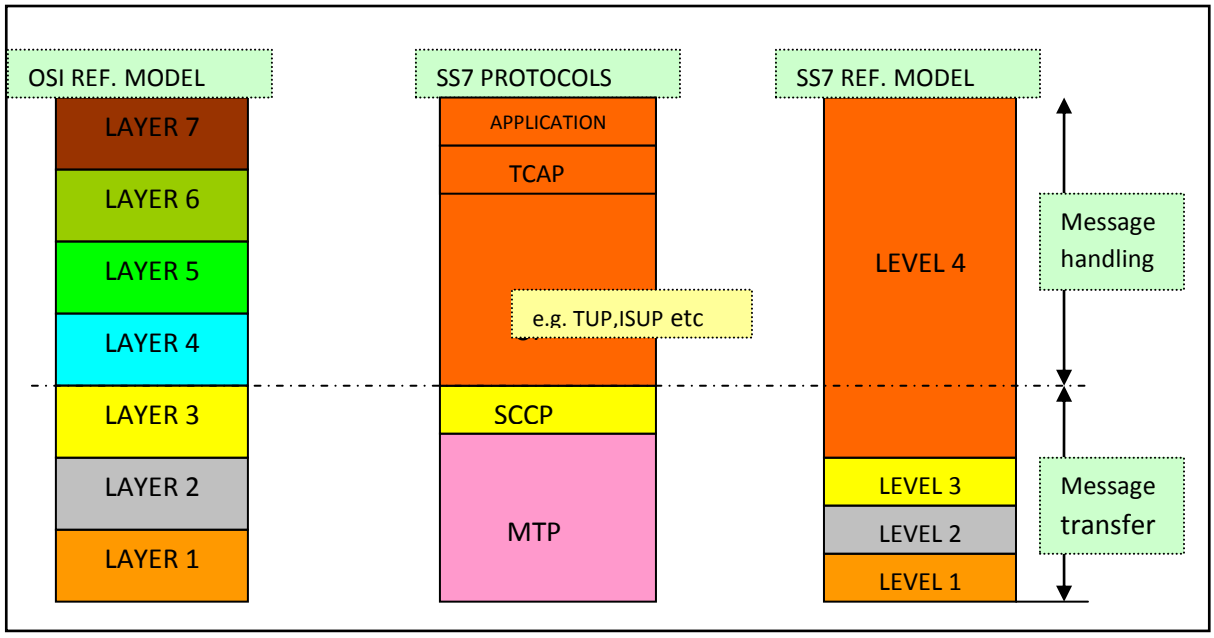


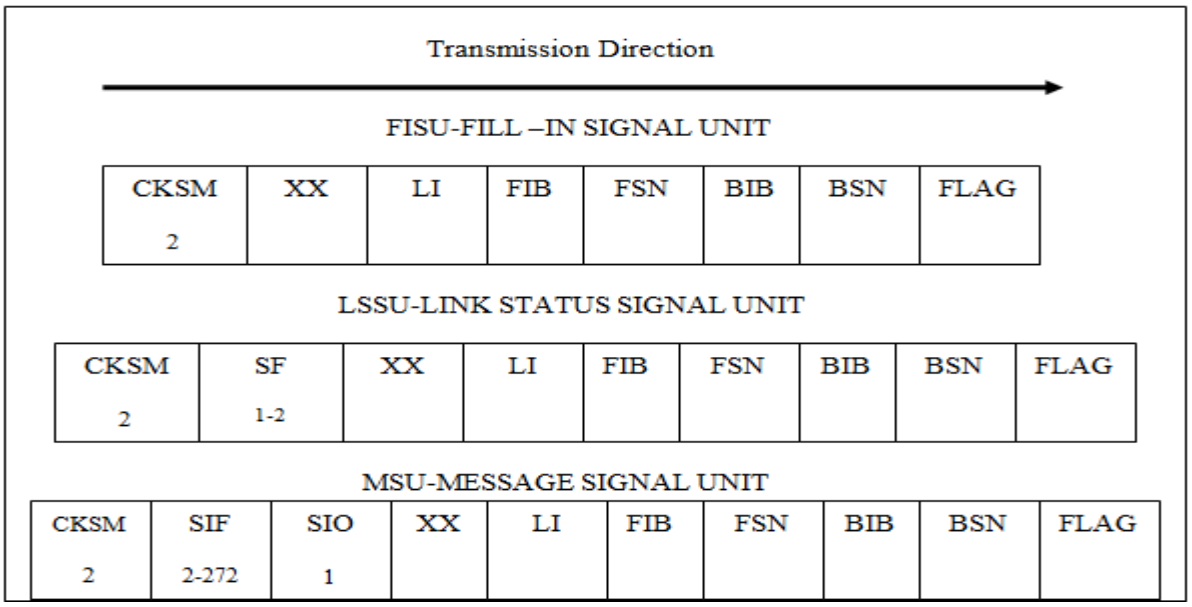
Figure 2.1 Relationship between the SS 7 protocols and junctions used in the OSI and SS 7

SCCP offers both connectionless and connection-oriented network transport service and provides an interface between the transport and network layers that in general conforms to that of OSI. SCCP makes it possible to use a SS7 network, based on MTP, as the carrier between applications that use OSI protocols for the exchange of information in the upper layers. This is an advantage, particularly in cases where SS 7 networks already exist.The functions of the SCCP from the SS 7 point of view belongs to level 4 but from the OSI model point of view these belongs to layer 3. (It is common the use of the word layer when referring to OSI model and level when referring to SS 7).There are no protocols currently used in SS 7 architecture to map into layers 4-6. Protocols may be included in these layers in the future if the need for such services arises.In the CCITT Blue Book (recommendations of 19'88) is also a general protocol for Transaction Capabilities (TCAP) and an Application Part for Operation and Maintenance described. They together correspond to layer 7 in the OSI model.Each User Part defines the functions and procedures of the signaling system that are particular to a certain type of user of the system.Applications are modeled in layer 7. They are the processes that provide the end user.

2.1 Message Formats

SS7 messages are measured in Octets (one octet = eight bits). The maximum length of a SS7 message is 279 octets. This is a MTP limitation. Higher levels are capable of handling larger data streams. Included in the 279 octets is the overhead information added to the data by level two and higher levels.

There are three basic message formats used within the SS7 protocol. They are the Fill in Signal Unit (FISU), Link Status Signal Unit (LSSU), and Message Signal Unit (MSU).



2.2 Message Formats

III. MOBILE APPLICATION PART (MAP)

3.1 INTRODUCTION

The Mobile Application Part (MAP) specifies the application protocols between Mobile Switching Centers (MSC) and related SSS7 network equipment assemblies and databases that are used in wireless network. Figure 3.1 shows how MAP related services information is contained within the TCAP portion of the SS7 Protocol Stack.

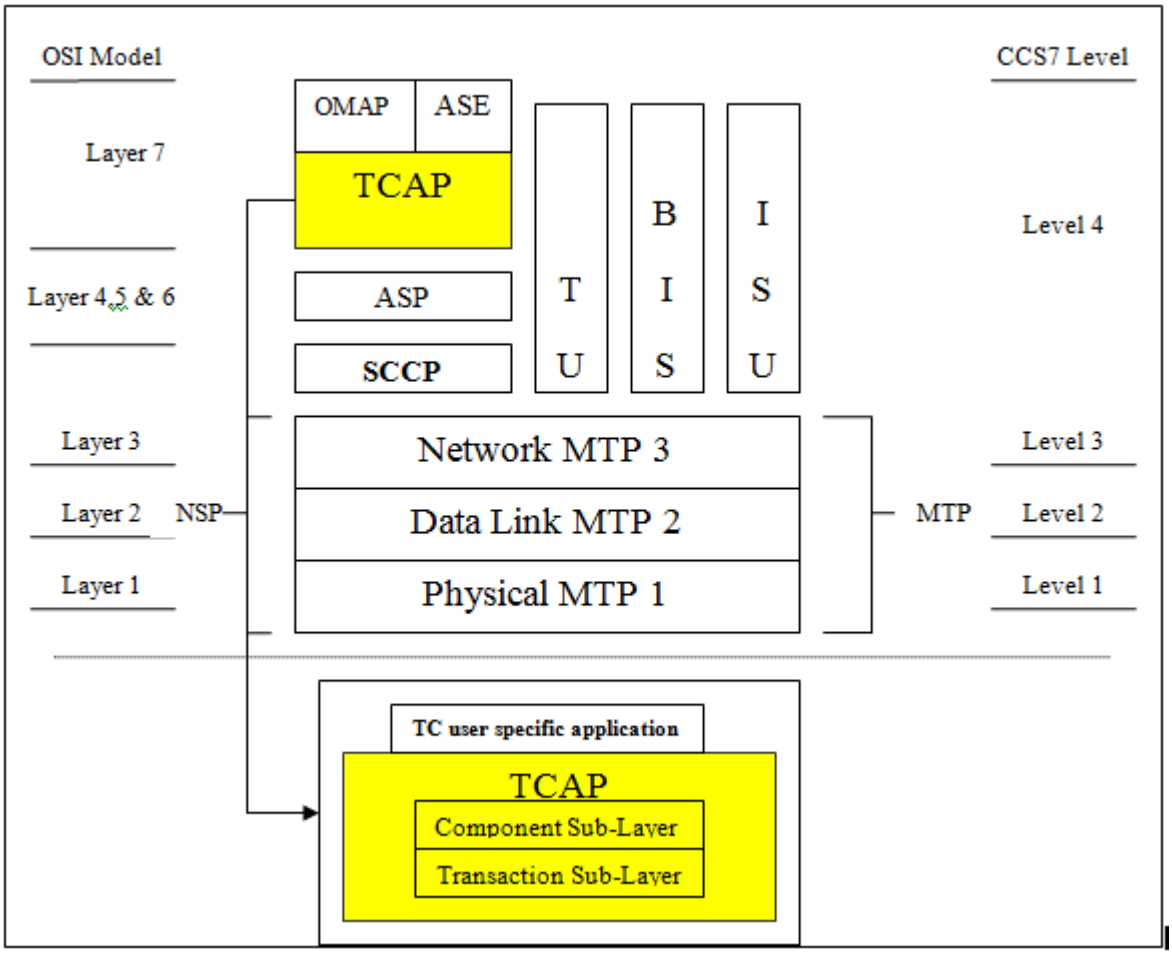


Figure 3.1 MAP in the SS7 Protocol Stack

Within the GSM network, C7 signaling is required between MSC and all the registers (HLR, VLR, EIR and AUC). The signaling protocol used for this purpose is generally called Mobile Application Part (MAP).

C7 signaling is also required between MSC and BSC. The signaling protocol used in this part of the network is called Base Station System Application Part (BSSAP) and contains the BSSMAP (Base Station System Mobile Application Part) and DTAP (Direct Transfer Application Part) protocols.

Between BSC and BTS, as well as between BTS and MS, the signaling system used is based on the DSS1 (Digital Subscriber Signaling system No. 1) which is the same as used in the access network for ISDN subscribers. The protocol used for transport of signaling messages between the BSC and BTS is LAPD (Link Access Procedure on D-channel, layer 2), which has the same structure as the corresponding layer 2 protocol in ISDN (D-channel signaling).Between the BTS and the MS, which from the transmission point of view represent the `air interface', a modified LAPD protocol (usually called LAPDm) is used;

The LAPDm protocol is based on the LAPD functionality but has been adapted to match radio requirements. For example, when using TDMA (Time Division Multiple Access) it is impossible to send signaling frames of the length used in LAPD (up to 249 + 11 octets for the layer 3 header).

Therefore the message is divided into segments of 18 to 22 octets depending on the signaling channel in use.In the air-interface, between the BTS and the MS, the GSM system has a number of different logical signaling channels for different purposes such as:General system information., Paging/access, Handover. Call control, etc.

IV. SS7 AND INTERNET PROTOCOL (IP)

4.1 INTRODUCTION

Public telephone systems today use the Internet for both; telephony voice and to carry signaling system 7 (SS7) messages. The Internet can provide reliable communication services by using the packet based transmission technologies used by IP-based protocols.There is a difference between the Internet and IP based networks. IP based networks uses Internet protocol to route information within the network.

The Internet is a public data network that interconnects private and government computers together. An IP based network does not have to be part of the Internet and it is possible for an Internet network operator to partition their data network to allow for different quality of service (QoS) levels. As a result, it is possible to reliably send SS7 control messages over IP based networks that may be part of the public Internet.

The Internet transfers data from point to point by packets that use Internet protocol (IP). Each transmitted packet in the Internet finds its way through the network switching through nodes (computers). Each node in the Internet forwards received packets to another location (another node) that is closer to its destination. Each node contains routing tables that provide packet forwarding information. These routing tables may be dynamically changed as a result of new connections or paths that may become available through the network.T he pri-mary signaling protocol in use today is Signaling System 7 (SS7) which interconnects heterogeneous networks [1].This is different than the SS7 system that allows the operator to have more precise control over the routing tables. The use of IP based networks for voice, data, multimedia, and signaling offers new potential levels of network efficiency (utilization). A key protocol that has been developed to allow the sending of signaling control messages over IP based networks is Signaling Transport (SIGTRAN). The SIGTRAN protocol stack utilizes the Stream Control Transmission Protocol (SCTP).

SCTP is an IP protocol that combines near-real time data transfer with reliable packet delivery and validation. To allow the use of protocols with SS7 systems, several protocol adaptation layers have been created. These protocols adapt the message structures and flow of messages to emulate the message transfer parts (MTP) of the SS7 protocol stack. Internet telephone systems are primarily composed of media gateways (MGs) and one or more media gateway controllers (MGCs). When Internet telephone systems interconnect to other networks such as the Public Switched Telephone Network (PSTN), they use signaling gateways (SG) or Network Gateways (NGWs). Some of the more common IP Telephony Systems include session initiated protocol (SIP), media gateway control protocol (MGCP), MEGACO, and ITU's H.323 protocol. The SS7 protocol stack consists in several individual protocols, in-cluding Message Transfer Part (MTP) levels1, 2 and 3, Integrated Services Digital Network Users Part (ISUP), Signaling Connection
Control Part (SCCP), and the Transaction Capabilities ApplicationPart (TCAP)[2].

4.2 SS7 and Internet Protocol (IP) Signaling Systems

SS7 messages can be directly transported over IP networks or the functional equivalent of SS7 control message can be sent as control messages (e.g. text based messages) directly between elements connected to a data network(e.g. the Internet)[3]. Figure 4.1 shows that SS7 signaling systems can be interconnected with voice

over data networks and that SS7 messages can be transported over the Internet protocol. This diagram shows that analog and digital telephones are connected to the PSTN. To interconnect these telephones to voice over data network telephones, the media portion of each communication session is routed through a media gateway where it is converted from the PSTN circuit switched form to a IP packet data media format (packetized voice.) This diagram shows that the packet media can be routed through a data network

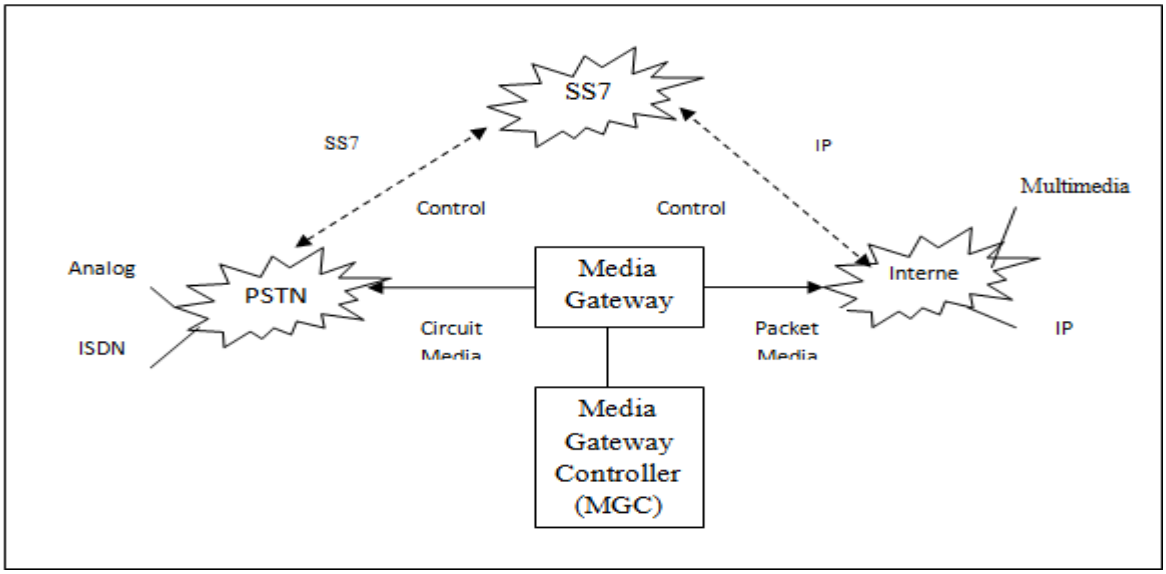


Figure 4.1 Hybrid SS7 and Internet Protocol Network

E.g. Internet- to an end point communication terminal such as a multimedia computer or an IP telephone. This diagram also shows that the SS7 network can control the PSTN through SS7 signaling messages and it can communicate to the media gateway through IP signaling messages.

Figure 4.2 shows a basic voice over IP protocol stack. This diagram shows that the layers for a Voice over IP (VoIP) system may be composed of multiple technologies. The physical layer may be dial-up modems, DSL, cable modems, or any other physical transport system that can transfer digital information. The data link layer includes point-to-point protocol (PPP) and other link management systems. The network layer is the Internet protocol (IP). The session layer is managed uses H.323 or SIP to setup, coordinate and teardown communication sessions. The presentation layer is the conversion of raw information into a usable form such as G.729 and G.711 speech coding. The application layer may include voice, data, and video media display and control.

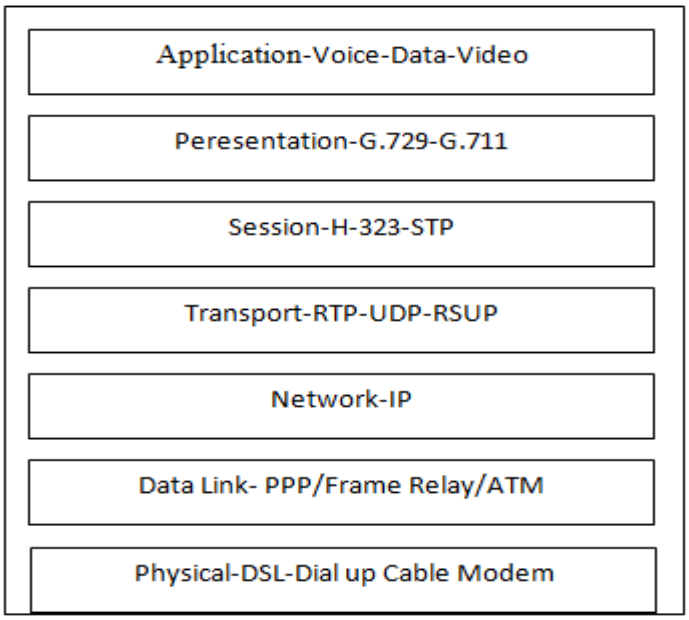


Figure 4.2, VoIP Protocol Stack

V. REMOTE CONTROL OBSERVER

5.1 REMOTE CONTROL OBSERVER

The purpose of this device is to start, switch off, open, lock, break down and display the location of the vehicle on the electronic map which is fixed inside it; also it enables the Security Department to locate the place and direction of vehicle inside the GSM Network.

The device is consists of a screen (displays the electronic map), and a box consists of a device similar to the cellular phone (with few differences) , batteries and electronic circuit used to break down the electrical circuit of the vehicle ,where the device is subscribed with the GSM Network.

The main advantage of this device is to use the available technologies and applications with adding and amending some of the programs and tasks for cellular phone and using the data base of the Home Location Register (HLR) and Visitor Location Register (VLR) by connecting a terminal to enable the user to search for any vehicle.

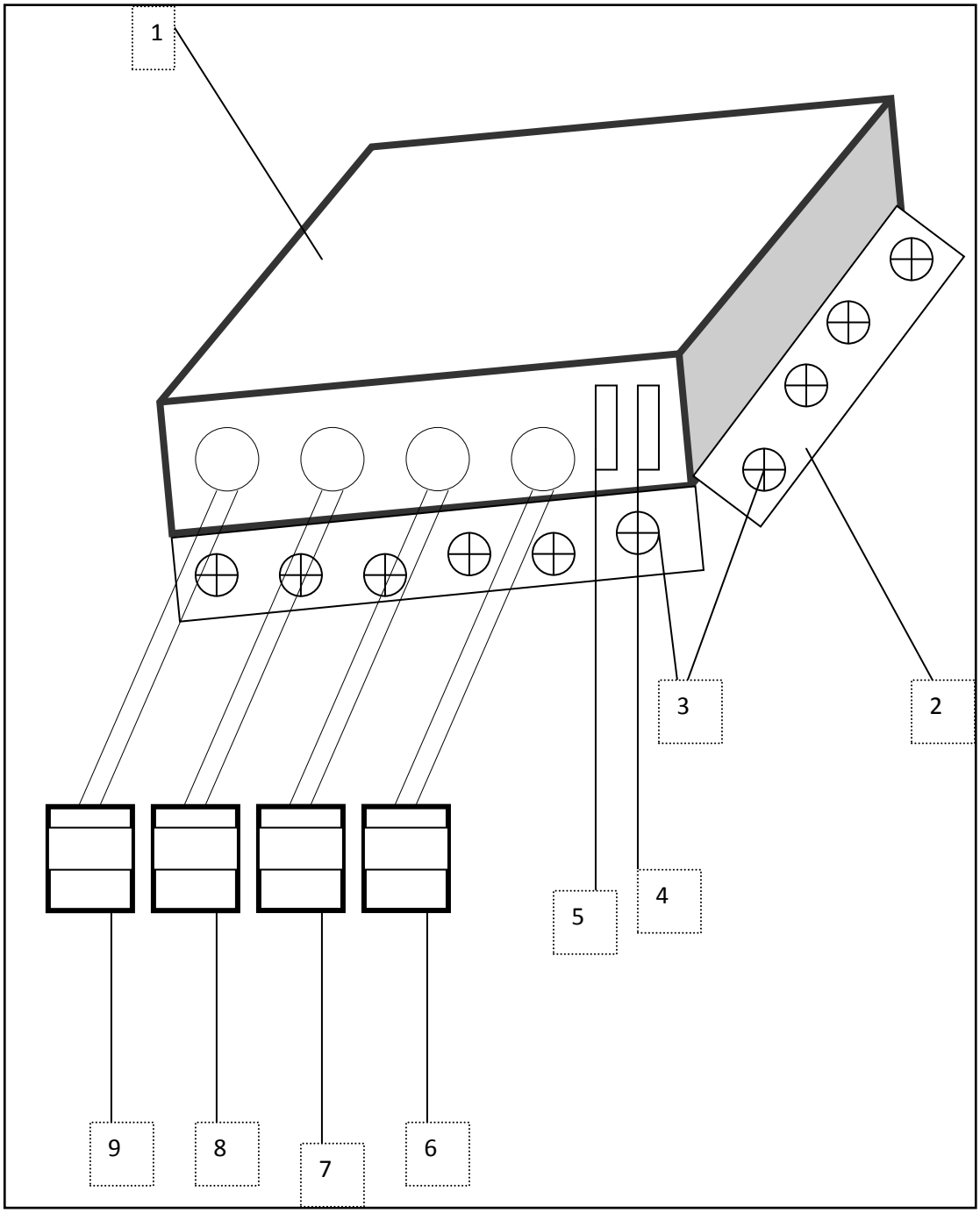


Figure 5.1 Box of the device

5.2 DESCRIPSION

5.2.1 BACKGROUND

The device is a new application using the same technologies of the GSM System and Signaling System # 7 with some amendment and addition in each system to get the target device.

In GSM System we will benefit from the tower, exchange and data base (HLR & VLR), with some amendment in the dealing strategies for the incoming massages and data into the exchange and tower.

In Signal System # 7, we will improve the format of some out going device's massages to get full data which will inform us about the location of the vehicle.

This devise will allow the Security Department to locate the place and direction of vehicle which has fixed it (where it should be fixed in new manufactured vehicles) also it will allow the owner to start, switch off, open, lock, break down and display the location of the vehicle on the electronic map which is fixed inside it.

5.2.2 GENERAL DESCRIPTION

By studying the technology of the Global System Mobile (GSM) and the Signaling System # 7, and by reviewing the applications which is improved and used by the previous systems, we observe that this device used the same technology where it is considered as a new application. So this device should offer big advantage for Security Department, Telecom Company and the vehicle's owners by knowing the location of the vehicles at any time control it remotely and prevent stealing the vehicle.

Therefore, this device will do the same job which is done by cellular phone with some amendment; where the cellular phone sending the location of itself inside the network in a "location update" massage by specify the (location area identification LAI)-it is a place of a group of towers related to base station controller (BSC)- and by measuring the time advance-it is the time which guarantee that the RBS will receive the data in the specific time slot without any interference with the data of the previous and next channel. Then, the cellular phone will send this data with all other data to the related (RBS) which will use some of this data and pass the others to the mobile switching center (MSC) and to the data base (HLR). So the location of the cellular phone will be known if there is any call.

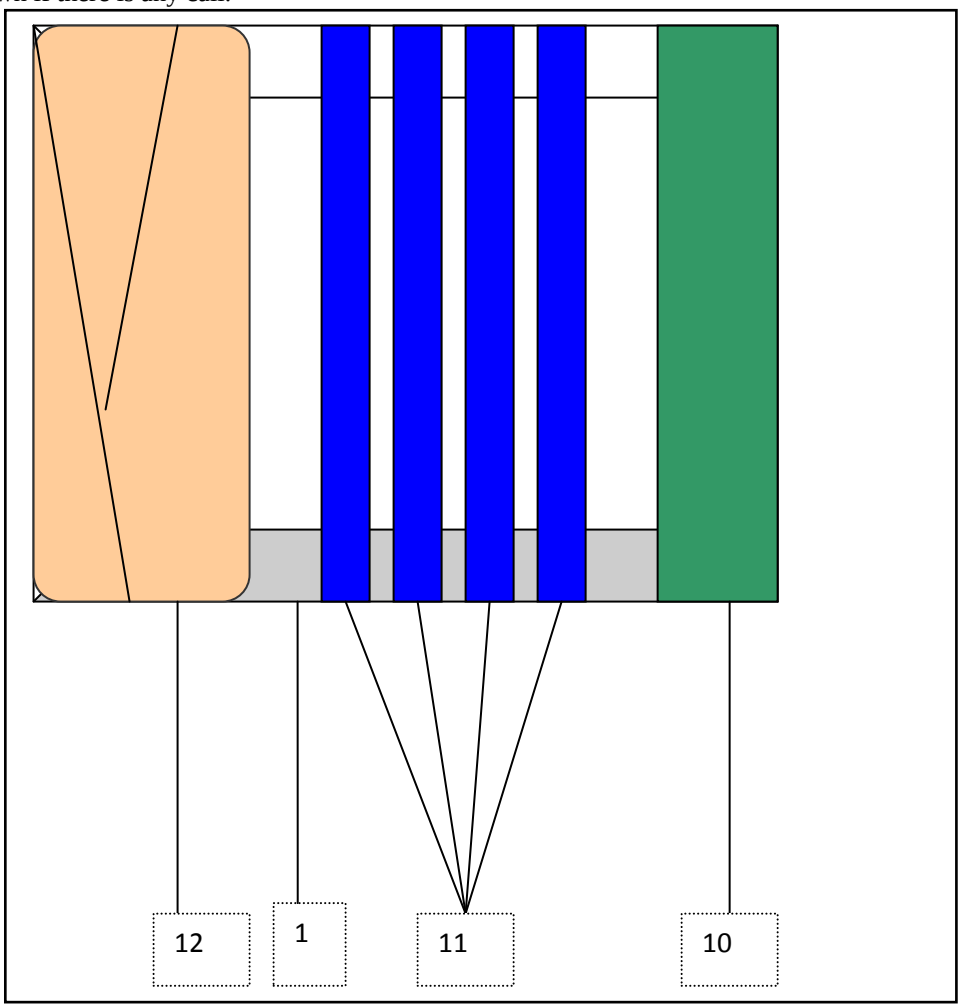


Figure 5.2 horizontal section for box devices

In this device we will specify the cell group identification (CGI) instead of location are identification (LAI) and we will send the time advance with the previous information in new massage called "location information" through the related (RBS) toward the exchange and the date base (HLR) where it will be restored. So when we connect the terminal to the base station and after we do some calculation we will know the tower which serves nearby the vehicle and the distance between the tower and the vehicle.

One of the targets of this device is to prevent stealing vehicles by programming the device to send an invocation massage to the data base and to the owner incase of up normal start up or incase of carry it by truck.Another target is to enable the owner to start, switch off, open, lock and break down the electrical circuit of the vehicle by using any cellular phone to send a normal SMS (short massage service) contains the pass word and the order.Another target is to offer the information of the location and direction of the vehicle to be used by security department to follow up the wanted, and display the location of the vehicle on the electronic map which is fixed inside the vehicle to be used by the owner.

Another target is to open for new cheap applications to reduce the accident and to help the police's observation center; for example, to program the device to send a message to the police's observation center in case of faster driver, also in case of accident to request the ambulance.[4][5][6][7][8][9]

5.2.3 Description of Figure

In progress to clarify the device functions and features, we will introduce for a details section by explain and describe the figure.

Figure 5.1 represents the device box, where the numbers describe as following:

1. External box device.
2. Sectional part for fixing.
3. Screw.
4. Vehicle's negative wire connection (in)
5. Vehicle's negative wire connection (out)

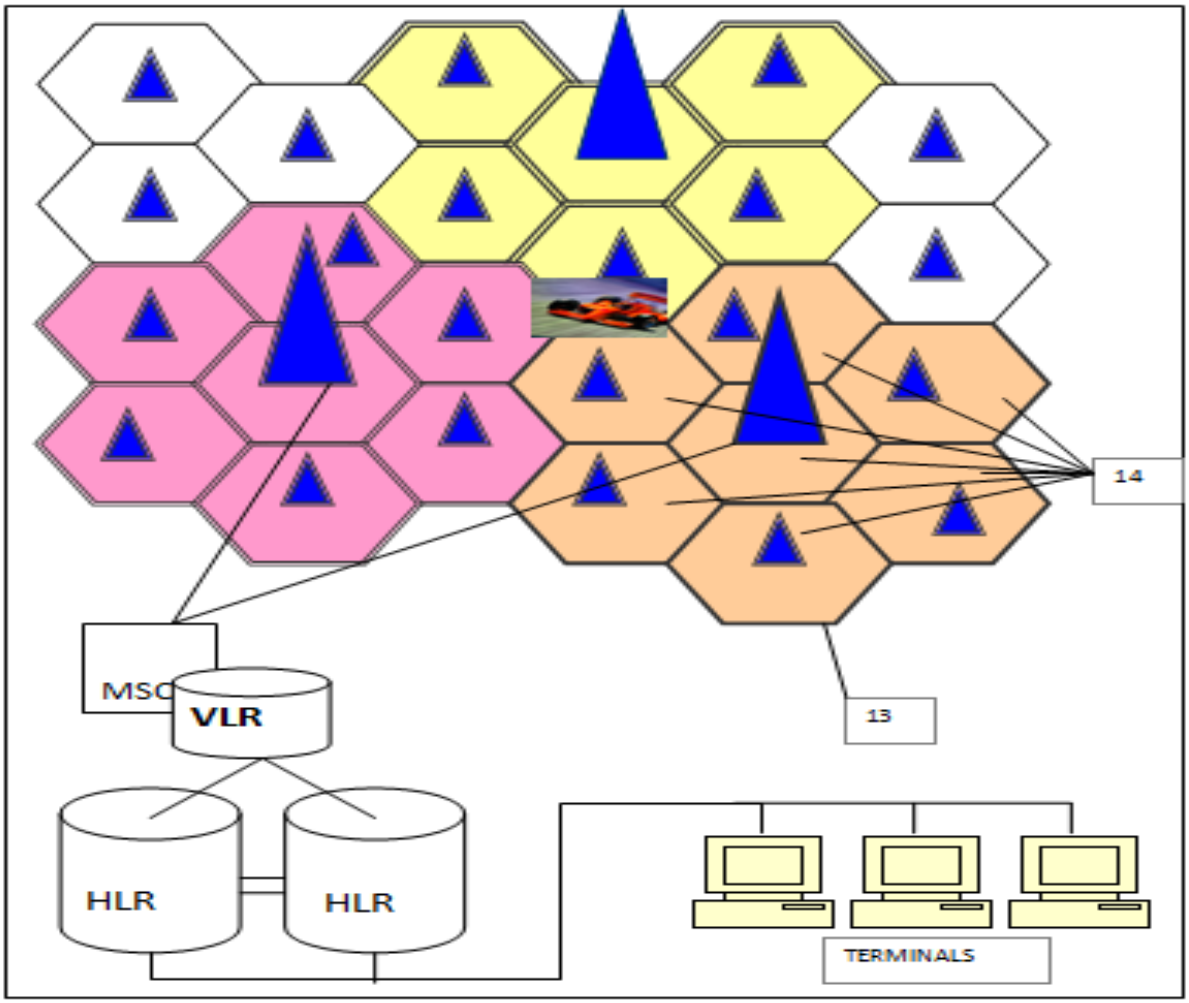


Figure 5.3 simple GSM network

6. Battery charging connection wire.
7. Display screen connection wire.
8. Vehicle's start up switch connection wire.
9. Vehicle's doors lock connection wire.

Figure 5.2 represents the horizontal section for the box device, where the numbers describe as following:

10. Electronic circuit which is use to breakdown the negative cable.
11. For battery
12. The device which will do the same job of cellular phone.

Figure 5.3 represents simple GSM network, where the numbers describe as following:

13. Cell, where each cell include tower (RBS) and called by (CGI) –Cell Group Identification- where it is represent as following: Mobile Country Code (MCC) + Mobile Network Code (MNC) + Location Area Code (LAC) +Cell Identification (CI). i.e. -CGI=MCC+MNC+LAC+CI.
14. Set of Cell serve by same (BSC) - Base Station Controller- , where it is called as (LAI) –Location Area Identification- and represent by following: Mobile Country Code (MCC) + Mobile Network Code (MNC) + Location Area Code (LAC), i.e. LAI=MCC+MNC+LAC.
15. Terminals (to accesses the HLR)

Details Description

By view the previous figures I will describe the specific and feature for the remote control observer device.

The device is consisting of three main parts- where we must prepare each one alone then we can join it all to get the remote control observer device work on- as following: the main device box which will be fixed in the vehicle –this device will do the same job of the cellular phone with some adding and amending which will be describe later on this section.

Correction for the operation program of the towers (RBS & BSC) ,Switching (MSC) , and Data Base (HLR &VLR) , also connection of a special Terminals to the Data Base (HLR &VLR), where this Terminals supporting by special data base and program for calculation and counting as will be describe later on this section.Display screen –fixed in the vehicle- to view the electronic map for different cities.

To describe the details of the device, we can say that this device is consisting of a closed box (1) include a similar cellular phone device with the following deferent's:There is no keyboard and display screen.

the different program and procedure is as following: Location Information Message instead of Location Update Message, where the data of the Location Information Message will include the CGI –Cell Group Identification- and the Time Advance, also this message will be sent with moving of the vehicle , with MSC request and every 15 minuets in case of no moving for the vehicle. Adding of some logarithm as following - where it will be selection- :Comparing logarithm, to compare the password which will be sent by SMS Order Message with the saved password. Applying logarithm, to apply the Order which will be sent by SMS Order Message; for example; break down the negative cable of the vehicle.

Generation logarithm, to generate an invocation massage incase of 15 days remaining of the battery charging , incase of trail for removing the remote control observer device out of the vehicle, incase of up normal start up and incase of carry the vehicle by truck. Repeater logarithm, to repeat sending the Location Information message to twice; to the related tower and to the cable which will send it to the display screen.

Intelligent logarithm, to issue order for start up and switch off the vehicle incase of needing to recharge the battery. And it consists of electronic circuit (10) to apply the order; where the negative cable passes through it (4&5); for example if the remote control observer device receiving SMS from the owner to break down the vehicle, and after the comparing logarithm does the compare between the receiving password and saved password and incase of identical password, the device will use the applying logarithm to pass a signal to the electronic circuit to disconnect the negative cable which is pass through. And it consists of four recharging battery slide (each one enough for one week) connecting with the vehicle battery for charging purpose; where it is starting charge with vehicle start up moment, hence it will be enough for one month incase of no charge and if the charging energy is reduce to less than the halve! Then the Generation logarithm will generate an invocation massage daily to the data base (HLR&VLR) and owner.

The owner can send an order by SMS message to activate the Intelligent logarithm which will start up the vehicle till full charge and then to switch it off.The display screen will be connect by cable (7) to the remote control observer device to receive the Location Information message and then to display the location of the vehicle in city on the screen.It is important to fix the remote control observer device in a hidden place inside the vehicle (2), screw it (3) and connected logically with the Generation logarithm, to generate an invocation massage incase of trail for removing it out of the vehicle, so this will inform the police department about all trail if it is fixed officially in the vehicle.Antenna of the remote control observer device will be connecting to the frame of the vehicle.For more understanding between the Towers (RBS &BSC), MSC, Data Base (HLR &VLR)

and the remote control observer device and its program, message, procedure and logarithm, we should do some amendment on it.

All Towers (RBS &BSC), MSC and Data Base (HLR &VLR) will be programmed to sent the CGI instead of the LAI and the Time Advance on the Location Information message from Towers to the Data Base (HLR) directly without opening in the BSC and MSC incase of Location Information request.

Incase of invocation message there is tow type, the first is toward the owner of the vehicle (the mobile phone number of the owner is saved on the device at installation time) where it deals lock like a normal SMS, the second is toward the Data Base (HLR) where it will be pass directly to HLR without opening in the BSC and MSC.Also we will connect the Terminal (15) to the Data Base (HLR) directly to view the data and information of a specific vehicle as it is done for cellular phone, thus data will be analysis and use by special program and then comparing it with the related Data Base to specify the serving Towers and the direction and distance of the vehicle from towers. Also we can store all data for a specific vehicle and for specific time interval for security purpose. Finally there is more available application can be done with this device such as:sending SMS message incase of faster vehicle (this is request to connect the speed counter to the remote control observer device and also to add some logarithm) sending SMS message incase of accident (this is request to connect the device with the air bag system and also to add some logarithm) And so on. Regarding the use and operation of the device is clear by the previous description, and for new installation for the device we need to save the owner mobile phone number and to insert the point code of the HLR to grant that the the message will reach correctly.

VI. CONCLUSIONS

We developed a device here named REMOTE CONTROL OBSERVER. The purpose of this device is to start, switch off, open, lock, break down and display the location of the vehicle on the electronic map which is fixed inside it; also it enables the Security Department to locate the place and direction of vehicle inside the GSM Network. The device is consists of a screen (displays the electronic map), and a box consists of a device similar to the cellular phone (with few differences) , batteries and electronic circuit used to break down the electrical circuit of the vehicle ,where the device is subscribed with the GSM Network.

The main advantage of this device is to use the available technologies and applications with adding and amending some of the programs and tasks for cellular phone and using the data base of the Home Location Register (HLR) and Visitor Location Register (VLR) by connecting a terminal to enable the user to search for any vehicle.

REFERENCES

[1]. P.KUHN , et ali. , Broadband Communications: Convergence of Network Technologies , Kluwer Accademic Publishers , Boston , Massachusetts , 1999.
[2]. T. Russell , Signalling System # 7,Mc Graw Hill , New York , 2000.
[3]. DDI R. MODARRESSI, MEMBER, IEEE, AND RONALD A. SKOOG, MEMBER, IEEE , An Overview of Signaling System No. 7, PROCEEDINGS OF THE IEEE, VOL. 80, NO. 4, APRIL 1992.
[4]. Signaling system # 7 by Travis Russel-third edition 2001.
[5]. SS7 and Internet protocol (IP) by Lawrence Harte. July 5,2002 .
[6]. Signaling system 7 basics-2nd edition –May 1-2002.
[7]. SS7 manual for Lucent Company (5ESSswitch).
[8]. SS7 manual for Siemens Company (EWS switch).
[9]. SS7 manual for Ericson Company (AXE switch).