INTEGRATING A BASIC EMULATING NETWORK WITH MOBILE COMMUNICATION INFRASTRUCTURE

Oana FILIP, Marian ALEXANDRU, Dan Nicolae ROBU

Transilvania University of Brasov, Romania
(oana2filip@yahoo.com; marian.alexandru@unitbv.ro; dan.robu@unitbv.ro)

DOI: 10.19062/1842-9238.2017.15.3.4

Abstract: *The continued technological advancement in the telecommunications sector and the continuing need to improve the services provided to subscribers have led to ongoing research to meet the growing demands. For these reasons, in this paper we implemented the testing procedures so as to take into account the feasibility studies in the field. Using both real-world networking equipment and laboratory equipment with advanced emulation and simulation capabilities, the versatility and timeliness of a 2G network have been highlighted. This is possible by integrating and interconnecting the available hardware, which through a firmware approach allowed us to make advanced scenarios that highlight the complexity of such a network. The University Laboratory outperforms the network of a telephone operator in terms of architectural complexity, due to its presence in the architecture of the Tektronix K1297, which provides testing, emulation, and network management features.*

Keywords: *GSM, location update, K1297, emulation, MSC, BSC*

1. INTRODUCTION

In the present paper, the central point will be cellular communication systems, the study being conducted over a Global System for Mobile Communications (GSM) network.

To highlight the impact that various parameters have on the GSM network there has been implemented a location update scenario at the level of the A interface. By implementing this procedure, we made both hardware and software links between the K1297-G20 and the real GSM infrastructure of the laboratory. Since the interface A is between the Base Station Controller (BSC) and the Mobile Switching Center (MSC), which is not available in the lab, the first step in building the location update procedure was to emulate this communication node.

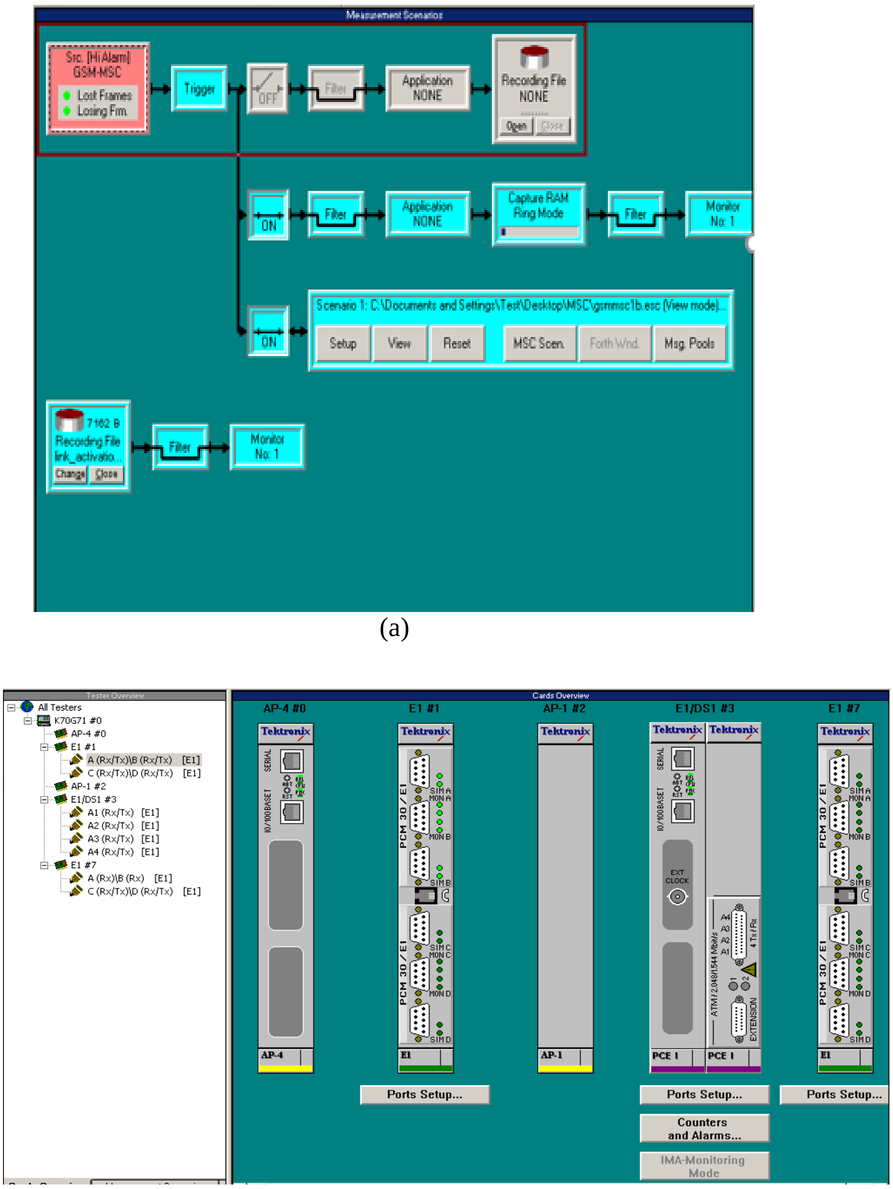
The emulation procedure in the field of telecommunications is a technique that integrates a hardware, software, netware suite to imitate the behavior of the replaced element. The emulated system must behave identically to the replaced node and comply with all the rules that are required for the exchange of information between real equipment and the emulated equipment. In the present paper, the MSC has been emulated at the interface A. At this interface, information is provided to allocate channels, time frames, and handover, location update, paging procedures [5].

2. LOCATION UPDATE PROCEDURE DESCRIPTION

The location update procedure is the starting point of procedures that take place within the GSM network such as Mobile Originating Call or Mobile Terminating Call, as the network must always know the position of the mobile terminal within the network. For this purpose, the mobile station periodically reports its location using the location update procedure.

The location update procedure is done in three distinct situations: when the mobile station is being switched on and wants to become active; when the mobile station is active, but not involved in a telephone conversation and wants to move from one location to another; after a fixed time [4].

The figure bellow is a general overview of the data flow in the K1297-G20 protocol analyzer regarding the implementation of the location update procedure. The structure of the scenario consists of 3 branches with clearly defined roles in the way data is being presented:



(a)

(b)

FIG. 1. (a) General overview of data flow in the emulated MSC (b) Port structure for PRIME E1 card

• *Recording Branch*: At this level, we have the icon where the source of the "Src GSM-MSC" scenario is located from where the SS7 stack can be parameterized in depth, starting at the MTP (Media Transfer Protocol) level 2. In addition, at the level of this branch are presented the options for recording the procedure for future use;

• *Real-time monitoring branch*: This section shows the settings that show the succession of the real-time procedures; Here, the user can filter the messages according to the parameters of interest for each situation;

• *Emulation*: Under this section, a summary of the Mobile Station Controller emulation is presented, from where the user can access the parameters related to MTP Layer 1 going up to the highest levels of the SS7 (Signaling System no. 7) stack, reset the scenario and other options.

The construction of the scenario started from the physical level, as can be seen in Figure 1(b), where we determined which ports to use from the PRIME E1 board of the emulator. For emulation, we opted for the use of port B, which, as specified, is dedicated to emulation procedures within a communications network. To make the connection with the physical BSC, we used a twisted pair cable with 120 Ω impedance, which allows bidirectional data transmission and reception. This link is in fact, an E1 connection.

The step preceding the establishment of the port used was to set up the parameters related to it in accordance with industry standards and recommendations. The type of frame used is CRC-4, in the structure of which the first bit is the one that stores the check sum. This bit specifies whether there is one or more error bits in the last block of incoming data, a block consists of 8 frames.

Since the location update procedure is implemented at signaling level, the scenario has been built based on the 16th channel within the E1 carrier.

Tektronix K1297-G20 provides a set of protocols from which the user can choose. For the scenario in case, we have opted for a stack of protocols built specifically for the A interface, according to GSM Release 97 specifications.

The protocol on which the decoding stack has been built is the BSS (Base Station Subsystem) Application Part (BSSAP), which is a protocol within the SS7 stack used to exchange signaling messages between MSC and BSC, signaling that is compatible with MTP and SCCP (Signaling Connection Control Part) levels [2].

3. CONTROL CENTER CHART AND ACTIONS AVAILABLE AT MTP LAYER 2 LEVEL

Tektronix K1297-G20 provides the user with a representation in the form of an emulation control center diagram where the link between the physical layer LDS Placeholder and the top levels is presented in a layered form.

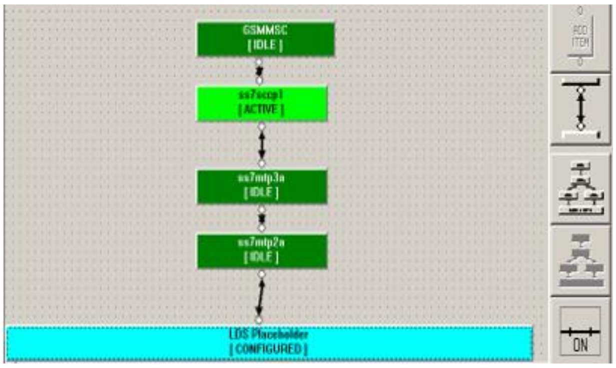
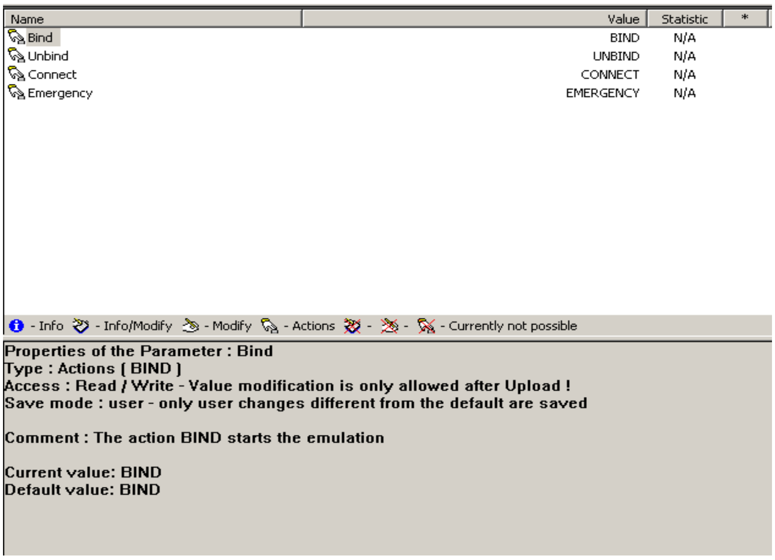


FIG.2. Emulation Control Center and the buttons responsible for activation and deactivation of the scenario

When all these levels are green, the test scenario is loaded in the system and functional, as it can be seen in the figure above.

The equivalent of this diagram is the window view of the scenario parameters, showing both the values of each parameter as well as the actions available for each SS7 stack level, starting from the MTP Layer 2 level.

In the Fig. 3, there are the steps to initiate the simulation at the logical level of the SS7 stack. The steps to be followed are “binding” through which the emulation begins, followed by “connect” which serves as alignment.



Name		Value	Statistic	*
Bind		BIND	N/A	
Unbind		UNBIND	N/A	
Connect		CONNECT	N/A	
Emergency		EMERGENCY	N/A	

Properties of the Parameter : Bind
Type : Actions (BIND)
Access : Read / Write - Value modification is only allowed after Upload !
Save mode : user - only user changes different from the default are saved

Comment : The action BIND starts the emulation

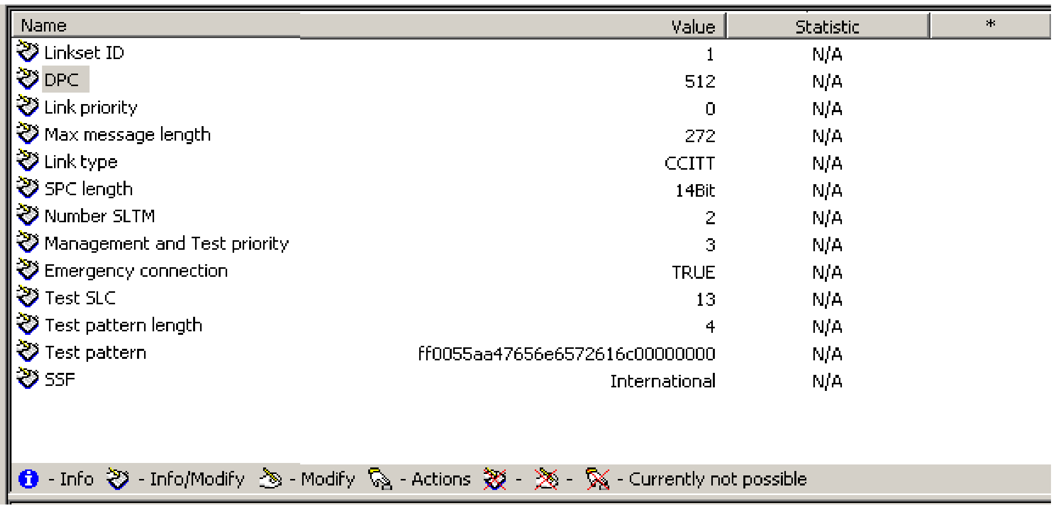
Current value: BIND
Default value: BIND

Fig. 3. Emulation initialization at MTP layer 2 level

4. CONFIGURING THE EMULATED MSC WITH MTP LAYER 3 LEVEL PARAMETERS

Another important step in building the location update scenario is to configure the emulated MSC at the MTP Layer 3 level. Values with the highest importance are the variables called "point codes" because they can identify the two network nodes involved in the testing process. In this case, the emulated MSC is identified by the "point code" with a value of 512, while the BSC in the lab is 256. The length of these codes is in line with the ITU specifications, in this case 14 bits. Within the capture files, these point codes are presented in 4-3-4-3 format, so the MSC will appear with 0-4-0-0, while the BSC will have "point code " 0-2-0-0. In Fig. 4 the configuration table for the emulated MSC it is presented, where the following information is present:

- within the scenario, a single link is used, its identifier is 1 and the MSC Point Code is 512;
- the number of test messages which have to be sent is 2, “Number SLTM”;
- having a single link, the priority of the message does not affect the functionality of the message;
- the Service Switching Function (SSF) parameter plays an important role in the routing of messages; it is important to have the same value at the BSC, as the equipment may have more point codes, the decision to send the message being taken based on the SSF;
- there can be seen two routes, one “inbound” and one “outbound” in order to clarify the direction on the messages within the capture files.



Name	Value	Statistic	*
Linkset ID	1	N/A	
DPC	512	N/A	
Link priority	0	N/A	
Max message length	272	N/A	
Link type	CCITT	N/A	
SPC length	14Bit	N/A	
Number SLTM	2	N/A	
Management and Test priority	3	N/A	
Emergency connection	TRUE	N/A	
Test SLC	13	N/A	
Test pattern length	4	N/A	
Test pattern	ff0055aa47656e6572616c00000000	N/A	
SSF	International	N/A	

FIG. 4. MTP layer 3 parameters for the emulated MSC

5. BUILDING UP THE MESSAGE FLOW

The next step in designing the location update scenario is to model the exchange of messages that takes place between the emulated MSC and the BSC. The messages involved

in this procedure comply with the ITU-T requirements. Fig. 5 shows the succession of messages between "Component Test", which in this case is MSC and "Interface Under Test" represented by BSC seen from the perspective of interface A.

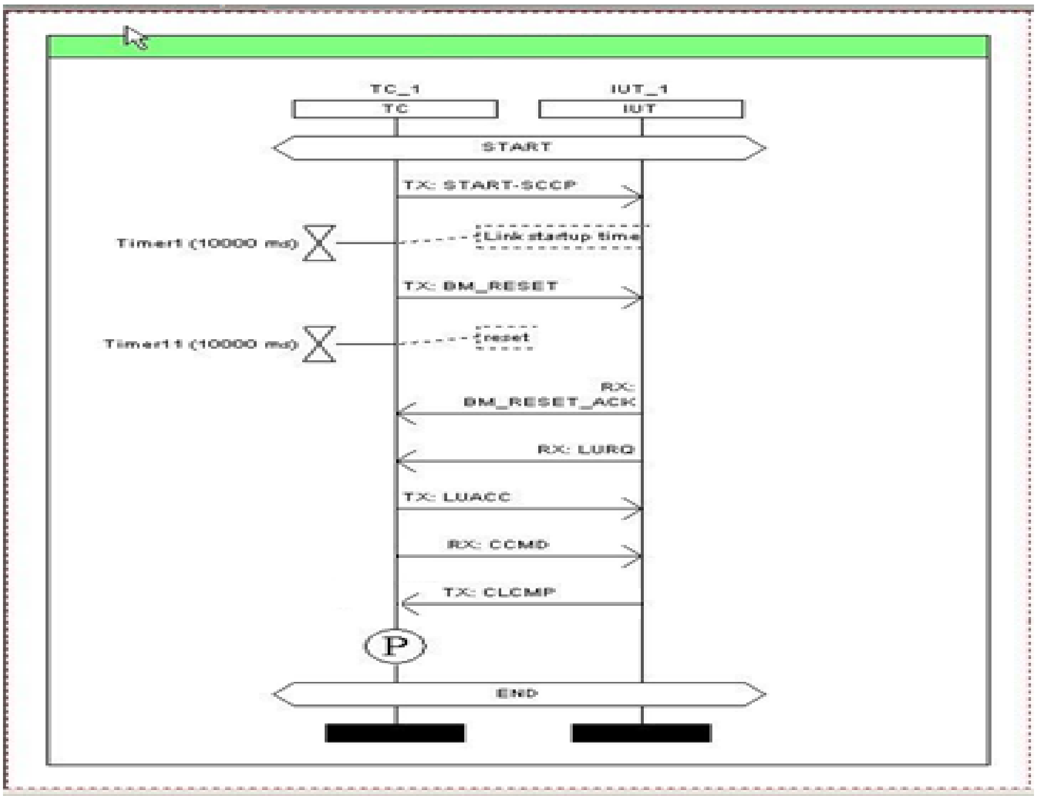


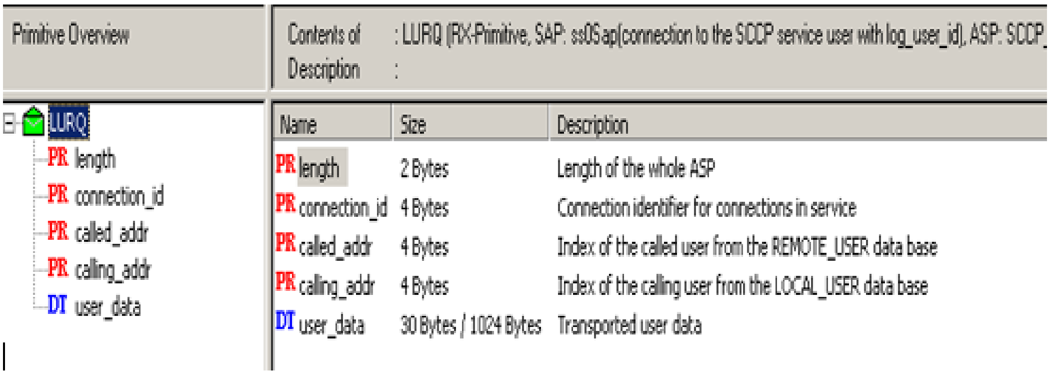
FIG. 5. Message flow between MSC and BSC

a) Since location update is a connection-oriented procedure, the message that initiates the exchange of signaling data between MSC and BSC is "Start SCCP" where MTP Layer 2, MTP Layer 3 and SCCP levels are initialized and a dedicated channel is allocated for the exchange of signaling messages. Also, with this message, the connection between the two network nodes is established.

b) By sending the Tx_BM_Reset message to the MSC, a BSSAP subsystem initialization request identified by ID 254 according to 3GPP specifications is sent, a message that was not included in the message collection available on K1297. For these reasons, the message had to be created using MBS, a proprietary software.

c) Confirmation of receipt of the link reset message is made via the BM_RESET_ACK message that is sent to MSC from BSS, a message that was not included in the message collection available on K1297. Just like in the case of Tx_BM_Reset, the acknowledge message had to be created via MBS.

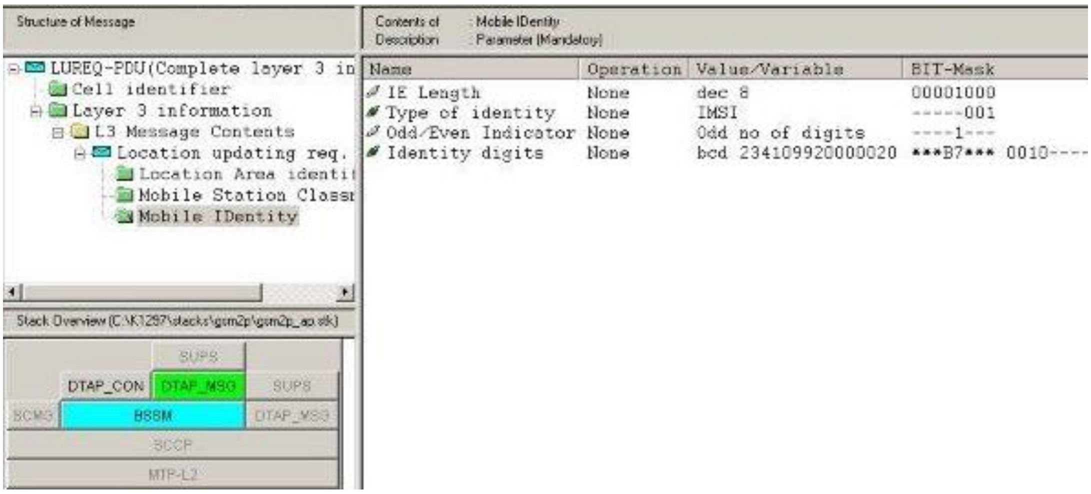
d) The actual location update request message is sent from BSC to MSC. This message includes data about the subscriber who initiates the procedure as well as information about the current location of the mobile station. The message building principle lays on the actual function where the mandatory parameters are presented as well as its primitive which establishes the length and the name of the parameters. These details can be seen in Fig. 6, where the primitive is shown, also in Fig. 7, where the proper function can be observed.



Contents of : LURQ (RX-Primitive, SAP: ss0Sap(connection to the SCCP service user with log_user_id), ASP: SCCP_
Description :

Name	Size	Description
PR length	2 Bytes	Length of the whole ASP
PR connection_id	4 Bytes	Connection identifier for connections in service
PR called_addr	4 Bytes	Index of the called user from the REMOTE_USER data base
PR calling_addr	4 Bytes	Index of the calling user from the LOCAL_USER data base
DT user_data	30 Bytes / 1024 Bytes	Transported user data

FIG. 6. Structure of the primitive for the location update procedure

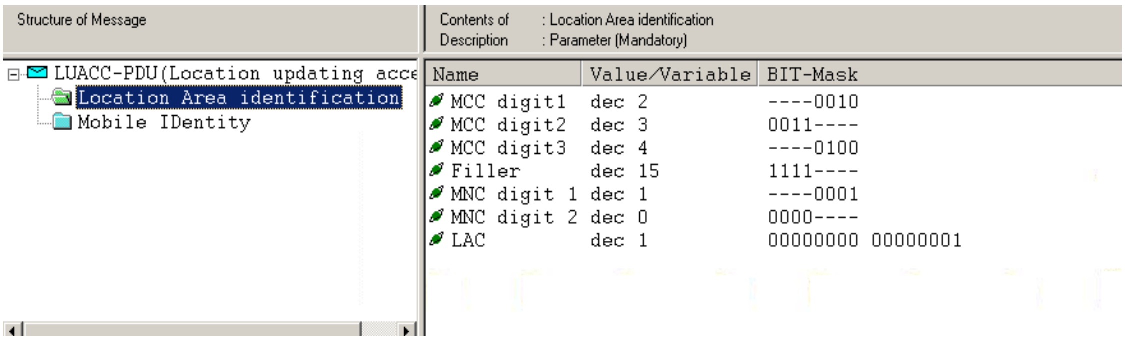


Contents of : Mobile IDentity
Description : Parameter (Mandatory)

Name	Operation	Value/Variable	BIT-Mask
IE Length	None	dec 8	00001000
Type of identity	None	IMSI	-----001
Odd/Even Indicator	None	Odd no of digits	----1---
Identity digits	None	bcd 234109920000020	***B7*** 0010----

FIG. 7. The structure for the function responsible for the location update

e) The emulated MSC is the one that sends the request acceptance message that includes data such as: mobile identity and parameters related to the new location of the mobile station, as it can be seen in Fig. 8.



```
Structure of Message                     Contents of   : Location Area identification
                                         Description   : Parameter (Mandatory)

LUACC-PDU(Location updating acce         Name           Value/Variable  BIT-Mask
  Location Area identification           MCC digit1     dec 2           ----0010
  Mobile IDentity                        MCC digit2     dec 3           0011----
                                         MCC digit3     dec 4           ----0100
                                         Filler         dec 15          1111----
                                         MNC digit 1    dec 1           ----0001
                                         MNC digit 2    dec 0           0000----
                                         LAC            dec 1           00000000 00000001
```

FIG. 8. The parameters passed in the update request acceptance message

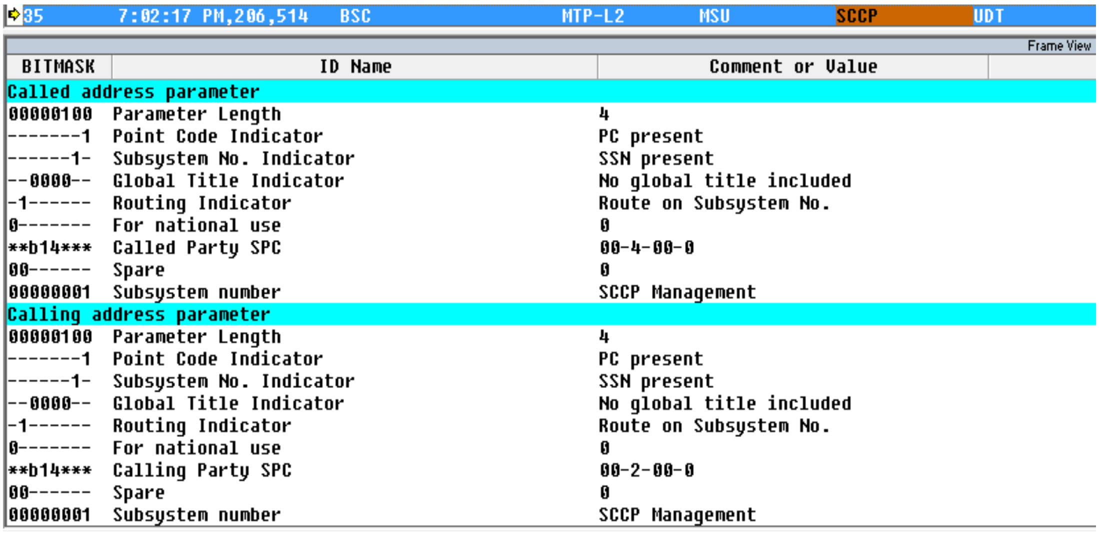
f) The message "Release command RX: CCMD" is sent by the MSC to the BSC requesting the release of the channel on which the signaling messages have been exchanged

g) The last message in the location update procedure is the channel release confirmation message

6. PROTOCOL ANALYSIS. RESULT INTERPRETATION FROM THE CAPTURE FILE

As far as the interpretation of the results is concerned, the manner adopted to pursue this task will follow the methodology used in designing the message exchange between MSC and BSC.

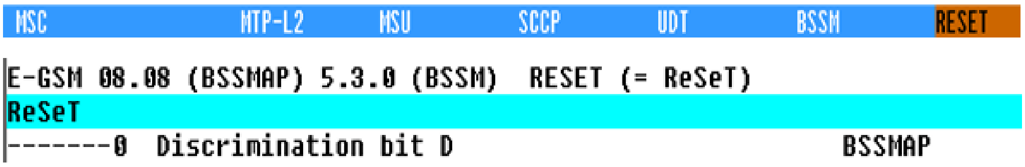
In this regard, once the connection between the two nodes involved in the location update procedure has been established, the request to initiate the SCCP connection is received. The message is split into two parts, one for MSC “Called Party” and the other for BSC “Calling Party”. Each component is identified by MTP Layer 3: calling SPC and called SPC, which are equivalent to "Originating Point Code" and "Destination Point Code" in 4-3-4-3 format.



```
35      7:02:17 PM,206,514   BSC          MTP-L2     MSU      SCCP      UDT
                                                                         Frame View
BITMASK                  ID Name                       Comment or Value
Called address parameter
00000100  Parameter Length                             4
-------1  Point Code Indicator                         PC present
------1-  Subsystem No. Indicator                      SSN present
--0000--  Global Title Indicator                       No global title included
-1------  Routing Indicator                            Route on Subsystem No.
0-------  For national use                             0
**b14***  Called Party SPC                             00-4-00-0
00------  Spare                                        0
00000001  Subsystem number                             SCCP Management
Calling address parameter
00000100  Parameter Length                             4
-------1  Point Code Indicator                         PC present
------1-  Subsystem No. Indicator                      SSN present
--0000--  Global Title Indicator                       No global title included
-1------  Routing Indicator                            Route on Subsystem No.
0-------  For national use                             0
**b14***  Calling Party SPC                            00-2-00-0
00------  Spare                                        0
00000001  Subsystem number                             SCCP Management
```

FIG. 9. SCCP message from the capture

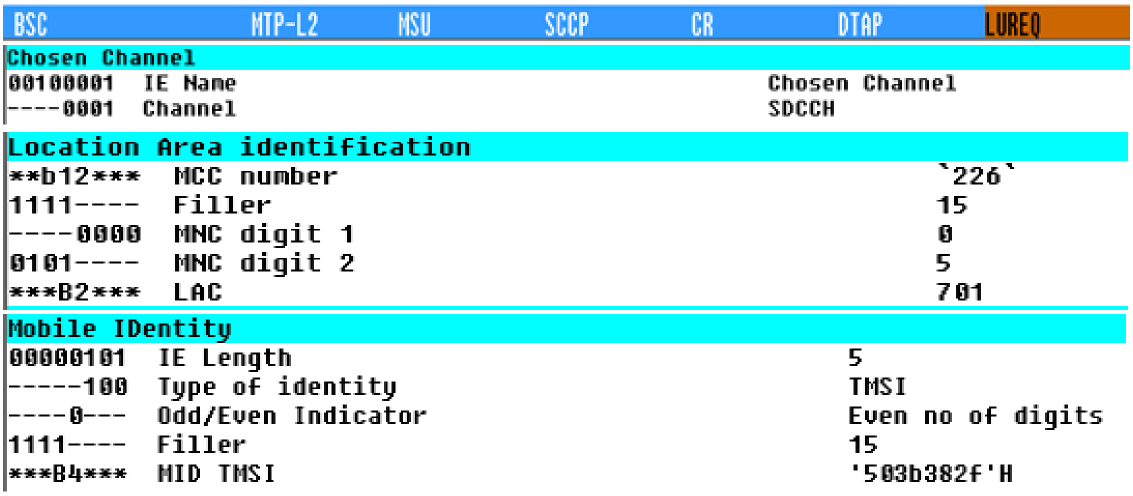
Following the "SCCP" initialization message is the link reset request message which initiates the BSSAP subsystem. In the figure below, there can be seen the BSSAP identifier that is compliant with 3GPP specifications.



```
MSC                 MTP-L2      MSU         SCCP        UDT         BSSM        RESET
E-GSM 08.08 (BSSMAP) 5.3.0 (BSSM)  RESET (= ReSeT)
ReSeT
-------0  Discrimination bit D                                 BSSMAP
```

FIG. 10. BSSAP subsystem identifier

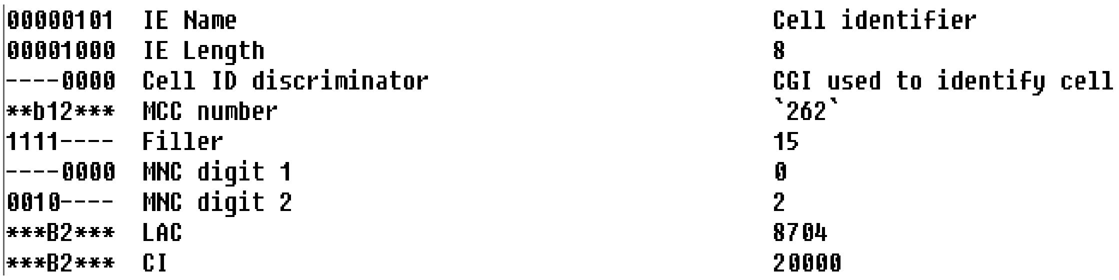
The following message of interest is the location update request where the following parameters can be seen with their values: Country Code of the country of origin (Mobile Country Code) equal to 226, specific for Romania; Mobile Network Code equal to 05, assigned to the Digi Mobil Network; Identifier for subscriber's origin area with the value of 701; The TMSI associated with the mobile station 503b382fH; The channel on which the request is received is “Standalone Dedicated Control Channel”.



```
BSC                 MTP-L2      MSU         SCCP        CR          DTAP        LUREQ
Chosen Channel
00100001  IE Name                                     Chosen Channel
----0001  Channel                                     SDCCH
Location Area identification
**b12***   MCC number                                          `226`
1111----   Filler                                              15
----0000   MNC digit 1                                         0
0101----   MNC digit 2                                         5
***B2***   LAC                                                 701
Mobile IDentity
00000101   IE Length                                  5
-----100   Type of identity                           TMSI
----0---   Odd/Even Indicator                         Even no of digits
1111----   Filler                                     15
***B4***   MID TMSI                                   '503b382f'H
```

FIG. 11. Subscriber data and information about the source location are

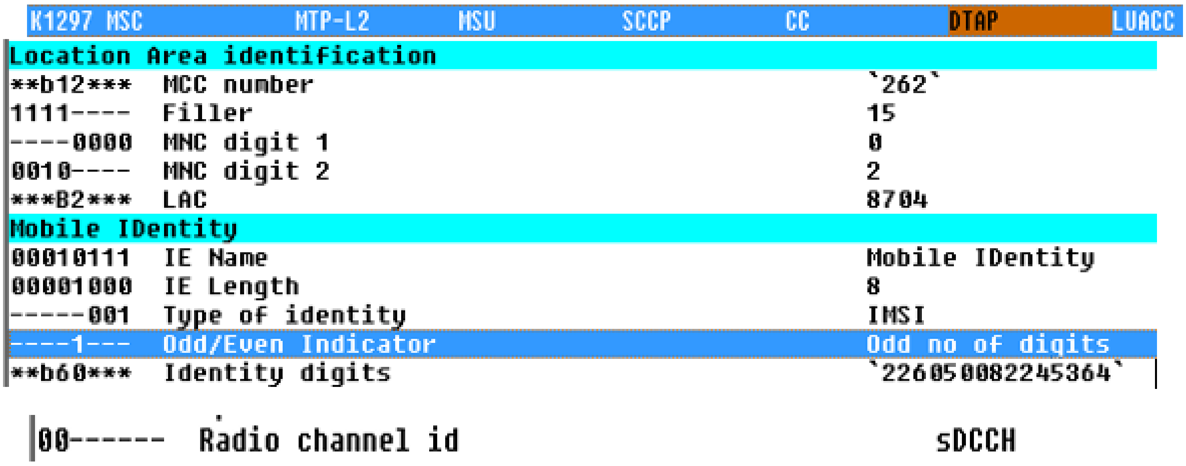
Other values (Fig. 12): The country code where the mobile station is to be authenticated equals to 262, which is the German code, because the database loaded in the laboratory BTS is specific to the Vodafone operator; The operator code in which the subscriber enters the network, namely 02, the code associated with the Vodafone D2 network; "Location Area Code" of the area where the subscriber is to enter, its value is 8704, value assigned to the BSC in our laboratory; The cell identifier in which the MS tries to authenticate the "CI" (Cell Identifier) equal to 20000.



```
00000101  IE Name                                      Cell identifier
00001000  IE Length                                    8
----0000  Cell ID discriminator                        CGI used to identify cell
**b12***  MCC number                                   `262`
1111----  Filler                                       15
----0000  MNC digit 1                                  0
0010----  MNC digit 2                                  2
***B2***  LAC                                          8704
***B2***  CI                                           20000
```

FIG. 12. The data of the new network and the location where the subscriber is about to authenticate

As it has been established in the design of the emulation, it can be noticed the fact that the message for accepting the location update request comes from the MSC. In the response message, there are several data available, among the most important are: IMSI of the subscriber: 226050082245364; the channel via which the messages are being sent SDCCH; Mobile Country Code 262; Mobile Network Code 02; Location Area Code 8704.

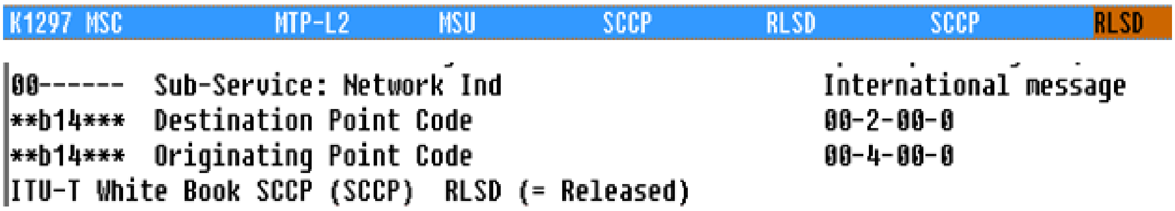


```
K1297 MSC        MTP-L2     MSU      SCCP      CC       DTAP      LUACC
Location Area identification
**b12***   MCC number                                `262`
1111----   Filler                                    15
----0000   MNC digit 1                               0
0010----   MNC digit 2                               2
***B2***   LAC                                       8704
Mobile IDentity
00010111   IE Name                                   Mobile IDentity
00001000   IE Length                                 8
-----001   Type of identity                          IMSI
----1---   Odd/Even Indicator                        Odd no of digits
**b60***   Identity digits                           `226050082245364`

00------   Radio channel id                          sDCCH
```

FIG. 13. Data available in the acknowledge message SCCP

Once the location update request acceptance message has been received, the MSC asks the BSC to release the SDCCH channel through the RLSD message. To determine the direction of the message, we can follow the MTP 3 level parameters, where we can see that the "Originating Point Code" belongs to the MSC, while the "Destination Point Code" is the SPC of the BSC.



```
K1297 MSC        MTP-L2     MSU      SCCP      RLSD      SCCP      RLSD

00------   Sub-Service: Network Ind             International message
**b14***   Destination Point Code               00-2-00-0
**b14***   Originating Point Code               00-4-00-0
ITU-T White Book SCCP (SCCP)  RLSD (= Released)
```

FIG. 14. Data contained in the request for realizing the SDCCH channel

Confirmation of channel release marks the completion of the location update scenario and comes from the BSC, which contains the signaling "point codes" of the MSC and BSC network nodes.

6. CONCLUSIONS

In this paper, we have integrated the mobile communications network available in the laboratory with the emulated core network consisting of the protocol emulator K1297-G20, which is a very high complexity equipment at the upper limit, where the test-emulation function blends with the management level functions. The placement of the emulator and simulator within the communication network is at the level of the Maintenance Administration Operations Center, a level at which we have highlighted the versatility of the equipment by merging the communication process between real-life and emulated equipment.

The main pillar we followed in the development of communication within the GSM network was that of the Signaling System number 7, which dictates the requirements of the testing and emulation process from the lower level, the physical one, climbing to the higher levels, the Mobile Application Part level, at which we designed the location update procedure.

REFERENCES

[1] Peter Stuckmann, *The GSM Evolution: Mobile Packet Data Services*, John Wiley & Sons, 2003;

[2] Eberspächer J., Vögel H-J., Bettstetter Ck., Hartmann C., *Gsm: Architecture, Protocols and Services*, John Wiley & Sons, Chichester, 2009;

[3] Friedhelm Hillebrand (editor): *GSM and UMTS, the creation of Global Mobile Communication*, Wiley 2001;

[4] Marian ALEXANDRU, Gheorghe MORARIU, *Comunicatii Mobile Celulare şi Calcul Mobil. Evolutia de la 3G la 4G*, Editura Universității Transilvania din Brașov 2015, ISBN 978-606-19-0567-6;

[5] Titus BĂLAN, Dan ROBU, Florin SANDU, *Integrarea Sistemelor de Calcul şi Telecomunicaţii*, Editura Universității Transilvania din Brașov, ISBN 978-606-19-0609-3;

[6] Jörg Eberspächer, Hans-Jörg Vögel, Christian Bettstetter, *GSM Switching, Services and Protocols*, Second Edition, Editura John Wiley & Sons, Ltd 2001, ISBN 978-047-149-9039;

[7] Michel Mouly, Marie-Bernadette Pautet, *The GSM System for Mobile Communications, Cell & Sys*, Jan 1, 1992;

[8] Joachim Tisal, *The GSM network: GPRS evolution: one step towards UMTS*, Wiley 2001.