Call Processing and Analyzing SS7 Messages in GSM Switching Network

J. NirmalaDevi, A. Farjana Parveen and R. Nanthini

Abstract--- In this Information and Technology era, the mobile communication becomes mandatory service to one and all. The mobile network is being utilized not for only voice communication but also for day to day business events. Any disturbance or delay in the establishment of call or any other service may lead to huge loss. Hence analysis of faults occurring and immediate solution for the same is very much needed. In this paper, the SS7 signaling messages involved in call establishment and other services involved between various telecommunication network elements is being analyzed using protocol analyzer tool. The failures in call establishments may be due to many reasons, which could not be easily found out. By using this analyzer tool each and every events are monitored and captured with details of messages involved. The signaling units of the MTP layers are captured and analysed. This helps in enhancing the method of trouble shooting and enhances the performances of the switching element. The Message Transfer Part (MTP) is the basic functional layers of this Signaling System 7 (SS7) architecture. MTP is responsible for reliable, unduplicated and in-sequence transport of SS7 messages between communication partners. The call may be failed during the transmission of signaling at any stage.

Keywords--- SS7 Message, Protocol Analyzer, Signaling Unit, MTP Layer

I. INTRODUCTION

INTERNET employs the TCP/IP protocol suite, and wireless networks use the CDMA, TDMA and GSM protocols. For intercommunication of all National and International Telecom Network, SS7 is a communication protocol. SS7 is an ITU-T standard signaling protocol which is suitable for any heterogeneous telecom systems[1]. SS7 signaling establishes faster and effective communication[2]. In this paper, GSM network has been taken for our analysis purpose. Multiple network elements are involved in a mobile call process. MSC is the core element of the network switching system which maintains network connectivity between other MSCs, BSCs connected, SMS center, Internet cloud, PSTN Switches etc.[4]. We are analyzing the SS7 signaling messages between MSC and BSC by capturing the signals involved in a mobile originated call through protocol analyzer. MSC is the main unit which communicates with various databases like HLR, VLR, EIR, AuC for relevant call processing and call routing functions. Like most modern protocols, the SS7 protocol is also a layered protocol which has four MTP layers. We are going to analyze the communication messages on MTP layer 2 which is a data link layer. Message Transfer Part Level 2 (MTP2) resides at Layer 2 in the SS7 protocol stack, it is responsible for the reliable transmission of signalling units over an individual Signalling Link. MTP2 reliability is achieved through retransmission techniques [5]. It is also responsible for flow control, error detection etc. Signaling link status is updated in this MTP layer 2 any interruption in the physical link will also be immediately communicated [5]. All these messages are captured and the analysis is made for effective and immediate solutions.

II. EXISTING SYSTEM

The traffic reports are post analysed for finding the call failure reasons. Sometimes failure of calls can even be reported by the customers. The call failures are rectified by changing or modifying the available connections on trial and error basis. It may not be a fool proof method. Optimization may not be obtained in this method. There is no provision for capturing the call processing messages thereby we cannot ascertain the exact reason of fault. In this technique the fault restoration may be delayed since the real time observation is not possible. This leads to customer dissatisfaction and wastage of time and resource.

III. PROPOSED SYSTEM

The SS7 architecture comprises three signaling points: service switching points (SSPs), signal transfer points (STPs) and service control points (SCPs). Each signaling point is identified by a unique point code that facilitates the routing of signaling messages. Signaling points are connected via signaling links, typically 56 or 64 kbps bi-directional X.25 data links. SSPs are the entry and exit points for SS7 networks, i.e., they strictly originate, terminate and tandem telephone calls. They are analogous to order routers on the Internet and are the primary entry points.

An MSC will be configured as SSP and STP. The HLR and VLR will be configured as SCP. Hence we are using the protocol analyzer for capturing all the signaling messages from a MSC. The messages on all MTP layers including the application layer are captured. The detailed analysis gives upto binary level observations. The various process involved in
establishing a call is captured including the MTP Layer protocols. The duration taken place for each and every event, the elements queried etc. are being captured and available for analysis.

Here we are observing the specific application layer functions on MAP and BSSAP. Signaling connection control part provides additional functions to the MTP to enhance routing capabilities. Mobile application part (MAP) provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. The Mobile Application Part is the application-layer protocol used to access the Home Location Register, Visitor Location Register, Mobile Switching Center, Equipment Identity Register, Authentication Centre, Short message service center and Serving GPRS Support Node (SGSN). Base station system management application part (BSSMAP) supports all of the procedures between the MSC and the BSS that require interpretation and processing of information related to single calls, and resource management. Some of the BSSMAP procedures result in, or are triggered by, Radio Resource (RR) management messages.

A. SS7 Protocol Architecture

**MTP Level 1**

This defines the physical and electrical characteristics of the signaling links of the SS7 network. Signaling links utilize DS–0 channels and carry raw signaling data at a rate of 56 kbps or 64 kbps (64 kbps is the more common implementation).

**MTP Level 2**

The level 2 portion of the message transfer part (MTP Level 2) provides link-layer functionality. It ensures that the two end points of a signaling link can reliably exchange signaling messages. It incorporates such capabilities as error checking, flow control, and sequence checking.

**MTP Level 3**

The level 3 portion of the message transfer part (MTP Level 3) ensures that messages can be delivered between signaling points across the SS7 network regardless of whether they are directly connected. It includes such capabilities as node addressing, routing, alternate routing, and congestion control. It routes SS7 signalling messages to public network nodes by means of Destination Point Codes, and to the appropriate signalling entity within a node by means of a Service Info Octet.

**Figure 1: SS7 Protocol Architecture**

- FISU - Fill-In Signal Unit
  - Provides link error detection detection in the SS7 network. As its name signifies, the FISU packets fill in when no traffic is being sent on the network. This enables you to monitor the link at all times, even when no traffic is on the network. FISUs are constantly transmitted on the signaling links when the LSSU and MSUs are not present. FISUs are sent only between signaling points and are not sent across the SS7 network.

2. **Link Status Signal Unit**

LSSU Provides link status information on the link between two directly connected signaling elements. LSSUs provide link status information over the signaling links between two adjacent signaling endpoints. Use this information to maintain link alignment and to identify a processor outage at the remote endpoint.

3. **Message Signal Unit**

MSU Provides the structure to carry the information messages in the SS7 network. These information messages carry the payload for higher-level messages such as SCCP, TUP, ISUP, and TCAP. The MSU provides the structure for transmitting circuit- and non-circuit based messages in the SS7 network. Use circuit-based messages to set up, manage, and release telephone calls.
IV. RESULTS AND DISCUSSION

1 13:08:44.658 *** Start Capturing ***
2 13:08:46.014 Rx 0.1.1 PH Activate Indicate
3 13:09:13.834 Rx 0.1.1 Raw FISU
4 13:09:13.834 Tx 0.1.1 Raw FISU
5 13:09:36.918 Rx 0.1.1 Raw MSU Testing 100 10449 SLTM
8 13:09:36.934 Tx 0.1.1 Raw MSU Testing 10449 100 SLTA
11 13:09:49.552 Tx 0.1.1 Raw MSU SCCP 10449 100 CR '0F6100'H BSSAP BSSAP CPL_L3_INFO MM CM_SRV_REQ F100010CB
14 13:09:49.608 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '0F6100'H 'C08CFE'H
15 13:09:49.616 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '0F6100'H BSSAP MM ID_REQ
21 13:09:50.248 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 'C08CFE'H BSSAP MM ID_RES 354350008246920
24 13:09:50.728 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 'C08CFE'H BSSAP CC SETUP
27 13:09:50.824 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '0F6100'H BSSAP CC CALL_PROC
30 13:09:50.840 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '0F6100'H ASN_REQ
33 13:09:51.608 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 'C08CFE'H ASN_CPL
36 13:09:51.680 Rx 0.1.1 Raw MSU SCCP 100 10449 UDT BSSAP BSSAP PAGING
39 13:09:52.840 Tx 0.1.1 Raw MSU SCCP 10449 100 CR '106110'H BSSAP BSSAP CPL_L3_INFO RR PAG_RES
42 13:09:52.912 Rx 0.1.1 Raw MSU SCCP 100 10449 CC '106110'H '408DFE'H
43 13:09:52.920 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '106110'H BSSAP CC SETUP
47 13:09:53.544 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 '408DFE'H BSSAP CC CALL_CONF
50 13:09:53.600 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '106110'H ASN_REQ
53 13:09:54.432 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 '408DFE'H ASN_CPL
56 13:09:54.528 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 '408DFE'H BSSAP CC ALERT
59 13:09:54.568 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '0F6100'H BSSAP CC ALERT
62 13:10:12.355 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 '408DFE'H BSSAP CC CONN
65 13:10:12.387 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '106110'H BSSAP CC CONN_ACK
66 13:10:12.395 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 'C08CFE'H BSSAP CC CONN_ACK
70 13:10:12.595 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 'C08CFE'H BSSAP CC CONN_ACK
73 13:10:37.447 Rx 0.1.1 Raw MSU Testing 100 10449 SLTM
76 13:10:37.463 Tx 0.1.1 Raw MSU Testing 10449 100 SLTA
79 13:10:43.800 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 'C08CFE'H BSSAP CC DISC
82 13:10:43.864 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '0F6100'H BSSAP CC REL
83 13:10:43.864 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '106110'H BSSAP CC DISC
87 13:10:44.040 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 'C08CFE'H BSSAP CC RLC
90 13:10:44.064 Tx 0.1.1 Raw MSU SCCP 100 10449 DT1 '408DFE'H BSSAP CC REL
93 13:10:44.080 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '0F6100'H CLR_CMD
96 13:10:44.112 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '106110'H BSSAP CC RLC
97 13:10:44.112 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 'C08CFE'H CLR_CPL
98 13:10:44.120 Rx 0.1.1 Raw MSU SCCP 100 10449 DT1 '106110'H CLR_CPL
104 13:10:44.160 Rx 0.1.1 Raw MSU SCCP 100 10449 RLD '0F6100'H 'C08CFE'H
106 13:10:44.168 Tx 0.1.1 Raw MSU SCCP 10449 100 DT1 '408DFE'H CLR_CPL
110 13:10:44.184 Tx 0.1.1 Raw MSU SCCP 10449 100 RLC 'C08CFE'H '0F6100'H
113 13:10:44.208 Rx 0.1.1 Raw MSU SCCP 100 10449 RLD '106110'H '408DFE'H
116 13:10:44.248 Tx 0.1.1 Raw MSU SCCP 10449 100 RLC '408DFE'H '106110'H
119 13:11:06.106 *** Stop Capturing ***

This is the analysis on various phases involved in a mobile to mobile originated call. The A interface ie., Between MSC...
and BSC is connected to the analyzer and call process is captured.

Various phases on a call setup:
1. Location updation
2. Request for service
3. Authentication
4. Equipment Validation
5. Call setup
6. Call release

A. Location Updation

The user enters the digits and presses the "send" key after all digits have been entered. The MS transmits a service request message to the BSS over the SDCCH. Included in this message is the MS TMSI and Location Area Identification (LAI). The BSS forwards the service request message to the MSC/VLR. BSSAP – Base station subsystem application part is connected by the SCCP – Signaling Connection control protocol by identifying the network id of the sender in the network layer.

B. Authentication

MSC communicates with HLR/AUC for authentication, and after authentication, sends message for ID request.

C. Equipment Validation

ID response is by sending the IMEI and the MSC is communicating with EIR for equipment validation.

D. Request for Service

The Service request message and service accept is communicated after validation of the equipment.

E. Connection Control Call Setup Messages

Request for a traffic channel assignment and as per the command from MSC the BSS allocating the traffic channel to the mobile station. Paging message and paging response communicated. MS is given with alert of ringing. On answer the call connection establishment completed and the switching starts at MSC. The voice path is established and this is informed to MS on SDCCH. Call process information message will be sent to the mobile station. CC CALL_CONF Connection control, call conformation message, CC CONN_ACK connection control, call connection acknowledgement message. Till the conversation ends, there is no further signaling communication between BSC and MSC on BSSAP. If any handover takes place between two BTS, then once again the BSSAP comes and BSC sends request for traffic channel assignment for the new visited BTS.

F. Call Release

MS is sending the release signal to the network when the disconnect (RED) button is pressed. The MSC receives a Release message from BSS to terminate the end-to-end connection. The MSC gives command BSSAP to clear the assignment of traffic channel.

The various signaling units like FISU and MSU are shown here. FISU is Fill in Signaling unit, it is for the testing of the link. If message type is MSU, then SCCP is connecting the corresponding application part for further communication. The Application layers involved, signaling units involved, communication messages exchanged during a call process.

V. Conclusion

The output of captured SS7 signaling messages using Protocol Analyser during a mobile to mobile call set up is given in this paper as a sample. The call observations are made between MSC and one BSC. The same Analyser can be used to for all call setup scenario and for all services between any network elements. The stages of mobility management, service request and service accept etc. are observed. The reason for failure of a call during location updation process may easily be found out by analyzing these first three steps. After acceptance of the service request, the call setup process takes place. The time taken for the allocation of Traffic Channel on Radio Resource management is also observed. The Signaling point code of the connected BSC is displayed, thereby the failure of calls in a particular location be easily be found out. The time taken for clearing of the traffic channel after disconnection of the call is also analysed. The exact reason for the failure is being found out and hence the optimum solution is possible. This may be very much useful during installation of a new network system and also during the maintenance stage for enhanced performance.

REFERENCE