MCS

MCS Lab 4 Report

SAKKA MOHAMAD-MARIO
EL-GHOUL LAYLA
MAHMOUD MIRGHANI ABDELRAHMAN

MCS Lab 4 Report

1. LAB OBJECTIVE

The aim of this lab was to become familiar with the main GSM radio resource parameters and to see how they can be monitored and interpreted using the TEMS software together with a SIM card analysis tool. We replayed several pre-recorded log files, examined information about serving and neighbouring cells, analysed handovers and location updates, and checked which services are supported by the SIM card.

2. VISUALISATION OF GSM NETWORK INFORMATION (LOG_1_1.LOG)

Using TEMS, we replayed the file log_1_1.log. From the "Serving Cell" and "Serving & Neighbouring Cells" windows we identified the main parameters of the current serving cell:

- Cell Identity (CI): 0x2a27
- BSIC: 41
- BCCH ARFCN: 6
- MCC: 226
- MNC: 01
- LAC: 0x2b62 → LAI = (226, 01, 0x2b62)

Several neighbouring cells were also present on ARFCNs 10, 2, 5, 7 and others, all received with lower levels than the serving cell. We then examined the "Mode Reports" window. When the mobile is idle, TEMS shows only IDLE REPORTs, which contain parameters related to the BCCH carrier. When the mobile is in a call, TEMS displays DEDICATED REPORTs, which also include information about the traffic channel such as RxLev, RxQual, Time Advance (TA), transmit power and neighbour cell levels.

We also used the menu File → Define Cell Names in TEMS to assign descriptive names (Cel_start, Cel_1, Cel_2, Cel_3, Cel_4, Cel_end) to the cells corresponding to the BSIC/ARFCN combinations observed in log_1_1.log. The configuration was saved in a .cel file so the same naming can be reused when replaying the logs.

ANSWERS TO QUESTIONS

Q1. WHAT IS THE VALUE OF THE LAI CODE OF THE LOCATION AREA IN WHICH THE FILE RECORDING WAS DONE?

From the Serving Cell window we read MCC = 226, MNC = 01 and LAC = 0x2b62. Therefore, the Location Area Identity for the area where the recording was made is LAI = (226, 01, 0x2b62).

Q2. DURING FILE RUNNING THE MNC PARAMETER MAY CHANGE. EXPLAIN THIS PHENOMENON.

The Mobile Network Code may change if the mobile reselects or hands over to a cell belonging to another PLMN (for example, a roaming partner network). This can happen close to coverage borders between operators or when the user manually selects a different network. In such cases TEMS shows a different MNC corresponding to the new network.

Q3. DEFINE AND EXPLAIN THE FUNCTIONING OF THE TIME ADVANCE (TA) PARAMETER IN GSM.

Time Advance is a value sent by the base station to the mobile station so that the mobile shifts its uplink bursts in time. The goal is that bursts from different mobiles arrive correctly aligned in their timeslots at the BTS and do not overlap. TA is directly related to the distance between the MS and the BTS (one TA step corresponds to roughly 550–550 m). As the distance changes, the network updates the TA value accordingly.

3. OPERATION ON THE MS (SIM CARD) – SIM_CARD.EXE

Using the sim_card.exe application we read several fields from the SIM card of the monitored mobile. The relevant values for this lab are:

- Access control: 00 04
- SIM service table: cf 3c (bit mask describing allocated and active SIM services)
- LAI (MCC / MNC / LAC): 208 / 01 / 1902
- T3212 value: 10
- Updating status: 0
- Preferred PLMN list: 26201, 22201, ...

ANSWERS TO QUESTIONS

Q1. IS IT POSSIBLE TO ACTIVATE THE PIN CODE AND TO STORE SHORT MESSAGES IN THE SIM? WHICH OF THESE SERVICES ARE ALLOCATED AND/OR ACTIVE?

By decoding the SIM service table with the program, we see that both the PIN management service and the SMS storage service are available. They are marked as allocated and active, so for this SIM it is possible to activate a PIN code and to store SMS directly on the SIM card.

Q2. CAN INFORMATION RELATED TO CHARGING/FEES BE VISUALISED USING THIS SIM?

The SIM service corresponding to charging information (Advice of Charge) is not active in the SIM service table. Therefore, this SIM does not allow the phone to display detailed charging information based on SIM-stored data; billing information is handled only by the network/operator.

Q3. WITH THIS SIM, CAN A CERTAIN NETWORK BE SELECTED FROM A LIST OF AGREED NETWORKS?

Yes. The SIM contains a PLMN selector list with entries such as 26201 and 22201, and the corresponding service is active in the SIM service table. As a result, the handset can rely on a list of preferred or agreed networks when it performs automatic or manual network selection.

Q4. DETERMINE IF THE LOCATION OF THE MS WAS UPDATED.

In sim_card.exe the field “Updating status” has the value 0, which indicates the state “location updated”. The current location of the mobile station is therefore correctly stored in the VLR.

Q5. DETERMINE IF THE MONITORED MOBILE NETWORK USES PERIODICAL UPDATING.

The parameter T3212 is set to 10, which is different from the value that would disable periodic location updating. This shows that the network uses periodic updating. T3212 = 10 means that the mobile must perform a periodic location update every 10 basic timer units (10 × 6 minutes ≈ 1 hour).

Q6. EXPLAIN THE IMPLICATIONS OF SETTING T3212 TO THE MINIMUM VS. MAXIMUM POSSIBLE VALUE.

If T3212 is configured to a very small value, mobiles have to perform periodic location updates more often. This increases signalling in the network and drains the battery faster, but the location information stored in the VLR is more accurate and paging can be restricted to smaller areas. If T3212 is set to a very large value, updates are performed less frequently, which reduces signalling and power consumption but makes the subscriber's stored location less precise, forcing the network to page over larger areas.

4. PARAMETERS OF THE GSM RADIO INTERFACE (GRAPHICAL PRESENTATION)

For this part we replayed log_21.log and used the "Graphical Presentation" window. From the "Serving Cell" window, the current cell parameters were:

- CI = 0x28ca
- BSIC = 72
- BCCH ARFCN = 3
- MCC = 226
- MNC = 01
- LAC = 0x2b5d

Using cursors in the Graphical Presentation, we selected several time instants and read the corresponding radio parameters. The values are summarised below.

TABLE 8 – SAMPLES FROM LOG_21.LOG (SERVING CELL ARFCN 3 / BSIC 72)

Time [hh:mm:ss]	RxLev [dBm]	RxQual	TA	TxPwr	Nearest neighbour level [dBm]
19:24:44.03	-66	0	1	5	-81
19:24:48.35	-67	0	1	5	-81
19:25:06.09	-66	0	1	7	-80
19:25:19.05	-66	0	1	6	-81
19:25:35.39	-66	0	1	5	-81

For all selected instants the serving cell remained ARFCN 3 / BSIC 72 with RxLev of about −66…−67 dBm, RxQual = 0 and TA = 1. Neighbouring cells on ARFCN 12 and 2 had considerably lower levels (typically −80 to −97 dBm).

ANSWERS TO QUESTIONS

Q1. EXPLAIN THE PHYSICAL MEANING OF THE INCREASE AND DECREASE OF TA WHILE RUNNING LOG_2.LOG.

Time Advance is proportional to the distance between the mobile and the serving BTS. An increase in TA indicates that the mobile is moving farther away from the base station so that its uplink bursts must be sent earlier. A decrease in TA means that the mobile is getting closer to the BTS. The TA variations observed in the log therefore reflect the movement of the user inside the cell.

Q2. WHY CAN WE ONLY INCREASE THE MS TRANSMIT POWER FROM TEMS AND NOT DECREASE IT BELOW THE NORMAL VALUE?

In GSM the mobile station's transmit power is mainly controlled by the network through its internal power control algorithm. TEMS can request higher transmit power (within the allowed range) to test worst-case conditions, but it cannot force the mobile to transmit at a lower power than requested by the BTS. Forcing a lower power could break the connection or make the measurements unrepresentative.

5. HANDOVER IN GSM (LOG_2.LOG AND LOG_23.LOG)

In this part we examined several handover events. For log_2.log we focused on the handover around t = 09:23:49.85, when the serving frequency changed from ARFCN 6 to ARFCN 10. In log_23.log we analysed a sequence of handovers between cells on ARFCN 82, 106, 11, 54 and 5, and we monitored the Time Advance evolution using a set of selected samples.

For the event at approximately t = 09:23:48.90 (before the handover in log_2.log), the serving cell was ARFCN 6 / BSIC 41 with RxLev around −69 dBm and RxQual 0, while the first neighbour on ARFCN 10 had a slightly better level (around −66 dBm). After the handover (t ≈ 09:23:50.34), the serving cell became ARFCN 10 / BSIC 41 with RxLev around −76 dBm and RxQual 0.

TABLE 9 – PARAMETERS BEFORE AND AFTER HANDOVER AT 09:23:49.85 (LOG_2.LOG)

Moment	Serving ARFCN	Serving RxLev [dBm]	Serving RxQual	Neighbour 1 (ARFCN, level) / Neighbour 2 (ARFCN, level)
09:23:48.90 (before HO)	6	-69	0	10, -66 dBm / 6, -73 dBm
09:23:50.34 (after HO)	10	-76	0	6, -71 dBm / 10, -73 dBm

From log_23.log we noted in particular the following time instants and handovers between different ARFCNs.

TABLE 10 – ARFCN AND QUALITY FOR SELECTED MOMENTS (LOG_23.LOG)

Time	Serving ARFCN	RxQual
19:42:35.03	82	6
19:43:01.20	106	0
19:44:32.23	106	7
19:44:33.68	54	0
19:44:38.31	5	7

Using the TA values from 19:44:38.31 to 19:46:10.52 (TA fluctuating between 18 and 19 and then dropping to 9), we sketched an approximate trajectory of the mobile relative to the base station.

TABLE 11 – TIME ADVANCE EVOLUTION BETWEEN 19:44 AND 19:46 (LOG_23.LOG)

Time	TA value
19:44:38.31	18
19:44:39.75	17
19:44:42.63	18
19:45:06.62	19
19:45:17.67	18
19:46:10.52	9

ANSWERS TO QUESTIONS

Q1. WHAT MAY CAUSE THE HANDOVER AT T = 09:23:49.85 IN LOG_2.LOG?

Just before the handover the neighbour cell on ARFCN 10 provided a stronger signal than the serving cell on ARFCN 6. To maintain good radio conditions, the network transferred the call to the neighbour with the better level. The handover was therefore triggered because the neighbour cell offered more favourable radio conditions.

Q2. AFTER THIS HANDOVER THE CELL IDENTITY IS UNCHANGED. EXPLAIN THIS PHENOMENON.

The handover from ARFCN 6 to ARFCN 10 takes place between two carriers belonging to the same logical cell. Only the radio frequency (ARFCN) is changed; the cell identity (CI) remains the same. This is an intra-cell handover between different carriers of the same BTS.

Q3. AT T = 09:24:26.44 (LOG_2.LOG) ARFCN CHANGES FROM 10 BACK TO 6 WITHOUT TEMS SIGNALLING A HANDOVER. WHY?

This change corresponds to a frequency change within the same cell (for example due to frequency hopping or a change of traffic channel) rather than a change of cell. Because the cell identity does not change, TEMS does not mark this event as a separate handover.

Q4. WHAT IS THE REASON FOR THE HANDOVER AT T = 19:46:10.52 IN LOG_23.LOG?

Just before this time, the serving cell on ARFCN 5 had a very low received level (around −103 dBm) and rather poor quality (RxQual about 5), with TA ≈ 18, while some neighbour cells had better levels. To avoid a call drop, the network handed the call over to another cell (on ARFCN 54/106) that provided improved level and/or quality.

Q5. WHAT IS THE REASON FOR THE HANDOVER AT T = 19:44:33.68 IN LOG_23.LOG?

Immediately before 19:44:33.68, the serving cell on ARFCN 106 showed very poor quality (RxQual ≈ 7), even though the received level was not extremely low. After the handover to ARFCN 54, RxQual drops to 0 and the level improves slightly. This indicates that the handover was mainly triggered by poor quality (high bit error rate/interference) on the original cell.

Q6. AFTER THE HANDOVER AT T = 19:44:38.31 (LOG_23.LOG) THE QUALITY BECOMES MUCH WORSE, EVEN THOUGH THE POWER IS NOT VERY LOW. WHY WAS THIS TRANSFER STILL PERFORMED?

The handover at 19:44:38.31 moves the call from ARFCN 54 to ARFCN 5. On the new cell the TA jumps to about 18 and the quality degrades (RxQual ≈ 7). The main reason for this transfer is related to coverage and distance: the mobile is leaving the coverage area of the previous BTS and must be served by the new cell that covers that region, even if local interference temporarily produces worse RxQual. In other words, cell coverage and distance constraints, not just instantaneous quality, drive this handover.

Q7. IN WHAT CATEGORY CAN WE CLASSIFY THE HANDOVERS BETWEEN T = 19:43:01.20 AND T = 19:44:33.68 IN LOG_23.LOG?

All these handovers are hard handovers. In GSM the mobile is connected to only one cell at a time (break-before-make). Thus, even when handovers are initiated due to quality or load, they are still hard handovers, unlike the soft handovers encountered in CDMA/UMTS systems.

6. UPDATING THE LOCATION IN GSM (LOG_24.LOG)

In the last part of the lab we used log_24.log to observe how the location area changes as the mobile moves between different cells.

Before the location area change, the Serving Cell window showed:
• CI = 0x0029, BSIC = 44, BCCH ARFCN = 93
• MCC = 655, MNC = 10, LAC = 0x0066
with RxLev ≈ −73 dBm, RxQual 0 and TA = 1.

After moving to the new area, the serving cell became:
• CI = 0x2761, BSIC = 00, BCCH ARFCN = 5
• MCC = 655, MNC = 01, LAC = 0x008d.

TABLE 12 – LOCATION AREAS IN LOG_24.LOG

Location area	MCC	MNC	LAC (hex)	BCCH ARFCN	RxLev [dBm]	RxQual
LA 1 (before change)	655	10	0x0066	93	-73	0
LA 2 (after change)	655	01	0x008d	5	not clearly read	not clearly read

ANSWERS TO QUESTIONS

Q1. EXPLAIN THE ADVANTAGES OF USING LOCATION AREAS FROM THE POINT OF VIEW OF SENDING PAGING MESSAGES.

The network does not have to page a mobile station in all cells of the entire MSC area. It sends paging messages only within the location area where the subscriber is currently registered. This significantly reduces signalling load in the radio network and speeds up call setup, while still allowing the network to find the user.

Q2. A LOCATION AREA IS CONTROLLED BY:

A location area can include cells belonging to one or more BSCs, but it is associated with only one MSC. Therefore the correct statement is: “one or more BSCs, but only one MSC”.

Q3. WHY, WHEN RUNNING LOG_24.LOG, IS THE CHANGE OF LOCATION AREA NOT SIGNALLED EXACTLY AT THE MOMENT OF THE HANDOVER AT 12:13:06.21?

Handover and location update are distinct procedures. The handover only changes the serving cell in order to maintain the ongoing call, whereas the location update procedure refreshes the LAI stored in the VLR and on the SIM. The mobile first performs the radio handover and only afterwards, when it recognises that the new

cell belongs to a different location area, does it initiate a location update. As a result, the change of location area recorded by TEMS does not occur exactly at the same instant as the handover.

7. CONCLUSIONS

In this lab we used TEMS together with a SIM card analysis application to connect the theoretical GSM concepts with practical measurements. We identified serving and neighbouring cells, interpreted RxLev, RxQual, TA and transmit power, and studied the conditions that trigger handovers. We also examined the SIM service table and location updating parameters such as T3212, LAI and the updating status. Overall, the lab provided a clearer picture of how GSM networks manage radio resources and keep track of subscriber locations in real networks.

We used the true (with-earth) relation implemented in trueReflPlan, which internally calls ErthRefC with $\boldsymbol{\varepsilon_r = 15}$ and $\boldsymbol{\sigma = 0.012}$. For $\boldsymbol{d = 1}$ kmat $\boldsymbol{f = 1}$ GHzwith our antenna gains and heights, we supplied a small incidence angle $\boldsymbol{\psi}$(in radians). The function returns a complex-aware expression; following the lab demo, we report the losses as $-|\boldsymbol{trueReflPlan}|$ in dB. The result is: $\boldsymbol{-91.55\ dB}$