

## **Abstract**

The Location Updating procedure occurs when a Mobile Station \User Equipment is switched on in Mobile Switching Center service area or when an idle Mobile Station moves to a new Mobile Switching Center service area or MSC. Location Update can also occur prior to a call set-up. The Location update signaling message coming from the mobile station holds useful information. We can use this information to build a data base that can contain Brand, Make and Model, Radio Support Capability (GSM 850 /900 / 1800 /1900, GPRS, EDGE, UMTS), Application Support Capability (MMS, Presence, PTT...).

In this research standard SS7 protocol analyzer used to analyze the signaling messages coming from the mobile station to the GSM core network and then applied a code using C++ language to extract the required data such as International Mobile Element Identity “IMEI”, Location Area Code “LAC”, and Cell identity “Cell ID”. That information can be used to build applications that can help Mobile operator and service companies to provide new services.

## التجربة

تبدأ عملية تجديد الموقع عندما يبدأ مستخدم الموبايل بتشغيل جهاز الموبايل جهاز في موقع الم قسم او عندما يتحول / يتحول من موقع الي موقع جديد عندها يقوم جهاز الموبايل بارسال اشارات تحكم الي الم قسم. تحتوى تلك الاشارات على بيانات ومعلومات عن جهاز الموبايل يمكن الاستفادة منها لتكوين قاعده بيانات تحمل الاتي: موديل ونوعه وتقنيه الجهاز "GSM 850 /900 GPRS, EDGE, UMTS" بالاضافه الى نوع الخدمات المتاحة الى الجهاز "رسال نصيه رسال صوت او صوره .

في البحث استخدم SS7 protocol analyzer لتحليل اشارات التحكم ال قادمه من جهاز الموبايل وعرضها في ملف وباستخدام برنامج بلغه ++C تم وضعها فى قاعده بيانات. يمكن لشركات الموبايل وشركات الخدمات الاستفادة من البيانات الموجوده داخل قاعده البيانات لتقديم افضل الخدمات للمشركين.

## ACKNOWLEDGMENTS

*I express sincere appreciation to Dr. Abd Alrasol for his guidance, insight throughout the research, his suggestions and comments. To my wife, Amna, I offer sincere thanks for her unshakable faith in me and her willingness to endure with me the vicissitudes of my endeavors. To my Father and Mother, I thank them for understanding my frequent absences. I also thank my friends in Electronic department for their support and assistants.*

# TABLE OF CONTENTS

<b>ABSTRACT.....</b>	<b>I</b>
التجريدة .....	II
<b>ACKNOWLEDGMENTS.....</b>	<b>III</b>
<b>TABLE OF CONTENTS.....</b>	<b>VI</b>
<b>LIST OF FIGURES.....</b>	<b>VII</b>
<b>LIST OF TABLES.....</b>	<b>VIII</b>
<b>ABBREVIATION LIST.....</b>	<b>IX</b>
<b>CHAPTER 1 INTRODUCTION TO GSM.....</b>	<b>1</b>
1.1 MOBILE TELEPHONY.....	1
1.2 HISTORY OF WIRELESS COMMUNICATION.....	1
1.3 MOBILE STANDARDS.....	2
1.4 GSM HISTORY.....	3
1.5 GSM SPECIFICATIONS.....	4
1.6 GSM PHASES.....	5
1.6.1 Phase 1.....	6
1.6.2 Phase 2.....	7
1.6.3 Phase 2+.....	7
1.7 GSM NETWORK COMPONENTS.....	7
1.7.1 Mobile Switching Center.....	8
1.7.2 Home Location Register.....	9
1.7.3 Visitor Location Register.....	9
1.7.4 Authentincation Center.....	9
1.7.5 Equipment Idententy Register.....	9
1.7.6 Base Station Controller.....	10
1.7.7 Base Transceiver Station .....	10
1.7.8 Operation and Maintenance Center.....	10
1.7.9 Network Management Center.....	10
1.7.10 Mobile Station.....	10
1.8 GSM CEROGRAFICAL NETWORK STRUCTURE .....	11
1.8.1 Cell.....	11
1.8.2 Location Area .....	12

1.8.3	MSC Service Area .....	12
1.8.4	PLMN Service Area .....	12
1.8.5	GSM Service Area.....	13
1.9	GSM FREQUENCY BANDS .....	14
1.9.1	GSM 900.....	14
1.9.2	GSM 1800 .....	14
1.9.3	GSM 1900 .....	15
1.10	EVOLUTION OF THE GSM NETWORK.....	15
<b>CHAPTER 2 TRAFFIC CASES in GSM</b>		<b>16</b>
2.1	MOBILE STATION MODES.....	16
2.2	MS REGISTRATION AND ROAMING.....	17
2.2.1	MS in Ideal Mode.....	17
2.2.2	RR Connection Establishment.....	18
2.2.3	Location Updating, Ttype Normal.....	19
2.2.4	IMSI Detach.....	19
2.2.5	Location Updating Type IMSI Attach .....	20
2.2.6	Location Updating, Ttype periodic registration.....	21
2.2.7	MS Purging.....	23
2.3	CALL FROM MS.....	24
2.4	CALL TO MS.....	26
2.5	INTERNATIONAL CALL.....	29
2.6	DATA CALLS.....	31
2.6.1	Accessing ISDN .....	32
2.6.2	High Speed Circuit Switched Data.....	33
2.6.3	Internet Access.....	34
2.7	HANDOVER.....	34
2.7.1	Intra BSC Handover.....	35
2.7.2	Inter BSC Handover.....	36
2.7.3	Inter MSC Handover.....	37
2.7.4	Intra Cell Handover.....	39
2.7.5	Handover on SDCCH.....	39
2.7.6	Short Speech Interrupts at Handover .....	39
2.7.7	Handover Power Boost.....	39
2.8	SHORT MESSAGE SERVICE.....	40
2.8.1	Mobile Originating SMS.....	40
2.8.2	Mobile Terminated SMS .....	42
2.8.3	Unsuccessful Mobile Terminated SMS deleviry.....	43
2.8.4	Note MS Present.....	44
2.9	SUPPLEMENTARY SERVICES CONTROL.....	44
<b>CHAPTER 3 SIGNALING IN GSM.....</b>		<b>45</b>

3.1	SIGNALING INTRODUCTION.....	45
3.1.1	<i>Access Signaling</i> .....	46
3.1.2	<i>Trunk Signaling</i> .....	46
3.2	CHANNEL ASSOCIATED SIGNALING .....	49
3.3	COMMON CHANNEL SIGNALING.....	49
3.4	OSI REFERENCE MODEL.....	49
3.4.1	<i>Introduction</i> .....	49
3.4.2	<i>OSI Reference Model</i> .....	49
3.4.3	<i>Communication Process</i> .....	50
3.4.4	<i>Description of Layers</i> .....	51
3.5	SIGNALING SYSTEM NO.7.....	52
3.5.1	<i>Introduction</i> .....	52
3.5.2	<i>Characteristics</i> .....	54
3.5.3	<i>User Parts</i> .....	54
3.5.4	<i>OSI Model and SS No.7</i> .....	56
<b>CHAPTER 4 LOCATION UPDATE.....</b>		<b>58</b>
4.1	LOCATION UPDATE TYPES.....	58
4.2	LOCATION UPDATE STEPS .....	58
4.2.1	<i>RR connection establishment</i> .....	58
4.2.2	<i>Service Request</i> .....	59
4.2.3	<i>Authentication</i> .....	59
4.2.4	<i>Ciphering</i> .....	61
4.3	EIR FUNCTIONS.....	62
4.4	UPDATE LOCATION.....	63
4.5	LOCATION UPDATE REJECT.....	65
<b>CHAPTER 5 SS7 TRACE &amp; DATA BASE CODE.....</b>		<b>66</b>
5.1	SS7 TRACE.....	66
5.2	DATA BASE CODE.....	68
<b>CHAPTER 6 CONCLUSION.....</b>		<b>70</b>
<b>REFERENCES.....</b>		<b>73</b>

## LIST OF FIGURES

Figure No.	Figure Title	Page
Figure 1.1	GSM Phases	6
Figure 1.2	GSM Network	8
Figure 1.3	Range of different type of MS	11
Figure 1.4	GSM Cell	11
Figure 1.5	MSC Serving Area	12
Figure 1.6	Relation Between Areas	13
Figure 1.7	View of Sample Network	13
Figure 1.8	GSM Frequency Bands	14
Figure 1.9	GSM data service evolution	15
Figure 2.1	Radio Resources Connection establishment	18
Figure 2.2	Location updating, type normal. MS already registered in VLR	19
Figure 2.3	IMSI Detach	21
Figure 2.4	Location updating, type IMSI attach.	22
Figure 2.5	Location updating, type periodic registration	23
Figure 2.6	Purge MS	24
Figure 2.7	Mobile Originating Call establishment	25
Figure 2.8	Mobile originating call establishment (early assignment)	25
Figure 2.9	Call to MS from PSTN	26
Figure 2.10	Mobile terminating call establishment	27
Figure 2.11	Immediate Assignment on TCH, MO call	28
Figure 2.12	Making an international call today	29
Figure 2.13	Interrogation and routing possibilities in a local exchange	30
Figure 2.14	Mobile terminating data call, through PSTN	31
Figure 2.15	Mobile terminating data call, through ISDN	31
Figure 2.16	Multi slot channel combination on Um for HSCSD	32
Figure 2.17	Intra BSC handover of a call	34
Figure 2.18	Inter BSC handover of a call	35
Figure 2.19	Inter MSC handover of a call	37
Figure 2.20	Basic network architecture for SMS	39
Figure 2.21	Mobile originated short message transfer	40
Figure 2.22	Successful mobile terminated short message transfer	41
Figure 2.23	Short message transfer	42
Figure 2.24	Unsuccessful SMS transfer	42
Figure 2.25	MS present	43
Figure 2.26	Supplementary Services Control for idle MS	44
Figure 3.1	Signaling in Telecommunication Networks	45

Figure 3.2	CCITT R2 Signals	47
Figure 3.3	Simplified Call Setup using the CAS System	48
Figure 3.4	OSI Reference Model	49
Figure 3.5	Schematic Figure of Information Adding in Each Layer	51
Figure 3.6	CCITT SS No. 7 General Structure	53
Figure 3.7	CCITT SS No. 7 Protocols in GSM	55
Figure 3.8	Relationship between OSI and CCITT SS No. 7	57
Figure 4.1	Location updating, RR connection	58
Figure 4.2	Location updating, service request	59
Figure 4.3	Provision of triplets	60
Figure 4.4	Authentication procedure	61
Figure 4.5	Ciphering procedure	62
Figure 4.6	Equipment identification	63
Figure 4.7	Location updating accepted	63
Figure 4.8	Connection release	64
Figure 4.9	SCCP (CO) release	64
Figure 6.1	BSSAP Signaling at Location Updating	76

## LIST OF TABLES

Table No.	Table Title	Page
Table 1.1	Major milestones in the development of wireless communications	1
Table 1.2	The main cellular standards	3
Table 1.3	History of GSM	4
Table 1.4	GSM Recommendations	5
Table 2.1	Key terms	16
Table 6.1	SS7 Output Results	77



## **LIST of ABBREVIATION**

3GPP	3rd Generation Partnership Project
ATM	Asynchronous Transfer Mode
AUC	Authentication Center
BSC	Base Station Controller
BSS	Base Station System
BSSAP	Base Station System Application Part
CAMEL	Customized Applications for Mobile Enhanced Logic
CAS	Channel Associated Signaling
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CDMA	Code Division Multiple Access
DTAP	Direct Transfer Application Part
DTMF	Dual Tone Multi Frequency
EDGE	Enhanced Data rates for the GSM Evolution
EIR	Equipment Identity Register
ETSI	European Telecommunications Standardization Institute
FNR	Flexible Number Register
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile services Switching Center
GPRS	General Packet Radio Services
GSM	Global System for Mobile telecommunication
GSN	GPRS Support Node (GPRS)
HLR	Home Location Register
IMEI	International Mobile Equipment ID
IMSI	International Mobile Subscriber ID
IN	Intelligent Network
INAP	Intelligent Network Application Part
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
ITU	International Telecommunications Union
LAPD	Link Access Procedures for D-channel
MAP	Mobile Applications Part
MS	Mobile Station
MSC	Mobile services Switching Center
PLMN	Public Land Mobile System
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephony Network
SCCP	Signaling Connection Control Part
SGSN	Serving GPRS Support Node

TCAP      Transfer Capabilities Application Part