National Taiwan University
Department of Computer Science
and Information Engineering

GSM Mobility Management

Phone Lin

Ph.D.

Email: plin@csie.ntu.edu.tw

Outlines

- Introduction
- GSM Location Update
- Basic Call Origination and Termination Procedures
- Mobility Databases
- Failure Restoration
- VLR Identification Algorithm
- VLR Overflow Control
- Summary

Introduction

- To exercise location tracking, a mobile service area is partitioned into several Location Areas (LA) or registration areas.
  - **Every LA consists of a group of BTSs.**
- The major task of mobility management is to update the location of an MS when it moves from one LA to another.

Location Update Concept (Registration)

- The location update (registration) procedure is initiated by the MS.
- **Step 1.** The BTs periodically broadcast the corresponding LA addresses to the MSs.
- **Step 2.** When an MS receives an LA address different from the one stored in it memory, it sends a registration message to the network.
- **Note that**
  - **Every VLR maintains the information of a group of LAs. When an MS visits an LA, a temporary record of the MS is created in the VLR to indicate its location (i.e. LA address).**
  - **For every MS, a permanent record is maintained in HLR. The record stores the address of VLR visited by the MS.**

Two Issues of GSM Mobility Databases

⌘ Fault Tolerance.

- If the location database fail, the loss or corruption of location information will seriously degrade the service offered to the subscribers.

⌘ Database Overflow.

- The VLR may overflow if too many users move into the VLR-controlled area in a short period.
- If the VLR is full when a mobile user arrives, the user fails to register in the database, and thus cannot receive cellular service.
- This phenomenon is called **VLR overflow**.

GSM Basic Location Update Procedure

- **Case 1.** Inter-LA Movement
- **Case 2.** Inter-MSC Movement
- **Case 3.** Inter-VLR Movement

GSM Basic Location Update: Inter-LA Movement (1/3)

- The MS moves from LA1 to LA2, where both LAs are connected to the same MSC.
- In GSM 04.08, Nine message are exchanged between the MS and the MSC, and ten messages are exchanged between the MSC and the VLR.
- Four major steps are discussed here.

GSM Basic Location Update: Inter-LA Movement (2/3)

⌘ Step 1.

- A location update request message is sent (MS->BTS->MSC) .

  Location Update Request (Prev. LA, Prev. MSC, Prev. VLR). Note that New MSC = Prev. MSC, New VLR = Prev. VLR

- The MS identifies itself by the **Temporary Mobile Subscriber Identity (TMSI)**, which is an alias for **IMSI**.
- **IMSI (International Mobile Subscriber Identity)** is used to identify the called. IMSI is not known to the User but GSM network.
- TMSI is used to avoid sending the IMSI on the radio path, which is temporary identity is allocated to an MS by the VLR at inter-VLR registration, and can be changed by the VLR.

GSM Basic Location Update: Inter-LA Movement (3/3)

- **Step 2.** The MSC forwards the location update request to the VLR by a TCAP message, MAP_UPDATE_LOCATION_AREA.
  - **This message includes (Address of the MSC, TMSI of MS, Prev. Location Area Identification (LAI), Target LAI, Other Related Information).**
- **Steps 3 and 4.**
  - **Part I. The VLR notices that both LA1 and LA2 belong to the same MSC.**
  - **Part II. The VLR updates the LAI field of the VLR record.**
  - **Part III. The VLR replies an ACK to the MS through the MSC.**

GSM Basic Location Update: Inter-MSC Movement (1/2)

- The two LAs belong to different MSCs of the same VLR.
- **Steps 1 and 2**. The location update request is sent from the MS to the VLR.
- **Step 3.**
  - **Part I. The VLR notices that the Prev. LA and the Target LA belong to MSC1 and MSC2, which are connected to the same VLR, respectively.**
  - **Part II. The VLR updates the LAI and the MSC fields of the VLR record.**
  - **Part IV. The VLR derives the HLR address of the MS from the MS's IMSI stored in the VLR record.**
  - **Part V. The VLR sends the MAP_UPDATE_LOCATION to the HLR.**

(IMSI of MS, Target MSC Address, Target VLR Address, other related information)

GSM Basic Location Update: Inter-MSC Movement (2/2)

- **Step 4.**
  - **Part I. By using the received IMSI, the HLR identifies the MS's record.**
  - **Part II. The MSC number field of the record is updated.**
  - **Part III. An acknowledgement is sent VLR.**
- **Steps 5 and 6.** Similar to steps 3 and 4 in Inter-BTS movement, the acknowledgement is forwarded to the MS.

GSM Basic Location Update: Inter-VLR Movement (1/2)

- **Step 1.** The location update request is sent from MS to the VLR.
- **Steps 2 and 3.**
  - **Part I.** Since the MS moves from VLR1 to VLR2, VLR2 does not have a VLR record of the MS, and the IMSI of the MS is not known.
  - **Part II.** From the **MAP_UPDATE_LOCATION_AREA** message, VLR2 identifies the address the VLR1.
  - **Part III.** VLR2 sends **MAP_SEND_IDENTIFICATION** to VLR1.
  - **Note that** to enhance security, **confidential data (IMSI)** typically is not sent over the air.

GSM Basic Location Update: Inter-VLR Movement (2/2)

- **Steps 4 and 5.**
  - VLR2 creates a VLR record for the MS, and sends a registration message to update the HLR.
  - The HLR updates the record of the MS.
  - An acknowledge is sent back to VLR2.
- **Step 6.**
  - VLR2 generates a new TMSI and sends it to the MS. In GSM, the TMSI is changed from time to time to avoid fraudulent usage.
- **Steps 7 and 8.** The obsolete record of the MS in VLR1 is deleted.

GSM Basic Call Origination

- **Step 1.** The MS u1 sends the call origination request to the MSC.
- **Step 2.** The MSC forwards the requets to the VLR by sending MAP_SEND_INFO_FOR_OUTGOING_CALL.
- **Step 3**. The VLR checks the u1's profile and sends MAP_SEND_INFO_FOR_OUTGOING_CALL_ack to the MSC to grant the call request.
- **Step 4.** The MSC sets up the trunk according to the standard PSTN call setup procedure.

GSM Basic Call Termination (1/2)

- **Step 1.** When the MSISDN number is dialed by a PSTN user, the call is routed to a gateway MSC by an SS7 **ISUP IAM** message.
- **Step 2.** To obtain the routing information, the GMSC or ISDN exchange interrogates the HLR by sending **MAP_SEND_ROUTING_INFORMATION** to the HLR.
  - **The message contains the MSISDN of the MS and other related info.**
- **Step 3.** The HLR sends a **MAP_PROVIDE_ROAMING_NUMBER** message to the VLR to obtain the Mobile Subscriber Roaming Number (MSRN).
  - **The message consists of IMSI of the MS, the MSC number.**

GSM Basic Call Termination (2/2)

- **Steps 4 and 5.** The VLR creates the MSRN by using the MSC number stored in the VLR record of the MS. This roaming number is sent back to the gateway MSC through the HLR.
- **Step 6.** The MSRN provides the address of the target MSC where the MS resides. An SS7 **ISUP IAM** message is directed from the gateway MSC to the target MSC to setup the voice trunk.

Mobility Databases: Home Location Register (HLR)

- Mobile Station Information. For example,
  - the **IMSI** (used by the MS to access the network), and
  - **MSISDN** (which is the ISDN number—"Phone Number" of the MS)
- Location Information. For example,
  - the **ISDN number (address) of the VLR** (where the MS resides), and
  - the **ISDN number of the MSC** (where the MS resides)
- Service Information. For example,
  - **service subscription**,
  - **service restrictions**, and
  - **supplementary services**

Mobility Databases: Visitor Location Register

- **Mobile Station Information.** For example,
  - IMSI
  - MSISDN
  - TMSI
- **Location Information.** For example,
  - MSC Number
  - Location Area ID (LAI)
- **Service Information.**
  - **A subset of the service Information stored in HLR**
- Note that in the MS-related fields
  - **Length TMSI <= 8 digits (TMSI structure defined by the operator)**
  - **LAI = XXX + XX + XXXXXXXXXXXXXXX**

(Mobile Country Code) (Mobile Network Code) (location access code)

VLR Failure Restoration

- **Service Information** of a VLR record recovered by
  - **The first contact between the VLR and the HLR of the corresponding MS.**
- **Location Information** of a VLR record recovered by
  - **First radio contact between the VLR and the MS**
- **Mobile Station Information** of a VLR record recovered by
  - **Either by contact with the HLR or the MS**

VLR Record Restoration Initiation Event 1 – MS Registration

- The VLR considers the registration as a case of inter-VLR movement.
- Following the normal registration procedure defined in inter-VLR movement.
- In this case, the TMSI sent from the MS to the VLR cannot be recognized, and the MS is asked to send IMSI over the air.

VLR Record Restoration Initiation Event 2—MS Call Origination

- When the VLR receives the call origination request **MAP_SEND_INFO_OUTGOING_CALL** from the MSC, the VLR record of the MS is not found.
- The VLR considers the situation as a system error, with the cause "**unidentified subscriber**".
- The request is rejected, and the MS is asked to initiate the location registration procedure.

VLR Record Restoration Initiation Event 3—MS Call Termination (1/)

- **Steps 1-3.** Similar to the first three steps of the basic call termination procedure, the VLR is queried to provide the MSRN.
  - **Note that since the record has been erased after the failure, the search fails. The VLR creates a VLR record for the MS.**
  - **Neither the service nor the location info is available.**
- **Steps 4 and 7.**
  - **Since the VLR does not have the routing information, it uses the MSC number provided by MAP_PROVIDE_ROAMING_NUMBER message to create MSRN.**
  - **The number is sent back to the gateway MSC to setup the call in Step 8.**

VLR Record Restoration Initiation Event 3—MS Call Termination (2/)

- **Steps 5 and 6.**
  - The VLR recovers the service information of the VLR record by sending a MAP_PROVIDE_ROAMING_NUMBER message to the HLR.
  - The HLR sends the service information to the VLR using the MAP_INSERT_SUBSCRIBER_DATA message.
  - At this point, the service information of the VLR record has been recovered.
  - However, the location information, specifically, the LAI number, still not available. This information will be recovered at Step 11.
- **Note that** Steps 4 and 5 can be executed in parallel.

VLR Record Restoration Initiation Event 3—MS Call Termination (3/)

- **Step 8.** After the gateway MSC receives the MSRN in Step 7, the SS7 ISUP message IAM is sent to the target MSC.
- **Steps 9-11.**
  - **The target MSC does not have the LAI info of the MS.**
  - **In order to proceed to set up the call, the MSC sends the message MAP_SEND_INFO_FOR_INCOMING_CALL to the VLR.**
  - **Unfortunately, the VLR does not have the LAI info either.**
  - **Hence the VLR asks the MSC to determine the LA of the MS by sending a MAP_SEARCH_FOR_MOBILE_SUBSCRIBER message.**

VLR Record Restoration Initiation Event 3—MS Call Termination (4/4)

- **Steps 12 and 13.**
  - The MSC initiates paging of the MS in all LAs.
  - If the paging is successful, the current LA address of the MS is sent back to the VLR by the MAP_PROCESS_ACCESS_REQUEST message.
  - At this point, the location information of the VLR record is recovered.
- Note that
  - MAP_SEARCH_FOR_MOBILE_SUBSCRIBER is an expensive operation because every BTS connected to the MSC must perform the paging operation.
  - To avoid this "Wide Area Paging", the GSM system may periodically asks the MSs to re-register.

HLR Failure Restoration

- It is mandatory to save the updates into nonvolatile storage.
- Changes of the **service information** are saved into the backup storage device immediately after any update.
- The **location information** is periodically transferred from the HLR into the backup.
- After an HLR failure, the data in the backup are reloaded into the HLR.

HLR Restoration Procedure (1/3)

- After an HLR failure, the data in the backup are reloaded into the HLR.
- An Uncovered Period = the time interval after **the last backup operation** and **before the restart of the HLR**.
- Data that have been changed in the uncovered period can not be recovered.

HLR Restoration Procedure (2/3)

- **Step 1.** The HLR sends an SS7 TCAP message **MAP_RESET** to the VLRs where its MSs are located.
- **Step 2.** All the VLRs derive all MSs of the HLR. For each MS, they send an SS7 TCAP message, **MAP_UPDATE_LOCATION**, to the HLR.

HLR Restoration Procedure (3/3)

- The HLR restoration procedure is not robust.
  - **An MS may move into a VLR (which does not have any other MSs from the given HLR residing) during the uncovered period.**
  - **The new location is not known to the HLR at the last check-pointing time.**
  - **If so, the HLR will not be locate the VLR of the MS during Step 1 of HLR restoration.**
- VLR Identification Algorithm is to solve the problem.

Data Structure in VLR Identification Algorithm (VIA) (1/2)

- To simply the description, we assume that every VLR covers exactly one MSC.
- To implement VIA, extra data structures are required.
- In the backup, the extra data structure is a set **VLR_List*** of VLRs that have been modified during the uncovered period.
- After an HLR failure, the HLR only needs to send the **MAP_RESET** messages to VLRs listed in **VLR_List***.

Data Structure in VLR Identification Algorithm (VIA) (2/2)

- In HLR, every record includes two extra fields.
  - **The ts field = the last time of location update**
  - **The PVLR field = the address of VLR where the resided at the lat check-pointing time. Thus, for any MS p, we have**

$$HLR^*[p].VLR = HLR[p].PVLR$$

- Two extra data structures are introduced in the HLR.
  - **TS = the last check-pointing or backup time**
  - **VLR_Counter = {(*VLR1*,*Count*), (*VLR2*,*Count*), …, (*VLRn*,*Count*)} where Count represents the "effective number" of MSs entering the VLR *VLRn* during the uncovered period.**
  - **An MS is not effective to a VLR if it entered the VLR area then left the area during uncovered period.**
  - **Note that the VLRs recorded in VLR_Counter are the VLRs in VLR_List*.**

VIA Procedure 1: Check-Pointing

- In VIA, information of the HLR is periodically saved into the backup by this procedure.
- **Step 1.** For every entry p in HLR* do:

  HLR[p]*.VLR <- HLR[p].VLR;
- **Step 2.** TS <- current time;
- **Step 3.** For every location entry p in HLR do:

  HLR[p].ts <- TS; HLR[p].PVLR <- HLR[p].VLR;
- **Step 4.** VLR_Counter <- NULL; VLR_List* <- NULL;

VIA Procedure 2: Registration (1/3)

- Step 1. Update HLR:
  - V_{old} <- HLR[p].VLR;
  - Send message, MAP_CANCEL_LOCATION, to cancel the VLR entry of p at V_{old};
  - HLR[p].VLR <- V_{new};
  - t_{old} <- HLR[p].ts;
  - HLR[p].ts <- t;

VIA Procedure 2: Registration (2/3)

- **Step 2.** Update the V_{new} Count field in VLR_Counter:

```
If (HLR[p].VLR <> HLR[p].PVLR){
    If (VLR_Counter[Vnew] exists){
      VLR_Cpunter[Vnew].Count <- VLR_Counter[Vnew].Count+1;
    }else{
      create VLR_Counter[Vnew] and VLR_List*[Vnew];
      VLR_Counter[Vnew] <- 1;
    }
}
```

VIA Procedure 2: Registration (3/3)

- **Step 3.** Update the V_{old} counter entry:

```
If (t_old > TS and Vold <> HLR[p].PVLR){
    VLR_Counter[V_old].Count <- VLR_Counter[V_old].Count – 1;
    If (VLR_Counter[V_old].Count = 0){
      Delete VLR_Counter[V_old] and VLR_List*[V_old];
    }
}
```

VIA Procedure 3: Restore

- **Step 1.** TS <- current time;
- **Step 2.**

```
for (every location entry p in HLR){
    HLR[p].PLVR = HLR[p].VLR <- HLR[p]*.VLR;
    HLR[p].ts <- TS;
}
```

- **Step 3.**

```
for (every VLR entry V in VLR_List*){
    send an SS7 TCAP MAP_RESET message to V;
}
```

VLR Overflow Control

- The number of records in the VLR can change dynamically.
- It is possible that the number of the records in the corresponding VLR may be larger than that of the HLR, and the VLR may overflow if too many mobile users move into the LA in a short period.
- When a VLR is full, the incoming mobile users cannot register using the registration.
- To Solve the problem, overflow control algorithms O-I, O-II, O-III, and O-IV are presented.

Summary

- GSM Location Update
- Basic Call Origination and Termination Procedures
- Mobility Databases
- Failure Restoration
- VLR Identification Algorithm
- VLR Overflow Control