Project I

Mobile Network System for Special Communication

Project employer:
The Tenth Research Institute of Telecommunication Technology
Project period:
August 1998 to May 2000
Project Characteristic:
The system is a kind of special communicating device for the purpose of security management for GSM mobile communication system. The designed device involves various technologies including **mobile communication, telecommunications exchange, signal 7, computer control system, computer operating system, computer network and software engineering**.
My role in the project:
I was responsible for software subsystem R&D, system communication and monitoring and as one of the project managers.
Project Description:
The system can implement the monitoring function toward mobile monitoring station under different circumstances (calling, called, switching or waiting), and acquires the communicating message (including the contents of the voice, phone number, calling period, calling time and the exact location) from the objected station, the status (power on/off, the area belongs to). Furthermore, the system can flexibly add or delete the monitored objections, and carried out some special tasks according to the customer's specific requirements.

The system consists of two parts: the foreground message intercept & analysis system located in the mobile machine room and background monitoring center system handled by users. I was responsible for software subsystem developing and research, and my duties mainly included:

- Signals analysis
- System control
- Foreground applicable software development
- Assist in foreground and background communicating software development
- The whole set monitoring and testing
- Prepare documentation on the system

I. Technology analysis and design

1. Signal

The system adopts A-interface of GSM system to perform information monitoring function by the way of information intercept. A-interface is between

BSS (Base Station System) and MSC (Mobile Switching Center), which support all the services to GSM customers. All the information between mobile station and the system is through this interface, through which the message of mobile holders can be acquired by performing information intercept function.

As the basis and key of the system design, A-interface signaling process should be analyzed firstly. A-interface signal can be divided into several layers as (from bottom to up) MTP, SCCP, BSSMAP and DTAP, etc. And MTP is handled by way of hardware, and signaling of the software subsystem began from SCCP.

SCCP protocol is a protocol defined in the 7 signaling system, which locates at the bottom of the signaling part of software subsystem. The basic connecting model and oriented connecting model of SCCP are mainly used in A-interface, i.e. the 0- and 2- category work type of SCCP, which are mainly responsible for link setup and link dismantle of the signal link as well as message transmission to the upper side.

BSSMAP and DTAP in A-interface belong to GSM specialized protocol, which is combined and called BSSAP. According to design requirements of the system, BSSAP mainly handles with signaling message related to mobile management, calling and switch when handling wireless signals.

A. Mobile Management (MM) process

In the GSM system, each mobile subscriber is allocated with a unique IMSI, which has fixed corresponding relations with the mobile phone number issued by the manufacturer. For the sake of security, TMSI is defined as the communication identification. TMSI is allocated randomly by the network through TMSI reallocation procedure, which is a unique one within a specified area. If outside the area, it must be used with LAI (Location of Area Identification) in order to identify a mobile subscriber.

The task of MM is to follow the tracks of the location of mobile platform (which is being monitored) and the corresponding relationship between TMSI and IMSI by monitoring the reallocation and re-location process of TMSI, which is related to GSM mobile management, thus laid a foundation for voice intercepting.

TMSI reallocation process can be regarded either as an independent process in GSM, or as a process implied accompanying the performances of other procedures.

As an independent process, TMSI reallocation process can be triggered by the network at any time, and its process is as follows:

The network issues TMSI reallocation command to the Mobile Station (MS), which includes the new-allocated TMSI and LAI by the network. If delete TMSI, IMSI is deleted too.

When MS receives TMSI reallocation command, it installs LAI in SIM card. If MS receives IMSI, it will delete the original TMSI; if MS receives TMSI, it will install it in SIM card; meanwhile, MS transmits “TMSI reallocation complete” message to the network.

When the network receives the message of “TMSI reallocation complete”, it will finish TMSI reallocation process.

The Location Updating Process is closely related to TMSI reallocation process, which includes normal location updating, periodic location updating and IMSI attaching process. Though their objections and triggering conditions are different, they all adopted the universal location updating procedure.

The basic procedure is as follows:

MS issues location-updating request and started location updating process.

When the network receives the request, it will release the message of “LOCATION UPDATING ACCEPT”. Generally, location-updating process is accompanied with TMSI reallocation process. At that time, LOCATION UPDATING ACCEPT includes LAI and TMSI. When MS receives, it will transmit “TMSI REALLOCATION COMPLETE” to the network and finish the location updating process.

The corresponding process to IMSI attaching process is IMSI separating process, which has only one message transmitting to the network to identify “MS inefficient” (power off etc.).

Through the monitoring performance toward MM-related process, message can be obtained, such as the location of the monitored mobile station, working status and TMSI. Furthermore, it laid a foundation for monitoring the calling.

B. Calling Control Process

It is the core task to monitor the calling of controlled objections. In GSM, the calling can be divided as mobile calling and mobile terminal calling. In the calling process, the important message appearing one after another, which is related to monitoring and voice recovery, is as follows:

a. The third-layer initial message (CM service request, calling response, ect.)

b. Set up message
c. Allocate request message
d. Connect message

The third-layer initial message is generally included in SCCR CR message. It is the first message in the connecting and setup procedure, which includes mobile station identification (TMSI or IMSI), through which to judge the monitored objections.

SCCP message, as the corresponding message to CR, is CC message, which is only used for link setup and does not include customers' data.

SETUP message includes bearer services such as voice and data, and probably includes principle called number.

CIC message unit of the assignment request message includes PCM (where voice locates) and time slot message.

The last calling setup message is CONNECT message, which demonstrates that the monitored objects have established normal communication with their counterparts. The system can utilize the obtained voice information to perform intercept and recovery functions.

Calling release message mainly covers DISCONNECT, RELEASE, etc. When acquired these messages, the system will terminal the monitor and release relevant resources.

C. Handover process

During the process of mobile communication, due to the change of circumstances (such as change of mobile station location, the influence of the surrounding environment), handover may occur at any time.

The common handover in GSM system is BSC interior regions handover and handover between BSC.

The typical BSC handover process starts from BSSMAP's "Handover request" message transmitted from BSS to MSC. The reason for triggering the handover mainly lies in the quality of wireless link or in the traffic jam. The message includes region identification list which BSS hopes MS to handover.

When MSC receives the "handover request" message from BSS, it will transmit "handover request" message to the objected BSS, and request for wireless resources, including required ground resources, such as PCM, time slot, etc.

If the condition is normal, that is to say, the requested wireless resources are usable; the objected BBS will return the “handover request confirmation” message. The third information unit of the message includes “handover command” message of wireless interface. MSC assembles the “handover command”, which is in the “handover command” of BSSMAP, and sends it to the former BSS, and the former BSS sends the “handover command”, which includes in the BSSMAP’s “handover command”, to MS through wireless interface. The message includes BSS-chose new wireless channel and handover reference number.

After the objected BSS returned “handover request confirmation” message to MSC, the allocation program procedure of handover resources is completed. Then the handover implementation program begins.

When MS receives “handover command” message, it will submit a “handover access” message with handover reference number to the objected BSS.

If the reference number is correct, BSS will submit a “handover tested” message to MSC.

When MS sets up the communication link with network successfully, the objected BBS soon issues a BSSMAP “handover completed” message to MSC and finalizes the handover program. MSC issues the “clear command” message to the former BSS and completes the handover program of BSS.

Based on the above technology analysis, we conducted project demonstration and determined **Visual C++** as the developing tool for signal handling part and **Windows NT Server 4.0** as the operation system.

2. System Control

The system control part implements the functions of system resources management, voice exchange and system control.

System hardware subsystem adopts distributed control system mode. The whole set is made up of several devices. Each device can be installed with one CPC, 13 DTC at most, voice handling bar at most, 2 power main board at most. CPC adopts the common-used industrial control machine and implements the functions of system control and software running system by means of hanging interface board. There is a MITEL MT90280 and a PEB2445 in CPC, which can conduct the voice exchange and synthesis, and can communicate with other circuit boards in other devices by means of the double-port RAM; DTC is controlled through Motorola 68K communication processor; the signal-processing chip adopts SIMENS SAB82525 chip and MT9075, among which

MT9075 is responsible for framing function, SAB 82525 for HDLC function, and the exchange chip is PEB2045. Each DTC and handle 4-relay; the voice processing board changes the digital voice into simulation signal under the control of the main control board, and transmits the voice into the specified background number by means of dial-up mode. Each voice processor can handle with 4-line voices simultaneously. The circuit board inside the device adopts the bus-mode of board-back-board to communicate, and the transmission of voice and time slot between boards is achieved by MT 90820 in CPC. Every board in the device is corresponding to a series digital relay of MT 90280, and messages between boards are communicated by double-port RAM mode. Voices and signal communication are also conducted by using MT 90820 in CPC. And the message communication is conducted in networking mode by RJ-45 port of the industrial control machine.

Based on full understanding of system hardware system working principles, the task of system management control is to develop the device driver, real-time control and voice exchange programs, system resources management scheduling programs, thus conducted the functions as system resources management, voice exchange and system control.

System control and voice exchange are completely demonstrated in the off-hook process and on-hook process.

Off-hook process:
When off-hook, the system acquires PCM and time slot of the controlled objected voice on the basis of analyzing BSSMAP “assignment request” message. By querying the corresponding list, it acquires the corresponding board location of the device and the HV number, and then chooses two free time slots from 92820’s HV link circuit, which corresponds to the board, and issues the off-hook command to the corresponding DTC. The command includes the above-mentioned parameters. DTC exchanges the calling and called voices of the controlled objection to the obtained two 90820 time slots through PEB2045 exchange chip on the board. Then, the system chooses three free time slots from HV line in 90280, which is connected with PEB2445 in the main control board. Then exchange two voices into the access HV in PEB2445 through 90280; then use the conference exchange function of PEB2445 to conduct conference exchange, to combine the calling and called voices into a complete one. The synthetic voice is on the third time slot; the system chooses the free voice communicating dialer, and exchanges the synthetic voice into HV and time slot of the corresponding free dialer through 90280, meanwhile it gives notice to the voice communicating board about the line location of the voice and background telephone number. The voice communicating board fetches PCM voice signal in the corresponding time slot, and recovers it to the simulating voice and dial it onto the set background

telephone number.

On-hook process:

When the system receives the disconnect signal message from the network (such as DISCONNECT, RELEASE, etc.), it starts the on-hook process. On-hook process is the anti-process of off-hook, the purpose is to dismantle the established link circuit in the off-hook process and release the occupied resources. The process is as follows:

Querying the voice-occupied DTC board location and the corresponding time slot, issue the on-hook command to the corresponding DTC; issue on-hook command to the occupied dialer; anti-exchange of 90280 and set the occupied time slots as silence; anti-exchange of 2445; complete conference link dismantle; and set the occupied resources as FREE for the coming communications.

This part mainly involves **Visual C++, Win32 SDK/NT DDK, Mcs-51 Assembly Language, ANSIC** etc. and **Windows NT Server 4.0, Psos+**.

3. Foreground-background communication

Foreground-background communication system conducts voice-return of foreground and two-way data communication between foreground and background. The foreground voice-return adopts the mode of software plus hardware, and its scheduling function belongs to the function of the control part of foreground software system. Background voice adopts part of voice card to receive voice, and stores the voice in the background database through software programming as data files. The background database uses **Microsoft SQL Server**, and data communication is conducted by self-defined protocol and Modem dialing-up.

II. Software Implementation

Upon the above-mentioned analysis, we can see that the software subsystem of the project (Mobile Network System for Special Communication) is very complicated, which involves knowledge of many fields, such as mobile communication, telecommunication exchange, computer network, software engineering, etc. Hence, I strictly follow the communication software design standard in the design in order to ensure the coupling between modules. Meanwhile, as a real-time monitoring software system, I should do my best to ensure the high-efficiency of the system.

Here is a brief description about software module and database structure.

1. Modules design and communication

The system is made up of hardware interface module, signal handling and system control module, and network interface module.

The signal handling and system control module is the principle module of the system, which conducts signal handling and system control; hardware interface module provides software and hardware interface for address mapping and information transmission between boards; the network module provides network services for the system, and complete the task of message communication between various devices as well as between foreground and background.

2. Data structure design

Data structure designing plays an important part in the process of communicating software design, it decides the stability of the system operating.

The developing tasks include calling process control, conversation control, system status control, timer control, various communicating messages structures, various system resources management and control (including system voice link circuit management, voice time slot control management, voice exchange control, various data sheet, message structures to control different hardware resources).

In the data structure design, I divided the data sheet into several parts: the system status sheet, the conversation data sheet, the message data sheet, timer data sheet, affairs data sheet (controlling the messages inside the system), system resources status sheet and the communicating message structure (coordinating the operation of different modules within the system).

The above-mentioned data structures can be divided into many sub- sheet structures according to different circumstances, and they can couple or include each other accordingly. The sheet structures in the same category can be organized through circular chain sheet. The circular chain sheet can register the space when starting the system initialization according to the required capacity. During the communication process, the resources allocation, the querying of calling control block can be found out through the chain or conducted by HaXi calculation method.

III. System Testing

I was responsible for the testing work of the whole set in order to test the efficiency of the system. Due to the complexity of mobile communication, some contingencies might happen during the testing. Based on my deep understanding on mobile communication system and system software and hardware, I had a keen judge on the causes of problems and proposed the plan to solve them. Thanks to the hard work, the system was completed successfully and conducted end-to-end joints with GSM mobile communication equipment of Datang Telecom Company and North Telecom Network.