2G, 3G Network Planning and Optimization...

Archives

▼ 2009 (56)
► Октябрь (15)
▼ Сентябрь (41)
3.8 Network Capacity Comparison For the comparis...
3.7 Multiple Reuse Pattern Technology3.7.1 Basic...
3.6 Concentric Cell Technology 3.6.1 Concept I...
3.5 Aggressive Frequency Reuse Technology 3.5.1 ...
3.4 Normal Frequency Reuse Technology 3.4.1 C...
3.3 Frequency Planning Principle Generally, when ...
3.2 Frequency Division and C/I Requirement 3.2.1 ...
3 GSM Frequency Planning 3.1 Overview Frequency ...
2.13 Conclusion Network planning is the foundatio...
2.12 Repeater Planning 2.12.1 Application Backg...
2.11 Tunnel Coverage 2.11.1 Characteristic of T...
2.10 Design of Indoor Coverage System2.10.1 Ch...
2.9 Dual-Band Network Design 2.9.1 Necessity for...
2.8 Location Area Design 2.8.1 Definition of Loc...
2.7 Design of Base Station Address 2.7.1 Address d...
2.6 Base Station Number Decision After traffic an...
2.5 Traffic Analysis 2.5.1 Traffic Prediction an...
2.4 Network Structure Analysis When considering t...
2.3 Coverage Analysis 2.3.1 Area Division I. Typ...
2.2 Planning Foundation 2.2.1 Coverage and Capacit...
2 GSM Radio Network Planning 2.1 Overview The de...
1.17 CBS Cell Broadcast Service (CBS) is similar ...
1.16 Call Re-Establishment 1.16.1 Introduction ...
1.15 HOAs a key technology in the cellular mobil...
1.14 MS Originated Call Flow 1.14.1 Enquiry Afte...
1.13 MS Originating Call Flow The MS needs to set ...
1.12 Location Update In GSM, the paging informati...
1.11 Authentication and Encryption GSM takes lots...
1.10 Immediate Assignment Procedure The purpose o...
1.9 Power Control 1.9.1 Power Control Overview P...
1.8 Discontinuous Reception and Discontinuous Tra...
1.7 Frequency Hopping With the ever growing traff...
1.6 Cell Selection and Re-Selection 1.6.1 Cell S...
1.5 System Information System information is sent ...
1.4 Timing advance Signal transmission has a dela...
1.3 Data Transmission Radio channel has totally d...
1.2 Multiple Access Technology and Logical Channel...
1 GSM Principles and Call Flow 1.1 GSM Frequency ...
Radio Network Planning Optimization The objective ...
History of GSM 1 GSM Development Mobile telecommun

среда, 2 сентября 2009 г.

1.11 Authentication and Encryption

GSM takes lots of measures to protect the safety of system, such as using Temporary Mobile Subscriber Identity (TMSI) to protect IMSI, using Personal Identification Number (PIN) to protect SIM card, authentication through authentication center (AUC) for network access, encryption, and equipment identity register.

Authentication and encryption require a group of three parameters that generated in AUC. Each client is assigned a Mobile Station International ISDN Number (MSISDN) and IMSI when registers in GSM network. IMSI is preserved onto SIM card through SIM printer and SIM printer will generate a corresponding client authentication value Ki that is stored in SIM card and AUC as permanent information. AUC has a pseudo number generator used to generate a random number RAND. GSM defines algorithm A3, A8, and A5 that are used for authentication and encryption. In AUC, RAND and Ki together produce a response number SRES through A3 authentication algorithm and a Kc through A8 encryption algorithm. RAND, Kc, and SRES form a three-parameter group of client. This group is stored in the data base of this client in HLR. Generally, AUC transfers five groups of parameters to HLR for automatic storage. HLR can save ten groups of such parameters. When MSC/VLR requests for three-parameter group transfer, HLR sends five groups at the same time for MSC/VLR to use one by one. When there are two groups left, MSC/VLR will request for transfer again.

1.11.1 Authentication

Authentication is the process that GSM network checks whether the IMSI or TMSI from MS at radio interface is valid or not. The purpose of authentication is to avoid unauthorized access to GSM network and the theft of private information by illegal users. Authentication also provides parameters for MS to calculate new encryption key.

The network initiates authentication procedure in the following situations:

MS requesting for the change of information in VLR or HLR;

Service access, including MS originated call, MS terminated call, MS activation and deactivation, and supplementary services;

The first network access after MSC/VLR reboot;

Mismatching Cipher key Sequence;

Whether to initiate authentication procedure depends on if the Kc value of the last service processing stored in network consistent with that of the present access stored in MS. If consistent, authentication procedure can be escaped and this Kc value is used directly for encryption; if not, Kc value needs to be recalculated. MS does not send Kc value to network through radio path for the sake of privacy. Therefore, Cipher Key Sequence Number (CKSN) is introduced. CKSN is sent to MS by MSC/VLR through authentication request message during the last network access. It is stored in both SIM card and MSC/VLR. During the initial access of MS, CKSN is sent to MSC/VLR through the initial request message of SABM frame. MSC/VLR compares it with the last CKSN. If they are not consistent, authentication is required before encryption. If CKSN=0, it means no Kc is assigned. Authentication procedure is initiates and controls by network. MSC/VLR sends an authentication request message to MS to initiate authentication procedure and T3260.

I. Authentication Success

2) AUTHENTICATION REQUEST contains a RAND (128 bits) and a CKSN. The Ki and RAND together generate a SERS (32 bits) through algorithm A3 and a Kc (64 bits) through algorithm A8. The new Kc replaces the former key and is stored in SIM card together with CKSN.

3) MS sends AUTHENTICATION RESPONSE to network. After receiving this message, the network stops T3260 and checks its validity (network compares it with the SERS generated by Ki and RAND through algorithm A3 and check whether they are consistent or not), and then enters the subsequent procedures, such as encryption.

II. Authentication Reject

If authentication fails, it means AUTHENTICATION RESPONSE is invalid.

If the MS uses TMSI, the network will initiate identity procedure. If the IMSI provided by the MS is different from that in network, the network will restart the authentication procedure; if the IMSI is correct, the network will send AUTHENTICATION REJECT to the MS.

If the MS uses IMSI, the network will send AUTHENTICATION REJECT directly to MS. After sending AUTHENTICATION REJECT message, the network releases all the MM connections under establishment and restarts the procedure for RR connection release.

After receiving AUTHENTICATION REJECT message, MS sets the roaming disabled flag and deletes information such as TMSI, LAI, and cipher key.

If MS receives AUTHENTICATION REJECT message in IMSI DETACH INITIATED state, it stops T3220 after RR connection is released. If possible, MS initiates local release procedure after the normal release procedure or T3220 timeout; if not (such as the IMSI detach after switch off), MSRR exits abnormally.

If MS receives AUTHENTICATION REJECT message in other state, it exits all MM connections and call re-establishment procedures, stops T3210 and T3230, sets and starts T3240 to enter WAIT FOR NETWORK COMMAND state and wait for the release of RR connection; If RR connection is not released after T3240 timeout, MS will exit RR connection abnormally. Under the two conditions above, MS enters MM IDLE and NO IMSI state.

1.11.2 Encryption

Encryption occurs in service requests such as location updating, service access, and inter-office handover. It requires the support of GSM network equipment (especially BTS), as well as the encryption ability of MS.

I. Signaling Procedure

1) MSC sends BSC a Ciphering Mode CMD that contains encryption algorithm, Kc, and whether the

MS is required to add IMEI in Ciphering Mode CMP.

2) BSC decides the final algorithm based on the encryption algorithm in Ciphering Mode CMD, the encryption algorithm that BSC allows, and the encryption algorithm that MS supports, and then inform BTS.

3) BSC sends MS Ciphering Mode CMD to inform MS of the selected encryption algorithm.

4) After receiving Ciphering Mode CMD, MS starts the transmission of ciphering mode and sends Ciphering Mode CMP to the system.

5) After receiving the Ciphering Mode CMP from MS, BSC transfer it to MSC.

II. Procedure Description

A5 algorithm

GSM protocol specifies eight kinds of encryption algorithm from A5/0 to A5/7. A5/0 stands for no encryption. The encryption procedure is initiated by the network. The encryption information of Cipher Mode CMD specifies the required encryption algorithm. The algorithm that generates encrypted code is called A5 algorithm. It calculates by using the Kc (64 bits) and the current frame number (22 bits) to generate a 114-bit encryption sequence and then implements XOR operation with the 114-bit burst. Two encryption sequences are used for uplink and downlink. For each burst, one sequence is used for MS encryption and BTS decryption, the other sequence is used for BTS encryption and MS decryption.

Encryption algorithm selection

When MS initiates call request, the SABM frame carries Classmark 1 or 2 to indicate whether the MS supports algorithm A5/1, A5/2, or A5/3, and reports Classmark 3 in CLASS MARK CHANGE to further indicate whether the MS supports Algorithm A5/4, A5/5, A5/6, or A5/7(In system information, if ECSC=1, MS reports Classmark 3 immediately; if ECSC = 0, the Classmark 3 is reported after CLASSMARK ENQUIRY is initiated by the network. Therefore, the configuration of ECSC = 1 is recommended when the encryption is used). MSC sends encryption command based on the configuration of secret data. BSC chooses the intersection of the encryption algorithm allowed in the command sent by MSC, the encryption algorithm allowed in BSC data configuration, and the encryption algorithm supported in the MS report. In the intersection, BSC selects a proper algorithm based on the priority level of A5/7 > A5/6 > A5/5 > A5/4 > A5/4 > A5/3 > A5/2 > A5/1 > A5/0.

Encryption in handover

The HANDOVER REQUEST contains the encryption information unit that indicates the required encryption algorithm and key. If one of the two A interfaces of BSS is in PHASE I, due to the limitation of ETSI GSM PHASE I protocol (no ciphering mode setting information unit in handover command), the two A interfaces match only when they share the same encryption algorithm (such as A5/2) to ensure the normal inter-BSC handover. Otherwise, special treatment has to be made to the target MSC or target BSC (or the source MSC or source BSC) to change the handover command for inter-BSC handover.

For the interconnection of A-interfaces when the encryption is used, whether special data configuration is required for BSC and MSC must be considered.

1.11.3 TMSI Reallocation

After authentication and encryption, the system sends CM SERVICE ACCEPT or TMSI reallocation command to MS and initiates T3250.

When MS registers in the location area for the first time, the network allocates a TMSI to it. When the MS leaves this location area, it releases the TMSI. When the MS receives the TMSI reallocation command, it saves the TMSI and LAI and sends TMSI reallocation complete message. After receiving this message, the network stops T3250.

If the system cannot identify TMSI of the MS, for example, when the data base error occurs, the MS must provide its IMSI. The identification program is initiated before the TMSI reallocation to request for the IMSI.

The identification program sends identity request message to the MS, after receiving this message, the MS provides its IMSI by sending identity response message to the network. When this procedure is over, authentication, encryption, and IMSI reallocation are implemented if required.

1.11.4 Exceptional Situations

I. Authentication

RR connection failure

If the network detects RR connection failure before receiving AUTHENTICATION RESPONSE, it releases all the MM connections and terminates all the active MM procedures.

T3260 timeout

T3260 is started when MSC sends authentication request to BSC and stops when MSC receives AUTHENTICATION RESPONSE. If the T3260 times out before the AUTHENTICATION RESPONSE is received, the network releases RR connection, terminates the authentication procedure and all the active MM procedures, and then releases all the MM connections and initiates RR connection release procedure.

Unregistered SIM card

If the SIM card of the MS is not registered, the network sends AUTHENTICATION REJECT message directly to the MS.

II. Encryption

Encryption reject

If BSS does not support the encryption algorithm specified in CIPHERING MODE CMD, it sends CIPHER MODE REJECT message to MSC.

If the encryption is initiated in BSS before MSC requests for the change of encryption algorithm, BSS also sends CIPHER MODE REJECT message to MSC.

Un-encrypted MS

The CIPHERING MODE COMMAND message is valid when:

–The un-encrypted MS receives CIPHERING MODE COMMMAND message that requires encryption.

–The un-encrypted MS receives CIPHERING MODE COMMMAND message that requires non-encryption.

–The encrypted MS receives CIPHERING MODE COMMMAND message that requires non-encryption.

In other cases, CIPHERING MODE COMMAND is considered wrong. The MS sends RR STATUS message with the cause of protocol error and performs no action.

III. TMSI Reallocation

RR connection failure

If RR connection fails before TMSI reallocation complete message is received, all the MM connections are released and both the old and new TMSIs are saved during a certain recovery time.

T3250 timeout

T3250 is started when MSC sends TMSI_ REALL_ CMD message or LOC UPD ACC message with the new TMSI and stops when MSC receives TMSI _REALL_COM. If T3250 times out before the TMSI _REALL_COM is received, MSC sends CLEAR COM message to release RR connection and terminate TMSI reallocation.

Автор: ourdot на 1:06

0 коммент.:

Отправить комментарий

Подпись комментария: Выбрать профиль...

Отправить комментарий Просмотр

Следующее Главная страница Предыдущее

Подписаться на: Комментарии к сообщению (Atom)