Chapter 3
3G Security Features

3.1 Wireless security :

Communications on shared media like radio communication are no longer private. Privacy and authentication are lost unless some method is established to regain it. Cryptography provides the solution to regain control over privacy and authentication. All digital mobile systems provide security through some kind of encryption system. Data can be encrypted in many ways, but algorithms used for secure data transfer fall into one of the two broad categories: Symmetric and Asymmetric .Both rely on performing mathematical operations using a secret number known as a key. Symmetric algorithms depend on both parties knowing the keys. Larger key means better encryption. DES and A5 are examples of symmetric algorithms. The difficulty with symmetric algorithms is that both parties need to have a copy of the key. To transmit the key freely over the air would render the whole exercise pointless. Asymmetric algorithms use two separate keys for encryption and decryption. Usually, the encryption key can be publicly distributed, while the recipient holds the decryption key securely. RSA is an example of asymmetric algorithm.

The privacy needs of a wireless system can be described in the following areas:

- **Privacy of call set up information:** During call set up, the mobile station (MS) will communicate information to the network. .Some of the information that a user could send is calling number, calling card number, type of service requested etc. The system must send all this information in a secure way.
- **Privacy of speech:** The system must encrypt all spoken communication so that hackers cannot intercept the signals by listening on the air waves.
- **Privacy of the data:** The system must encrypt all user data communications so that hackers cannot I ntercept the data by listening on the airwaves.

- **Privacy of user location:** A user should not transmit any information that enables a listener to determine the user's location. The usual method to meet this is to encrypt the user ID. Three levels of protection are needed:
  1. Radio link eavesdropping
  2. Unauthorized access by hackers to the user location information stored in the network at the HLR and VLR
  3. Unauthorized access by insiders to the user location information stored in the network. This level is difficult to achieve, but not impossible .
- **Privacy of user identification:** When a user interacts with the network, the user ID is sent in a way that does not show the user ID. This prevents analysis of calling patterns based on user ID.
- **Privacy of calling patterns:** No information must be sent from MS that enables a listener of the radio interface to do traffic analysis on the mobile user. Typical traffic analysis information is calling number, frequency of user of MSs, caller identity and privacy of financial transaction.

If the user transmits credit card information over any channel, the system must protect data. Users may choose to speak their credit card numbers rather than dialing them via a keypad. User may access bank voice response system, where they send account information via tone signaling. He may also access calling card services of various carriers and may speak or use tone signaling to send card number. All these communications need to be private. Since the user can send the information on any channel-voice, data or control-the system must encrypt all channels.

3.2 Examples of wireless security breaches and thefts:

The major contributors to the loss of revenue for cellular operators are as follows:

- Theft of airtime
- Equipment theft and modification
- Breaches in network security, causing loss of confidential information
- Breaches in the integrity of billing systems
- Misuse of customer database information
- Vandalism at cell sites
- Loss of customer and industry confidence

SMT. HANSA MEHTA LIBRARY
M. S. University of Baroda

Security is becoming a major cost factor in the industry , since the cellular carriers have been diverting much of the income to tracking down these problems. The money that is being diverted is obviously better suited to network enhancements than to problem resolution.

3.3 General objectives for 3G security features: The third generation partnership project (3GPP) clearly outlines the objectives as

(a) To ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation

(b) To ensure that the resources and services provided by serving networks and home environments are adequately protected against misuse or misappropriation

(c) To ensure that the security features standardized are compatible with world-wide availability

(d) To ensure that the security features are adequately standardized to ensure world- wide interoperability and roaming between different serving networks

(e) To ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks

(f) To ensure that the implementation of 3G security features and mechanisms can be extended and enhanced as required by new threats and services

Furthermore, it has been agreed that the basic security features employed in 2G systems be retained or where needed enhanced.

3.4 UMTS security features: It basically covers authentication mechanism, confidentiality and integrity of the data. These features are integrated into various network entities as described below.

3.4.1 Access security to UMTS: Radio access technology will change from TDMA (Time Division Multiple Access) to WCDMA (Wideband Code Division Multiple Access) when 3G mobile networks are introduced .UMTS (Universal Mobile Telecommunications System) requires that end users of the system are authenticated. Cryptography provides the required solutions for network operators and subscribers.

One of the major security features of 3GPP system specifications (Release 1999) is mutual authentication. The authentication mechanism of UMTS involves Home Environment (HE), Serving Network (SN) and terminal containing USIM (Universal Subscriber Identity Module) The serving network checks the subscriber's identity by a challenge and response mechanism. The terminal also checks that the serving network has been authorized by the home network to do so. The authentication data request and response are shown in fig. 3.1

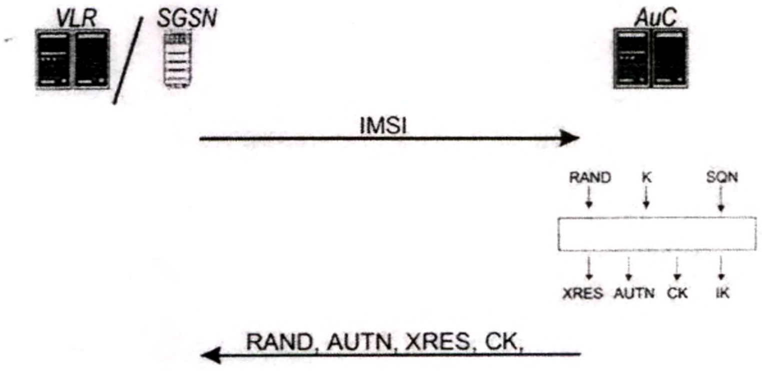

Figure 3. 1 Authentication data (Request and Response)

For the purpose of authentication, a subscriber authentication key K is shared between the USIM of the user and home network database, Authentication centre(AuC).The key has a length of 128 bits. There are temporary keys also which are derived from permanent key K and are used for encryption and integrity checking. Temporary keys are more frequently derived for bulk data protection. The authentication procedure begins when the user is identified in the SN. Identification begins when International Mobile Subscriber Identity (IMSI),Temporary Mobile Subscriber Identity (TMSI) or Packet TMSI is transmitted to the VLR (Visitor location register) or SGSN (Serving GPRS support node).VLR or SGSN sends an authentication data request to the AuC in the home network. Master key of each user is available with AuC and after gaining information about IMSI, AuC generates authentication vectors by running several cryptographic algorithms. Generated vectors are sent back to the VLR/SGSN in the authentication data response. The SN sends a user authentication request to the terminal, which contains two parameters RAND and AUTN. These parameters are transferred to the USIM which exists inside a tamper- resistant environment. The USIM contains the master key K and using it with the random number RAND and authentication token (AUTN) parameters along with other input values,USIM carries out a computation resembling generation of authentication vectors in AuC. The result of the computation is used by USIM to verify whether the AUTN parameter was indeed generated in AuC and was not sent beforehand to the USIM. If the answer is positive,the computed RES parameter is sent back to the VLR/SGSN .VLR/SGSN compares the user response RES with the expected response XRES ,which is part of authentication vector. The authentication procedure ends here if RES and XRES match. This is depicted in fig. 3.2

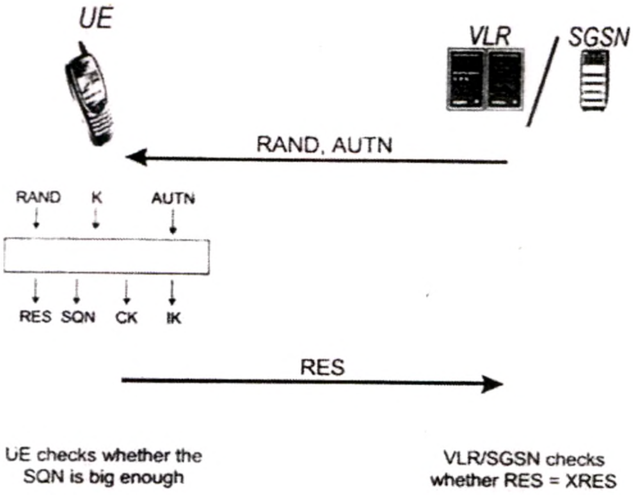
UE
VLR / SGSN
RAND, AUTN
RAND
K
AUTN
RES
SQN
CK
IK
RES
UE checks whether the SQN is big enough
VLR/SGSN checks whether RES = XRES

Figure 3.2 : User authentication (Request and Response)

The cipher key CK and integrity key IK are created as a byproduct in the authentication process. They are used for Radio Access Network (RAN) encryption and integrity protection.

Five one way functions namely f1,f2,f3,f4 and f5 are used to compute the authentication vector. The output of f1 is a message authentication code (MAC)(64 bits).Outputs of f2,f3,f4 and f5 are respectively XRES(32-128 bits),CK(128 bits),IK(128 bits) and AK(64 bits).The authentication vector consists of parameters RAND,XRES,CK,IK and AUTN.

3.4.2 Authentication on the USIM side : Same functions f1-f5 are involved on this side but in a slightly different order. The function f5 is computed before f1 because f5 is used to conceal the SQN. The output of the function f1 is marked XMAC on the user side. This is compared with the MAC received from the network as part of parameter AUTN. If there is a match, it implies that RAND and AUTN have been created by some entity that knows K.

The choice of algorithms f1-f5 are operator specific and they are only used in AuC and in the USIM and the home operator controls both of these entities. The transfer of authentication vectors from AuC and the actual use of these vectors for authentication are done somewhat independently .It is possible that authentication vectors may be used in a different order from which they were originally generated. The most obvious reason for this is because of the fact that mobility management functions for the CS (Circuit switched) and PS(Packet switched)domain are independent of each other ,implying that authentication vectors are fetched to the VLR and SGSN independently of each other and that the vectors are also used independently.

3.4.3 UTRAN Encryption: Once the user and the network have authenticated each other, they may begin secure communication. A CK is shared between the CN and the terminal after a successful authentication event. Before encryption can begin, the communicating parties have to agree on the encryption algorithm. Encryption and decryption take place in the terminal and in the RNC on the network side. For this purpose, CK has to be transferred from core network to the RAN. This is done in a specific Radio Access Network Application Protocol(RANAP) message. After the RNC has obtained CK, it can switch encryption on by sending a Radio Resource Control (RRC) command to the terminal.

The UMTS encryption mechanism is based on a stream cipher ,which means that plaintext data are added bit by bit to a random looking mask data generated by the CK and a few other parameters. The stream cipher concept is shown in the figure 3.3.

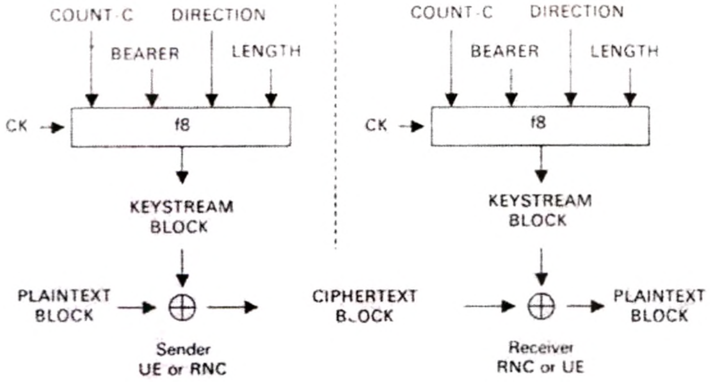

Figure 3.3 : Stream Cipher f8

UTRAN encryption occurs either in the Medium Access control (MAC) layer or in the Radio Link Control (RLC) layer. In both cases, there is a counter that changes for each Protocol Data Unit (PDU).In the MAC, this is a Connection Frame Number (CFN) and in the RLC ,it is a specific RLC sequence number (RLC-SN).

The core of the encryption mechanism is the mask generation algorithm denoted as function f8.It is based on a block cipher KASUMI. This block cipher transforms 64-bit input to 64-bit output. It uses 128 bit key CK.

The radio bearer identity BEARER is needed as an input to the encryption algorithm since the counters for different radio bearers are maintained independently of each other. The DIRECTION parameter indicates whether we encrypt uplink or downlink traffic. The LENGTH parameter indicates the length of data to be encrypted.

3.4.4 Integrity protection of RRC signalling : The purpose of integrity protection is to authenticate individual control messages. Integrity protection is implemented in the RRC layer. The IK is generated during the AKA procedure. The IK is transferred to the RNC together with the CK in the security mode command.

The integrity protection is based on the concept of message authentication code and it is a one way function controlled by the secret IK. The function is denoted by f9 and its output is a 32 bit random looking bit stream MAC-I.

The function f9 is shown in figure 3.4.The algorithm for integrity protection is based on same core function as encryption. The KASUMI block cipher is used in special mode to create message authentication code function.

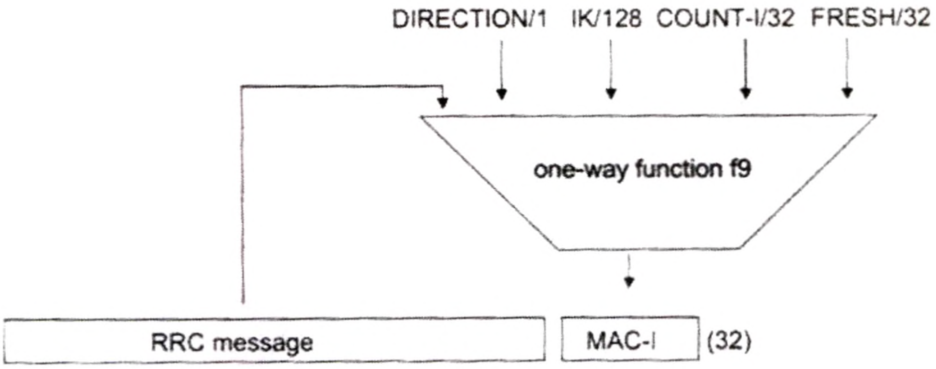

Figure 3.4 : Function f9

3.5 Set-up of UTRAN Security Mechanisms : We discuss actual set up of security mechanism when the user wants to establish connection with the network.

3.5.1 Negotiation of algorithms: Assume that the UE wants to establish connection with the network. First a class mark that indicates the capabilities of UE is sent to the network. These capabilities include support for encryption and integrity algorithms. Based on the received class mark, the network decides which algorithms to use:

- If there are no integrity protection algorithms in common then the connection is shut down immediately
- If there are no encryption algorithms in common, then the network may establish the connection without encryption.

When a new connection is established, some parameters are inherited from the previous connection. The UE has stored the value of START for both CS and PS domains to the USIM. At the same time, whether either of these values have reached the maximum allowed value called THRESHOLD has been checked. The latter is configured to the USIM and provides a means of limiting security key lifetimes. If the START has reached THRESHOLD for a CN domain, then CK and IK for this domain are deleted from the USIM and START is set to be equal to the THRESHOLD.

At the beginning of new connection, START values and security keys are read from the USIM. The Key Set Identifier (KSI) is associated with a pair of security keys: the CK and IK that were generated during the same run of an AKA procedure. The KSI consists of three bits. The value of KSI wraps around fairly often, every seventh time but a period of this length is enough to remove risk of ambiguity in practice. The values of START and KSI are transmitted to the network as a part of the first messages as soon as the connection is made.

3.5.2 Security mode set-up procedure : Integrity protection is not turned on

1. if the connection is only for periodic location registration
2. if the connection is only indicating deactivation from the UE
3. if authentication fails and therefore connection is immediately shut down
4. if the connection is for an emergency call and there is neither a USIM nor a SIM in the UE

At uplink, the first encrypted message is the first message sent after the "security mode complete" message has been sent. At downlink the first encrypted message is the one sent after the RANAP security mode complete message has been sent to the CN. Because there are many messages in different layers waiting to be sent at the same time, it is not easy to decide which message should be very first to be encrypted. For this purpose, a specific ciphering activation time parameter is exchanged between the UE and the RNC.

3.6 Interworking with GSM: The UMTS CN is a straight evolution from that of GSM. The radio interfaces are completely different in both systems, but the early terminals still support both, allowing roaming from one system to another and handovers between the systems. As the security features in two systems are different, management of security during interoperation is difficult.

A smooth transition is needed from a pure GSM network to a mixed network that has wide area GSM coverage enhanced by WCDMA islands. A user can use a 3G terminal without the need to change his or her smart card. This results in lower level of security because when a SIM card is used to access UTRAN, no authentication of the network is possible.(This is because of different key lengths).When a 3G subscriber with a proper USIM needs to gain access outside WCDMA coverage, longer keys are compressed by the USIM to 64 bits in order to use GSM encryption.

In 3GPP technical report TR 31.900, all possible interworking scenarios in a mixed 2G/3G environments are systematically studied. There are basic five entities in the system : the security module, terminal, radio network, serving CN and the home network .Each of these entities could be classified as either 2G or 3G. From security point of view, clear-cut division between 2G and 3G for each entity should be defined:

- The security module can be either a SIM card (GSM-2G case) or a UICC(UMTS-3G Case).A UICC may contain a SIM application in addition to a USIM application.
- The mobile equipment (ME) is classified as 2G if it supports exclusively the GSM RAN and interworks with either a SIM card or a SIM application in a UICC. Otherwise the ME is 3G:in which case it supports either UTRAN only or both GSM radio access and UMTS radio access.
- The division of RAN is clear: the GSM Base Station Subsystem (BSS) is used for 2G and UTRAN for 3G.
- The SN VLR/SGSN is classified as 2G if it supports exclusively GSM authentication and can be attached exclusively to a GSM BSS. Otherwise, the VLR/SGSN is 3G.A 3G SN supports conversion functions.
- The HLR/AuC is 2G if it supports exclusively authentication triplet generation for 2G subscriptions A 3G HLR/AuC supports authentication quintet generation for 3G subscriptions and conversion functions to support GSM authentication.

The summary of entire UMTS security mechanism is shown in next figure 3.5.

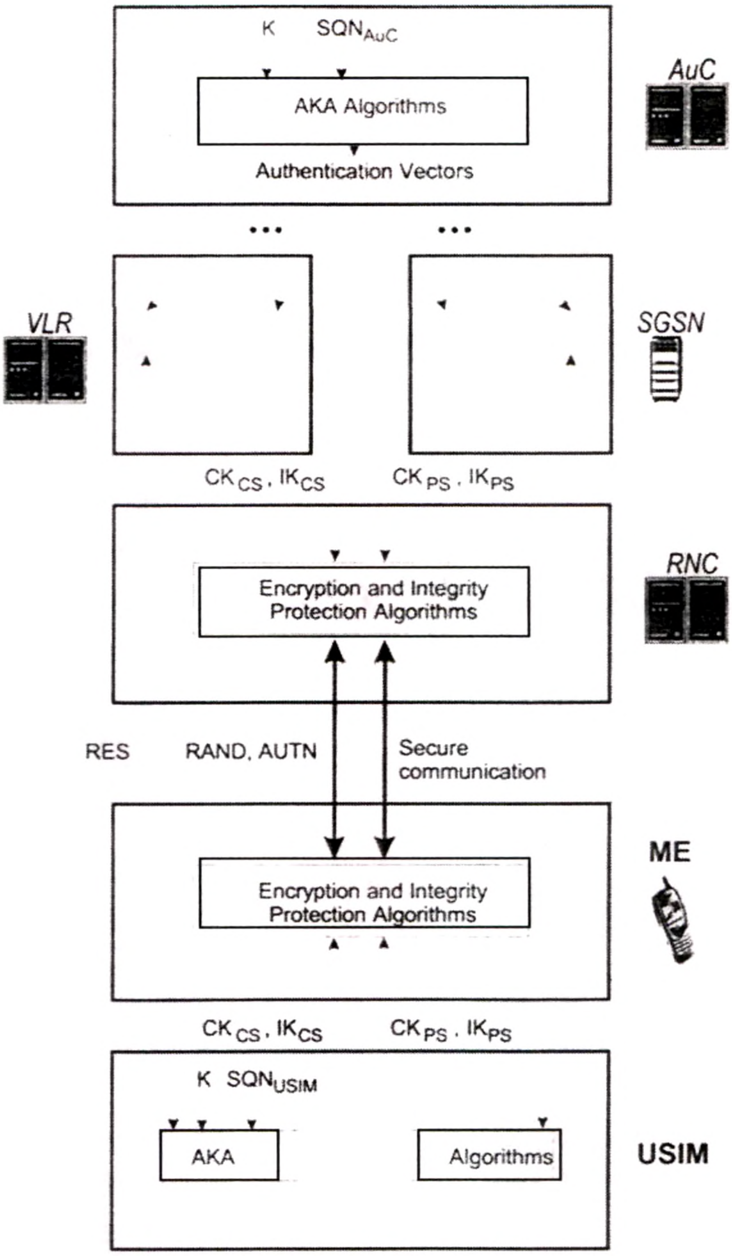

Fig. 3.5 : UMTS access security summary

3.7 Summary : In this chapter, UMTS security features are discussed. The Mutual Authentication and UTRAN encryption methods are discussed in detail. Brief introduction of encryption and integrity algorithms is also given. The chapter ends with discussion of interworking scenario with GSM for mixed 2G/3G environments.