"Security Technologies for Mobile Radio Systems"

This report was written as a part of the MSc Degree in CCDSP at the University of Strathclyde

Ioannis Doukas

Glasgow, 2 May 2003

Department of Electronic and Electrical Engineering

CONTENTS

LIST OF ABBREVIATIONS

AH	Authentication Header
AK	Authentication Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AuC	Authentication Centre
AUTN	Authentication Token Number
3G	Third Generations
3GPP	Third Generation Partnership Project
BSS	Base Station Subsystem
BSC	Base Station Controller
BTS	Base Transceiver Station
CE	Customer Equipment
CK	Confidential Key
CN	Core Network
CS	Circuit Switch
DoS	Denial of Service
EEPROM	Electrically Erasable Read Only Memory
EIR	Equipment Identity Register
ESP	Encapsulation Security Payload
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Centre
GPRS	General Packet Radio System
GSM	Global System of Mobile Communication
HN	Home Network
IK	Integrity Key
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
MAC	Medium Access Control
MAC	Message Authentication Code
MAP	Mobile Application Part
ME	Mobile Equipment

MS	Mobile Station
MSC	Mobile Switching Centre
OSI	Open System Interconnection
PSTN	Public Switched Telephony Network
PKI	Public Key Infrastructure
PLMN	Public Land-based Mobile Network
PS	Packet Switching
P-TMSI	Packet Temporary Mobile Subscriber Identity
RAM	Read Access Memory
RAN	Radio Access Network
RAND	Random Number
RLC	Radio Link Control
ROM	Read Only Memory
RRC	Radio Resource Layer
RNC	Radio Network Controller
RNS	Radio Network Subsystem
SGSN	Serving GPRS Support Node
SN	Serving Network
SQN	Sequence Number
SRES	Signed Respone
SSI	Service Set Identifier
TMSI	Temporary Mobile Subscriber Identity
TLLI	Temporary Logical Link Identity
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
XMAC	Expected Message Authentication Code
XRES	Expected Response

LIST OF FIGURES **Page**

ABSTRACT

Security requirements and services of a mobile communication system differ, due to the radio communication path between the user and the base station. There is no physical link in terms of (fixed) telephone line between the user and the local exchange, which could serve to identify the user for routing and charging purposes. Therefore, authentication is required to stop intruders from taking the identity of somebody else and transferring calls and charges. Eavesdropping on the radio path, intercepting data or tracing the location of a user by listening to the signalling data are additional threats.

First generation analogue cellular phones were designed with minimal security features that became insufficient really fast. Moving to Second generation and GSM systems, solutions to a few important aspects of security such as subscriber authentication, user confidential identity and confidentiality of voice and data was provided. Even though security issues were improved, GSM is still vulnerable to security attacks.

GPRS is an enhancement of GSM network, which can be considered as a step towards 3rd generation mobile systems. Apart from the higher speed rates, GPRS also integrates together telecommunication and data communication worlds. The security issues applied on GSM are improved significantly, but GPRS is still exposed to intruders.

The vast demands from social markets are pushing the development of mobile communications faster and therefore new applications and services are required. Third generation mobile systems (UMTS) can be considered as an answer to the additional requirements, providing even higher speed rates and other enhancements. Moreover new security features are also provided in order to ensure a better level of security. However, the evolution of mobile systems could not stop here. Consequently 4th generation systems research has already started.

This paper gives an overview of the security issues provided in a GSM, GPRS and UMTS network and also draws conclusions to their strengths and weakeness. Furthermore, an introduction on 4G mobile systems and their associated security threats will be provided.

1. GSM SECURITY

1.1 Introduction

The arrival of the 2nd generation digital mobile systems brought the impression that the digital mobile telephones would be secure from eavesdropping in contrast to the first generation analogue mobile systems. Although the situation was improved, there is still some uncertainty about the level of security that is provided. This chapter introduces the Global System for Mobile Communications (GSM) network structure, all the provided security features and possible threats.

1.2 GSM Architecture

In order to appreciate and understand all the security features applied on GSM it is required to give a brief description on the architecture. A GSM system is arranged into three main components, i.e. the mobile station, the base station subsystem and the network subsystem (See Figure 1.1).

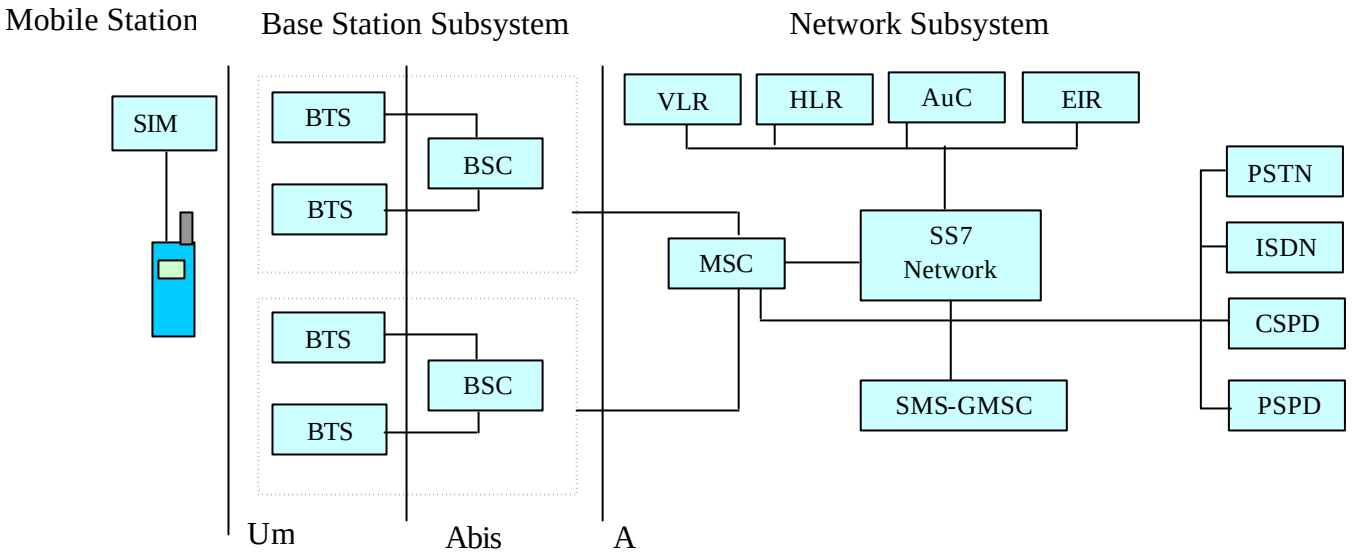

Figure 1.1 GSM Architecture [6]

The Mobile Station Subsystem contains the mobile terminal which includes a SIM card. The Base Station Subsystem (BSS) consists of a number of Base Transceiver Stations (BTS) and a Base Station Controller (BSC). The BTS controls the radio traffic

between the MS and itself through the Um Interface (Air). The BSC controls the BTS communicating over the Abis interface.

The Network Subsystem contains the Mobile Services Switching Centre (MSC) which performs all the necessary applications in order to route calls to and from the mobile users and the various telephone networks such as Integrated Services Digital Network (ISDN) or Public Switched Telephony Network (PSTN). The HLR carries all information concerned with the subscriber for that region of the corresponding GMSC. The Visitor Home Register (VLR) contains temporary details of any visiting mobile to the corresponding MSC [1]. It also carries the TMSI (see later). The Authentication Centre (AuC) is located in the HLR and is one of the most significant security issues as it provides all the necessary data required for authentication and ciphering between MS and BTS.

1.3 User Confidential Identity

When a user logs into a network the identity of the subscriber has to be identified by the network. Instead of sending the subscriber's International Mobile Subscriber Identity (IMSI) which uniquely identifies the subscriber worldwide, a temporary identity (TMSI) is transmitted by MS. The purpose of this TMSI is to deny an intruder the possibility of gaining information on the resources used by the subscriber, preventing of tracing the user's location.

1.4 GSM Subscriber's Authentication

The Authentication Centre (AuC) is used to authenticate the subscriber's SIM card as shown in Figure 1.2. The procedure initiates by AuC which generates a 128-bits random number RAND that is sent to the MS. The received RAND number along with the authentication key Ki (128 bits) that is stored in the SIM card, is implemented by the A3 algorithm to generate a 32-bit Signed RESponse (SRES). The SRES is transmitted back and compared with the expected SRES which is computed by the AuC. The MS is granted access to the network only if the value of the computed SRES from the MS equals the value of the SRES evaluated by the AuC. To provide a better

level of security, on each login occasion, the RAND number is changed and consequently the SRES.

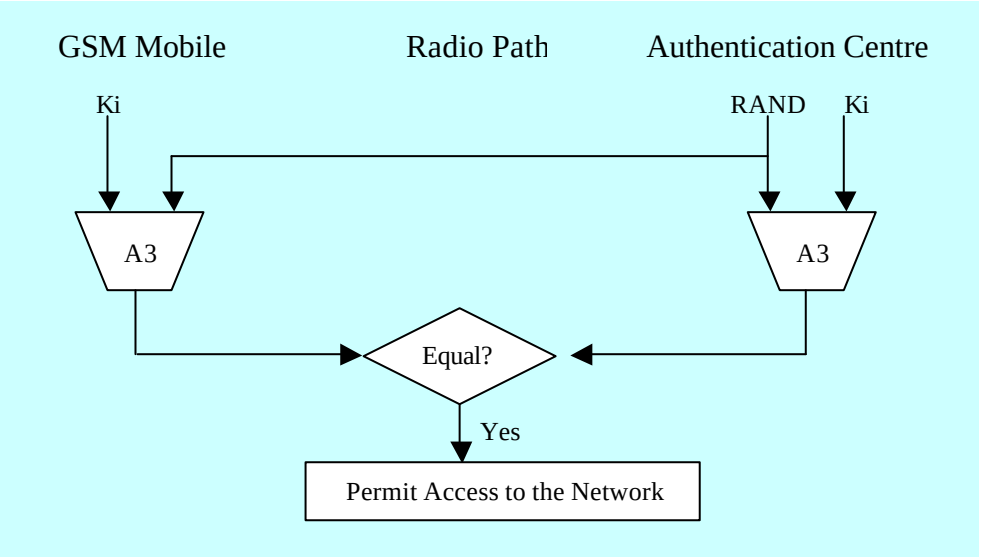

Figure1. 2 Authentication Procedure

1.5 GSM Encryption

The purpose of this security issue is to ensure the privacy of the user information carried in the radio path. After a successful authentication, the user's authentication key Ki along with the RAND number and the algorithm A8 are implemented to generate a 64-bit ciphering key Kc. The algorithm A5 that was derived in the SIM during the authentication process implements this key in order to generate a keystream that ciphers the digitised transmitted voice signal and decipher the received voice signal [1] (See Figure 1.3).

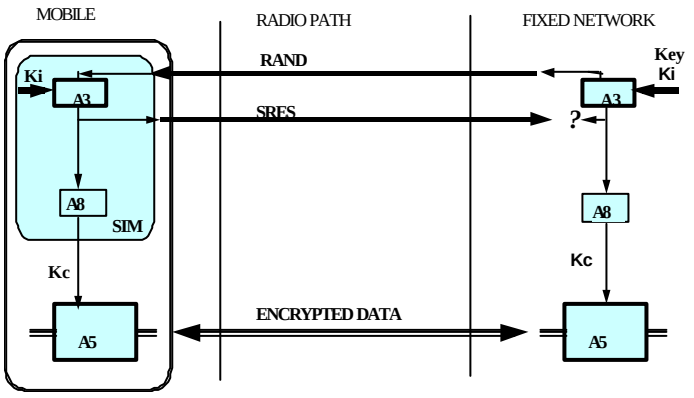

Figure 1.3 Cipher Key generation and enciphering [12]

The enciphering stream at one end and the deciphering stream at the other end must be synchronized, for the enciphering bit stream and the deciphering bit streams to coincide [8]. The complete authentication and ciphering processes are described below in Figure 1.4.

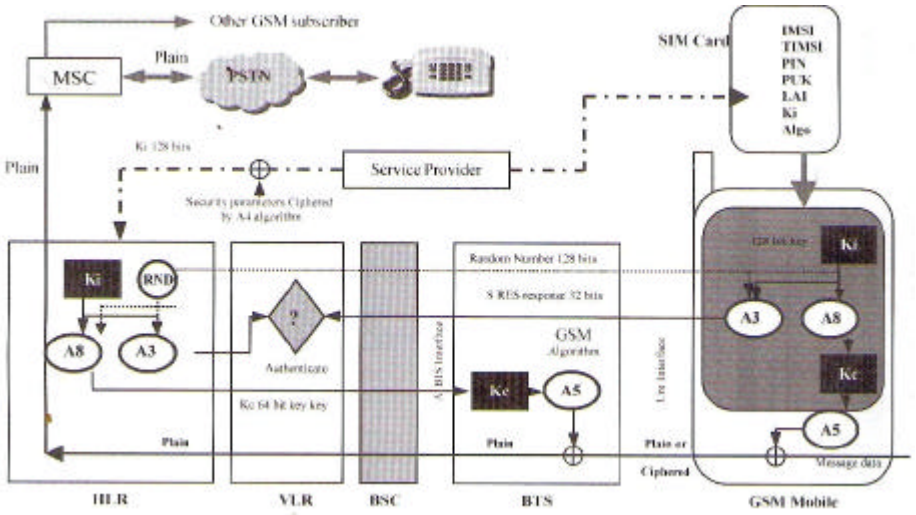

Figure 1.4 Authentication and Encryption Procedure [1]

1.6 The Subscriber Identity Module (SIM)

The SIM is a security device that contains all the necessary information and algorithms to authenticate the subscriber to the network. To achieve its main task of authenticating the subscriber to the network, the SIM contains a microcomputer, which consists of a CPU and three types of memory. The programmed ROM usually contains the operating system of the card, the code for the GSM application and the security algorithms A3, and A8. The RAM is used for the execution of the algorithms and as a buffer for the transmission of data. Sensitive data such as Ki, IMSI, dialling numbers, short messages, network and subscriber information such as TMSI are stored in the Electrically Erasable Read Only Memory (EEPROM) [9].

1.7 Equipment Identity Register (EIR)

The purpose of EIR is to identify whether a mobile device is valid or not. In other words EIR carries serial numbers of all stolen or lost mobiles that must not be authorised by the system. Users are identified as Black (i.e. non valid), White (i.e. valid) or Grey (i.e. under suspicion) [1].

1.8 GSM Security Threats

The most important component of the GSM security is the user's authentication key Ki. A reproduction of this key enables the possibility to clone SIM cards and consequently to monitor any call made by the user that uses that key. However, there is a security mechanism that monitors all the keys and in the case of simultaneous use of the same key a termination of this account occurs.

Generally, a terminal needs to be authorised by a network in order to operate. However, there is no mechanism that checks the validity of the network. Therefore, attacks to the network are possible by somebody who has the appropriate mechanisms required so as to masquerade as a valid network or as a valid user's terminal.

It is also important to note that the point of interface where the MS leaves the somewhat protected path and goes to the PTSN or any other telephone network, is quite significant in terms of security as it is very susceptible to potential intruders [1]. It is also important to ensure that the security applied on the HLR is satisfactory as it contains all the fundamental components of GSM security such as IMSI, subscriber's authentication key Ki, telephone number and billing details.

Another significant issue in terms of security threat might be considered the uncertainty of whether or not the above security procedures are provided by the GSM service providers.

2. GPRS SECURITY

2.1 Introduction

General Packet Radio System (GPRS) is a data network that was designed to coincide with the existing GSM network. More precisely GPRS allows both Packet Switched (PS) such as IP, and Circuit Switched (CS) traffic to coexist on the GSM network. Furthermore, GSM has been updated to a High Speed Circuit Switched Data (HSCSD) that can implement up to four CS channels instead, providing channel capacity up to 40kbs [6]. The purpose of this chapter is to give a description on the GPRS network structure and underline all new security issues that apply on this enhancement.

2.2 GPRS Architecture

In order to understand all the applied security issues and their related weakness, it is required to give a brief description on the structure of GPRS and all of its mechanisms (see Figure 2.1)

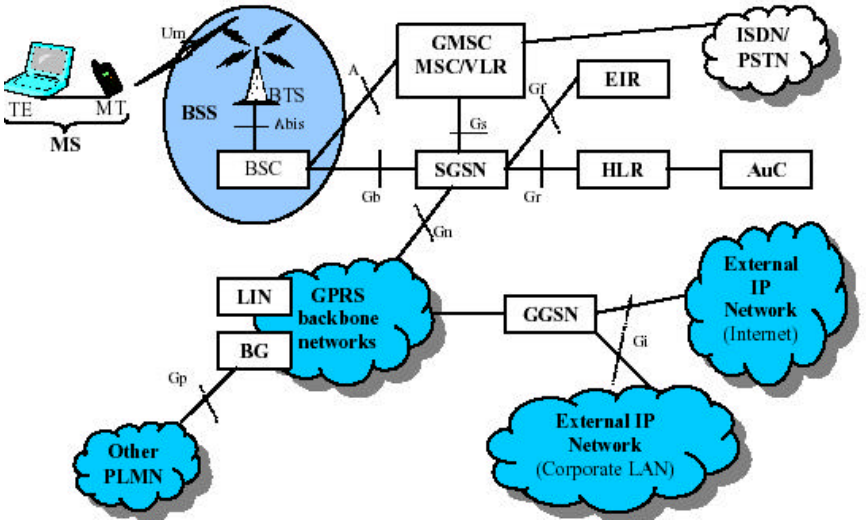

Figure 2.1 GPRS Architecture [10]

The MS consists of a Terminal Equipment (TE) (i.e. pocket pc) and a Mobile Terminal (MT). MS can operate in three different modes depending on the mobile and network capabilities [7].

- Class A mode, can handle both packet switched and circuit switched transmission operations at the same time.
- Class B mode, allows the MS be in either PS or CS mode, but not both. While a MS is transmitting packets, if a CS connection is requested, automatically PS transmission is set on suspend mode.
- Class C mode allows the MS to perform one service at a time. If a MS is supports only PS traffic (GPRS) then it operates in C mode [10].

In the BSS, BTS handles both CS and PS traffic. It forwards the PS data to SGSN and CS to MSC. In addition to the GSM features, HLR is also used to identify if the GPRS subscriber has a static IP address or not, and which access point uses to connect to external networks [7]. For GPRS, subscriber's information is exchanged between HLR and SGSN.

The Serving GPRS Support Node (SGSN) handles the traffic of IP packets addressed to and from a mobile station that is attached within the SGSN service area, and it also provides packet routing and transfer to and from the SGSN service area [10].

The Gateway GPRS Support Node (GGSN) provides connection with external packet switched networks such as Internet or private networks. It is connected with SGSN via an IP-based GPRS backbone network [6]. It also forwards all IP packets and is used in the authentication and ciphering procedures.

The AuC operates similarly as the original GSM network. More precisely, it includes information for identifying authorized users of the GPRS network and thus prevent unauthorized use of the network.

2.3 GPRS Subscriber's Authentication

The GPRS authentication procedure is performed in the same way as GSM with the difference that the procedures are executed in the SGSN instead of MSC. In other words SGSN authenticates the MS using the authentication data that retrieves from the HLR.

2.4 GPRS Encryption

In GPRS the ciphering procedure is different than the GSM. A new algorithm 64-bit A5-GPRS is used instead.

During transmittance of IP packets, each data is ciphered by the GPRS-A5 algorithm. The ciphering process is performed between the SGSN and the MS. Again synchronisation between the enciphering and deciphering stream is necessary. Synchronisation is performed by a ciphering key sequence algorithm and by ensuring that the input and direction bits drive the GPRS encryption algorithm as illustrated in Figure 2.2.

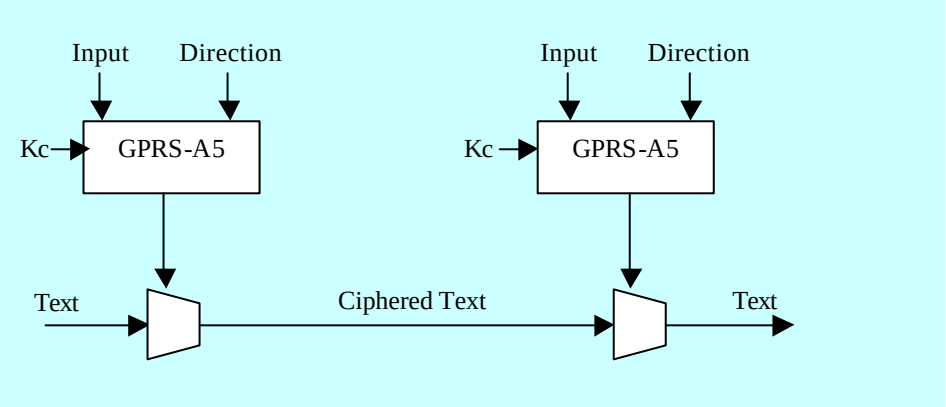

Figure 2.2 GPRS Ciphering Procedure [10]

2.5 GPRS User Confidential Identity

GPRS uses the same procedure to identify a subscriber with the only difference that the MS sends a Temporary Logical Link Identity (TLLI) and Routing Area Identity (RAI) to the SGSN, which handles the procedure instead of MSC. The TLLI must be accompanied by a RAI to avoid ambiguities [6].

2.6 GPRS Security Threats

Mobile phones can face similar threats as the personal computers connected to a network. It is possible for an attacker to view, modify and implement applications or stored data in the mobile. Not only the terminal, but also the SIM card might be exposed to an intruder in the same way.

However, a security mechanism called IPSEC was obtained in order to solve the security weakness of IP. This is performed by protecting both the integrity and confidentiality without changing the interface of IP [11]. One of the IPSEC's drawbacks is the excessive cost and overhead traffic that creates [11].

Another important point in terms of security is the radio interface between the MS and the SGSN (air interface). The transmitted information might receive attacks by intruders. By manipulating this information it is possible to give access to valuable secure data such as authentication keys or produce disturb on the network's performance.

GPRS is also vulnerable to intruders who can masquerade as a potential network or terminals using the appropriate mechanisms.

Another possible threat that a subscriber might phase is the Denial of Service (DoS). This is performed by generating disturbing traffic to the network with the consequence of not allowing users from accessing network services. This kind of attack is discussed in more details in the following section.

3. UMTS SECURITY

3.1 Introduction

Universal Mobile Telecommunications System (UMTS) is a new mobile communication system, which will be a significant innovation over today's system because of its high operating flexibility, and its ability to provide a wide range of applications that cannot be covered by second generation (GSM) systems.

The following chapter gives a brief description on the UMTS architecture, while a more detailed discussion is made on the security features that are used along with a number of possible attacks that 3rd generation might accept.

3.2 UMTS Architecture

A UMTS network consists of three main sections: The User Equipment (UE), UMTS Terrestrial Radio Access Network (UTRAN) and Core Network (CN) as shown in Figure 3.1. The UE includes three equipments: The terminal equipment, the mobile equipment and the UMTS Identity Module. The UTRAN consists of Radio Network System (RNS) and each RNS communicates with various Base Stations. The section CN handles both PS and CS traffic using the PS domain and CS domain respectively.

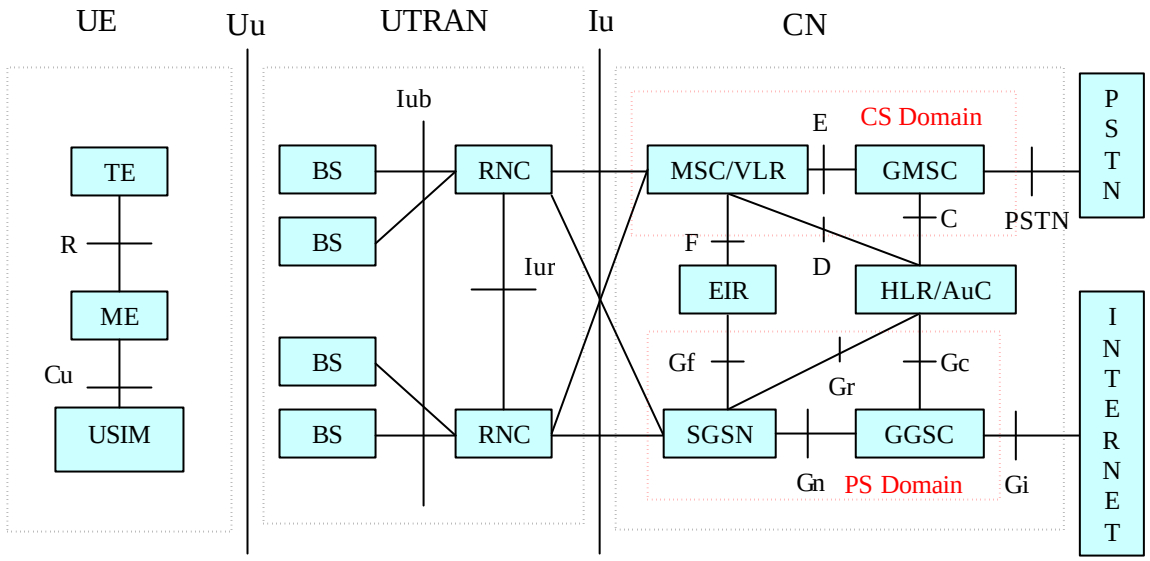

Figure 3.1 UMTS Structure [13]

3.3 UMTS User Authentication (Mutual)

In order to provide authentication on UMTS network a consideration of three entities is required. These are the Home Network (HN), the Serving Network (SN) and the USIM.

The SN verifies the subscriber's identity in the same way as in GSM, while the terminal ensures that the SN has been authorised by the HN to perform this. However, it should be mentioned that although authentication cannot prevent the masquerade of an intruder it ensures that the attacker cannot take advantage of this situation [2].

The authentication procedure is performed just after the identification of a subscriber by the serving network. This is done when the VLR (case of a CS) or the SGSN (PS case) sends an authentication request to the AuC. Then, the SN sends a user authentication request to the terminal. This request contains the RAND and the Authentication Token Number (AUTN) parameters which are transmitted into the USIM.

USIM includes a master key K (128 bits) that is implemented along with the two received parameters (RAND, AUTN) in order to compute a user response parameter RES. The computed user's 168-bit RES is then sent back to the HN and compared with the expected response XRES, which is produced by the AuC. If these two parameters match, authentication occurs. This process is depicted in Figure 3.2.

It should be noted that along with the RES parameter three more parameters are generated. Two of these parameters are the Ciphering Key (CK) and Integrity Key (IK) which are used for encryption and integrity protection respectively. The last and very important generated parameter is the Sequence Number (SQN), which ensures that the authentication vector used for ciphering the authentication process is unique and has not been used before [2]. This whole process is also known as Authentication and Key Agreement (AKA).

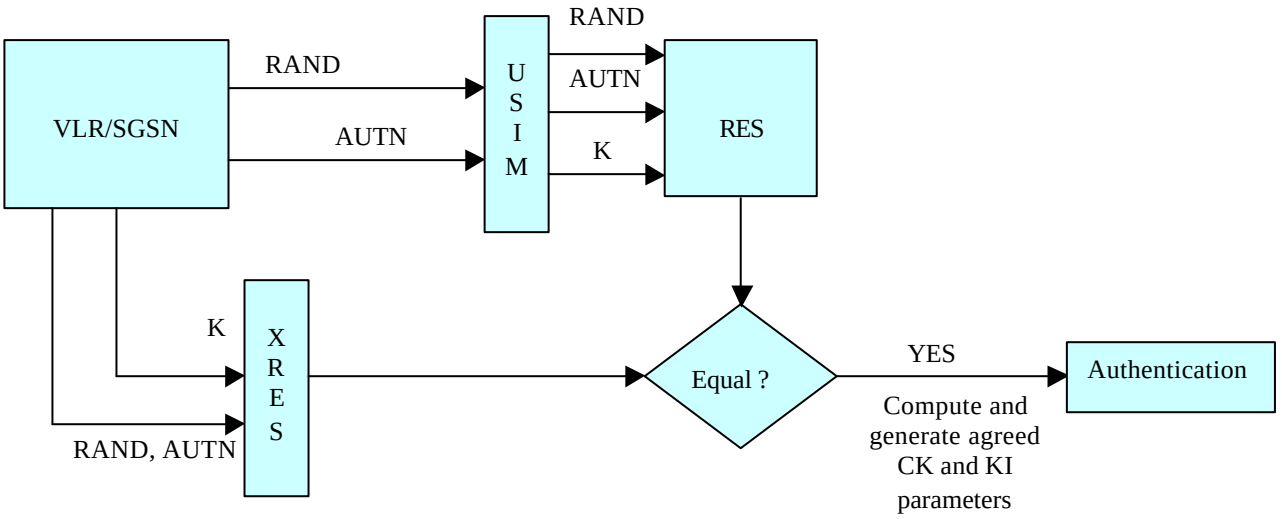

Figure 3.2 Authentication Process

3.4 Authentication Cryptography

The process initiates by choosing a proper SQN, preferably in an increasing order. Along with SQN parameter, a 128-bit RAND number is produced as well. It is significant to mention that the authentication vector is one-way function meaning that is not possible for the process to be inverted. In other words, if the authentication vector is known, it is not plausible to derive any of the inputs.

For the production of the authentication vector, five functions are required. These one-way functions are: f1, f2, f3, f4, f5 as shown in Figure 3.2. The function f1 is produced by four input parameters; the master key K, the SQN and the authentication management field AMF parameter [2]. The rest functions (f2-f5) are produced by the parameters K and RAND [2]. It is important that these functions differ from each other in order to be impossible to identify the output of any functions if one is known. The output of the function is a 64-bit parameter called Message Authentication Code (MAC) and the outputs of the functions f2, f3, f4, and f5 are XRES (32-128bits), CK (128 bits), IK (128 bits), and a 64 bit Acknowledgement Key AK respectively [2].

Finally, the produced parameters RAND, XRES, CK, IK and AUTN construct the authentication vector (See Figure 3.3).

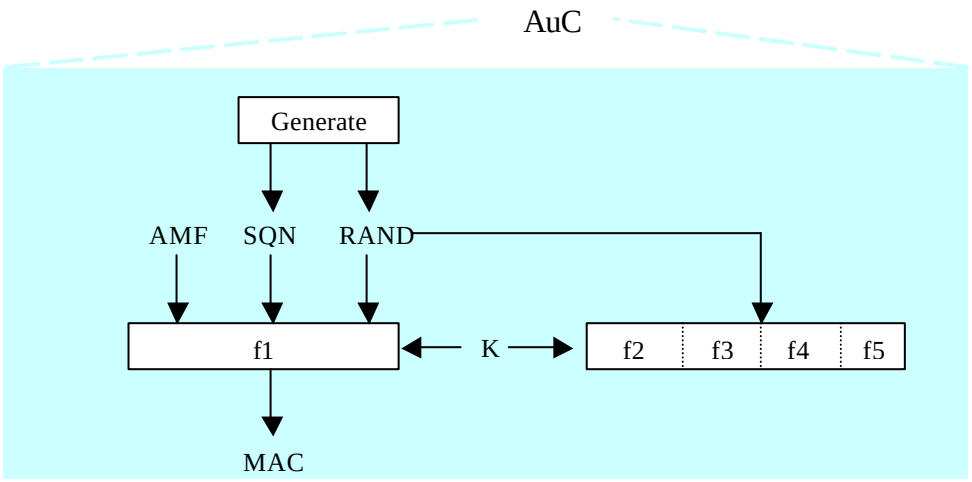

Figure 3.3 Generation of the authentication vector [2]

Furthermore, a more detailed discussion about the process of authentication on the USIM card follows in order to provide a better understanding of this important process. It is important to mention that the function f5 needs to be calculated before f1 as it conceals the SQN, which is required for the production of f1 [2]. Again this is done in order that the eavesdropper won't have the chance to get any information about SQN. As it can be seen from Figure 3.4, the XMAC which is produced from the function f1 is compared to the received MAC by the network as a part of the Authentication Token Number (AUTN). In the case that both parameters (MAC-XMAC) agree it can be considered that an entity that knows the master key K created both RAND and AUTN, which in our case is the AuC of the user's home network [2].

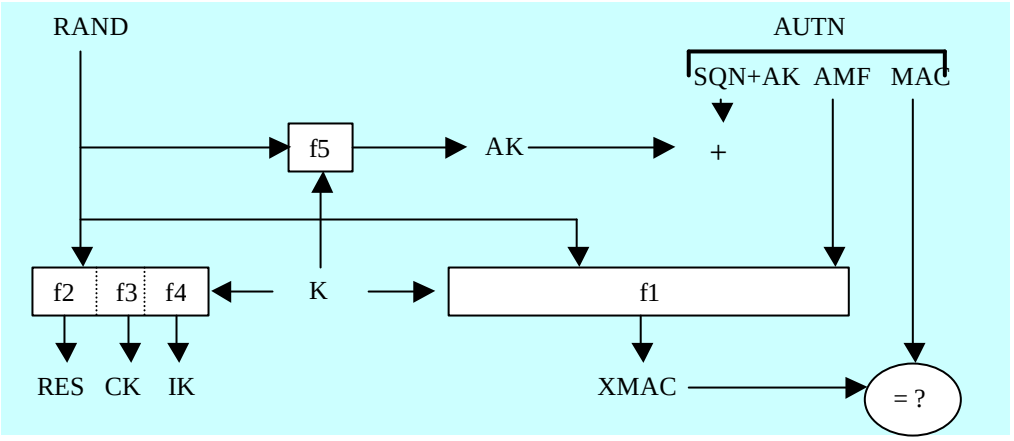

Figure 3.4 USIM Authentication [2]

The most significant components in terms of security are the K and the SQN, which are stored in both the USIM and AuC, and never transferred out of these two locations. It is also necessary that these parameters are maintained in a synchronised manner on both sides.

3.5 UTRAN Encryption

After both user and the network authentication, a secure communication can start. In order that encryption can occur, both communicating parties have to agree on the encryption algorithm that is going to be used and fortunately only one algorithm is defined [2].

The ciphering process is performed in the terminal and in the Radio Network Controller (RNC). Consequently the CK is transferred from the CN to the RAN. After RNC has obtained CK, it switches on the encryption mode by sending an RRC security command to the terminal [2]. In UMTS encryption, the plaintext data is added bit-to-bit to random looking mask data that is generated by the CK and some other parameters [2] as shown in Figure 3.5. A great advantage of this encryption is that the mask data can even be generated before the actual plaintext is known [2]. Therefore, the final encryption is executed really fast. The decryption is performed in a similar way as encryption.

Since the product of the data mask is not dependent on the text, another input parameter is required in order that the mask would be different for different key streams.

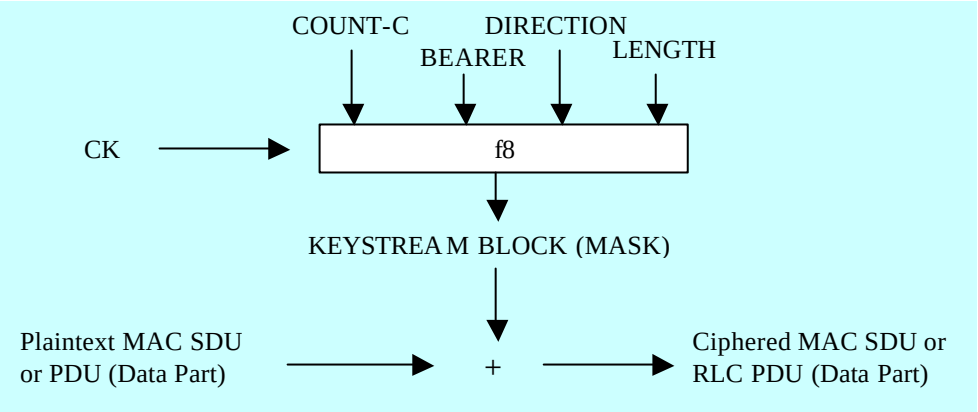

Figure 3.5 Stream Cipher in UMTS [2]

3.6 Integrity on RRC Signalling

The purpose of integrity protection is to authenticate individual control messages [2]. This is performed on the RRC layer between the terminal and the RNC. The IK that was generated in the authentication process is transferred to the RNC along with the CK in security mode command [2]. As illustrated in Figure 3.6 the function is represented by f9 and its output is a 32 random bit called MAC-I. The MAC-I is added to each RRC message and is also generated on the receiving side [2].

The COUNT-I parameter resembles to the counter that is used for encryption [2]. The parameter FRESH is produced by the RNC and is used to protect the network against maliciously chosen start value for COUNT-I [2].

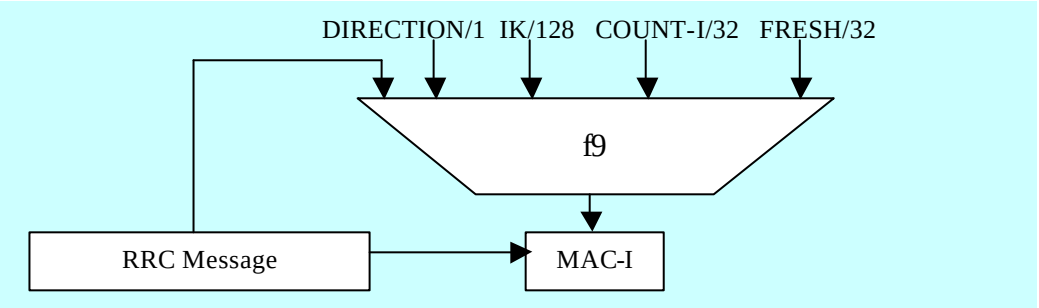

Figure3.6 Message Authentication Code [2]

3.7 Network Security

The most significant feature that is used for the protection of network domain traffic is the IPSEC protocol [2]. It provides confidentiality and integrity of communication in the IP layer. Communicating parties can also authenticate each other using IPSEC [2]. In addition to the protection of IP-based network, a specific security mechanism called MAPSEC has been developed to protect existing signalling protocols and applications.

3.7.1 IPSEC

The main parts of IPSEC are the Authentication Header (AH), the Encapsulation Security Payload (ESP) and the Internet Key Exchange (IKE).

IPSEC is used to protect IP packets. This is performed by ESP which provides both confidentiality and integrity protection, while AH provides only the latter [2]. Both ESP and AH require keys to perform authentication and encryption of the packets. Consequently a negotiation of these keys must be performed before ESP and AH can be used [2]. This is performed in a secure way by IKE which is based on the idea of public key cryptography where secret keys for secure communication can be exchanged over an insecure path [2].

"There are two ESP modes, transport mode and tunnel mode. In transport mode everything in an IP packet is encrypted except the header. Then a new ESP header is added between the IP header and the encrypted part. Finally a message Authentication Code (MAC) is calculated over everything except the IP header and placed at the end of the packet. The receiving part integrity is being performed by removing the IP header from the beginning of the packet and the MAC from the end of the packet. Then by running the MAC function and comparing it with the result to the MAC in the packet, if the outcome of the integrity is positive the ESP header is removed and the remaining part is decrypted" [2]. This process is shown in Figure 3.7.

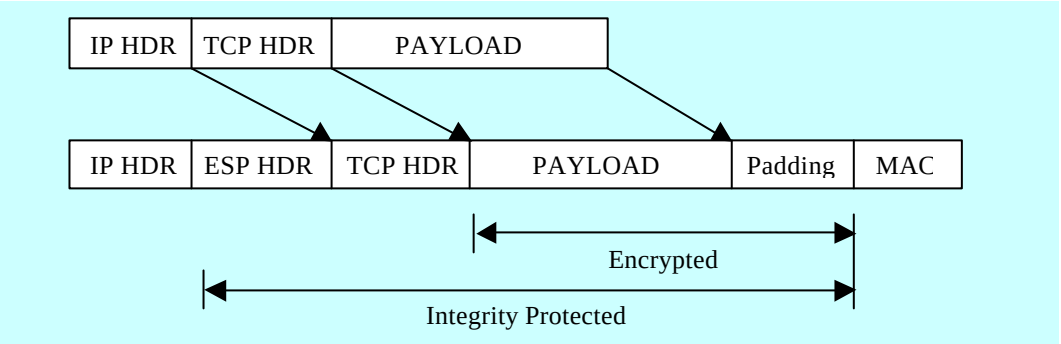

Figure 3.7 Transport Mode [2]

"In the tunnel mode a new header is added to the beginning of the packet and then all the operations performed in the transport mode are carried out for the new packet (See Figure 3.8). This means that the IP header of the original packet is protected" [2].

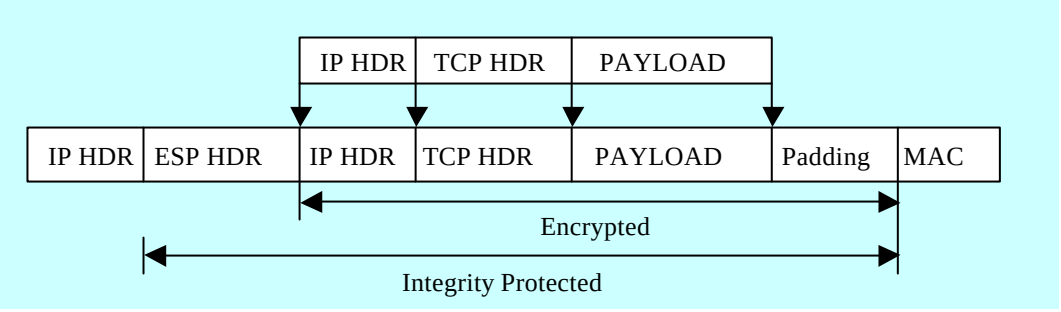

Figure 3.8 Tunnel Mode [2]

ESP communication between two end points uses the transport mode. In order for this to be performed, it is required that the communicating parties know the IP address of each other and implement all the IPSEC functionality [2].

The typical use case of the tunnel mode is related to the concept of a VPN. The preferred protection method for core network control messages is to use ESP in the tunnel mode between security gateways [2].

3.7.2 MAPSEC

MAPSEC's purpose is to protect confidentiality and integrity of Mobile Application Part (MAP) operations [2]. MAPSEC protection operates in three different modes. In the first no security is guaranteed. In the second mode only integrity is protected, while in the third both confidentiality and integrity is provided.

"For confidentiality the header of the MAC operation is encrypted. A security header is added in order to indicate how decryption should be done. For integrity, again a MAC is calculated over the payload of the original MAP operation and the security header. A time variant parameter is also used to prevent replay attacks" [2].

3.8 UMTS User Confidential Identity

The identification process in UMTS uses the same permanent identity (IMSI) as in GSM. However, UTRAN identification is performed using the temporary (TMSI) in CS traffic and P-TMSI in PS traffic. A registration though is required at the beginning of subscription since the network will not know the permanent identity of the user.

Once the user has been identified by the SN, a TMSI and P-TMSI is provided by SN ensuring that each user is using different identity and maintains the relation between the IMSI and TMSI [2]. The provided TMSI is transferred to the user after the encryption has been activated. This TMSI is used till the point a new TMSI is allocated by the network [2]. When a new TMSI is allocated and acknowledged by the network, the old temporary identity is removed from the VLR or SGSN. In the case that an

acknowledgment has not been received, VLR/SGSN keeps both TMSI and accept either of them.

3.9 UMTS Security Threats

A typical type of attack is the effort of trying to gain access to a terminal. The user can protect himself/herself by setting a PIN. Electronic eavesdropping (i.e. Sniffing) is another commonly used attack method and is very difficult to be detected and prevented. With sniffing the hacker tries to get valuable information such as user ID and password. Unfortunately sniffing programs are available in the Internet to be downloaded by anyone. In the wrong hands it is a powerful tool [2] which allows the monitoring of the network.

The information collected by the sniffing can be implemented using the spoofing method. This method allows the attacker to use someone else's IP address and receive packets from the other users [2]. This could be a great menace for companies where the employers and their customers exchange data over the Internet.

One step further the spoofing is the hijacking session. There the attacker tries to take over the existing connection and even the stronger authentication mechanisms cannot prevent against hijacking [2].

Another type of attack is the Denial of Service (DoS). The intruder tries to cause harm and inconvenience to users and service providers. This is done by generating disturbing traffic which can jam the target server so as not to be able to provide service anymore [2]. This can be done by sending a huge number of requests and then ignore all the acknowledgments that the server sends back. When the buffer that contains all the connection attempts is continuously filled with new requests, the server stacks [2].

4. INTEROPERATION BETWEEN 2G AND 3G

4.1 Introduction

With the introduction of 3G networks it is necessary to provide mechanisms that will give the opportunity for interoperation between 3G and 2G networks. More precisely, it will be important for the two networks to be able to cooperate with each other. Dual-mode handsets are therefore required for the 2G users in order to access the UMTS network. However, undoubtedly, problems will occur when a 2G subscriber will try to register with the UMTS or the opposite.

In this chapter, a discussion will be concentrated on the scenarios required in order for the two networks (2G, 3G) to interoperate with each other.

4.2 Roaming Cases

There are two fundamental cases required in order that the roaming procedures (moving from 3G to 2G or vice versa) can be performed. In the first case the 3G VLR should be able to control both 2G and 3G RAN's while, in the second case a 2G is required to control only 2G RAN. Both cases are illustrated in Figure 4.1.

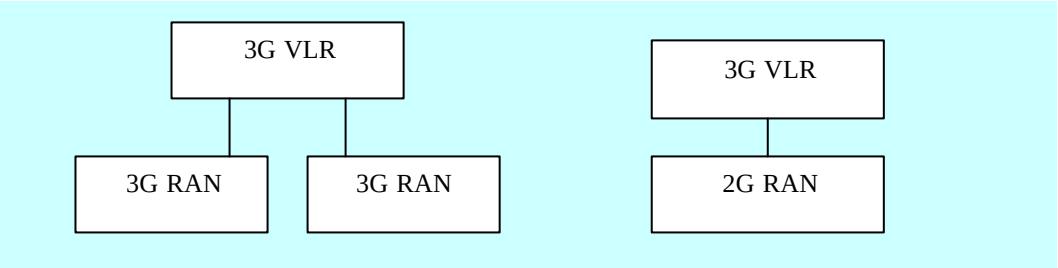

Figure 4.1 Hybrid Network Architecture [14]

4.2.1 Interoperability for UMTS users

The scenario that can be applied in order for an UMTS user requests access to 2G or 3G radio access network is illustrated in Figure 4.2. The UMTS HLR/AuC generates a RAND parameter which is used to derive the parameters XRES, AUTN, Kc, Ki.

Furthermore, the construction of the authentication vector depends whether the VLR controls both UTRAN and GSM Base Station Subsystems or only GSM BSS. In the first case (3G RAN) the authentication vector is derived directly. However, in the second case (2G RAN) the GSM VLR receives the required parameters RAND, SRES, and Kc which are constructed by the HLR/AuC by compressing the long UMTS values (i.e. CK=128-bit, XRES 128-bit) to the appropriate GSM values (i.e. Kc=64-bit, SRES 32-bit).

When a UMTS user requires authentication in a 3G RAN (UTRAN) the controlling VLR performs the authentication and key agreement procedure. On the other hand if a 3G subscriber is handed over an area controlled by a 2G network, authentication is performed by the associated VLR which initiates the authentication procedure and key agreement using the corresponding authentication vector.

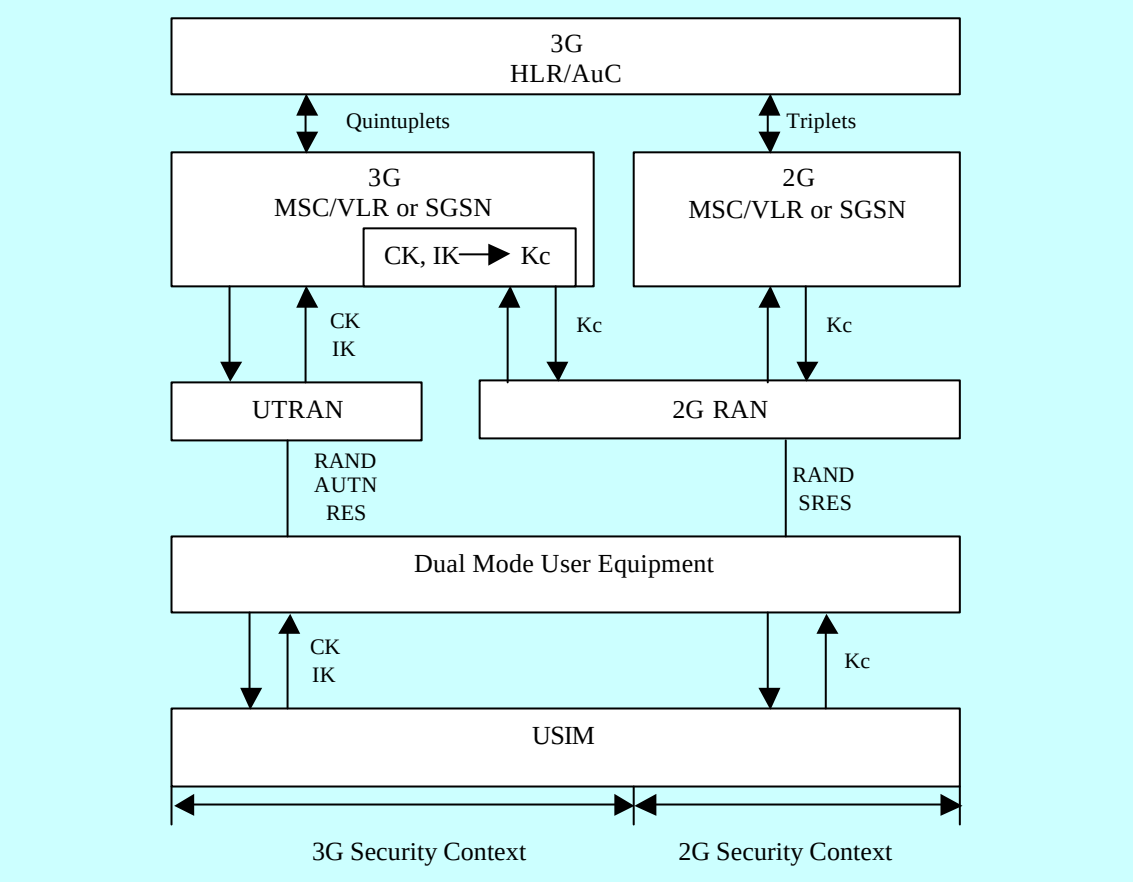

Figure 4.2 UMTS Subscriber Roaming [13]

4.2.2 Interoperability for GSM/GPRS Users

In the case that a GSM subscriber requires access to a 2G or 3G network, another scenario is applied as depicted in Figure 4.3. The HLR/AuC generates an authentication that is derived by the RAND, SRES, and Kc parameters. In addition, the HLR/AuC distributes the authentication vector regardless of the type of VLR's [14]. However, the part of the user authentication is more complicated. If a GSM subscriber needs to move into a 3G network, the user authentication in the 3G RAN (UTRAN) is performed by the VLR which sends a RAND parameter to the user. The user's equipment (Dual mode) implements the received RAND along with other parameters (discussed in Section 1.4) and produces the SRES and Kc parameters. The derived SRES is sent back to the VLR and compared with the expected SRES that is derived by the HLR. After successful match of these two parameters an agreement is applied, based on the cipher key Kc that is going to be used. The controlling 3G VLR along with the user's equipment are then derive the UMTS security parameters (CK, IK) by decompressing the corresponding GSM values to the appropriate UMTS. On the other hand, if the GSM requires authentication in a 2G RAN then the controlling VLR initiates authentication and key agreement directly [14].

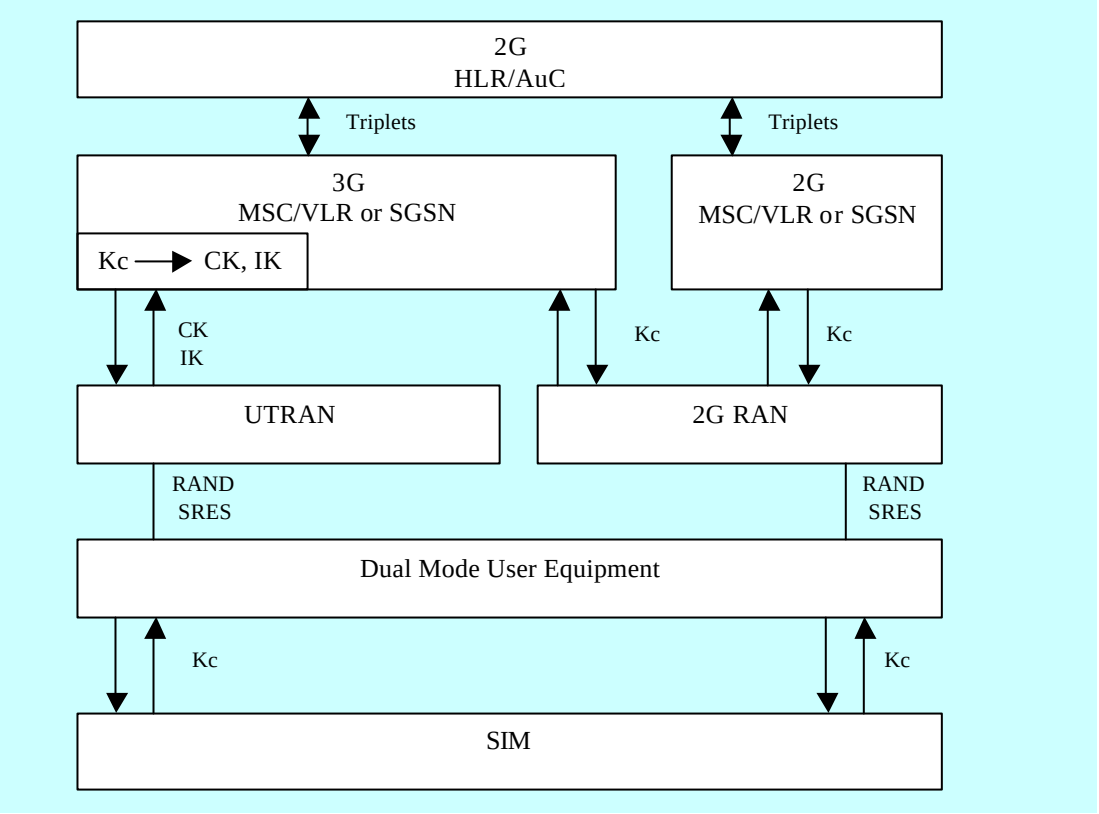

Figure 4.3 GSM Subscriber Roaming [13]

5. 4TH GENERATION MOBILE COMMUNICATION SYSTEMS

5.1 A Vision of 4G

After the deployment of the 3G network it is implied that further research is going to take place, as it is not possible for the UMTS to satisfy all the security issues and subscribers services.

Fourth generation mobile communications involves a combination of various concepts and technologies. Some can be identified and derived from 3G, while others involve new approaches concerned with Wireless Local Area Networks applications.

Therefore, technologies beyond 3G imply a movement toward a new wireless world that is in total convergence of wireless mobile and wireless access communications. These converged broadband wireless systems are the future trend in the wireless industry in consideration of the emerging issues on spectrum efficiency, dynamic bandwidth allocation, secure wireless application, improved quality of service, revolutionary digital transceiver technologies, and so on [15].

At the time of writing, the deployment of 3rd generation mobile communication system has just started and therefore the above considerations cannot be addressed in terms of security as they are still in progress. However, it would be helpful to provide an introduction on WLAN applications in terms of security threats.

5.2 WLAN Security Threats

Wireless LAN rely on radio waves and therefore are susceptible to any kind of eavesdrop. In fact, most WLANs don't implement any form of reliable security, enabling access to almost everyone [16].

Most of the wireless standards use spread spectrum technology, a modulation technique where the transmission signal is spreading over a wide range of the radio spectrum [17]. Spread spectrum is capable of implementing the spreading codes in such a way

that it is nearly impossible to decrypt the transmitted signal unless the code is known [16]. Unfortunately, the 802.11 standard describes these spreading codes publicly with result to be reachable to attackers.

Furthermore, 802.11 standard also specifies the Service Set Identifier (SSID) in order to allow only authorized users to access the LAN. More precisely, only if the user's Network Interface Card (NIC) have the same SSID as the access point can be authorised to access the network. The use of SSID is weak in terms of security since the access point broadcast the SSID within each transmitted data [16]. An intruder can easily monitor frames that are sent over the WLAN (sniff) and detect the SSID.

Wireless LAN also includes a Wired Equivalent Privacy (WEP) which ciphers every frame individually. This can be considered as an additional option for preventing an intruder to access sensitive data such as user names, passwords, documents and e-mails. However, the encrypted WEP information can be tracked again similarly by monitoring the network. Consequently, it is not effective to rely on WEP protection but this can be improved by changing the key frequently.

Another form of security attack is the Denial of Service (DoS). There, the intruder might not decrypt any information from the users but will try to prevent a user to access the network's services (described in section 3.9). This can be done by producing interferences within the radio frequency (RF) [16]. The 802.11 MAC layer avoids transmitting when senses other RF activity and therefore allows attackers to keep users from accessing network services [16].

6. CONCLUSIONS AND DISCUSSION

Security is one of the most important issues that a mobile network should support in order to provide appropriate privacy to subscribers. More precisely it should be able to protect users against billing fraud and generally against all kind of frauds, while information and user details must be encrypted in such a way that will be available only to the correct receivers, preventing any potential eavesdropper.

The most fundamental mechanisms required to provide all the above services are the confidential identity, identity authentication and signalling data confidentiality (encryption). The objective of confidential identity is to provide privacy to user so as to prevent the identification of the person by listening to the signalling channel. In addition, authentication is used in order to identify the user who is using the system for billing purposes, and permit only access to the appropriate users preventing intruders from taking over the connection. Furthermore, signalling protection is applied in order to protect the sensitive user's data that is transmitted over the radio path.

First generation analogue cellular phones were designed with minimal security features that became insufficient really fast.

Consequently, the second generation (GSM) was deployed with main objective to provide a more satisfactory security. Mechanisms such as confidential identity, user's authentication and signalling encryption were introduced, which were implemented using strong algorithms. However, the main disadvantage of the provided security was the fact that all the significant security issues (i.e. Keys, Algorithms) were transmitted over the radio path unprotected. In addition, an intruder with the appropriate mechanisms could masquerade as a potential network or as a user and steal important information. The use of radio frequencies at the transmission media allows a number of potential threats from eavesdropping the transmissions. It is obvious that the weakest part of the system is the radio path, as this can be easily intercepted. Consequently, security was not efficient as there was a possibility of breaking it by various bodies.

However, it is important to mention that the main objective of security for GSM system was to make the system as secure as the public switched telephone network. Therefore in this aspect GSM not only succeeded but also provided a much superior speech quality, and a variety of new facilities and services. The security mechanisms specified in the GSM standard make it the most secure cellular telecommunication system available. For all these reasons GSM is considered as the most successful mobile network in our days.

GPRS is undoubtedly a very important step towards the evolution of third generation mobile networks. It is a based on packet switched traffic that can provide Internet services. More or less, GPRS is using similar security technologies in relation to GSM network. However, data packets do not arrive at a BTS as a sequence, plus the fact that a new algorithm A5 encrypts the traffic makes GPRS undoubtedly a more secure network. Threats to the GPRS network are very different from the Circuit Switched GSM. The GPRS system are a much more exposed to intruders, because of its IP based backbone.

Third generation mobile systems are based on the success of the GSM/GPRS networks and introduce new and enhanced security features in order to improve security and protect new services that cannot be covered by second generation mobile systems. The confidentiality of voice call is protected in the radio access network as well as the confidentiality of transmitted user data.

The most important security enhancement is that not only the subscriber needs to be authorised by the SN, but SN must be authorised by the associated HN as well. In addition, the most significant component in terms of security is the master K that is shared between the UMTS network and user's USIM card and never transferred out of these two locations. Furthermore, other important security issues are transferred through the radio path encrypted and therefore secured from eavesdropping.

The authentication mechanism is performed generating an Authentication Vector, which is one-way function. This means that if the authentication vector is known, it is

not possible to derive any of the inputs. The mechanism also provides the exchange of the CK and IK. CK is extended to 128-bit making it more difficult to break.

Moreover, IPSEC improves the security at the network layer of the IP based core network and MAPSEC protects existing signalling and applications. All security mechanisms together make the security for UMTS to look quite improved, compared to the 2G systems.

It is important to state that the UMTS is not being used in a real time and thus additional security threats will be faced and further improvements will be applied on the security mechanisms. Furthermore, the success of UMTS will depend on the interoperability between 2G and 3G networks and consequently this is going to have consequences to the level of security as 2G security won't be able to support some of the 3G security issues.

The deployment of third generation does not imply that the evolution of the mobile systems could stop here. Research on the 4G mobile systems has already started. 4G networks can be considered as a combination of 3G network and WLAN applications. According to the WLANs there exist some mechanisms that attempt to provide an efficient level of security (i.e. SSID, WEP etc). However, intruders who listen to the transmission path can easily intercept the provided security. Therefore further improvements and mechanisms will be required.

It is also important to state that it is uncertain whether or not the corresponding network providers use all of the security features. Subsequently an additional threat is introduced. However, many network providers are obliged by the government to have little choice in this matter.

The most secure mobile communication is performed using strong algorithms supported by efficient secure key management between end-to-end parties and not from point-to-multipoints (public communication). This kind of communication is used for military purposes.

Closing, it is important to mention that during the writing of this report and especially for the UMTS chapter, there weren't enough information on the provided security features. The most electronic resources concerned with this topic were more or less copying the information from the book [2]. However, a great effort was made in order to make this report as unique as possible. Furthermore, the reader is expected to have a basic knowledge on the functionality of GSM, GPRS and UMTS networks. These can be found in [3], [4] and [5] respectively.

BIBLIOGRAPHY

BOOKS:

[1]. R.J. Sutton, "Secure Communications: Applications & Management", John Willey & Sons, Ltd, 2002.

[2]. H. Kaaranen, S. Naghian, L. Laitinen, A. Ahtiainen, V. Niemi, "UMTS Networks: Architecture, Mobility and Services", John Wiley & Sons, 2001.

[3]. J. Eberspacher, H. J. Vogel, "GSM: Switching, Services and Protocols", John Willey & Sons Ltd, 1999.

[4]. C. Andersson, "GPRS and 3G Wireless Applications", John Willey & Sons Ink, 2001.

[5]. F. Muratore, "UMTS: Mobile Communications for the Future",John Willey & Sons Ltd, 2001

PAPERS:

[6]. C. Peng, "GSM and GPRS Security", Helsinki University of Technology, 2000.

[7]. J. Rautpalo, "GPRS Security-Secure Remote Connections over GPRS", Helsinki University of Technology, 2000.

[8]. L. Huovinen, "Authentication and Security in GPRS Environment: An Overview", Helsinki University of Technology, 2000.

[9]. V. Khu-Smith, C.J Mitchell "Enhancing e-commerce security using GSM authentication", Royal Holloway, University of London, 2002.

[10]. G.S. Bjaen, E. Kaasin, "Security in GPRS", Adger University College, 2001.

[11]. C. Bettstetter, H.J. Vogel, J. Eberspacher, "GSM Phase 2 + General Packet Radio Service GPRS: Architecture, Protocols and Air Interference" IEEE, 1999.

[12]. C. Brookson, "GSM (and PCN) Security and Encryption", Charles Brookson, 2000.

[13]. K. Howker, Vodafone, "USECA: UMTS Security Architecture", USECA, 2001.

[14]. S. Putz, R. Schmitz, “Secure interoperation between 2G and 3G mobile radio networks”, 3G Mobile Communication Technologies, First International Conference on (IEE Conf. Publ. No. 471), 2000.

[15]. B.G. Evans, K. Baughan, “Visions of 4G”, Electronics & Communication Engineering Journal, Volume: 12 Issue: 6, 2000.

ELECTRONIC PAPERS:

[16]. J. Geier, “Minimising WLAN Security Threats”, Tutorials 802.11 Planet, Available http://www.80211-planet.com/tutorials/article.php/1457211, 2002.

[17]. A. Carve, “802.11 and Spread Spectrum”, Network Magazine, Available http://www.networkmagazine.com/article/NMG20000726S0001, 1997.