SECURITY ASPECTS OF THE CELLULAR COMMUNICATIONS

Metodi POPOV

Introduction

Important aspects of protection and security of the cellular radio systems and networks are discussed in this paper. It is shown that Public Land Mobile Networks (PLMN) need a higher level of protection than traditional telecommunication networks.

At an early stage in the development of the mobile radio systems and networks, it was apparent that the weakest part of the system was the radio path. To protect the system against unauthorized use of its resources and easy eavesdropping with radio equipment, it is necessary to perform two procedures concerning authentication of the users and their equipment and ciphering the user's information and data.

The cellular systems, being a type of a mobile radio system, have the ability to guarantee to its users the so called information and subscriber security: *secrecy* and *authentication.*

T*he secrecy* is a mechanism that rules out the possibility to derive information from a communication channel.

The authentication of cellular service users is an approach that prevents the utilization or bringing in any changes in the telecommunication channel.

The encryption of information and signaling between Base Transceiver Station (BTS) and Mobile Station (MS) is a basic method of insuring the secrecy. At this stage digital cryptographic methods are also utilized to authenticate the messages.

Authentication of the messages by means of cryptographic methods is performed by bringing an identification code (IC) into the text. The identification code is a word or number with a fixed or variable length depending on the transmitted data. ICs are either well known to the sender and the receiver of the massage, or selected during

the process of exchange. The receiver, after decrypting the message, through comparison makes sure that the received message has been transmitted by an authorized subscriber.

1. Basics of ciphering

A system of ciphering has to meet the following requirements [4,5,6]:

- the relation between the plain and the ciphering text has to be nonlinear;
- the ciphering parameters have to be changeable during the exchange.

The first requirement excludes the possibility to falsify the IC without knowing the identification key. The second one excludes the possibility of system malfunction caused by an unauthorized user trying extract a message from the system's memory and to profit by it.

The best approach to providing these requirements is to use the synchronous mode for signaling, which requires the system to posses a frame and symbol synchronization, which is undesirable for the better part of the cases. The more convenient way of meeting these requirements is to include symbols in the information sequence, which are correlated to the encryption data.

Now the encryption algorithms are divided into two groups [6]:

- classical algorithms;
- open key algorithms.

The first group algorithms use only one key for ciphering and deciphering, and the second one uses two keys: one for the transition from plain text to encryption text, and the other one for the transition from encryption to plain text. The main feature of this algorithm is that being familiar with only one of the keys does not allow you to find out the other one.

The open key algorithms are widely used in cellular systems. In these algorithms the key used for ciphering is the same for all the subscribers, and the other key used for decryption is secret. This feature is very useful for the limitation of the complexity of the protocol and the integration of the ciphering structure in cellular networks.

The open key ciphering algorithm is based on determining the, so called *one side function f*, which value y=f(x) from its definition area could easily be computed for any value of its argument x. To compute however the *inverse function* x=g(y)= g(f(x)) is practically impossible. In other words the one side function f(x) can be easily computed with the help of a computer in an acceptable short time range, but the time for the determination of the inverse function is unacceptably great in the modern conditions of development of the computer mathematics.

The first open key ciphering algorithm is called RSA (abbreviation of the first letter of its inventors' names - ***R**ivest, **S**hamir* and ***A**ldeman*). The algorithm is based on two functions E and D. The relation between these functions is given by the following equation [6]

$$D(E(*))=E(d(*))$$

One of them is used for the encryption of the messages, and the other for its decryption. By the way, the value of the function E (or D) does not allow to compute the function D or E easily, e.g. any subscriber of the system can compute the function E and guard in secret the function D. For example, for user of cellular services A there is an open key E_A and a secret key D_A.

Two subscribers A and B can use the RSA algorithm to send encryption messages. If subscriber A wants to send the message M to subscriber B, he can do it in three ways:

- to cipher the message M;
- to sign the message M;
- to cipher and sign the message M.

In the first case subscriber A converts the message M in message $C=E_B(m)$ using a secret key, then sends it to subscriber B. The later, after receiving the message C computes $D_A(C)=D_B(E_B(M))=M$.

In the second occasion subscriber A signs M by computing $F=D_A(M)$ and sends it to subscriber B (this is possible only if A knows the secret key D_A). B receives F and determines $E_A(F)=E_A(D_A(M))=M$. In this case, however, the secrecy is not guaranteed because each subscriber can do this operation by using the common key E_A.

In the third case A computes $F=D_A(M)$ and $C=E_B(F)=E_B(D_A(M))$. Then A sends C to B. B computes $D_B\ (C) = D_B(E_B(F)) = D_A(M)$ after receiving C. Then he computes $E_A(D_A(M))=M$.

The RSA algorithm provides an excellent protection of voce and data and is recommended for use in digital systems for mobile communications, including second generation cellular systems. In these systems the term "security" and "protection" means shutting out an unauthorized use of the system resources and ensuring secrecy of conversations between mobile users. In this aspect there are few approaches for achieving this protection:

- authentication;
- secrecy of transmitted voce and data;
- secrecy of subscriber;

- secrecy of equipment;
- secrecy of connections;
- secrecy of signals for command end control.

Table 1

GSM 02.09	Secrecy aspects	Determines the features of secrecy used in GSM networks Recommends its use in mobile station and systems
GSM 03.20	Secrecy related with network functions	Determines the network functions, Which are necessary for providing secrecy features, given in Rec. 02.09
GSM 03.21	Secrecy algorithms	Determines the cryptographic algorithms in communication system
GSM 02.17	User smart card (SIM)	Determines the main features of SIM

In the European standard for cellular communication GSM these approaches are fixed in Recommendations, which are given in table 1.[2,3]

The following security related information is stored in the GSM hardware:

RAND - Random number, used for the authentication of a mobile subscriber;

SRES - Answer from a mobile station to the random number;

K_I - Individual user authentication key, which is used to compute SRES and the ciphering key;

K_C - Ciphering key, used for encryption/decryption of the messages and signals for command and control, transmitted over the radio channel;

A3 - Authentication algorithm, used to compute SRES;

A5 - Encryption/decryption algorithm;

A8 - Algorithm for the calculation of K_c;

CKSN - The Number of key sequences, which gives the real value of K_c. It is necessary to utilize different keys for transmitting and receiving;

TMSI - Temporary mobile subscriber international number;

IMSI - Identification mobile subscriber international number;

IMEI - International mobile equipment identity;

LAI - Location area identification number.

The distribution of this secrecy information in different elements of the cellular system is given in table 2.

Table 2

N	Network elements and other hardware	Types of secrecy information
1.	Mobile station (MS)	A5
2.	Subscriber identity module (SIM)	A3, A8, IMSI, K_i, TMSI/LAI, K_c/CKSN, IMEI
3.	Authentication center (AUC)	A3, A8, IMSI/K_I
4.	Home location register (HLR)	Packet IMSI/RAMD/SRES/K_c
5.	Visitor Location register (VLR)	Packet IMSI/RND/SRES/K_c, Packet MSI/TMSI/LAI/K_c/CKSN
6.	Mobile switching center (MSC)	A5, triplet TMSI/IMSI/K_c
7.	Base station controller (BSC)	A5, triplet TMSI/IMSI/K_c

2. Coding in cellular communications

Generally speaking, the term *security* includes an error protection of information. To perform a procedure of RSA algorithm we need the messages to be divided into blocks with fixed length. Then every block is encoded in a CRC and a convolution code. Then the digital stream interleaves and is ciphered, as it is seen on figure 1. [7]

The speech coder reduces the data rate by compressing the 64 kbit/s input digital voice stream (μ-law PCM) to create a 8 (in IS-54, IS-136 standard) or 13 kbit/s (in GSM standard) data stream. The IS-54 and the IS-136 standard accept a full-rate speech coder called *Vector Sum Excited Linear Prediction* (VSELP), which is replaced later from an ACELP (Algebraic Code Excited Linear Prediction) coder; the GSM standard and their derivative accept a full-rate speech coder called *Regular Pulse Excitation-Long-Term Prediction* (RELP or RPE-LTP). The incoming 64 kbit/s data are grouped into segments at a rate of 50 segments/s. Hence each segment contains 160 samples and represents a duration of 20 ms. Each segment is coded into 159 bits (in IS-54) or 260 bits (in GSM).[7]

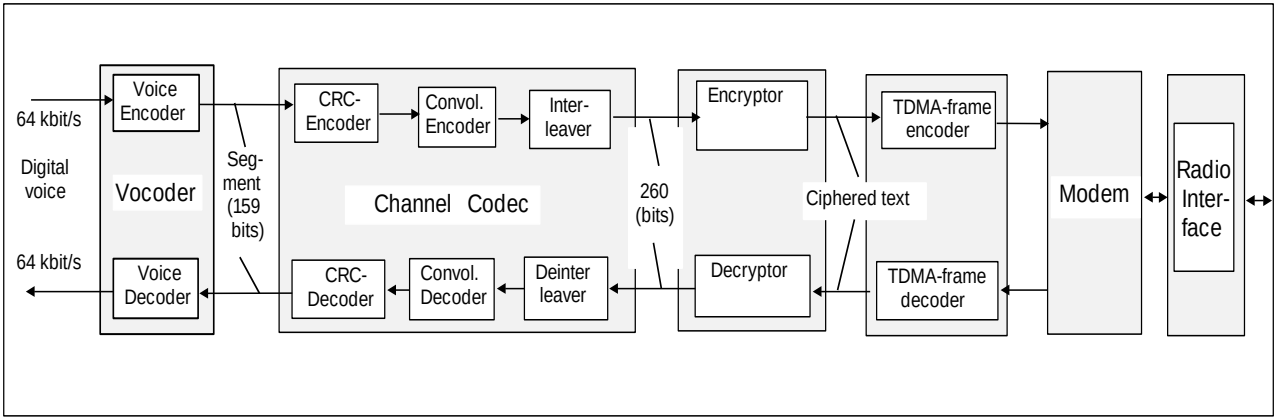

Figure 1: Basic scheme of coding and protection

Channel coder. The main function of the channel coder is to protect the data stream against the noise and fading that are inherent to a radio channel. The coder accomplishes this by adding extra or redundant bits. The greater the number of redundant bits, the higher the immunity to interference and the lower the bit-error rate. The tradeoff is an increased data rate.

The channel coder protects the data stream in five stages, represented on figure 2 [7]:

- Convolutional coding;
- Cyclic redundancy check (CRC) generation;
- Re-ordering and division;
- Interleaving;
- Burst generation.

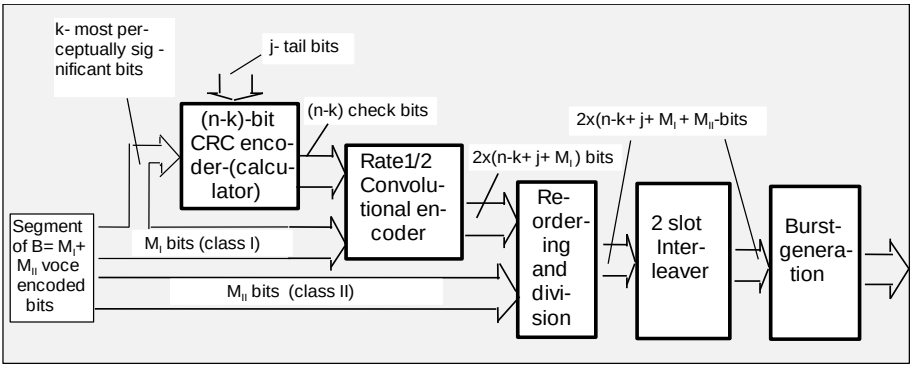

Figure 2: Cannel coding scheme

The first two are mathematical operations, whereas the last two are heuristic approaches. The receiver performs an inverse operation to determine errors have occurred during propagation.

The output bit stream from voice encoder, consisting of segments with length, equal to B bits, is divided into two groups, consisting of M_I and M_{II} bits respectively. The bits of group M_I is called bits of class I. This bits is the most significant bits and it must be protected, against the nose and fading effects. In addition, k of these M_I bits are very important for decoding with high quality (these bits are called the most perceptually significant), and it must be CRC-encoded (usually it is used block (n, k) codes).

The M_I +(n-k)+j bits are then convolutional encoding in the 1/2 rate convolutional encoder. So the output segment will consist of 2 . (M_I +n-k +j) encoded bits. The last

j bits fed into the convolutional encoder are tail bits of state 0 to force the encoder to also return to the zero state.

The remaining M_{II} bits, called class II bits are not protected. The encoding only significant bits (class I bits) reduces the bit rate in the system.

Convolutional coding provides error-correction capability by adding redundancy to the transmitted sequence. Convolutional encoding is implemented by linear feed forward shift registers. A convolutional coder is described by the rate at which data enters the coder and the rate at which data leaves the coder. For example, a rate 1/2 convolutional coder implies that for every 1 bit of data entering the coder, 2 bits leave the coder. The smaller the ratio, the greater the redundancy. This improves the error-protection capability.

GSM standard recommends that the bit of class 1 to be 182 and bits class II to be 78. IS-54 standard recommends that the bits of class I to be 77 and the bits of class 2 to be 82.

Cycle redundancy check (CRC) generation. Of the class 1 bits that are error-protected, it has been found that only 132 bits (in GSM) and 12 bits (In IS-54) are perceptually significant. Hence these bits are protected by using (n, k) CRC code .[7]

Re-ordering and division. After block and convolutional encoding the length of the segment is 2 . (M_I + n-k=j) bits. These bits are re-ordering first and then the segment is divided into eight frames [6] (figure 3-a).

Interleaving. In radio propagation, it has been found that the fading occurs at localized instances of time and space. As a result, interleaving spreads the information of the data stream across two frames, because it is unlikely that a clustered bit error would occur in successive frames. Finally, data propagated in burst.

To interleave the data from each frame is divided and spread across two transmitted slots using a MxN interleaving array. As a result, not all bits from a speech frame are lost by one bad slot (figure 3-b).

Burst generation. After the data has been compressed and error-protected, the bit stream is compressed (in time only) into a burst format. Burst timing offsets may be applied to facilitate dynamic time alignment (figure 3-c). After burst generation (division on packet) the packet interleaving is performed.

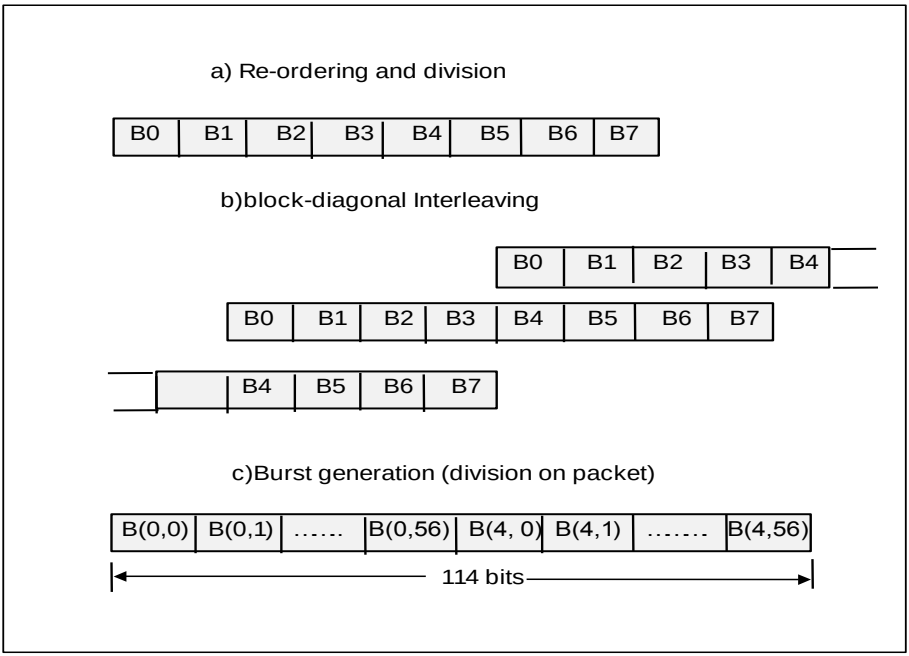

Figure 3: Re-ordering and interleaving coding information in GSM

Table 3

SYSTEM/ CODER	**GSM**	**IS-54**	**IS-136**
Type	RELP	VSELP	ACELP
Traffic channel			
Raw data rate	13 kbit/s	7,95 kbit/s	7,40 bit/s
Input bits distribution	Class Ia: 50 Class Ib: 132 Class II: 78	Class I: 77 Class II: 82	Class Ia: 48 Class Ib: 48 Class II: 52
Type of channel codes	1/2 rate convolution; K=5	1/2 rate convolution; K=6	1/2 rate convolution; K=5
CRC	3 bits on 50 bits or 1 bit per 16, 7 bits (53, 50)	7 bits on 77 bits or 1 bit per 11 bits (74, 77)	7 bits on 48 bits or 1 bit per 6,9 bits (55, 48)
Encoding data rate	22,8 kbit/s	13 kbit/s	13 kbit/s
Interleaving	Over 8 time slots	Over 2 time slots	Over 2 time slots
Control channel			
Type of the channel codes	1/2 convolution K=5	1/4 convolution K=6	1/4 convolution K=6
CRC (block code)	40 bits on 184 (224, 184)	12 bits on 49 (61,49)	12 bits on 49 (61,49)

The cannel coding of data and signals in the control cannel is performed by the same way. Table 3 shows the basic features of coding in three standards [7]:

The length of the system cycle is chosen to be very long. For example, in the cellular system GSM this cycle is called hyperframe and its period is equal to 3 h 28 min 53 s and 760 ms. Such a long period is imposed for the purposes of ciphering. The hyperframe consists of superframes; superframe of multiframes; multiframe of TDMA frames. One hypreframe contents 2715647 TDMA frames. In cycle period every TDMA frame is numbered from 0 to N f_{max}. In RSA cryptographic algorithm the frame number is used as an input parameter.

The encryption/decryption process is discussed later in sections 4, 5, 6 and 7.

3. Authentication procedure

The purpose of the authentication is to protect the network against unauthorized use. It also enables the protection of the GSM Public Land Mobile Network (PLMN). Subscriber authentication is performed at each registration, at each call setup attempt (mobile originating or terminating), and before performing some supplementary services, such as activation or deactivation of the mobile station.

The frequency with which a particular PLMN applies the authentication procedure to its own subscribers is their responsibility. However, a PLMN shall apply the authentication procedure to visiting subscriber as often as this feature is applied to those subscribers in their home PLMN.

The procedure starts with the termination of the mobile *initialization* and *identification.*

Initialization.[1] Prior to establishing any communication links with other parties, the MS must first acquire synchronization with the GSM system. This process begins after the MS is turned on in a PLMN. The first step of the process is for the MS to search for and acquire a frequency control channel (FCCH) burst on some common control frequency cannel. The MS will scan all or part of 124 RF channels and obtain the average strength of each channel. During the scanning process, several readings of the RF level have to be taken so that the MS gets an accurate estimate of the channel power. Thus the scanning may take several seconds.

For each of the 124 channels, starting with the one of highest signal strength level, the MS searches for the Frequency Control Channel (FCCH). This is the first step of the process known as frequency synchronization. A diagram of the process is presented on figure 4. [1]

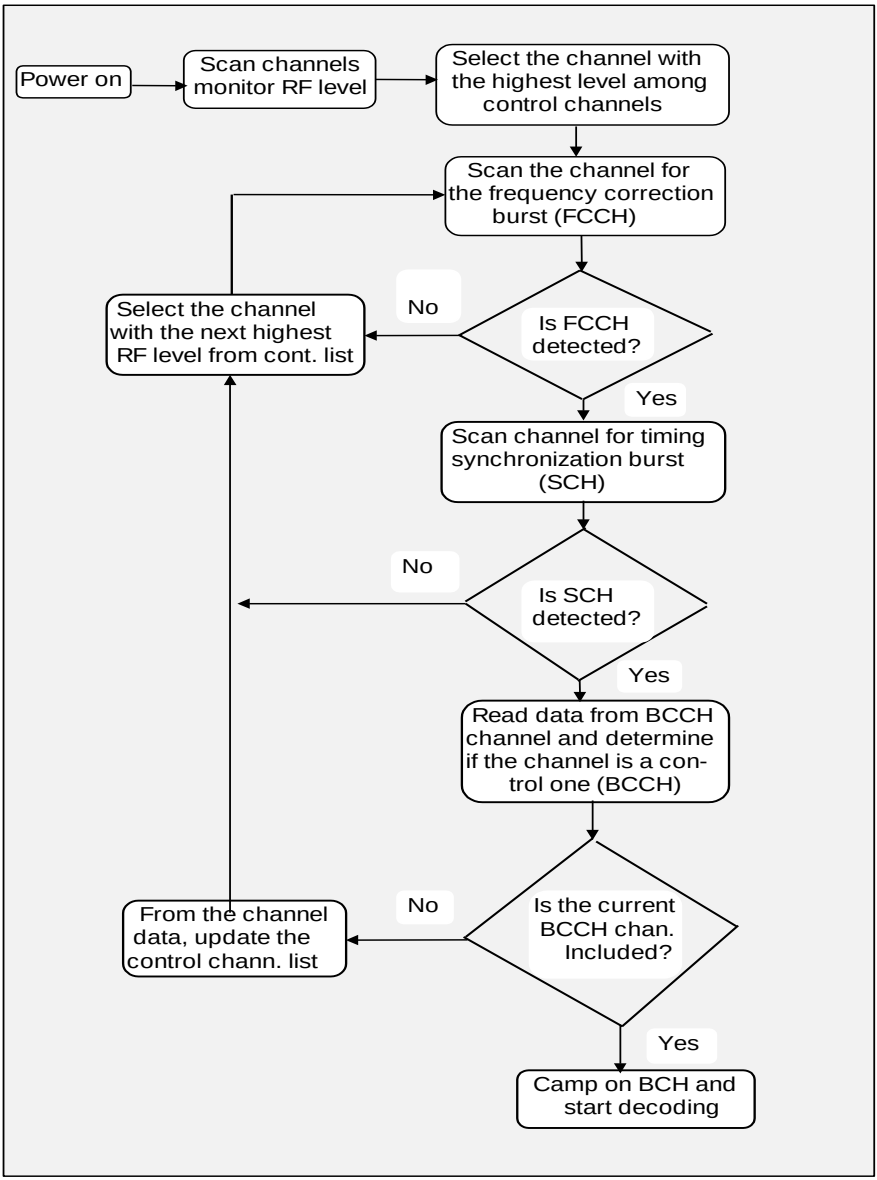

Figure 4: Initialization algorithm

For this purpose is used the frequency burst which is unique and easily recognizable. IF no frequency burst is detected, then the MS can go to a channel with the next highest signal strength level.

After the frequency correction burst is detected, the MS will try to synchronize with the time synchronization burst Synchronization Channel (SCH). The SCH always occurs in the next frame in the same time slot as the FCCH. This is eight burst periods later than the FCCH. SCH contains precise timing information on the time slot boundaries to permit refining the received slot timing. The SCH message also contains the current frame number to which the MS synchronize. This time synchronization is generally carried out in two steps: coarse and fine.

If synchronization does not occur, the process of frequency one with the next highest channel in the list may start. If the synchronization is successful, the MS will read the TDMA frame number and the Base Station (BS) identity code.

Assuming that the MS is in sync and decodes the information on a Broadcast Control Channel (BCCH). The BCCH information will contain such items as adjacent cell list. All BCCH transmissions are at standard power level, which permits the MS to compare received power from its own BTS as well as from adjoining BTS's. In case that the BCCH information is correctly decoded, the MS follows one of the two paths [1]:

- if the BCCH information includes the present BCCH channel, then the MS will simply stay on the channel;
- if the current channel is not in BCCH information list, or the received signal strength level is below the desired level, the MS will continue searching for the next control channel.

After the MS has successfully synchronized to a valid BCCH, the MS is now ready to register, receive paging, originate an outgoing call and doing identification and authentication.

Identification.[1] This procedure is used to identify the MS/SIM by its IMSI if the VLR does not recognize the TMSI sent by the MS. This lack of recognition can be a result of the mobile user's changing the MSC/VLR area from the last time he accessed the system or can be due to some other reason. If identification is required, the VLR sends a message, containing IMSI to the MSC. As a result of this message, MSC sends an Identity Request message to the MS. The ME responds by returning an Identity Response message containing its IMSI to the MSC. The MSC then sends the IMSI acknowledge to the VLR. If the IMSI is currently not in the VLR, then the VLR must get its file from the HLR identified in the IMSI. To du this, The VLR sends the HLR an Update Location message. Assuming that the IMSI is in fact registered in the HLR, the HLR responds with an Update Location Result message, followed by an Insert Subscriber Data message containing other pertinent data needed by the VLR. The VLR acknowledges the data transfer with an Insert Subscriber Data Result message to the HLR.

ALL this exchange of the messages is performed in accordance to RIL3-MM and MAP/D protocols.

Authentication.[1] GSM standard uses a sophisticated technique for authentication that consists of asking a question that only the right subscriber equipment (in this case the SIM-card) can answer. The core of this method is that a large number of such questions exist, and it is unlikely that the questions can be answered correctly by the wrong MS. The generic process of authentication is shown in figure 5.

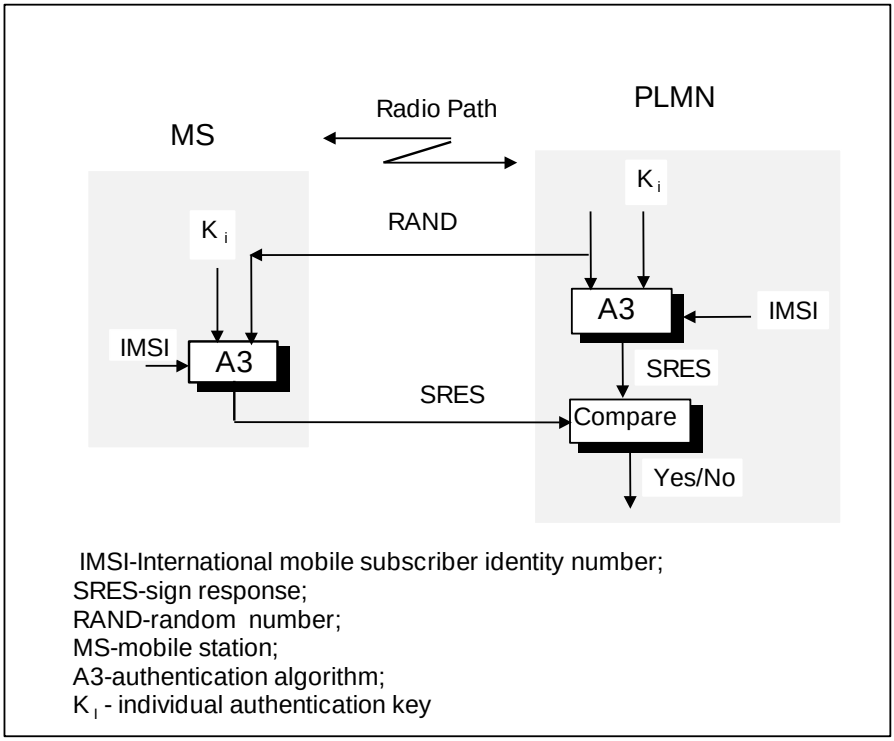

Figure 5: Authentication algorithm

The authentication algorithm A3 computes from a RAND, both at the MS and network (PLMN)

After the frequency correction burst is detected, the MS will try to synchronize with the time synchronization burst channel (SCH). The SCH always occurs in the next frame in the some time slot as the FCCH. This is and at Authentication Center (AuC). A signed response SRES, using an individual secret key K_i, attached to the mobile subscriber. The number RSND, whose value is drawn randomly between 0 and 2^{128}-1,

is used to generate the response by the MS as well as by the fixed part of the network. It should be noted that the authentication process is carried out both at the MS and the network center MSC simultaneously. The Base Subsystems (BSS) remain transparent to this process.

It should also be noted that the MS only receives the random number over the radio path and in turn returns the SRES to the network. Thus an air interface mobile designation is not disclosed.

At the subscription time, the subscriber authentication key K_I is allocated to the subscriber together with its IMSI. The key K_I is stored in the AuC and used to generate a triplet (K_c, SRES, RAND) within the GSM system. As stated above, the same K_I is also stored at the MS in the SIM-card. In the AuC, The following steps are carried out in order to produce one triplet: a non predictable RAND is produced; RAND and K_I are used to calculate the SRES and ciphering key K_c using two different algorithms A3 and A8. This triplet is for each and every user and is then delivered to the network database HLR. This procedure is shown in figure 6.

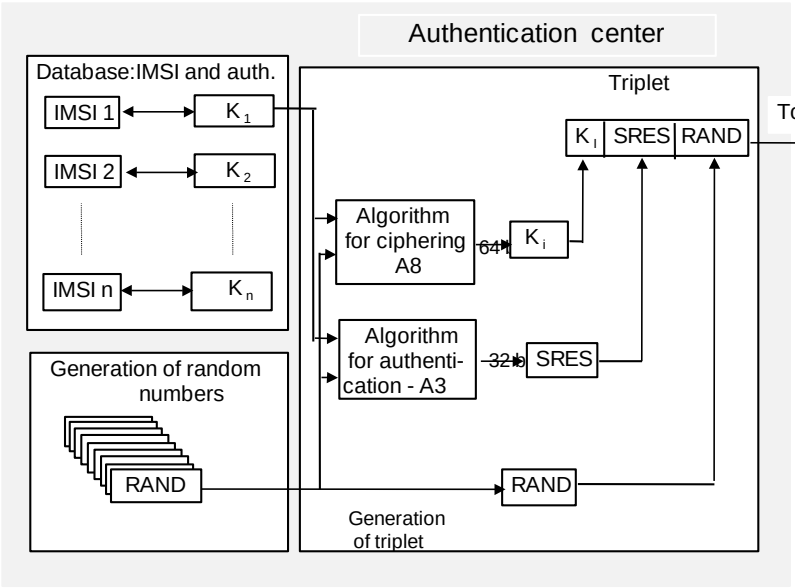

Figure 6: Generation of triplet (K_i, SRES, RAND)

The AuC begins the authentication and ciphering key generation procedure after receiving an identification of the subscriber from MSC/VLR. The AuC first queries the HLR for the subscriber's authentication key K_i. It then generates a 128 bits

RAND for use as a challenge, to be sent to the MS for verification of the MS' authenticity. RAND is also used by the AuC, with K_I in the algorithm A3 for authentication, to calculate the expected correct SRES from the MS. RAND and K_I are also used in the AuC to calculate the cipher key K_c with algorithm A8. The SRES is a 32-bit number, and K_c is a 64-bit number.

The HLR transmits the value of RAND, SRES and K_c to the MSC/VLR (see figure 7 [1]) for interaction with the MS.

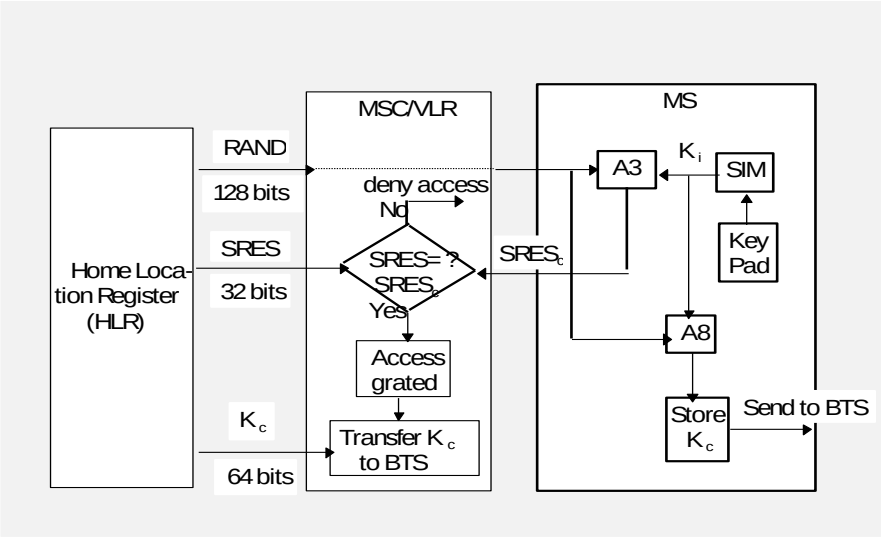

Figure 7: Full authentication process in GSM system

Algorithms A3 and A8 are not fully standardized by GSM and may be specified at the direction of PLMN operators. To protect the secrecy of the user, the authentication key is not sent to the MSC/VLR.

Based on the discretion of the PLMN operator, the authentication key can be of any format and length. The MSC/VLR forward the value of the RAND to the MS, which also has the correct K_I and algorithm A3 stored in its SIM card. The SIM then uses RAND and K_c in these algorithms to calculate the authentication $SRES_c$ and cipher key. The MS sends the calculated $SRES_c$ back to MSC/VLR, which compares it with the value signet response received from the HLR/AuC. If the $SRES_c$ and SRES agree, the subscriber access to the system is granted, and the cipher key K_c is transferred to the BTS for use in encrypting and decrypting messages to and from the MS. If the

computed signed response at the MS and the signed response disagree, the subscriber access to the system is denied.

In summary, the VLR initiates authentication toward the MS and checks the authentication result.

4. The secrecy of voice and data

The secrecy of data and voice on the radio path is obtained by its encryption. It is well known that cellular systems of second and third generation use digital transmission and hence it brings an excellent level of protection by using digital cryptographic methods.

The ciphering algorithm is synchronized with the TDMA clock and adds very little complexity to the MS. The cipher key is obtained as a side product of the authentication procedure and differs from call to call. The GSM is designed so that a single encryption algorithm is used for protection of all transmitted data in dedicated mode, whether it is user information (speech or data), user-related signaling (messages carrying the called phone numbers) or even system-related signaling (the messages carrying radio measurement result to prepare handover)

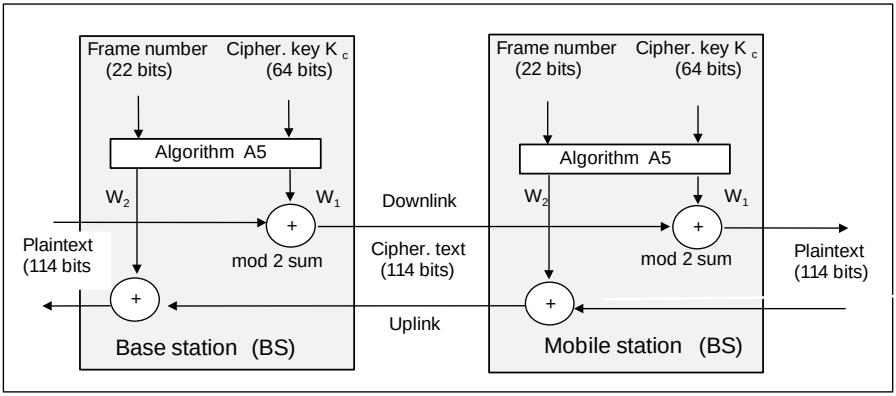

Figure 8: Data flow encryption/decryption process

Data flow on the radio path is obtained by a bit-per-bit binary addition of the user data flow and ciphering bit-stream generated by the GSM algorithm A5 using a ciphering key K_c. This exact process of encryption/decryption at the MS and at the base station is shown in figure 8. [1]

Code words W_1 and W_2 for downlinks and uplinks are changed at every frame. When modulo 2 is added with plain text, W_1 outputs ciphered text. On other side, the

ciphered text, when modulo 2 is added with W_2, outputs the plain text. The ciphering/deciphering function is placed on the transmission chain between the interleave and the modem (refer to figure 1). Since A3 and A8 are always running together, these two are implemented as a single algorithm in most cases. The algorithm A5 is standardized in the whole of GSM.

The encryption/decryption procedure starts by CMC (ciphering mode command), transmitted from MSC/VLR to MS via BSS.

5. Secrecy of subscriber

For excluding a determination (identification) subscriber by the interception of messages, sent on the radio link, any subscriber is assigned "temporary identity card" TMSI, which real only within the Location Area (LA). In other LA he is assigned new TMSI. If subscriber is not yet assigned temporary number (for instance, under first including the rolling stations), identification is conducted the attach (or detach) the international identification number (IMSI). After the completion of the procedure of authentication and beginning of ciphering mode, TMSI will be sent to the MS only in the scrambled type. This TMSI will be used under all following accesses to the system. If MS moves over to the new area of location, its TMSI must be sent together with identification area numbers (LAI), in which TMSI was assigned to the subscriber.

6. Secrecy of the equipment

The aspects of secrecy of the equipment are realized by means of equipment identification. The complete equipment identification process is shown in figure 9.

The administrative use of the International Mobile Equipment Identity (IMEI) enables the operator to check the mobile equipment identity at call setup**.** The purpose of this feature is to make sure that no stolen or unauthorized mobile equipment is used in the system.

The equipment identification procedure consists of the MSC/VLR's requesting the IMEI from the MS and sending it to a standalone entity called Equipment Identification Register (EIR).

On reception of the IMEI at the AuC, the EIR makes use of three possible defined lists [1,4,5]:

- *A white list* containing all numbered series of all equipment identities that have been allocated in the different participating GSM countries;
- *A black list* containing all equipment identities that are barred. This listing may be a result of information on stolen equipment;

- *A gray list* containing faulty or unapproved mobile equipment. This equipment is under observation but not barred for service.

Although the GSM specification recommends using the equipment identity at each and every call, the frequency of identification really lies with the individual operators. The system operator can make decisions in this regard.

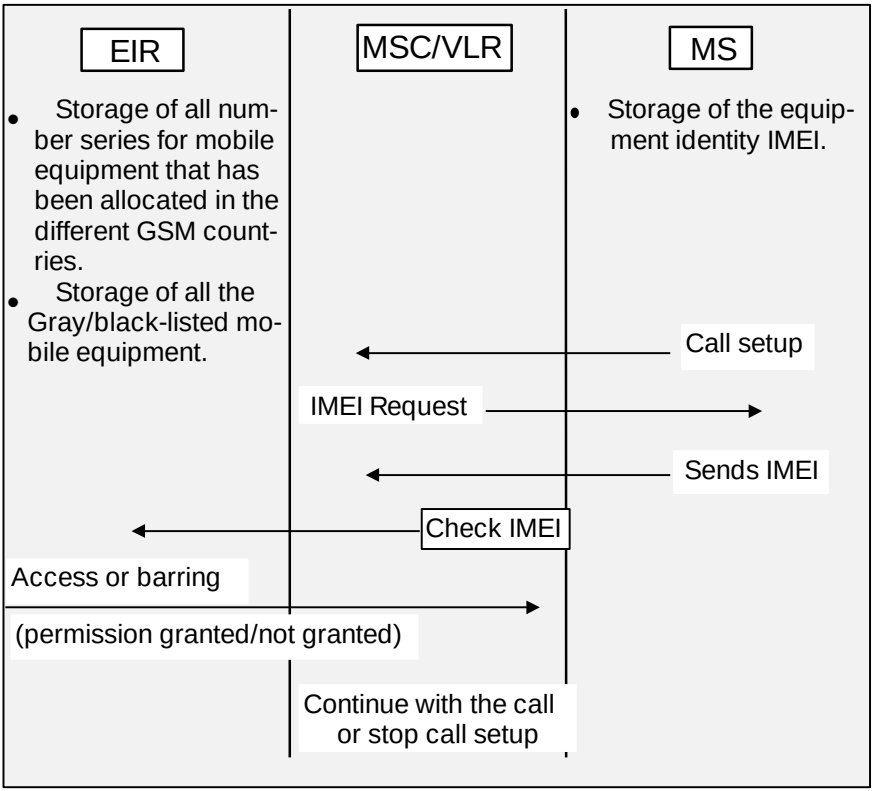

Figure 9: Equipment identification process

The equipment identification process starts with the MSC/VLR's requesting MS for its IMEI. In response, The MS sends its identity that, if positively checked by the equipment identity register (EIR), allows the MS to proceed further with the call. The MS is not allowed to continue with the call if the equipment identity does not match the stored value of the identity in the register.

As shown on figure 9, an IMEI request is initiated by the MSC/VLR combination as a result of MS's requesting a call setup. Upon receiving the IMEI request, The MS

sends the equipment identification to the MSC/VLR, which is subsequently checked against the stored values in the EIR.

7. Secrecy of connections

When performing a procedure of adjustment of location on the control channel is realized exchange between MS and BTS service messages, containing the temporary subscriber number TMSI. In this case in the radio link it is necessary to ensure secrecy of renaming TMSI and its attribute to the concrete subscriber.

Let's consider, the ensured secrecy in the procedure adjustment of the location, if the subscriber conducts a communication link and at the same time goes from one area of location in the another.

In this case the mobile station has already registered in the Visitor Location Register (VLR) with the temporary number TMSI, corresponding to the former area of location. When entering in the new area of location a procedure of recognition is realized, which is held at hold, scrambled in the radio link TMSI, sent with the name of location area identity (LAI) simultaneously. LAI gives information to the MSC/ VLR and allows to require a former area of location on the status of subscriber and its file, having excluded exchange by these service messages on control channel. In this way the messages transmitted on the communication channel is send as a scrambled information text, with the interruption of messages in the handover process, on 100-150 ms.

The procedure of adjustment of location, including features of secrecy is shown in figure 10. [6]

8. Secrecy of signaling and control massages

The confidentiality feature of physical connections (physical radio channels) means that the user information and signaling exchanged between the BTS and the MS are not made available or disclosed to unauthorized individuals, entities or processes. The purpose of this feature is to ensure the privacy of the user information (voice and non voice) as well as the user related signaling elements. All speech and data are ciphered, and all associated signaling information is protected.

Privacy protection during the exchange between network's elements, is realized by means of Authentication Center (AuC). AuC is a main object, and is in charge of all safety aspects. This center can be a separate object or part of some equipment, for instance, in HLR. How to control AuC decides, who will be entrusted access to the network. GSM Interface with AuC is not determined.

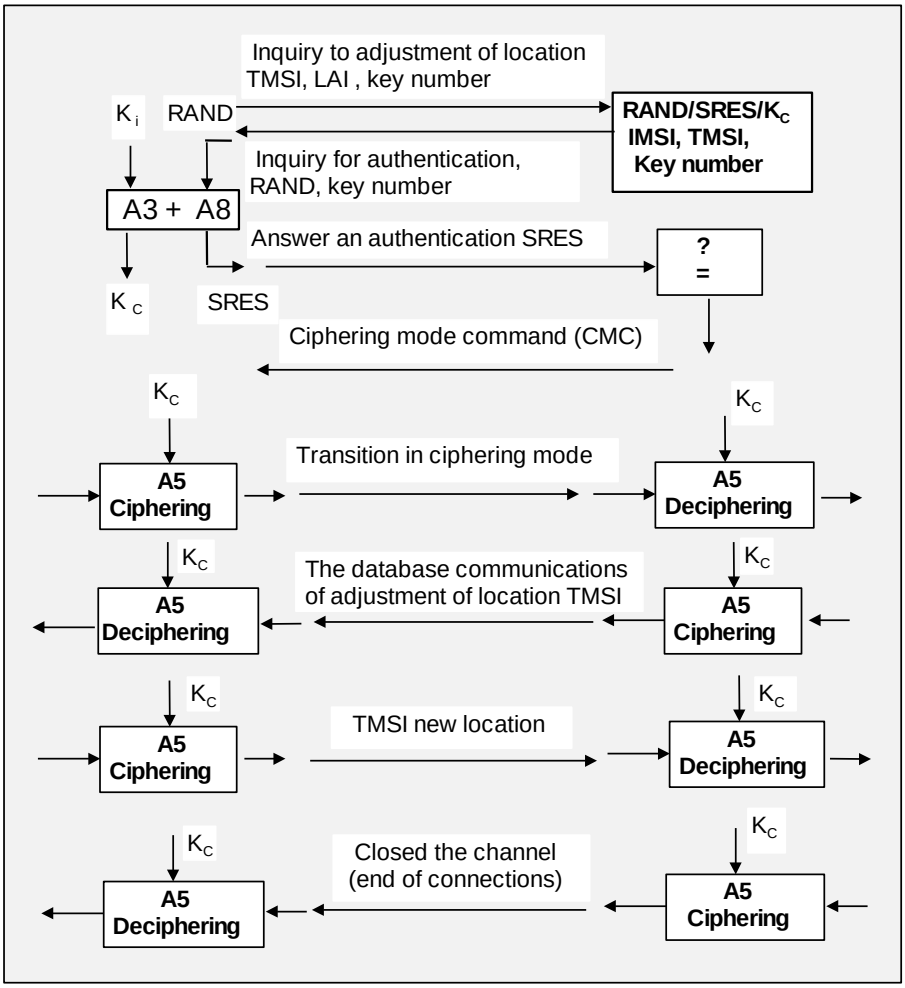

Figure 10: Procedure of adjustment of location

AuC deals with the following:

- generation of the individual authentication keys K_i of the users and its corresponding IMSI;
- generation of a triplet RAND/SRES/K_C for each IMSI and decryption this triplet for HLR at needed.

If MS moves over to the new area of location with new VLR, the later one will get secret information on this MS. This can be provided in two ways:

- MS conducts a procedure of identification on its IMSI. For the purpose, VLR requires from HLR the triplet RAND/SRES/$K_{C,}$ belonging this IMSI;
- MS conducts an authentication procedure using an old temporary number TMSI with LAI name. The new VLR requires old VLR for sending IMSI and staying groups from RAND/SRES/K_C, belonging this TMSI/LAI.

If a mobile subscriber stays on for a longer period in VLR, then after certain amount of accesses with authentication, VLR from considerations of secrecy will require new triplet RAND/SRES/K_C from HLR.
All these procedures are determined in recommendations GSM 09.02.

Checking an authentication is executed in VLR. VLR sends RAND on MSC and takes SRES corresponding responses. After positive authentication TMSI is placed with IMSI. TMSI and used encryption key K_C are sent in MSC. These procedures are also determined in recommendations GSM 09.02.

The issues of security of information on the radio link were described in section 4. Further details may be found in recommendations GSM 09.08.

Conclusion

Important aspects of security and protection of information of cellular communications (channel coding, authentication, encryption of user data and signaling information and the positive mobile equipment identification), before providing the user with service have been fully explored. The radio path information is protected due to channel coding and ciphering. The authentication procedure ensures that the network is accessed only by legitimate subscribers. Equipment ID ensures that the MS is using the correct brand of transceivers. All these features provide the secrecy of subscribers, equipment, user's data and signaling information and different connections.

References:

1. Asha Mehrotra and Leonard Golding, "Mobility and Security Management in the GSM System and Some Proposed Future Improvement," *Proceedings of the IEEE* 86, 7 (July 1998).
2. European Telecommunication Standard Institute/Global System for mobility, ETSI/GSM specification vol.3.20, Section 3 (January 1993).

3. European Telecommunication Standard Institute/Global System for mobility, ETSI/GSM specification vol.2.17, Section 3 (January 1993).
4. V. Michel, "The Security Features in the GSM System," in *Proceedings of the 6-th World Telecommunications Forum* (Geneva: October 1991).
5. P.Vander Arend, "Security Aspects and the Implementation in the GSM System," in *DCRC Conference Proceedings* (Hagen, Gernmany: October1988).
6. U.A. Gromakov, *Standards and Systems of Mobile Communications* (Moscow: EkoTrandz, 1998) - in Russian.
7. Metodi Popov, *Coding in the Cellular Communications* (Sofia: ProCon, 2000) - in Bulgarian.

METODI KOSTADINOV POPOV is born in 1941. He holds a M.Sc. degree in Radio and Telecommunications from the "G.S. Rakovsky" Defense Academy (1980) and Ph.D. degree in communication networks and systems from the "G.S. Rakovsky" Defense Academy. Since 1982 Dr. Popov is Associated Professor at the Radioelectronics Department of the "Vassil Levsky" Army Academy in Veliko Tirnovo. Author of ten books and over 80 papers devoted to the problems of communications signals, systems and devices. Main research interests are in the area of cellular communications. Member of IEEE and BSUAE. Address for correspondence: Radioelectronics Department, "Vassil Levsky" Army Academy, Veliko Tirnovo, Bulgaria. E-mail: Kalbanov@usa.net.