ABACUS, Pages 89 - 99 , Vol. 36, No. 2, 2009

DEVELOPMENT OF A MODEL FOR THE IMPLEMENTATION OF GSM SECURITY ALGORITHM

ABIKOYE, O. C. AND BAJEH, A. O.
Department of Computer Science, University of Ilorin, Ilorin, Nigeria.

ABSTRACT

The motivations for security in cellular telecommunications systems are to secure conversations and signaling data from interception as well as to prevent cellular telephone fraud. With the older analog-based cellular telephone systems such as the Advanced Mobile Phone System and the Total Access Communication System, all these motivation were not achieved. Another security consideration with cellular telecommunications systems involves identification credentials such as the Electronic Serial Number, which are transmitted "in the clear", in analog systems. With more complicated equipment, it is possible to receive the Electronic Serial Number and use it to commit cellular telephone fraud by "cloning" another cellular phone and placing calls with it. This led to the development of digital technologies, with the advent of digital technology; wireless voice communications are much difficult to intercept than analog systems. GSM is a standard for a digital mobile cellular communication.

In this paper the three different GSM security algorithms namely A3, A5 and A8 were studied and we present a computer model for one of the three GSM security algorithms known as A3 (user authentication) algorithm.

The model is implemented using Visual Basis 6.0 Programming Language.

1. INTRODUCTION

In older analog-based cellular telephone systems such as the Advanced Mobile Phone System (AMPS) and the Total Access Communication System (TACS), it is a relatively simple matter for the radio hobbyist to intercept cellular telephone conversations with a police scanner. A well-publicized case involved a potentially embarrassing cellular telephone conversation with a member of the British royal family being recorded and released to the media. The motivations for security in cellular telecommunications systems which are to secure conversations and signaling data from interception as well as to prevent cellular telephone fraud were not achieved with the older analog – based cellular telephone systems.

The security and authentication mechanisms incorporated in GSM make it the most secure mobile communication standard currently available, particularly in comparison to the analog systems described above. Part of the enhanced security of GSM is due to the fact that it is a digital system utilizing a speech coding algorithm, Gaussian Minimum Shift Keying (GMSK) digital modulation, slow frequency hopping, and Time Division Multiple Access (TDMA) time slot architecture. To intercept and reconstruct this signal would require more highly specialized and expensive equipment than a police scanner to perform the reception, synchronization, and decoding of the signal. In addition, the authentication and encryption capabilities that will be discussed in this project ensure the security of GSM cellular telephone conversations and subscriber identification credentials against even the determined eavesdropper.

GSM security and encryption algorithm are used to provide authentication and radio link privacy to users on GSM network. GSM uses different security algorithm called A3, A8 and A5 algorithms. A3 and A8 algorithms are implemented in Subscriber Identity Module (SIM) cards and in GSM authentication centers. They are used to authenticate the customer and generate a key for encrypting voice and data traffic. Development of A3 and A8 algorithm is considered a matter for individual GSM network operators. Though, there is a GSM standard, which can be used by any administrations that do not wish to develop their own proprietary algorithm. The authentication algorithms need not to be universal and different networks are free to use algorithms of their choice (provided that the parameter are of the correct length)

2. OVERVIEW OF GSM

GSM (group special mobile or general system for mobile communications) is the Pan-European standard for digital cellular communications. The Group Special Mobile was established in 1982 within the European Conference of Post and Telecommunication Administrations (CEPT) [4]. A Further important step in the history of GSM as a standard for a digital mobile cellular communications was the signing of a GSM Memorandum of Understanding (MoU) in 1987 in which 18 nations committed themselves to implement cellular networks based on the GSM specifications. In 1991 the first GSM based networks commenced operations. GSM provides enhanced features over older analog-based systems, which are summarized below [2]:

- Total Mobility: The subscriber has the advantage of a Pan-European system allowing him to communicate from everywhere and to be called in any area served by a GSM cellular network using the same assigned telephone number, even outside his home location. The calling party does not need to be informed about the called person's location because the GSM networks are responsible for the location tasks. With his personal

chipcard he can use a telephone in a rental car, for example, even outside his home location. This mobility feature is preferred by many business people who constantly need to be in touch with their headquarters.

- High Capacity and Optimal Spectrum Allocation: The former analog-based cellular networks had to combat capacity problems, particularly in metropolitan areas. Through a more efficient utilization of the assigned frequency bandwidth and smaller cell sizes, the GSM System is capable of serving a greater number of subscribers. The optimal use of the available spectrum is achieved through the application Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), efficient half-rate and full-rate speech coding, and the Gaussian Minimum Shift Keying (GMSK) modulation scheme.
- Security: The security methods standardized for the GSM System make it the most secure cellular telecommunications standard currently available. Although the confidentiality of a call and anonymity of the GSM subscriber is only guaranteed on the radio channel, this is a major step in achieving end-to- end security. The subscriber's anonymity is ensured through the use of temporary identification numbers. The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping which could only be realized using digital systems and signaling.
- Services: The list of services available to GSM subscribers typically includes the following: voice communication, facsimile, voice mail, short message transmission, data transmission and supplemental services such as call forwarding.

3. ARCHITECTURE OF THE GSM NETWORK

A GSM network is composed of several functional entities, whose functions and interfaces are specified. The GSM network can be divided into three broad parts. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile services Switching Center across the A interface. Figure 3.1 shows the layout of a generic GSM network [4].

3.1 Mobile Station

The mobile station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to subscribed services irrespective of a specific terminal. By inserting the SIM card into another GSM terminal, the user is able to receive calls at that terminal, make calls from that terminal, and receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The IMEI and the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

3.2 Base Station Subsystem

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the standardized Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The Base Transceiver Station houses the radio tranceivers that define a cell and handles the radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed, thus the requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile station and the Mobile service Switching Center (MSC).

3.3 Network Subsystem

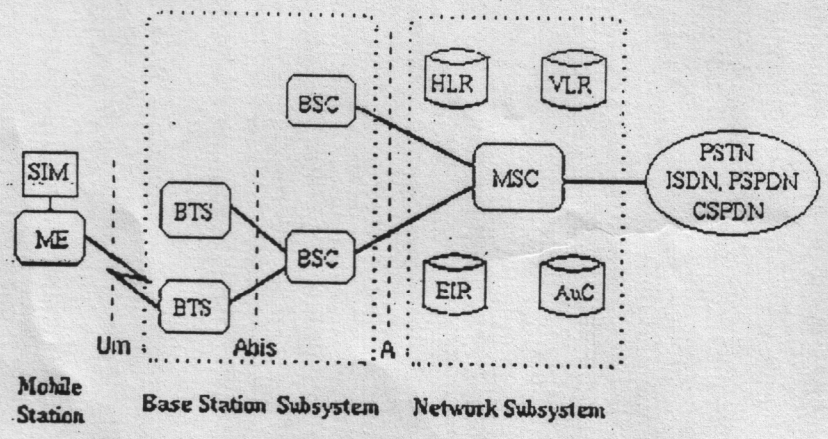
The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the fixed networks (such as the PSTN or ISDN). Signalling between functional entities in the Network Subsystem uses Signalling System Number 7 (SS7), used for trunk signalling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signalling address of the VLR associated with the mobile station. The

actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signaling required. Note that the MSC contains no information about particular mobile stations --- this information is stored in the location registers.

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.



SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transceiver Station
BSC Base Station Controller
HLR Home Location Register
VLR Visitor Location Register
MSC Mobile services Switching Center
EIR Equipment Identity Register
AuC Authentication Center

Figure 3.1: A Generic Layout Of GSM Network

4 GSM SECURITY FEATURES

Security in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the International Mobile Subscriber Identity (IMSI). This information, along with the individual subscriber authentication key (Ki), constitutes sensitive identification credentials analogous to the Electronic Serial Number (ESN) in analog systems such as AMPS and TACS. The design of the GSM authentication and encryption schemes is such that this sensitive information is never transmitted over the radio channel. Rather, a challenge-response mechanism is used to perform authentication. The actual conversations are encrypted using a temporary, randomly generated ciphering key (Kc). The MS identifies itself by means of the Temporary Mobile Subscriber Identity (TMSI), which is issued by the network and may be changed periodically (i.e. during hand-offs) for additional security.

The security mechanisms of GSM are implemented in three different system elements; the Subscriber Identity Module (SIM), the GSM handset or MS, and the GSM network [3]. The SIM contains the IMSI, the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN). The GSM handset contains the ciphering algorithm (A5). The encryption algorithms (A3, A5, A8) are present in the GSM network as well. The Authentication Center (AUC), part of the Operation and Maintenance Subsystem (OMS) of the GSM network, consists of a database of identification and authentication information for subscribers. This information consists of the IMSI, the TMSI, the Location Area Identity (LAI), and the individual subscriber authentication key (Ki) for each user. In order for the authentication and security mechanisms to function, all three elements (SIM, handset, and GSM network) are required. This distribution of security credentials and encryption algorithms provides an additional measure of security both in ensuring the privacy of cellular telephone conversations and in the prevention of cellular telephone fraud.

Within the GSM network, the security information is further distributed among the authentication center (AUC), the home location register (HLR) and the visitor location register (VLR). The AUC is responsible for generating the sets of RAND, SRES, and Kc which are stored in the HLR and VLR for subsequent use in the authentication and encryption processes [4].

5. GSM ALGORITHM

There are three proprietary algorithms used to achieve authentication and confidentiality in the GSM. These are known as A3, A5 and A8. A3 is used to authenticate the SIM (Subscriber Identity Module) for access to the network. A5 and A8 achieve confidentiality by scrambling the data sent across the airways. Anonymity is achieved by use of temporary identities (TMSI).

5.1 Authentication Algorithm A3

It is operator-dependent and is an operator option. The A3 algorithm is a one-way function. That means it is easy to compute the output parameter SRES by using the A3 algorithm but very complex to retrieve the input parameters (RAND and KI) from the output parameter [6].

Authentication is achieved using a basic challenge-response mechanism between the SIM and the network. The actual A3 authentication algorithm used is the choice of the individual GSM network operators, although some parameters (input, output and key length) are specified so that interoperability can be achieved between different networks.

A3 is implemented in the SIM card and the Authentication Center (AuC) or the Home Local Register (HLR). A3 takes a 128 bit value *Ki* (subscriber *i*'s specific authentication key) and 128 bit *RAND* random number (challenge sent by the network) as input data. It produces a 32 bit output value *SRES*, which is a *S*igned *RES*ponse to the networks challenge. The SIM and the network both have knowledge of *Ki* and the purpose of the authentication algorithm is for the SIM to prove knowledge of *Ki* in such a way that *Ki* is not disclosed. The SIM must respond correctly to the challenge to be authenticated and allowed access to the network. The authentication procedure is outlined in the following steps [5]:

1. The process is initiated by the user wanting to make a call from his mobile (Mobile Station or MS) or go on standby to receive calls.
2. The Visitor Location Register (VLR) establishes the identity of the SIM. This is determined through a 5 digit temporary identity number known as the Temporary Mobile Subscriber Identity (TMSI). The TMSI is used in place of the International Mobile Subscriber Identity (IMSI). The IMSI is a unique number that identifies the subscriber worldwide. If the IMSI was used then this would enable an adversary to gain information about a subscriber's details and location. The TMSI is frequently updated (every time the user moves to a new Location Area (LA) and/or after a certain time period) to stop an adversary from gaining such information. Note that there are situations where the IMSI will be used, for example on the first use of the mobile after purchase.
3. The VLR sends a request for authentication to the Home Location Register (HLR). This request will contain the SIM's IMSI (as the IMSI and the related TMSI should be stored in the VLR).
4. The HLR generates a 128 bit random *RAND* challenge and sends it to the MS via the VLR.
5. Using *Ki* (128 bits) which is stored in the HLR and *RAND* (128 bits), the HLR then calculates *SRESHLR* (32 bits) using the A3 authentication algorithm. *SRESHLR* is then sent to the VLR.
6. Using *Ki* (128 bits) which is stored in the SIM and *RAND* (128 bits) that is received as a challenge, the SIM calculates *SRESSIM* (32 bits) using the A3 authentication algorithm. *SRESSIM* is then sent to the VLR.
7. If *SRESHLR* = *SRESSIM*, then the SIM is authenticated and allowed access to the network.
8. If *SRESHLR* ≠ *SRESSIM*, an authentication rejected signal is sent to the SIM and access to the network is denied.

5.2 Ciphering Key Generating Algorithm A8

It is operator-dependent, in a similar fashion to the A3 authentication algorithm, A8 takes *RAND* and *Ki* and produces a 64 bit output value that is then used as the ciphering key *Kc*. In most providers the A3 and A8 algorithms are combined into a single hash function known as COMP128. COMP128 algorithm creates KC and SRES, in a single instance.

5.3 Ciphering Algorithm A5

Once the user has been successfully authenticated to the network, he can make calls and use the services he is subscribed to. It is necessary to encrypt the data that is transmitted over the airways, so that if it is intercepted, it will not be intelligible and in effect useless to an adversary.

The algorithm used to encrypt the data to be transmitted is called the ciphering algorithm A5. The key *Kc* used in this algorithm is generated by the cipher key generation algorithm A8.In a similar fashion to the A3 authentication algorithm, A8 takes *RAND* and *Ki* and produces a 64 bit output value that is then used as the ciphering key *Kc*. A5 is a type of stream cipher that is implemented in the mobile station (MS) (as opposed to the

SIM, where A3 and A8 are implemented). It takes *Kc* as input and produces a key stream *KS* as output. The key stream is ex-ored (modulo 2 addition) with the plaintext *Pi*, which is organised in 114 bit blocks. The resulting ciphertext block is then transmitted over the airways 114 bits at a time.

Currently, there exists several implementations of this algorithm though the most commonly used ones are A5/0, A5/1 and A5/2. The reason for the different implementations is due to export restrictions of encryption technologies. A5/1 is the strongest version and is used widely in Western Europe and America, while the A5/2 is commonly used in Asia. Countries under UN Sanctions and certain third world countries use the A5/0, which comes with no encryption.

6 SYSTEM DESIGN

Design is both a process and a product [1]. The creative process of system design is the transformation of a process into a solution. The resulting product is a description of the solution, otherwise known as "System Design"

6.1 A3 Algorithm Input and Output

The A3 authentication algorithm has some parameters such as input and output with the specified key length. See table 1 and table 2

6.2 A3 Algorithm Model.

The concept that is used in developing a model for A3 algorithm is the concept of a 2 by 2 matrix. A 2 by 2 matrix is formed with the two inputs, Random Chanllenge and the subscriber's / authentication key (RAND and Ki) both of 128 bits to get the output Signal response(SRES) of 32 bits.

Below is the computer model.

Note: RAND = rnd;

1. $$\begin{pmatrix} \frac{rnd}{ki} & \frac{ki}{rnd} \\ \frac{rnd^2}{ki^2} & \frac{ki^2}{rnd^2} \end{pmatrix}$$
2. Find largest L
3. Find smallest S
4. Find v1 which is the first to be encountered and it is not the smallest in the matrix i.e not S
5. Find v2 which is the first to be encountered and it is not the largest in the matrix i.e not L
6. *Sres = v1 + v2 * ki*
7. Divide *sres* by *ki* until *sres* is 32 bits in size
8. *Sres* becomes the value gotten in 7.

6.3 Network databases

The network subsystem uses the following databases for the authentication and security purposes:

- The HLR database contains all administrative information about each registered user of a GSM network along with the current location of the MS
- The VLR tracks mobiles that are out of their home network, so that the network will know where to find them
- The EIR contains a list of each MS IMEI allowed on the network
  White listed – Allowed to connect to the network
  Grey listed – Under observation for possible problems
  Black listed – Not allowed to connect to the network
- The AUC database contains:
  IMSI: International Mobile Subscriber Identity
  TMSI: Temporary Mobile Subscriber Identity
  LAI: Location Area Identity
  Ki: Authentication Key

In this paper for the implementation of the A3 algorithm, two network databases were used, the HLR and VLR. See database table 3 and table 4

6.4 System Flowchart

The flowchart implementing the model in section 6.2

User authentication Algorithm (A3) Flowchart

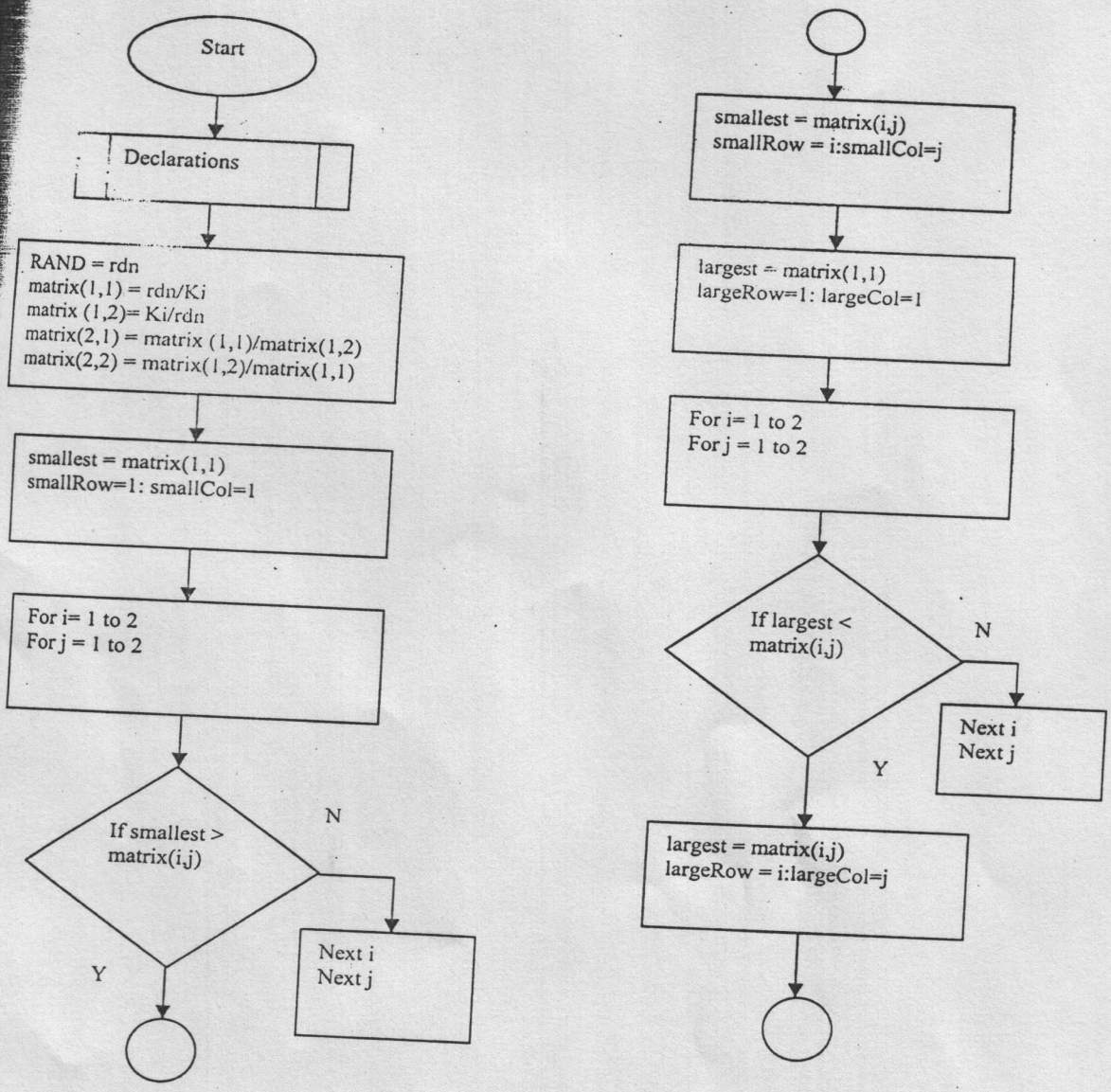


Figure 6.1

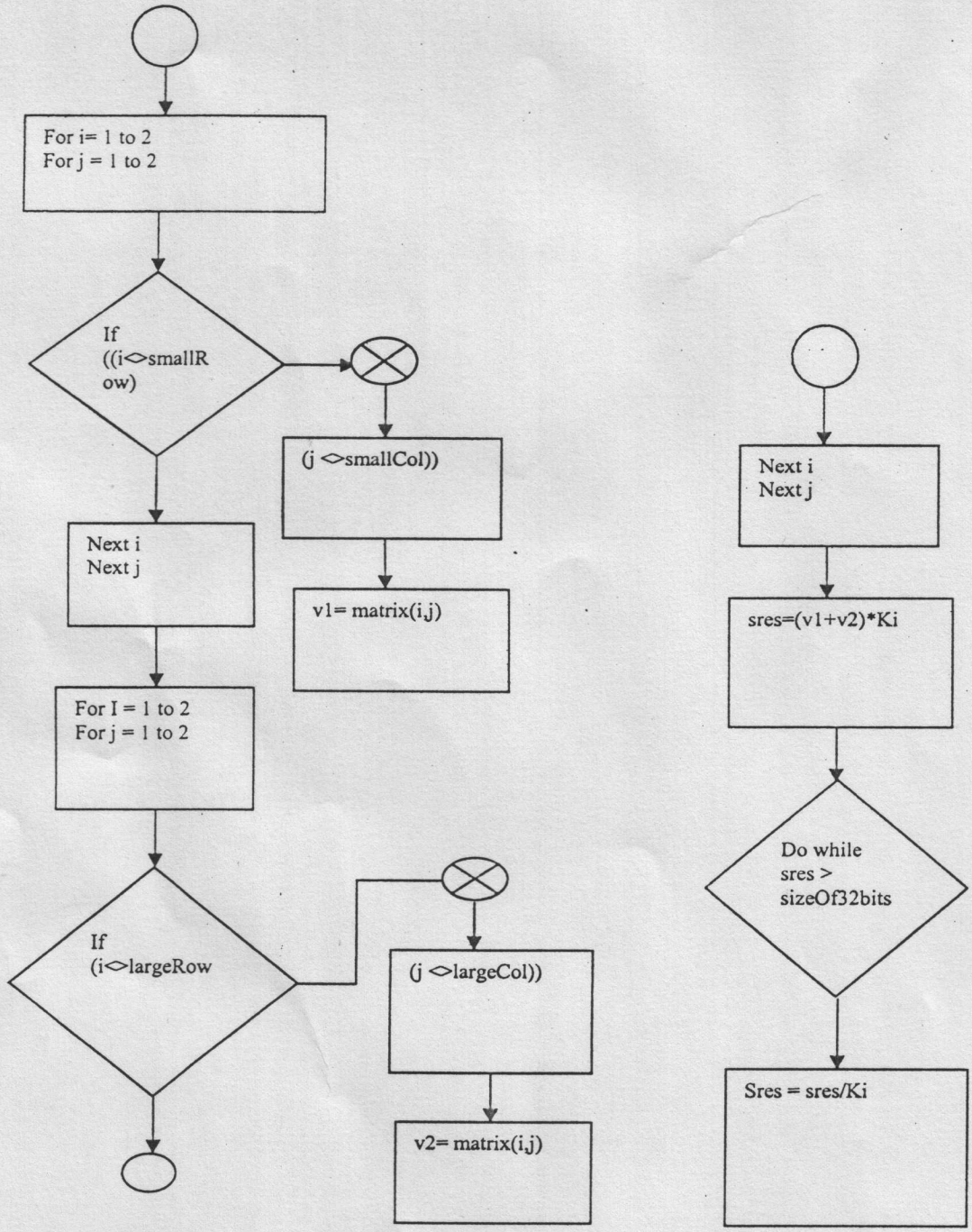


Figure 6.1(continued)

6.5 Performance evaluation of the implemented A3 algorithm model

By performance of an algorithm, we mean the amount of computer memory and the time needed to run algorithm. We have two approaches, the analytical and the experimental [1].

Analytical methods is used in computational analysis while conduction of experiment is used in performar analysis

In computational analysis we have both the space complexity of a program which is the amount of memc it needs to run to completion and the time complexity of a program which is the amount of the computer time needs to run to completion.

In this paper, using the space complexity for the evaluation of the performance of the implemented A algorithm model presented, it was discovered that sufficient memory was available to run our program and usii time complexity for the evaluation the program developed provide a satisfactorily real – time response. The runnir time of the algorithm is linear.

Table 1.Inputs to A3 Algorithm

PARAMETER	SIZE	COMMENT
K_i	128	Subscriber key $K_i[0]...K_i[127]$
RAND	128	Random challenge RAND[0]...RAND[127]

Table 2. A3 Algorithm Output

PARAMETER	SIZE	COMMENT
SRES	32	Signed response SRES[0]...SRES[31]

Table 3.HOME LOCATION REGISTER (HLR)

FIELD NAME	DATA TYPE	FIELD SIZE	DESCRIPTION
IMSI	Integer	20	International Mobile Subscriber's Identity
KI	Byte	16	Authentication key

Table 4.VISITOR LOCATION REGISTER (VLR) Table

FIELD NAME	DATA TYPE	FIELD SIZE	DESCRIPTION
IMSI	Integer	20	International Mobile Subscriber's Identity
TMSI	Integer	13	Temporary Mobile Subscriber's Identity
SIM NUMBER	Integer	11	Subscriber's Mobile Number

7. CHOICE OF PROGRAMMING LANGUAGE

Programs are a sequence of instruction given to the computer to carry out in order to accomplish a specific task. The choice of programming depends on the type of application involve.

The programming language chosen for the implementation of the A3 algorithm (user authentication) is Visual Basic 6.0. Visual basic 6.0 is an Object Oriented programming language that has the following features:

1. Visual Basic 6.0 can model a real life situation.
2. It is user friendly, easy to code and understand.
3. Active X technologies which allows for the usage of functionalities by other application (This features allow the system to be incorporated into existing application)
4. Pre-built objects can be utilized instead of writing numerous lines of codes to describe the appearance and location of the interface element.
5. Allows database integration with wide variety of applications
6. Authentication implies security. If the program source code is not secure, then the encrypted data can easily be decrypted by anybody who can read the program source codes. VB offers a way of making source codes secure through program compilation, thus offering great security.

8. PROGRAM SAMPLE OUTPUT

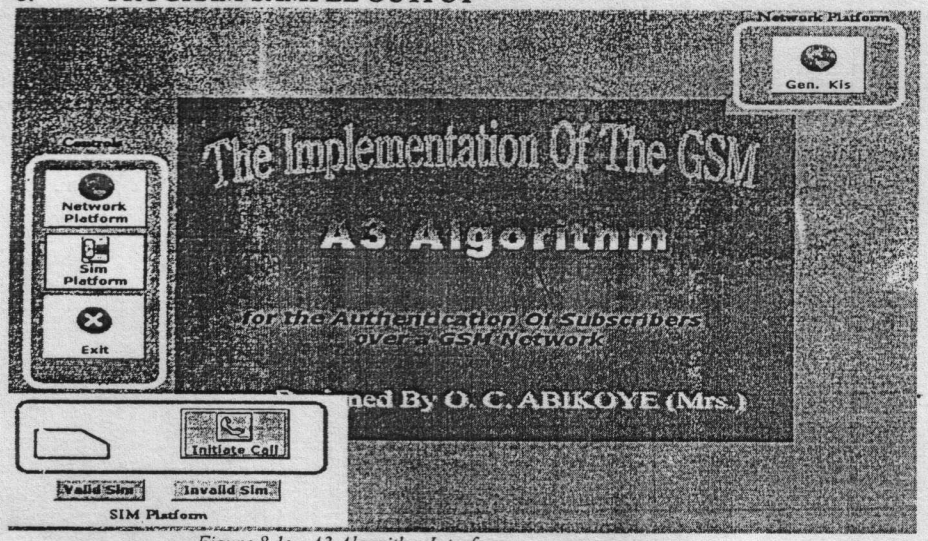


Figure 8.1: A3 Algorithm Interface

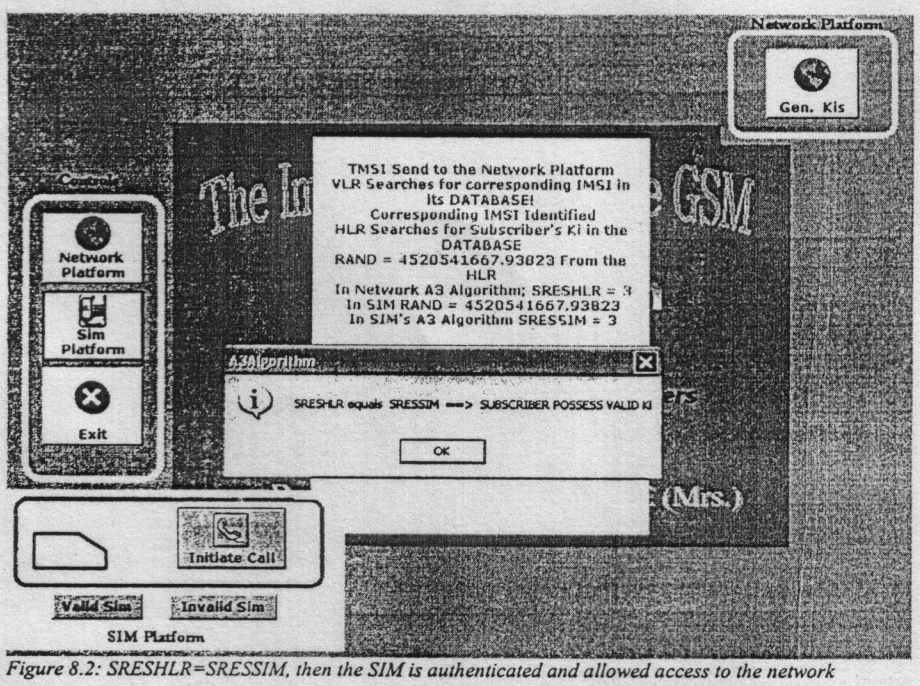


Figure 8.2: SRESHLR=SRESSIM, then the SIM is authenticated and allowed access to the network

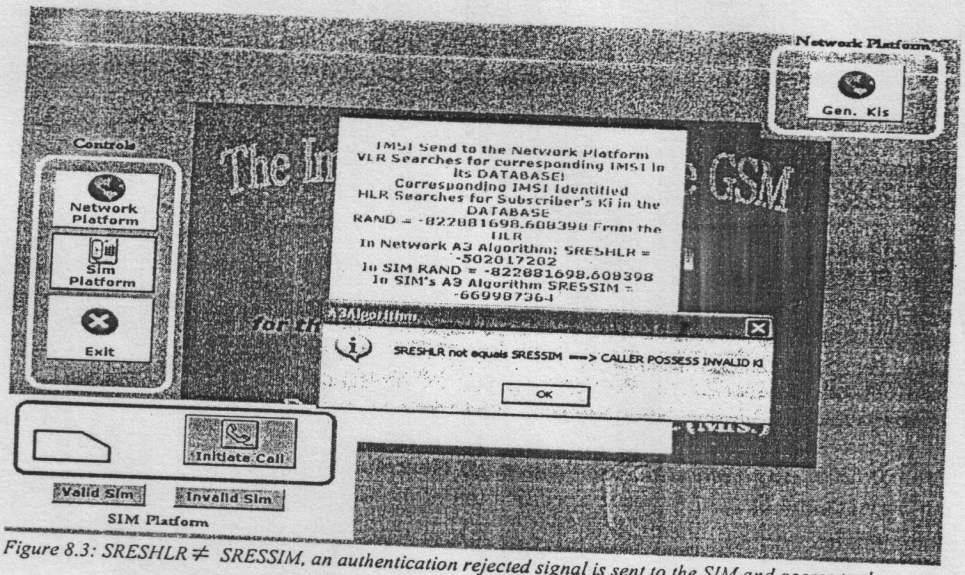


Figure 8.3: SRESHLR ≠ SRESSIM, an authentication rejected signal is sent to the SIM and access to the network is denied.

8.1 Discussion on the Simulation of the Proposed Model

The model presented for the A3 Authentication algorithm is simulated using Visual Basic 6.0 prograı language. The simulation is done using two platforms, the Network platform and the Sim platform. The simulation was test runned and the results obtained are as shown above in figure 8.1, 8.2 and 8.3.

Figure 8.1 shows the interface of the two platforms as designed (i.e the A3 Algorithm Interface).

In Figure 8.2, to generate 128bit *Ki* (Subscriber's key), the Network platform button is clicked or validity of *Ki* is its availability in one of the Network platform databases (HLR) and also in the Sim platform. T generated is stored on both the Sim platform and HLR for the authentication process.

To initiate a call for a subscriber with a valid Sim number is by clicking on the Valid Sim button and initiate call button on the Sim platform. To perform the authentication process, the Network Platform gener 128bits Random Chanllenge Number (*RAND*) and sends it to the Sim platform. On receiving the *RAND*, the platform uses the *Ki* that is already stored in its platform together with the *RAND* received from the Net platform to calculate 32bits SRESSIM using the model developed to implement the A3 authentication algor The SRESSIM is sent back to the Network platform for comparism with SRESHLR that is also calculated i network platform using 128 bits *Ki* which is stored in the HLR and 128 bit *RAND*. On comparism SRESHL SRESSIM, then the SIM is authenticated and allowed access to the network

In figure 8.3, to initiate a call for a subscriber with a invalid Sim number is by clicking on the invalid button(a Sim not having the correct 128 bit *Ki*) and on the initiate call button on the Sim platform. This initiate authentication process, and the SRESHLR and SRESSIM is calculated in the Network Platform and Sim plati respectively following the same procedure as discussed above. The SRESSIM is sent back to the Network platf for comparism with SRESHLR. On comparism SRESHLR ≠ SRESSIM, an authentication rejected signal is se the SIM and access to the network is denied. This is due to the fact that the Sim is invalid (i.e does not have correct *Ki*)

In the simulation of the entire system, the individual platforms were implemented as a program packag its own, and they communicate as a network oriented packages implemented using Visual Basic 6.0 programn language

9. CONCLUSION

GSM provides a basic range of security features to ensure adequate protection for both the operator customers. Its specification addresses three key security requirements, which are authentication, confidentiality a anonymity. There are three proprietary algorithms used to achieve authentication and confidentiality. These known as A3, A5 and A8. A3 is used to authenticate the SIM (Subscriber Identity Module) for access to network. A5 and A8 achieve confidentiality by scrambling the data sent across the airways. Anonymity is achie by use of temporary identities (TMSI).

This paper has presented a model for GSM A3 (User Authentication) algorithm and the model w implemented using Visual Basic 6.0 programming language. The GSM A3 algorithm model developed, no doubt useful for different GSM network operators like GLOBACOM, MTN, ZAIN etc

REFERENCES

[1.] Abikoye O.C(2006)" Computational Analysis and Implementation of GSM Security Algorithm:, M.Sc Project Work.

[2] David Margrave, George Mason University," GSM Security and Encryption" (www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html)

[3] GSM Security , Helsinki University of Technology S-38.153 Security of communication Protocols Mikko.Suominen@hut.fi(15.4.2003)URL:www.netlab.hut.fi/opetus/s38156

[4] Scourias, John "Overview of the Global System for Mobile Communications" (http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreprt.html)

[5.] Olivier Benoit, Nora Dabbous, Laurent Gauteron, Pierre Girard, Helena Handschuh, David Naccache, St´ephane Soci´e , Claire Whelan. "Mobile Terminal Security"

[6.] 3GPP TS 55.205 V6.0.0 (2002-12) *Technical Specification,*3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the GSM-MILENAGE Algorithms: An example algorithm set for the GSM Authentication and Key Generation functions A3 and A8 (Release 6).URL: http://www.3gpp.org