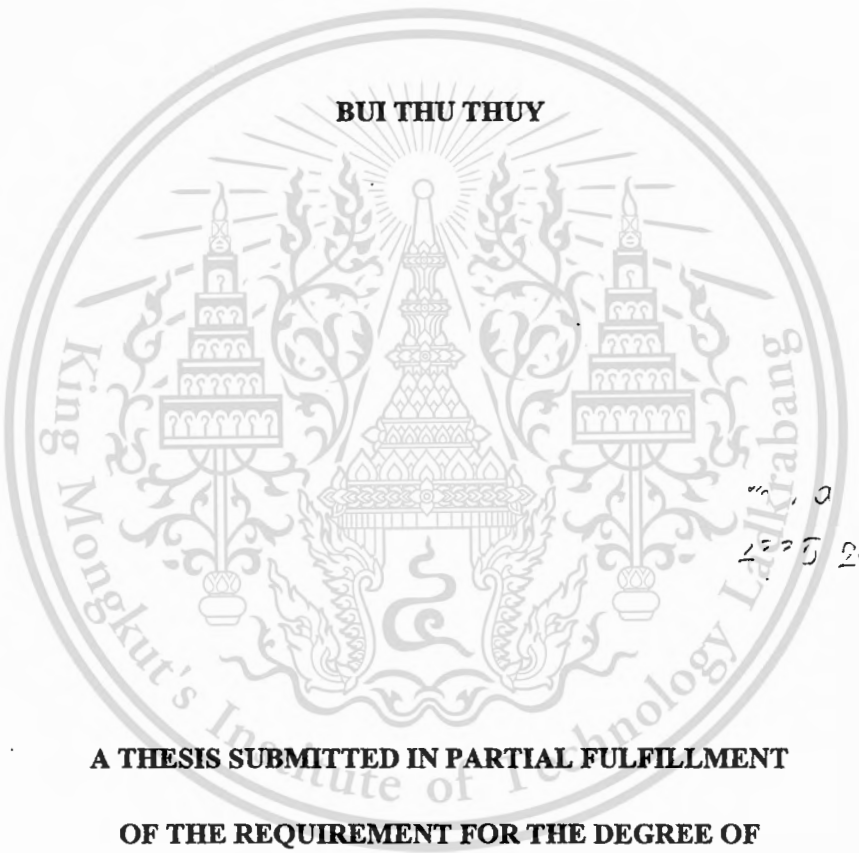
EFFICIENCY IMPROVEMENT OF AUTHENTICATION PROCESS FOR SECURITY IN GSM COMMUNICATION NETWORK

BUI THU THUY



A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN ELECTRONICS ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2010

KMITL-2010-EN-M-040-040

หัวข้อวิทยานิพนธ์	การปรับปรุงประสิทธิภาพของขบวนการรับรองตัวตนเพื่อความปลอดภัยในเครือข่ายสื่อสารจีเอสเอ็ม
นักศึกษา	นางสาว Bui Thu Thuy
รหัสนักศึกษา	51060417
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมอิเล็กทรอนิกส์
พ.ศ.	2553

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ. ดร. รัตติกร วรากูลศิริพันธุ์

บทคัดย่อ

การสื่อสารเคลื่อนที่ในระบบจีเอสเอ็ม (GSM) เป็นเทคโนโลยีด้านเซลลูล่าที่ได้ถูกใช้อย่างแพร่หลายไปทั่วโลกประชากรโลกประมาณ 3,000 ล้านคน กำลังใช้ระบบการสื่อสารจีเอสเอ็มในจุดประสงค์ต่างๆโดยเฉพาะอย่างยิ่งด้านการสื่อสารทางเสียงและบริการส่งข้อความสั้นๆ(SMS) แต่เนื่องจากการสื่อสารไร้สายเป็นระบบเปิดดังนั้นการป้องกันความเป็นส่วนตัวของการสนทนาระหว่างบุคคลสองฝ่ายจึงเป็นประเด็นสำคัญและเป็นส่วนทำให้เกิดวิธีการรักษาความปลอดภัยในการสื่อสารข้อมูลตลอดจนการป้องกันการหลอก ลวงทางโทรศัพท์เคลื่อนที่

โดยทั่วไปแล้วบริการด้านความปลอดภัยที่มีอยู่ในระบบจีเอสเอมที่มีส่วนสำคัญอย่างหนึ่งได้แก่ขบวนการรับรองตัวตน อย่างไรก็ตามขบวนการรับรองตัวตนในระบบจีเอสเอ็มปัจจุบันทำเพียงข้างเดียวนั่นคืออุปกรณ์โทรศัพท์เคลื่อนที่จะได้รับการรับรองตัวตนจากฝ่ายเครือข่ายเท่านั้น ซึ่งเป็นจุดอ่อนทำให้เกิดปัญหาด้านความปลอดภัยจากสาเหตุที่ถูกก่อกวนจากผู้ไม่ประสงค์ดีที่โจมตีระหว่างการสื่อสารได้ง่ายด้วยการแทรกตัวเองเข้าสู่เครือข่ายและสามารถแอบรับรหัสกุญแจรับรองตัวตนของผู้ใช้ที่ถูกต้องเพื่อนำไปใช้ แอบอ้างเสมือนกับเป็นผู้ใช้โทรศัพท์ เคลื่อนที่มีสิทธ์ใช้บริการ

ดังนั้นวิทยานิพนธ์นี้จึงได้เสนอการปรับปรุงประสิทธิภาพของขบวนการระบุตัวตนโดยใช้เทคนิค กุญแจสาธารณะ (Public Key) และกุญแจส่วนตัว (Private Key) สำหรับโปรโตคอลความปลอดภัย (Security Protocol)ในเครือข่ายสื่อสารจีเอสเอ็มซึ่งเทคนิคกุญแจสาธารณะจะถูกนำมาใช้เพื่อเข้ารหัสข้อมูลและ พิสูจน์ตัวตนในขบวนการรับรองตัวตนทำให้เกิดการรับรองตัวตนแบบร่วมกัน (Mutual Authentication)ระหว่างโทรศัพท์เคลื่อนที่และเครือข่ายจีเอสเอ็มพร้อมทั้งได้นำเสนอการ

ปรับปรุงการจัดเก็บข้อมูลในการ พิสูจน์ตัวตนในระบบจีเอสเอ็มเพื่อลดแบนด์วิดท์ (Bandwidth) ในการส่งข้อความในการรับรองตัวตน (Authentication Message)

จากการจำลองระบบแสดงให้เห็นว่าวิธีการเทคนิคกุญแจสาธารณะที่นำเสนอเพิ่มเวลาในการทำงานในระบบโดยรวมเพียงเล็กน้อยเมื่อเทียบกับระบบเดิมนอกจากนี้จากวิธีการที่นำเสนอยังสามารถลดการใช้ แบนด์วิดท์ในเครือข่ายในการส่งข้อความในการรับรองตัวตน

Thesis Title	Efficiency Improvement of Authentication Process for Security in GSM Communication Network
Student	Bui Thu Thuy
Student ID	51060417
Degree	Master of Engineering
Program	Electronics Engineering
Year	2010
Thesis Advisor	Assoc. Prof. Dr. Ruttikorn Varakulsiripunth

ABSTRACT

The Global System for Mobile Communications (GSM) is the most widely used cellular technology in the world. Approximately 3 billion people around the world are using GSM for different purposes, but mostly for voice communication and Short Message Service (SMS). However, because of the openness of wireless communications, how to protect the privacy between communicating parties is becoming a very important issue. The motivation for security in cellular telecommunications systems is to secure conversations and signaling data from interception as well as to prevent cellular telephone fraud.

Generally, one of the most important security service provided in GSM communication is the authentication process. However, the current authentication process in GSM is one-sided authentication. The mobile unit is only authenticated by the network. This is the weak point that leads to many security problems due to vulnerability against man-in-the-middle attack. The attacker who can interfere into the network is able to obtain the authentication key of a valid subscriber for impersonating itself as the valid or right mobile user.

Therefore, in order to overcome this problem, an efficiency improvement of identity process based on Public-key techniques for GSM security protocol is proposed. These techniques are used to provide mutual authentication in encryption and identification between mobile unit and GSM network. Finally, the storing of authentication data to decrease bandwidth for transmitting the authentication message is improved.

The results of simulation show that the time taken to apply the Public-key techniques is very small and our approach decrease bandwidth for transmitting the authentication message.

ACKNOWLEDGEMENTS

First of all, I am deeply indebted to my supervisor, Assoc. Prof. Dr. Ruttikorn Varakulsiripunth, for his helpful suggestions and constant support during this research at King Mongkut's Institute of Technology Ladkrabang (KMITL).

I would like to express my sincere thank to all the professors, lecturers, and staffs of Electronics Engineering Department, for their constructive comments and helpful discussions which gave me a better perspective on my own results.

My deep thanks go to ASEAN University Network/ Southeast Asia Engineering Education Development Network (AUN/Seed-Net) for awarding me the scholarship to study in Thailand where I can produce this thesis.

I should also mention that Hanoi University of Technology (HUT) was gave me the opportunity to pursue my study.

Many of my colleagues had contributions for this thesis. I would like to say thank to my special friends, Mr. Narissorn Sangkanong, Mr. Saiyan Saiyod, and Ms. Teav Keov Kolyan, who have accompanied me throughout my master journey. They have always been there when I needed them. Without their support and helpful discussion, I could not have succeeded in my research as well as my life in Thailand. I will always remember the time we had together and wish them all success in their careers and happiness in their lives. I also want to thank all members of Communication Network Laboratory for their help and support to my research in the Laboratory.

And finally, I would like to acknowledgement the support of my father and my mother. Their love, encouragement, belief and understanding made everything I have possible.

Bangkok, Thailand
April, 2010

Bui Thu Thuy

Table of Contents

List of Tables

List of Figures

ABBREVIATIONS

A3	Authentication algorithm A3
A5	Encryption algorithm
A5/1	Encryption algorithm A5/1
A5/2	Encryption algorithm A5/2
A8	Encryption key generating algorithm A8
AuC	Authentication Center
BCCH	Broadcast Channels
BS	Base Station
BSC	Base Station Controller
BSS	Base Station System
BTS	Base Transceiver Station
CA	Certificate Authority
CCCH	Common Control Channels
CEPT	Conference of European Post and Telecommunications
COMP128	A single algorithm performing the functions of A3 and A8
DC	Digital Certificate
DCCH	Dedicated Control Channels
DSA	Digital Signature Algorithm
EIR	Equipment Identification Register
ETSI	European Telecommunications Standards Institute
ECC	Elliptic Curve Cryptography
FDMA	Frequency Division Multiple Access
Fn	Frame Number
GMSK	Gaussian Minimum Shift Keying
GSM	Global System for Mobile Communications
GSM MoU	The GSM Memorandum of Understanding, an agreement signed between all the major European operators to work together to promote GSM. The precursor of the GSM Association

HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telecommunications
ISDN	Integrated Services Digital Network, a data network usually provided by public carries (providing digital communication at 56k (US and Japan) or 64k (rest of world)).
K_c	Ciphering Key
K_i	Individual Subscriber Authentication Key
LAI	Location Area Identifier
LFSR	Linear Feedback Shift Register
ME	Mobile Equipment
MNC	Mobile Network Code
MSC	Mobile-service Switching Center, Mobile Switching Center
MU	Mobile Unit
NMC	Network Management Center
NSS	Network Subsystem
OMC	Operation and Maintenance Center
OSS	Operation Support Subsystem
PCS	Personal Communication Services
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
PLMN	Public Lands Mobile Network
PSTN	Public Switched Telephone Network
PUK	Personal Unblocking Key
RAND	Random Number
RR	Radio Resource
RSA	Stands for Rivest, Shamir, and Adleman
RSS	Radio Subsystem
SIM	Subscriber Identity Module
SMS	Short Message Service

SRES	Singed Response
SS7	Signaling System 7
TCH/FR	Traffic Channel/ Full-Rate speed
TDMA	Time Division Multiple Access
TMN	Telecommunication Management Network
TMSI	Temporary Mobile Subscriber Identity
TRAU	Transcoder and Rate Adapted Unit
UMTS	Universal Mobile Telephone System
VLR	Visitor Location Register

Chapter 1

Introduction

1.1 Motivation

Global System for Mobile Communication (GSM) is the European standard for second generation mobile system. In the past decade, GSM has become widespread throughout the world. While earlier analog wireless systems were used by only few people, GSM was used by over 1.5 billion worldwide subscribers at the end of 2005. On June 2008, more than 2.9 billion subscribers were using GSM corresponding to a market share of more than 81%, and its story continues, even now, despite the introduction and development of next-generation systems such as International Mobile Telecommunications (IMT-2000) or Universal Mobile Telephone System (UMTS) (3G) and even systems beyond 3G, dubbed IMT-Advanced.

The GSM standard was designed to be a secure mobile phone system with strong subscriber authentication and over-the-air transmission encryption. The security model and algorithms were developed in secrecy and were never published.

Eventually some of the algorithms and specifications have leaked out. The algorithms have been studied and critical errors have been found. Thus, after a closer look at the GSM standard, one can see that the security model is not all that good.

The motivation of the research in cellular telecommunication systems is to secure the conversations and the signaling data from interception as well as to prevent cellular telephone fraud. Therefore, security is an important concern at the core of GSM technologies. The most notable demonstration is the use of a Subscriber Identity Module (SIM) card to store sensitive data on handsets and to protect against mobile fraud. Although it seems to be secure enough over the past 15 years, with the new methods of recent cryptanalysis, GSM security system becomes vulnerable and possible to be attacked.

In this research, the security of the GSM network is evaluated. A complete and brief review of GSM network security problems is also presented. The measurement used in the GSM, such as

authentication, confidentiality and anonymity, gives the mobile phone's users some privacy and anonymity, and protects the system from the fraudulent use.

1.2 Goal and Objective

GSM standard was supposed to prevent phone cloning and over-the-air eavesdropping. It is possible to be done with little additional work compared to the analog mobile phone systems. It also can be implemented through various attacks.

The objectives of this thesis are:

1) to show some weaknesses in the security of GSM such as in algorithms, fake base station, authentication protocol,

2) to propose some measurement to prevent flaws in order to implore the new technologies that overcome the weaknesses in GSM security,

3) to simulate, analyze and evaluate the proposed measurement. The evaluation will be done through simulation.

The goal of this thesis was to:

- Get a general understanding of GSM network
- Found out some flaws in GSM security
- Overcome the weakness in GSM security model by new methods.

Furthermore, with the expanded developments in the GSM technology, it is believed that, secured methods will be used in the system to give better security.

1.3 Theory

GSM operates in the 900MHz, 1800MHz, or 1900MHz frequency bands by "digitizing and compressing data and then sending it down a channel with two other streams of user data, each in its own time slots", GSM provides a secure and confidential method of communication.

Security system in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. Authentication is intended to allow a GSM network operator to verify the identity of

a user in such a way so that someone is impossible to make fraudulent calls by masquerading as a genuine user. Confidentiality protects the user traffic, voice and data, and sensitive signaling data, such as dialed telephone numbers, against eavesdropping on the radio path. Anonymity was designed to protect the user against someone, who knows the user's International Mobile Subscriber Identity (IMSI), to use the information to track the location of the user or to identify calls that is made to or from that user by eavesdropping on the radio path.

The subscriber is uniquely identified by the IMSI. This information is identified along with the Individual Subscriber Authentication Key (K_i). The design of the GSM authentication and encryption schemes is designed in the way so that the sensitive information is never transmitted over the radio channel. Moreover, a challenge-response mechanism is used to perform authentication. The actual conversations are encrypted using a temporary, randomly generated ciphering key (K_c). The mobile unit identifies itself by means of the Temporary Mobile Subscriber Identity (TMSI), which is issued by the network and may be changed periodically for additional security.

The security mechanism of GSM is implemented in three different system elements; the Subscriber Identity Module (SIM), the GSM handset or Mobile Unit (MU), and the GSM network.

The SIM contains the IMSI, the individual 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, and A8) are present in the GSM network as well.

The Authentication Center (AuC), part of the Operation and Maintenance Subsystem (OMC) of the GSM network, consists of IMSI, TMSI, Location Area Identity (LAI), and the individual subscriber authentication key (K_i) for each user.

In order to do the authentication and security mechanism, all three elements (SIM, handset, and GSM network) are required. The distribution of security credentials and encryption algorithms provides an additional measurement of security both in ensuring the privacy of cellular telephone conversations and in the prevention of cellular telephone fraud.

Figure 1.1 demonstrates the distribution of security information among the three system elements, the SIM, the MU and the GSM network. Within the GSM network, the security information is further distributed among the AuC, the Home Location Register (HLR), and the Visitor Location Register (VLR). The AuC is responsible for generating the sets of RAND, SRES, and K_c which are stored in the HLR and VLR for subsequent use in the authentication and encryption processes.

Here, RAND is the random number that generated by SIM and HLR in term of variable number of bits for authentication when a MU will access to the network. SRES is the signed response that generated by SIM and HLR based on RAND and K_i in term of variable of bits used for allowing a MU to access to the network. K_c is the session key that generated by SIM and HLR based on RAND and K_i in term of variable of bits used for encrypting and decrypting authentication message between a MU and the network.

According to the GSM specifications, neither authentication nor data encryption is carried out between the VLR and HLR. These two components exchange data, under the auspices of a mutual trust relationship. Within the Public Land Mobile Network (PLMN) setting, the level of trust can be justified.

However, when international roaming is taken into consideration, there is a need to enhance the security, i.e. based on strong cryptographic methods.

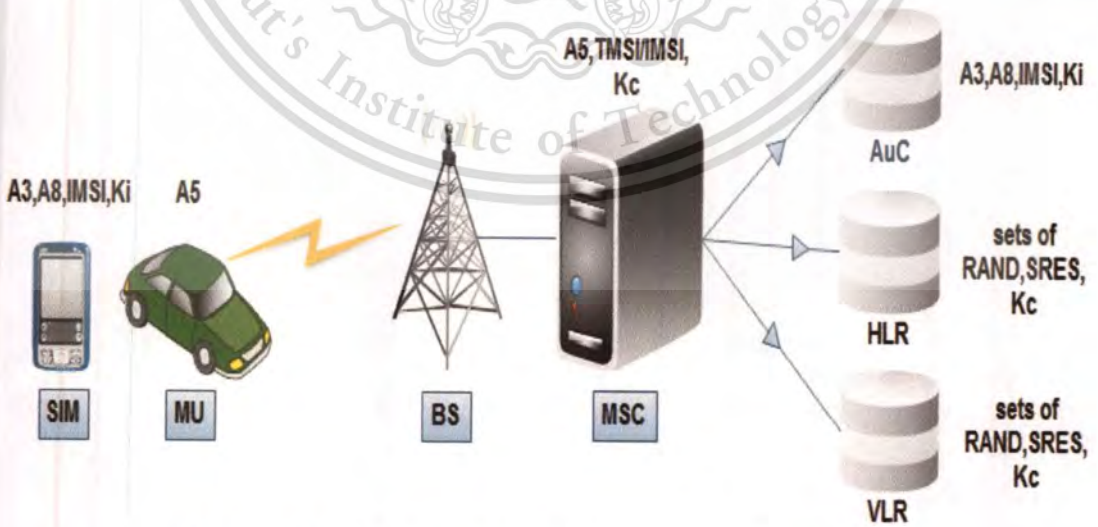


Figure 1.1 Distribution of Security Features in the GSM Networks.

In any event, the VLR-HLR link remains vulnerable to third-party attacks. Moreover, the MU-VLR link is also vulnerable. The lack of mutual authentication and the absence of data encryption, during the initial phase of the authentication process, render this link insecure. As a matter of fact, data encryption cannot be initiated until the authentication process is completed.

1.4 Process of the Study

The research was begun with the comprehensive review of the concept GSM network. Then, the security issues and challenge in GSM network which concern with the problems in GSM network security is observed. Finally, the new idea in authentication protocol which overcomes the GSM security weakness is proposed. The proposed method uses Public-key techniques inside the authentication process.

The simulation script in program Java to define the network is written. The result of simulation is an output trace file. Finally, this research work is concluded by providing the conclusions and some issues for future work.

1.5 Scope and Organization of this Thesis

As a guide to read this thesis, its structure and contribution are briefly summarized as follows

Chapter 1 gives a short review of the GSM network and security system used in GSM, as well as the motivation of the research.

Chapter 2 provides some fundamental background related to this thesis. It covers the basic elements of a GSM system, GSM security model, as well as their combination.

Chapter 3 contains the main contribution of the thesis. In this chapter, the problem in authentication protocol security of the GSM network is defined. Furthermore, the existing solutions for both algorithms and authentication protocol weaknesses are presented. Importantly, the solution to the current problem of authentication process by using Public-key techniques and comparing the existing scheme is proposed.

Chapter 4 illustrates the performance of the proposed solution.

Chapter 5 concludes the thesis by summarizing the main results and discussing potential future work.

Chapter 2

Literature Review

This chapter presents the main concepts and fundamental techniques of the GSM networks.

The technology that has applied to the GSM system work is introduced. It will describe the architecture of its complex signaling system by presenting the logical layers used in GSM, the functional entities in the signaling system, the way signaling is done and the channels used for signaling and traffic. The goal is to get a feeling and a basic understanding of the protocols and functions necessary to establish, maintain and terminate mobile connections. Furthermore, a brief introduction to GSM functions and the architecture of the GSM network is provided. This will include a description of the components that build up the system, how these are interconnected, and also to introduce the mechanism used that protect the system's valuable assets. Then, security model in GSM networks reviews is also included. This information will later be used in attacking the system.

2.1 Background

GSM is an acronym for Global System for Mobile Communication (derived from *Group Special Mobile*) which is the most widely accepted standard for digital cellular communications. Even though the idea of a cell based radio communication system originated at the Bell Labs in the early 1970s the idea was not implemented until mobile communication systems experienced a rapid growth in Europe, particularly in UK and Scandinavia. In the early 1980s when the initial growth of cellular phones was just starting in Europe, a need was felt to have a uniform standard for mobile phones that would equipment and technology being developed could be used in different regions. To overcome the problems posed by the rapid growth of mobile phones, the Group Special Mobile (GSM) was formed by the *Conference of European Post and Telecommunications* (CEPT). The GSM had to meet the following criteria:

- Spectrum
- Smooth international roaming
- Cheaper mobile phones

- Enhanced voice quality
- Compatible with *Integrated Services Digital Network* (ISDN) and other systems
- Ability to provide new services

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 [1]. The most important events in the development of the GSM system are presented in Table 2.1.

Nowadays, GSM is not just a European standard; GSM networks are operational in more than 200 countries around the world. The number of GSM subscribers is increasing at an exponential rate. GSM provides enhanced features over older analog-based systems, which are summarized below:

- 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.
- 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 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.

Table 2.1 Events in the development of GSM System.

Year	Events
1982	CEPT establishes a GSM group in order to develop the standards for a Pan-European cellular mobile system.
1985	Adoption of a list of recommendations to be generated by the group.
1986	Field tests were performed in order to test the different radio techniques proposed for the air interface.
1987	*Time Division Multiple Access* (TDMA) is chosen as access method (in fact, it will be with *Frequency Division Multiple Access* (FDMA)) Initial *Memorandum of Understanding* (MoU) signed by telecommunication operators (representing 12 countries).
1988	Validation of the GSM system.
1989	The responsibility of the GSM specifications is passed to the *European Telecommunication Standards Institute* (ETSI).
1990	Appearance of the phase 1 of the GSM specifications.
1991	Commercial launch of the GSM service.
1992	Enlargement of the countries that signed the GSM-MoU > Coverage of larger cities/airports.
1993	Coverage of main roads GSM services start outside (the new name "*Global System for Mobile Communications*" was given to GSM).
1995	Phase 2 of the GSM specifications coverage of rural areas.

One major force for change to fully digital cellular systems is the need for higher system capacities. A further driving force is the worldwide digitization of the telephone network and its progress to ISDN. Digital cellular systems, forming extensions of the PSTN, called PLMN, will be an extension of the ISDN, using digital radio techniques for the short trip between the cellular infrastructure and the mobile subscriber terminal equipment.

2.2 Channel and Signaling Principles in the GSM System

2.2.1 Frequency-Division Multiple Access and Time-Division Multiple Access

GSM uses Time-Division multiple access (TDMA) on top of Frequency-Division multiple access (FDMA) in order to provide users with access to the radio resources in GSM. With FDMA, users are assigned a channel from a limited set of channels ordered in the frequency domain. Usually, the initial assignments to channels are made from a common control channel, to which all radios tune for instructions when they first try to use the system. Since there is a limited divide the use of each channel between several users. In TDMA, users share a physical channel where they are assigned time slots. All the users sharing the physical resource have their own assigned repeating time slot within a group of time slots called a frame. So in GSM, users are sorted onto a physical channel in accordance with simple FDMA techniques. Then the channel's use is divided up in time into frames, during which eight different users share the channel. A GSM time slot is 577ms, and each user gets to use the channel for 577ms every 4.615 ms (577ms. 8 slots = 4.615 ms) [2].

2.2.2 The Radio Channel

Cellular radio uses the word channel in many ways. It is a pair of radio frequencies, used by two entities to communicate with each other. There are two sources of trouble in the channel: noise and interference. Channel coding is applied to the channel in order to minimize the influence of these destructive forces on the transmitted signal [2].

2.2.3 The Frequency Band

The frequencies used in GSM are defined in the FDMA part of the physical layer. GSM uses three different frequency bands, 900 MHz, 1800 MHz and 1900 MHz. The frequency bands used within each of the three ranges are similar and therefore only the frequency usage in the 900

MHz range is described in Figure 2.1. In the 900 MHz GSM, two 25-MHz frequency bands are used. The mobile unit transmits in the 890- to 915-MHz range, and the base station transmits in the 935- to 960-MHz [2].

The end points within the physical layer are the mobile unit and the BTS. The MU- to- BTS direction is referred to as the *uplink* (ul) and the BTS-to-MU direction as the *downlink* (dl) [2].

The frequency bands are divided into 125 channels widths of 200 kHz each. These channels are numbered from 0 to 124. Channel number 0 is used as a guard band between GSM and other services on lower frequencies. Any frequency may be assigned to a mobile unit by the base station from a selection of between 1 and approximately 16 frequencies. The number of channels a base station may have at its disposal depends on network planning considerations and the traffic density expected in the base station's coverage area [2].

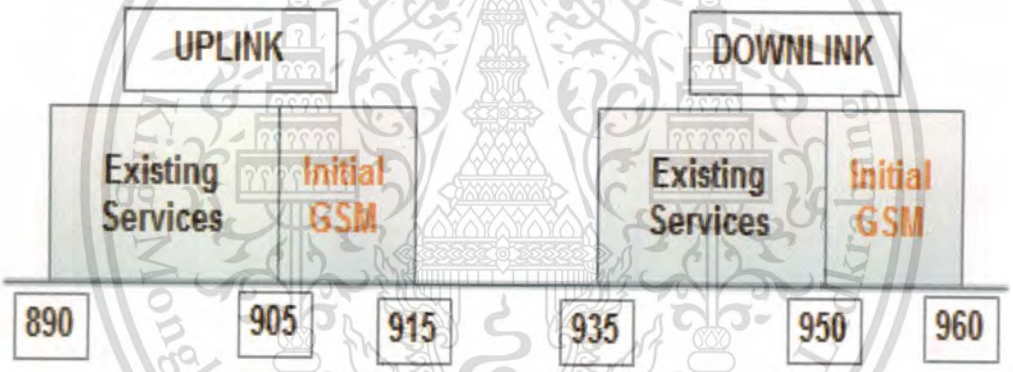


Figure 2.1 The GSM 900MHz frequency band.

2.2.4 Transmission on the Radio Channels

As mentioned in Section 2.2.1, TDMA is used to make additional allocation in the time domain. This means that each frequency channel is further subdivided into eight different time slots numbered from 0 to 7. Each of the eight time slots is assigned to an individual user. A set of eight time slots is referred to as a TDMA FRAME in Figure 2.2, and all of the users of a single frequency share a common frame.

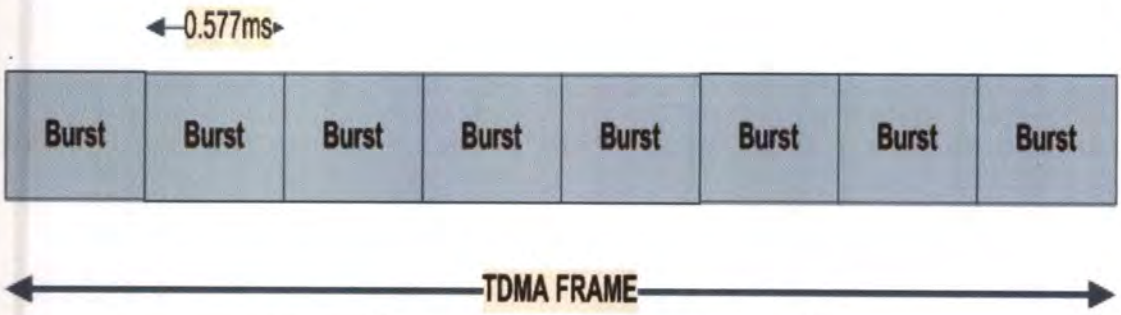


Figure 2.2 The structure of the TDMA frames [3].

If a mobile, for example, is assigned time slots number 1, it transmits only in this time slot and stays idle for the remaining seven time slots with its transmitter off. The mobile's regular and periodic switching (on and off) of its transmitter is called *bursting* and results in a so called *burst*. The length of a time slot, which is equivalent to a burst from a mobile, is as already mentioned 577 ms, and the length of a TDMA frame is 4.615 ms (8. 577ms = 4.615 ms) [2].

Information is moved between mobiles as data (ones and zeros) that are confined to time slots. Each slot contains a burst, which is the information. Depending on the sort of information to be transmitted, different burst structures are used. GSM uses four different burst structures:

- The normal burst
- The "F" of frequency control burst
- The "S" of synchronous control burst
- The access control burst [2].

A fifth type of burst is the *dummy burst* which is to be sent downlink continuously in order to make the detection of a base station easier.

The *normal burst* is the most common burst in GSM and will therefore be described below. The normal burst is used to carry data and most signaling. It has a total length of 156.25 bits, made up of two 57 bits information bits, a 26 bits training sequence used for equalization, 1 stealing bit for each information block, 3 tail bits at each end, and an 8.25 bits guard sequence as shown in Figure 2.3. The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 Kbps [4].

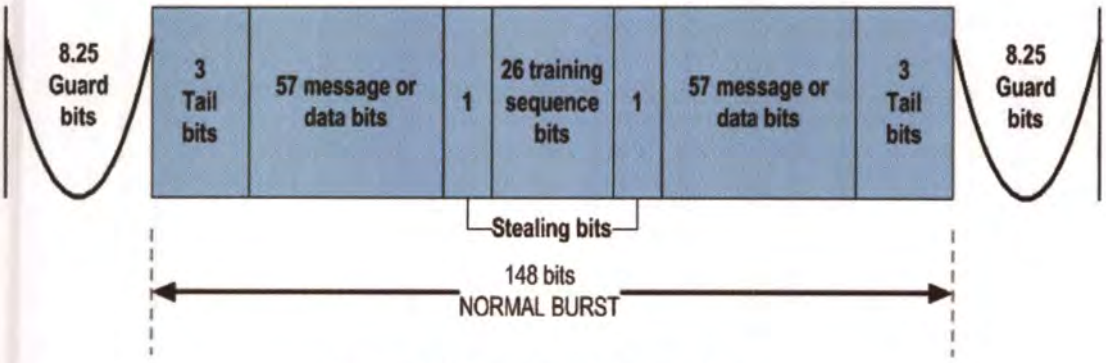


Figure 2.3 Structure of a normal burst.

This burst carries the conversation content in digital form. That's what the two 57 information, message, or data bits are for. The normal burst also carries signaling information needed to manage, call processing, which is data for setting up, maintaining and ending a call. The different types of bits are described below:

- *Training sequence bits*: These bits get the BTS and the MU in "tune" with each other.
- *Stealing bits*: These bits are used to keep the mobile terminal linked to the base station even when there is no connection, when entering a tunnel or possible when a large truck gets in the way.
- *Tail bits*: These bits are always set to zero and are used as guard time.
- *Guard bits*: These bits are empty time spaces separating data packets to make sure one burst does not run into another [4].

2.2.5 Logical Channel

With the concept of logical channels, the physics of the signals in GSM is getting farther away and the information carried is getting closer. The way information is moved depends on the type of information. Different types of information can exist in the system on different types of logical channels. The contents of the different logical channels can appear in any physical channel (frequency and time slots) [2].

A logical channel carries signaling data, or a user's data. The data, of whatever kind, are mapped onto a physical channel. The manner in which the data are mapped onto the physical resource depends on the data's content. One should be more careful with important data than the more trivial data [2].

GSM distinguishes between *traffic channels*, which are reserved for user data (speech and data), and *control channels*, which are used for network management messages and some channel maintenance tasks. The signaling (using the control channels) is the most important here and will be described more closely [2].

The control channels are divided into four different classes:

- Broadcast channels (BCCH)
- Common control channels (CCCH)
- Dedicated control channels (DCCH)
- Associated control channels [2].

Transmission of speech is done using the *traffic channel/full-rate speech* (TCH/FR). The net speech rate is 13 Kbps.

2.2.6 Frame Structures

In a manner similar to the TDMA frame structure that allows time slots to be ordered on a carrier, there are also some *multiframe* structures made of a fixed number of TDMA frames that allow logical channels to be ordered into time slots. There is big difference between the logical channels that carry speech data and those that carry signaling data. A 26-*multiframe* structure is used for the traffic, and a 51-*multiframe* structure is used for the signaling. To combine both structures onto the radio interface, a new frame format is introduced: the *superframe*. The superframe has a length of 51. 26 = 1.326 TDMA frames. Superframes are used to build *hyperframes*, which consists of 2.048 superframes [2] as illustrated in Figure 2.4 and Figure 2.5.

The system sometimes refers to frame numbers within a hyperframe context, and the hyperframe represents the most comprehensive structure in the system and lasts for nearly 3.5 hours before it is repeated. This organization of frames and frame types makes it easy to determine what sort of information communicating entities expect to find in a given period of time [2].

When speaking about signaling, it is important to know exactly which frame is currently being transmitted. To remove the possibility of ambiguity, the frames are numbered in a special way: there are three counters, which will be called T1, T2 and T3. Counter T1 counts the superframes [2].

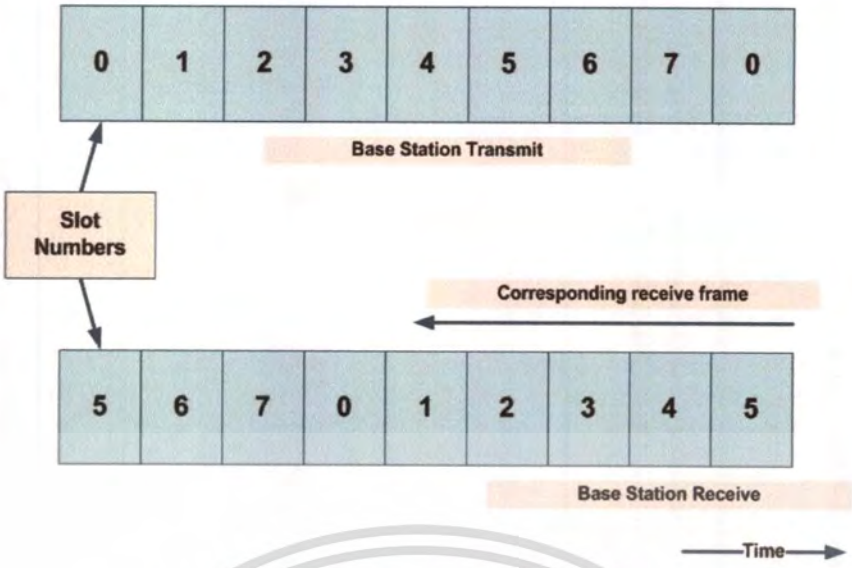


Figure 2.4 Basic GSM frame structure.

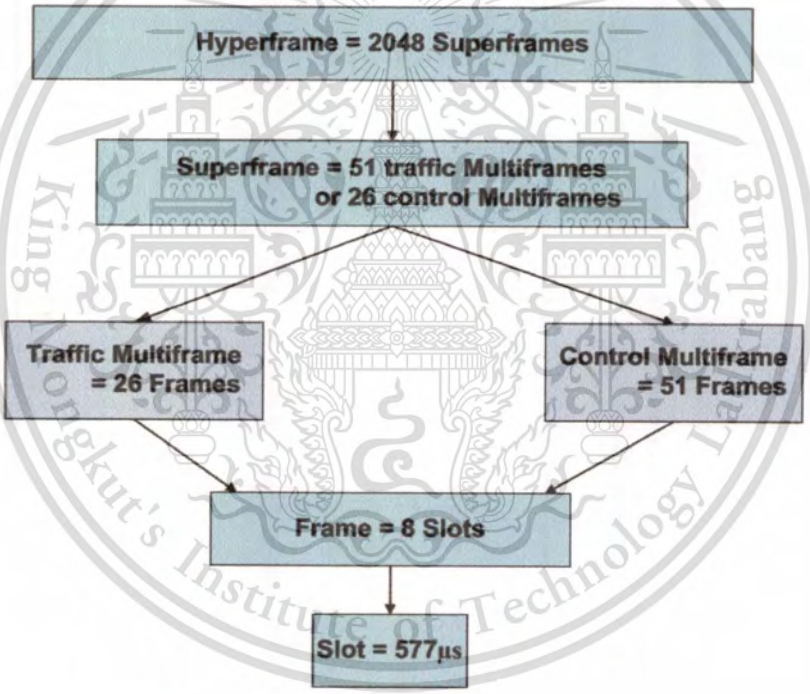


Figure 2.5 GSM frame structure summary.

Whenever a superframe is completed, T1 is incremented by 1. T1 has values between 0 and 2.047; there are 2.048 superframes in a hyperframe. T2 counts the speech frames, which only occur in 26-multiframe structures. T2's value, therefore, ranges from 0 to 25. Finally, T3 counts the signaling frames, which are 51-multiframe structures. Similarly to the traffic counter, T3's contents can be anything from 0 to 50. At some starting time, all three counters are set to 0, and then the

frames start to be transmitted. Whenever a speech or a signaling multiframe structure is finished, its respective counters (T2 and T3) are reset to 0 and start again. After 1.326 TDMA frames, both T2 and T3 are finally reset together and start counting again from 0 at that time. This marks the duration of one superframe. When the first superframe is completed, T1 is increments by 1 count. T1 only reset after 2.047 counts, which takes exactly 3h28 min 53s 760ms to do, and this is the duration of a hyperframe. If one knows the values in the T1, T2 and T3 counters, then one knows exactly what is in each and every time slot at that instant, provided one knows what kind of multiframe was assigned to each of the eight available time slots in the TDMA frame. An entity knowing T2 and T3 easily finds the BCCH and the system information. This fact makes it easy for MUs entering a new area to find the frequency of the specific area and start tuning the new cell. The counters mentioned above make up the *Frame Number* (Fn), which is used together with the session key as input to the encryption algorithm used for voice encryption in GSM [2].

2.3 An overview of the GSM network

A GSM system is basically designed as a combination of three major subsystems: the network subsystem, the radio subsystem, and the operation support subsystem. In order to ensure that network operators will have several sources of cellular infrastructure equipment, GSM decided to specify not only the air interface, but also the main interfaces that identify different parts. They form a Public Land Mobile Network (PLMN) together [5]. There are three dominant interfaces, namely, an interface between MSC and the Base Station Controller (BSC), an A-bis interface between BSC and the Base Transceiver Station (BTS), and an Um interface between the BTS and MU. These three major subsystem and interfaces are shown in Figure 2.6.

The RSS is composed of the mobile telephone, which is called the Mobile Unit (MU) and the Base Station Subsystem (BSS).

The MU consists of two physically and logically separate components, which are called Mobile Equipment (ME) and the Subscriber Identity Module (SIM). The ME is the radio and encryption component with the user interface, while the SIM is the correct designation for a GSM-specific smart card. These two components together form the operational mobile telephone.

As a rule, the BSS is formed by the base stations located at the center of each cell. The functions of the BSS are to establish contact with the mobile telephones via the air interface and to supply data to the higher-level components of the network. A base station consists of one or more a Base Transceiver Stations (BTSs) and a Base Station Controller (BSC).

A BTS performs all the transmission and reception functions relating to the GSM. In some ways, the BTS can be considered to be a complex radio modem that takes the up-link radio signal of the MU and convert it into data. An important part of the BTS is *Transcoder and Rate Adapted Unit* (TRAU).

The function of BSC is to manage all radio interfaces through command control from BTS and MU, release wireless channel and manage transmission.

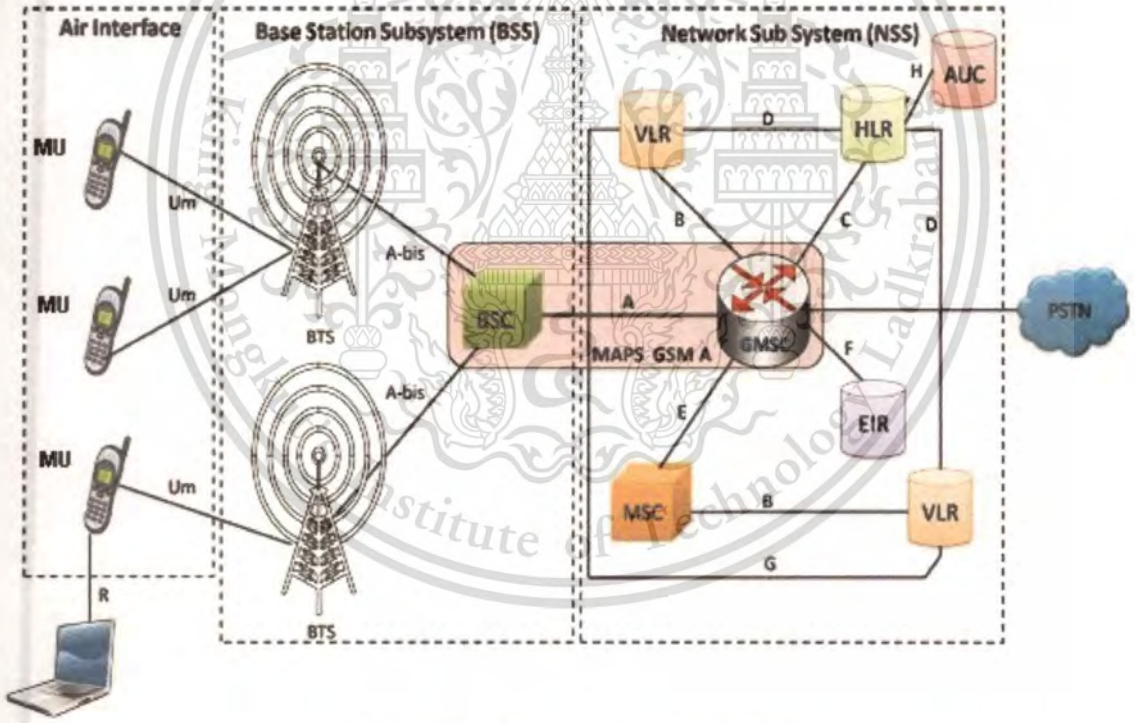


Figure 2.6 Basic GSM architecture.

The NSS essentially consists of the Mobile Switching Center (MSC) and the Visitor Location Register (VLR). A MSC manages multiple BSS. It forms the link between the BSS connected to it, other MSC and, the Public Switched Telephone Network (PSTN). The MSC is

responsible for setting up, managing and shutting down connections, handling call charges and supervising supplementary services, such as call forwarding, call blocking and conference calling.

The VLR contains information about all MUs currently within range of the associated MSC. This information is needed for functions such as routing a call to a particular mobile phone via the proper BSS and radio cell. The VLR also maintains a list of mobile units which belongs to subscribers of other networks that have logged into the network of the associated MSC via roaming.

The topmost hierarchical level in a GSM system is the Operation Subsystem (OSS). It consists of the Operation and Maintenance Center (OMC), the Authentication Center (AuC), the Home Location Register (HLR) and the Equipment Identity Register (EIR).

The OMC is responsible for regular network operation, subscriber administration and call billing.

The AuC is the security component on the network side, and in a manner of speaking it is the counterpart to the SIM on the mobile side. It generates and manages all keys and algorithms needed for operating the system, especially for authentication of the MU.

Another central component is the HLR, which contains all of the subscriber data as well as the localization data for each of the MUs.

The EIR is the component to the HLR for MUs instead of subscribers. It contains essential data, such as the serial number of all MUs represented in the network.

These different components are described below:

- The Mobile Unit (MU)
- The Base Transceiver Station (BTS)
- The Base Station Controller (BSC)
- The Mobile Services Switching Center (MSC)
- Home Location Register (HLR)
- Authentication Center (AuC)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)

- Operation and Maintenance Center (OMC)
- Network Management Center (NMC).

2.3.1 The Mobile Unit

The primacy functions of Mobile Unit (MU) are to transmit and receive voice and data over the air interface of the GSM system. MU performs the signal processing functions of digitizing, encoding, error protecting, encrypting, and modulating the transmitted signals. It also performs the inverse functions on the received signals from the base station. A list relevant function includes the following:

- Voice and data transmission;
- Frequency and time synchronization;
- Monitoring of power and signal quality of the surrounding cells for optimum handovers;
- Provision of location updates;
- Equalization of multi-path distortions;
- Display of short message up to 160 characters long;
- Timing advance.

The MU is carried by the subscriber. It is made up of the ME, also known as the terminal, and a smart card known as the Subscriber Identity Module (SIM).

The SIM, which is basically a smart card, determines the directory number and the calls billed to the subscriber. The SIM contains the following subscriber related information:

- The International Mobile Subscriber Identity (IMSI), which uniquely identifies a subscriber and without which the GSM service is not accessible. IMSI is only used by the network.
- A secret subscriber authentication key K_i and a cryptographic algorithm A3/A8 which provide security functions for authenticating the SIM, and generating session keys.
- Temporary network related data like the Temporary Mobile Subscriber Identity (TMSI), Location Area Identifier (LAI), K_c, forbidden PLMNs, etc.
- Service related data like Language Preference and Advice of Charge.

- Card Holder Verification Information that authenticates the user to the card and provides protection against the use of stolen cards. A Personal Identification Number (PIN) is used. If the wrong PIN is entered three times in a row, the card locks itself, and can only be unlocked by providing a Personal Unblocking Key (PUK).

2.3.2 The Base Transceiver Station

The Base Transceiver Station (BTS) controls all of the radio related tasks and provides connectivity between the network and the MU via the radio interface.

A list of functions performed by BTS is as follows:

- Encodes, encrypts, multiplexes, modulates and feeds the RF signals to the antenna;
- Transcoding and rate adaptation;
- Time and frequency synchronization signals transmitted from BTS;
- Each BTS serves a single cell;
- Voice communication through full rate or haft rate speech channel;
- Received signal from mobile is decoded, decrypted and equalized before demodulation;
- Random access detection;
- Uplink radio channel measurements.

2.3.3 The Base Station Controller

The Base Station Controller (BSC) takes care of all the central functions and controls a set of BTSs. The BSC and the controlled BTSs form the BSS. The functions of BSC are as follows:

- Radio resource (RR) management for BTSs under its control;
- Intercell handover;
- Reallocation of frequencies among BTSs;
- Power management of BTSs;
- Time and frequency synchronization signals to BTSs;
- Time delay measurement of the received signals from MUs with respect to BTS clock
- Performs traffic concentration to reduce the number of lines from BSC to MSC and BTSs;
- Provides interface to the OMC for BSS.

2.3.4 Mobile Services Switching Center

The Mobile Services Switching Center (MSC) controls a large number of BSCs. It is very similar to a digital telephone exchange or a switch and it handles the routing of incoming and outgoing calls and the assignment of user channels on the A-interface.

A list of relevant functions performed by MSC includes the following:

- Coordinates of call set up from all MUs in its jurisdiction;
- Dynamic allocation of resources;
- Location registration;
- Interworking function with different networks;
- Handover management;
- Billing for all subscribers based in its area;
- Reallocation of frequencies to BTSs in its area to meet heavy demands;
- Encryption;
- Signaling exchange between different interfaces;
- Synchronization with BSSs;
- One MSC may interface several BSSs;
- Gateway to SMS.

2.3.5 Home Location Register

The Home Location Register (HLR) is a data repository that stores the subscriber specific parameters of a large number of subscribers. The most important parameters of a subscriber, like the K_i and IMSI are stored in the HLR. Every PLMN requires at least one HLR and every user is assigned to one specific HLR.

2.3.6 Authentication Center

The Authentication Center (AuC) has as a key component a database of identification and authentication information for each subscriber, and is in most cases an integral part of the HLR.

Attributes in this database include the subscriber's IMSI, secret key K_i, LAI, and TMSI. The AuC is responsible for generating triplets of values consisting of the RAND, SRES (Signed RESponse), and session key K_c which are stored in the HLR for each subscriber.

2.3.7 Visitor Location Register

The Visitor Location Register (VLR) network element was devised to off-load the HLR of user database related functions. The VLR, like the HLR, contains subscriber information, but only information for those subscribers who roam in the area for which the VLR is responsible. When a subscriber roams away from the network of his/her own service provider, information is forwarded from the subscriber's HLR to the VLR of the serving network, in order to complete the authentication process. When a subscriber moves out of a VLR area, the HLR takes care of the relocation of the subscriber information from the old to the new VLR. A VLR may have several MSCs, but one MSC always uses one VLR [6].

2.3.8 Equipment Identity Register

Since the SIM and the ME are treated independently by GSM, it is possible to operate any GSM ME with any valid GSM SIM. This makes cellular terminal theft and attractive business and probably starts a possible black market for stolen GSM terminals. To protect against such theft, the Equipment Identity Register (EIR) was introduced in the GSM system. Every GSM terminal has a unique identifier, called the International Mobile Equipment Identity (IMEI), which (according to the GSM organization) cannot be altered without destroying the terminal. It contains a serial number and a type identifier [7]. The EIR maintains three lists:

- The White list: is composed of all numbers series of equipment identities that are permitted for use.
- The Black list: contains all equipment identities that belong to equipment that need to be barred.
- The Grey list: MEs on the grey list are not barred (unless on the black list or not on the white list), but are tracked by the network (for evaluation or other purposes) [6].

Equipment identification can be done by the network operator by requesting the IMEI from the ME [7].

2.3.9 Operations and Maintenance Center

The main purpose of the Operations and Maintenance Center (OMC) is to perform all operations and maintenance functions on elements of the GSM PLMN system. The OMC uses a separate *Telecommunication Management Network* (TMN) to communicate with the various components of the GSM system.

2.3.10 Network Management Center

The Network Management Center (NMC) provides global and centralized management for operations and maintenance of the network supported by OMCs that are responsible for regional network management. It provides both administrative and commercial management, security management of the facilities, system change control, and physical maintenance. The NMC is generally connected to the PLMN subsystems through leased lines via PSTN.

2.4 Security Implementation

Security goals for wireless networks are focused on privacy and authentication. Privacy or confidentiality is a fundamental for secure communication. It provides resistance to interception and eavesdropping. Message authentication provides integrity of the message and the sender authentication, corresponding to the security attacks of message modification and impersonation.

To achieve these goals, the GSM specification addresses three key security requirements:

- Authentication – To correctly identify the user for billing purposes and prevent fraudulent system use.
- Confidentiality – To ensure that data (i.e. a conversation or SMS message) transmitted over the radio path is private.
- Anonymity – To protect the caller's identity and location.

There are three proprietary algorithms used to achieve authentication and confidentiality. These are known as A3, A5, and A8. A3 is used to authenticate the SIM for access to the network. A5 and A8 achieve confidentiality by scrambling the data sent across the airways. Anonymity is achieved by use of TMSI. The process of anonymity, authentication and confidentiality will now be explained in more detail.

2.4.1 Anonymity

One of the main goals of GSM security was to avoid having to use the IMSI in plaintext over the radio link, thus stopping an eavesdropper from determining if a particular subscriber was in an area and what services they were using.

Anonymity is provided by using temporary identifiers. When a user switches on his/her mobile terminal, the real identity (IMSI) is used to identify the MU to the network and then a temporary identifier TMSI is issued and user for identifying the MU to the network in future sessions. According to the ETSI specification the network should always encrypt TMSI before transmitting it to the MU.

This is avoided by addressing the phones by a 32-bit TMSI, which is only valid in a particular LAI. The subscriber addresses itself or is paged by the 32-bit TMSI from then on [8].

The TMSI is updated at least during every location update procedure (i.e. when the phone changes LAI or after a set period of time). The TMSI can also be changed at any time by the network. The new TMSI is sent in ciphered mode whenever possible so an attacker cannot maintain a mapping between an old TMSI and a new one and "follow" a TMSI. The process is shown in Figure 2.7 and Figure 2.8.

The phone must store the TMSI in non-volatile (so it is not lost at switch off). It is normally stored in the SIM.

Initially, the phone will have no TMSI, and thus is addressed by its IMSI. Once ciphering has commenced the initial TMSI is allocated. The VLR controlling the LAI in which the TMSI is valid, maintains a mapping between the TMSI and IMSI such as that the new VLR (if the MU moves into a new VLR area) can ask the old VLR who the TMSI (which is not valid in the new VLR) belonged to.

From then on the temporary identifier is used. Only by tracking the user is it possible to determine the temporary identifier being used.

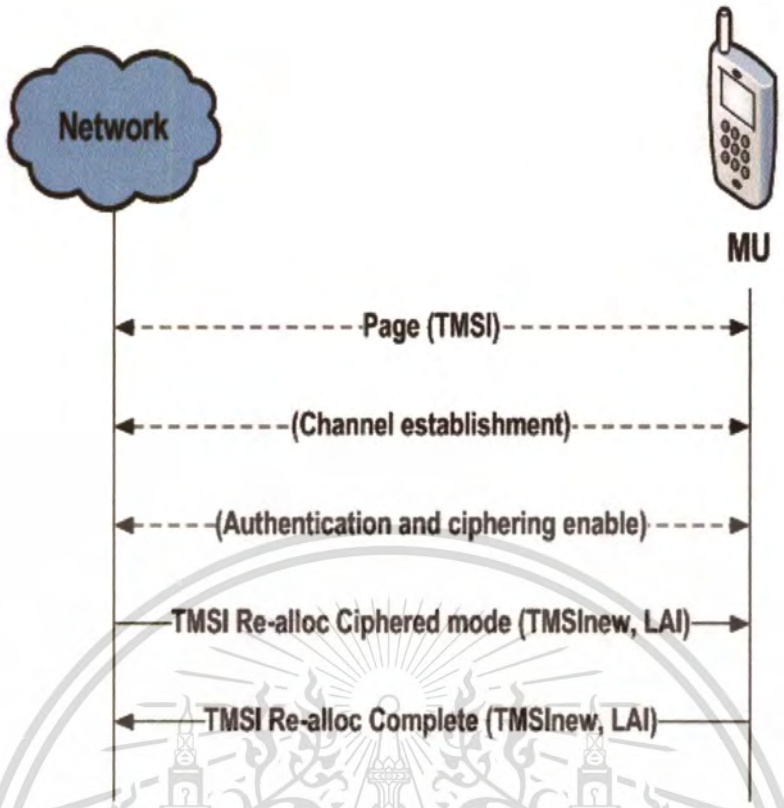


Figure 2.7 Allocating a new TMSI (when no location updating or no location changes during connection).

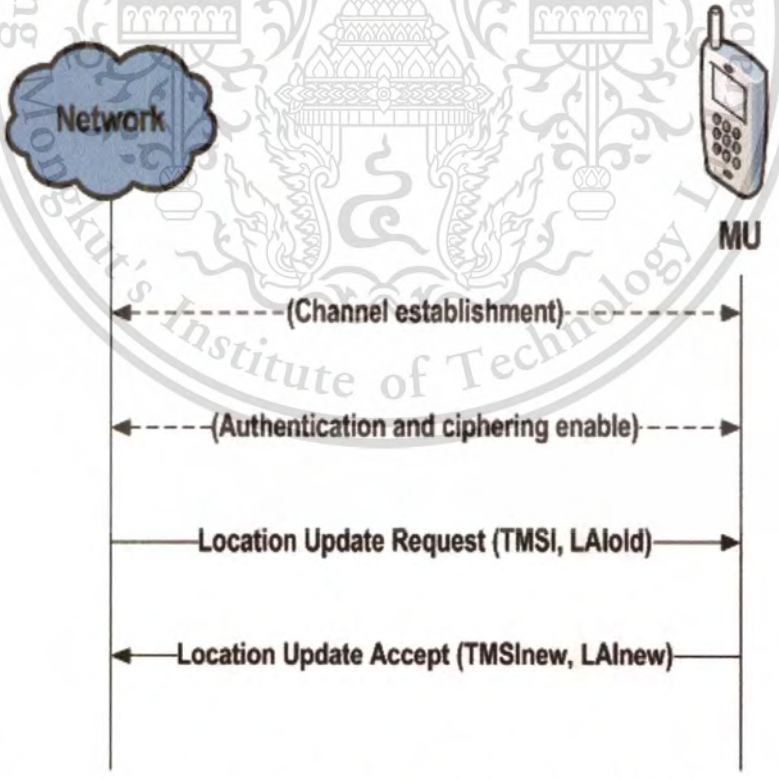


Figure 2.8 Allocating a new TMSI (when MU is moving into a new locations area in idle mode).

2.4.2 Authentication

Since the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be is a very important element of a mobile network. Authentication involves two functional entities, the SIM card in the mobile, and the AuC. One of the primary security functions of the SIM is to authenticate the subscriber to the network. This process assures the network that the MU requesting service is a legitimate subscriber through a not some intruder. A GSM network verifies the identity of a subscriber through a *challenge-response* process. When a MU requests service, the network sends a mathematical challenge to the MU (RAND), which must be answered correctly before being granted access [9].

The challenge sent by the network to the MU consists of a 128 bits *Random Challenge Number* called RAND. It is very important that RAND is unpredictable and has a very slim chance of being repeated; otherwise an attacker could easily make a codebook of (RAND, SRES) pairs and use the information to gain access to services. When the MU receives RAND it passes it into the SIM for processing. The SIM sends RAND and the secret 128-bits key K_i through the A3 algorithm to produce a 32-bits "*signed response*". The response, called SRES, is transferred out of the SIM into the terminal, where it is then transmitted to the network. This is the MU's response to the network's challenge. Meanwhile the network (the AuC) has performed the same set of operations as in Figure 2.9. Using the same value of RAND and an identical copy of K_i, the network has computed its own value for SRES. When the network receives SRES from the MU it compares to its own SRES. If the two values are identical, the network assumes the MU is legitimate and allows service to proceed. If the two values are not the same, the network assumes the SIM does not have the proper secret key K_i and therefore denies service to the MU [10]. Figure 2.9 illustrates the authentication process.

The authentication is achieved by using a basic challenge-response mechanism between the SIM and the network. The actual A3 authentication algorithm is used in 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.

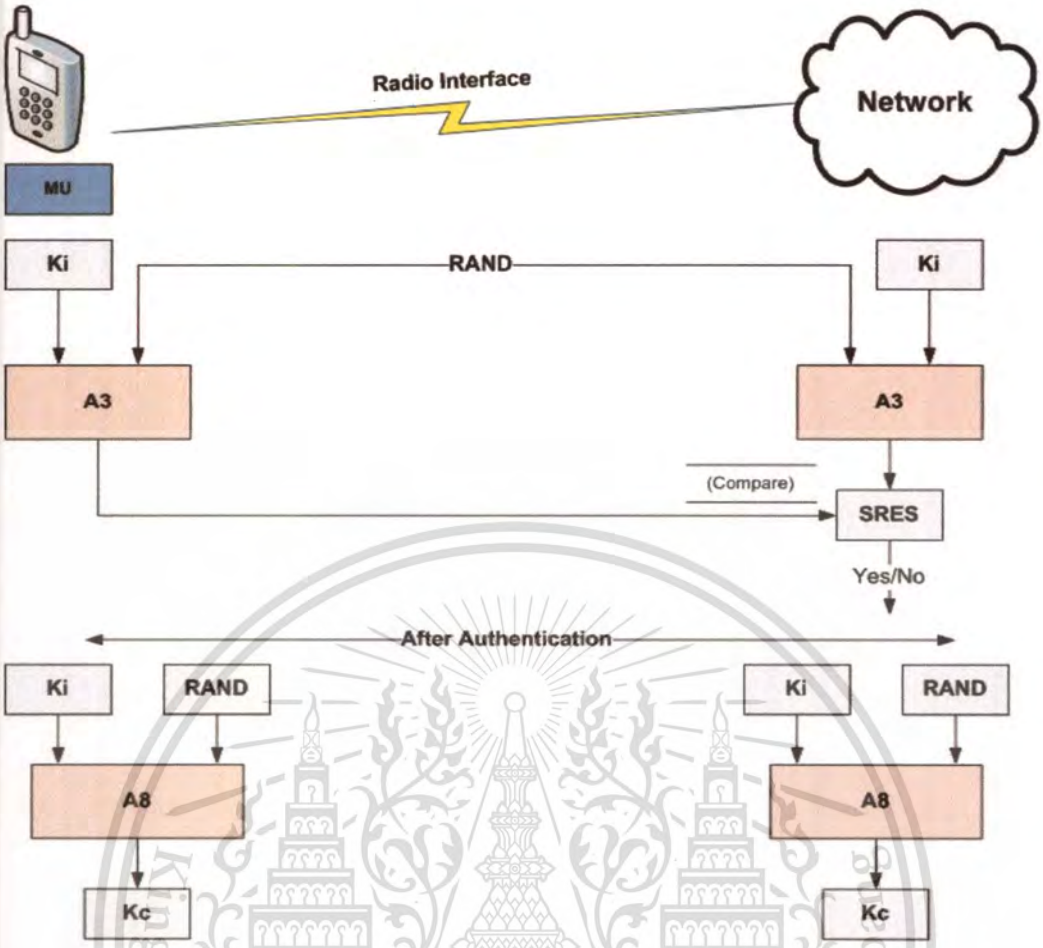


Figure 2.9 Authentication and session key generation in GSM.

A3 is implemented in the SIM card and the AuC or the HLR. A3 takes a 128 bits value K_i from the SIM and 128 bits RAND random number from the MSC as input data. It produces a 32 bits output value SRES. The output value SRES is a Singed RESponse to the network challenge. The input and the output from A3 are shown in Figure 2.10. Both the SIM and the network have the knowledge of K_i and the purpose of the authentication algorithm is to respond correctly in authenticating the challenge and allowing access to the network.

A3 algorithm can be called as a one-way hash function. Generally, one-way hash functions produce a fixed-length output from an arbitrary input. Secure one-way hash functions are designed so that it is computationally unfeasible in determining the input given by the hash value, or in determining two unique inputs that hash to the same value.

The A8 algorithm is the key generation algorithm in the GSM security model. The A8 generates the session key, K_c, from the random challenge, RAND that is received from the MSC and from the secret key K_i. The A8 algorithm takes the two 128-bits inputs and generates a 64-bits output from them. This output is the 64-bits session key K_c, as shown in Figure 2.11. The BTS received the same K_c from the MSC. HLR was able to generate the K_c, because the HLR knows both the RAND and the secret key K_i, which is holds for all the GSM subscribers of the network operator. One session key K_c, is used until the MSC decides to authenticate the MU again.

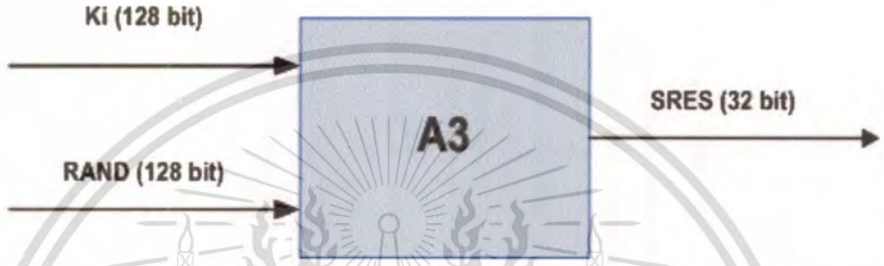


Figure 2.10 Signed responses (SRES) calculation by using A3 algorithm.

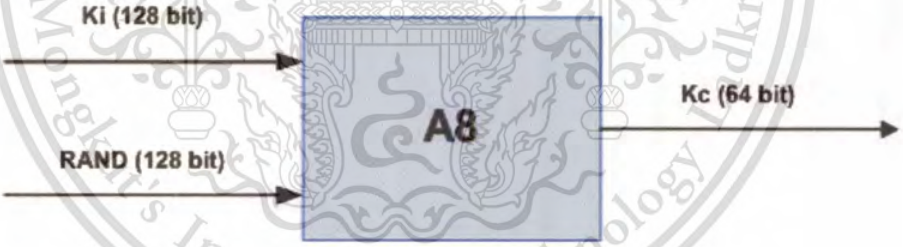


Figure 2.11 Session key (Kc) calculation by using A8 algorithm.

The purposes of the A8 algorithm is to derive a 64-bits session key (K_c) from the 128-bits K_i and the 128-bits RAND. On the other hand, the purpose of the A3 algorithm is to derive a 32-bits SRES from the same two inputs (the K_i and the RAND). The important thing is that A3 and A8 are just labels (reference names) for algorithms. In other words, a service provider is free to use any algorithm that it wishes to generate SRES from K_i and RAND. The GSM specification just uses the name A3 to reference such an algorithm. Similarly, the service providers is also free to use any

algorithm that it wishes to generate K_c from K_i and the name A8 is just used by the specification to reference this algorithm. Most GSM implementation combines the A3 and A8 functionality and use a single algorithm to serve both the purposes is produces the SRES and K_c. The COMP128 algorithm was designed to be a reference model for GSM implementation but for various reasons has been adopted by almost all GSM providers world-wide.

The COMP128 algorithm is illustrated in Figure 2.12. The COMP128 takes the 128-bits K_i and the 128-bits RAND as input and generates 32-bits SRES and a 64-bits session key K_c. COMP128 was cracked in April 1998 and a new stronger version, COMP128-2 was developed. However, due to the huge amount of cost involved in replacing COMP128 (or maybe ignorance in some cases), it is believed that most operators are still using the old flawed algorithm [11].

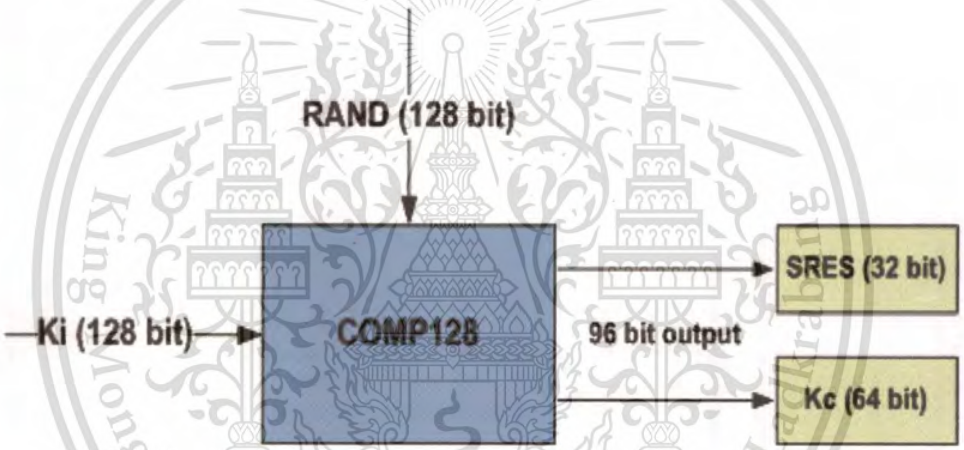


Figure 2.12 A popular A3/A8 implementation (COMP128).

2.4.3 Confidentiality

The SIM also provides information needed to encrypt the radio connection between the MU and the BTS. More specifically it computes the session key K_c, which is later, used in some version of A5 for encrypting the voice or data before transmission on the radio path. The algorithm used for computing the 64 bits K_c, is called A8 and is invoked according to Figure 2.11 [10]. A3/A8, as mentioned in the previous section, is often realized in practice using the initial design specification given by the GSM MoU, which is a single algorithm called COMP128 as showed in Figure 2.12.

Recall that GSM uses a technique called *time division* to share the radio channel with up to eight other users. Each user takes turns using the common radio channel, sending and receiving information only during one of the eight available time slots in every frame. Each frame is very short, lasting only about 4.6 milliseconds, and is identified by a *frame number*. A GSM conversation uses two frames, one going from the base station to the MU and another going from the MU back to the base station. Each of these frames (time slots) contains 114 bits of user information, which is often digitized and compressed speech. Thus, every 4.6 milliseconds the MU receive 114 bits of information from the base station and transmit another 114 bits to the base station. It is these 228 bits that require encryption to protect it from eavesdroppers.

Using RAND and the secret key K_i, the SIM runs the A8 algorithm (or COMP128) to produce a 64-bits long session key called K_c. K_c is transmitted out of the SIM and into the MU, where it is used by a third algorithm (A3 and A8 are the other two) called A5.

A5 uses K_c and the current, publicly known, frame number to produce a key stream of 228 bits, half of which encrypts the downlink and the other half encrypts the uplink. For each new frame to be transferred a new 228 bits key stream is produced by the A5 to be used to encrypt (and decrypt) the frame see Figure 2.13. A5 resides in hardware in the terminal, not in the SIM, and must operate quickly and continuously to generate a fresh set of 228 bits every 4.6 milliseconds. Also, because GSM terminals are designed to operate in different networks, the A5 algorithm must be common to all GSM networks.

At present, there are at least two known versions of A5. The first, called A5/1, is only used in countries that are members of CEPT, provides the strongest level of encryption across the air link (Actually A5/3 is stronger but it is to be used in future networks). Although officially using 64 bits keys, in actual practice the keys are no more than 54 bits long, the last ten bits are forced to be zeros. The second algorithm, A5/2, is considered to be much weaker than A5/1 and is designed for export to countries outside CEPT where presumably there is an interest in easily cracking encrypted conversations. The two algorithms A5/1 and A5/2 will be described in the following subsections.

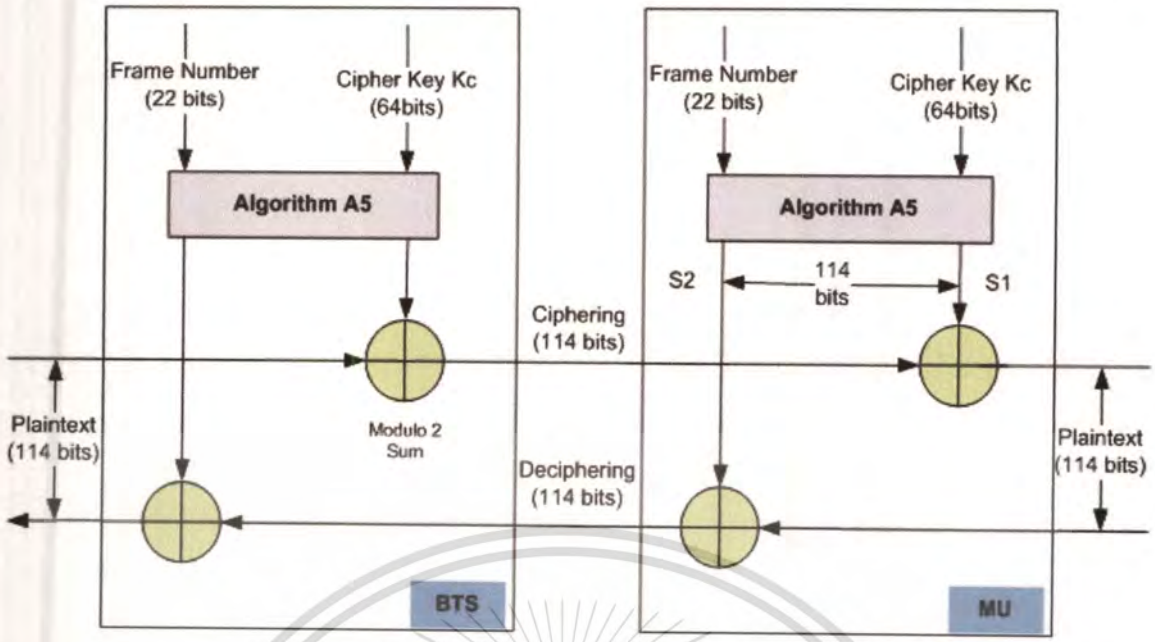


Figure 2.13 Encryption/decryption process of authentication message.

2.4.3.1 Description of the A5/1 Stream Cipher

A5/1 built from three short linear feedback shift registers (LFSRs) of length 19, 22, and 23 bits, which are denoted by R1; R2 and R3 respectively in Figure 2.14. The rightmost bit in each register is labeled as bits zero. The taps of R1 are at bits positions 13, 16, 17, 18; the taps of R2 are at bits positions 20, 21; and the taps of R3 are at bit positions 7, 20, 21, 22. When a register is clocked, its taps are XORed together, and the result is stored in the rightmost bit of the left-shifted register [12].

The three registers are maximum length LFSRs with periods 2^{19}-1, 2^{22}-1, and 2^{23}-1, respectively. They are clocked in a stop/go fashion using a majority rule as follows. Each register has a single "clocking" tap (bit 8 for R1, bit 10 for R2, and bit 10 for R3); each clock cycle, the majority function of the clocking taps is calculated and only those registers whose clocking taps agree with the majority bit are actually clocked, then at each step either two or three registers are clocked, and each register moves probability ¾ and stops with probability ¼ [12].

Each 4.6 millisecond a fresh set of 228 bits are generated and XORed with 228 bits of plaintext to produce the ciphertext, before transmitting it on the radio link.

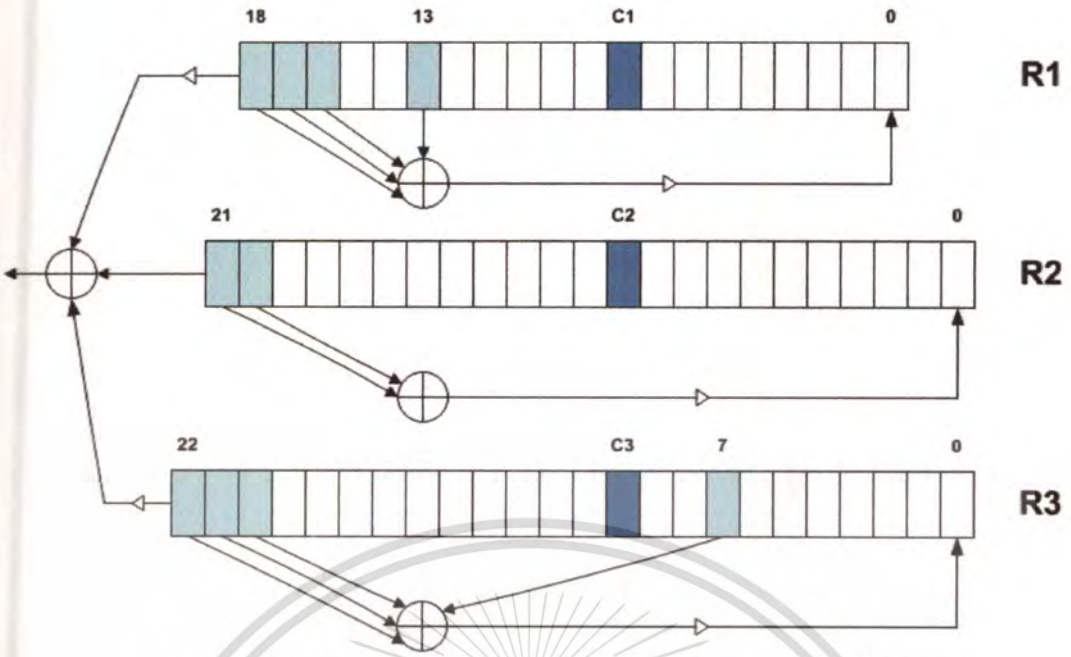


Figure 2.14 The internal structure of the A5/1 Stream cipher [12].

2.4.3.2 Description of the A5/2 Stream Cipher

The A5/2 stream cipher is very similar to A5/1. It consists of four LFSRs: R1, R2, R3 and R4 with the lengths 19, 22, 23, and 17 bits respectively as depicted in Figure 2.15.

Each register has taps and a feedback function. At each step of A5/2 R1, R2, and R3 are clocked according to a certain clocking mechanism that is determined using R4. After the three registers are clocked R4 is clocked. Post clocking, one output bit is ready at the output of A5/2. The output bit is, as in the case of A5/1, a non-linear function of the internal state of R1, R2, and R3 [13].

After the first clocking is performed the first output bit is ready at the output of A5/2. The clocking mechanism works as follows: R4 controls the clocking of R1, R2 and R3. When clocking of R1, R2 and R3 is to be performed, bits R4 [3], R4 [7] and R4 [10] are the input of the clocking unit. The clocking unit performs a majority function on the bits. R1 is clocked if and only if R4 [10] agrees with the majority. R2 is clocked if and only if R4 [3] agrees with the majority. R3 is clocked if and only if R4 [7] agrees with the majority. After these clocking R4 is clocked [13].

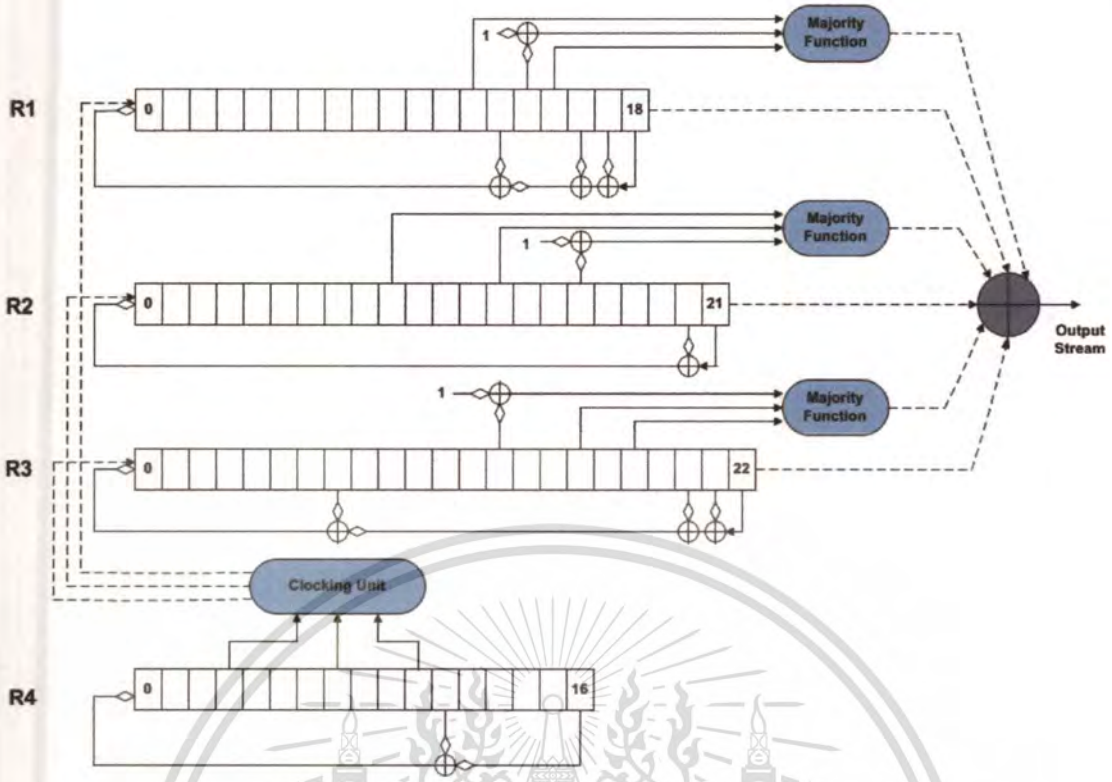


Figure 2.15 The internal structure of the A5/2 Stream cipher [14].

Once the clocking is performed, an output bit is ready. The output bit is computed as follows: in each register the majority of two bits and the complement of a third bits is computed; the results of all the majorities and the rightmost bit from each register are XORed to form the output. Note that the majority function is quadratic in its input: $maj\ (a,b,c) = a.b + b.c + c.a$.

The difference between A5/1 and A5/2 is that A5/2 also initializes R4, and that one bit in each register is forced to be 1 after initialization. Then A5/2 discards 99 bits of output while A5/1 discards 100 bits of output. The clocking mechanism is the same, but the input bits to the clocking mechanism are from R4 in the case of A5/2, while in A5/1 they are from R1, R2, and R3. The designers meant to use similar building blocks to save hardware in the mobile terminal [15].

This algorithm outputs 228 bits of key-stream. The first block of 114 bits is used as a key-stream to encrypt the link from the network to the customer, and the second block of 114 bits is used to encrypt the link from the customer to the network. Encryption is performed as a simple XOR of the message with the key-stream.

2.5 Conclusions

In the previous section, the way of the GSM authentication and confidentiality process establishes security is presented.

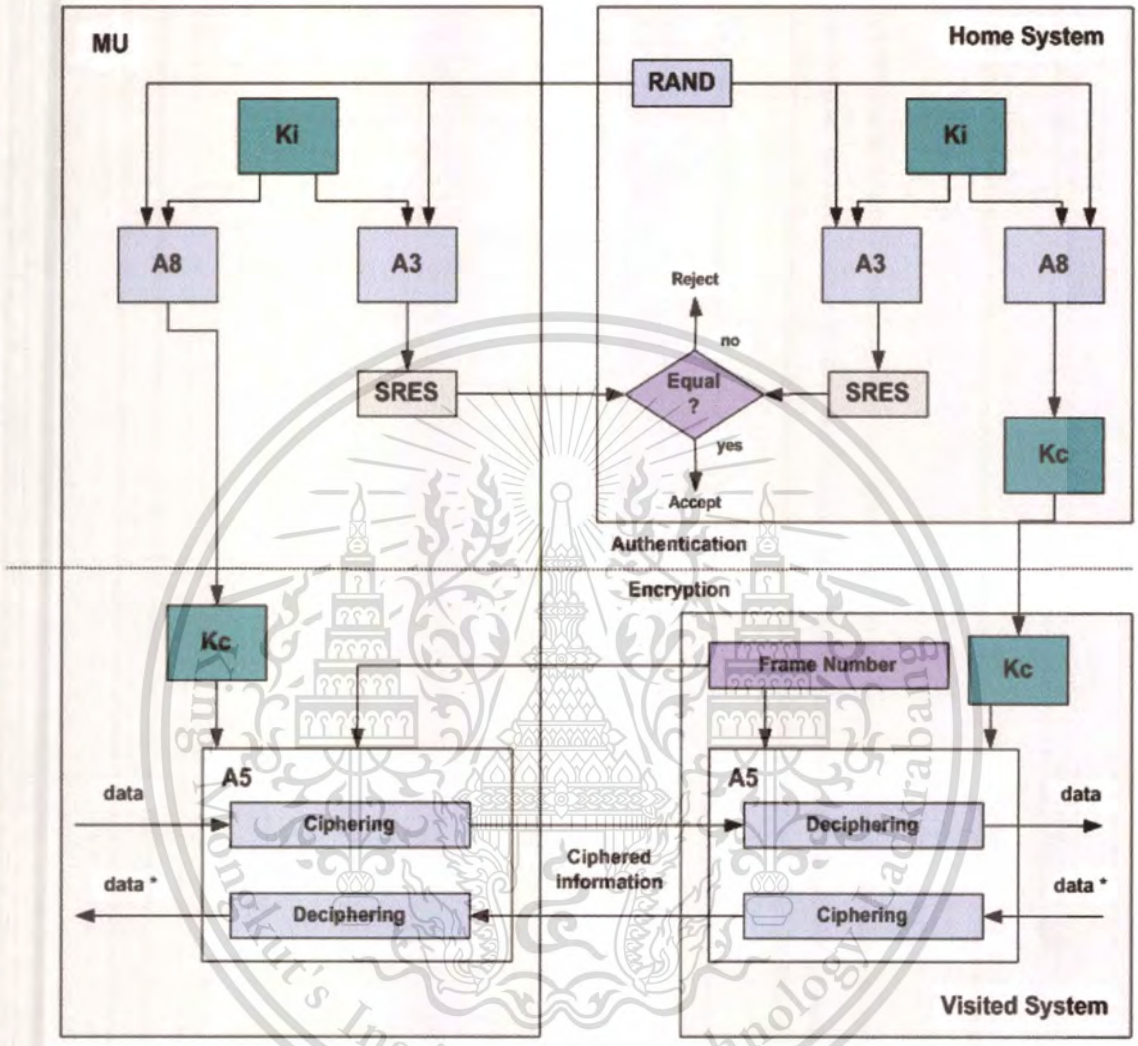


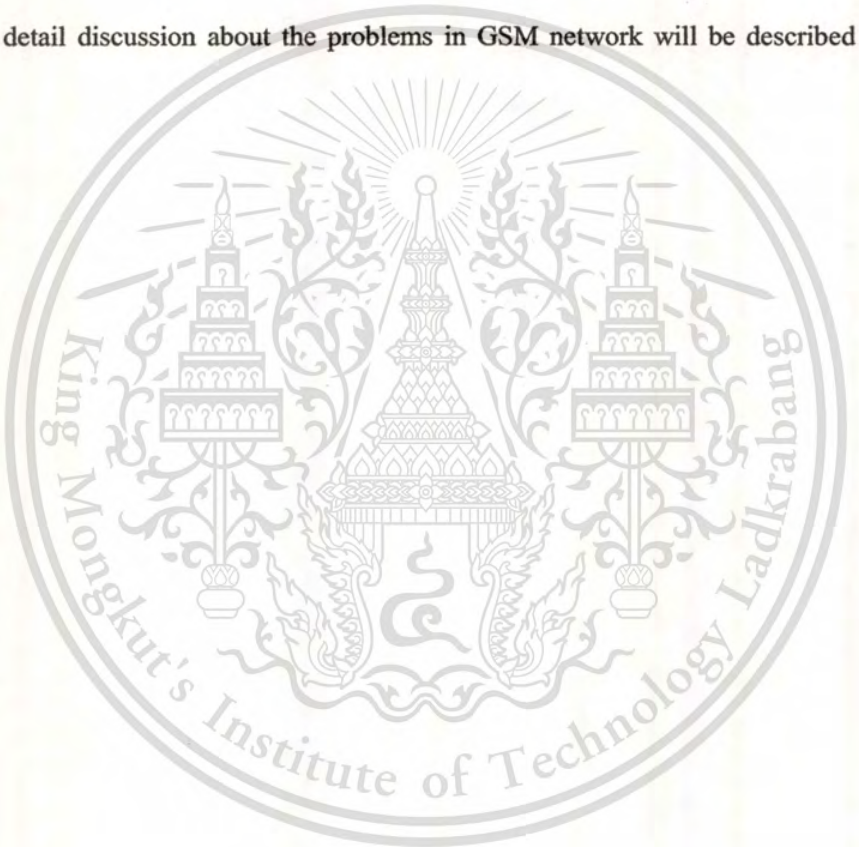
Figure 2.16 Outline of Authentication and Confidentiality in Basic GSM network.

The security of GSM is based on algorithms A3, A5 and A8. The outputs of SRES and K_c are computed, respectively, using K_i and RAND through algorithms A3 and A8 as inputs, where K_i is the MU secret key shared between the MU and the HLR and saved in the SIM card, and RAND is generated by HLR. SRES is a certificate to authenticate MU and K_c is the session key between MU and the VLR. To transmit messages confidentially, algorithm A5 is used to encrypt/decrypt the transmitted messages. The encryption algorithm (A3, A5, A8) are present in the GSM network as well. So, the security implementation in GSM network is summarized as shown in Figure 2.16.

As mentioned earlier, in GSM the customer subscription and authentication capability is contained within a smart card (SIM). Any mobile will take on the identity of a subscriber by insertion of a smart card. The mobiles now become attractive item to steal, as they can be used with another SIM card.

To prevent this, GSM has specified an International Mobile Equipment Identifier (IMEI). Although at first evaluation to an operator, it may seem as the stolen mobiles have no effect since they do not affect a subscription, there will be problems with an increase in customer facing staff to handle esquires and a possibility that GSM terminals are expensive to insure.

The detail discussion about the problems in GSM network will be described in the next chapter.



Chapter 3

Improving on Authentication Process of Security in GSM Network

The openness of wireless communications makes the communicating parties more vulnerable to the security threats. GSM was intended to be a secure wireless system that provides the user authentication and over-the-air encryption. Unfortunately, it is completely vulnerable to several attacks that aim each part of the network.

In this chapter, several flaws in the existing GSM security which is focus on the cryptographic and protocol flaws in GSM are discussed. However, the most devastating attacks on GSM due to invalid security assumptions are made by the original designers of GSM. These research works have provided the solutions to solve these promise weaknesses such as new algorithms and new protocols. Most of these algorithms are required. However, the extensive computation power and unrealistic quantities of known plaintext make it difficult to be used in practice. The difficulty of using cryptanalytical attacks to break the confidentiality of GSM calls does not mean that the conversations are well protected. In this thesis, the technique to improve the authentication process by using the Public-key based protocols is proposed.

The exit protocol and its main drawbacks are firstly discussed. Then, some approaches that used to improve this protocol are presented. Finally, the ideas to make GSM authentication protocol more secure and efficient are proposed.

3.1 Problem in Authentication Protocol

GSM architecture consists of mobile unit (MU) and base station (BS) which communicate each other through radio links. BS is connected to the MSC which is responsible for routing the signals to and from the fixed networks. Several databases are defined to perform management and authentication purposes. The HLR database contains information and the location of every user in the system. The VLR database, located in every MSC, contains the information of visiting users in the location area. The AuC is the user authentication center which contains the secret keys K_i that every user shares with the system.

The authentication process in GSM is based on algorithms A3, A8 and A5. A5 is responsible for communication encryption between MU and BS using a session key K_c, once MU has been authenticated. This authentication requires MU to compute a response $SRES_m$ to the challenge RAND, received from BS, by using A3 and the secret key K_i. It can be written as follows:

$$SRES_m = A3\ (K_i, RAND) \quad (1)$$

The same challenge RAND is then used to compute the session key

$$K_c = A8\ (K_i, RAND) \quad (2)$$

According to Figure 3.1, the authentication process begins when a user of MU changes the current location. Simultaneously, MU sends an authentication request that contain its temporal identification (TMSI) and the LAI to VLR. Theoretically, LAI is an old LAI which is introduced by the old VLR to the new VLR.

After receiving the request, the new VLR obtains the real identity IMSI from the old VLR by using TMSI. Then the VLR tells the identity of the user who is requesting the authentication to the HLR. When HLR receives the request, it generates *n* triplets ($RAND_i$, $SRES_i$, K_{ci}) and sends them to the new VLR.

The VLR receives the triplets and stores them in the database. Next, it selects a triplet to authenticate the MU, and sends $RAND_i$ to MU. When MU receives $RAND_i$, the response $SRES_m$ is computed and returned to VLR. MU also computes the session key K_c, where K_c is kept secret for subsequent communications.

Finally, upon receiving $SRES_m$, the VLR compares it with the selected $SRES_i$ kept in its own database. If they are not the same, the authentication fails; otherwise, the VLR authenticates the MU.

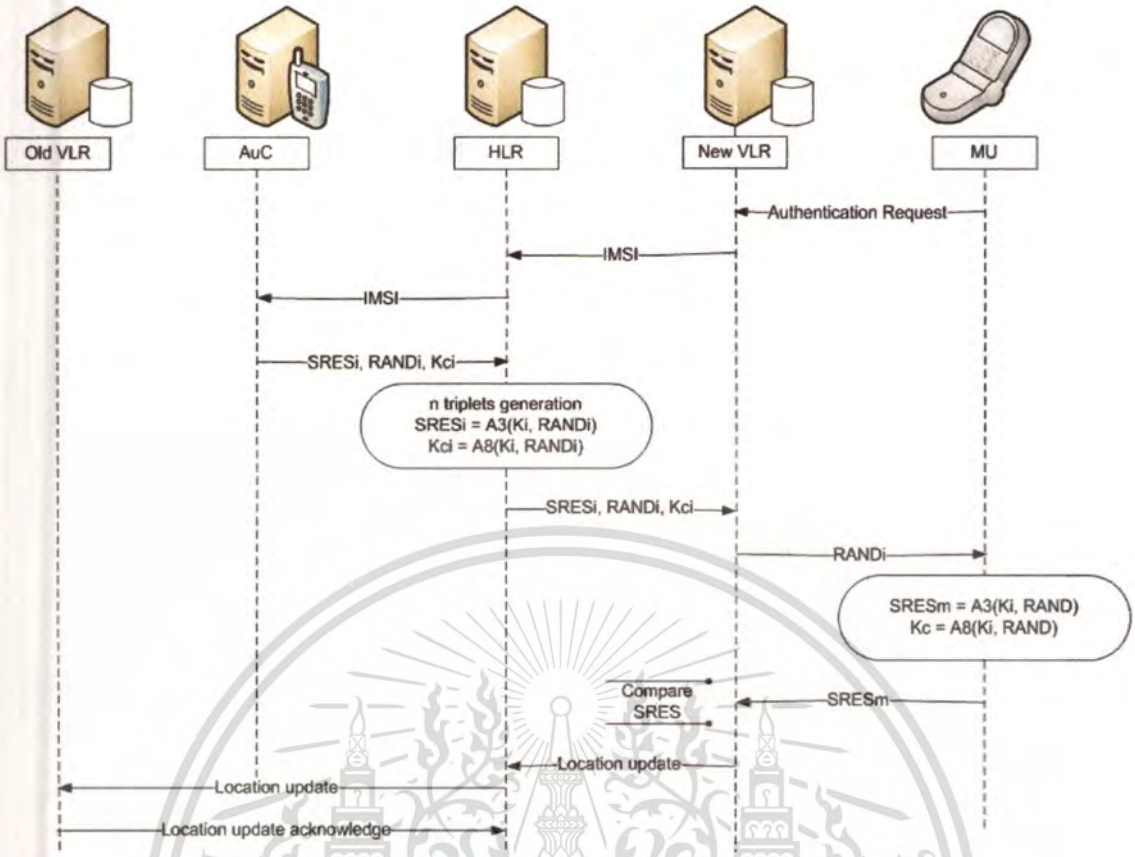


Figure 3.1 Basic GSM authentication protocol.

In the first authentication, VLR sends the location update message to the HLR. The HLR, in turn, sends the same message to the old VLR and receives a confirmation.

The algorithms incorporate with the authentication mechanism in the GSM network in the purpose of making the GSM network become the standard secure mobile communication.

Unfortunately, these techniques have several main security flaws, which are described as the follows:

- As one can observe, this process does not provide mutual authentication, since VLR is not authenticated by MU. This is the security breach which has allowed the GSM's cards to be cloned. Using the challenge/ response mechanism, the identity of a MU is verified. However, the identity of VLR cannot be authenticated. It is therefore possible for attacker to pretend to be a legal network entity and thus to get the MU's credential.
- Furthermore, the VLR must turn back to the HLR to make a request for another set of authentication parameters when the MU stays in the VLR for a long time and exhausts its

set of authentication parameters for authentication. There is bandwidth consumption between the VLR and HLR.

- Every MU is the particular VLR has *n* copies of the authentication parameters. The parameters are stored in the particular VLR database and then, the space overhead occurs.
- The confidentiality of user identity is violated by transmitting the user identities (IMSI) in unprotected form through the intermediate transport network between the GSM registers.
- In addition to the SIM cards, individual authentication key (K_i) of the users are also stored in the GSM authentication centers (AuC). Any person who has the rights and capabilities to access to authentication center can obtain the authentication key of a valid subscriber to impersonate the mobile user. An unauthorized person can thus capture and decipher the encrypted traffic on the radio channel between the MU and the BS. As the results, SIM or eavesdrop in the entire GSM conversations can be cloned. Therefore, security value of K_i is necessary and important.
- Security algorithms of the GSM (A3, A5, and A8) are all unpublished and secret algorithms. Researchers have reverse-engineer these algorithms and they have shown that these algorithms have many important security flaws [8].
- In the GSM authentication phase, two related parameters, RAND and SRES, are transmitted on the air interface clearly. Thus, any listener on the air interface is able to know the plaintext attack on the RAND-SRES pair to obtain the authentication key K_i.

Based on the security flaws in GSM network that is mentioned before, most of researchers have proposed the solutions in order to improve the authentication of GSM network security. Their findings will be discussed in the following sections.

3.2 Existing Authentication Protocols

There are many problems in GSM network security which can be divided into two main points. They are the problem in algorithms and the problem in authentication protocol.

Many GSM operators use the defined design specification in the GSM MoU, COMP128 (combined for both A3 and A8 algorithms), instead of designing their own algorithms for authentication and session key generator. The difficulty occurs when starting to use the different algorithms. The reasons are the algorithm resides inside the SIM, and subscribers who bought

subscriptions (SIMs) before the eventual introduction of a different (presumably stronger) algorithm are forced to use their SIMs with the old algorithm.

The design of COMP128 was never made public, but the design has been reverse engineered and cryptanalysed. Since the GSM specification for SIM cards is widely available, all things that are needed to clone a SIM card is the 128 bits COMP128 secret key K_i and the IMSI which is embedded in the card.

The most popular attack requires physical access to the SIM in order to clone the SIM. The attack can be completed in about 8 hours. It can be speeded up with the risk of damaging the SIM. The most efficient way to clone a GSM smartcard is partitioning attack, proposed by a team from IBM. It requires challenging the target SIM only 8 hours in the best case, which means that cloning can be done in minutes or even seconds.

By using brute-force attack, A. Biryukov, A. Shamir, and D. Wagner presented two cryptanalytic attacks on A5/1, in which the single PC can extract, the conversation key K_c in real time from a small amount of generated output. Moreover, the new algorithm A5/2, that was proposed by Barkan. E, Biham. E and Keller. N in [13], presented the cryptanalysis of both A5/1 and A5/2. As the result, they can find the K_c and then re-calculate it in order to find K_i.

However, some of these existing flaws have been fixed by the 3GPP and the others remaining are left to be discussed afterward. From the security perspective, the most important component in GSM is the authentication protocol.

In the last decade, many alternative authentication protocols for GSM have been proposed. The important group amongst them is based on the asymmetric cryptography. Lin and Jan [16] proposed a mutual authentication protocol in which a user takes a ticket during user authentication in the first phase of the protocol. The second phase of the protocol allows the MU to anonymously access the system for a limited period of time. This process can be done via prepaid tickets that are generated by the HLR which can be used with the VLR.

In contrast, in [17], A.M.Barbancho and A.Peinado analyzed that Lin and Jan protocol is not secure. The main weakness of this protocol is the foreign authentication (second) phase, not the

anonymity. The VLR cannot obtain the identity information of the foreign users that access to the system, but it is possible that any unauthorized user gains access to the network.

In [18], Alberto Peinado proposed another *Public-Key Infrastructure* (PKI) protocol based on mutual authentication that is similar to [16]. This protocol also has two phases. In the first phase, a user takes a ticket from the HLR during initial authentication and uses it for subsequent authentication. Despite the lack of any need to change the GSM architecture, this protocol is still based on PKI and the MU has a heavy computational local.

In [19], V.Bocan proposed against a DoS (Denial of Service) attack. However, it requires significant computations and memory from both the MU and the network. In addition, the network has to send the broadcast messages continuously and has to wait for the MU to respond.

The other group that proposes improvements retains the MU restrictions and employs symmetric cryptography. In [20], C.Lee proposed a mutual authentication technique for the GSM network. The main idea is focus on the issuing a ticket for the new VLR by the HLR when the MU is authenticated in the new location at the first time. The VLR and MU authenticate each other by using the ticket without any need of-referencing to the HLR. The analysis shows that this technique works correctly only for the first MU authentication, and cannot subsequently verify the network.

Moreover, Khalid Al-Tawil proposed a new authentication protocol for GSM networks in [22], as shown in Figure 3.2. In this research work, the "mobile user events counter (COUNTM)" was utilized in basic GSM network. A random number RANDM (64 bits) is generated locally by the MU to compute a pre-authentication result AUTHR. Furthermore, the counter (COUNTM) concatenated to the RANDM form the global random number called RANDG (128 bits). As the results, it is impossible for the attacker to collect the RANDM and AUTHR in order to retrieve secret key K_i. However, the bandwidth needed of this new protocol is still considered to be much lower than the GSM capacity.

A secure communication mechanism for GSM networks was proposed by Chi-Chun Lo in [21]. Successfully, he applied a public key cryptography for user authentication and stream cipher for message encryption and decryption in basic GSM networks. The authentication protocol was divided into two different phases, namely connection phase and release phase, as shown in Figure

3.3. Based on cryptanalysis and operational analysis, it was shown that the C3 protocol is secure and efficient. Key stream M cannot be reveled from the attacker. MU and BS can verify each other identity by using the certificate. Hence, the protocol can avoid the man-in-the-middle attack, replay attack, and guessing attack. Unfortunately, they still faced two main problems such as bandwidth consumption and overload of database storage.

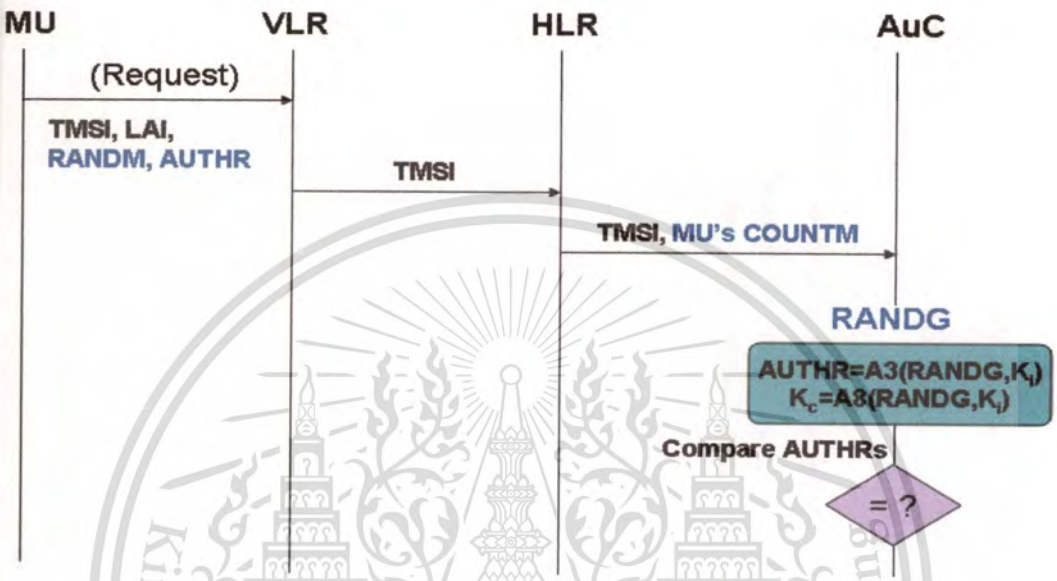


Figure 3.2 New authentication protocol for GSM Networks.

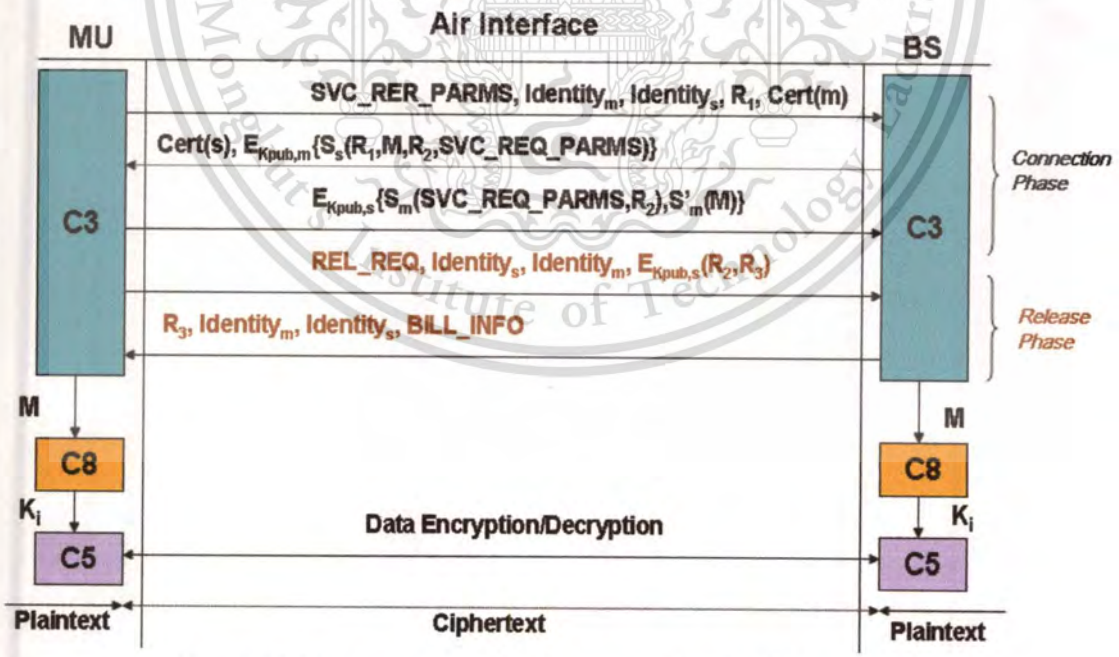


Figure 3.3 Secure communication mechanisms for GSM Networks.

It can be clearly seen that the purpose of almost proposed protocols are keeping K_i secret and providing mutual authentication. Based on this aspect, a new protocol is proposed, which will be discussed in the next section.

3.3 Proposed Authentication Protocol

In principle, there are several typical attacks on authentication protocols. Message replay attack is one of the most common attacks on authentication and authenticated key establishment protocols. If the messages that exchange in an authentication protocol do not carry appropriate freshness identifiers, an adversary can easily get itself authenticated by replaying a message that is copied from a legitimate authentication session. Man-in-the-middle attack is another classic attack and is generally applicable in a communication protocol where mutual authentication is absent. Furthermore, there are other familiar attacks such as: parallel session attack, reflection attack, interleaving attack, attack due to type flaw, attack due to name omission, and attack due to misuse of cryptographic services.

Therefore, the new proposed protocol of the GSM authentication should be satisfied by the five requirements that are listed and illustrated as follows:

1. Mutual authentication: the proposed authentication protocol should be able to achieve bilateral authentication between the MU and the VLR.
2. Reduction of bandwidth consumption.
3. Reduction in the storage of the VLR database.
4. Authentication of an MU has to be carried out by a VLR instead of an HLR; even the VLR does not know the MU secret key K_i and algorithm A3.
5. The proposed protocol must keep the security and the efficiency of the existing GSM authentication protocol. It should not add any extra computations, and should not change the architecture of the existing GSM system.

GSM communication standards adopt the symmetric-key cryptography between users and their home networks to establish session keys. For symmetric-key based protocols, two communication parties share a long-lived key (in this case, each party has to maintain a set of distinct keys for communicating with different parties) or have a third party involved during

runtime. Hence, key management and scalability are two major issues when deploying the schemes in practice. But as mentioned before, GSM authentication process has flaws that network does not authenticate itself to the phone (or GSM does not provide mutual authentication). This is the most serious fault with the GSM authentication system. The authentication procedure that is described before does not require the network to prove its knowledge of the K_i, or any other authentication context to the phone. Thus, it is possible for an attacker to introduce himself as a valid network to a user via a man-in-the-middle attack. By this way, an attacker can capture the IMSI of an MU and even discover K_i using a collision attack.

In the proposed integration system, an efficient mutual authentication protocol for GSM is introduced. The main objective of the protocol is enabling the MU to authenticate the network. In addition, other GSM authentication problems presented in section 3.1 that related to the efficiency is solved. In fact, our protocol employs concurrent acquisition to decrease memory overhead in the VLR, reduces the processing loads for the MU and HLR, reduces the control messages for authentication, and improves call set up time. It can be achieved by extending the authentication protocol based on the existing GSM authentication, using of Public-key techniques for user authentication, and using the stream cipher for message encryption and decryption.

Public-key algorithms are based on mathematical functions rather than on substitution and permutation (based on number theory). But more important, public key cryptography is asymmetric involving the use of two separate keys, in contrast to the symmetric conventional encryption, which uses only one key.

Each of the communicating parties has a pair keys; "Public Key" and "Private Key". The relation between the keys is used for the following purposes:

- **Public key encryption** is used to send encrypted data to someone. The sender encrypts the data with the receiver's **public key**, which may be known by anybody, and the receiver decrypts it with his/her (corresponding) **private key** that is known by the recipient only. Compared to the symmetric-key encryption, public-key encryption requires more computation and not always appropriate for large amounts of data.
- **The reverse scheme**, sometimes called **private key encryption**, is also useful. The scheme is being used for digital signatures. A person can digitally sign the data by encrypting it

with his/her private key. The receiver can use the signer's **public key** to verify the digital signature. The data that is verified with the public key can be signed only with the corresponding private key, which is possessed by its owner only.

In the proposed system, a public key algorithm is mounted on the MU with A5, A8 and A3. It can be provided either in the next generation of mobile communication operators or the new users in the existing system.

Reduction in key size brings the advantage of less storage area and less required bandwidth. The advantages are important requirements of wireless network architectures. The proposed system is based on the idea of obtaining a digital certificate from a trusted third-party.

A *Digital Certificate* (DC) is an electronic identity. It consists of the owner's public-key and identification. The corresponding public-key Digital certificates are issued, managed and revolved by a Certificate Authority (CA). CA is the trusted entity of the public key infrastructure that is certified by its digital signature. Generally, CA put on a data structure that contains a user identity and a public key, and also performs a binding between the given user and its public key. Usually, CA is related directly with the *Registration Authority* (RA). RA is responsible for establishing and confirming identities, distributing shared keys, and initiating the certification process.

Before describing the proposed system, the requirements have to be mentioned. The requirements are listed as follows:

- The SIM/ HLR/ AuC/ VLRs should have Digital Certificate along with their public keys.
- HLR has its own private and public keys for some unspecified asymmetric cryptosystem. Hence, mobile users MU must know the HLR's public key. This fact does not imply modifications in the structure.
- The Digital Certificate of the home network should be distributed when a new SIM card is issued to a customer.
- A public key algorithm should be mounted on the MU.
- Well-known and accepted algorithms such as RSA (stands for Rivest, Shamir, and Adleman) are used in the protocols.

The brief process of the proposed protocol, based on the basic GSM authentication protocol, is summarized in Figure 3.4 as the following:

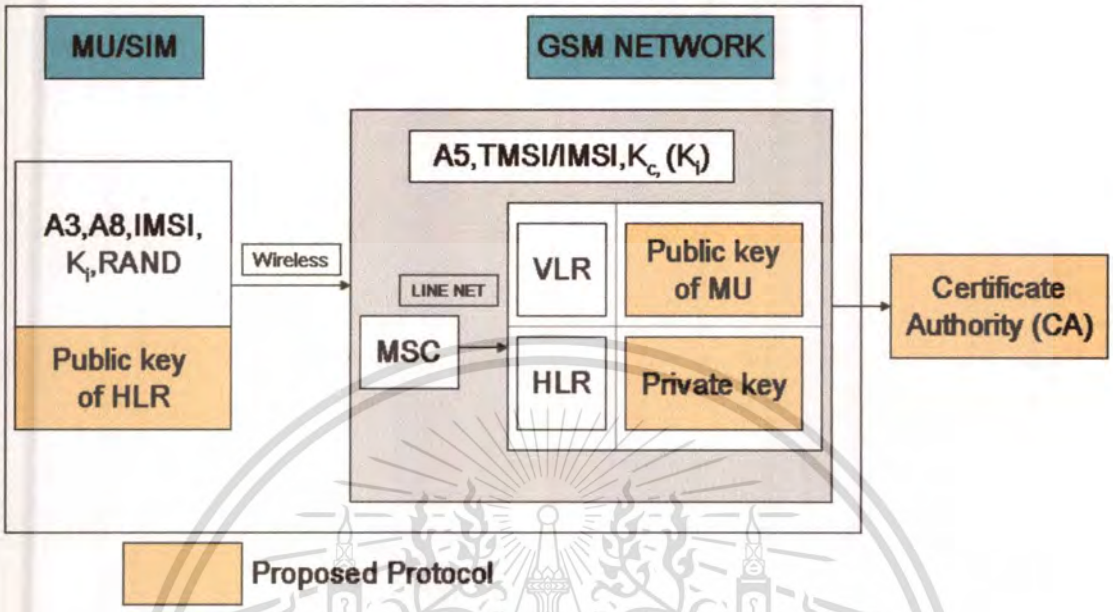


Figure 3.4 Block Diagram of proposed authentication protocol based on basic GSM authentication protocol.

The goal of proposed protocol is mutual authentication which not only overcomes the drawbacks described in section 3.2, but also makes the authentication mechanism more efficient. Mutual authentication protocols consist of two unilateral authentication protocols which are independent from each other. One is used for network authentication, and the other performs MU authentication. The proposed scheme consists of two parts and will be discussed afterwards. Moreover, some of the problems that have been mentioned will be emphasized. Truly, using Public-key technique in mobile communication is not un-explored before but it was not used due to the high computations that will cause the delay. The proposed solutions are practiced when flow occurs, such as losing the IMSI. The use of public key system should be triggered.

As discussed before, the most serious fault with the GSM authentication system is when the network does not authenticate by itself to the phone. The authentication procedure described before does not require the network to prove its knowledge of the K_i. Thus, it is possible for an attacker to set up a false network node with the same Mobile Network Code as the subscriber's network.

Since the authentication procedure initiation is up to the network's discretion, the false network, which can be seen in Figure 3.5, may choose to not authenticate at all, or simply send the RAND and ignore the response. It does not have to activate the ciphering either. The attacker can set the cell reselection parameters of his false base station to values that will highly encourage his "victims" to camp on it.

Therefore, the SIM should have the option to initiate the authentication process, for both HLR and VLR. Two solutions are proposed:

- Authentication the Home Network
- Authentication the Visiting Network.

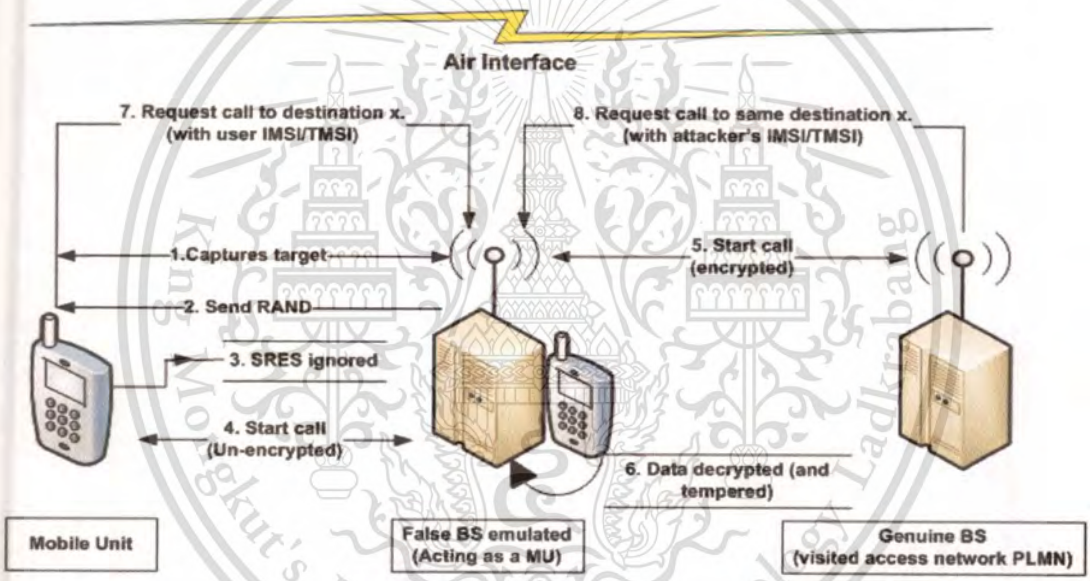


Figure 3.5 The false base station.

3.3.1 Authentication the Home Network

Authenticity can be proven by proving the knowledge of K_i. The procedure will be described in Figure 3.6. SIM will send a RAND to the network and the network will produce the correspondent SRES and send it back to the SIM. This procedure is not safe because an attacker can obtain both SRES and RAND and perform a "Known plaintext attack" to retrieve the K_i. Therefore, RAND should be sent encrypted by the HLR public key. In this case the attacker cannot obtain both SRES and RAND together.

By using the public key, the new protocol will be presented as follows: SIM will extract the public key of the Home Network. Then, SIM will send a RAND code (that is changed every time the authenticating process is initiated) to the network. The Network will encrypt the RAND code using its private key and then send the ciphered data to the SIM. The SIM then decrypt the ciphered data using the Network Public key and compares the two codes. If the two codes is not match then the SIM will send a "Reject/Registration" message and the connection will fail. This process should be optimal for the user to initiate. This procedure is illustrated in Figure 3.7.

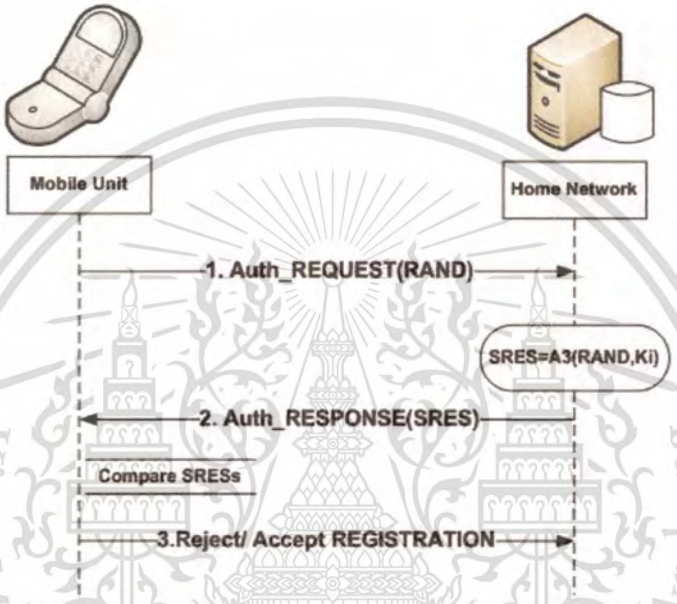


Figure 3.6 Mobile Unit - Home Network Authentication Procedure using K_i.

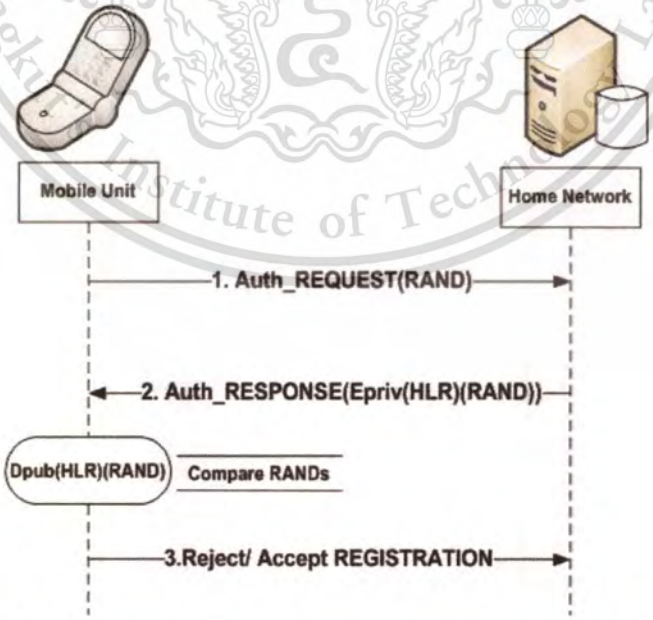


Figure 3.7 Mobile Unit - Home Network Authentication Procedure using Public Key.

3.3.2 Authentication the Visiting Network

Authenticity can be proven by proving the knowledge of the K_i (known only by the SIM and the home AuC). If the MU is authenticating a foreign VLR, the Home Network will not send and reveal K_i of the specified SIM. A proposed scenario is provided as follows:

- Since the SIM will not keep all the public keys for the VLRs, SIM and the VLR should exchange public keys for future use in the initiation phase.
- SIM will send a RAND along with the TMSI encrypted using the VLR public key.
- VLR will decrypt the message and extract the RAND.
- VLR will encrypt the RAND using the Home Network public key and send it to the HLR/ AuC.
- The HLR will check the "Chain of trust" of the VLR and check its validity. If the validity is valid, the VLR computes the SRES using RAND and K_i. The HLR will also compute the K_c using RAND and K_i.
- The K_c and SRES are sent to the VLR encrypted using the VLR public key. A VLR/HLR connection is illustrated in Figure 3.8.
- The VLR will decrypt the message and obtain SRES and K_c.
- The VLR will encrypt SRES using K_c and send it to the phone.
- SIM has calculated the K_c and use it to decrypt the message and compare the two SRESs, then the SIM send either Accept or Reject RESPONSE.

Another scenario to reduce the computation overhead in the SIM is to do the following:

- SIM will send the RAND in plain form to the VLR.
- The VLR will encrypt RAND using HLR public key and send the encrypted RAND to the HLR.
- The HLR will check the "Chain of trust" of the VLR and also its validity. If the validity is valid, the HLR computes the SRES using RAND and K_i. The HLR will compute the K_c using RAND and K_i.
- The Kc and SRES is sent to the VLR encrypted using the VLR public key.
- The VLR will decrypt the message and obtain SRES and K_c.

- The VLR will encrypt SRES using K_c and send it to the phone.
- The SIM will decrypt the message and compare the two SRESs and send either Accept or Reject RESPONSE.

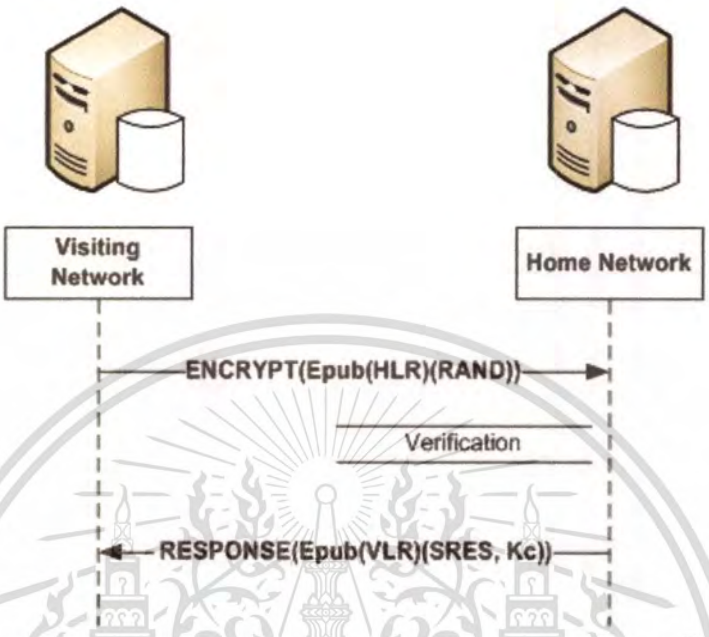


Figure 3.8 VLR/HLR connection to get SRES and Kc.

Message between the mobile unit and the visiting network for both case above are illustrated in Figure 3.9.

By following the procedure, the VLR authentication will rely on the HLR validation procedure. If CA is available, the HLR will check the validity of the VLR by sending its information to the CA. On the other hand, K_i is never been sent in plain or in encrypted from. RAND and SRES are not sent in plain form too. So, attacks of getting both SRES and RAND to calculate the K_i is not possible.

Moreover, the increasing length of the GSM specification's key of occurs in order to avoid the phone of being addressed or identified them in plaintext using their IMSI. This is suppose to prevent an eavesdropper to listen in the initial plaintext stage of the radio communication and to learn a particular subscriber is in the area (and what they are doing- the nature of communication can be known prior to ciphering- SMS, voice call, location update, etc.). Thus, there is a possibility that the network pages users by using their TMSI and also maintains a database in the VLR by

mapping from TMSIs to IMSIs. If the network somehow loses track of a particular TMSI, and cannot determine who the user is, then it must ask the subscriber for his IMSI over the radio link. Obviously, the connection cannot be ciphered if the network does not know the identity of the user, and thus the IMSI is sent in plaintext.

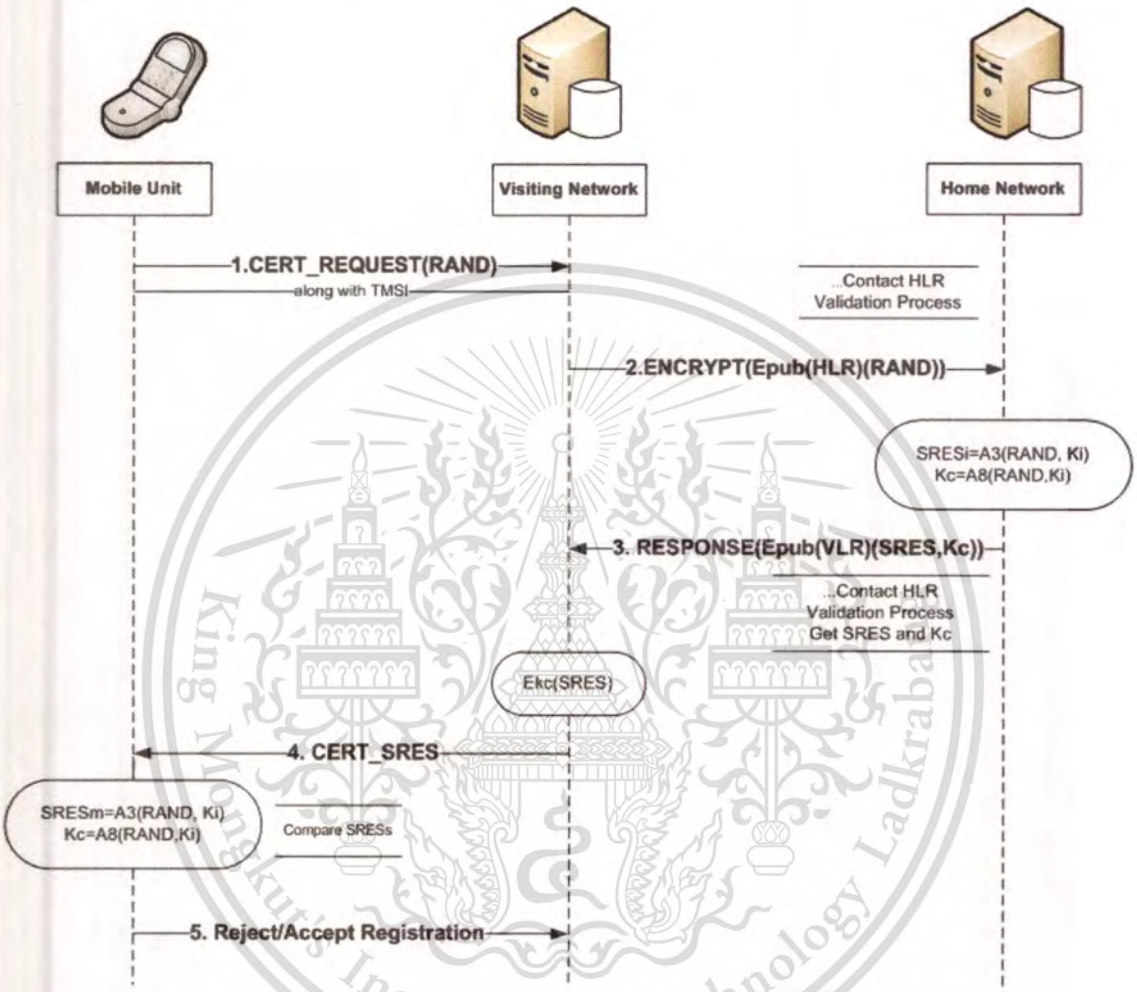


Figure 3.9 Mobile Unit- Visiting Network authentication procedure.

By using public key, SIM will extract the HLR public key from its certificate. In SIM-VLR communication, the public key of the VLR is distributed in the initiation process. The SIM then encrypts the IMSI using the public key and send it to the HLR/AuC. The VLR in this case will decrypt the ciphered data using the corresponding private key. Thus, the IMSI is not sent in plaintext anymore.

Similarly with K_c, HLR will identify the last K_c that is being used by the user and encrypt it using VLR public key. The VLR then will decrypt it using the correspondent private key. This

procedure can be applied if K_c is lost from the VLR that send the HLR a request to K_c. If the last used K_c is not updated in the HLR, then a new RAND should be sent to the SIM to calculate a new K_c by taking into consideration that RAND in this case should not be transmitted in plain form.

The comparison between the basic protocol in section 3.1 and the proposed protocol in section 3.3 can be summarized in the flowchart as the following:

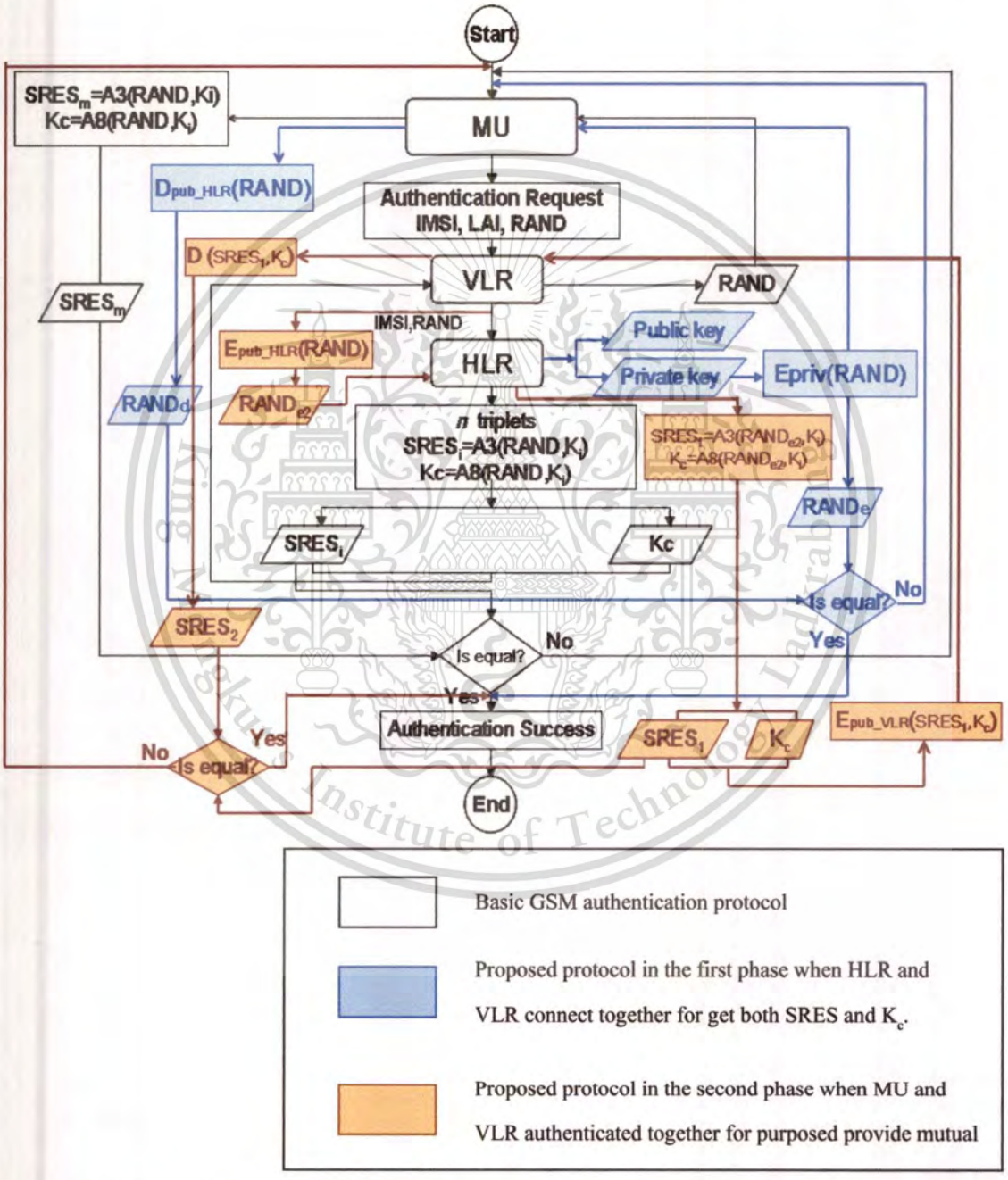


Figure 3.10 The comparison between the basic GSM protocol and proposed protocol.

The advantages of the new protocol are:

- Our main advantage that our system is action triggered due to flaws occurrences.
- The VLR authentication will rely on the HLR validation procedure. Note that there is a list of forbidden network operators in the HLR. Also if CA is available then the HLR will check the validity of the VLR by sending its information to the CA.
- K_i is never being sent in plain or even encrypted form.
- RAND and SRES are not sent in plain form. The attacks to get both SRES and RAND to calculate the K_i is not possible now.
- IMSI is not sent in plain form anymore.
- Secure communication between HLR and VLR can be implemented.
- Network can authenticate itself to the user. And the user will have the choice to authenticate the network.

The following explanation shows that the proposed protocol can achieve the requirement:

- Mutual authentication: The HLR use Digital Certificate to identity the VLR. Once the VLR is identified, the HLR can distribute its certificate to VLR. By authenticating the certificate, MU can ensure that it is communicating with a legitimate VLR. Therefore, the proposed protocol can achieve bilateral authentication between MU and VLR.
- Reduction of bandwidth consumption: in the proposed protocol, HLR gives the VLR Certificate Authority (CA) to authenticate MU. As long as the MU stays in the coverage area of the visiting VLR, the VLR can use the CA to authenticate MU for each call. Since the visiting VLR does not go back to HLR to require another set of authentication parameters, the signaling load is reduced between the VLR and HLR. Therefore, the proposed protocol can reduce bandwidth consumption.
- Reduction in the storage of the VLR database: in the proposed protocol, it is seen that the VLR only stores one copy of authentication parameters (RAND, K_i) instead of *n* copies ($RAND_i$, $SRES_i$, Kc_i). Therefore, the proposed protocol can save VLR database space.

- In the exiting authentication protocol for GSM, authentication of an MU is carried out by the VLR with the assistance of HLR when the authentication parameters are used up. In the proposed protocol, authentication of MU is to be done by VLR alone without the presence of HLR. The key point is that the HLR gives the visiting VLR of the MU authorization CA to authenticate the MU without knowing K_i.
- Owing to its simplicity and efficiency, the GSM system is widespread in the world. In order to not lose these advantages, the proposed protocol does not add any computations to it, nor is there any change in the architecture of the existing GSM system. The security of the new protocol is still based on algorithms A3, A5, and A8.

Public-key based authentication and key exchange protocols have the following enhancements and flaws:

- A number of well known and accepted security algorithms, such as DES and MD5, are used in these protocols.
- Classical public key cryptography techniques, such as the Diffie-Hellman (DH) protocol, are used in the proposed system. These techniques are characterized by higher key sizes and lower speed performance. These flaws are not acceptable in the mobile network environment where the mobile equipment has a small storage area and a limited computing power.
- No protocol that used to perform secure communication between the foreign and the home network authentication centers is defined.

3.4 Conclusions

The proposed protocol can be implemented without modifications of GSM system architecture. Hence, its security is based on the algorithms A3, A5 and A8. This fact does not imply that this protocol suffers from the same weakness in basic GSM authentication scheme that allowed the attackers to obtain the key K_i. The new protocol is used to protect this situation since mutual authentication is performed between MU and VLR at anytime. With the proposed protocol, an adversary cannot impersonate a network entity. A random number generated by the BSC for the

MU and network authentication is used. This random number is validated by the HLR. A counter held in the MU and VLR protects against a replay attack.

The Public key techniques employed by the new protocol do not modify the GSM architecture. However, the MU and the HLR must store additional information, i.e. MU must store the HLR's public key while HLR must store its own private key. Furthermore, the terminals must incorporate the functionality to perform a public key encryption. The simulation results of this proposed protocol will be shown in the next chapter.

Chapter 4

Performance Evaluation

In this chapter, the methodology for evaluating the proposed schemes in the GSM environment which is concentrated on the system performance results is described.

4.1 Simulation Environment

In traditional cryptography, a message in its original form is known as *plaintext* or *cleartext*. The encrypted information is known as *ciphertext* and the process of producing this ciphertext is known as *encryption* or *enciphering*. The reverse process of encryption is called *decryption* or *deciphering*. Cryptographic systems tend to involve an algorithm and a secret value. The secret value is known as the *key*. The reason for having a key in the algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information. There are three types of cryptographic paradigms: secret key cryptography, public key cryptography and hash algorithms/functions. The secret key cryptography has been used in basic authentication protocol. The public key cryptography is used in the proposed protocol. The COMP128 algorithm is a hash function which is used in GSM for authentication and session key generation [23].

4.1.1 Secret Key Cryptography

Secret key cryptography involves the use of a *single key* (K_c) that is shared by the communicating parties as show in Figure 4.1. This is the method used in GSM for providing confidentiality. Given a message (plaintext), encryption produces the ciphertext, which has the same length as the plaintext. Decryption retrieves the plaintext, using the *same key* used for encryption. This kind of encryption is also called *conventional* or *symmetric cryptography*.

Symmetric cryptosystems are further classified into *block cipher* and *stream cipher*. Block cipher divides the plaintext into blocks and encrypts each block independently. On the other hand, stream cipher encrypts the plaintext on a bit-by-bit (or byte-by-byte) basis. In essence, GSM networks mostly carry voice, which is one type of continuous data. Since stream cipher is based on the eXclusive OR (XOR) operation, using stream cipher to encrypt/decrypt voice data bit-by-bit (or

byte- by-byte) is very efficient. The GSM A5 algorithm, which is used to encrypt voice and signaling data in GSM, is a stream cipher based on three clock-controlled LFSRs [24].

The major problem in stream cipher cryptography is the difficulty of generating a long unpredictable bit pattern (keystream). In the one-time pad of stream cipher, a keystream is a sequence of randomly generated bits, and the probability of one bit becomes 1, independent from other bits, is equal to one and a half. An ideal keystream in one-time pad is pure random and has infinite length. The keystream cannot be generated by the receiving end, and cannot be distributed to the receiving and either. Pseudorandom bit generator has been widely used to construct the keystream. It generates a fixed-length pseudorandom noise as the keystream. The way to increase the length of the keystream produced by pseudorandom bit generator is important to the security of stream cipher. Thus, the security of a stream cipher is determined by the properties of the keystream. A complete random keystream would effectively implement an unbreakable one-time pad encryption; and a deterministic keystream with a short period would provide very little security.

Moreover, the GSM network adopts the symmetric cryptography that makes it insecure according to the use of one key for both encrypt and decrypt. Thus, by using man-in-the-middle attack, an attacker can verify the network and derived K_c. The attacker can also determine K_i and clone the SIM or eavesdropper the conversation in the entire GSM network as mentioned in chapter 3.

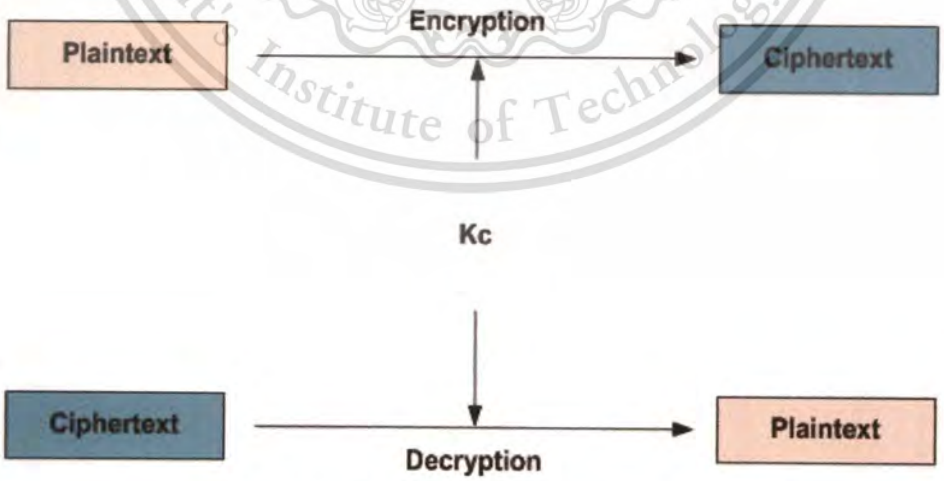


Figure 4.1 A Secret key cryptographic system.

4.1.2 Public key cryptography

Public key cryptography is not used in the current GSM security model. It is still an important technology to be presented in this thesis due to many proposals for increasing the security in GSM that use public key protocols.

In the public key cryptography, the keys are not shared. Instead, each individual user has two keys: a *Private Key* (that is not revealed to anyone) and a *Public Key* (that is open to the public) [25, 26]. This kind of cryptography is also commonly called *Asymmetric Cryptography* and was invented by Diffie and Hellman in 1975.

In the proposed protocol, the public key and private key, which are stored in MU, HLR, and VLR, are used. In these systems, encryption is done by using the public key and decryption is done by using the private key as shown in Figure 4.2.

Public-key cryptographic has gained extreme popularity since it was first published to the unclassified community. Public key cryptography is also the facilities of digital signatures, whereby a person can sign plaintext using his/her private key and anyone can verify the person's identity by using the public key of that person. Further, others cannot forget the signature of the person since it involves the use of his/her private key. The actual signature is generated from one of the following two methods based on the different mathematical problems:

- The RSA-Signature which uses the integer factorization problem and;
- The *Digital Signature Algorithm* (DSA) which is based on the discrete logarithm problem. The digital signature is based on a public key infrastructure and is a result of a cryptographic operation that guarantees signer authenticity, data integrity, and non-repudiation of the signed documents. The DS cannot be copied, tampered, or altered. The DSA uses the public/private key pairs, which are created to use with the RSA algorithm, to create and verify signatures as described in Figure 4.3.

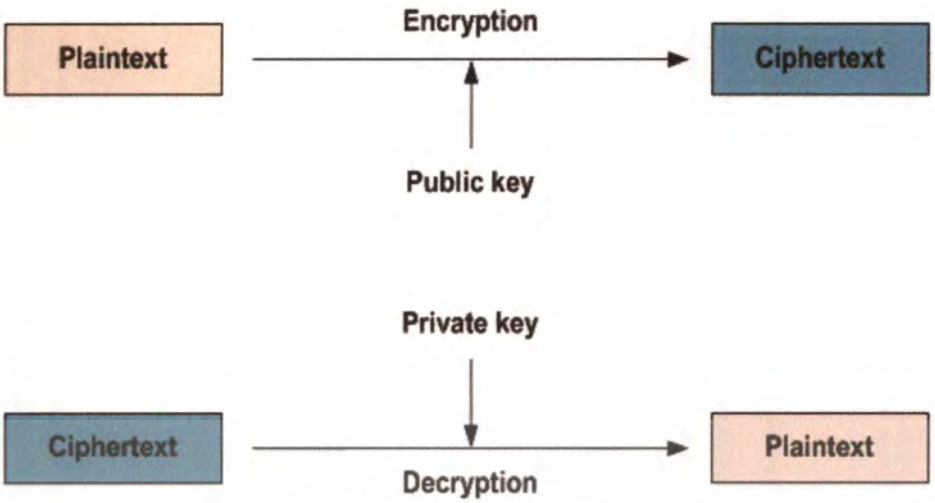


Figure 4.2 A Public key cryptographic system.

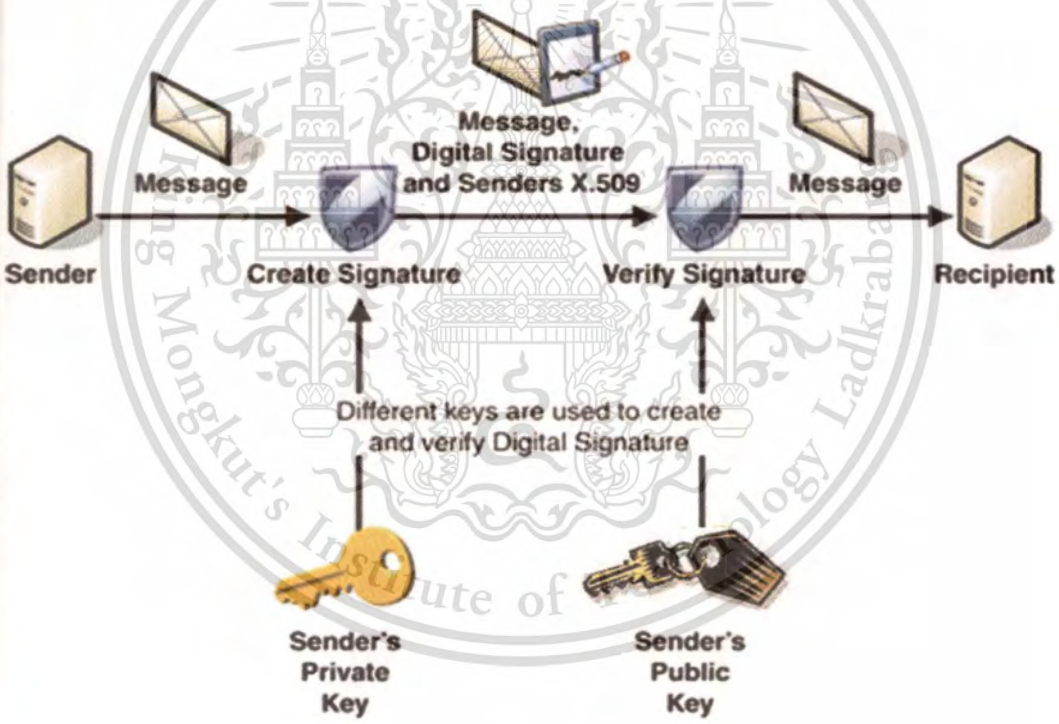


Figure 4.3 Digital Signature Creation and Verification.

One of the most popular public key cryptographic algorithms is RSA. As mentioned in chapter 3, the remaining problem is that message authentication is not provided. Any eavesdropper can intercept the message and send new messages. Digital Signature solves this problem by providing the second security objective message authentication.

RSA is an algorithm for public-key cryptography [27]. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure by giving sufficiently long keys and the use of up-to-date implementations. The security of RSA that relies on a fact in factoring huge integers, which is used as a public key in RSA, is infeasible.

In public key encryption technique, a key is split into two keys and they are called as public and private keys. The public key is advertised to the world and the private key is kept secret. It is not possible to generate private key using the public key. Therefore, someone who knows the public key cannot decrypt a message that is encrypted using the public key. A diagrammatic representation of public key encryption is shown in Figure 4.4.

In RSA algorithm, decryption is only possible through private key. It is impossible that private key is generated using public key. Therefore, the message transmitted from A to B using RSA encryption is secured even through others knows B's public key. For two-way communication between A and B there will be another set of keys for A.

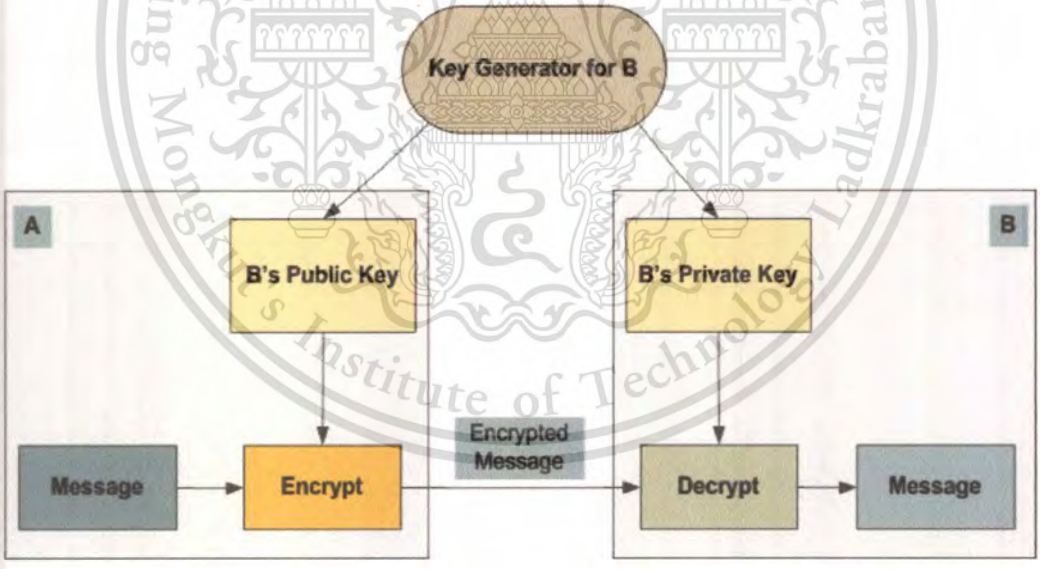


Figure 4.4 Diagrammatic of public key encryption.

RSA can be divided into two steps as shown in Figure 4.5:

Step 1: Generate a Public/Private key pairs by RSA setting

- "B" generates two large primes, p and q.

- "B" computes n = p.q and $\varphi(n) = (p-1)(q-1)$ (n will be used for the modulus)
- "B" chooses a random e ($0 < e < \varphi(n)$) where e is relatively prime to $\varphi(n)$ and e is used as the public exponent.
- "B" computes d as the inverse of e mod $\varphi(n)$ (d will be used as the private exponent).
- "B" publishes (n, e) as its public key and keeps (n, d) as its private key. The prime p & q must be kept in a secret or destroyed.

Step 2: Encrypt and decrypt data by using RSA algorithm.

- Instance: group Zn and the set (n, e, d)
- Assumption: A knows B's public key (n, e), but does not know B's private key (n, d).
- Algorithm:
  - A encrypts message M by computing $c = M^e \bmod n$.
  - A sends c to B.
  - Upon reception, B decrypts c by computing $M = c^d \bmod n$ and gets back M.

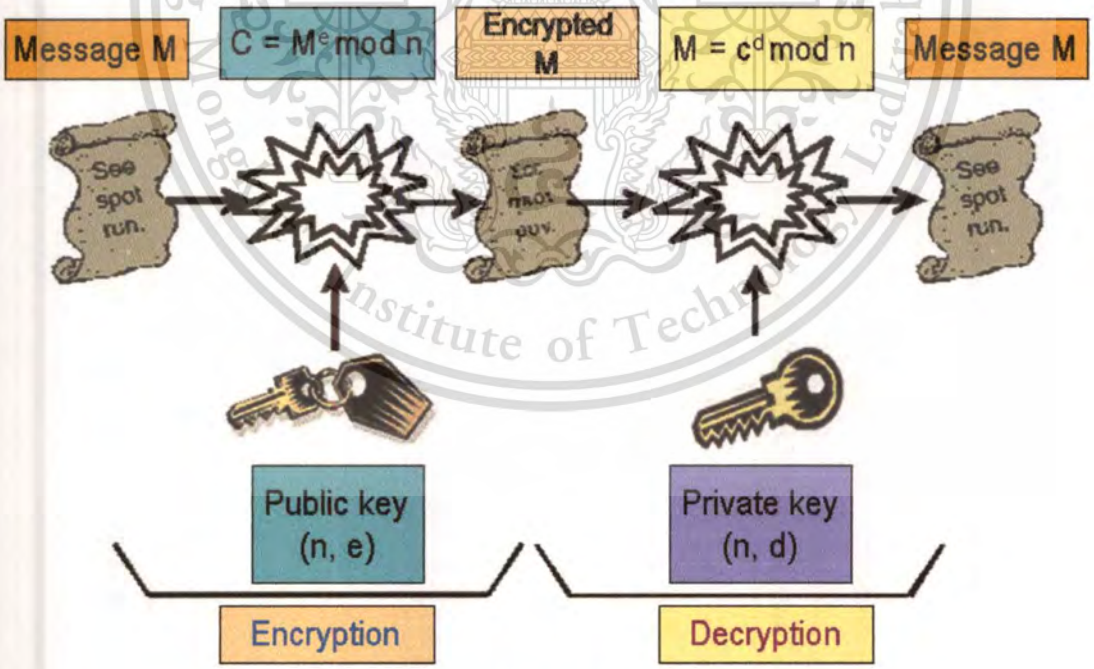


Figure 4.5 RSA algorithm.

In the proposed integration system, public key technique is the main factor. Public-key algorithms are based on mathematical functions rather than on substitution and permutation (based on number theory). More importantly, public-key cryptography is asymmetric that involves the use of two separate keys, in contrast to the symmetric conventional encryption, which uses only one key.

4.1.3 Hash function

Hash functions take a message string (with a variable length) as input and produce a fixed-length string output. The length of the input string is usually unrestricted or constrained by a very large number. Instead of the input message string the output string is used for transmission.

In the literature there are a lot of synonyms for hash functions that is used. The most common ones are compression functions (COMP128 algorithm), contraction functions, message digest, fingerprint or cryptographic checksum.

4.2 Programming Language Used in Simulation

In RSA, the most operation are power operation and module operation, and computing the result of (a^e mod N) is often be done, where N is the product of two big primes and e is the public key of encryption or the private key of decryption. To forestall the attack of public module number and low exponent, N and e must be large enough, and in the proposed software implementation N has 512 and 1024 bits size. Because of the limit of bit length, power module operation cannot be computed directly, several integers can be combined as one big integer. Therefore, this reduces the speed of RSA. Thus, the way to find practical methods to develop RSA is becoming an important.

There are many methods of implementing RSA cryptosystem in the environment that requires the speed to be very high. It can be developed with C language. The shortcomings must implement all algorithms that include the implementation of large integer, the generation of big primes, and the method of computing the greatest common division of two integers. Therefore, these are very tedious.

To make it easy to maintain the system, to develop quickly, and to solve the problem of cross platform, this system is developed by using Java language. Java is an object-oriented language. The system developed with Java language can be run on all platforms with cross-platform

language. It also provides a lots of classes library which are implemented with native programming language. Thus, its execution efficiency is very high. These are the reasons to choose this type of programming language to simulate the proposed system performance.

4.3 Simulation results

The simulation is implemented in Java language. Server side and Client side modules are implemented by J2SE v1.5. The codes run on Intel® Pentium® M 1.4 GHz machine with 512MB RAM. The RSA algorithm is implemented in the proposed protocol which is shown in the simulation procedure as in Figure 4.4. Time taken for the following operations is measured to evaluate the delay that will be caused by applying the RSA algorithm. The input parameters are shown in Table 4.1.

Table 4.1 The input parameters.

Inputs	Variable
Kc	64 Bits
RAND	128 Bits
SRES	32 Bits
IMSI (minimum)	10
IMSI (maximum)	15

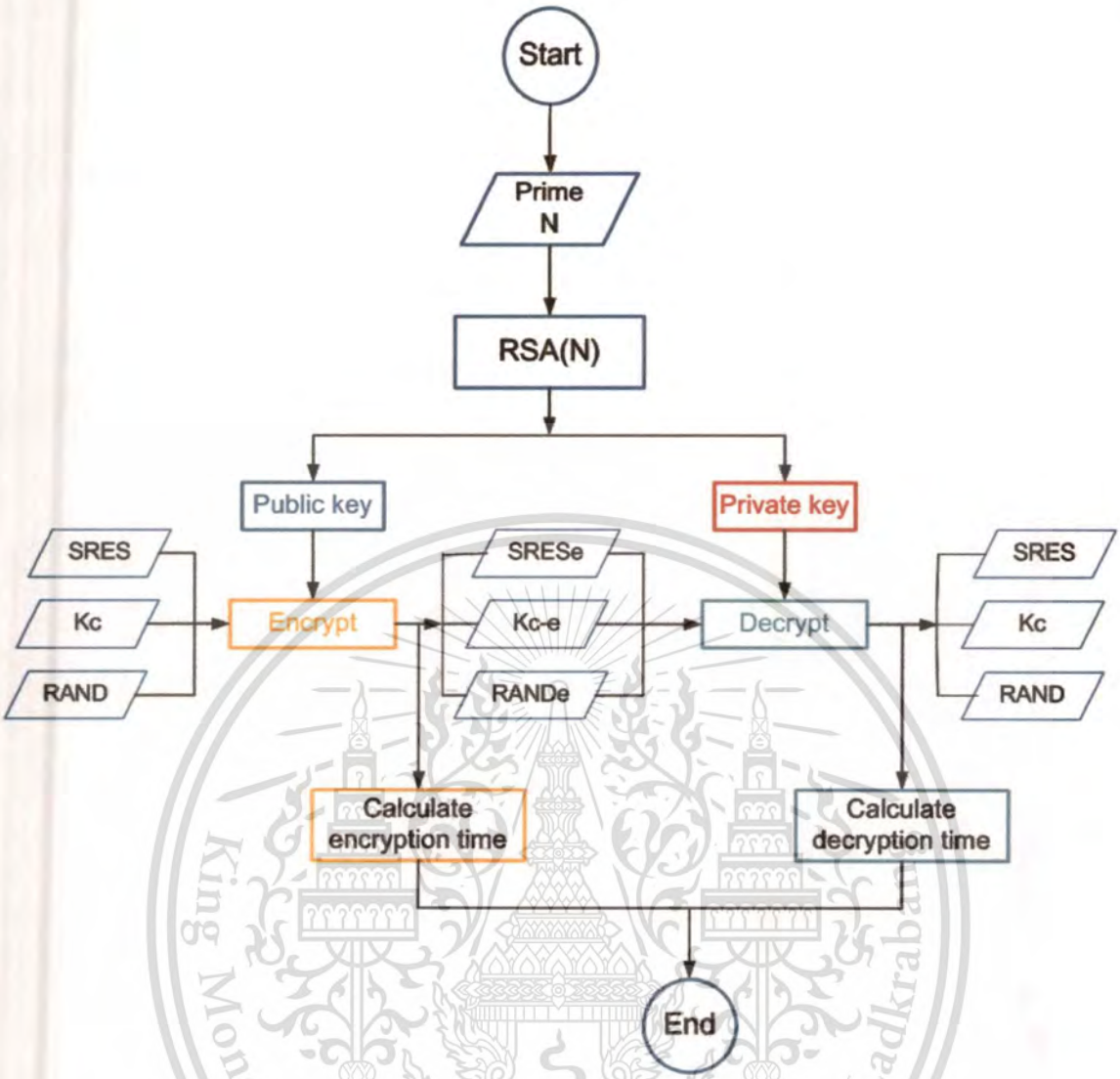


Figure 4.6 Simulation procedure.

The simulation is run for 1000 times and computation times are recorded for 512 and 1024 bits RSA keys. The standard Authentication time (Creating both SRES and Kc) is recorded. The time taken to Encrypt/Decrypt data (84 and 160 bytes) - using A5 is also recorded. Algorithms are seeded using 20 different RANDs and 20 different K_is.

The main purpose of the simulation is implementing the Public-key techniques. According to the results in the following tables, the average processing time of data encryption and decryption is very fast while two separate keys (Public and Private Key) are used. As the results, there are two benefits were obtained. The authentication process is more secure and the implementation of Public-key cryptography by using RSA algorithm can be achieved.

Table 4.2 The time taken in milliseconds to Encrypt/Decrypt an IMSI using RSA algorithm.

Value of IMSI	512 Bits key RSA		1024 Bits key RSA	
	Encryption time (ms)	Decryption time (ms)	Encryption time (ms)	Decryption time (ms)
10	1.065	2.219	9.575	15.495
15	1.487	2.235	9.966	15.641

Table 4.3 The time taken in milliseconds to Encrypt/Decrypt a 64 Bits K_c using RSA algorithm.

RSA	512 Bits key	1024 Bits key
Encryption time (ms)	1.519	9.581
Decryption time (ms)	2.233	15.520

Table 4.4 The time taken in milliseconds to Encrypt/Decrypt a 64 Bits K_c using A5 algorithm.

Encryption time (ms)	Decryption time (ms)
0.149350010	0.112074315

Table 4.5 shown the average time taken for Network encrypts 128 bits RAND by using its Private Key and SIM decrypts RAND using network Public key

Table 4.5 The average time when Network encrypts RAND and SIM decrypts RAND in milliseconds.

RSA	512 Bits key	1024 Bits key
Encryption time (ms)	2.225	15.719
Decryption time (ms)	1.488	9.568

The average processing time taken for RAND authentication is shown in Table 4.6; where SIM encrypt RAND using Network Public key and SIM decrypts RAND using Network Private Key

Table 4.6 The average time when SIM encrypts RAND and network decrypts RAND in milliseconds.

RSA	512 Bits key	1024 Bits key
Encryption time (ms)	1.509	9.521
Decryption time (ms)	2.253	15.552

The average time taken to encrypt and decrypt SRES by using A5 is shown in Table 4.7 and the time taken to create SRES by using RAND and K_i is 0.101146905 ms.

Table 4.7 The average time to Encrypt/decrypt SRES using A5 algorithm.

Encryption time (ms)	Decryption time (ms)
0.14442755	0.12689325

From these tables' results, it can be clearly seen that the time taken to apply the RSA is very small:

- Using 512 and 1024 bits key, the highest delay to authenticate a network to a user using RSA algorithm is 2.23 and 16.01 milliseconds in average respectively, which is a very few price to pay in terms of ensuring security.
- Encrypting a 64 bits session key with the RSA algorithm will take an average of 2.237 milliseconds for 512 bits key and 15.552 milliseconds for 1024 bits key. This time is only taken in the initial setup session when the session key is distributed.

In basic GSM authentication protocol, the time taken to encrypt and decrypt the 64 bits session key K_c is used for only A5 algorithm. The results show that the cumulative time need for encrypt/decrypt 64 bits K_c is 1.112ms at 1000 iteration process per simulation.

In RSA algoritms, 512 bits and 1024 bits are used in simulation:

- RSA 512 bits: time taken to encrypts/ decrpt 64 bits kc is 3.701 ms
- RSA 1024 bits: time taken to encrypts/ decrpt 64 bits kc is 25.001 ms

The comparison of cumulative time for engcryption/decryption between basic GSM network and proposed authenticaiton protocol by using RSA 512 bits and 1024 bits is shown in Figure 4.5.

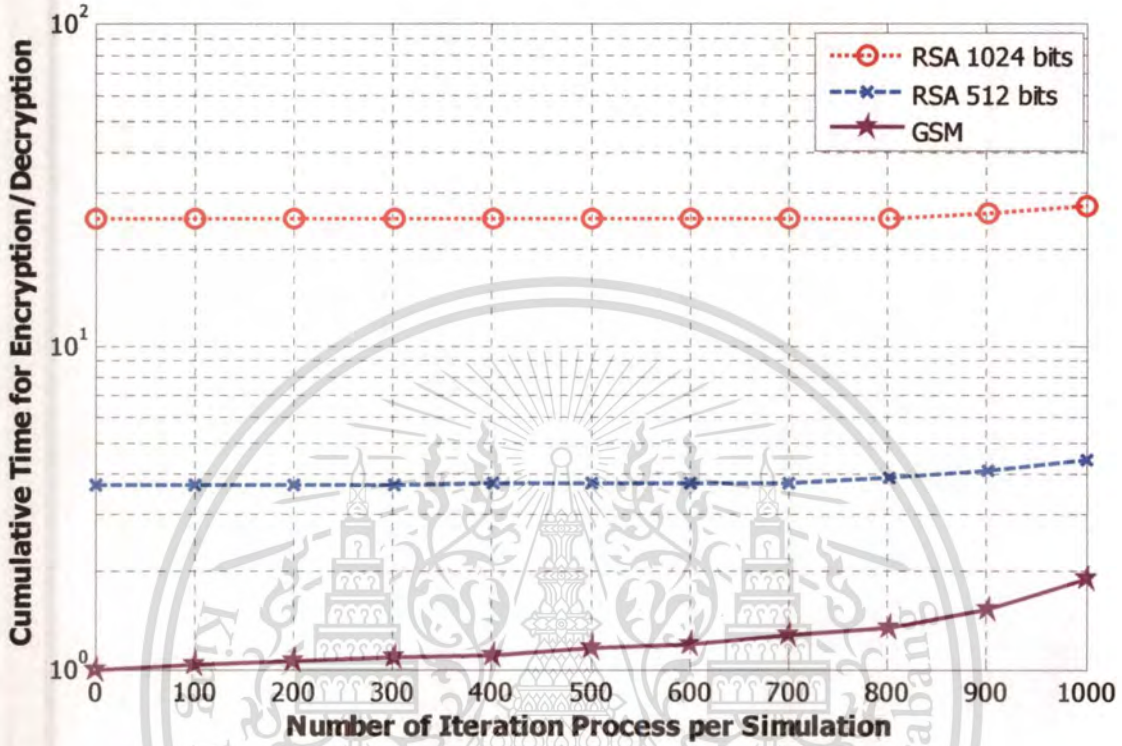


Figure 4.7 Cumulative time for Encryption/Decryption.

The different time taken by using basic GSM and RSA algorithm are shown in Table 4.8. As the results, the average time taken between basic GSM and RSA 512 bits is:

Average time A1 = 28.675/11 = 2.606818 (ms)

and the average time taken between basic GSM and RSA 1024 bits is:

Average time A2 = 265.965/11 = 24.178636 (ms)

Time taken for encryption/decryption in basic GSM is used only for one process while there are three processes in proposed authentication protocol. However, the different time A1 is only 2.606818ms. Therefore, it is possible to apply this proposed protocol by using RSA 512 bits in basic GSM network.

Table 4.8 Average time for encryption/decryption comparison.

Number of Iteration process per simulation	GSM (ms)	RSA 512 Bits (ms)	RSA 1024 Bits (ms)	RSA (512Bits) – GSM (ms)	RSA (1024Bits) – GSM (ms)
1	1.000	3.700	25.000	2.700	24.000
100	1.035	3.710	25.010	2.675	23.975
200	1.060	3.720	25.020	2.660	23.960
300	1.090	3.730	25.030	2.640	23.940
400	1.110	3.740	25.040	2.630	23.930
500	1.155	3.750	25.050	2.595	23.895
600	1.200	3.760	25.060	2.560	23.860
700	1.270	3.770	25.070	2.500	23.800
800	1.345	3.920	26.080	2.575	24.735
900	1.520	4.110	26.090	2.590	24.570
1000	1.900	4.450	27.200	2.550	25.300
				$\sum$ = 28.675	$\sum$ = 265.965

According to Table 4.8, the average time A2 is bigger than that of A1. Hence, the cumulative time to encrypt/decrypt data is also bigger. In RSA algorithm, the network security is based on the difficulty of factoring large integers, which is called key length. Key length is referred to the length of the modulus n in bits. Thus, it means that if the key length is longer, the authentication is more secure. However, the duration of time to communicate between MU and the network is slower.

4.4 Conclusions

Secure communication architecture for the GSM network is proposed. In the proposed architecture, public-key cryptography for user authentication, and stream cipher for message encryption and decryption are used. Message encryption is fast. SIM only stores user's personal information and the authentication process is very secure. Therefore, this architecture significantly improves the security of today's GSM network. In Table 4.8, the proposed protocol is compared with the basic protocols and other researcher's protocols. The proposed protocol can achieved mutual authentication because of the network can be authenticated by MU and vice versa. The reduction of the bandwidth consumption is achieved because the visiting VLR does not need to be transferred back to HLR for acquiring another set of authentication parameter. By using CA, The VLR only stores one copy of authentication parameters. Therefore, the required storage space for

VLR database is reduced. Since the proposed protocol does not change the current GSM architecture, the implementation of the proposed protocol can be applied.

Table 4.9 Comparisons between the Proposed Protocol with the existing GSM Authentication Protocols.

	Characteristics	Basic	Proposed protocol	A	B
1	Mutual authentication	No	Yes	Yes	No
2	Reduction of bandwidth consumption	No	Yes	No	Yes
3	Reduction of the storage of VLR database	No	Yes	No	No
4	Authentication of MU by VLR instead of HLR	No	Yes	No	No
5	Change architecture of current GSM	-	No	Yes	Yes

A= Secure Communication Mechanisms for GSM networks [21]: C3, C5, and C8 algorithms were used in the GSM authentication protocols instead of using A3, A5, and A8 algorithms.

B= A new Authentication Protocol for GSM Networks [22]: A new efficient authentication approach using "mobile user events counter" (COUNTM) was proposed.

According to the simulation results, it is found out that the time taken to apply public-key techniques is very small (with maximum of 15 m-sec using 1024-bits key length for authentication or encryption); which is very few prices to pay in terms of ensuring security. In order to apply the proposed system, both Mobile Unit and Network entities must include digital certificates and a public key algorithm. The software that implements the RSA algorithm can be mounted in both MU and Network HLR/VLR.

The findings of this thesis work and also the potential future work will be summarized in the last chapter.

Chapter 5

Conclusion and Future works

In this chapter, the proposed protocol is concluded and several possibilities for future works are explained.

5.1 Conclusion

Mobile communication is one of the fastest growing sectors of the telecommunication industry. Mobile users can make and receive calls while they are moving independent of time, location and network access. The Global System for Mobile Communication (GSM) is a Pan-European digital cellular mobile system supporting widespread roaming and *Personal Communication Services* (PCS) in a worldwide wireless communication network. However, wireless systems are more vulnerable to fraudulent access and eavesdropping. Although the authentication process in GSM gives a reasonable security level, it overloads the network with significant signaling traffic and increasing the call set up time. The signaling load and the authentication delay are of particular importance and become the subject of widespread research interest.

In this thesis, the GSM privacy and authentication protocol are studied and analyzed. The new authentication protocol with less signaling traffic and better call set up time that can be used in GSM network is also proposed.

Although the proposed protocol can achieve requirements security, the existing GSM system together with the proposed protocol is still not supported fully with security functions as the follows:

- Non-repudiation: the system does not provide the non-repudiation of origin or delivery.
- End-to-end confidentiality: GSM only ensures the confidentiality of data between the MU and VLR over wireless networks. It does not provide end-to-end confidentiality. Generally, it is assumed that a secure channel between the VLR and HLR over a fixed network is already set up.

It is shown that the proposed protocol enhances to address that these security flaws are not completely effective. These security issues the Public-key techniques which is characterized efficiently by both key sizes and speed performance, which are favored over classical public key systems. The use of the Public key cryptography methods in both user authentication and the key distribution services ensures that mobile user's private parameters are stored only in their SIM cards. Public key certificates used in the proposed system do not contain the identities of their owners which ensure user identity confidentiality on the air interface. However, the digital signatures on these certificates use the user identities to ensure the binding between the certificates and their owners. Since all of the data flow through the intermediate transport network between the home and the visited networks is encrypted with a private key algorithm, the proposed protocols do not rely on the security of that intermediate network.

5.2 Future works

In order to apply our system for GSM, both MU and Network entities must contain the Digital Certificates and a public key algorithm; which are also required in the changing of the Mobile Equipment (ME). Due to the evolution in ME industry, it is possible to work on this process.

For more research, the testing of Elliptic Curve Public Key instead of RSA is suggested. *Elliptic Curve Cryptography* (ECC) is an emerging method of asymmetric cryptosystems. Many standard committees (ISO, ANSI, and IEEE) are currently developing new standards for this method. The reason is that the *elliptic curve discrete logarithm problem* is much harder to solve than the normal *discrete logarithm problem (DLP)*.The RSA System requires the length of 1024 bits of security while the ECC methods need only 163 bits. Thus, this system should be preferred when computational time, memory capacity, or bandwidth are constrained.

The developed security protocols were explained in terms of the GSM environment. During the design of these protocols, it can be applied extensively to any wireless network architecture. Implementation and integration of the designed protocols in UMTS 3G wireless networks can be conducted in the future.

REFERENCES

[1] Javier Gozalvez Sempere, **"An overview of the GSM System"**, http://www.comms.eee.strath.ac.uk/~gozalvez/gsm/gsm.html

[2] S.M.Redl, M.K. Weber, M.W. Oliphant, **"An introduction to GSM"**, Artech House 1995.

[3] Azizi N, **"GSM 900"**, http://www.eecg.toronto.edu/~nazizi/gsm/ma/

[4] http://www.privateline.com/PCS/GSM06.html

[5] GSM01.02, European Telecommunications Standards Institute (ETSI), European digital cellular telecommunications system (Phase 2+) (GSM), **"General descriptions of a GSM Public Land Mobile Network (PLMN)"**, 1997, http://www.etsi.org

[6] Vijaya C, **"Security, Authentication and access control for Mobile Communications"**, http://www.ittc.ku.edu/~rvc/documents/865/865_securityreport.pdf

[7] GSM02.16, European Telecommunications Standards Institute (ETSI), European digital cellular telecommunications system (Phase 2), **"International Mobile Station Equipment Identities (IMEI)"**, http://www.etsi.org

[8] GSM04.07 (TS 100 929), European Telecommunications Standards Institute (ETSI), European digital cellular telecommunications system (Phase 2+), **"Security related network function"**, http://www.etsi.org

[9] Brookson C, **"Security and Cryptography Applications to Radio Systems"**, IEE Colloquium on GSM Security: a description of the reasons for security and the techniques 1994.

[10] GSM02.17 (ETS 300 509), European Telecommunications Standards Institute (ETSI), European digital cellular telecommunications system (Phase 2), **"Subscriber Identity Module (SIM)"**, Functional characteristics, http://www.etsi.org

[11] Brookson C, **"Can you clone a Smart Card (SIM)?"** http://www.brookson.com/gsm/clone.pdf

[12] Biryukov A, Shamir A, Wagner D, **"Real time Cryptanalysis of A5/1 on a PC"**, http://www.technojunkie.gr/gsm/data/gsmes/a51-bsw.htm

[13] Barkan E, Biham E, Keller N, **"Instant Cipher text-Only Cryptanalysis of GSM Encrypted Communications"**, 2003, http://www.cs.technion.ac.il/~biham/publications.html

[14] Ekdahl P, Johansson T, **"Another Attack on A5/1"**, Abstract, Proceeding of International Symposium on Information Theory (ISIT), Washington, 2001, http://www.it.lth.se/patrik/publications.html

[15] Security Algorithms Group of Experts (SAGE), **"Report on the specification and evaluation of the GSM cipher algorithm A5/2"**.

[16] W. D. Lin and J. Jan, **"A wireless-based authentications and anonymous channels for large scale area"**, Proceeding of the Sixth IEEE Symposium on Computers and Communications (ISCC'01), Tunisia, 3-5 July, 2001, pp.36-41.

[17] A. M. Barbancho, A. Peinado, **"Cryptanalysis of anonymous channel protocol for large-scale area in wireless communications"**, Computer Networks 43(2003)777-785.

[18] Alberto Peinado, **"Privacy and authentication protocol providing anonymous channels in GSM"**, Computer Communications 27(2004)1709-1715.

[19] V. Bocan and V. Cretu, **"Mitigating denial of service (DoS) threats in GSM networks"**, Proc. Int. Conf. on Availability, Reliability and Security, pp.523-528, 2006.

[20] C. Lee, M. Hwang, and W. Yang, **"Extension of authentication protocol for GSM"**, IEE Proc-Commu, Vol.150.no.2, pp.91-95, Apr.2003.

[21] Chi-Chun Lo and Yu-Jen Chen, **"Secure communication mechanisms for GSM networks"**, IEEE Trans. Consum. Electro, 1999, 45, (4), pp.1074-1080.

[22] Al- Tawil, K. Akrami, and Youssef. H, **"A new authentication protocol for GSM networks"**, Proceeding of IEEE 23rd Annual Conference on Local Computer Networks (LNC'98), 1998, pp.21-30.

[23] Menezes, Van Oorshot, and S. Vanstone, **"Handbook of applied Cryptography"**, CRC Press, 1996.

[24] Margrave D, **"GSM Security and Encryption"**, http://spyhard.narod.ru/phreak/gsm-secur.html

[25] William Stallings, **"Cryptography and Network Security: Principles and Practice"**, Prentice Hall, 2003, ISBN: 0130914290.

[26] Limor Elbaz, **"Using Public key Cryptography in Mobile Phones"**, Discretix Technologies Ltd, VP. Research, October 2002.

[27] RSA Data Security Inc, **"Public Key Cryptography Standard"**, Technical standards, 2004, http://www.rsasecurity.com/rsalabs/node.asp?id=2125

Biography

Personal Information

Name	BUI THU THUY
Nationality	Vietnamese
Date of birth	September 20, 1984
Place of birth	Phu Tho, Vietnam

Education

Bachelor degree

Field	Electronics and Telecommunications
Duration	2002-2007
Department	Department of Electronic Engineering
Faculty	Electronics and Telecommunications
University	Hanoi University of Technology, Vietnam

Master degree

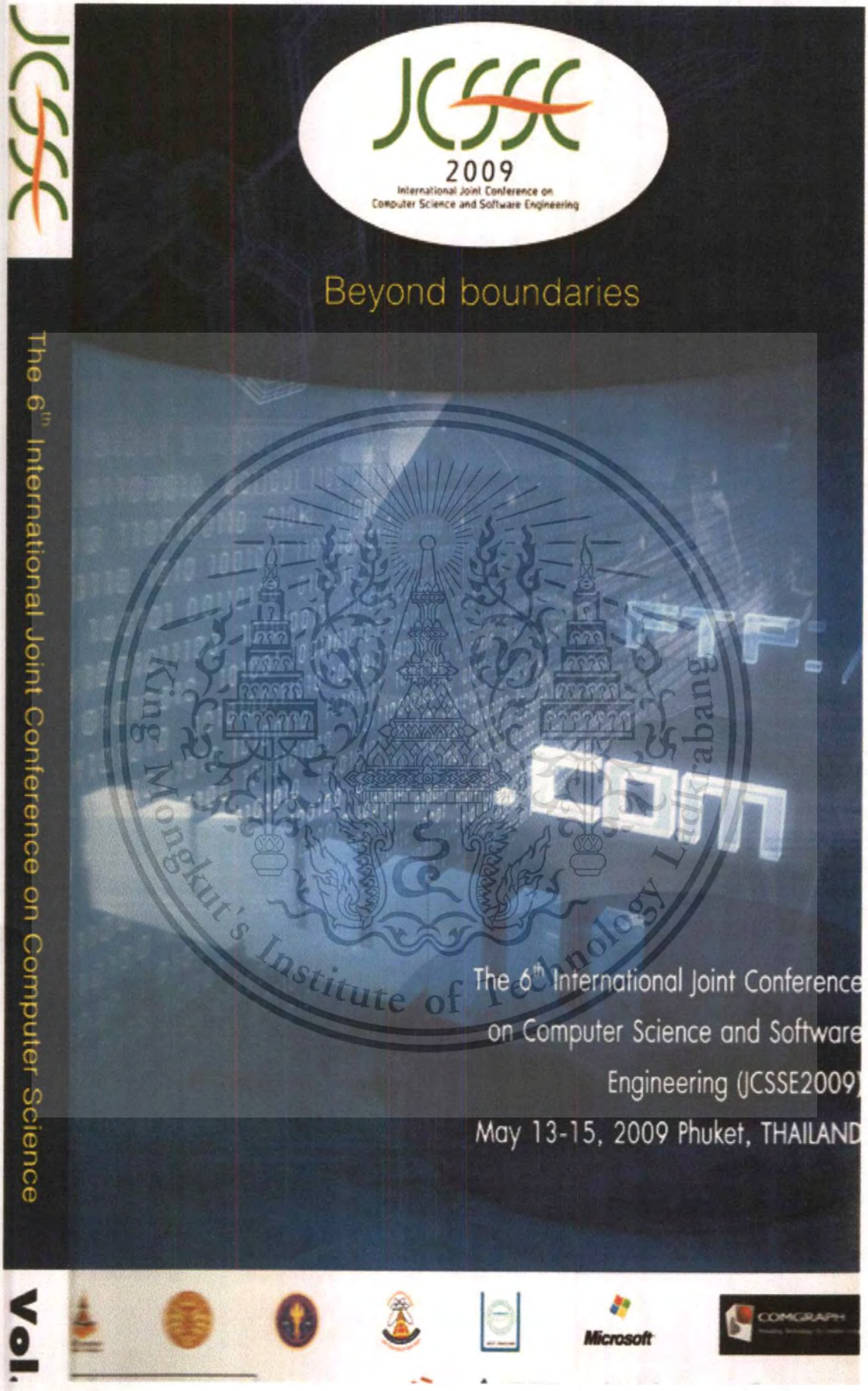
Field	Electronic Engineering
Duration	2008-2010
Department	Department of Electronics
Faculty	Engineering
University	King Mongkut's Institute of Technology Ladkrabang (KMITL), Thailand

Research Interests

Security Network System, Cryptography and Cryptanalysis, Coding Theory.

List of International Conference Proceeding Paper

1. Bui Thu Thuy, Narissorn Sangkanong, and Ruttikorn Varakulsiripunth, "A Study on Security in EAP-SIM Authentication Process with GSM Networks," *2009 6th International Joint Conference on Computer Science and Software Engineering (JCSSE2009)*, May 13-15, 2009, Phuket, Thailand, Vol.1, pp. 138-143.



JCSSE2009, May 13-15, 2009 (Vol. 1)

A Study on Security in EAP-SIM Authentication Process with GSM Networks

Bui Thu Thuy[*,†] Ruttikorn Varakulsiripunth[*] Narissorn Sangkanong[**]
[*]Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang
[**] Faculty of Technical Education, King Mongkut's University of Technology North Bangkok
Email: [*,†]thuy_pt209@yahoo.com (student), [*] kvruttik@kmitl.ac.th, [**]nss@kmutnb.ac.th

Abstract

A study on security in Extensible Authentication Protocol Subscriber Identity Modules (EAP-SIM) authentication process with GSM networks has been introduced in this paper. We present the concept of authentication procedure and authentication algorithm of EAP-SIM for GSM networks. After analyzing, we found the problem about security key and show some solutions. Finally, we propose the specification of EAP-SIM in authentication.

Key Words: EAP, EAP-SIM, GSM network.

1. Introduction

An Extensible Authentication Protocol (EAP) provides an infrastructure for clients to authenticate with a central authentication user. There are generally two ways of EAP: link control phase and authentication phase, and only authentication phase was considered here. That is, EAP will not select a specific authentication mechanism at link control phase but can delay this until the authentication phase. Due to this reason, the authenticators are able to request more information before determining the specific authentication mechanism. Examples of authentication schemes supported by EAP are MD5 challenges, One Time Passwords (OTP), and Generic Token Card.

802.1X, the IEEE standard for Port Based Network Access Control, can ensure that authenticated users or authenticators are granted to access through the controlled port on the access devices. The authentication software on the user's station is referred to as the supplicant. Until the user is authenticated, the supplicant can communicate with the authentication server (typically a Radius server), using the EAP. EAP server plays a role as a framework for a variety of authentication methods. The best EAP methods provide mutual authentication; that is, the supplicant is authenticated to the authentication server and the authentication server is authenticated to the supplicant. Global System for Mobile (GSM) Communication is an accepted standard for digital cellular services. EAP-Subscriber Identity Module (SIM) is an implementation of an authentication method of the EAP used in GSM-based mobile phone networks; that is, it provides the mutual authentication of the client device to the network, and the network to the mobile telephony network. EAP-SIM, containing user information, features the use of a SIM card as a type of smart card used in accounting/billing procedures and data used in the encryption of transmitted voice and data. Usually, SIM cards used in mobile phones are mostly used with laptops, notebooks, PDA handhelds, and other devices to integrate the wireless LAN (WLAN) and GSM-capable intelligent networks. The SIM card is a small printed circuit board inserted in a GSM-based mobile phone or other devices when signing on as a subscriber. This card, containing subscriber details, security information, and memory for a personal directory of numbers, is a small plug in type or sized as a credit card for use in mobile phones, PDA (Personal Digital Assistants) and personal computers.

This paper presents a study on security in EAP-SIM authentication process with GSM networks. Section I gives a background and overview of EAP, GSM [1,2,3] and EAP-SIM. Section II demonstrated authentication process using Radius server and EAP-SIM in GSM networks and terms [4]. Authentication algorithm for security in EAP-SIM [1,5] was described in Section III. Section IV discusses some features and solution for security in EAP-SIM [6,7,8,9]. Section V gives the conclusion drawn from the aforementioned evidence and makes the argument for interoperability of an EAP-SIM [1,2,3,4].

2. Authentication process with radius server and eap-sim in gsm networks

2.1 Terminology

The frequent uses of terms and abbreviations in this paper are given as follow:

- AAA (Authentication, Authorization and Accounting) is a security protocol implemented in a server for controlling access of voice and data into the networks.
- AuC: Authentication Center known as the GSM network element that provides the authentication triplets for authenticating the subscriber.
- Fast re-authentication: An EAP-SIM authentication exchange that is based on key derived upon a preceding full authentication exchange. The GSM authentication and key exchange algorithms are not used in the fast re-authentication procedure.
- Fast re-authentication identity: A fast re-authentication identity of the peer, including an NAI realm portion in environments where a realm is used (used on fast re-authentication only).
- Full authentication: An EAP-SIM authentication exchange based on the GSM authentication and key agreement algorithms.
- GSM triplets: The tipple formed by the three GSM authentication values RAND, K_c, and SRES.
- MAC: Message Authentication Code.
- NAI: Network Access Identifier.
- Permanent Identity: The permanent identity of the peer, including an NAI realm portion in environments where a realm is used, usually based on the IMSI (used on full authentication only).
- SS7; Signaling System 7: It is the architecture for performing out-of-band signaling in support of the Public Switched Telephone Network (PSTN). It identifies functions to be performed by a signaling-system network and a protocol to enable their performance.

2.2 Authentication in a GSM network

Every mobile subscriber is assigned as a unique International Mobile Subscriber Identity (IMSI) number to identify both the subscriber and their subscription within the GSM network [1]. The IMSI is made up of a 3 digit Mobile Country Code (MCC), a 2 digit Mobile Network Code (MNC), and a 10 digit Mobile Subscriber Identity Number (MSIN). The IMSI resides in a SIM, plugged into any Mobile Station Equipment (MSE). The IMSI is not dial-able so each subscriber is assigned as dial-able Mobile Subscriber ISDN (MSISDN) numbers. The mapping between IMSI and MSISDN along with a secret shared key, K_i, and the information of other subscribers maintained in a database called as the Home Location Register (HLR). As a mobile subscriber roams to other networks, it must be authenticated back to its home network as shown in Fig.1, which gives GSM-SIM authentication in a GSM network.

The mobile user is registered on the foreign network's Visitor Location Register (VLR). From the subscriber's IMSI, the VLR can communicate with the subscriber's HLR through the SS7 network using the Mobile Application Part (MAP) protocol. The VLR sends a MAP SendAuthInfo request with the subscriber's IMSI to the subscriber's HLR. The HLR responds to a MAP SendAuthInfo response with a triplet such as:

1. A random number challenge.
2. A secret response generated with the IMSI, random number, and K_i.
3. A session key, K_c.

Then, the VLR challenges the SIM using the random number. If the result responded from this SIM match with the one provided by the HLR, then the subscriber is authenticated; otherwise, the call is rejected.

2.3 Authentication procedure with EAP-SIM

Fig. 2 shows EAP-SIM authentication procedure. A user using the EAP-SIM to authenticate itself to the network should have a wireless card or a SIM reader and the EAP-SIM software in the user's laptop or PDA. The user inserts the SIM into the WLAN card and connects it to a PDA or a laptop. Note that the SIM issued by the service provider, be able to use for voice and data. When the user is within the range of an access point, the communication will be set up to connect the user, the access point, and the Radius server through the IP network. Based on the SIM card's IMSI, the server contacts the users' HLR through the SS7 network using the triplets - the session keys, the secret response and the random challenge. The server then challenges the SIM with the secret response. The SIM in GSM authentication generates the secret response from the Random Challenge with its secret key. This secret response is sent back to the server and compared to the secret response from the HLR and SIM. If they are equal, the server asks the access point to grant access to the

user. This access point connects the user to the WLAN and sends the server some accounting information to indicate that the user's wireless connection is complete. This accounting information might include the time, data, and location where the connection was established. Based on that information, the server from the access point inserts the data into its SQL database used for billing. When the user is connected to the WLAN, the access point keeps sending message to ensure the message connection. Once the user disconnects or someone wants to move out of range, the access point sends the server an accounting stop message to show the disconnection of the user from the network. Finally, the server will enter this information into its database used for billing.

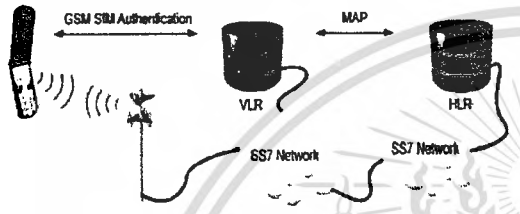


Figure 1. GSM-SIM authentication in a GSM network

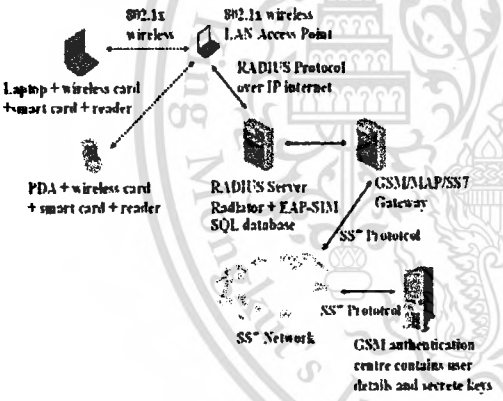


Figure 2. EAP-SIM authentication procedure

3. Authentication algorithm

GSM networks utilize encryption for three purposes: Authentication, Encryption and Key generation. The authentication algorithm used in the GSM system is known as the A3 algorithm and show in the Fig. 3. Most GSM network operators utilize a version of the COMP128 algorithm as the implementation of the A3 algorithm.

A3's task is to generate the 32-bit Signed Response (SRES) utilizing the 128-bit random challenge (RAND) generated by the HLR and the 128-bit Individual Subscriber Authentication Key (K_i) from the Mobile Station's SIM or the HLR.

A3 actually generates 128 bits of output. The first 32 bits of those 128 bits form the SRES.

The A3 algorithm is implementation in the SIM. The choice of A3 algorithm is given to the operator to give maximum security.

The encryption algorithm used in the GSM system is a stream cipher known as the A5 algorithm and show in the Fig. 4. The stream cipher is initialized with the K_c and the number of each frame. The same K_c is used throughout the call, but the 22-bit frame number changes during the call, thus generating a unique key stream for every frame. Both ciphering as well as deciphering are performed by applying an "Exclusive-Or" function between the 114 codes bits of a radio burst and a 114 bits ciphering sequence generated by a specific algorithm.

The same K_c is used as long as the Mobile Services Switching Center (MSC) does not authenticate the MS again. In practice, the same K_c may be in use for days. Authentication is an optional procedure in the beginning of a call, but it is usually not performed. The A5 algorithm is implementation in the MS.

The key generation algorithm used in the GSM system is known as the A8 algorithm and show in the Fig. 5. Most GSM network operations utilize the version of the COMP128 algorithm as the implementation of the A8 algorithm. A8's task is to generate the 64-bit Session key (K_c), from the 128-bit RAND received from the MSC and from the 128-bit K_i from the mobile station's SIM or the HLR.

A session key (K_c) is used until the MSC decides to authenticate the MS again. This might take days.

A8 actually generates 128 bits of output. The last 54 bits of those 128 bits form the K_c. Ten zero-bits are appended to this key before it is given as input to the A5 algorithm.

In practice the two algorithms A3 and A8 are combined into a single algorithm, called A38 which is used to simultaneously compute SRES and K_c from RAND and K_i. This combined algorithm is referred to as the authentication algorithm.

The A3/A8 authentication and key derivation algorithms that run on the SIM can be given a 128-bits random number (RAND) as a challenge. The SIM runs operator specific algorithms, which take the RAND and a secret key K_i (stored on the SIM) as input, and procedure a 32- bits response (SRES) and a 64-bits long key K_c as output.

The K_c key is originally used as an encryption key over the air interface, but in this protocol, it is used for deriving keying material and is not directly used. Hence, the secrecy of K_c is critical to the security of this protocol.

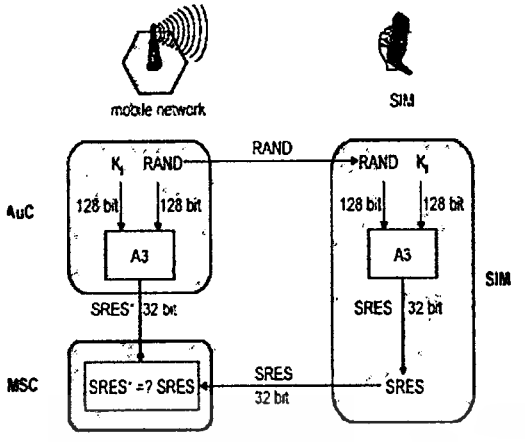


Figure 3. A3 authentication algorithm

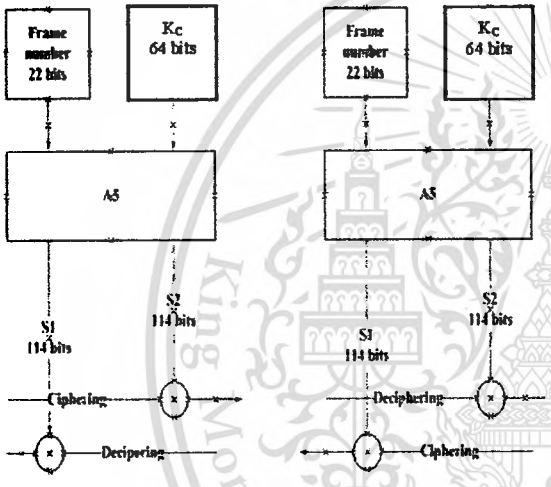


Figure 4. A5 authentication algorithm

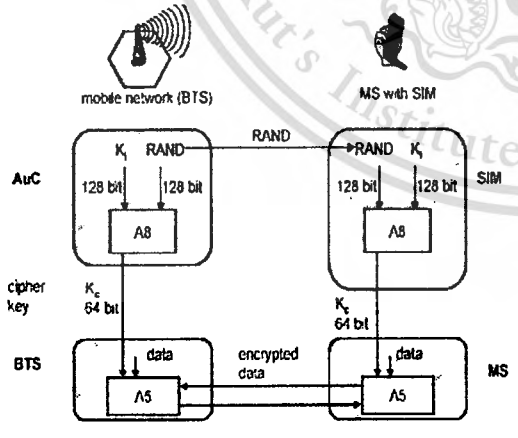


Figure 5. A8 authentication algorithm

COMP128 is the default algorithm used by GSM network operators for authentication and key exchange as shown in Fig 6. COMP128 generates the SRES using A3 algorithm and K_c using the A8 algorithm in one round of running. It takes in the K_i and RAND as input and procedures the 128 bits output. Out of which the first 32 bits form the SRES and the last 54 bits form the secret key K_c. The last 10 bits of the K_c are zeroed out for padding. This is a common procedure for all A8 implementations.

EAP-SIM specifies a mechanism for mutual authentication and session key agreement using the GSM-SIM to enhance the GSM authentication procedures. Unfortunately, it cannot succeed in its goal of providing 128 bits security from the current 64 bits security of GSM. Furthermore, it does not provide session independence between different sessions.

GSM authentication is based on a challenge-response mechanism. The A3 algorithm has a one-way property and is the core of a challenge-response protocol needed for authentication of users.

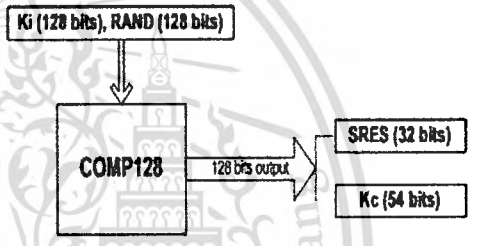


Figure 6. COMP128 authentication algorithm

Key generation is tightly linked to authentication and another algorithm with one-way property called A8 and is used for this purpose.

4. EAP- SIM Security Analysis

4.1 Analysis

GSM keys K_c are only 64 bits long and thus directly using them would not provide greater security. EAP-SIM tries to use a vector of them to create session keys. Since now, if 3 K_c's are used the overall key size can be 192 bits long and one can hope that we have achieved 128 bit security.

4.1.1 Only 64 bits security

Unfortunately, as we show that the security reached is only 64 bits and not 128 bits even when 3 K_c's are used. One simple way to attack an encryption key is to guess its value and proceed with the protocol. If the session key is 128 bit strong then the probability of success should be around $\frac{1}{2}^{128}$. However, we will show how to proceed with a guessing attack with success probability $\frac{1}{2}^{64}$. This should not happen with a secure 128 bit key and indicates the security is actually still 64 bits.

<Solutions>

There are couple of solutions to solve this problem which be proposed. The first is a simple solution which the client has to insist that the RANDs have to be different from each other. For example, if 2 RANDs are used then insist that R1 not equal R2. If there RANDs are used then insist that R1 not equal R2 and R1 not equal R3, and R2 not equal R3. This way the adversary will have to guess values at least two different points and that means the success probability will be less than $\frac{1}{2}^{128}$.

However, this does not help if only one RAND is used in the vector. Another solution is to insist that SRES also be part of the master key (MK) calculation. In that case the adversary would have to guess not only the values of K_c but also SRES. Even if only one RAND is used, this means the adversary has to guess at 96 bits which is better than 64 bits.

Of course, the two solutions can be combined, so that in the case where more than 1 RAND is used we would hope to get 128 bits of security and where only one RAND is used we still hope to get to 96 bits of security.

4.1.2 Lack of session independence

The protocol, however, suffers from a serious deficiency that is sessions are not independent. If the values of K_c from one of the sessions are compromised then an adversary can use them to carry fraudulent conversations with the client. We can see this is the case because the K_c values are dependent on the RANDs and not on the random challenge from the client. Thus if the RAND and K_c vectors are ever compromised, an attack can use them directly. The client who receives the RANDs would not know that these were compromised values and would go ahead with the protocol, verify the MAC and accept the attacker as a legitimate network.

A secure mutually authenticated session key agreement protocol should not have this problem. It might be suggested to everyone to make sure that the K_c vector is never compromised. This is not practical to assume in a general protocol because even if the authenticator is trusted today. It is not clear that it can be trusted for all future times which would be needed to make sure that a past K_c vector is never used again. Secondly, even if a user trusts an authenticator for a type of conversation in a location, it is not clear that that user would want to trust for other types of conversation. But a compromised K_c could effect all future conversations at all locations.

Another way to see that session independence is important is to look at why are we using different session keys at all for encryption and message authentication? A part of the answer is to not expose lots of plaintext/ciphertext but a large part of the answer is what we just stated about independence.

Furthermore, if a user could trust that the K_c vectors will never be compromised, then that user never has to generate more than K_c vector and just use the same K_c vector for different sessions. Since the Rc challenge from the client will be different, we can assume that the message encryption and authentication session keys will be different. There is no reason to generate different triplets at all. Actually, there is no reason to even generate one triplet; a user could just share the root key K_i itself if a user is assured that it will not be compromised. Then the security can be strongly guaranteed by using the 128 bit K_i with mutually authenticated session key agreement protocol.

<Solutions>

There is actually no solution for this problem as long as GSM triplets are used as the fundamental source of keying. The above solutions to strengthen the 64 bit to 128 bit are of no use in creating session independence, and it is hard to see how we could do it easily.

One approach possible but not practical is for the client to store all the past RAND vectors it is seen and to make sure that they are not repeated. If it sees that a previous RAND vector is being re-used it should satisfy the protocol but abort before using the session keys to actually encrypt anything. In this case, if the real network ever repeated a previous vector accidently, that vector would be used up and at the next try the network would use a fresh vector which will be different. The chance of a vector being accidently repeated is negligible because an individual RAND is 128 bits.

Since it is not practical to store all past values, perhaps the client can store the most recent n RAND values and make sure they are not repeated. This may give some partial protection in practice. Actually the whole RAND vector does not need to be stored, just a part of the RAND, for example 32 bits can be stored and looked for repeats; this way many previously used values can be checked for repeats. Of course, if a previous value was repeated then the client should make sure that value is always checked for repetition in the future and never allowed.

The EAP-SIM protocol does not provide 128 bits of protection and we gave an attack showing that only 64 bits of protection is provided. We also gave solutions to address this problem. Secondly, EAP-SIM does not provide session independence and this is a serious deficiency. Unfortunately, there does not seem to be a solution which can fully eliminate this problem as long as the keying material is based on the GSM triplets.

4.1.3 Another limitations of GSM and possible improvement

GSM only provides access security; it does not protect against active attacks. Another weakness with GSM lies in a particular implementation of the A3/A8 authentication and cipher key generation algorithm COMP128. Last but not least, GSM networks lack the flexibility to quickly upgrade and improve security elements such as the cryptographic algorithms.

One solution is to use another cryptographically secure algorithm for A3. This would require issuing new SIM-cards to all subscribers and updating HLR software. This solution is easy to be implemented because the network operators can make the changes themselves and do not need the support of hardware or software manufactures or the GSM. There is now a new algorithms available called COMP128-2.

The operator can employ a new A5 implementation with strong encryption too. A new A5/3 algorithm has also been agreed upon to replace the aging A5/2 algorithm. This improvement would require the co-operation of the hardware and software manufactures because they will have to release new versions of their software and hardware that would comprise with the new algorithm.

4.2 EAP-SIM Specification

We have defined some specification of EAP-SIM in authentication security as shown in Table 1 below.

Table 1: EAP-Sim specification in authentication security

	SPECIFICATION	YES	NO	N/A
1	Cipher suite negotiation		×	
2	Mutual authentication	×		
3	Integrity protection	×		
4	Replay protection	×		
5	Confidentiality (except method-specific success and failure indications)	×		
6	Key derivation	×		
7	Key strength (supports key derivation with 128-bits effective key strength)	×		
8	Dictionary attack protection			×
9	Fast reconnect	×		
10	Cryptographic binding			×
11	Session independence		×	
12	Fragmentation		×	

5. Conclusion

This paper presents about the security of EAP-SIM builds on underlying GSM mechanism. EAP-SIM makes a secure access possible by combining the 802.1x, EAP and GSM authentication protocol.

GSM authentication is based on challenge-response mechanism. The A3/A8 authentication and key derivation algorithms that run on the SIM can be given a 128-bits random number (RAND) as a challenge. EAP-SIM also extends the combined RAND challenge and other message with a message authentication code in order to provide message integrity protection along with mutual authentication. Many of the security features of EAP-SIM rely upon the secrecy of the K_c value in the SIM triplets, so protecting these values is important to the security of the EAP-SIM protocol.

The EAP-SIM protocol does not provide 128-bits of protection and we show an attack that only 64 bits of protection provided.

We also show solutions to address this problem. The lack of mutual authentication is a major weakness in GSM authentication because it only has 64-bits in security key. In some cases, EAP-SIM provides better security properties than the underlying GSM mechanism by increases security key to 128 bits.

6. References

[1] H. Haverinen, and J. Salowey, "*Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", IETF RFC 4186, January 2006.*

[2] E. Barkan, E. Biham, and N. Keller, "Instant cipher text-Only Cryptanalysis of GSM Encrypted Communication", *Proc. of CRYPTO*, Springer Lecture Notes in Computer Science, 2003.

[3] John Scourias, Report, "Overview of the Global System for Mobile Communication", http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html, 9th September 2005.

[4] Online- Education Tutorial, International Engineering Consurtium, "EAP Methods for 802.11 Wireless LAN Security", http://www.iec.org/online/tutorial/eap-methods/index.html 9th September 2005

[5] Article, GSM Association 2005, "GSM Security Algorithms", http://www.gsmworld.com/using/algorithms/index.shtml, 9th September 2005.

[6] L. Blunk and J. Vollbrecht, "*PPP Extensible Authentication Protocol (EAP")*, Internet Engineering Task Force, Request for Comments (RFC) 2284.

[7] William Stallings, "Cryptography and Network Security, Principles and Practices, Third Edition", Prentice Hall, 2003.

[8] A. Salomaa,Public-key Cryptography,2nd ed., Springer 1996.

[9] N. Asokan, V. Niemi, and K. Nyberg, "Man-in-the-middle in tunneled authentication protocols", *Proc. of 11th Cambridge Workshop on Security Protocols*, Springer Lecture Notes in Computer Science. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

Acknowledgment

This research is funded by ASAEN University Network/Southeast Asia Engineering Education Development Network (AUN/SEED-Net) Project through the Japan International Cooperation Agency (JICA).