Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2015
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Authentication for Mobile Communication using Aka Protocol

A.Kirthika[#1], S.Karpagavalli[*2]
[1, 2] *Department of Computer Applications, S.A Engineering College*
kirthikamca994@gmail.com, sskvalli005@gmail.com

***Abstract*—** Mobile communication is widely used by all over the world. Mobile phones are developed by day by day and the security issue are increasing. The using of handset is increasing due to the request of marketing side. In this paper focus on the architecture of GSM and UMTS and Authentication and key agreement (AKA) protocol. While using the encryption algorithm A3, A5, and A8 to solve the problem of transmission process authentication vector in secure manner into a secure manner.

***Keywords*—** *Authentication, GSM, AKA protocol, keys.*

1. Introduction

Communications which are wireless is experienced an impulsive growth and it became more important part of the society. Mobile communication is an important aspect in the most common tool of communication over the recent year. Several improvements regarding the mobile communication technology has been made by developing various multiple accessing schemes for wireless communication.

Mobile phones use for an in case of emergency. Authentication, encryption, security and access control are some important features that should be present the communication network. The main reason of security is so much important to the communication process of radio waves.

In mobile communication it has some popular standard in 2G GSM, 3G UMTS and 2.5 General Package Radio Service (GPRS), 4G LTE (Long Term Evolution).

2. GSM

The mobile telephone networks are becoming more popular by every day by day, Global System for Mobile communication or Group Special mobile (GSM) is the most popular standard for mobile phone in the world. It is developed in second generation. GSM standard developed to cater voice services and data delivery using digital modulation. The GSM network for wireless voice and low data rate applications, such as SMS (Short Message Service). GSM network operators have roaming agreements with foreign operators, user can continue of using their mobile phone while they travelling to other country.

The European Telecommunication Standards Institute (ETSI) developed the GSM specification in 1989. In old GSM system used as 25 MHz frequency spectrum in the 900 MHz band. The 25 MHz frequency spectrum was then divided into 124 carrier frequency of 200 kHz. Now GSM standards are currently used in the 900 MHz and 1800 MHz band. It using the technique Frequency Division Multiplexing (FDM) for transmits the signal. It was the first one which introducing the encryption and cryptographic mechanisms for confidentiality and authentication of mobile communication system.

GSM it also suffering some security problem of weak encryption and authentication algorithms, along with the short length of using secret key and no authentication process in the network.

The main features of 2G are launching of information transmission in digital signal form though the air interface. Advantages of 2G were improved speech quality, better network capacity, easy data communication process and security. The main goal of GSM security is to provide exact billings of phone calls.

In GSM have four security services. That is,

- Anonymity: That is not easy to identifying the user of the system.
- Authentication: The operator can know who using the system for billing process.
- Signalling protection: sensitive information of a signalling channel, signal are protected by the radio path. Such as telephone numbers.
- User data protection: protected the user data and passing over the radio path.

Other GSM security are

- On air interface, GSM uses encryption and TMSI instead of IMEI
- SIM provided 4-8 digits PIN to validate the ownership of the SIM.
- 3 algorithms are specified as.

A3 algorithm for authentication
A5 algorithm for encryption
A8 algorithm for key generation

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

In GSM it has three services and they are,

- Tele services - It is like a voice communication. For example mobile telephone for the emergency call.
- Bearer or Data services - It is like a SMS 160 character data transmit from mobile terminal to voice mail box.
- Supplementary services – It such like a call waiting, call barring, call forwarding, call hold.

2.1 UMTS

The Universal Mobile Telecommunication System (UMTS) is a Third Generation (3G) mobile system which was fully based on the Global System Mobile Communication. It was specified by Third Generation Partnership Project (3GPP)[3]. It is developed after the success of GSM. UMTS have more bandwidth and spectral efficiency to the network operation using Wideband Code Division Multiple Access (WCDMA) technology.

Third generation was initiated by some organizations like UMTS Forum, European Telecommunications Institute (ETSI), Telecommunication Conference (CEPT) and European Posts.

The main idea was to achieve the global roaming, so it will become easy for mobile user to access their mobile system entire world.

The UMTS (3G) networks are backward compatible with 2G GSM and 2.5G GPRS networks. Over the next few years, GSM and GPRS operators would move towards UMTS. It will be more important during in this time, in which multi-mode handsets will appear. It can make imperative to know about the GSM and GRPS.

UMTS it will do the theoretical concepts. It helps network inside the devices the authentication process of a roaming mobile device which are generated by the home network.

2.2 Authentication and Key Agreement(AKA) protocol

Authentication is used to identify whether data is access by the valid user or not. Authentication uses a technique that can be described as a “Challenge and Response”, based on mechanism encryption. AKA is a mechanism which performs authentication and session key distribution in UMTS networks. Authentication and Key Agreement is also used for one-time password generation mechanism for Digest access authentication.

2.3 Existing system

During the process of authentication a session key (Kc) is generated which is security. With the help of the key and encryption algorithm A5 and all calls are changed into encrypted format. There are three different algorithm standards for A5 present, which are A5/1, A5/2 and A5/3. A5/1 and A5/2 are confidentially managed by the association of GSM which provides them some special access license only to the vendor. The A5/3 is a new approach and it will base on f8 ciphering algorithm of UMTS and is easily available on websites.

There two main goal in GSM ciphering, they are

- Protection of call from eavesdropping scenario between the base station and mobile device.
- Protection of call from those who are non-paying users.

The process of ciphering is managed by the base station, it also choose the algorithm which has to use in the process. But using only ciphering algorithm cannot provide the complete solution for this problem [3]. This type of flaws occur in the security architecture of GSM has been improved in the 3G by using different types of encryption algorithm for confidentially and integrity over in the air interface and by using the mutual authentication.

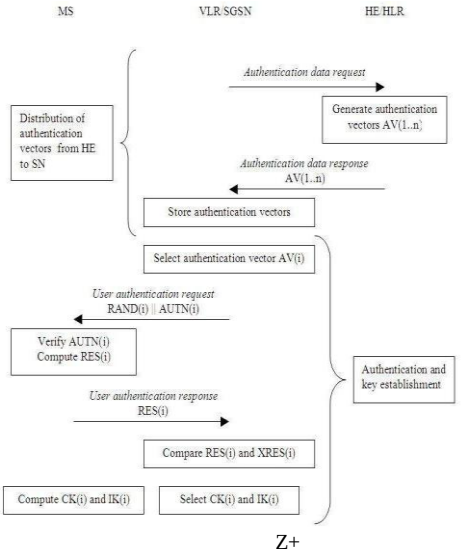
Mutual authentication means both the network and the device engage in response and challenge of exchange. Main goal of authentication and key agreement is to verify the network contain the secret key for the client and client have the secret key , without any actual exchange of the key.

There three entries involved way to process the authentication of UMTS system, they are

- Authentication centre (Auc) and Home environment
- Visitor location registers (VLR).
- Terminal or USIM.

When the home environment receives an authentication request and it generate the authentication vectors of five components are Expected Result (XRES), Integrity check (IK), Session key (Kc), Random Challenge (RAND) and Authentication Token (AUTN). Authentication vector can be used only one time in authentication of USIM. Authentication vector will be generated by sequence number and (SQN) and key. After receiving the authentication vector are stored into the visitor location register. One of authentication vector is selected and a user authentication request which contains Random Challenge (RAND) and authentication Token (AUTN) is send to the mobile station (MS). The mobile station (MS) check the network authentication token (AUTN) by verifying the sequence number (SQN) is not in sync then it disconnect the authentication process but it allow for the retry. If the sequence number (SQN) and token AUTN are verified by the mobile station (MS), then it will shows the network has successfully authenticated by the client. After the Mobile station is generates its authentication response by the random challenge and key then it sent it to the network. Network also compare where the response (RES) and Expected result (XRES) similar to the GSM. If both are equal then shows the successful authentication done between to the network and the client.

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)



The most important of the authentication mechanism in AKA is combination of authentication vector. Every authentication vector have one session key of authentication and key agreement between authentication centre (AUC) or the Home Environment (HE) and the mobile station (MS).

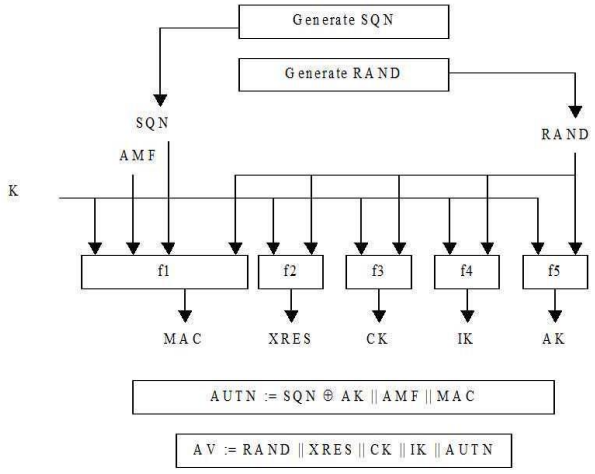


Fig 2: Authentication vector generation process

The authentication vector (AUTN) is of size 16 bytes, CK is of size 16 bytes, Expected result (XRES) is size range of between to the 4-16 bytes and RAND is size 16bytes.

f1 : Calculation of Message Authentication Code (MAC)
f1* : Calculation of MAC-S
f2 : Calculation of RES and XRES
f3 : For the computation of CK
f4 : For the computation of IK
f5 : For the computation of AK
f5;For the computation of AK but in the re-synchronization process.

There are some flaws, which are

- Transmission process of authentication vector is unsecure.
- Only same key are used between the mobile equipment and home environment.
- Operating the sequence number is difficult
- Incomplete bidirectional authentication process.

2.4 Proposed system and methodology

GSM network can be modelled on its three basic parts or sub-system, namely mobile station (MS), Base Station sub-system (BSS) and the network and switching sub-system (NSS) or home subsystem. The Mobile Station (MS) subsystem consists of the mobile equipment (ME) and the card called the subscriber identity module (SIM). The mobile station is radio handset used by a subscriber/ user to access the services provided by the mobile network.

The base station subsystem is an access network and performs functions specifics to the radio access technique used in GSM. The BSS has two different types of entities; the Base Transceiver Station (BTS) that terminate the radio connection with the mobile station and the Base Station Controller (BSC) control the resources in the BTS.

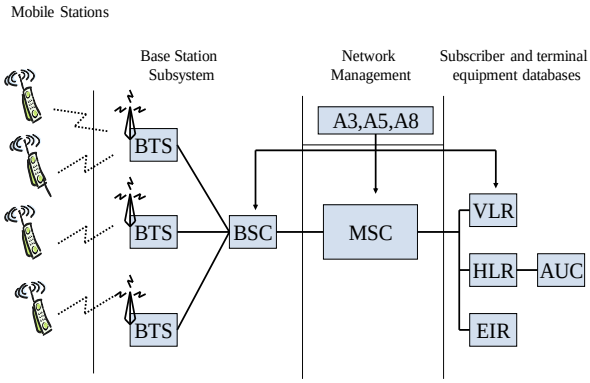


Fig 3: GSM architecture

The home subsystem is consist of five parts, the Mobile Switching Center (MSC), home location register (HLR), Authentication center (AuC), visitor location register (VLR) and the Equipment Identify Register (EIR).

The network switching subsystem (NSS) perform the core function of the network, which include the mobility management, call control, switching and routing. The BSC interface acts between the core network and the air-interface. The core network can also manage the

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

subscription information of a subscriber or user and provides service based on the information. The HLR is a database it collect the complete information of the local customer and its main database also. The VLR contains of roamer information that make sure if the valid subscriber or user and retrieve the information from HLR to manage your phone call. The VLR is act has a storage place.

In GSM it using three security algorithms is A3, A5 and A8 algorithm. The A3 and A8 are implemented in the Subscriber Identity Module SIM card. A3 algorithm will do the authentication process in the mobile station. A8 algorithm is used to generate key and the key is session key. A5 algorithm used to encrypt the data transmission in between the mobile station and the BTS. A5 it can signalling the data and user data encryption.

The A3 algorithm use the individual subscriber Authentication key (Ki). The key is of size 128 bits and the A8 algorithm use the session key (Kc) key is of size 64 bits.

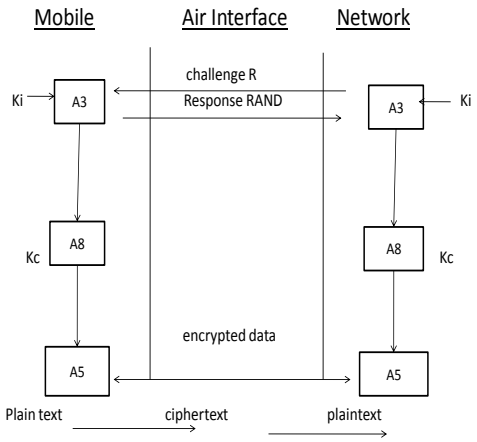


Fig. 4: working of the A3, A5, and A8 algorithm

The A3 and A8 both take a 128 bits key (Ki) and a 128 bits challenge (RAND) as inputs. The mobile station receives the random challenge from the Base Transceiver Station and encrypted it with the subscriber authentication key (Ki) assigned to the Mobile Station utilizing the A3 algorithm.

3. Conclusion

Security system is widely important now a day because most of the components that we use today are basically with the electronics component. Example: mobile phone, computer, door, car, weapons, machines, and many others. In this paper using of encryption algorithm to make secure in GSM and UMTS using A3, A5 and A8 algorithm which helps to avoid the man-in-middle attack were it little possible in GSM. But still they are flaws in security of the system, which have an area for future work.

References

[1] "2G Mobile Networking: GSM and HSCSD" – Nishit narang, Sumit kasera.
[2] Atishay Bansal, Dinesh Sharma, Gajendra Singh, Tumpa Roy " New Approch For Wireless Communication Security Protocol By Using Mutual Authentication"
[3] Jyoti Kataria, Dr. Abhay Bansal – "Exploration of GSM and UMTS Security Architecture with Aka protocol"
[4] Othman O.Khalifa, Abdulrazzag Aburas, A.Al Bagul, Meftah Hrairi, Muhammad Shahril bin – " Security management System of Cellular Communication"
[5] S.R.Bharanialankar,C.S ManikandaBabu–" Intelligent Home Appliance Status Intimation Control and System Using GSM"
[6] Amritanshu Srivastaval, Hrishikesh Narayan, Tripathi –" GSM Calling based Multi-tasking Robot vehicle with password"
[7] Ozer Aydemir, Ali Aydin Selcuk- " A strong User Authentication protocol for GSM"
[8] Muxiang Zhang, Yuguang Miyake-" Security Analysis and Enhancements of GSM Authentication and key Agreement protocol"
[9] Ryu Watanabe, Yutaka Miyake-" User Authentication Method with Mobile Phone as Secure Token"
[10] Chenthurvasan Duraiappan And Yuliang Zheng –" Improving Speech Security And Authentication In Mobile Communications

A.kirthika is holding a under graduation degree B.Sc Computer Science from Mahalakshmi womens's college of arts & science and pursuing post graduation in Master of computer applications from S.A.Engineering college. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report Writing.

S.karpagavalli is holding a under graduation degree in BCA Computer Application from Bharathi women's arts & science college,Kallakurichi and pursuing post graduation in Master of computer applications from S.A.Engineering college. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report Writing.