International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10951-10958
© Research India Publications
http://www.ripublication.com

# One-Time Hashing Secret For 4g Mobile Telecommunication Networks

**Rama Prabha K.P**
*Assistant Professor (SITE)*
*Vellore Institute of Technology,*
*Vellore, India*
*mail2ramaprabha@gmail.com*
**Jayanthi R**
*Assistant Professor (SITE)*
*Vellore Institute of Technology,*
*Vellore, India*
*profjai14@gmail.com*
**B.Rubadevi**
*Assistant Professor(CSE)*
*Arunai Engineering College*
*Tiruvannamalai, India*
*ruparuba@gmail.com*

## Abstract

The fourth generation of telecommunication is the paramount expansion in the field of communication. There is a need of providing the authentication for such mobile systems which is the crucial one that needs to be answered more effectively and efficiently for crisis such as expanding security dangers and attacks. Authentication protocols for Endorser and System Mutual Authentication in a versatile frameworks is a methodology by which portable system picks up the trust about the character of the conveying supporter and endorser checked that he is speaking with the right system. This paper deals about the failures and existing models and proposal of the new model for providing authentication by one time hashing password technique and also the advantages of using this model. Whenever the user needs an access to the network they have control to it by the login id and password.

**Index terms:** Long Term Evolution (LTE), Data Base Management System (DBMS), one time hashing

## Introduction

The term 4G this means fourth generation of the wireless telecommunication technology. This is the enhanced version of third generation wireless telecommunication technology which is known as 3G.The fourth generation wireless telecommunication technology (4G) which Supports the basic features of 3G such as voice, data rate, etc. in addition to that it provides mobile ultra-broadband internet access. It includes applications such as cloud computing, video conferencing, IP telephony, 3D television etc. Two candidate systems were deployed for 4G technology namely WiMAX standard and Long Term Evolution (LTE) [8]. According International Telecommunications Union- radio communication sector (ITU-R) which specified some of the data rate that should besatisfied by 4G technology. The 100 (Mbit/s) for high portability remote correspondence such as cars and trains. For low portability remote Correspondence such as stationary users and pedestrians. The 4G technology uses OFDMA multi-carrier transmission and some frequency domain equalization and these makes the technology possible to transmit very high data rate. The peak bit rate of 4G is enhanced by smart antenna arrays for multiple –input multiple output (MIMO) communications.

The preferences of utilizing 4G over 3G is the pace obtained by the 4G over 3G is four times more excellent and its forward error correction (FEC) which uses concatenated codes for corrections. The switching technique used by the 4G technology is both packet switching and message switching. This message switching was not available in the 3G technology. Because of those advantages it paved way for Wi-MAX2 and Long Term Evolution (LTE-Advance).

The Long Term Evolution is a developing radio access system technology institutionalized in 3GPP and it is advancing as a development of Universal Mobile Telecommunication Systems (UMTS). It plans to give consistent Internet Protocol (IP) connectivity between the Client Equipment (CE) and Packet Data Network (PDN) without any interruption to the end users provisions throughout versatility. The 4G LTE methods help for up to 86 Mbps dependent upon particular engineering and programming bases. It utilizes multiple access scheme called Orthogonal Frequency Division Multiple Access (OFDMA) and it is similar to approach followed in the WiMAX which also uses OFDMA. OFDMA likewise divides the bits in a solitary information transmission into various subcarriers to expand the rate and rearranging it at the objective. The LTE convention however, has the added capacity to relegate specific clients on the fly, advancing the transfer speed accessible at any given time.

The WiMAX2 is the advanced version of WiMAX. It works on the same general standards of Wi-Fi. A workstation furnished with WiMAX might get information from the WiMAX transmitting station, presumably utilizing the scrambled information keys to keep unapproved clients from taking access. The quickest Wi-Fi association can transmit up to 54 megabits for every second under ideal conditions and it ought to have the capacity to handle up to 70 megabits for every second. The most amazing distinction isn’t speed; its distance. WiMAX surpasses Wi-Fi by miles. Wi-Fi’s reach is around 100 feet i.e. 30 meters. WiMAX will cover a sweep of 30 miles with a remote access. The expanded reach is because of the frequencies utilized and the force of the transmitter. Obviously, at that separation, landscape, climate and huge structures will act to decrease the most extreme go in a few circumstances, yet the potential is there to blanket immense tracts of the area.

Despite the fact that the 4G technology has the significant preferences over the 3G innovation but its major impediments over the 3G technology is its security authentication model that fails. The existing authentication protocol fails to provide security to 4G which is explained in the Literature Survey. As the 4G technology arrives to the customers as of late there is a need to provide the best security authentication protocol for the same which is dealt in this paper. The model proposed here is the one time hashing password technique and anew password based mutual authentication technique.

## Literature Survey

There are several encryption and decryption techniques existing in the wireless communication that strives to give best security to those wireless networks. Similarly the 4G-LTE has several authentication models with encryption and decryption to be performed. As every models will have their own advantages and limitations these are well explained in this chapter.

The first model is the Kasumi cipher [10] for 4G-LTE which is a block cipher used in GPRS and UMTS communication systems. It involves the usage of S-boxes. The major advantages of this cipher model are: it fits the prerequisites of the 3G authentication environment, offers solid encryption by the means 128- bit keys and also offers strong security against most common block figure strike strategies. The strong limitations of this cipher models is the needs of satisfactory assurance against new manifestations of attacks and the other disadvantages of this model is it obliges an trade-off between execution and intricacy (as far as space) owing to the usage adaptability. These impediments leads to the development of the new model called SNOW 3G.

The second model for the 4G- LTE security is the SNOW 3G which is the stream cipher for 3GPP encryption calculations. Some changes were made to the original SNOW model that lead to the development of the new model called SNOW 3G model. And this model can withstand any algebraic attacks that were present in the kasumi cipher. This cipher model has the advantage of dodging the comparative outline standards with the kasumi cipher model. The cipher model has the disadvantage of more computationally convoluted in terms of fitting region space in regards to a provision for uprightness assurance.

Subsequently, the Milenage cipher model for 4G-LTE security. The model involves the usage of 128 bit block cipher. The block size and the key size are equal in terms. This cipher model offers secure execution and security against side-channel assaults by means of Advanced Encryption Standard (AES) as center capacity. The limitations of this cipher model are it obliges interoperability of distinctive general Subscriber Identity Module (SIM) usage and for similarity purposes; it might be less demanding if a standard algorithm was utilized.

The next model is the ZUC cipher model which also a stream cipher model that suits the 3G technology security environment which started its phase in the development especially for 4G-LTE systems. This model has the advantages such as; it seems to have a powerful design configuration with a vast security range and it expands on configuration standards of well-known ciphering calculations.The disadvantage of using this cipher model is the model requires more examination to increase further certainty.

These disadvantages of each cipher model lead to development of the new model called one time hashing password technique which proves to be efficient and economical for the subscribers as well as service providers.

## Methodology

The methodology of the proposed model is explained in this chapter. Initial phase is the enrollment phase in which the subscriber registers their number allotted by the service provider on the network. This phase may include the processes like enrollment of Subscriber Identity Module (SIM) number and the mobile IMEI number to the network service provider. The service provider checks whether the correct user is making contact with it by checking the number in their own database. If the subscriber is the existing user of the network then it sends a simple handshake message stating that it can make communicate. Otherwise the user is new to the network then the subscriber has to enroll their number to the service provider. This finishes the initial phase of the one-time hashing password technique.

The second stage of this one-time hashing password technique involves the usage of the user authentication phase. In this phase the user is provided with a login identity and password by the network service provider. When the user enters their password and login identity, the information reaches the service provider. Then the network searches its database whether the subscriber has the access rights over the network. If yes, then the network generates a one-time password to its subscriber. Otherwise the network returns the message with information stating that it is not the registered user. The process is terminated here. This is the user authentication phase in one-time hashing password technique.

The last phase of this one time hashing secret procedure is the gathering of one-time password generated by the service provider for their subscriber [3]. After obtaining the password from the user to his/her own number it is written in that website page that asks for the password. After that process a secure connection is established between the subscriber and the service provider. This finishes the one-time secret word hashing technique.

When this methodology is compared with the other cipher models, it has the most major advantages than any other model due to its ease of usage and simple technique involved. The architecture of the proposed model is explained in the below chapter.

## Architecture of The Proposed Model

This chapter explains the architecture of the proposed simple one-time hashing secret word technique. The following figure depicts the detailed architecture of the proposed model. The mobile station that is subscriber is shown as mobile nodes. The service provider and the database server and the database is also shown in the below architecture.

The number 1, 2, 3 in fig 1 denotes a connection between the users and the service provider. The double side arrow mark shows the request and receives commands. The number 4 denotes the connection between the service provider and the database server in order to verify the requested subscriber is present in their database or not. The number 5 denotes the connection establishment between the database server and the database. The database server checks in the database whether the user number is there or not. The double sided arrow shows the one time message carrying scheme between the user mobile phone and the service provider.

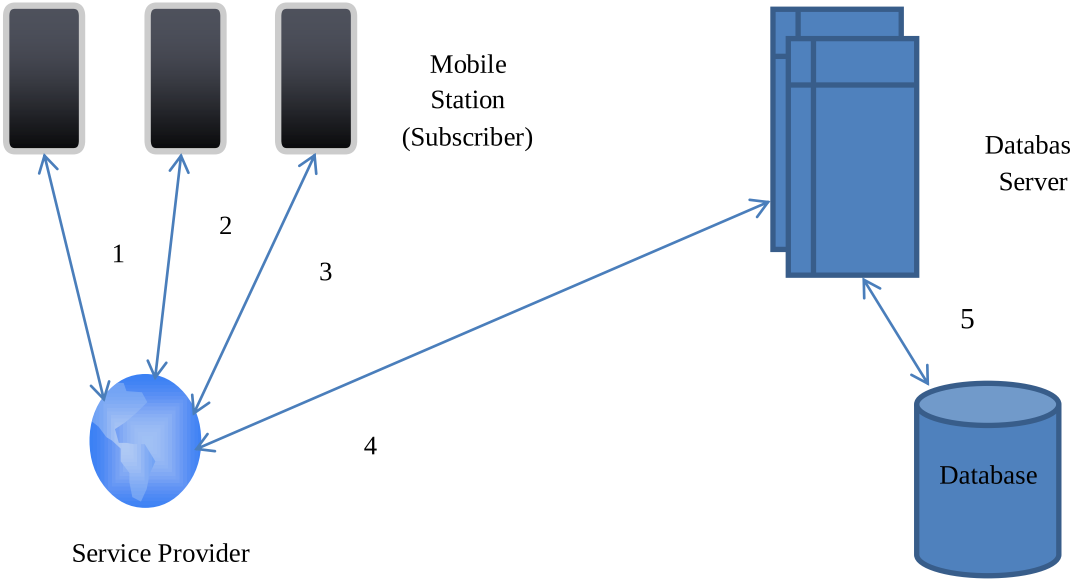

**Figure 1:** Architecture of the proposed model

## Working Mechanism

The working of this one-time hashing password authentication scheme for 4G telecommunication mobile networks is very simple and precise. The subscriber who wants to connect to particular operator can get connected to it by the usage login id and password provided by the service provider at the time of purchase of the SIM card as

As shown in figure 2. After entering the login identity and password, the Service provider checks its database server, whether it has subscriber registered under their network. If the subscriber is the registered subscriber then he/she is provided with a one-time hashing password generated by the service provider to the number requesting the login. If not then the service provider will return a foul message to the requesting user as the false one. Then the user can enter the one-time password it has received in the one-time login window shown in their mobile phone. After this process a secure connection is established between the subscribers and the service provider. In this one time password a hashing is performed which is defined as one time hashing password. The method is very simple and connection between the service provider and the user can be well established, even if the user is in roaming.

## Authentication Scheme

The authentication scheme used here is the one-time hashing secret word method. In this method the subscriber wishing to connect to a service Provider is provided with a random number generated by the service provider which is of exponential in form. After sending the random number to the subscriber, a key is produced for the service provider network and the one time key is produced in the service provider network with a random number ($R_{s)}$ taken and the can be given as Key ($K_s$) where suffix‘s’ denotes the service provider side.

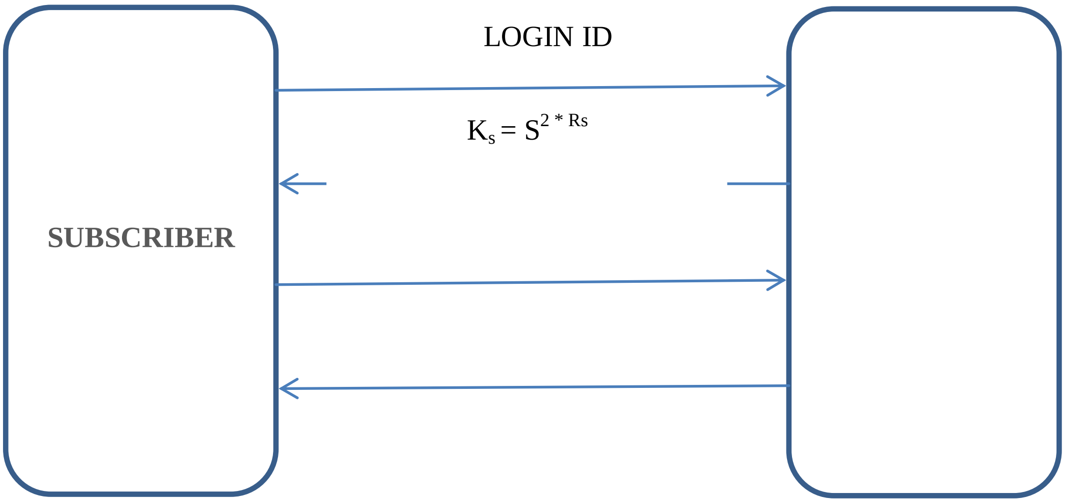

Fig 2 Working mechanism of the proposed model

$K_{s=}S^{2 * Rs}$

The subscriber after sending the one time password, a key is generated by default with an alternate random number other than the one generated by the service provider which is also in an exponential form say ($R_c$)with a key ($K_c$) where ‘c’ denotes the client side that is subscriber.

$K_{c\,=}\,S^{2 * Rc}$

Subsequently, the subscriber sends the one time key to service provider. After that a hashing function is utilized dependent upon both the random key. The random numbers used is known to both the subscriber and the service provider and the hashing used on them is also the same. This produces processed hashed information and this hashed information is considered as a one-time password by the subscriber.

The processed hashed information is sent to the service provider who checks with the hashed information that it has already. If both the information is same then a secure connection is established between them else the service provider rejects the request sent by the mobile user. And this technique is explained clearly with the hashing formulae's. The keys $K_s$ and $K_c$ which are traded off between the subscriber and the service provider produces a hashing variable so called G and it is also called as processed hashed information.

$G = \text{hash}\ (K_s{}^{2 * Rc})$

The above function shows the hashing in the subscriber side and produces a hashed function. Similarly the same is produced in the service provider side and it is shown as,

$G = \text{hash}\ (K_c{}^{2 * Rs})$

After that this value is sent as one time secret word to the service provider and the process is finished if the values of both the hashed function are same. This finishes the authentication procedure and a secure connection can be maintained between both of them.

The above diagram gives a clear view of the one-time hashing secret word methodology. In the above diagram S denotes the hash (secret word) that is password and the random number Rs is the exponential number generated by the service provider for the subscriber. Similarly the random number Rc is the exponential number generated by the subscriber for the service provider along with a hashed key value of the random number and similarly it is received from the service provider also.

## Results and Discussions

The implementation part of this paper is done with network simulator version 2. Initially three nodes were created. In that three nodes the first one acts as a subscriber module and the next one act as a service provider and the final node acts as a database server where the information about the subscribers is held there. Once the subscriber requests for the connection to the service provider, the node 3 is used there for connection establishment with the requested service provider. The hash algorithm used in this authentication procedure is the Secure Hash Algorithm version-1 (SHA-1) [4] which intakes the input message of length maximum of less than $2^{64}$bits and produces an output of 160 bit message digest which is more sufficient for this kind of authentication scheme. The possibility of intrusion is least possible because cracking of 160 bit message digest which is impossible and takes several years to break it. Hence this authentication scheme is most needed for the market.

## Conclusion

By this methodology the security levels in the fourth generation telecommunication networks can be protected from any kind of intrusion that is made during the one time password entering time. This kind of attacks can be eliminated by this one time hashing secret word methodology. This method provides the advantages of very simple use for the service providers as well as users. The users can get better connectivity even though they are in the case of roaming. It provides a good user friendly interface, which were not available in any kind of existing models and this makes the added advantage for this method of protection. The makes this method eases use. Under the future circumstances computation time that takes place in this methodology can be reduced.

## References

[1]. Dake He et al, "User authentication scheme based on self-certified public key for next generation wireless network" in IEEE wireless magazine.

[2]. Raphael Pan et al, "Providing security in 4G systems and unveiling the challenges" in IEEE journal.

[3]. Tamal Dhar et al, "A novel password based mutual authentication technique for 4G mobile communications", in IJRET 2013.

[4]. "Cryptography and network security-principles and practices" by Williams Stallings, third edition.

[5]. Richard Duncan, "An overview of different authentication methods and protocols" by SANS institute.

[6]. Xiaoyan yang et al, "Application study on public key cryptography in mobile payment" in WSEAS international conference on information security.

[7]. Ndibanjebruce et al, "A secure authentication protocol among mobile phone and wireless sensor networks" in ICACT 2013.

[8]. Anastasios N. Bikos et al, "LTE/SAE security issues on 4G wireless networks" in IEEE 2013.

[9]. Kelley R. Klepzig, "Modelling and simulation of public key infrastructure applications" in SANS institute.

[10]. Maude ma, "Security investigation in 4G LTE wireless networks" in IEEE 2013.

[11]. Qian Wang et al, "Time valid one-time signature for time-critical multicast data authentication" in IEEE infocom 2009.

[12]. Hilda C.P et al, "Basic model of multicast authentication based on batch signature- MABS" in IJCSI volume 2 2013.

[13]. A. Diaz et al, "Modelling and simulation of wireless sensor networks" in Spanish MICCIN.