ROBUST SECURITY OF GSM NETWORKS BASED
UPON THE CERTIFICATE-LESS AUTHENTICATION
MODEL

Staffy Jain\textsuperscript{#1}, Amitabh Sharma\textsuperscript{#2}
\textsuperscript{#1}, Student, Department of Information Technology, Chandigarh Engineering College, Landran, Mohali, 140307, INDIA, 9646685580. 
\textsuperscript{#2}, Professor, Department of Information Technology, Chandigarh Engineering College, Landran, Mohali, 140307, INDIA, 8872014307.

ABSTRACT:
The cellular networks are on the rise since many years. The cellular networks have gained the millions of users every year, which means the higher order bandwidth becomes the requirement of the networks for the transmission of the data of millions of users from one region to another region. In this model, security mechanism has been proposed for the privacy protection of the GSM networks. The major GSM networks are considered in the second generation and third generations. Also the fourth generation of the GSM network is emerging rapidly and capable of handling the higher number of users on one point of time. The proposed model is defined with the certificate less cryptography which utilizes the public key based cryptography for the implementation of the extra layer of security among the network nodes. The proposed will be analyzed by using the performance measures associated with the network performance and security measures. The proposed model is expected to solve the problems associated with the existing models.

Key words: GSM, certificate-less public key cryptography. Security,2G, 3G.

Corresponding Author: Staffy Jain

INTRODUCTION:
In large metropolis cities, where multiple people travel with various types of vehicles can visualize the whole enviornment with a small handled wireless device called cellphone. Hence, imagine a scineario in which every person can get to know about every buildings, street, highway and shopping mall that is in there way to enroute the destination, on other hand they can track the vehicles that may come in there way to avoid accidents. To make it possible the next generation of wireless system is here which may defined as intelligent wireless system termed as GSM, which focus on user-personalized service which lead to make it being highly intelligent , and satisfy the vision of virtual navigation. The worldwide research organization and industries
like Motorola, Nokia, Ericsson, WWRF, ITU, IEEE, Docomo, Mobile VCE and 4GW-PCC these all are set to launch wireless system to the commercial market initially in 2010[1,2].

The evolution of network system are started in early 1970's, when the design of analog-voice-oriented First Generation(1G) system began. Conversion of the digital voice and data-oriented second generation(2G) systems in 1991 initiated the beginning of a multi-service platform from the previous mono-service era. Eventhough in various multiple global location system the low bit-rate data and the mono-media system like GSM, CDMA one, IS-95 and TDMA still exist. The meanwhile step between 2G and 3G is 2.5G systems like(GPRS), provide various pros like enhanced channel capacity, higher data rate and throughput and optimized data packet transmission sped up the internet access via various wireless devices. The inception of truly multimedia era[3] is begin by the commercialized transition to 3G system in 2002 where frequent person-to-machine interactions are happen as compare to person-to-person interactions. CDMA 2000 and WCDMA provide high channel capacity, broadband data up to 2 Mbps, high speed multimedia transmission and global roaming across a cellular network.
The span lead to the birth of fully-fledged huge revenue generating multimedia internet applications and e-commerce. As mobile users are increase day by day worldwide and the use of facilities like completely user-centric services, high speed streaming internet, multimedia services (telemedicine, tele-geoprocessing, virtual navigation and VoIP), seamless global roaming with ubiquitous coverage and unhampered QoS support, are increases which lead the 3G systems to increase their bandwidth availability, spectrum allocation, air interference standards and lack of seamless transport mechanisms between different networks. The situation get more difficult for 3G systems, because of various short range communication like WLAN, Bluetooth and HIPERLAN as well as broadcast communication systems which have different features neglect their merits and demerits targeting in increase in users and and provide many service [4].

An all inclusive structure ought to be generated to encoprate the current heterogenous wired and remote framework being used to debase the restrictions and disadvantage. This IPv6-based potential GSM framework, commonly described as MAGIC [5,6] (Mobile multimedia, anytime

**Figure 3**: The paired-key authentication model

**Figure 4**: The 4G cellular security architecture in general

---

©2016 RS Publication, rspublicationhouse@gmail.com
anywhere access, Global mobility support, Integrated wireless solution and Customized personal service), is beneficial service that handle the limitations of 3G systems. So, work on the multiple diverse networks appropriate solution is required which can relocating to the GSM environment satisfying the plenty of cutting edge dream perceptions on actualizing a straightforward open remote engineering (OWA), ought to be critically designed[7,8]. This clearly welcomes new difficulties on each progression and analysts overall face a tough errand of planning reasonable arrangements. Figure 4, shows such a GSM vision.

LITERATURE REVIEW:

1. Alezabi, Kamal Ali, et. al. have proposed an Efficient EPS-AKA protocol (EEPS-AKA). The proposed protocol is based on the Simple Password Exponential Key Exchange (SPEKE) protocol. They compared their method and found their method is fast than other, because of using secret key method that performs faster than certificate-based methods. In addition, they have reduces the size of messages exchanged between User Equipment (UE) and Home Subscriber Server (HSS), with the help of which the authentication delay and storage overhead effectively is reduced.

2. N. Suganthi, V. Sumathy, “they have proposed the algorithm that support three types of keys for each sensor node, first one is single key shared with the base station, second is pair wise key shared with neighbor sensor node, and third is group key that is shared by all the nodes in the network. They have used energy efficient mechanism to update the key and decreased the association of the base station. Polynomial function is used in the study”

3. Zongwei Zhou et. al. proposed “they proposed Key it Simple and Secure (KISS) algorithm. In their paper new key management architecture is given, called KISS, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. The function of KISS is to save the entire life cycle of cryptographic keys. KISS have responsibility that only authenticated user can use the key. For this authenticated commands is send by administrator to KISS and verify system output. KISS have sufficient hardware and trusted which protects the system from malware attacks and insider attacks.”

4. Ivan Damgård et. al. proposed “A secure key management method for cloud environments., authors have proposed a higher security light-weighted protocol, and report on their practical performance. They have taken a servers that control amongst online and disconnected periods without speaking with anybody from outside the cloud, and semi-self-governing servers that need a constrained sort of help from outside the cloud while doing the move. "

PROBLEM FORMULATION:
The basic problem is being addressed under this research is the fake of false base stations, which are used hack into the GSM networks. The fake base stations usually hacks the multiple channels of the cellular base stations, which reduces the available bandwidth. The fake base station attacks collectively belong to the snooping and resource hijacking categories of the hacking methods. The existing system is using the public key cryptography technique to mitigate the threat of fake base stations. In the existing research, the authors have proposed the design and implementation of a new authentication scheme by using certificate-less public key cryptography (CL-PKC) over the GSM system was attempted to miss some system detail. The existing algorithm offers the secure GSM system using the security mechanism with public key cryptography with a focus in the CL-PKC, which is a simple, useful and robust security scheme designed and implemented.
over GSM. Existing security solution has solved the GSM problem in A3 algorithm such as eavesdropping and this problem solved by CL-PKC because of its robustness against this type of attack by providing mutual authentication make the system more secure. The existing solution is able to check the fake base station during its attempt to become the transceiver station neighbor of the GSM station. But it is not capable of checking the fake base station duplicate entries, connections or channels. In case a hacking attempt has taken on one of the existing GSM BTS, and also the cryptographic key details has also been hacked. The hacker would be then capable of creating a transceiver communication channel with the neighbor GSM station, hence becomes able to perform the snooping as well as reduce the availability of bandwidth of the GSM station for its real users. To take on this problem, the security mechanism has to be fool proof and adaptive, so that after hacking a single node and cryptographic keys table, the hackers can be prevented from creating more fake BTS channel from the hacked node or other fake BTS nodes under their control.

CONCLUSION:
The GSM networks are adding the million of the users every year, which are registered to receive the variety of services over the GSM networks. The GSM security is considered very important in order to protect the privacy and integrity of the data among the networks. The GSM network is primarily considered as the infrastructured networks, where the base transceiver station (BTS) based infrastructure is utilized for the realization of the connectivity. Hence the security mechanisms are applied over the BTS nodes, which monitor and establish the authentication over the client nodes, whenever they launch the network nodes. The proposed model is intended to improve the level of security by the means of the authentication and data protection. The proposed model can improve the security of the GSM network by using the certificate less security, which may work among the infrastructure networks for the higher level of security.

REFERENCES: