Implementation of Location based Encryption in GSM Cellular Network using OPNET

Vijay S. More[1], Uma R. Godase[2]

[1]University of Pune, Sinhgad College of Engineering,
Vadgaon, Pune, India

[2]University of Pune, Sinhgad College of Engineering,
Vadgaon, Pune, India

Abstract: ***The "location-based encryption" is a security algorithm that limits the access or decryption of information content to specified locations and/or times. This algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security to exist stack. GSM is chosen as a case study to implement geo-encryption in its key generation part due to its many properties that are beneficial to this protocol. GSM's BTSs are distributed across the network and their signal can reach places like urban canyons and indoor environments inside the network. In GSM, data stream between mobile subscriber (MS) and BTS is encrypted by A5 encryption algorithm. A5's encryption and decryption key (kc) is generated base on MS's SIM card parameter (ki) and a random number, RAND. At this project we have used MS's location information to generate this key by location based encryption algorithm idea. Encrypted data only in the MS's location, that just GSM network is aware of it, can be decrypted and its accuracy depends on used positioning algorithm.***

Keywords: BTS, MS, PVT, IMSI, HLR, SIM, SRES, AUC, BSC, CGI, LAI, MCC, MNC, LAC, MSC, VLR

1. Introduction

Security is important issue in GSM Cellular Network. Inserting an additional layer of security to the standard security stack that provides assurance that the secure content can only be used at authorized (desired) location and time is the main concept of geo-encryption. The term "location-based encryption" or "Geo-encryption" is used to refer to any method of encryption wherein the cipher text can only be decrypted at a specified location. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext.

A guiding principle behind the development of cryptographic systems has been that security should not depend on keeping the algorithms secret, only the keys. This does not mean that the algorithms must be made public, only that they be designed to withstand attack under the assumption that the adversary knows them. Security is then achieved by encoding the secrets in the keys, designing the algorithm so that the best attack requires an exhaustive search of the key space.

Making key depended on target geographic position is an applicable way to strengthen its safety in the real-time applications. The device performing the decryption determines its location using some sort of location sensor, for example, a GPS receiver or some other satellite or radio frequency positioning system such as MS's positioning in GSM. GSM is chosen as a case study to implement geo-encryption due to its any properties that are beneficial to this protocol. GSM Base Transceiver Stations (BTS) are distributed across network and properly cover the area and their high power signal can reach places like urban canyons and indoor environments.

In order to function, serving MS and route calls, this technology requires the service provider to know the cell in which a MS is present. This gives service providers a record of the location and movement of each device, and probably its owner. Report presents a new location dependent key generation management mechanism, and its applicability in GSM is evaluated. For this we use "Cell ID, Sector ID and TA" positioning method to calculate MS's location. The structure of this paper is as follows. At first describes how the geo-encryption is built on conventional cryptographic algorithms and protocols and provides an additional layer of security. The paper then discusses the properties of GSM and its security structure. It then provides a discussion of MS positioning and its implementation on GSM. Finally a new method will be presented to key generation and evaluates its implementation.

2. Geographic Encryption

The idea of Geo-encryption and its use in digital film distribution was proposed and developed by Logan Scott, Dr. Dorothy Denning. They have mentioned a new solution for securing digital films by using geographical information to generate an additional security key, a "Geolock", that is necessary to access the encrypted data or application. These files are sent through a public network and are accessible inside the broadcasting area but only at an especial place can be decrypted At Geo-encryption, on the originating (encrypting) side, a Geo-lock is computed based on the intended recipient's Position, Velocity, and Time (PVT) block. The PVT block defines where the recipient needs to be in terms of position, velocity & time for decryption to be successful. The Geo-lock is then XORed with the session key (Key_S) to form a Geolocked session key. The result is then encrypted using an asymmetric algorithm and conveyed to the recipient. On the recipient (decryption) side, Geo-locks are computed using an Anti Spoof GPS receiver for PVT input into the PVT Geo-lock mapping function. If the PVT values are correct, then the resultant Geo-Lock will XOR with the Geo-Locked key to provide the correct session key (Key_S)

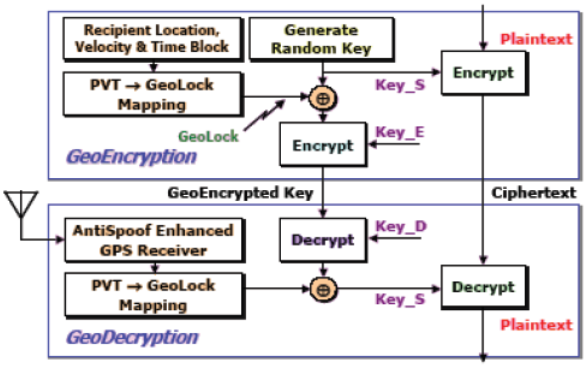

Figure 1: Geographical encryption structure

Figure shows a PVT Geo-lock mapping function where latitude, longitude and time constitute the inputs. Here, a regular grid of latitude, longitude and time values has been created, each with an associated Geo-lock value.

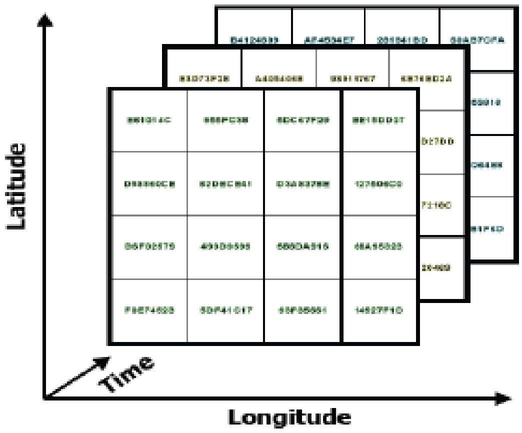

Figure 2: PVT→Geo-lock mapping function

Finally, for increasing the security, the PVT Geo-lock mapping function itself may incorporate a hash function or one way function with cryptographic aspects in order to hinder using the Geo-lock to obtain PVT block values.

3 Global System for Mobile Communication

3.1 GSM Security Structure

Security structure of GSM is based on Ki –individual subscriber authentication key- a unique 128 bit code assigned to each IMSI that permanently is stored in HLR and SIM card. This code is used to generate sign response –SRES- for authentication process and encryption key-Kc. In GSM, authentication process is performed by a challenge and response mechanism. In response to each authentication request, AUC generates a random sequence - RAND- that with Ki are used as inputs to A3 and A8 algorithms to provide SRES and Kc keys. A5 algorithm is used for encrypting data in each frame, while Kc is constant during conversation the frame number is changed regularly. Encryption process is applied only between BTS and MS, and its session key-Kc, is used until another authentication process that might take days.

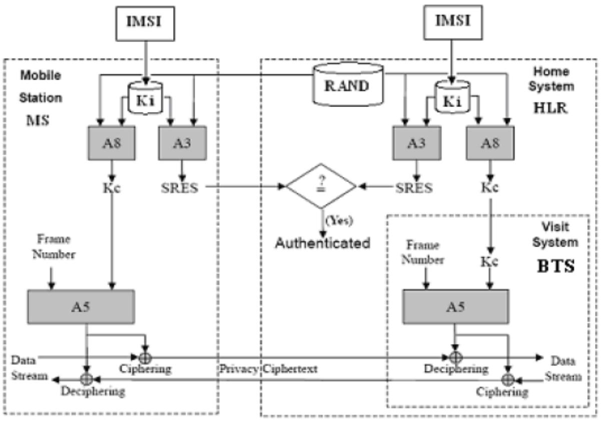

Figure 3: GSM security structure

3.2 Analyzing GSM Cryptography

Basically GSM encryption structure is based on authentication and its security has some challenges:

- Kc is produced based on Ki and if somebody extracts Ki from a SIM card (SIM cloning attack) and achieves RAND number which is sent clearly from BSC to BTS, he/she will be able to calculate Kc by A8 algorithm.
- The data stream only is encrypted between BTS and MS but at internal parts of GSM network especially between BSC and BTS that are connected together via radio links, there isn't any ciphering process.
- Kc is made to each conversation and is constant during it. Accordingly, producing KC based on Ki is the main security vulnerability of GSM (forging Ki under SIM cloning attack) that threats its safety.

4 Proposed GSM Security Structure

4.1 Mobile Station Position in GSM:

In the GSM, Cell Global Identity-CGI- indicates MS location and is stored at the HLR. CGI (32 bit) consists of Location Area Identifier (LAI) and Cell ID:

CGI=LAI + Cell ID
LAI=MCC+MNC+LAC

Coverage area of each MSC/VLR has a unique LAI code that indicates Mobile Country Code (MCC), Mobile Network Code (MNC), and Local Area Code (LAC). Each MSC is divided into several subareas- BSC- (with a unique LAC). BSC area is consisting of some BTS (each BTS has a unique Cell- ID) and depends on its designing and the number of antenna, each BTS maybe has several sectors (1 up to 6 sectors and Sector-ID).

BTS broadcasts LAI and its Cell-ID so that all MS under its coverage can receive them. MS's location information is updated by Location-Update (LU) process in any call setup, entering new MSC/VLR and regularly in the idle mode. In order to avoid excessive signaling traffic, as long as the MS is in idle mode, the network knows only the LAI. The network becomes aware of the Cell-ID only when the MS switch into dedicated mode, namely when the channel is used to actually establish a call. In contrast, the MS always knows the Cell-ID of the cell it is in. Selecting a BTS sector for connecting is based on the MS's location and the strength of received signal.

Unfortunately, the GSM Network itself lacks positioning functionality since historically it was not designed to carry any location or telemetry information. But several MS positioning techniques have been developed and tested with good results but in the most of them the GSM network should be changed and needs to be added some additional parts and so a huge costs. For example in several methods which - In the Assisted-GPS (A-GPS) method each MS and BTS are equipped with a GPS receiver and calculate their position by GPS technology.

The simplest way to describe the location of a MS that doesn't need to change the network is Cell ID+ Sector ID+ TA. It doesn't have accuracy as same as other methods but has lower implementation cost so that's service provider have chosen this method owing to its simplicity and cost.

4.2 Location Based positioning method

Cell ID+ TA positioning method uses Cell ID, Sector ID of corresponding BTS and Timing Advance (TA). TA is a crude measurement of the time required for the signal to travel from the MS to the BTS. In the GSM system, where each MS is allocated a specific frequency and time slot to send and receive data, this measurement is essential to make sure that time slot management is handled correctly and that the data bursts from the MS arrive at the BTS at the correct time (in the time slot allocated to them). The computed TA value is then used by the MS to advance transmission bursts so that the data arrives at the correct time slot. The resolution is one GSM bit, which has the duration of 3.69 microseconds. Since this value is a measure of the round trip delay from the MS to the BTS, half the way would be 1.85 microseconds, which at the speed of light would be approximately equal to 553 meters.

$$1.845\ \mu s \times 3 \times 108\ m / s = 553\ m$$

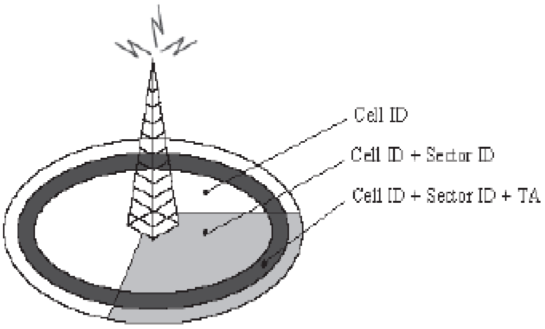

Figure 4: Cell ID+ Sector ID+TA positioning

The accuracy of this method depends on the cell's size, and the number of cell's sectors. Since the typical GSM cell is anywhere between 2 km to 20 km in diameter, therefore reducing the cell diameter or increasing the number of sectors can enhance its accuracy.

4.3 Proposed Method

By using MS position parameters they try to limit decrypting possibility to a dedicated area. At this project, AUC uses MS position as a Mobile Station Position (MSP) code that consists of CGI code (LAI and Cell ID), Sector ID and TA amount to generate KC. CGI and Sector ID are broadcasted by BTS but TA is dedicated for a MS isn't constant and will changed by MS movement.

MSP=CGI+ Sector ID+ TA

MSP consists of 64 bit: first 32 bit for CGI, 8 bit for Sector ID (33th- 40th), 8 bits show TA (41th- 48th) and the rest are assigned to zero (16 bit padding to achieve equal length to Kc).

At the proposed structure, when MS requests to be authenticated, AUC products Kc by using A8 (Ki and RAND as inputs) and then XOR it to MSP. The result is K'C:

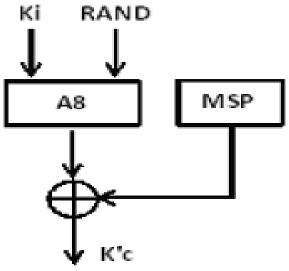

Figure 5: K'c Production

KC = A8(RAND , Ki)
K'C = KC XOR MSP

AUC generates five triple sets of {RAND, SRES, K'C} and sends them to HLR, BTS and MS. BTS uses K'C to encrypt and decrypt data.

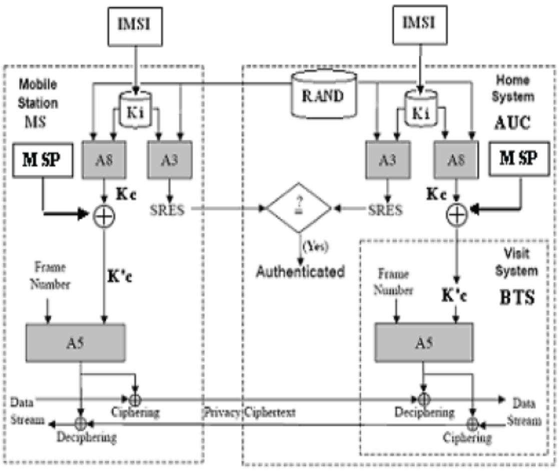

Figure 6: Proposed structure of GSM

In the other side, MS produces Kc by using RAND and Ki. It receives Cell ID and Sector ID from BTS and calculates TA for computing MSP, then XOR it with KC to compute K'c. By this method the encrypted data code can be decrypted just at MS position (at least in the TA area) with same MSP. The security of a key comes from the amount of entropy of the information that generates the key. In this case, CGI and Sector ID are both known, for this the entropy of MSP comes from TA (8 bits in the maximum distance case: 0 ≤TA≤63). Therefore this entropy is embedded into K'c as additional security by XORing MSP to Kc. Similarly, the secrecy of K'c same as Kc comes from Ki and MSP just generates additional security followed by MS's mobility. Base on Information Theory the minimum entropy of x is: rest is assigned to zero (16 bits padding to achieve Kc's length-64 bit). At the proposed structure, when MS requests to be authenticated, AUC products Kc by using A8 (Ki and RAND as inputs) and then XORs it with MSP.

5 Simulation

To obtain the network performance based on simulation, OPNET Modeler 14.5 has been used to implement different scenarios. We have used student version of OPNET Modeler 14.5. This tool has well defined user interface and a rich set of modules where users can efficiently create suitable simulation environments by dragging the needed objects modules. Different types of technologies can be used from start up wizard of OPNET Modeler

5.1 Performance Metrics

In order to evaluate performance of voice transmission over networks, we consider the following QoS parameters:

- Packet loss
- End to end delay
- Packet delay variation
- Throughput
- Jitter

Packet losses affect the quality of received voice data. As such, to evaluate the performance of the voice quality of service, we have taken this metric into account. End to end delay and packet delay variation also has a great impact on voice quality. If these delays increase, then the quality of received voice degrades. We have selected these delays as metrics to measure the performance of voice quality of service. Throughput is another important parameter to measure the data rates of communication in the network. In our case, we choose throughput to measure the data rates for voice transmission in GSM network. Jitter is another key parameter of QoS in voice conferencing. We consider this parameter to measure the variation of the packet latency in voice conferencing.

5.2 Simulation Model Design

We design simulation model to evaluate the performance of the QoS for voice transmission in GSM network. We create two scenarios to evaluate the performance of QoS. We implemented two scenarios. First is without location based encryption and the other scenario is with location based encryption. In both scenarios, we consider few GSM nodes that are suitable for voice GSM network. The salient characteristics of these nodes are that these nodes can support client server application and serve packets on a First-Come-First- Serve (FCFS) basis. In both scenarios, we consider two mobile stations namely UE and Attacker UE which are used for Voice application.

5.3 Attributes of the Designing Network Model

Different network elements have been used to create the network in order to fulfill the requirements of our scenarios. We have used following entities to create the network.

- Application Definition
- Profile Definition
- Umts_wkstn_adv
- Umts_Node_b_3sector_adv
- Umts_rnc_ethernet_atm_slip
- Umts_sgsn_ethernet_atm_slip9_adv
- Umts_ggsn_slip8
- ethernet4-slip8_gtwy
- Ethernet_server_adv
- 10BaseT

The above network elements have been used to create the scenarios based on intended requirement.

5.4 GSM Performance Evaluation

The objective of this scenario studies the performance of GSM network using the Voice application and the GSM quality speech. Many node models as part of the GSM specialized model library are grouped in the GSM and GSM_advanced object palettes in OPNET modulator such as routers, repeaters, stations, RNC, etc,. In our simulation, the GSM advanced node models were used. The architecture of this model can be found in simple and advance nodes. The MN model offers functionality related to terminal equipment and mobile termination, responsible for terminating the radio link. The UTRAN part consists of models for BTS and BSC. During this case study, a simulation scenario was built and run in order to obtain the desired results to achieve the objective. Figure displays the network topology of this case. The proposed topology of mobile network model consists of BTS, BSC, MN, and MSC/Gateway MSC nodes. The coverage of one cell is approximately 5km by 5km of area.

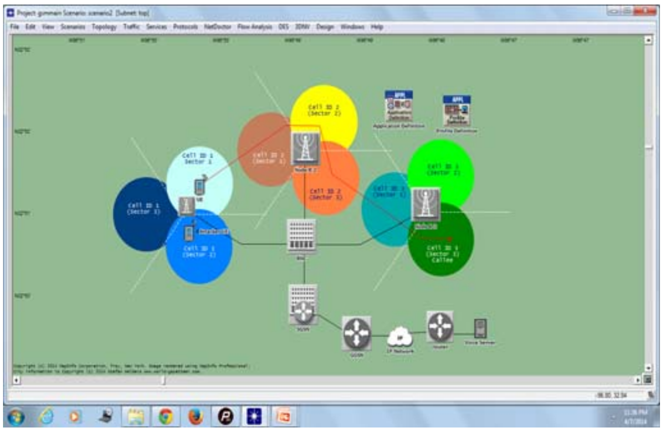

Figure 7: GSM Prototype

5.5 External System Definitions (ESD)

The ESD specifies the number and attributes of external system interfaces. Through the defined esys interfaces the external system can communicate with the co-simulation code implemented in the OM. There is the External System Editor in the OPNET Modeler that gives a way to build and edit the ESD model. The first ESD attribute that has to be defined is the esys interface name. It can be used to refer to the interface during co-simulation. The next attribute is a data type which defines the type of data that are transferred over the esys interface. One esys interface can handle only one selected data type, so it is very important to define right data type for both direction of co-simulation. Most of data type available in the OPNET Modeler responds to the C/C++ data types.

The ESD specifies the number and attributes of external system interfaces. Through the defined esys interfaces the external system can communicate with the co-simulation code implemented in the OM. There is the External System Editor in the OPNET Modeler that gives a way to build and edit the ESD model. The first ESD attribute that has to be defined is the esys interface name. It can be used to refer to the interface during co-simulation. The next attribute is a data type which defines the type of data that are transferred over the esys interface. One esys interface can handle only one selected data type, so it is very important to define right data type for both direction of co-simulation. Most of data type available in the OPNET Modeler responds to the C/C++ data types.

5.6 External System Interface

The esys interface is the only physical component in the OM which represents the communication instrument with the external system. The esys interface is a process module and thanks to this it can be implemented into a model structure of any network device along other processes where it is exactly needed. The properties of the esys interface process module are defined by the associated ESD module. Only esys interfaces specified in this way can be used for communication with the external system. Inside of the esys process module process model (algorithm) is created. The main task of this algorithm is to interact with the external system. The structure and setting of this process model (inner logic) reflect the way how the OM executes the information exchange with the external system. A variety of kernel procedures let you control data transmission as well as data transformation between the OPNET Modeler and external system.

Although the data transformations needed depend on specific circumstances, it will be often needed to transform objects (such as packets) to a form usable in the external system's domain. Conversely, it will be needed to take values received from the external system and convert them back into objects that Modeler can use. There are general mechanisms that can assist you with these conversions. For example, application of value vectors that are essentially arrays with a variable number of elements, directly to the esys interfaces.

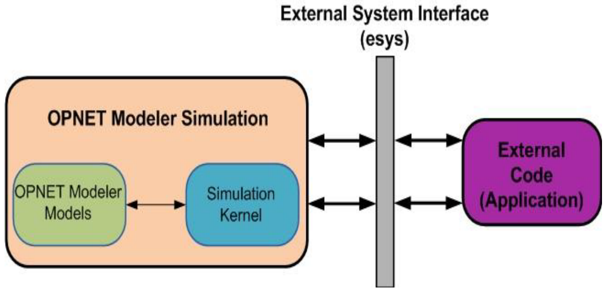

Figure 8: Basic co-simulation scheme in OPNET Modeler environment

5.7 Configuration of Simulation Descriptor

This file contains a information for the co-simulation builder and linker. Structure of this file is strictly defined. All definitions must be wrapped in the block starting with a start_definition and ending with a end_definition.

```
start_definition
                platform: windows
                use_esa_main: yes
               kernel: development
bitness: 32bit
           dll_lib: esys_udp_conn.dll
end_definition
```

We run the co-simulation under 32-bit Microsoft Windows operating system. We use the OM Debugger Console for debugging the simulation, so we need a development kernel. In our case, the OM side should be “in charge”. Setting use_esa_main on yes means that we use the external dynamic loaded library (DLL file) in the OM simulation. The co-simulation is started from the OM GUI like common simulations. With use_esa_main set on yes, we need to define a name of the DLL file with the external code. This name is a parameter of item dll_lib.

6 Simulation Results

The simulation results obtained for application under the three scenarios are outlined below. The global statistics collected for voice. The object statistics collected follow.

6.1 Voice: Time Average in End-to-End Delay

As can be observed, the time taken for packets to be transmitted from the source to the destination, or the End-to-End delay was found average out to approximately 1 second under scenario 1, and approximately 1 second under scenario 2 at start. Real time applications such as voice require the ETE to be as low as possible to provide for a seamless and more natural conversation to take place, therefore it is concluded that the both algorithm are better to use for voice communication. Table summarizes the approximate End-to-End Delay observed from Figure 8.7

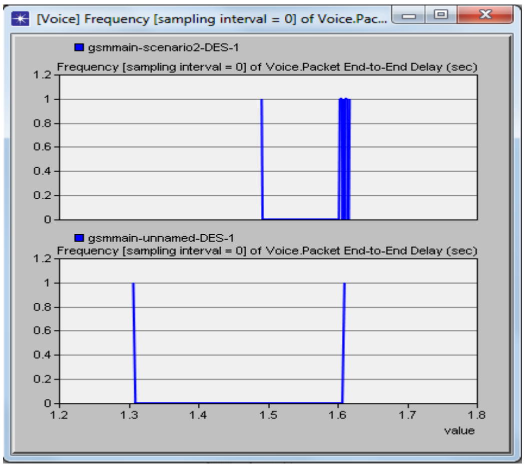

Figure 8: Voice: Time Average in End-to-End Delay

6.2 Voice: Jitter

Jitter, or the variation in the ETE delay, was expected to be the highest. As packets are placed into the two network of different algorithm; the ETE delay in the transmission of the packets from the source to the destination was expected to vary depending on the position of the packets in the queue.

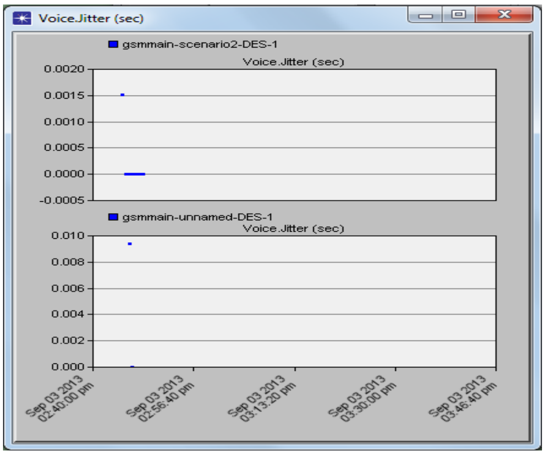

Figure 9: Jitter

6.3 Voice: Packet Delay Variation

As discussed in the background section, Packet Delay Variation is a measure of the difference in the End-to-End delay between packets in a flow while ignoring any packets that have been lost. Both scenarios showed a nearly constant PDV of approximately 0.10 s.

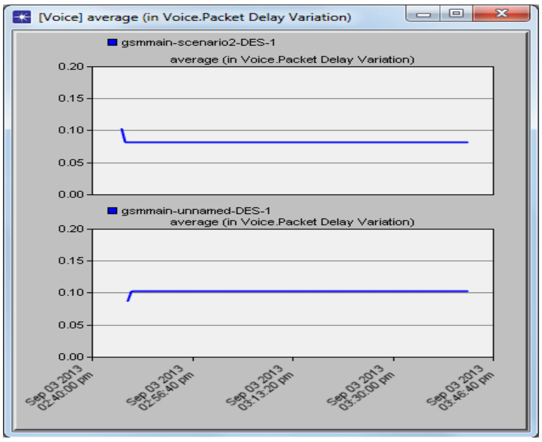

Figure 10: Packet Delay Variation

6.4 Voice: Traffic Sent

As can be observed in Figure, the time average in voice traffic that was initially sent is different for both scenarios.

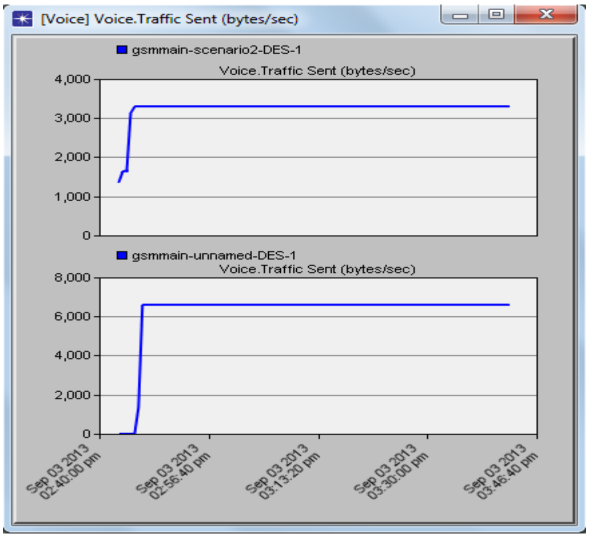

Figure 11: Traffic Sent

6.5 Voice: Traffic Received

The time average in the voice traffic that was received after the packets had been sent through the two different scenarios is shown in Figure. The results obtained show that the traffic received under scenario 1 was the less than scenario 2. This is especially important for voice applications as any loss would adversely affect the overall quality of the voice signal.

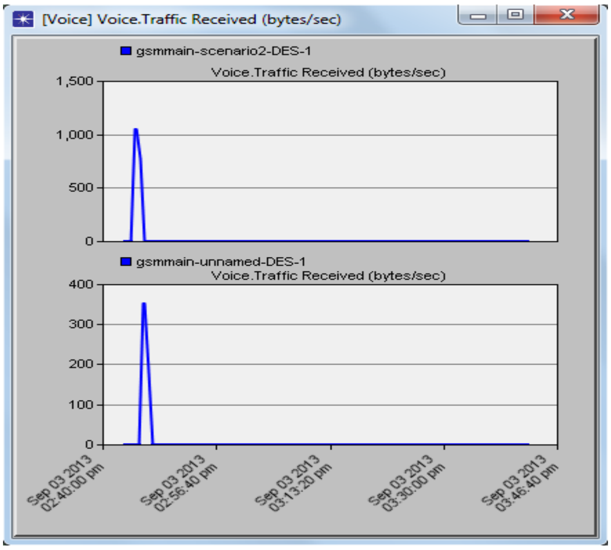

Figure 12: Traffic Received

6.6 Voice: Traffic Received in scenario 1

The time average in the voice traffic that was received after the packets had been sent through the two different mobile stations is shown in Figure. The results obtained show that the traffic received under scenario 1 is same for both mobile stations. Attacker using simcloning attack. Voice signal received by both mobile stations is same.

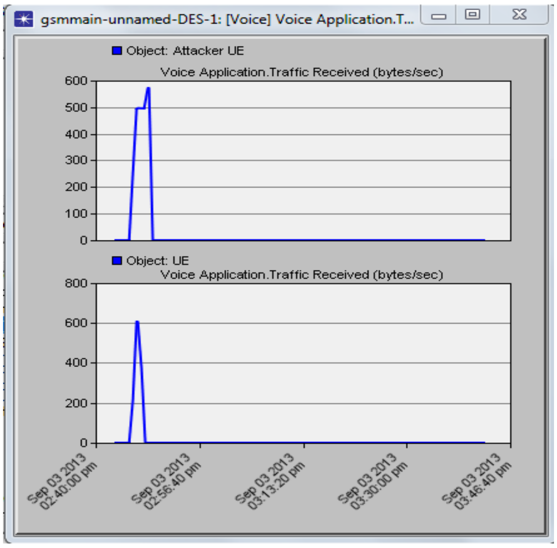

Figure 13: Traffic received by workstations

6.7 Voice: Traffic Received in scenario 2

The time average in the voice traffic that was received after the packets had been sent through the two different mobile stations is shown in Figure. The results obtained show that the traffic received under scenario 2 is different for both mobile station,. Attacker mobile station cant received any data due to location based encryption algorithm. Attacker using simcloning attack. Voice signal received by both mobile stations is different.

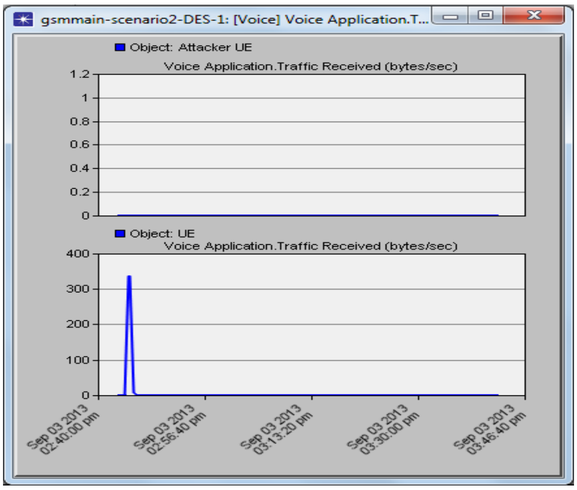

Figure 14: Traffic received by workstations

6.8 Comparison of result:

Table 1: Result Comparison

Application	*Statistic Collected*	*Scenario 1*	*Scenario 2*
Voice	End-To-End Delay	1 s	1 s
	Jitter	0.009 s	0.0016 s
	Packet Delay Variation	0.10 s	0.10 s
	Traffic Sent	6000 B	6000 B
	Traffic Received	350 B	1000 B
	Traffic Received by Attacker	600 B	0 B

7 Conclusion

Using Location Based Encryption in the stationary mode has same effectiveness but the encryption's key safety by being referred to MS location, becomes better. Statistically about 80% of mobile conversations are established in the stationary mode and the proposed method leads to a more strength key (with a factor 2-3 in the simulation) at this mode. It is essential to note that in the revealed Ki situation by increasing conversation time the encryption key becomes reveal able. Although in the others modes encryption safety becomes better but because of using an inaccurate positioning method, MS mobility in higher speed not only increase encryption process delay but also decryption fault. In the current GSM the session parameters to encrypt data continuously need to be changed (frame number) while Kc is constant. In the proposed scheme the encryption process need to be changed not only by frame number but also by MS position and mobility speed.

In future work, will concentrate on a better positioning technique to decrease the movement modes failures. When mobile station changing location, it is necessary to register with the new BST. To register with new BST mobile sends registration request to BST. In this registration mobile station sends new location information to BST. Mobile station sending this information over the air without any security. Again this location information is vulnerable. Attacker can catch this information. In future work, we will concentrate on to make registration procedure secure.

References

[1] Logan Scott & Dorothy E. Denning, "Location Based Encryption & Its Role in Digital Cinema Distribution", Proceedings of ION GPS/GNSS 2003, pp 288-297.

[2] Hector C. Weinstock, editor, "Focus on Cognitive Radio Technology", Nova Science Publishers, 2007, p. 87-92.

[3] Yoni De Mulder & Lejla Batina & George Danezis & Bart Preneel, "Identification via Location-Profiling in GSM Networks", Proceedings of the 7th ACM workshop on Privacy in the electronic society, Alexandria, VA, USA, 2008.

[4] D. Qiu & Sherman Lo & Per Enge & Dan Boneh, "Geoencryption Using Loran", Proceeding of ION NTM 2007.

[5] D. Qiu, "Security Analysis of Geoencryption: A Case Study usingLoran", Proceeding of ION GNSS 2007.

[6] Siegmnnd M. Redl & Matthias K. Weber & Malcolm W. Oliphant, "An Introduction to GSM", Artech House Publisher, 1995.

[7] Nokia Corporation, "Nokia mobile system structure", Nokia Telecommunications Oy, SYSTRA, NTC CTXX 1985.

[8] Ramesh Singh & Preeti Bhargava & Samta Kain, "Cell phone cloning: a perspective on GSM security", Ubiquity, Vol. 8, Issue 26, 2007.

[9] Emiliano Trevisani & Andrea Vitaletti, "Cell-ID location technique, limits and benefits: an experimental study.", Proceedings of 6th IEEE workshop on Mobile Computing Systems and Applications, WMCSA 2004.

[10] P. Brida, "Location Technologies for GSM", Transcom, June 2003, Žilina, p. 119-122. ISBN 80-8070-081-8.

[11] Josef Bajada, "Mobile Positioning for Location Dependent Services in GSM Networks", Computer Science Annual Workshop- CSAW, Department of Computer Science and AI, University of Malta, 2003.

[12] Ionescu Mircea & Stanescu Emil & Halunga Simona, "CellID positioning method for virtual tour guides travel services", ECAI 2007 - International Conference – Second Edition, Electronics, Computers and Artificial Intelligen0ce, June 2007, Pitesti, ROMÂNIA

[13] Marc Briceno, Ian Goldberg, David Wagner, An implementation of the GSM A3A8 algorithm, www.gsm-security.net/papers/a3a8.shtml, 1998

[14] http://www.opnet.com

[15] GSM Association, www.gsmworld.com, 2011

Author Profile

More Vijay received the B.E. degrees in Information Technology from University of Pune in 2008. Currently he is pursuing M.E, degree in Information Technology from University of Pune.

Mrs. Uma R. Godase received M.E. degree in Information Technology from University of Pune. Currently she is working as Assistant Professor in Information Technology department of Sinhgad College of Engineering. Her area of interest is Information security.