International Journal of Advanced Scientific Research
ISSN: 2456-0421; Impact Factor: RJIF 5.32
www.allscientificjournal.com
Volume 2; Issue 3; May 2017; Page No. 08-11

Increase a security in GSM SIM card by Geo-location

[1] Lav Narain Nishad, [2] Parul Yadav, [3] Vandana Dubey

[1] Department of Computer Science, Amity University, Lucknow, Uttar Pradesh, India
[2-3] Faculty, Dept. of Computer Science, Amity University, Lucknow, Uttar Pradesh, India

Abstract
The "geo-encryption" or "area based encryption" is a security calculation that constrains the get to or decoding of data substance to indicated areas or potentially times. This calculation does not supplant any of the traditional cryptographic calculations, however rather includes an extra layer of security to exist stack. GSM is picked as a contextual investigation to execute geo-encryption in its key era part because of its numerous properties that are gainful to this convention. GSM's BTSs are appropriated over the system and their flag can achieve places like urban gulches and indoor situations inside the system.
In GSM, information stream between portable endorser (MS) what's more, BTS is scrambled by A5 encryption calculation. A5's encryption and unscrambling key (kc) is created base on MS's SIM card parameter (ki) and an arbitrary number, RAND. In the symmetric figures it's better to utilize transient key rather than steady key for this at this venture we have utilized MS's area data to create this key by geoencryption calculation thought. Scrambled information just in the MS's area that just GSM system knows about it, can be decoded and itsexactness relies on upon utilized situating calculation.

Keywords: geo-encryption, GSM, positioning, ki, kc

1. Introduction
Nowadays application of the smartphones leads to the increasing requirement of SIM cards essentially. In the modern world, everyone have a cell phone device with application for daily necessities through mobile communication devices such as voice communication, short message services, payments etc. Soon after the invention of smartcards based Subscriber Identity Module cards, SIM cards technology are still developing more and more time progresses. These have evolved to smartphones due to the advancement in mobile communication technology and various values added services provided to the user.
Now mobile communication devices are developed to smartphones and used to fulfill users additional requirements such as GPS, GPRS, digital camera, online services (paytm, paypal and mobiwik) etc. Due to the changes in smart devices, changes day to day, SIM cards are also changed with respect to its features such as storage capacity and performance of smart cards. Capacity and performance of smart cards are also improved upto 8k to 512k for good communication, better storage capacity, faster calculation and improve security functions.
Embeddings an extra layer of security to the standard security stack that gives affirmation that the safe substance must be utilized at approved (sought) area what's more, time is the fundamental idea of geo-encryption. The term "area based encryption" or "Geo-encryption" is utilized to allude to any strategy for encryption wherein the figure content must be unscrambled at a predefined area. On the off chance that an endeavor is made to unscramble the information at another area, the unscrambling procedure comes up short and uncovers no data about the plaintext [1].
A controlling guideline behind the improvement of cryptographic frameworks has been that security ought not to rely on upon keeping the calculations mystery, just the keys. This does not imply that the calculations must be made open, just that they be intended to withstand assault under the presumption that the foe knows them. Security is then accomplished by encoding the mysteries in the keys, outlining the calculation so that the best assault requires a comprehensive pursuit of the key space, and utilizing adequately long keys that comprehensive pursuit is infeasible [2].
Making key relied on upon target geographical a property is a viable approach to reinforce its wellbeing in the continuous applications. The gadget playing out the decoding decides its area utilizing some kind of area sensor, for instance, a GPS recipient or a few other satellite or radio recurrence situating framework such as MS's situating in GSM. GSM is picked as a case study to actualize geo-encryption because of its numerous properties that are helpful to this convention. GSM Base Transceiver Stations (BTS) are disseminated crosswise over system furthermore, legitimately cover the range and their powerful flag can achieve places like urban ravines and indoor conditions.
Keeping in mind the end goal to capacity, serving MS and course calls, this innovation requires the specialist organization to know the cell in which a MS is available. These cells are of differing size, from a couple of kilometers in low-thickness regions, to a couple meters inside urban areas. This gives specialist organizations a record of the area and development of every gadget, and presumably its proprietor [3].
In this paper, another area depended encryption key era administration component is presented, and its appropriateness in GSM is assessed. For this we utilize GSM MS's situating strategy Cell ID, Sector ID and TA-to figure MS's area and it is taken an interest in the key era system.
The structure of this paper is as per the following. The paper first depicts how the geo-encryption expands on traditional

cryptographic calculations and conventions and gives an extra layer of security. The paper then examines the properties of GSM and its security structure, which are strong for geo-encryption approach. The paper then gives a talk of MS situating and its execution on GSM.

2. Geo-Encryption

Fundamentally, Geo-encryption expands on built up cryptographic calculations and conventions to fortify it in a way that gives an extra layer of security past that given by regular cryptography. It permits information to be encoded for a particular place or wide geographic region, and backings imperatives in time also as space. It can be utilized with both settled and versatile applications and backings a scope of information sharing and dispersion arrangements [4].

At Geo-encryption, on the beginning (scrambling) side, a Geo-bolt is registered in light of the planned beneficiary's Position, Speed, and Time (PVT) square. The PVT square characterizes where the beneficiary should be in terms of position, speed and time for decoding to be effective. The Geo-bolt is then XORed with the session key (Key_S) to shape a Geo-bolted session key. The result is then encoded utilizing an awry calculation furthermore, passed on to the beneficiary, as is demonstrated the Half breed calculation of figure 1 [1].

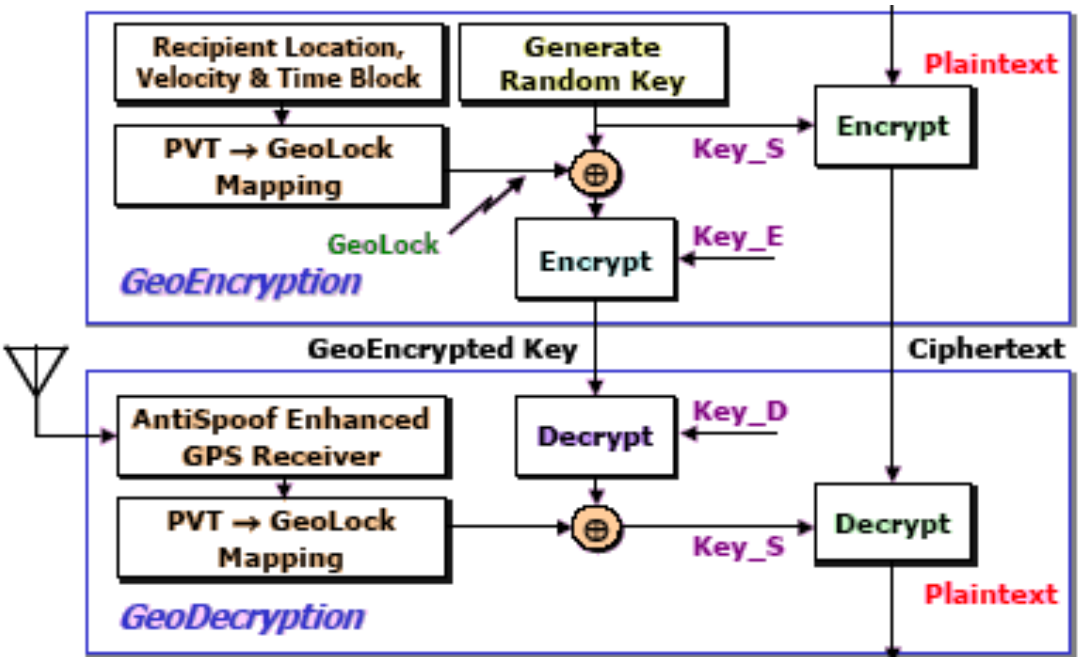

Fig 1: Geo-encryption structure

On the beneficiary (decoding) side, Geo-locks are figured utilizing an AntiSpoof GPS recipient for PVT contribution to the PVT→ Geo-lock mapping capacity. In the event that the PVT qualities are right, then the resultant Geo-Bolt will XOR with the Geo-locked key to give the right session key (Key_S).

At this capacity the separation between networks has coordinate connection to Geo-bolt values and for this the network dividing must consider the exactness of the GPS recipient at the decoding site; generally mistaken Geo-bolt qualities may come about. Utilizing each of scope, longitude, time furthermore, speed as info is rely on upon many-sided quality and exactness of utilization and each of sources of info can be overlooked on the off chance that important.

At long last, to increase the security, the PVT→ Geo-lock mapping capacity itself may fuse a hash capacity or one-path work with cryptographic viewpoints so as to prevent utilizing the Geo-bolt to get PVT square values. Additionally, the calculation might be intentionally moderate what's more, troublesome; maybe in light of settling a troublesome issue [1, 4].

3. GSM Security Structure

Security structure of GSM depends on Ki (128 piece) - singular supporter confirmation key-a one of a kind code allocated to each IMSI1 and for all time is put away in HLR2 and SIM3 card. This code is utilized for creating marked reaction –SRES- in the verification procedure and encryption key-Kc generation [6].

In GSM, verification process is performed by a test and reaction system and for each validation ask for AUC4 produces an irregular succession - RAND-that with Ki are utilized as contributions of A3 also, A8 calculations to give SRES and Kc keys [6, 7].

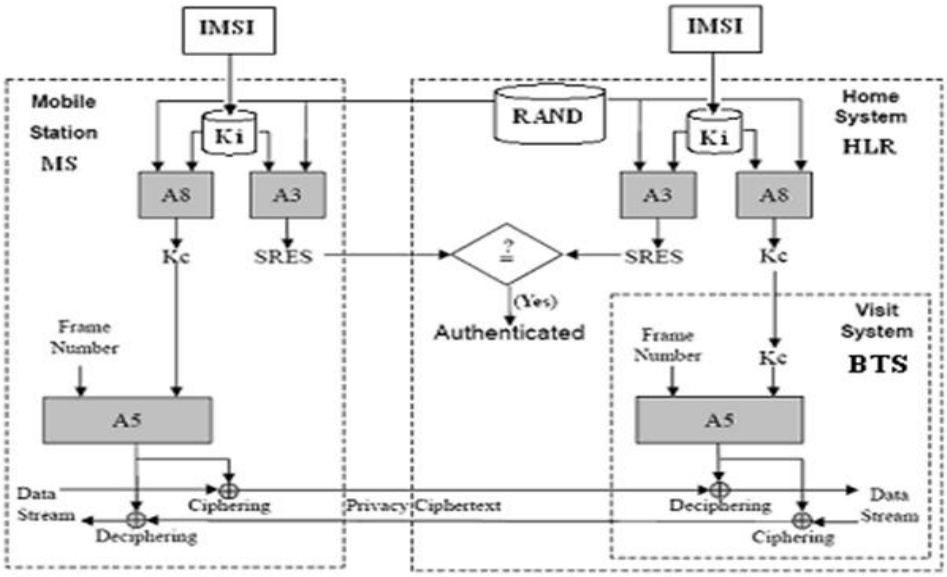

Figure 3. GSM security structure

A5 calculation is utilized for scrambling information and preformed for each casing, while Kc is steady amid discussion the casing number is changed [7]. The encryption process is connected just amongst BTS and MS, what's more, every session key, Kc, would be utilized until the MSC chooses to confirm the MS again which may takes days [8].

3.1 Examining GSM cryptography

Fundamentally GSM cryptography structure depends on confirmation and its security has some weakness for example,

- Kc is created in light of Ki, so if somebody extricates Ki from a SIM card (under SIM cloning assault) and accomplishes RAND number which is sent plainly from BSC to BTS, will have the capacity to compute Kc by A8 calculation.
- The information stream is scrambled just amongst BTS and MS yet at inner parts of GSM particularly between BSC and BTS (for the most part whit radio association joins), there isn't any cyphering procedure.
- Kc is made by every validation procedure what's more, is steady amid each call.

In like manner, Kc creation in light of Ki is the primary security helplessness variable of GSM (manufacturing Ki under SIM cloning assault) that restricts its wellbeing. Utilizing a few different components of GSM to fortify encryption key amid discussion is the primary point of this paper.

4. MS Positioning In GSM

In the GSM, Cell Global Identity-CGI- indicates MS location in the network and is stored at the HLR. CGI (32 bit) indicates 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 is arranged by 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 consists of some BTS (each BTS has a unique ID: 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) [6, 7].

BTS broadcasts LAI and its Cell-ID so that all MS under its coverage can receive these messages. Knowingthe Cell-ID, an MS can approximate its actual location by using the geographical coordinates of the corresponding BTS. 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 [7]. 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 [3]. Selecting a BTS sector for connecting is based on the MS's location and the strength of received signal [6, 7].

Unfortunately, the GSM Network itself lacks positioning functionality since historically it was notdesigned 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 equipped by some additional parts and so a huge costs.

For example in several methods which accurately measure the time difference such that the Time of Arrival (TOA) or Enhanced Observed Time Difference (E-OTD) of wireless radio transmissions there are huge costs involved in upgrading a substantial part of the network's BTSs with Location Measurement Units (LMUs) for calculating the difference of arrival time of signals from BTS by knowing the position of LMU [9]. Or in the Assisted-GPS (A-GPS) method each MS and BTS are equipped with a GPS receiver and calculate their position by GPS technology [9, 10].

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 makes lower implementation cost [11] so that we chose this method for its simplicity and cost.

4.1 Cell ID+ Sector ID+TA 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 mobile station 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) [11]. 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.

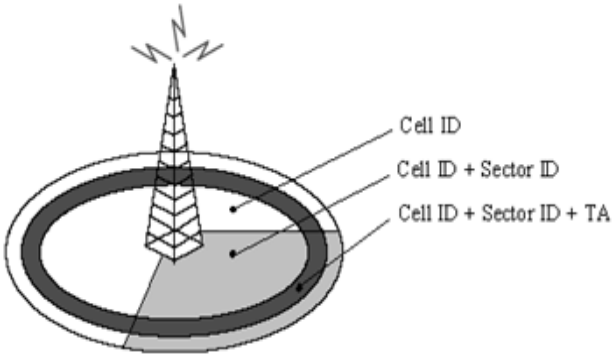

Fig 3: CELL ID + SECTOR ID + TA Positioning

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

5. Conclusion

Utilizing Geo-encryption in the stationary mode has same adequacy however the encryption's key security by being alluded to MS area, turns out to be better. Measurably around 80% of portable discussions are set up in the stationary mode and the proposed strategy prompts a more quality key (with a figure 2-3 the reproduction) at this mode. It is fundamental to note that in the uncovered Ki circumstance by expanding discussion time the encryption key turns out to be more uncover capable.

In spite of the fact that in the others modes, the security of encryption turns out to be better but since of utilizing an off base situating strategy, MS versatility in higher speed not just increment encryption handle delay additionally unscrambling blame.

In the current GSM the session parameters to encode information ceaselessly should be changed (edge number of the plaintext) while Kc is steady. In the proposed conspire the encryption procedure should be changed not just by edge number additionally by MS position and versatility speed. Dissimilar to the current GSM that the encryption key-Kc-is steady amid discussion in the proposed conspire, K'c, changes by MS position and speed.

6. ACKNOWLEGMENT

The authors are thankful to Mr. Aseem Chauhan (Additional President RBEF, Chancellor AUR), Maj. General K. K. Ohri, and AVSM (Retd.) Pro Vice Chancellor, AUUP, Lucknow Campus, Wg. Cdr. Dr. Anil Kumar (Director, ASET) and Prof. (Dr.) Deepak (HOD, Department of CSE, ASET) for their cooperation, motivation and suggestive guidance.

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. Qiu D, Sherman Lo, Per Enge, Dan Boneh. Geoencryption Using Loran. Proceeding of ION NTM, 2007.
5. Qiu D. Security Analysis of Geoencryption: A Case Study using Loran, Proceeding of ION GNSS, 2007.
6. Siegmnnd M Red, 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 2007; 8(26).
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. Brida P. Location Technologies for GSM, Transcom, Žilina, 2003; 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, Cell ID positioning method for virtual tour guides travel services, ECAI 2007 - International Conference – Second Edition, Electronics, Computers and Artificial Intelligence, Pitesti, ROMÂNIA, 2007.