IMPLEMENTING GEO-ENCRYPTION IN GSM CELLULAR NETWORK

Mahdi Daghmechi Firoozjaei[1], **Javad Vahidi**[2]

[1]Mobile Optimization Department
Telecommunication Company of Mazandaran-TCM, Babol, Iran

[2]Iran University of Science and Technology-IUST,
Behshahr, Iran,

Email: [1]mdaghmechi@gmail.com, [2]jvahidi@iust.ac.ir

Abstract

The "geo-encryption" or "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. In the symmetric ciphers its better to use transient key instead of constant key for this at this project we have used MS's location information to generate this key by geo-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: *GSM, Geo-encryption, Kc, Ki, MPC.*

I. INTRODUCTION

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 [1].

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, and using sufficiently long keys that exhaustive search is infeasible [2].

Making key depended on target geographical properties is an effective 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 many 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. These cells are of varying size, from a few kilometers in low-density areas, to a few meters within cities. This gives service providers a record of the location and movement of each device, and probably its owner [3].

In this paper, a new location depended encryption key generation management mechanism is introduced, and its applicability in GSM is evaluated. For this we use GSM MS's positioning method-Cell ID, Sector ID and TA- to calculate MS's location and it is participated in the key generation mechanism.

The structure of this paper is as follows. The paper first describes how the geo-encryption builds 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, which are robust for geo-encryption approach. The paper then provides a discussion of MS positioning and its implementation on GSM.

II. GEO-ENCRYPTION PRINCIPLES

Basically, Geo-encryption builds on established cryptographic algorithms and protocols to strengthen it in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies [4].

The idea of Geo-encryption and its use in digital film distribution was proposed and developed by Logan Scott, Dr. Dorothy Denning, at [1]. At that paper they have mentioned a new solution for securing digital films by using geographical information to generate an additional security key, a “Geo-lock”, 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 [4, 5].

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 Geo-locked session key. The result is then encrypted using an asymmetric algorithm and conveyed to the recipient, as is shown the Hybrid algorithm of figure 1 [1].

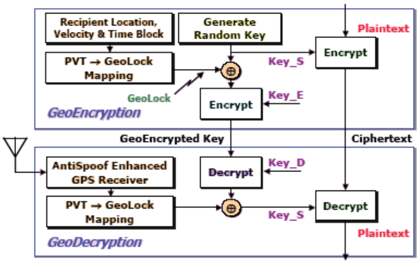

Figure 1. Geo-encryption structure [1]

On the recipient (decryption) side, Geo-locks are computed using an AntiSpoof 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 2 shows a notional diagram of 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 [1].

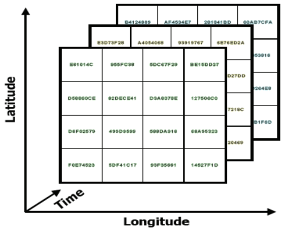

Figure 2. PVT → Geo-lock mapping function [1]

At this function the distance between grids has direct relation to Geo-lock values and for this the grid spacing must take into account the accuracy of the GPS receiver at the decrypting site; otherwise erroneous Geo-lock values may result. Using each of latitude, longitude, time and velocity as input is depend on complexity and accuracy of application and each of inputs can be ignored if necessary.

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. Similarly, the algorithm may be deliberately slow and difficult; perhaps based on solving a difficult problem [1, 4].

III. GSM SECURITY STRUCTURE

Security structure of GSM is based on Ki (128 bit) -individual subscriber authentication key- a unique code assigned to each IMSI and permanently is stored in HLR and SIM card. This code is used for generating signed response –SRES- in the authentication process and encryption key-Kc production [6].

In GSM, authentication process is performed by a challenge and response mechanism and for each authentication request AUC generates a random sequence - RAND- that with Ki are used as inputs of A3 and A8 algorithms to provide SRES and Kc keys [6, 7].

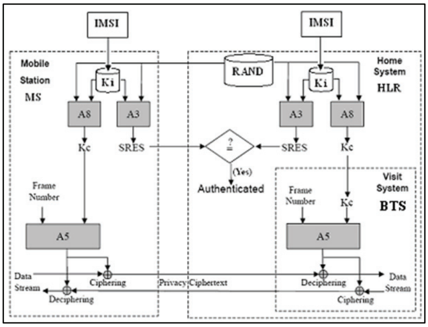

Figure 3. GSM security structure

A5 algorithm is used for encrypting data and preformed for each frame, while Kc is constant during conversation the frame number is changed [7]. The encryption process is applied only between BTS and MS, and each session key, Kc, would be used until the MSC decides to authenticate the MS again which might takes days [8].

A. Analyzing GSM cryptography

Basically GSM cryptography structure is based on authentication and its security has some vulnerability such as:

- Kc is produced based on Ki, so if some body extracts Ki from a SIM card (under SIM cloning attack) and achieves RAND number which is sent clearly from BSC to BTS, will be able to calculate Kc by A8 algorithm.
- The data stream is encrypted only between BTS and MS but at internal parts of GSM especially between BSC and BTS (usually whit radio connection links), there isn't any cyphering process.
- Kc is made according to each authentication process and is constant during each call.

Accordingly, Kc production based on Ki is the main security vulnerability factor of GSM (forging Ki under SIM cloning

[1] International Mobile Subscriber Identity
[2] Home Location Register
[3] Subscriber Identity Module
[4] Authentication Center- AUC

attack) that limits its safety. Using some other factors of GSM to strengthen encryption key during conversation is the main aim of this paper.

IV. MS POSITION 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. Knowing the 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 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 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.

A. 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.

$$1.845\,\mu s \times 3 \times 10^{8}\, m/s = 553\, m \tag{1}$$

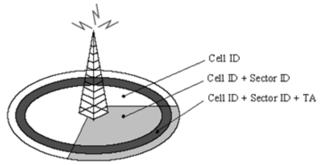

Figure 4. Cell ID+ Sector ID+TA positioning

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.

V. PROPOSED SCHEME

By using MS position parameters we 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 (LAI and Cell ID), Sector ID and TA to generate Kc. CGI and Sector ID are known and broadcasted by BTS but TA is modified by MS movement.

MSP=CGI+ Sector ID+ TA

MSP consists of 64 bits; first 32 bits for CGI, 8 bits for Sector ID (33th- 40th), 8 bits indicate TA (41th- 48th) and the rest are 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. The result is K'c:

$$Kc = A8(RAND\ , Ki) \tag{2}$$

$$K'c = Kc \oplus MSP \tag{3}$$

AUC generates five triple sets of {RAND, SRES, K´c} and sends them to HLR, BTS and MS. In the MS side, MS produces Kc by using RAND and Ki, calculates TA for MSP computing (receives Cell ID and Sector ID from BTS), then XOR it to Kc to compute K'c (Fig. 5 and 6).

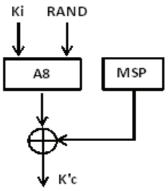

Figure 5. K'c production

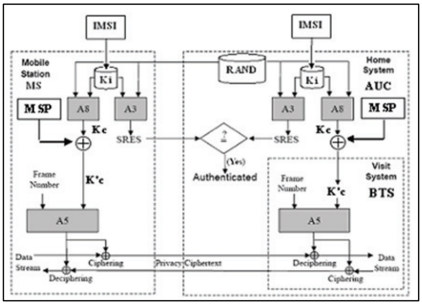

Figure 6. Proposed structure of GSM

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). Therefor 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:

$$\textit{Min-entropy: } H_{\infty}(X)=-log(max_{X}\,Pr_{X}(X=x)) \tag{4}$$

Message that has min-entropy k means that adversary's probability of guessing the message is 2-k. Based on this, if MS position in the sector is a uniform random variable we have maximum entropy for MSP:

$$H_{MSP}=-log(Pr_{MSP}(MSP=msp)) \tag{5}$$

VI. SIMULATION AND EVALUATION

In order to evaluation, a GSM network (with 4 cells) is simulated by MATLAB. Each cell consists of 3 sectors with 4km radius (0≤TA≤ 7), MS moves with constant velocity of 30 km/h along a cell toward its neighbor. This means it is moving with uniform motion. The transferred data is a 2 minute duration part of a conversation with 1000 frames (all frames are considered same with 8 bits). By this speed, each TA (500m) is passed by 1 minute, then at least two TAs are passed during any conversation, for this we limit the movement to these TAs in all movement modes and to avoid complexity we turn off hand over between sectors and cells.

The only unclear part of MSP is TA and in this case we assume uniform probability for TA with PTA=1/8 and its maximum entropy (maximum entropy in the uniform probability case) is:

$$H_{TA}=-log(1/8)=3bit \qquad (6)$$

In the movement modes by changing the position, MSP is changed and the guessing probability is decreased by a factor of time and MS velocity, depends on movement mode and changing quotas. Generally, a mobile communication is classified into 4 modes:

- Stationary mode: 80 percent of mobile conversations are established in this mode while MSP is constant and K'c depends on Kc. The additional security (additive probability of guessing) is 2-3 and doesn't change once be generated at beginning of conversation.
- Intra sector movement mode: MS moves inside a sector and doesn't defect it. At this mode TA is changed according to MS's movement and encryption process delayed until MS's location extracted. By going far away BTS, the variable part of MSP is TA and its entropy is same as previous mode. At the conversation in this mode MSP has 2 TA and the adversary has a time limitation to guess TA.
- Intra cell movement mode: In this mode MS enters another neighbor sector. TA and Sector ID parts of MSP are changed, and there is a delay same as previous modes. Similar to second mode, MSP changes at least two times and the probability of key guessing is reduced.
- Extra cell movement mode: MS enter to another cell and all parts of MSP are changed (TA, Sector ID and Cell ID) in this mode. To simplify the simulation, this movement is just considered from one sector to another sector of neighbor cell.

The simulation's results are shown in table 1. Our main aim in the simulation is to evaluate applicability of the scheme and its time. It should be considered that ciphering duration in the simulation differs from real situation. It is important to note that in the stationary mode the longer conversation increases the probability of guessing encryption key, Kc, but we couldn't obtain an accurate relationship between conversation duration and key strengths, for this we estimate just based on key guessing probability amount.

Table 1: Simulation Results

	Key	Decryption error	Addition security of key (max)	Encryption time (uplink)
Stationary mode	K_C	-	-	8.73ms
	K'_C	-	$2^{-3}t$	8.92ms
Intra sector movement	K_C	-	-	8.73ms
	K'_C	-	2^{-3}	9.845
Intra cell movement	K_C	-	-	8.73ms
	K'_C	10^{-11}	2^{-4}	10.003ms
Extra cell movement	K_C	-	-	8.73ms
	K'_C	10^{-10}	2^{-4}	10.10ms

In the stationary mode MSP is constant but in the other modes MSP is modified synchronously with MS velocity and its mobility increases key's secrecy. Thereupon, higher MS moving speed causes more K'c secretion but has another effect: decryption error. The rapid changing of TA in the high speed movement is the main factor of decryption error especially near the sector's/cell's borders. Additionally, in comparison with original method, MSP updating makes key generation delay and increases the encryption process time.

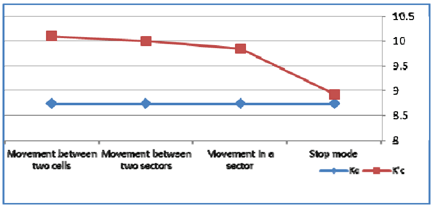

Figure 7. Key generation and encryption time comparison in two methods

VII. CONCLUSION

Using Geo-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 more revealable. Although in the others modes, the safety of encryption 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 of the plaintext) 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. Unlike the current GSM that the encryption key-Kc- is constant during conversation in the proposed scheme, K'c, changes by MS position and velocity.

In our next work we try to enhance the MS positioning method and will concentrate on a better positioning technique to decrease the decryption errors in the movement modes.

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 using Loran", 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 Intelligence, June 2007, Pitesti, ROMÂNIA