Communication Infrastructure: GSM Communication

Andreas Schöffl and Michael Irger

Abstract. In this Paper we describe the GSM Standard of Mobile Phones. The Global System for Mobile communications is the most popular standard for mobile devices in the world. Since 1994 as the first GSM Operator here in Austria offered its Services to Public, the use of mobile Phones raised until there where as much mobile Devices as Citizens or even more. The GSM Network Structure is build out of Cells which communicate with all the Devices in the supported Area and is able to hand over the Mobile Phone to other Cells, e.g. while driving, without interruption. Since the channels in GSM are digital, data communication was easy to build into the system. Security was quite important when the GSM Standard was designed so the System authenticates the user and the communication between the user and the base station is encrypted. The A5/1 and A5/2 algorithms are used to ensure in the Air Security. In 2001, the era of phone tracking has begun. The US FCC has required a positioning system in GSM networks. In this Paper we describe the fundamentals of GSM positioning systems and their architectures. We give a short overview of most important, relevant technical factors that can be used for tracking. The applications of positioning are also shown, so we give an impression how such systems work and what problems they have. It is also shown how you can position a GSM telephones either by a simple program or by your network provider with its number.

1 Introduction

Nowadays it is not possible to imagine the Communication World without the use of Mobile Phones. They are used all over the World and one of the most common and most used Standards is GSM. GSM is an abbreviation and stands for “Global System for Mobile communications”.

Back in December 1994 [HI] A1 (Mobilkom) was the first Provider in Austria and ever since the use of Mobil Phones was becoming more and more popular from all walks of life. Today, due to the low Data Bandwidth of GSM there is another popular communication system called UMTS (Universally mobile Telecommunication of system) which offers next to communication also a Broadband Data Bandwidth.

In the second chapter the basic construction of the GSM Network is described. How it is made out of cells which make the Mobile Device also named as “Cellular Phone”. Then we discuss Authentication and encoding in GSM. With the encoding becomes again on the encoding standards (A5/1, A5/2) more exactly received, as well as at the security draught according to and on the attacks on serve A5 algorithm.

2 GSM — Worldwide system for mobile Communications

GSM counts with its Ability to transfer digital data as a mobile phone standard to the second generation (2G). In the middle of the eighties there were some different and not compatible mobile phone systems developed in used in Europe, in USA and Japan which are known as analogous systems of the first generation (1G).

With the increasing number of users it was necessary to plan a future mobile phone system which should be capable of transferring digital data with clearly higher capacity.

From 1982 to 1990 the ETSI (European Telecommunications standards institutes) developed in cooperation with the European industry and the net operators the GSM standard.

2.1 GSM Network Structure

The GSM network is built up in a cellular way. That means in every single cell there is a base station (BTS - Base Transceiving Station), which uses radio waves to connect with the Mobile Devices within the Area of the Cell.

The controlling station (BSC - Base Station Controller) administers the resources (transmitter and receiver) of the connected base stations. The controlling stations are steered by a Mobile Switching Center (MSC). MSC has comparable functions to a fixed network switching node, e.g. passing participants to other cells.

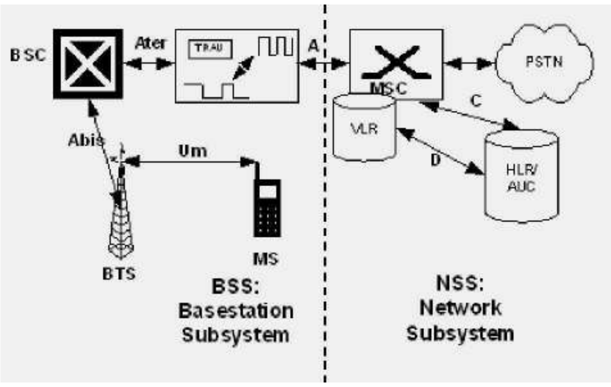


Fig. 1. Architecture GSM [RIE]

The second important unit is the Home Location register (HLR), which is a database for the management of the participant data. HLR stores the international phone number of the participant (IMSI), the ISDN phone number of the mobile station (MSISDN), as well as the address of the Visitor Location Register (VLR).

VLR contains data about the current place of the mobile stations. Another important component is the Authentication centre (AUC), a protected data base which contains a copy of the confidential key stored in every SIM card. This is used to the authentication and encoding. AUC offers additional security to protect from unauthorized use of the mobile station. Another data base is the Equipment Identity Register (EIR). EIR contains a list of all valid mobile stations on the network. Based on this List every mobile station is marked by its international device call sign (international mobile equipment Identity, IMEI). One of the most important aims was the security of GSM. The most important security point's are:

- authentication of the users
- encoding of the communication
- anonymity
- access control

All relevant data is stored on the SIM card by PIN (Personal Identity Number) and PUK (Personal Unlocking Key). The GSM Standard encrypts all personal Data. Therefore an A3 algorithm is used for the Challenge-Response-Authentification and an A8 algorithm to generate the session Key. The encryption of the transferred data works with the encoding standard A5. For data protection reasons the user is not identifiable via his IMSI.

2.2 Authentication and encoding in GSM

A device signals the access net with the use of its IMSI (stored in the SIM card), that it would like to make use of its services. After that the MSC asks the responsible HLR for the required authentication information. The HLR gets this information of the AUC.

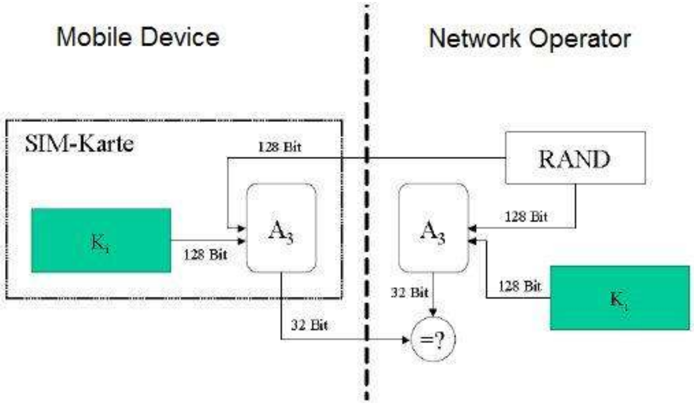


Fig. 2. GSM Authentification [UL]

A permanent key *Ki* exists for every user. This key won't be transferred. The authentication works with a "challenge response mechanism". The network generates a random 128 bit value (RAND - corresponds to "Challenge") and sends it to the MS (mobile phone). As soon as the mobile phone receives this value, a return value is calculated by a "disposable function" with the same stored key. As the AUC also knows this key, it calculates the expected answer SRES and compares it to the actual answer of the MS. If both values are identical, the user is authentified.
For the Transfer an additional key K_c is calculated with the "Challenge" and the key. The authentication function is called A3, the encoding function A8. These both functions are mostly packed into one algorithm and are kept secret by the net operator.

2.3 GSM security

GSM has never published the crypto algorithms. However as Time went by Information leaked and reverse engineering figured out details about the used procedures which have become known then.
The main disadvantage of GSM is that it does not provide an end to end encryption. The encryption takes only place between base station and mobile phone. The rest of the GSM net is transferred unencrypted.

2.4 Encoding standards in GSM

[SL]
The algorithm in the GSM standard which encrypts and decrypts digital speech data is named in the draft documents with the abbreviation A5. There are at least two versions of this algorithm. The stronger version is called A5/1 and is in Use in the European Networks. The second algorithm A5/2 has as "a weak" encoding procedure and is used in countries in which Cryptography is only allowed with restrictions.

At the beginning there was almost nothing known about the functionality of the standard because the documents were kept in secret. The first investigations of the algorithm are based on parts of certain documents which had reached the Bradford University in an anonymous way. Although the data was incomplete, the involved scientists got an impression of how the algorithm worked.

2.4.1 Description of the A5/1 stream cipher

[ABAS]
A GSM conversation is sent as a sequence of frames. Each frame contains 114 bits representing the digitized A to B communication, and 114 bits representing the digitized B to A communication. A new frame is sent every 4.6 milliseconds, and each frame has a publicly known 22 bit frame counter F_n which cycles every 2^{22} frames (i.e., a few hours).

Each GSM phone conversation can be encrypted by a new session key K, which is derived in a noninvertible way from the user's master key and a random value by another algorithm known as A8. For each frame, K is mixed with the frame counter F_n, and the result serves as the initial state of a generator which produces 228 pseudo random bits. These bits are XOR'ed with the 228 bits of the plaintext to produce the 228 bits of the cipher text.

A5/1 is built from three short linear feedback shift registers (LFSR) of lengths 19, 22, and 23 bits, which are denoted by *R1, R2* and *R3* respectively. The rightmost bit in each register is labeled as bit zero. The taps of *Rl* are at bit positions 13,16,17,18; the taps of *R2* are at bit positions 20,21; and the taps of *R3* are at bit positions 7, 20,21,22 (see Figure 1). When a register is clocked, its taps are XORed together, and the result is stored in the rightmost bit of the left-shifted register. The three registers are clocked in a stop/go fashion using the following majority rule: Each register has a single "clocking" tap (bit 8 for *Rl,* bit 10 for *R2,* and bit 10 for *R3);* each clock cycle, the majority function of the clocking taps is calculated and only those registers whose clocking taps agree with the majority bit are actually clocked. Note that at each step either two or three registers are clocked, and that each register moves with probability 3/4 and stops with probability 1/4.

The process of generating pseudo random bits from the session key *K* and the frame counter F_n is carried out in four steps:

- The three registers are zeroed, and then clocked for 64 cycles (ignoring the stop/go clock control). During this period each bit of *K* (from lsb to msb) is XOR'ed in parallel into the lsb's of the three registers.

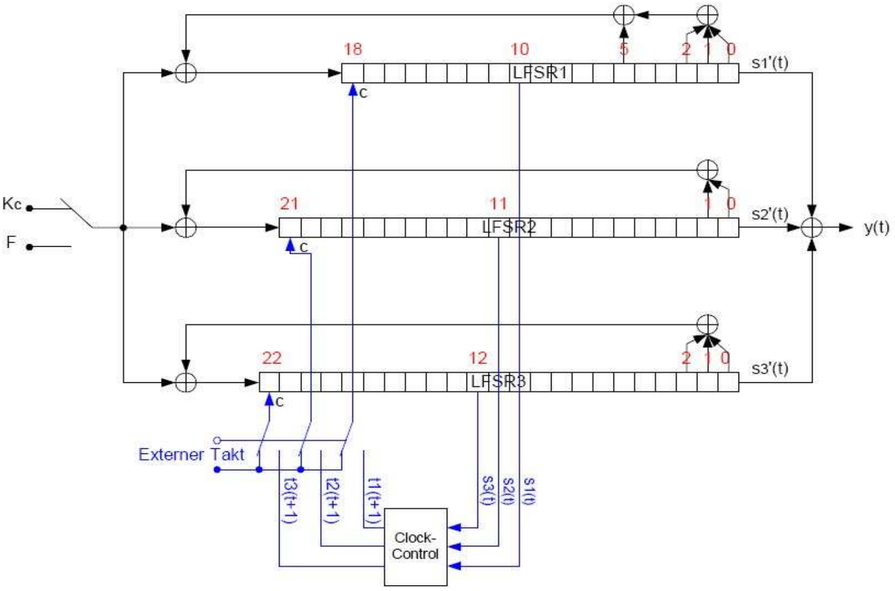


Fig. 3. The A5/1 Stream Cipher [NK]

- The three registers are clocked for 22 additional cycles (ignoring the stop/go clock control). During this period the successive bits of F_n (from lsb to msb) are again XOR'ed in parallel into the lsb's of the three registers. The contents of the three registers at the end of this step are called the initial state of the frame.

- The three registers are clocked for 100 additional clock cycles with the stop/go clock control but without producing any outputs.

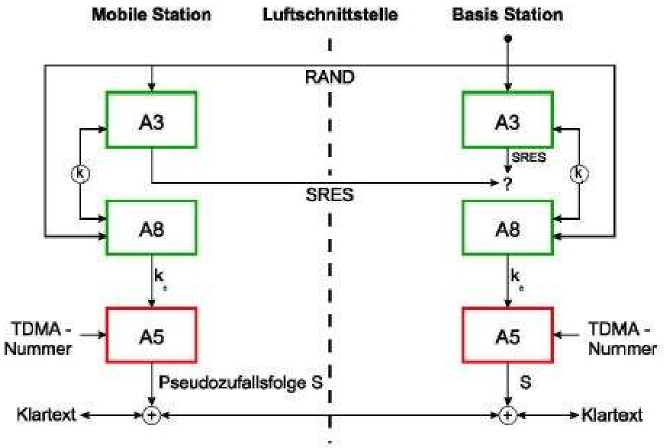
- The three registers are clocked for 228 additional clock cycles with the stop/go clock control in order to produce the 228 output bits. At each clock cycle, one output bit is produced as the XOR of the msb's of the three registers.

2.4.2 The A5/2 stream cipher

The A5/2 differs from the A5/1 only in the fact that the clock controlling bits were evacuated in the fourth register. However, this has a huge assuagement of the algorithm to the result. The problem is the clock controlling bits. Without this the contents of the third one can be determined from two arbitrarily elective registers easily. However, there is still a better possibility.

In the attack of S. Petrovic, A. Fúster-Sabater is not analysed three registers which deliver the key stream. Instead, the fourth register is analysed. Therefore internal states will be guessed and from it derived how the first three registers were clocked. On this way the contents of three registers can be determined again.

2.5 GSM-security Concept



k_i	:	geheimer Teilnehmerschlüssel (128 bit)
RAND	:	Zufallszahl (128 bit)
SRES	:	signed response (32 bit)
k_c	:	Übertragungsschlüssel (64 bit)
TDMA	:	time division multiple access (22 bit)

Fig. 3. GSM Concept [OS00]

The algorithm A3 serves the authentication of the mobile transceiver before the base station, and A8 serves the key generation. Both algorithms are not standard, and can be implemented by the mobile radio supplier individually. [OS00]

3 Positioning GSM telephones

3.1 Introduction

Cellular positioning, phone tracking is the ability to locate every powered-on, authorized cell phone in a GSM/UMTS network. “GSM implements the possibility of positioning a mobile device. In general case, this can be made with the IMSI number and the cell in which the wireless device is currently connected. It is a complex process, which depends on several components. These include the landscape, the signal strength, the utilization of the cell and the cell surface.” (“Positionssysteme mit GSM”, Vladimir Dimitrov, p1) It can be a useful feature for communication service providers and their subscribers. However this technology has significant some critical aspects, we want to show in this paper. The positioning system can be abused to violate the personal privacy. The beginning was in 2001, when the US Federal Communication Commission has required a solution for accurately positioning of GSM based cell phones. For example, people who request emergency with their mobile via 911. The problem to locate caller’s position had to be solved. Consequently the communication service providers had to produce a solution that works on every existing phone. The idea of integrating a GPS system was too expensive and not practicable, due to limited capabilities of cell phones and the imprecision of GPS tracking.

3.2 Fields of GSM positioning

There are few useful reasons for phone tracking. Some of them are shown below.

Location-Sensitive Billing – Communication providers can introduce tariffs depending on the position of cell phone. They can differ where the person is calling from, thus international calls can be charged higher than domestic calls (e.g. Roaming tariffs)

Increased subscriber safety – An increasing number of emergency calls are made from mobile phones. In many cases the caller cannot exactly announce his position. In such case it is useful to determine his position automatically by a positioning system.

Enhanced Network Performance - "At the microscopic level, accurately monitoring the movement of mobile telephones enables a cellular communications network to make better decisions on when to hand over from one cell to the next. Macroscopically, long-term monitoring of mobile telephone positions provides excellent input to the planning of the cellular network."
(Positioning GSM Telephones, IEEE Communication Magazine, p. 46)

The most important application is "increased subscriber safety", due to locating emergency calls.

3.3 Theoretical foundations

3.3.1 Types of positioning systems

For the classification of a positioning system it is important where the positioning is made and where the information is used. There are two typed of positioning systems: *self-positioning* and *remote-positioning*. The classification is useful for analyzing an existent system.

Self-positioning – In a self-positioning the receiver makes its signal measurement from geographically distributed transmitters and uses its results for determining the current position. A good example for a self-positioning system is a GPS receiver. It gets signal from several satellites and it compute the position.

Remote-positioning – In a remote-positioning system the receivers, located at different places, measure the signal, emitted by an object which has to be localized. The data is sent to a central server where the object's position is estimated. The information can be used for different applications (e.g. CAD-Systems).

Indirect-Positioning – It is possible to transmit data from a self-positioning system to a central site or vice versa via data link.

There a many methods to derive position of signal measurement, which can be applied to GSM. The most important parameters are propagation time, time difference of arrival (TDOA), angle of arrival (AOA) and carrier phase. The intersection of the measured values can be assumed as the current position of the mobile phone. A least squares approach of these values can be done for determining position with a minimal error. The more measurements are made, the more accurate the result. If too few values are available, the loci will intersect at more than one point, resulting in ambiguous position results.

Fig. 1 shows base functionality of a GSM positioning system that works with mentioned parameters propagation time, TDOA and AOA.

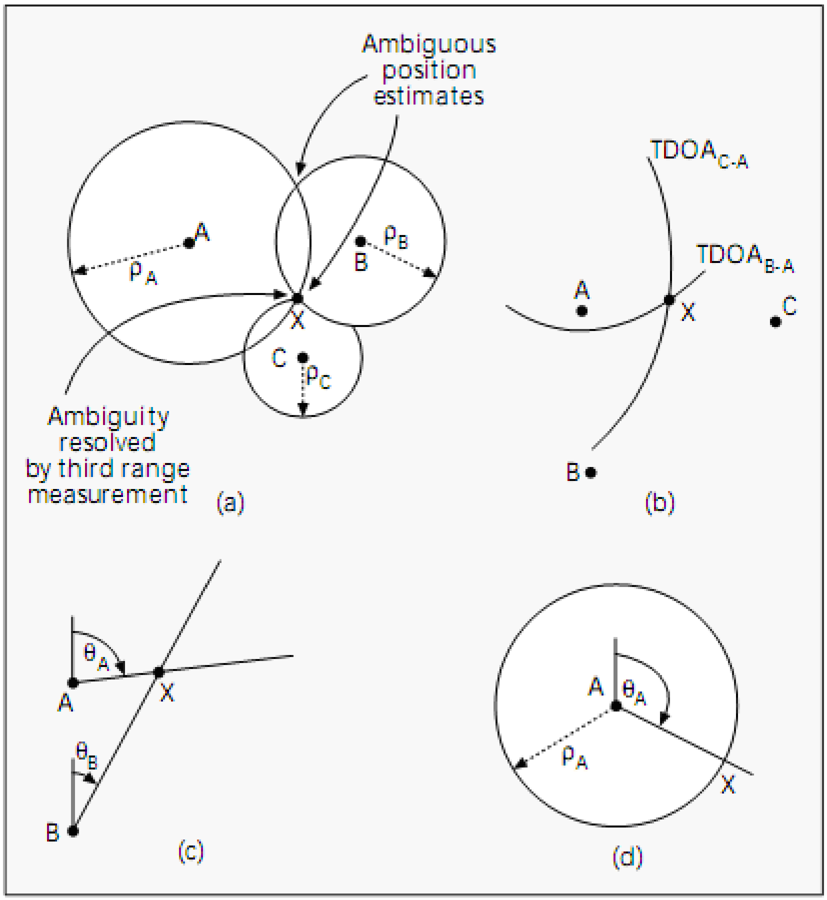


Fig. 1 theoretical model of GSM positioning system with shown parameters; A, B, C represent base stations, X is the locus of the telephone

We concentrate on four cases of positioning, shown above.

(a) Measurement with propagation time. It can differ from one location to the other, due to different signal runtimes. This results in an inaccurate position estimate. For exact estimate, we need more values.

(b) There are two TDOA values available, which are intersected. The result is an accurate position estimate.

(c) The same method with AOA.

(d) A combination of angle and time measurement.

The mentioned model is simplified. Theoretically, it is assumed that base stations and mobile phones lie in the same plane, due to better understanding how positioning works.

In reality, most of the base stations are located on hills because of better sight to the telephone. It is also assumed that the mobile phone has established connection to the base stations and the caller is not moving. In that case, the Doppler Effect must be included in positioning. It also happens that the connection is lost, when someone drives through a tunnel. In this document we only focus on basics of GSM based positioning systems.

3.3.2 Positioning parameters

In the last chapter we gave a short introduction how a GSM based positioning system works. We mentioned important parameters which will be explained in detail below.

3.3.2.1 Propagation time

"This involves measuring the time it takes for a signal to travel
between a base station and a mobile telephone or vice versa." (Positioning GSM Telephones, IEEE Communication Magazine, p. 47)
It can also be seen as the round- trip time of a signal: It is transmitted from a station to its destination and is echoed back.
This time can differ from one location to the other. In case of movement of the caller, it's more difficult to accurately estimate his position, because of different frequencies of the signal. When an object is moving toward a base station, the emitted wavelength of the object's signal is shorter than the current. When it moves away, the wavelength seems to be higher, caused by the Doppler Effect. Although there are mathematical models of describing this effect, but it would take too long to describe these models related to GSM positioning in here.
Let's take a look at the case figured in (*Fig. 1, (a)*). There are two different values measured. This leads to a circular view around the mobile phone. Each arrival of propagation time value can be seen around the phone because the angle of the incoming signal is not defined. Mathematically there two circles that intersect in two points. We see two positions that might be impossible. This case shows that positioning estimation with one or more propagation times is not efficient enough.

3.3.2.2 Time difference of arrival (TDOA)

A mobile phone can listen to several base stations and computes time difference between one pair of arrivals. For example, three values of three base stations are measured; two independent TDOA measurements can be made. Each TDOA measurement defines a hyperbolic locus, where the telephone must lie. The intersection of more values will define current position. (See *Fig. 1 (b))*

3.3.2.3. Angle of Arrival (AOA)

The angle of arrival is the angle of incoming signal of the base station at angle a mobile phone or angle from telephone at base station. One measurement produces a straight line from base station to phone. This is no more meaningful. A second measurement will yield a second line, which can be intersected with the first one. The result is the telephone's position. (See *Fig.1 (c)*)

3.3.2.4. Carrier phase

Mobile phones can use the GSM carrier wave to compute their positions, but there are many problems using this parameter.

The positioning receiver can measure the phase of the received signal, but it cannot count the cycles (wavelengths) between transmitter and receiver. Another problem is that carrier wave has to be watched continuously. Failures in carrier signal leads to errors in positioning. In addition, each cell phone would need more signal strength to smooth such errors. This could lead to bas performance and decrease of battery runtime. (See *Fig. 2 (d))*

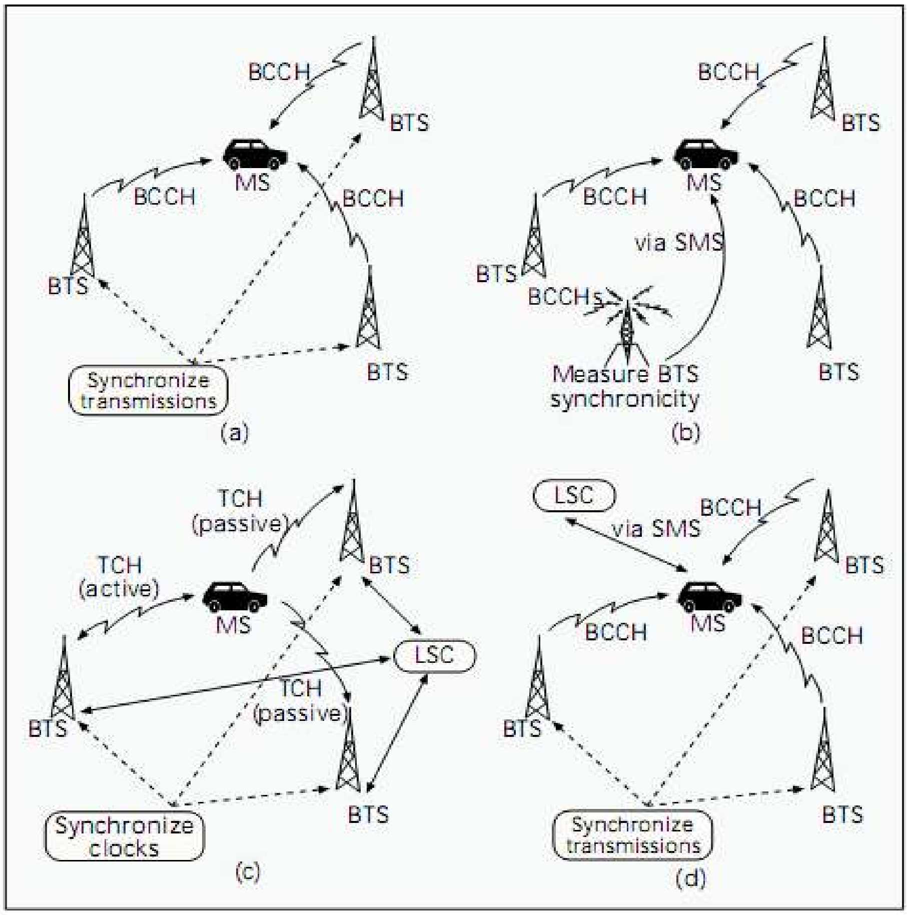


Fig. 2 schematic overview of different GSM positioning architecture

3.4 GSM positioning architectures

In the last sections we explained fundamental basics of positioning cell phones. In the next chapters we'll concentrate on current implemented architectures specified by the GSM standard. We will explain three physical architectures that are used for positioning: mobile-based, network-based and hybrid positioning. "There can be significant differences in system architectures affecting infrastructure costs, coverage, the total number of users that can be supported, and the number of users that can be simultaneously positioned. The needs of a given positioning application will determine where the position information is required, the position update rate for each object being tracked, the number of objects to be tracked, and the net value of the position information. The various architectures need to be evaluated in light of these requirements to select the most appropriate one." (Positioning GSM Telephones, IEEE Communication Magazine, p. 50)
Fig 2 gives a short overview of these 3 architectures. In general to understand, how GSM works, we refer to other documents that explain the basics of GSM. We assume in here that the reader knows these theoretical foundations related to.

Next we'll focus on these three architectures.

3.4.1 Mobile-based positioning

The call phone or mobile station (MS) uses the signals from BTSs to estimate its position by using the TDOA position technique. The phones have to be modified that they able to make TDOA measurements more accurate. The BCCH (broadcast control channel) is used for this architecture, because the bursts of this channel do not underlie frequency hopping and power control and they are repeated more frequently than others.
In addition, the network has to be synchronized for positioning. This can be done by placing GPS time transfer receivers at each BTS. Another possibility is to monitor measurements of time arrivals of several BTSs and send them to the mobile phone via SMS (*Fig 2(b)).* So it is possible to track every mobile, by sending a message which contains tracking information. This architecture is form of a self-positioning system, because the mobile phone estimates its position by geographically distributed base station. (See *Fig. 2*(a), *Fig 3*)

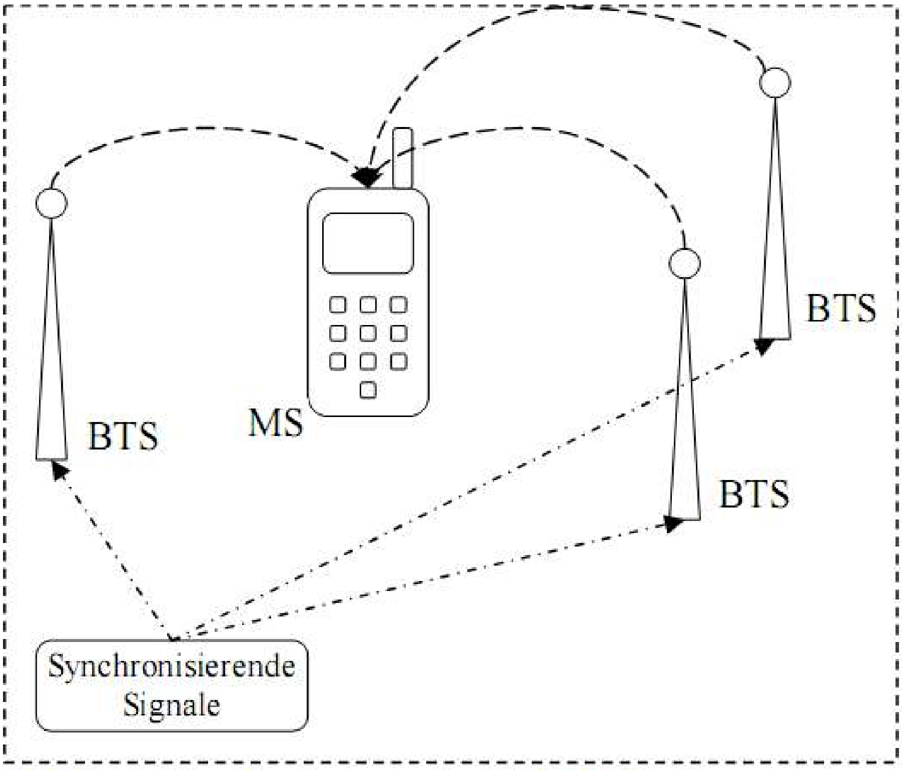


Fig 3 basic functionality of mobile-based architecture; the dashed-dotted lines represent synchronization signals

3.4.2 Network-based Positioning

Using the transmission of a mobile to work out its position is referred to as network-based positioning system. It is based on the TDOA method. Several distributed BTSs are required to monitor mobile's transmission in the area to increase performance of TOA measurements to determine the MS position. A locus function is required for that system. It processes the bursts on the uplink in a call. However the traffic channels can underlie frequency hopping and power control. This has influence to the result of positioning. The locus function has to offset these side effects. In this case a LSC (location service center) is used, for generating continuously TOA measurements of the given TDOA measurements of the MS. It estimates the MS's position. It can be seen as a transaction processor. It schedules positioning requests of the MSs for different applications. Positioning receivers can be collocated with BTSs. This has many result advantages, e.g. the mobile has to do no positioning calculation, lower costs, lower power consumption, etc. The signalling between LSC and positioning receiver is achieved by communication channels (TCH) between MSs and BTSs. While one BTS is collecting positioning requests, another BTS sends the positions back to MSs. It can also occur that the position is sent back to MS via SMS. For better results with minimal errors, the network has to be synchronized with the MS by using a synchronization clock (See *Fig 2. (c), Fig 4).*

This system is a kind of remote-positioning system, due to central processing of positioning information.

3.4.3 Hybrid positioning

This architecture represents a compromise between mobile-based and network-based system. “Hybrid positioning architectures combine different aspects of self- and remote-positioning architectures. A possible hybrid architecture has the locus function residing in the mobile but the fusion function situated at the LSC. When requested by the LSC, a given mobile will measure the TOA of bursts from various BTSs. These are then sent to the LSC, which generates TDOA measurements and computes a position estimate for that mobile.”
(Positioning GSM Telephones, IEEE Communication Magazine, p. 52)

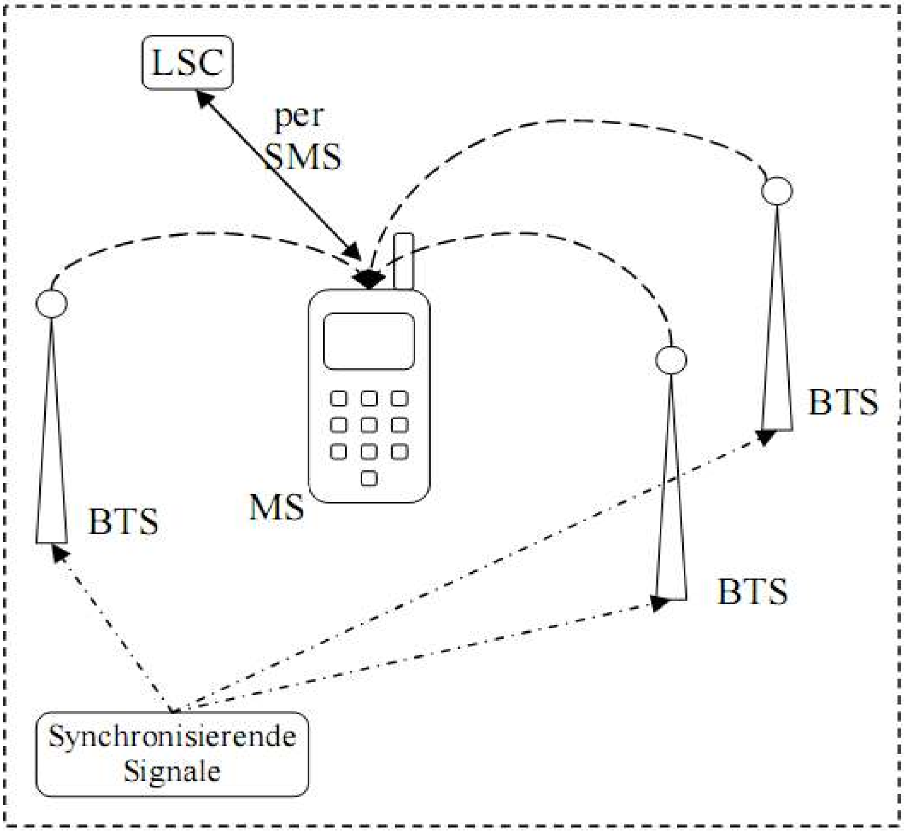
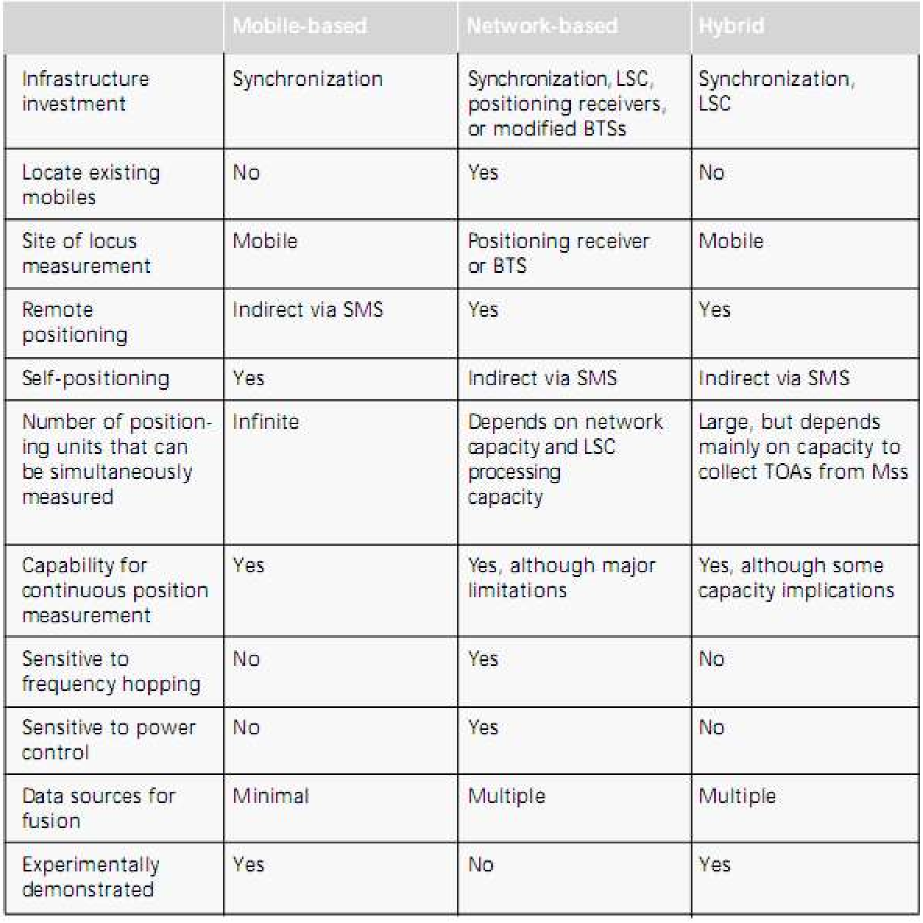


Fig. 4 hybrid architecture; the dashed-dotted lines represent synchronization signals

3.4.4 Table for comparing GSM positioning architectures

The following table gives a short overview of the most important aspects for comparing GSM positioning architectures.



	Mobile-based	Network-based	Hybrid
Infrastructure investment	Synchronization	Synchronization, LSC, positioning receivers, or modified BTSs	Synchronization, LSC
Locate existing mobiles	No	Yes	No
Site of locus measurement	Mobile	Positioning receiver or BTS	Mobile
Remote positioning	Indirect via SMS	Yes	Yes
Self-positioning	Yes	Indirect via SMS	Indirect via SMS
Number of positioning units that can be simultaneously measured	Infinite	Depends on network capacity and LSC processing capacity	Large, but depends mainly on capacity to collect TOAs from Mss
Capability for continuous position measurement	Yes	Yes, although major limitations	Yes, although some capacity implications
Sensitive to frequency hopping	No	Yes	No
Sensitive to power control	No	Yes	No
Data sources for fusion	Minimal	Multiple	Multiple
Experimentally demonstrated	Yes	No	Yes

Fig 5 shows table of most important aspects for architecture comparison

Depend on the application, what architecture will be implemented by the network providers,

- The main difference is the amount of infrastructure investment. All three architectures have to implement TDOA techniques. However, the hybrid- and network-bases systems need a LSC.

- Network-based systems need no mobile phone modification. This is a huge advantage to mobile-based systems.
- The locus and fusion functions vary from one architecture to the other.
- All networks have to be synchronized, either clockwise or by using synchronizing transmissions.
- In hybrid or network-based systems. The amount of simultaneously positioning MSs is limited by the capacity of TCHs and LSCs.
- Frequency hopping and power control can be a problem in network-based systems, due to usage of communication channels (TCH).

There are more aspects to compare, but this would take to long in here.

3.5 How you can position your mobile

There are many solutions how you can position a cell phone by specifying its number. There are several websites that provide software solutions for phone tracking with minimal charges. They'll send a SMS to the given number, so they'll know its position by retrieving the cell where the phone is authorized. By using a network-based positioning system the provider knows the involved BTSs and can estimate the location by using TDOA method. The information is sent to a server's database where you can query the position. The problem is that positioning isn't allowed in any case. Only public prosecution department can track your mobile in relation to a criminal issue. Positioning would violate privacy. Such systems that provide this functionality must ensure that the person who is tracked has agreed to the operation, otherwise it can be prosecuted.

References

[HI] GSM Entwicklung in Österreich:
http://www.umtslink.at/GSM/gsm_history_austria.htm

[UL] UMTS-Link: *GSM, UMTS*
GSM: http://umtslink.at/cgi-bin/reframer.cgi?../GPRS/vorteil gprs.php

[ABAS] Alex Biryukov, Adi Shamir: Real Time Cryptanalysis of the Alleged A5/1 on a PC
http://citeseer.ist.psu.edu/287068.html

[NK] Nils Kaufmann: *Angriffe auf das Verschlüsselungssystem von GSM*
www.fernuni-hagen.de/NT/kurse/sem_2000/kaufmann.pdf

[SL] Stefen Lucks, Erik Z. *Sicherheit des GSM-Verschlüsselungsstandards A5*

[Rie] Riedl, Reinhard: *Mobile Kommunikation (Vorlesungsfolien)*.
http://www.ifi.unizh.ch/~riedl/MK_last.pdf

[OS00] Oliver Stutzke, Bernhard L.: *Sicherheit aktuell verwendeter Stromchiffren*.
2000. http://ks.fernuni-hagen.de/aktuelles/archiv/23.5.pdf

[1] www.comsoc.org/ci/private/1998/apr/pdf/Scott.pdf, "Positioning GSM telephones", IEEE Communications Magazine, April 1998

[2] www.comsoc.org/ci/private/1998/apr/pdf/Scott.pdf "Positionierungssysteme mit GSM", Vladimir Dimitrov, Hochschule für Technik, Stuttgart

Picture Credits

[1] www.comsoc.org/ci/private/1998/apr/pdf/Scott.pdf, "Positioning GSM telephones", IEEE Communications Magazine, April 1998 (Fig. 1, 2, 5)

[2] www.comsoc.org/ci/private/1998/apr/pdf/Scott.pdf "Positionierungssysteme mit GSM", Vladimir Dimitrov, Hochschule für Technik, Stuttgart (Fig. 3, 4)