

Тема 14. GSM мрежи, архитектура, основни подсистеми.

Основни функции и действия – защита, локализация, повикване, хендоувър и роуминг. Обслужване на повикванията

GSM е проектирана по време на втората половина на 80-те години като цифрова европейска клетъчна система и е основната клетъчна радиомрежа в Европа. Тя е съобщителна мрежа за универсално безжично обслужване, която осигурява мобилни гласови комуникации, мобилен факс, текстови съобщения, както и нови авангардни услуги. . За GSM-системите са предоставени три честотни ленти: 900, 1800 и 1900 MHz. Системите GSM 1800/1900 са предназначени за голяма плътност на мобилния трафик. В тези системи, освен известните клетки, се използват и т.н. **клетки-чадъри**. Оригиналният GSM, публикуван през 1991 г., е проектиран да използва радиолента от 900 MHz. Системата е стандартизирана в два варианта:

1. 900 MHz с две ленти на 45 MHz, с по 124 съседни носещи честоти
2. 1800 MHz (1900 MHz) прав и обратен канал, отделени на 90 MHz.

Основните системни параметри на GSM 900 (виж тема 13)

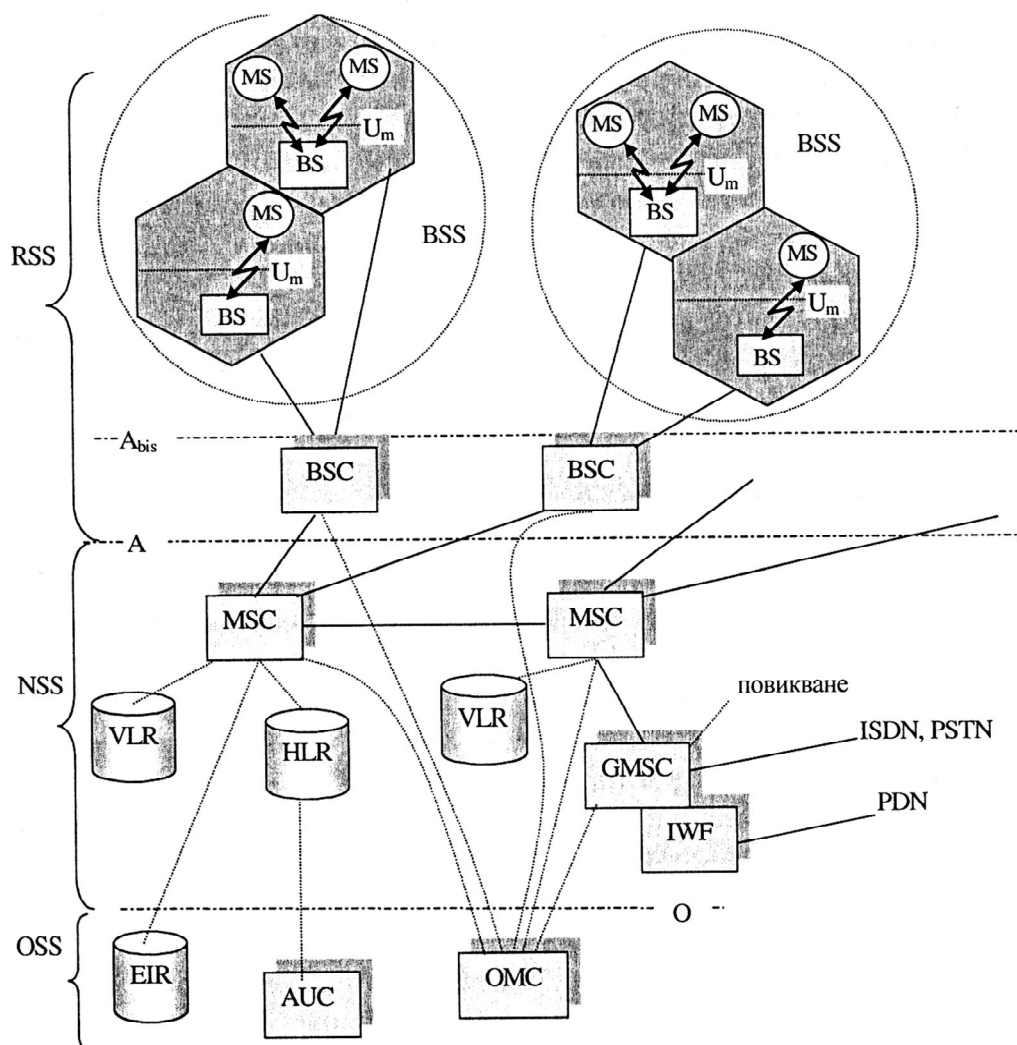
1. Честотна лента на базовия предавател 935.2 - 960 MHz (**Downlink**);
2. Честотна лента на мобилния предавател 890.2 - 915 MHz (**Uplink**);
3. Дуплексен режим с две честоти, по една за всяка посока на предаване във всеки канал;
4. Интервал между носещите честоти: 200 kHz;
5. Мултиплексиране с времоделене по осем канала на носеща честота;
6. Брой на носещите честоти във всеки диапазон (т.1 и т.2): 124;
7. Всеки канален време-интервал побира пакет от 156,25 разряда (Тема 9), заема 577μs и се повтаря 216,64 пъти в секунда.

Архитектура на система GSM. Блокова схема

Система GSM има сложна йерархична структура. Тя включва много обекти, интерфейси и абривиатури. По-долу са показани архитектурата и опростена илюстративна схема. GSM се състои от три подсистеми: **радиовръзка** (RadioSubSystem - **RSS**), **мрежи и комуникации** (Network & Switching System - **NSS**) и **операционна подсистема** (Operation Subsystem - **OSS**).

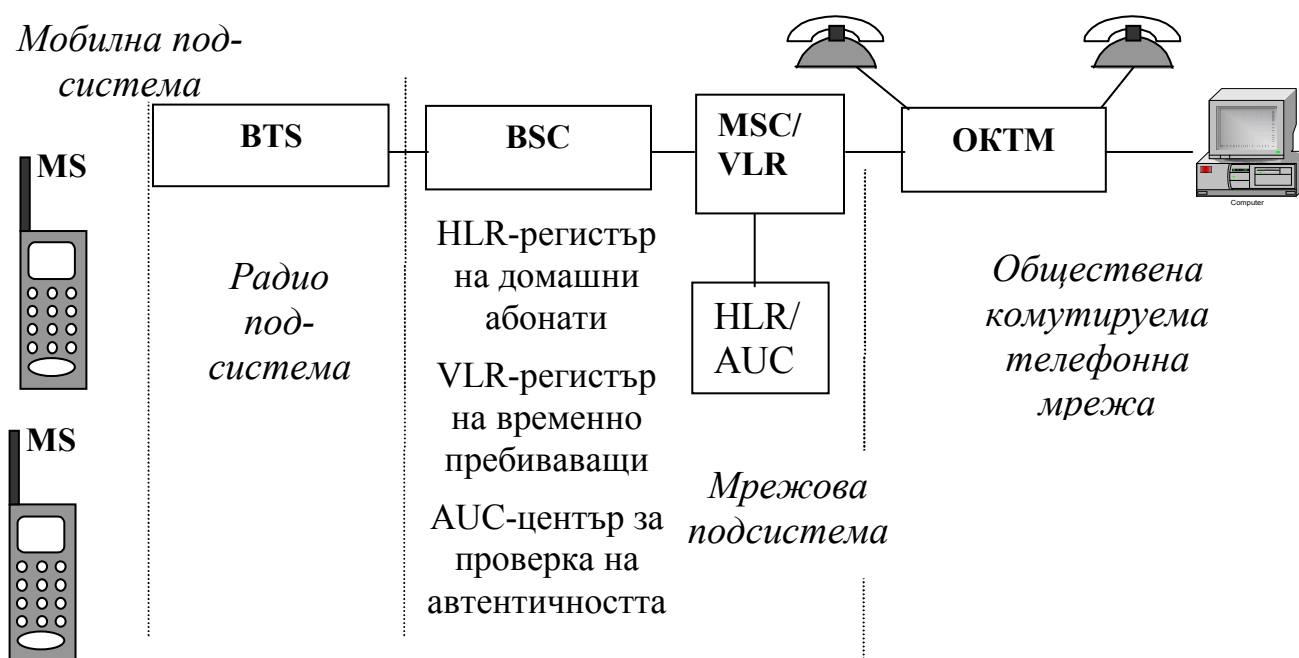
Подсистемата на радиовръзките включва базовите станции BS и мобилните станции (апарати) MS. Връзката между подсистемите RSS и NSS се осъществява чрез интерфейс А (плътните линии), а с OSS - чрез интерфейс О (пунктираните линии).

Интерфейс А функционира на базата на импулсно-кодовата модулация с комутация на каналите (2,048 Mbit/s) като поддържа до 30 канала със скорост 64 Kbit/s.



Архитектура на система GSM

Мобилна под-система



Опростена илюстрация на GSM клетъчна система

Интерфейс О използва Сигнализация No 7 (SS7). Тя се основава на предаване на управляваща информация през мрежа X.25 към подсистемата RSS и обратно.

Подсистема за радиовръзки RSS

RSS се състои от мобилни станции, базови станции и контролери BSC.

1. Мобилната станция (мобилен апарат) MS е мобилен терминал и като такъв има структура и функции, описани в Тема 9. MS съдържа цялото потребителско оборудване и софтуер, необходими за свързването на MS с мрежата на GSM. Към тях се отнасят:

- Независимото от абоната апаратно и програмно осигуряване: предавател с мощност 2W (за GSM 900) или 1W (за GSM 1800), схемата за опознаване на оборудването EI, чрез която се защитава от кражби, телефонен и други видове интерфейси (компютърни радиомодеми, за технологиите IrDA или Bluetooth), и др.;
- Модул за идентификация на абоната (**Subscriber Identity Module - SIM**) – SIM-карта, в която се съдържат всички индивидуални данни за потребителя (абонатен профил, такси и пр.), идентификатори (регистрационен номер, тип на картата, списък на абонатните услуги, личен идентификационен номер - **PIN**, ключ за снемане на блокировката - **PUC**, ключ за автентикация **Ki** и международната идентификация на мобилното оборудване **IMEI (International Mobile Equipment Identity)**).

SIM е персонална абонатна карта, която всеки получава, когато се регистрира като абонат на мобилния оператор и заплати абонатната такса. Съдържа памет и микропроцесор. Оформена е като малка печатна платка, адаптирана към всички телефонни апарати от съответния стандарт. Един абонат може да си купи нова MS или да ползва MS на друг абонат, но ще бъде таксуван за своя сметка. Това се постига благодарение на SIM-картата. При връзка с MSC за ползване на услуга, от SIM-картата се предава информация, по която HLR разпознава абоната.

При включването си в системата, мобилната станция запазва динамичната информация - данните за местонахождението и ключа на шифъра Kc.

2. Базовата станция BS отговаря за поддръжката на радиовръзките с MS, кодирането и декодирането на канала за защита от грешки, криптиране с цел засекретяване на разговора, измерване на нивото на сигналите и качеството на обслужване, регулиране на скоростта на предаване през безпроводната среда и др. BS съдържа оборудването, необходимо за радиокомуникациите - антени, усилватели, устройства за обработка на сигналите, и др. Връзката ѝ с MS се осъществява чрез интерфейс Um, а с контролерите - чрез Abis. BS осигурява входяща точка за множеството мобилни телефони, които присъстват в дадена клетка, разрешава им да правят и приемат повиквания.

Интерфейсът **Um** включва всички механизми, необходими за безжична връзка (TDMA, CDMA и др.).

Контролерът за базовите станции (BSC) в GSM-системата координира функциите на няколко базови станции. Той определя честотите, които могат да се използват от контролираните BS. Управлява превключването на разговора, което се прави при пресичане на границата между две клетки. Информира базовата станция в клетката, която трябва да поеме разговора, и изпраща на мобилния телефон информация за това. Базовите станции могат да се свържат с контролера по различни топологии - звезда , пръстен, каскада и др.

Подсистема на мрежите и комутацията NSS

Мрежовата подсистема NSS е ядро на GSM-системата. Тя съединява RSS-подсистемата със стандартните мрежи за общо ползване и може да определи местонахождението на абоната във всяка точка от планетата. Тя осигурява таксуването на потребителя, заплащането на услугите и роуминга на потребителите между различни оператори в различни страни. Към нея се отнасят:

- **Мобилна телефонна централа (Mobile Switching Center) MSC**, която обслужва стационарната магистрална мрежа на GSM. Това е високопроизводителна цифрова телефонна централа, която управлява изграждането, наблюдението и разпадането на връзките от своята област, обработва SMS-съобщенията, таксува услугите, комуникира с HLR и VLR, и др. Чрез А-интерфейса MSC установява връзки с контролерите BSC от принадлежащата ѝ географска област. Чрез О-интерфейс (Сигнализация No7) мобилната телефонна централа управлява комутациите с други MSC-централи, мрежи X-25, OKTM и ISDN и извършва допълнителни функции.

- **Регистърът за домашните абонати (Home Location Register) HLR** съхранява статичната информация за всички потребители на мобилния оператор: абонатния номер, идентификационните номера, абонатния профил, информация за идентичността (ключът за автентикация Ki), сметката за платените услуги, информация за мобилната централа, която обслужва и др.

- **Регистър за временно пребиваващите абонати (Visitor Location Register) VLR**, който е свързан с всяка MSC-централа. Предназначението му е да съхранява временна информация за абонатите, предвижващи се през мрежата. За да маршрутизира повикването и да му предостави обслужване, мрежата трябва да знае всеки момент къде е съответния абонат. Когато абонатът се придвижва от една на друго място, данните се предават от VLR на старото място към VLR на новото местонахождение. Обикновено един VLR се свързва с една централа, но може да обслужва и няколко централи.

Операционна подсистема

Подсистемата OSS изпълнява функциите по експлоатация и обслужване на мрежата. Към нея се отнасят следните обекти:

- **• Център за експлоатация на обслужването (Operation and Maintenance Center - OMC)**, който чрез O-интерфейс (SS7) управлява и контролира всички обекти на мрежата, наблюдава информационния обмен, безопасността на абонатите и техните сметки. Тук се регистрират (откриват и закриват) абонаментите и услугите, наблюдават се и се регистрират отказите.
- **• Център за автентикация (AuC)**, който съдържа алгоритми за автентикация и ключове за шифрите. Тъй като радиоинтерфейса и мобилните станции, за разлика от фиксираните мрежи и терминали, са много уязвими, за защита на предаването на данните и конфиденциалността на абонатите се налага те да се идентифицират по метода на автентикацията.
- **• Регистър за опознаване (проверка) на мобилното оборудване (Equipment Identifier Register - EIR)**, който е база данни за идентификация на мобилните телефони и техният статут в мрежата (правоспособен, неправоспособен). Тъй като мобилните станции са портативни, те лесно могат да бъдат изгубени или откраднати. Всеки, който има действаща SIM-карта, може да използва откраднат апарат. В EIR има "черен списък" на откраднатите или блокирани устройства. Достатъчно е собственикът да заяви за кражбата, мобилния телефон става безполезен, тъй като не може да се активира.
- **• Центърът за кратки съобщения (SMS)**, който се грижи за съхранение и пренасочване на SMS-съобщенията. Той следи, дали съобщението е доставено, и препредава съобщения, които не са приети коректно. Когато мобилния телефон е изключен или няма покритие, всички съобщения се запазват и ще му се доставят, щом апаратът се регистрира отново в мрежата.

Основни функции и действие на система GSM

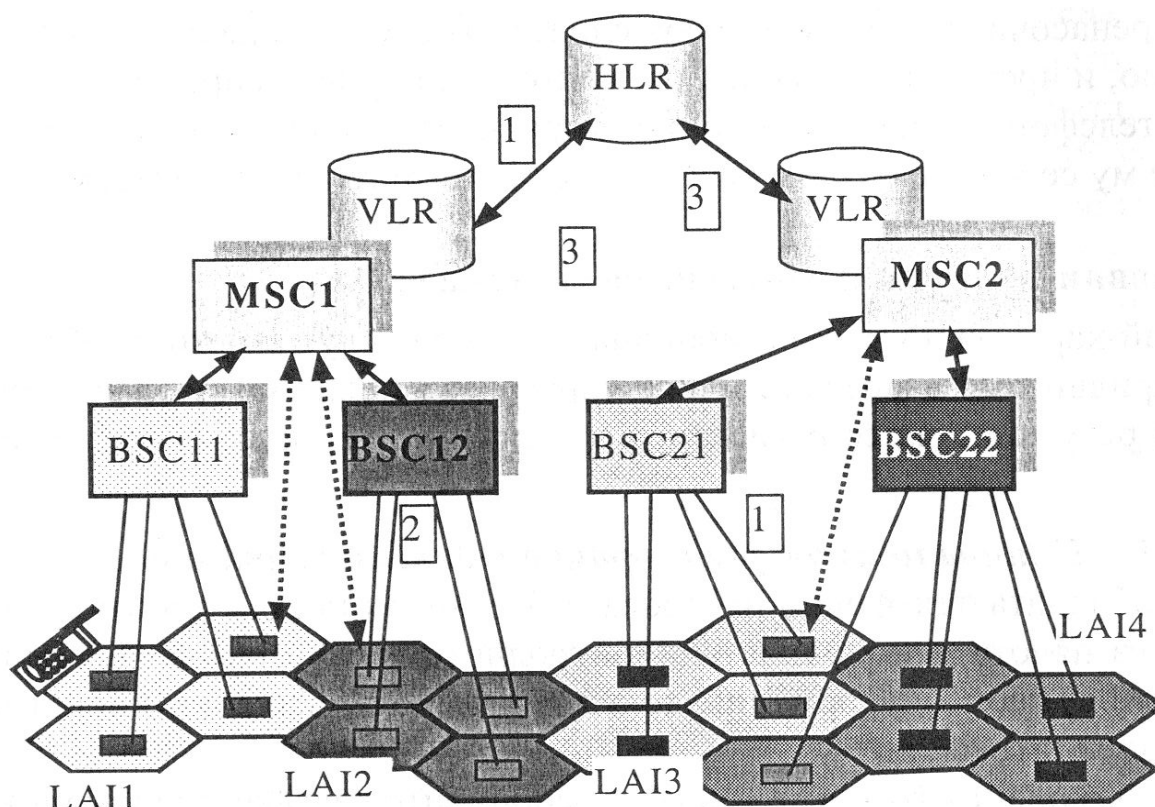
Най-характерно за една мобилна мрежа е обслужването на абонати, които се придвижват в мрежата. Да се управлява мобилността, значи мобилния телефон регулярно да се регистрира и непрекъснато да се следи къде се намира.

Инициализация, регистрация и режим на очакване

Мобилната телефонна централа и базовите станции работят непрекъснато през цялото денонощие. По контролните канали базовите станции им изпращат служебна информация, която се приема от всички мобилни телефони в съответните клетки.

За разлика от базовите станции, мобилните телефони (радиотелефоните) MS могат да се изключват. Това става по желание на абоната или за подмяна на батерията им.

Абонатът включва захранването със специалния за това бутон или поставя SIM-картата и мобилният телефон започва да работи. В този момент той още не принадлежи към никоя клетка, макар физически да е в някоя от тях. Етапът на идентификацията му и настройката му към системата (инициализацията) трае няколко секунди и става автоматично, без участието на абоната.



Инициализация и регистрация на абоната и следене на местоположението му

По време на **инициализацията** мобилният телефон MS сканира всички достигащи до него радиосигнали, по които в режим на радиоразпръскване се изпраща служебна информация, и избира онази базова станция, чийто сигнал се оказва най-силен. По получената от контролния ѝ канал информация разбира коя е **областта на идентификация** (Location Area Identity - LAI), т.е., към кой контролер принадлежи (в случая на чертежа - LAI1). Свързва се с централата и докладва за адреса си. MSC1 записва местоположението на мобилния телефон в своя регистър VLR и докладва в регистъра за домашни абонати HLR, че мобилният телефон е включен в нейната област на обслужване. След това по обратния сигнален канал мобилният телефон получава потвърждение за своята регистрация, синхронизира се, регулира нивото на сигнала и се "захваща" към базовата станция.

Но и базовата станция трябва да знае, че този мобилен телефон се намира на територията на нейната клетката. Това тя разбира чрез идентификационният му код, който се предава по обратния сигнален канал.

Мобилният телефон остава в "режим на очакване" (**standby mode**) и инициализацията завършва. Сега входящите повиквания към MS могат да се насочват към клетката, в която се намира.

Когато абонатът е извън зоната на радиопокрытие, той не може да влезе в контакт с мрежата и на дисплея на MS се показва съответно съобщение (напр. «Търсене»).

През цялото време, докато връзката между MS и BS е установена, чрез контролните сигнали мобилният телефон периодично обменя служебни съобщения с базовата станция. Чрез тях следи както нейната работа, така и собственото си преместване. Ако MS не потвърждава регистрацията си, системата го приема за изключен.

При преместването си в клетка на областта LAI2, MS се регистрира в новата област, а оттам - във VLR-регистъра. Там се изтрива старото му местоположение и се запомня новото. Когато мобилният телефон влезе в LAI3, регистрацията се приема от друга мобилна телефонна централа (MSC2). За нея той е нов обект и неговата поява се докладва в домашната база данни, която информира старата централа MSC1, че този телефон е влязъл в територията на съседната централа. Тогава MSC1 изтрива неговия номер от своята VLR-база данни.

Функции за защита

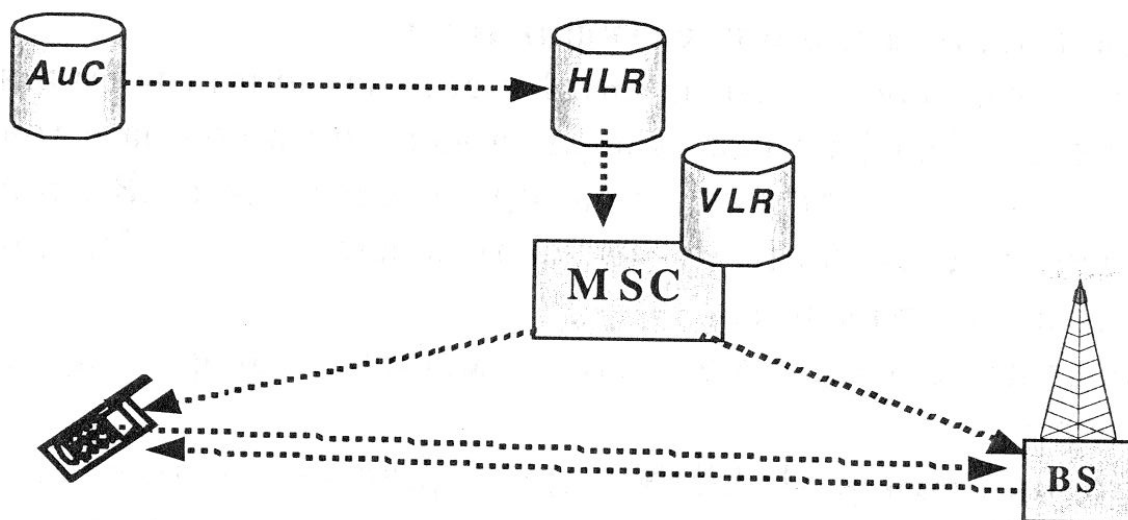
1.Проверка за автентичност

Когато при мобилния оператор се регистрира нов абонамент, освен телефонния си номер, абонатът получава SIM-карта, в която като двоични числа са записани секретен ключ **Ki** и уникална международна идентификация на абоната (**IMSI** - International Mobile Subscriber Identity). С IMSI е свързана цялата информация за него. Тези данни се съхраняват на две места - в SIM картата и в AuC-центъра и се използват за неговата идентификация.

Когато се проверява идентичността, AuC генерира случайно число RAND и го изпраща по контролните канали към абоната. Чрез ключа Ki се изчислява ново число, т.нар. **белязан резултат SRES**, който се връща към AuC. Центърът, който знае случайното число и има ключа Ki, е изчислил същия белязан резултат. Ако резултатите (двата SRES) са еднакви, мобилния абонат е автентичен. Ако резултатът не е един и същ, абонатът не е този, за който се представя. Изграждането на връзката е невъзможно без да се установи идентичността.

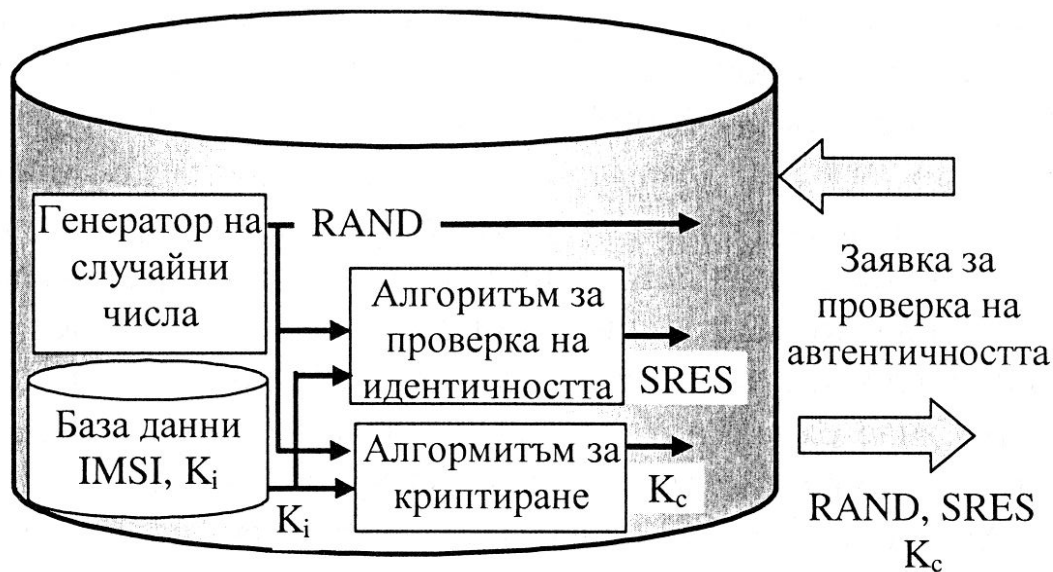
2. Криптиране

За да остане обменената информация конфиденциална и да не бъде подслушван разговора, както трафичните, така и контролните канали се криптират. В GSM речта се криптира по следния начин



Криптиране в GSM

Освен белязания резултат SRES, използвайки случайното число RAND и ключа K_i центърът AuC изчислява и друг ключ за криптиране K_c , който, заедно със SRES и RAND, се съхранява в домашната база данни. При проверката на автентичност мобилният телефон, като използва ключа K_i от SIM картата си и полученото случайно число RAND, също изчислява ключ за криптиране K_c . Ако резултатът от проверката на автентичност е положителен, през контролера на базовата станция мобилната централа изпраща на абоната ключа K_c . След това контролерът дава команда за преминаване към режим на криптиране. Всички сигнали оттук нататък, включително речта, са криптирани.



Проверка на автентичност

3. Проверка на оборудването

Целта на тази проверка е да се предотврати използването на нямащи право на обслужване и откраднати мобилни телефони. Всеки мобилен телефон си има свой международен номер IMEI. При изграждане на връзка мобилната централа иска от мобилния телефон този номер. Ако номерът е непознат или забранен, връзката се отхвърля.

Уникалната международна идентификация се предава в свободното пространство, само когато се включи мобилния телефон.

Локализация и повикване

1. Номера за локализация и идентификация

Една от ключовите особености на GSM е автоматичната всемирна локализация на абонатите. Телефонните номера са валидни в коя да е точка на планетата и GSM знае кой абонат къде се намира. В регистър HLR непрекъснато се съдържат данни за текущото му местонахождение, а чрез VLR непрекъснато се следи неговото движение.

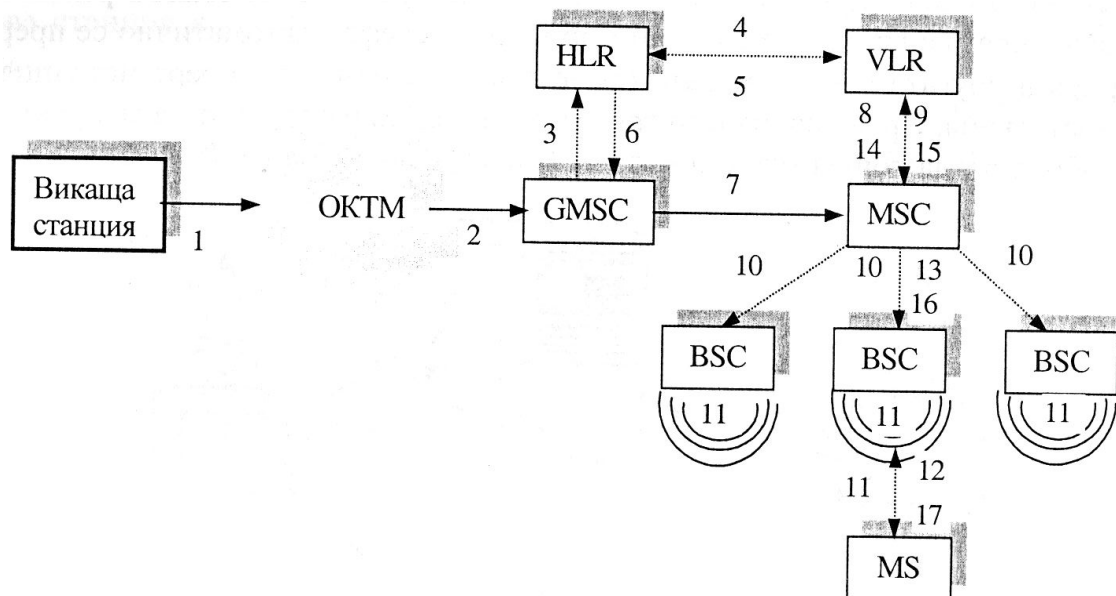
За да се определи местонахождението на мобилния апарат, са необходими следните номера:

- **Международния номер MSISDN.** Структурата на номера се определя по стандарт E.164 на ITU-T. Състои се от телефонния код на страната, националният код на мобилния оператор (неговия регистър HLR) и абонатния номер. Съдържа се в SIM-картата на потребителя. Този стандарт се използва и в стационарните мрежи ISDN.
- **Международната идентификация на мобилния абонат (International Mobile Subscriber Identity - IMSI)** (вж. ОНР 7).
- **Временната идентификация на мобилния апарат Time Mobile Subscriber Identity - TMSI.** За локално опознаване на абоната в система GSM не се използва директно IMSI, а временна идентификация TMSI (кодов вектор 4 байта). Това число се избира от VLR и действа временно в зоната на неговото местонахождение. За да се скрие личността на абоната, регистърът периодично изменя идентификацията, поради което тя е временна.
- **Номера на роуминга на мобилната станция (MSRN).** Този адрес се генерира от VLR след запитване от мобилната телефонна централа и се помни в регистър HLR. Той включва кода на страната, където абонатът гостува, кода на мобилния оператор, на който гостува, кода на MSC, от която се обслужва, и номера на абоната.

2. Установяване на връзка с мобилния телефон

Проблем тук е намирането на абоната. Това е търсене, принципно различно от фиксираните терминали, където маршрутят на връзката е известен

от телефонния номер. Къде е абонатът тук не се знае. Преди да се изгради връзката чрез последователни запитвания, трябва да се разбере неговото местонахождение и се установи направлението на търсене. Основните етапи на алгоритъма за установяването на връзка с мобилен от фиксиран телефон са показани по-долу

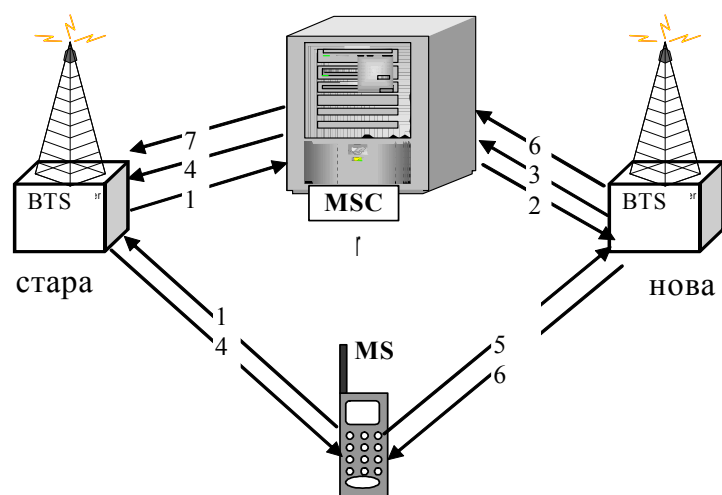


Установяване на връзка „фиксиран телефон – мобилен телефон”

На първата стъпка (1) викащия абонат набира номера на GSM-абоната. От кода на адреса ОКТМ разбира, че търсеният номер е от мобилната клетъчна система на съответния оператор. Тя преадресира повикването в код (2) за съответната входяща мобилна централа GMSC. Последната определя домашния регистър HLR, който е закодиран в търсения мобилен телефонен номер, и му изпраща повикването (3). Регистърът проверява съществуването на търсения номер в системата на мобилния оператор, както и услугите, за които е абониран. След това от текущия регистър VLR се издирва съответния номер MSRN (4). Щом го получи (5), домашният регистър определя коя от мобилните централи MSC отговаря за този мобилен телефон. Тази информация се връща в GMSC (6), която преадресира запитването (7) към съответната централа MSC. Оттук нататък тя отговаря за всички по-нататъшни действия. От регистъра VLR узнава (8, 9) текущото място на мобилния телефон. Ако той е достъпен, MSC инициира неговото търсене във всички свои клетки (10). Търсенето само в нужната клетка би отнело много време. Базовите станции на всички контролери BSC изпращат търсещи радиосигнали (11). След като се получи отговор в контролера (12) и станцията (13), че абонатът е намерен, се извършва автентикация (14) на абоната. Регистър VLR изпраща сигнал (15) и мобилната централа установява връзка с абоната (16,17). Всички тези действия се развиват докато викащия абонат чака връзката, след което той чува контролното повикване. Повикването от мобилен абонат е по-просто.

Процедура по предаване на обслужването (превключване, **handover**)

Тази процедура (американския термин е **handoff**, европейският **handover**) се отнася до случаите, когато мобилният абонат, разговаряйки, се премества от една в друга клетка. Когато такова преместване стане в режим на очакване, чрез контролните сигнали мобилният телефон автоматично се пререгистрира в другата клетка. Когато обаче той води разговор, пререгистрацията не е достатъчна. Превключването трябва да стане без разговорът да се прекъсва и без абонатът да почувства.



Опростена схема на процедурата по предаване на обслужването (handoff)

Както базовата станция BS, така и мобилният телефон MS, непрекъснато измерват нивото на изходящия, съответно, низходящия сигнал и по броя на грешките оценяват качеството на сигналите. В мобилния телефон едновременно се приемат контролните сигнали както от собствената базова станция, така и от BS на съседните клетки. Така получените данни за нивата на сигналите се предават на мобилната станция MSC всяка 1/2 секунда (1). Към коя клетка принадлежи в даден момент мобилният телефон в режим на очакване не се определя непосредствено от неговото физическо местоположение, а от това, на коя клетка сигналът се приема като най-силен. Неговото ниво е критерий за принадлежност.

Процедура по предаване на обслужването започва, когато се установи, че сигналът от старата базова станция е по-слаб от някой друг от получаваните контролни сигнали. MSC избира клетката с най-силен сигнал и предава команда на базовата ѝ станция да отдели трафичен канал за връзка (2). Тук са пропуснати транзитиращите сигналите контролери. Новата базова станция назначава канал и съобщава неговия номер на MSC (3). На свой ред мобилната телефонна централа, чрез старата базова станция, предава на мобилния телефон назначената ѝ нова базова станция и номера на канала за връзка, по който да продължи разговора (4).

Мобилният телефон се настройва към новата си базова станция (5) и чрез нея предава на мобилната телефонна централа своята готовност да завърши предаването на обслужването (6). Накрая MSC предава на старата базова станция команда да освободи канала за връзка, който е бил използван досега (7). На практика има различни случаи на превключване: (а) в рамките на един контролер; (б) превключване от един към друг контролер; (в) превключване от една към друга мобилна телефонна централа.

Роуминг

Думата произлиза от английското **roaming** (goam - бродя, странствам). Тя означава използване на услугите на чужда (не тази, на която е абонат) клетъчна мрежа. За да стане роуминга, е необходимо двете клетъчни мрежи - своята и чуждата - да са съвместими. Това обаче не е достатъчно. Трябва да има и роумингово споразумение между операторите на клетъчните мрежи, което определя техническото взаимодействие между тях, обмяната на необходимите данни за абонатите и взаимните финансови задължения на страните. Един оператор има споразумения с множество клетъчни системи в съседни страни. Благодарение на роуминга всеки абонат става единица от световната комуникационна система и може да бъде открит в коя да е точка от планетата.

Абонатът в чужда клетъчна мрежа инициира повикване по традиционния начин. Ако това е първото повикване в чуждата мрежа, то нейната мобилна телефонна централа, не намирайки сведения за този абонат в своята база данни (HLR), го възприема като гостуващ. По получените при взаимодействието с него отличителни белези тя разбира коя е домашната му система и изпраща до нея запитване за абоната. Получените данни се записват в регистъра VLR за гостуващи абонати на чуждата система, а в "домашната система" се въвеждат сведения за неговото гостуващо местонахождение. След тези подготвителни действия връзката с роумъра се организира по известния от по-горе начин.

Когато повикването на гостуващия абонат не е първо, чуждата система има вече неговите данни и го намира без да "пита" "домашната" система.

След завръщането "у дома" информацията за визитата се изтрива и от двете системи с изключение на сметката, която е направил гостуващият.

Следващи след 2G (но преди 3G) поколения

2.5G – GPRS – услуги с обобщен пакетен радиоинтерфейс (*General Packet Radio Services*) и **EDGE** - разширени скорости на данни за глобална еволюция (*Enhanced Data rates for GSM Evolution*).

2.5G плюс – HSCSD - високоскоростно предаване на данни с комутация на канали (*High-Speed Circuit-Switched Data*) и **EGPRS** (*Enhanced GPRS*).