ДИСЦИПЛИНА "БЕЗОПАСНОСТЬ МОБИЛЬНЫХ СИСТЕМ"

Лекция 4. Системы сотовой связи. Принципы построения. Технология и архитектура системы сотовой связи GSM. Системы связи GPRS

План:

4.1. Общие принципы построения систем сотовой связи.

4.2. Технология и архитектура системы сотовой связи GSM.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM.

4.4. Беспроводные сети на основе технологии GPRS.

4.5. Безопасность в GPRS.

4.6. Технологии EDGE.

4.7. Технологии 3G

4.8. Технология LTE.

4.1. Общие принципы построения систем сотовой связи

Потребности абонентов изменяются как во времени, так и в пространстве. Решение этой проблемы - увеличение емкости системы.

Емкость сотовой сети обычно увеличивается следующими методами:

1. ***Разделение сот на секторы*** - обычно соту разделяют на секторы по 120 градусов. При этом применяются секторные антенны;

2. ***Дробление сот на соты*** меньшего размера - путем создания сот меньшего размера в определенной части зоны покрытия соты. Радиусы меньших сот принимаются равными половине радиуса исходной соты, а их площади соответственно становятся меньше в четыре раза. Большие соты используются в районах с небольшим трафиком, а малые - в зонах с более интенсивным трафиком.

Распределение каналов в сотах. Правила распределения каналов среди сот и секторов. Влияние на выбор оказывают межканальные помехи (interchannel ***interference***). Этот тип помех возникает между сигналами, излучаемыми в одной и той же соте (секторе) на разных несущих частотах. Необходимо минимизировать искажения. Этого можно достичь соответствующим подбором частот каналов в каждой соте. Межканальные помехи также тесно связаны с перемещением подвижных станций в границах одной соты и различными расстояниями от подвижных станций до общей базовой станции (эффект ближний - дальний, англ. near-far effect).

4.1. Общие принципы построения систем сотовой связи

Межканальные помехи существенно влияют на качество принимаемого полезного сигнала. Способы уменьшения влияния межканальных помех:

1. ***Распределение канальных частот*** с целью увеличения частотного разноса каналов в данной соте. На практике соседние каналы разделены полосой , где - полоса пропускания приемного фильтра;

2. Использование сложных передающих и приемных фильтров. Это позволяет повысить избирательность приемника;

3. Прецизионное регулирование мощности сигналов, передаваемых базовыми и подвижными станциями по каждому каналу.

4.1. Общие принципы построения систем сотовой связи

Методы распределения каналов

Фиксированное распределение каналов - простейший метод распределения ресурсов системы. При фиксированном распределении каналов установление нового соединения в данной соте возможно только в том случае, если в ней есть незанятые каналы.

4.1. Общие принципы построения систем сотовой связи

Метод простого заимствования каналов - улучшенный вариант фиксированного распределения.

Если все каналы, выделенные соте, заняты, то свободный можно позаимствовать в соседней соте, при условии, что этот канал не интерферирует с уже используемыми.

С момента заимствования канала данной сотой, ряду окружающих сот запрещается использовать заимствованный канал во избежание меж- и внутриканальных помех.

Процессом заимствования управляет ЦКПС. Он блокирует заимствованные каналы в сотах, расположенных через одну или две соты от заимствующей соты. ЦКПС ведет базу данных свободных, заимствованных и блокированных каналов и информирует о них в соответствующие базовые станции.

4.1. Общие принципы построения систем сотовой связи

Метод гибридного распределения каналов устраняет недостатки предыдущего метода. В этом методе каналы в каждой соте делятся на две категории: *первая категория* - каналы, используемые только в данной соте; *вторая категория* - каналы, которые могут быть заимствованы. Соотношение количества каналов в обеих категориях определяется на основе ожидаемого трафика.

Метод заимствования с упорядочиванием - количество каналов, входящих в каждую категорию, динамически меняется в зависимости от объема трафика. Вероятность заимствования присваивается каждому каналу, подлежащему заимствованию.

4.1. Общие принципы построения систем сотовой связи

Метод динамического распределения каналов отсутствуют каналы, постоянно закрепленные за сотами. Каналы выделяются конкретному соединению или последовательно нескольким соединениям. Решение о выделении канала принимается либо ЦКПС, либо ПС. В первом случае речь идет о централизованном управлении; во втором - о распределенном управлении процессом выделения каналов.

Метод гибкого распределения каналов сочетает в себе преимущества фиксированного и динамического распределений. Каждая сота постоянно имеет в своем распоряжении набор каналов, достаточный для обслуживания трафика средней интенсивности. Остальные каналы – по мере изменения интенсивности трафика.

4.1. Общие принципы построения систем сотовой связи

Гибкое распределение каналов с планированием выделение дополнительных каналов планируется заранее с учетом времени суток и расположения соты. Распределение каналов изменяется в заранее установленные моменты, предшествующие критическому возрастанию интенсивности трафика.

Гибкое распределение каналов с прогнозированием интенсивность трафика измеряется в режиме реального времени, и ЦКПС может перераспределить каналы в любой момент времени.

4.2. Технология и архитектура системы сотовой связи GSM

В настоящее время аббревиатура GSM означает ***Global System for Mobile Communication*** (глобальная система подвижной связи).

В настоящее время известны такие спецификации как GSM 850, GSM 900, GSM 1800 и GSM 1900.

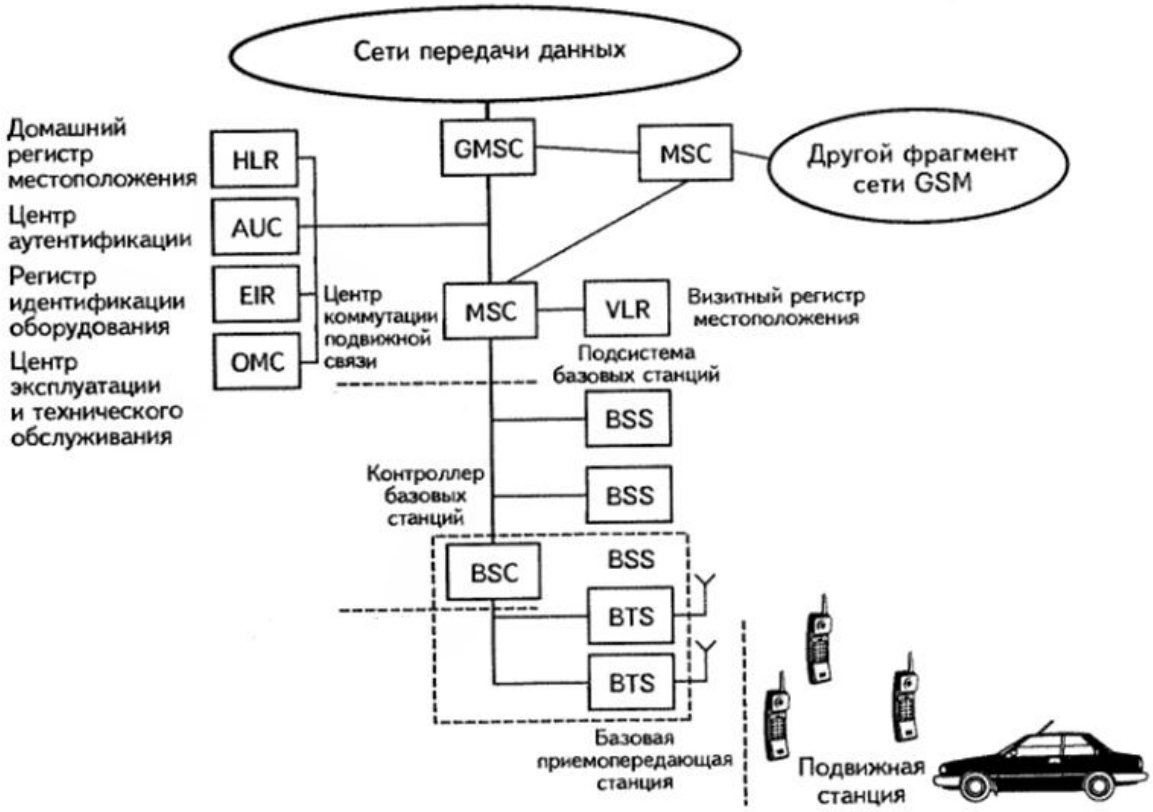
GSM 850 и 1900 нашли применение в США, Канаде, отдельных странах Латинской Америки и Африки.

GSM 900 и 1800 используется в Европе, Азии. Перечисленные спецификации отличаются в основном диапазоном рабочих частот и мощностью излучения *БС* и *ПС*. Далее будут рассмотрены два из них - GSM 900 и 1800.

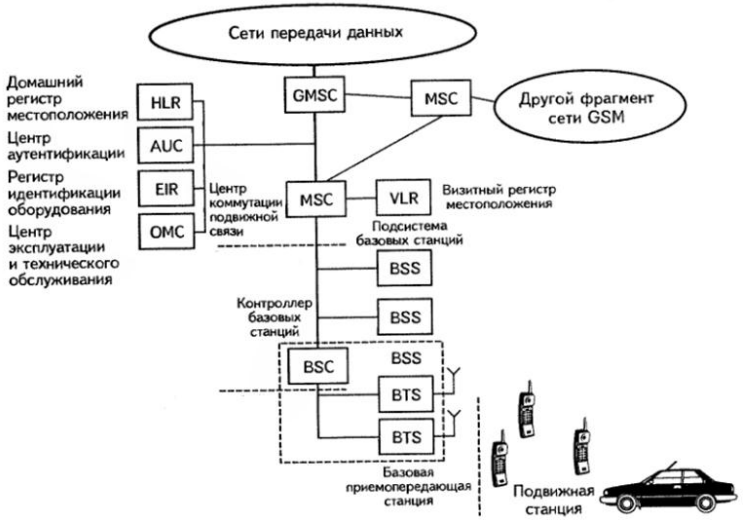
4.2. Технология и архитектура системы сотовой связи GSM

Основы архитектуры GSM

Зона обслуживания системы GSM разделена на фрагменты, каждый из которых обслуживает центр коммутации подвижной связи (***Mobile Switching Center, MSC***) (ЦКПС) - специализированный центр электронной коммутации, к которому добавлены функциональные блоки, решающие задачи, характерные для системы сотовой подвижной связи.



4.2. Технология и архитектура системы сотовой связи GSM



Каждый MSC (ЦКПС) соединен с соответствующим гостевым регистром местоположения или просто гостевым регистром **VLR (Visitor's Location Register)**. Этот регистр содержит необходимую информацию о подвижных станциях, временно расположенных в области обслуживания данного оператора (роуминг).

4.2. Технология и архитектура системы сотовой связи GSM

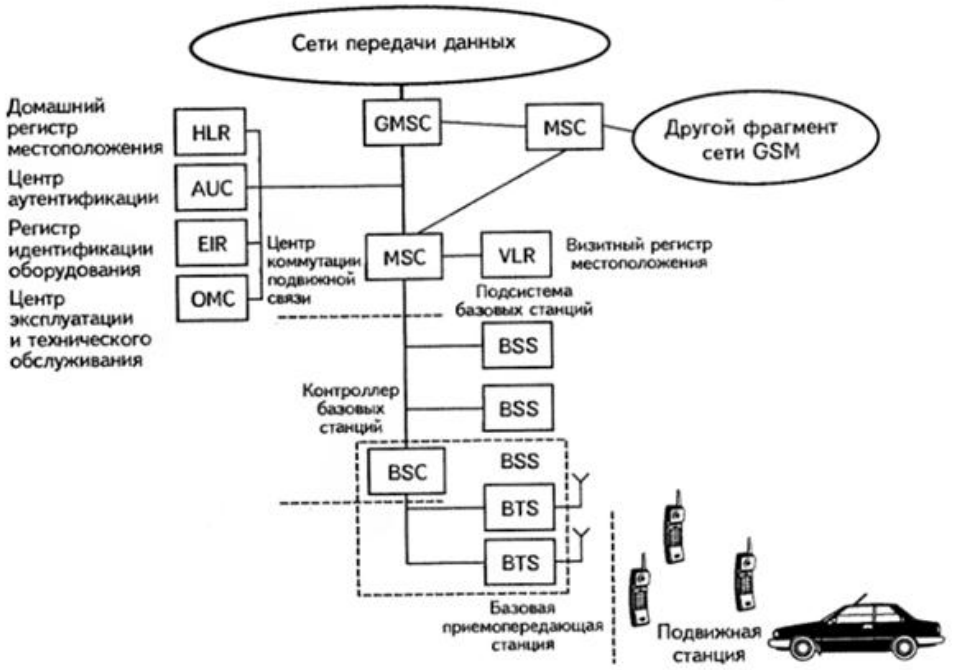
система GSM каждого оператора оборудована тремя другими регистрами:

- **HLR (Home Location Register)** - домашний регистр местоположения - база данных подвижных станций, постоянно зарегистрированных в системе конкретного оператора и наборе услуг предоставляемых этому абоненту. В HLR фиксируется местоположение абонента для организации его вызова, и регистрируются фактически оказанные услуги.

- **AUC (Authentication Center)** - центр аутентификации - база данных, позволяющая определить - разрешен ли допуск к услугам системы абоненту, имеющему данный модуль подлинности - SIM-карту (Subscriber Identity Module);

- **EIR (Equipment Identification Register)** - регистр идентификации оборудования - база данных серийных номеров подвижных станций, используемых в системе. Номера украденных или потерянных телефонов помещаются в **черный список**, что позволяет предотвратить дальнейшее использование в системе этих телефонов.

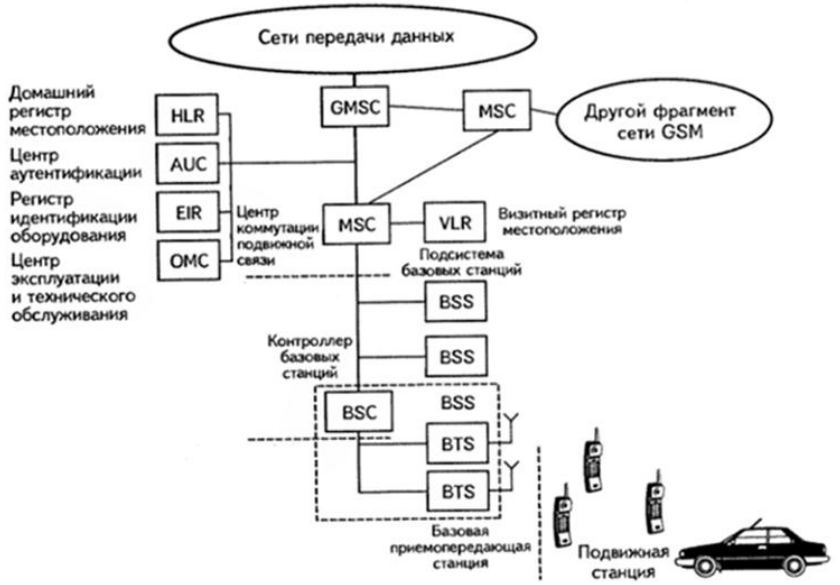
4.2. Технология и архитектура системы сотовой связи GSM



Все MSC (ЦКПС) в сети соединены друг с другом. Один или более MSC, называемые транзитными центрами коммутации подвижной связи **GMSC (Gateway Mobile Switching Center)**, играют роль шлюзов во внешние сети, такие, как, телефонные сети общего назначения.

Каждый MSC контролирует, по крайней мере, одну подсистему базовых станций **BSS (Base Station System)** которая состоит из контроллера базовых станций **BSC (Base Station Controller)** и некоторого количества базовых приемопередающих станций или просто базовых станций **BTS (Base Transceiver Station)** ***(БС)***.

4.2. Технология и архитектура системы сотовой связи GSM



Центр эксплуатации и технического обслуживания **OMC (Operating and Maintenance Center)** обеспечивает работу отдельных элементов сети GSM. Он соединен со всеми элементами коммутационной сети и выполняет функции администрирования, такие, как тарификация и мониторинг трафика, а также принимает необходимые меры в случае отказа отдельных элементов сети.

Одна из наиболее важных задач OMC это управление регистром HLR. В больших сетях имеется более одного OMC, и тогда всей сетью управляет центр управления сетью **NMC (Network Management Center)**. OMC соединяется с другими компонентами сети специальной сетью управления, реализованной по выделенным телефонным линиям или с помощью других сетей фиксированной связи.

4.2. Технология и архитектура системы сотовой связи GSM

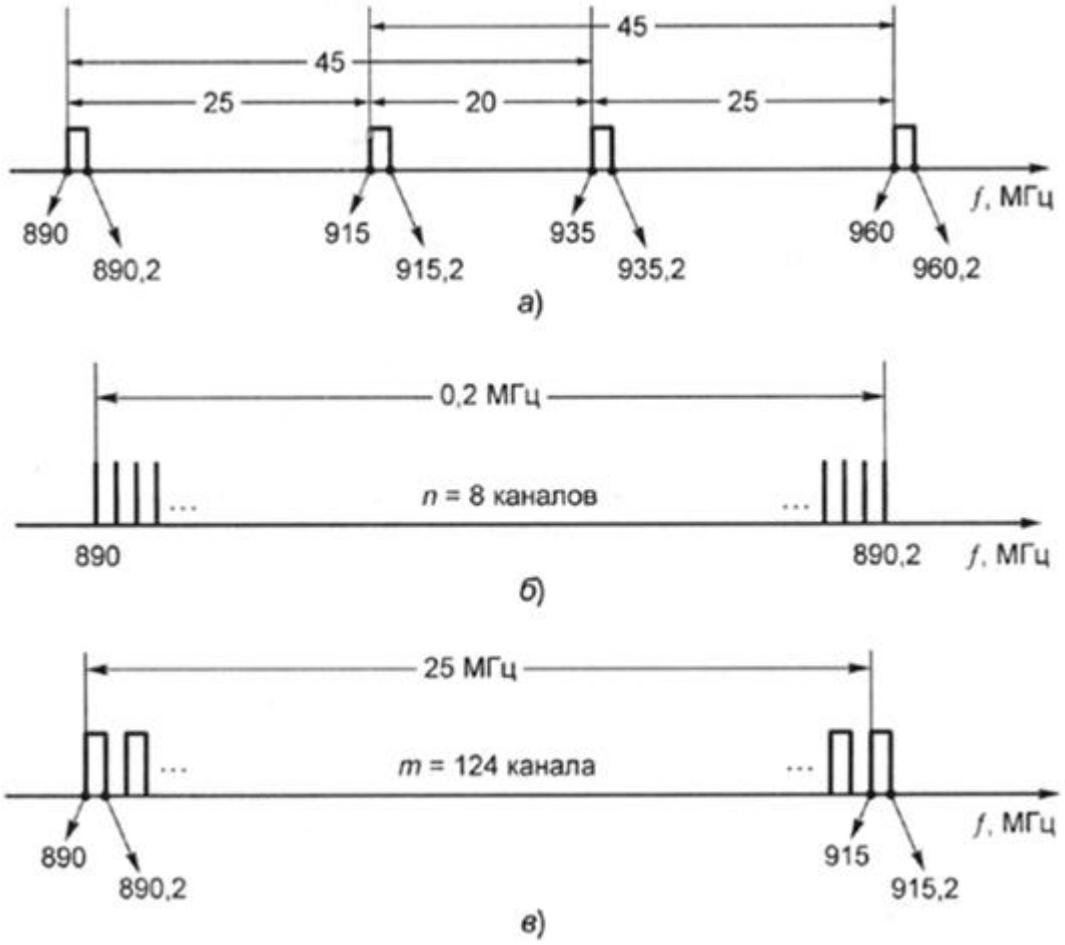
Основные параметры радиопередачи в системе GSM

Пример - стандарта GSM 900. Стандарт предусматривает работу передатчиков в двух диапазонах частот каждый шириной в 25 МГц:

1. Полоса частот 890-915 МГц - для передачи сообщений с ПС на БС (uplink);

2. Полоса частот 935- 960 МГц - для передачи сообщений с БС на ПС (downlink).

В стандарте GSM используется многостанционный доступ FDMA/TDMA. на одной несущей частоте - 8 речевых каналов.

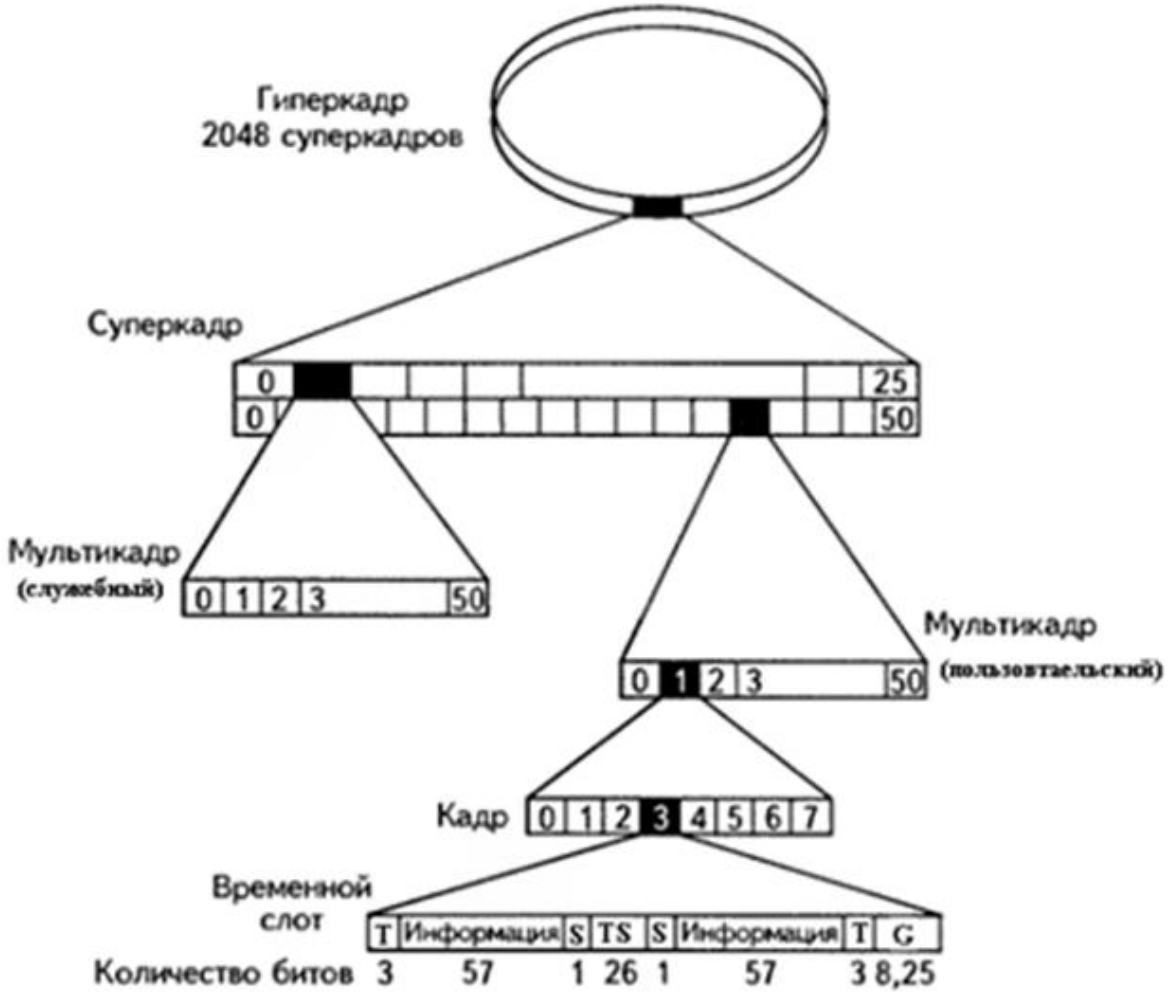


а) разнос между частотами в направлении ПС-БС и в направлении БС-ПС; б) число физических речевых радиоканалов в дуплексном радиоканале; в) число физических дуплексных речевых радиоканалов

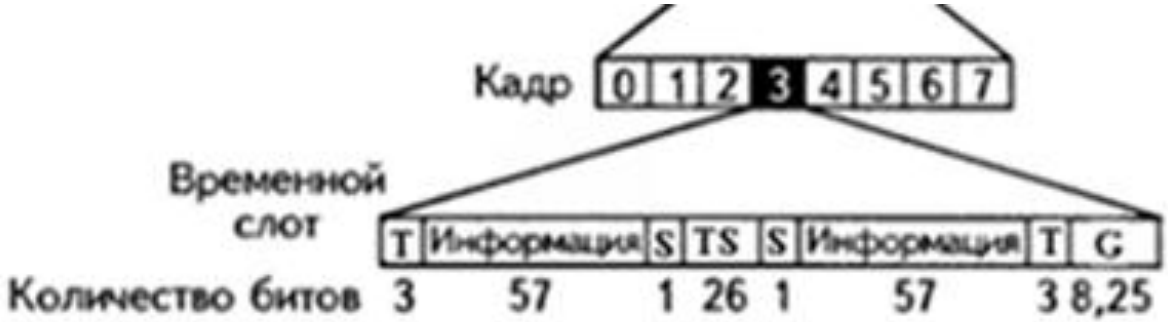
4.2. Технология и архитектура системы сотовой связи GSM

Временная структура системы GSM

Разделение на восемь временных слотов отнюдь не полностью описывает временную структуру системы GSM. **Наименьший временной элемент** - одиночный двоичный импульс (бит), длящийся 3,69 мкс. Скорость передачи данных в системе GSM составляет 270,833 кбит/с. В каждом временном слоте передается пакет из 148 битов. Длительность стандартного временного слота составляет 577 мкс.



4.2. Технология и архитектура системы сотовой связи GSM



Структура временного слота состоит из:

1. **T - Tail bit (хвостовые биты)**. Повторяется два раза. Необходимы как защитные бланки по краям пакета;

2. **S - Stealing flag (скрытые флажки)**. Повторяется два раза. Определяет тип передаваемой информации, т.к. она может как пользовательской так и служебной;

3. **TS - Training Sequence** (обучающая последовательность). Предназначен для оценки качества связи, определения задержек информации между БС и ПС;

4. **G- Guard period (защитный интервал)**.

4.2. Технология и архитектура системы сотовой связи GSM

Алгоритм функционирования систем GPS

1. Когда *ПС* находится в режиме ожидания, ее приемное устройство постоянно сканирует либо все каналы системы, либо только управляющие каналы.

2. Для вызова абонента всеми *БС* фрагмента сети по каналам управления передаются сигналы вызова.

3. *ПС* вызываемого абонента при получении сигнала вызова отвечает по одному из свободных каналов управления.

4. *БС*, принявшие ответный сигнал, передают информацию о его параметрах в центр коммутации *MSC*, который переключает разговор на ту БС, где зафиксирован максимальный уровень сигнала *ПС* вызываемого объекта.

4.2. Технология и архитектура системы сотовой связи GSM

Алгоритм функционирования систем GPS

5. Во время набора номера *ПС* вызываемого абонента занимает один из свободных каналов *БС*, уровень сигнала которой в данный момент максимален.

6. По мере удаления вызываемого абонента от *БС* или в связи с ухудшением условий распространения радиоволн уровень сигнала уменьшается, что ведет к ухудшению качества связи.

7. Улучшение качества разговора достигается путем автоматического переключения вызываемого абонента на другой канал радиосвязи. Аналогичные действия предпринимаются при снижении качества связи из-за влияния помех или при возникновении неисправностей коммутационного оборудования. Для контроля таких ситуаций БС снабжены специальными устройствами, периодически измеряющими уровни сигналов ПС, передающих речевые сигналы, и сравнивающими эти уровни с допустимыми пределами.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Общая характеристика безопасности связи

В стандарте GSM термин «безопасность» понимается как исключение несанкционированного использования системы и обеспечение конфиденциальности переговоров мобильных абонентов. Определены следующие механизмы безопасности в стандарте GSM:

- аутентификация;
- конфиденциальность передачи данных;
- конфиденциальность абонента;
- конфиденциальность направлений соединения абонентов.

Защита сигналов управления и данных пользователя осуществляется только по радиоканалу. Режимы безопасности в стандарте GSM определяются рекомендациями.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Механизмы аутентификации

Для исключения несанкционированного использования ресурсов системы в стандарте GSM реализуются механизмы аутентификации - проверки подлинности абонента.

Каждый мобильный абонент на время пользования системой связи получает стандартный модуль подлинности абонента (SIM-карту), который содержит:

- международный идентификационный номер мобильного абонента (IMSI);
- свой индивидуальный ключ аутентификации (*Ki*);
- алгоритм аутентификации (A_3).

С помощью заложенной в SIM информации в результате взаимного обмена данными между мобильной станцией и сетью осуществляется полный цикл аутентификации и разрешается доступ абонента к сети.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Процедура проверки сетью подлинности абонента реализуется следующим образом.

Сеть передает случайный номер (*RAND*) на мобильную станцию.

Мобильная станция определяет значение отклика (*SRES*), используя *RAND, Ki*, и алгоритм A_3:

SRES = *Ki* [RAND].

Мобильная станция посылает вычисленное значение *SRES* в сеть, которая сверяет значение принятого *SRES* со значением *SRES*, вычисленным сетью. Если оба значения совпадут, мобильная станция сможет осуществлять передачу сообщений. В противном случае связь прервется и индикатор мобильной станции покажет, что опознавание не состоялось.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

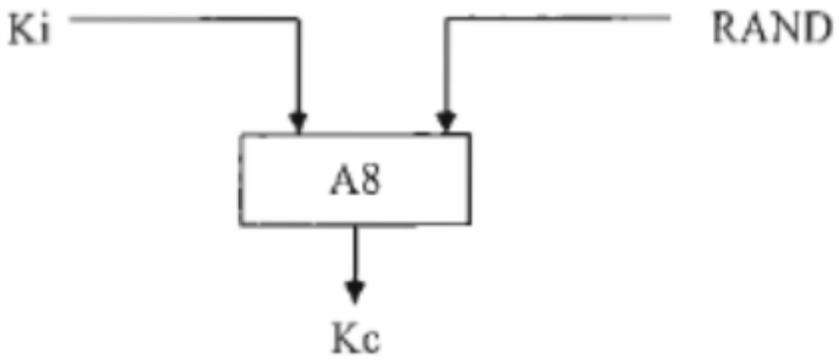
Конфиденциальность передачи данных

***Ключ шифрования*.** Для обеспечения конфиденциальности передаваемой по радиоканалу информации вводится следующий механизм защиты.

Все конфиденциальные сообщения должны передаваться в режиме защиты информации. Алгоритм формирования ключей шифрования (A8) хранится в модуле SIM. После приема случайного номера *RAND* мобильная станция вычисляет, кроме отклика *SRES*, также и ключ шифрования (*Кс*), используя *RAND*, *Ki*, и алгоритм A8:

Кс =К; [RAND].

Ключ шифрования *Кс* не передается по радиоканалу. Как мобильная станция, так и сеть вычисляют ключ шифрования, который используется другими мобильными абонентами. В интересах обеспечения безопасности вычисление *Кс* происходит в *SIM*.



4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Числовая последовательность ключа шифрования.

Кроме случайного числа *RAND*, сеть посылает мобильной станции числовую последовательность ключа шифрования.

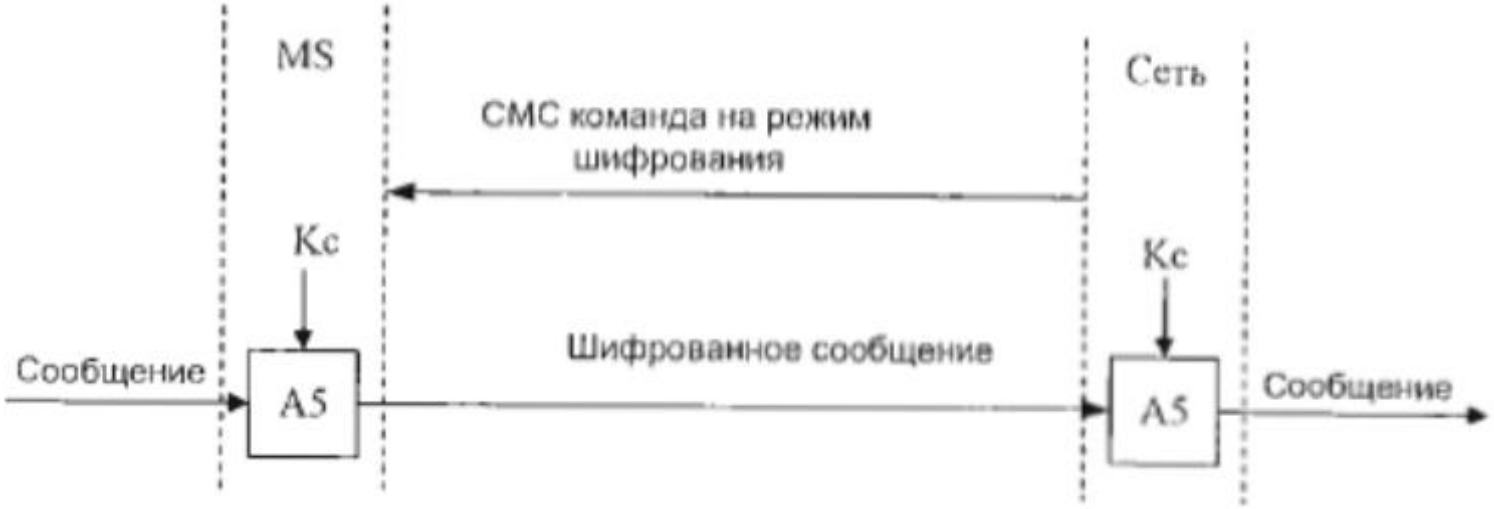
Это число связано с действительным значением *Кс* и позволяет избежать формирования неправильного ключа. Число хранится мобильной станцией и содержится в каждом первом сообщении,·передаваемом в сеть.

Установка режима шифрования. Для установки режима шифрования сеть передает мобильной станции команду CMC (Ciphering Mode Command) на переход в режим шифрования. После получения команды CMC мобильная станция, используя имеющийся у нее ключ, приступает к шифрованию и дешифрованию сообщений. Поток передаваемых данных шифруется бит за битом или поточным шифром, используя алгоритм шифрования A5 и ключ шифрования *Кс*.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Установка режима шифрования. Для установки режима шифрования сеть передает мобильной станции команду CMC (Cipheriпg Mode Command) на переход в режим шифрования. После получения команды CMC мобильная станция, используя имеющийся у нее ключ, приступает к шифрованию и дешифрованию сообщений. Поток передаваемых данных шифруется бит за битом или поточным шифром, используя алгоритм шифрования A5 и ключ шифрования *Кс*.

Процедура установки режима шифрования показана на рис.



4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Обеспечение конфиденциальности абонента

1. Для исключения идентификации абонента путем перехвата сообщений, передаваемых по радиоканалу, каждому абоненту системы связи присваивается «временное удостоверение личности» - временный международный идентификационный номер пользователя (TMSI), который действителен только в пределах зоны расположения (LA). В другой зоне расположения ему присваивается другой TMSI.

2. Если абоненту еще не присвоен временный номер (например, при первом включении мобильной станции), идентификация проводится через международный идентификационный номер (IMSI).

3. После окончания процедуры аутентификации и начала режима шифрования временный идентификационный номер - TMSI передается на мобильную станцию только в зашифрованном виде. Этот TMSI будет использоваться при всех последующих доступах к системе.

4. Если мобильная станция переходит в новую область расположения, то ее TMSI должен передаваться вместе с идентификационным номером зоны (LAI), в которой TMSI был присвоен абоненту.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Обеспечение конфиденциальности абонента при корректировке местоположения

При выполнении процедуры корректировки местоположения по каналам управления осуществляется двухсторонний обмен между MS- и BTS-служебными сообщениями, содержащими временные номера абонентов TMSI. В этом случае в радиоканале необходимо обеспечить защиту информации о переименовании TMSI и их принадлежности конкретному абоненту.

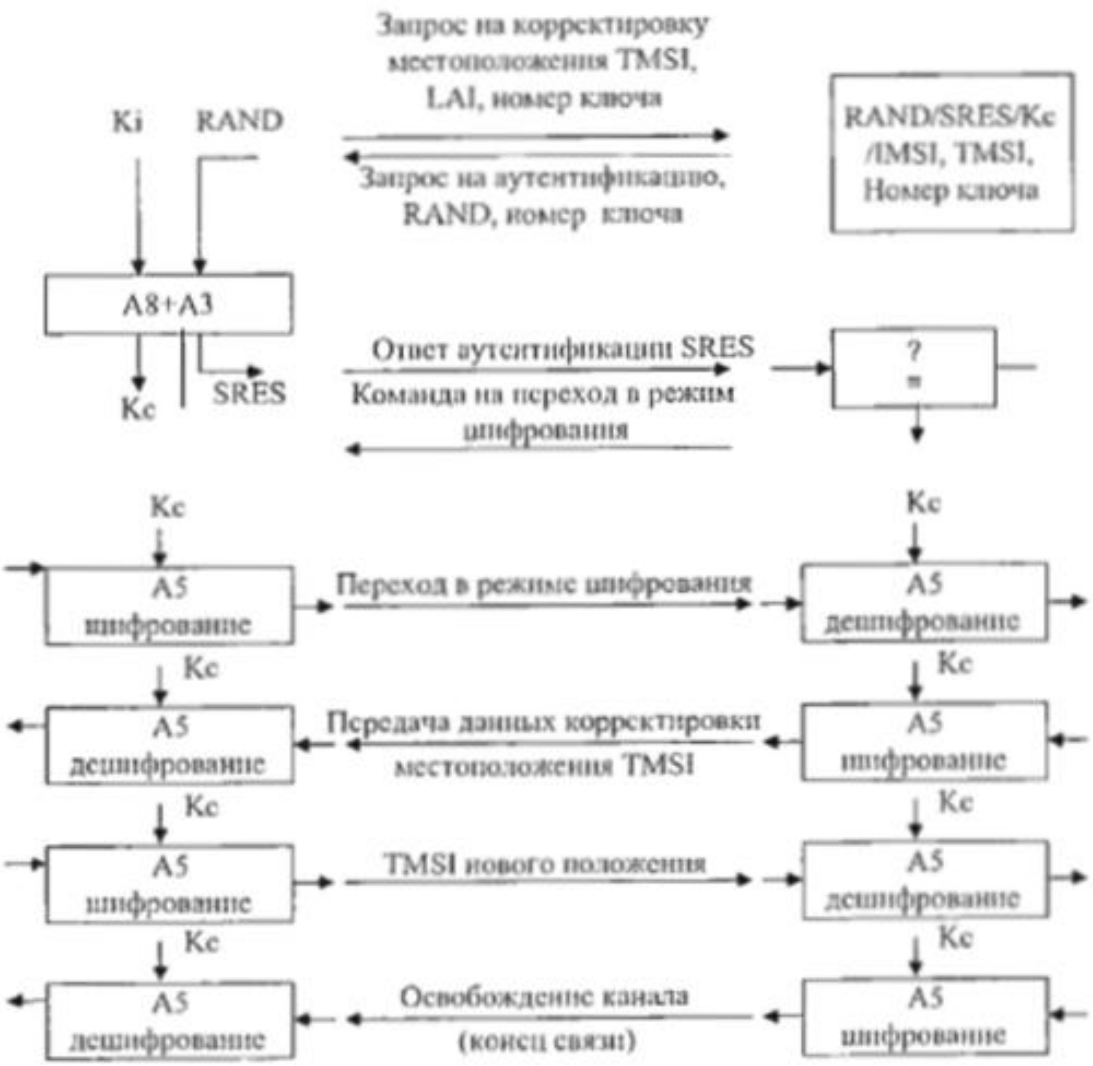
Рассмотрим, как обеспечивается конфиденциальность в процедуре корректировки местоположения в случае, когда абонент проводит сеанс связи и при этом осуществляет перемещение из одной зоны в другую.

1. Мобильная станция уже зарегистрирована в режиме перемещения VLR с временным набором TMSI, соответствующим прежней зоне расположения.

2.При входе в новую зону расположения осуществляется процедура опознавания, которая проводится по старому, зашифрованному в радиоканале TMSI, передаваемому одновременно с наименованием зоны расположения LAI.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

3. LAI дает информацию центру коммутации и центру управления о направлении перемещения мобильной станции и позволяет запросить прежнюю зону расположения о статусе абонента и его данные, исключив обмен этими служебными сообщениями по радиоканалам управления. При этом по каналу связи сообщение передается как зашифрованный информационный текст с прерыванием сообщения в процессе «Эстафетной передачи» на 100-150 мс.



4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Общий состав конфиденциальной информации в сетях GSM и ее распределение в аппаратных средствах

В соответствии с рассмотренными механизмами безопасности, действующими в стандарте GSM, конфиденциальной (защищаемой) считается следующая информация:

RAND - случайное число, используемое для аутентификации мобильного абонента;

SRES - значение отклика - ответ мобильной станции на полученное случайное число;

K_i - индивидуальный ключ аутентификации пользователя, применяемый для вычисления значения отклика и ключа шифрования;

K_c – ключ шифрования, используемый для шифрования-дешифрования сообщений, сигналов управления и данных пользователя в радио канале;

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

A3 - алгоритм аутентификации, применяемый для вычисления значения отклика из случайного числа с использованием ключа *Ki*;

A8 - алгоритм формирования ключа шифрования, используемый для вычисления ключа *Kc* из случайного числа с использованием ключа *Ki*;

A5 - алгоритм шифрования/дешифрования сообщений, сигналов управления и данных пользователя с использованием ключа *Kc*;

CKSN - номер ключевой последовательности шифрования, указывает на действительное число *Kc*, чтобы избежать применения разных ключей на передающей и приемной сторонах;

TMSI - временный международный идентификационный номер пользователя.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Таблица Распределение конфиденциальной информации в аппаратных средствах GSM

№ п/п	Аппаратные средства	Вид информации
1.	Мобильная станция (без SIM)	*A5*
2.	Модуль подлинности абонента (SIM)	*A3; A8; IMSI; K_i; TMSI/LAI; K_c/CKSN*
3.	Центр аутентификации (AUC)	*A3; A8; IMSI/K_i*
4.	Регистр местоположения (HLR)	Группа *IMSI/RAND/SRES/K_c*
5.	Регистр перемещения (VRL)	Группы *IMSI/RAND/SRES/K_c IMSI/TMSI/LAI/K_c/CKSN*
6.	Центр коммутации (MSC)	*A5; TMSI/IMSI; K_c*
7.	Контроллер базовой станции (BSC)	*A5; TMSI/IMSI; K_c*

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Обеспечение безопасности при обмене сообщениями между HLR, VLR и MS

Основным объектом, отвечающим за все аспекты безопасности, является центр аутентификации (AUC). Этот центр может быть отдельным объектом или входить в состав какого-либо оборудования, например в регистр местоположения (HLR).

AUC решает следующие задачи:

• формирование индивидуальных ключей аутентификации пользователей *Ki* и соответствующих им международных идентификационных номеров абонентов (*IMSI*);

• формирование набора *RAND/SRESI Kc* для каждого *IMSI* и раскрытие при необходимости этих групп для *HLR*.

Если мобильная станция переходит в новую зону расположения, новый VLR должен получить информацию об этой мобильной станции. Это может быть обеспечено следующими двумя способами:

• Мобильная станция проводит процедуру идентификации по своему международному номеру *IMSI*. При этом VLR запрашивает у регистра местоположения HLR группы данных *RAND/SRES/Kc*, принадлежащих к данному *IMSI*.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

• Мобильная станция проводит процедуру аутентификации, используя прежний временный номер TMSI с наименованием зоны рас положения *LAI*. Новый *VLR* запрашивает прежний *VLR* для посылки международного номера *IMSI* и оставшихся групп из *RAND/SRESI/Kc*, принадлежащих к этим TMSI/LAI.

Если мобильный абонент остается на более длительный период в VLR, тогда после некоторого количества доступов с аутентификацией VLR из соображений обеспечения информационной безопасности потребует новые группы *RAND/SRESI/Kc* от *HLR*.

Проверка аутентификации выполняется в *VLR*, который посылает *RAND* на коммутационный центр (*MSC*) и принимает соответствующие отклики *SRES*. После положительной аутентификации *TMSI* размещается с *IMSI*. *TMSI* и используемый ключ шифрования *Kc* посылаются в центр коммутации (*MSC*).

Все эти процедуры определены в Рекомендации GSM 09.02.

4.3. Особенности обеспечения безопасности информации в системах мобильной связи на примере стандарта GSM

Модуль подлинности абонента

Модуль подлинности абонента *SIM* содержит полный объем информации о конкретном абоненте. *SIM* реализуется конструктивно в виде карточки со встроенной электронной схемой. Введение *SIM* делает мобильную станцию универсальной, так как любой абонент, употребляя свою личную *SIM*-карту, может обеспечить доступ к сети GSM через любую мобильную станцию.

Несанкционированное использование SIM исключается введением в *SIM* индивидуального идентификационного номера (*PIN*), который присваивается пользователю при получении разрешения на работу в системе связи и регистрации его индивидуального абонентского устройства.

4.4. Беспроводные сети на основе технологии GPRS

GPRS **-** это доступ с мобильного телефона в Интернет с приемлемой скоростью передачи данных, быстрым соединением и тарификацией по количеству переданных/полученных данных.

Сокращение ***GPRS*** расшифровывается как ***General Packet Radio Service***, что в переводе на русский означает: **Общий Пакетный Радиосервис**, т.е. технология пакетной передачи данных посредством сотовой связи. Услуга GPRS позволяет создать постоянное подключение к сети Интернет.

Отличие от обычного Интернет состоит в ***способе передачи***. В GPRS пакеты передаются по незанятым голосовым каналам, однако, из-за этого при сильной нагрузке сети оператора скорость может заметно упасть.

GPRS - это стандарт ETSI (***European Telecommunications Standards Institute***) для пакетной коммутации в системах GSM. Технология GSM использует вариацию TDMA (Time Division Multiple Access) и является наиболее широко используемой из трех основных цифровых беспроводных технологий (TDMA, GSM и CDMA).

GPRS еще называют ***накладывающейся технологией***, распространяемой на сетях GSM, CDMA и TDMA. Технология пакетной коммутации основана на методах IP и X.25. Пакетная коммутация GPRS работает в целом так же, как и пакетная коммутация IP, т. е. данные расщепляются на пакеты и пересылаются по назначению разными путями по сети, затем снова собираются на принимающей стороне. Пакетная коммутация GPRS допускает любой существующий трафик IP или X.25 для пересылки данных через радиосеть GPRS.

4.4. Беспроводные сети на основе технологии GPRS

Безопасность в GPRS

GPRS строится на проверенной на практике модели аутентификации и авторизации, используемой GSM т.е. пользователя аутентифицируют, используя секретную информацию, содержащуюся на смарт-карте, называемой «модуль идентификации абонента» (***Subscriber Identity Module, SIM***).

GPRS дает возможность дополнительной аутентификации путем использования таких протоколов, как ***RADIUS*** - перед тем, как абонентам будет разрешен доступ в Интернет или корпоративную сеть данных.

GPRS поддерживает шифрование пользовательских данных при передаче через беспроводный интерфейс с мобильного терминала на SGSN. Кроме того, может иметь место высокоуровневое сквозное шифрование ***VPN*** (***Virtual Private Network***), когда пользователь подсоединяется к частной корпоративной сети.

Аутентификация GPRS. В SIM-карте мобильного телефона и на базовой станции реализован специальный алгоритм. Суть его заключается в следующем. В начале процедуры базовая станция отправляет на телефон случайную последовательность цифр. SIM-карта преобразовывает его в соответствии с алгоритмом, используя при этом собственный секретный ключ, а получившееся значение **SRES (Signed RESult - подписанный результат)** отправляет обратно. Точно такие же преобразования производятся и на базовой станции. Если оба значения SRES совпадают, то делается вывод о допуске данного телефона в сеть.

4.4. Беспроводные сети на основе технологии GPRS

Безопасность в GPRS

В сети GPRS используется **два типа каналов связи.**

Первый из них - радиоэфир, через который общаются между собой базовые и мобильные станции. Данный канал является наиболее уязвимым местом GPRS-сети.

Именно поэтому абсолютно вся информация, передающаяся по радиоканалу, предварительно зашифровывается с помощью специальных алгоритмов. В сетях GPRS для этого используются стандарты GEA1, GEA2, GEA3 - «близкие родственники» криптоалгоритмов GSM. Технология же GEA3 считается не взломанной.

Ко второму типу относятся каналы связи, использующиеся для передачи данных между внутренними узлами сети. Для обеспечения его безопасности был разработан и внедрен в GPRS специальный протокол **GTP (GPRS Tunneling Protocol)**. Он отличается от привычных хакерам технологий. Кроме того, внутренние компьютеры сети GPRS используют для маршрутизации принцип частных IP-адресов согласно международному стандарту RFC 1918.

Под **внешними угрозами** понимаются вирусы или удаленные атаки. Проблема решается с помощью обычных средств: антивирусной программы с постоянно обновляемыми базами данных и корректно настроенного файрвола.

Нерешенной остается только одна проблема. Речь идет о возможности проведения на узел маршрутизации профессиональной ***DDoS-атаки***. От этого не застрахован ни один сервер в Интернет.

4.4. Беспроводные сети на основе технологии GPRS

Безопасность в GPRS

Узел маршрутизации выполняет еще одну функцию. Он отвечает за связи своей сети GPRS с другими такими же сетями. Для того чтобы защитить эти каналы, используются так называемые пограничные шлюзы (**BG - border gateway**). Суть действия этого программного обеспечения похожа на работу файрвола. Администратор устанавливает правила обмена трафиком, вводит доверенные сети, подключает системы роуминга и т.п. После этого вся система будет защищена от атак из других сетей GPRS.

4.6. Технологии EDGE

Технология EDGE (Enhanced Data Rates for GSM Evolution - «передача данных на повышенной скорости») - следующий шаг развития мобильных систем передачи данных.

Технология EDGE позволит осуществлять перекачку информации на скоростях до 384 кбит/с в восьми GSM-каналах (48 кбит/с на канал). Для внедрения EDGE «поверх» GPRS операторы заменяют аппаратуру базовых станций, а пользователи – должны приобрести поддерживающие EDGE телефонные аппараты.

Радиоинтерфейс EDGE надстраивается над существующей инфраструктурой GSM и использует те же полосы частот.

В зависимости от качества связи предусмотрено 9 алгоритмов кодирования: от MCS-1 до MCS-9 (последний обладает самой малой избыточностью кодирования, соответственно - самый быстрый).

Таким образом, технология EGPRS (EDGE) способна обеспечить каждому абоненту, как высокий уровень обслуживания, так и широкую полосу пропускания.

Технологии GPRS и EDGE считают лишь промежуточными этапами миграции к 3G и зачастую их называют переходными технологиями поколения 2.5G.

4.7. Технологии 3G

Одно из главнейших требований - сеть 3G должна передавать данные от абонента и обратно со скоростью до 2,048 Мбит/с при низкой мобильности (менее 3 км/ч) и локальной зоне покрытая и до 144 кбит/с при высокой мобильности (до 120 км/ч) и широкой зоне покрытия.

Сегодня в мире существуют ***две основные конкурирующие концепции 3G:***

1. **UMTS (Universal Mobile Telecommunications Systems)** - универсальная мобильная телекоммуникационная система), поддерживаемая европейскими странами, и

2. **CDMA 2000 (Code Division Multiple Access)** - мультидоступ с кодовым разделением каналов), сторонниками которой традиционно являются азиатские страны и США.

В принципе, эти две технологии предполагают два различных подхода к организации сетей 3G:

- революционный (UMTS) и

- эволюционный (разновидности CDMA - CDMA 2000, CDMA 2000 IX, CDMA 2000 IX EvDo).

Эволюционный путь подразумевает сохранение частот и постепенный переход к новым технологиям путем наращивания технических мощностей оператора.

UMTS - совершенно новый стандарт.

CDMA, предложенные для 3G, являются развитием технологии второго поколения GSM.

4.8. Технология LTE

***Особенности LTE*:**

1. **Р**адиоинтерфейс LTE обеспечивает улучшенные технические характеристики.

2. Ширина полосы пропускания варьирует от 1,4 до 20 МГц, что позволяет удовлетворить потребностям разных операторов связи, обладающих различными полосами пропускания.

3. Оборудование LTE одновременно поддерживает не менее 200 активных соединений (т.е. 200 телефонных звонков) на каждую 5-МГц ячейку.

4. LTE улучшает эффективность использования радиочастотного спектра, т.е. возрастает объем данных, передаваемых в заданном диапазоне частот.

5. LTE позволяет достичь внушительных агрегатных скоростей передачи данных – до 50 Мбит/с для восходящего соединения (от абонента до базовой станции) и до 100 Мбит/с для нисходящего соединения (от базовой станции к абоненту) (в полосе 20 МГц).

6. Обеспечивается поддержка соединений для абонентов, движущихся со скоростью до 350 км/ч. Зона покрытия одной БС – до 30 км в штатном режиме, но возможна работа с ячейками радиусом более 100 км. Поддерживаются многоантенные системы MIMO.

7. Спецификация LTE уже содержит большую часть функций, изначально предназначавшихся для систем 4G, поэтому ее иногда именуют «технологией 3,9G». Но развитие технологии LTE продолжается. Уже разрабатываются спецификации следующего поколения, так называемые ***LTE-Advanced***.

4.8. Технология LTE

Принципы построения радиоинтерфейса по технологии LTE:

LTE базируется на трех основных технологиях:

- мультиплексирование посредством ортогональных несущих OFDM (Orthogonal Frequency-Division Multiplexing);

- многоантенные системы MIMO (Multiple Input Multiple Output);

- эволюционная системная архитектура сети (System Architecture Evolution).

В **LTE** дуплексное разделение каналов может быть как частотным (FDD), так и временным (TDD). Это позволяет операторам очень гибко использовать частотный ресурс. Поддержка FDD очень удобна для традиционных сотовых операторов, поскольку у них спаренные частоты есть «по определению» – так организованы практически все существующие системы сотовой связи.

В LTE используется модуляция OFDM, хорошо исследованная в системах DVB, Wi-Fi и WiMAX.

4.8. Технология LTE

Сетевая архитектура SAE:

Для технологии LTE консорциум 3GPP предложил новую сетевую инфраструктуру (**SAE – System Architecture Evolution**). Цель и сущность концепции SAE – эффективная поддержка широкого коммерческого использования любых услуг на базе IP и обеспечение непрерывного обслуживания абонента при его перемещении между сетями беспроводного доступа, которые не обязательно соответствуют стандартам 3GPP (GSM, UMTS, WCDMA и т.д.)

В сети с архитектурой SAE могут применяться узлы только двух типов – ***базовые станции (evolved NodeB, eNodeB***) и ***шлюзы доступа (Access Gateway, AGW)***. Уменьшение числа типов узлов позволит операторам снизить расходы как на развертывание сетей LTE/SAE, так и на их последующую эксплуатацию.

Предложенные архитектурные изменения позволяют значительно уменьшить задержки передачи данных, которые особенно критичны для таких приложений, как VoIP или онлайновые интерактивные игры.

В частности, задержки радиосети при передаче данных пользователя не должны превышать 10 мс (5 мс для коротких IP-пакетов при небольшой сетевой нагрузке). Эти значения, по крайней мере, на 50% лучше аналогичных показателей наиболее совершенных сетей 3G.

Контрольные вопросы:

1.
2.
3.
4.

Литература:

1.
2.
3.
4.