МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ
Кафедра программного обеспечения информационных технологий

А.А. Иванюк, Ю.В. Климец

МЕТОДИЧЕСКОЕ ПОСОБИЕ

по курсу "Системы телекоммуникаций"
для студентов специальности
"Программное обеспечение информационных технологий"

Минск 2001

УДК 681.3

А.А. Иванюк, Ю.В. Климец, Методическое пособие по курсу "Системы телекоммуникаций" для студентов специальности "Программное обеспечение информационных технологий". - Мн.: БГУИР, 2001. - 49 с.

Методическое пособие является дополнительным учебным материалом для студентов, изучающих вопросы современных систем телекоммуникаций. В данном методическом пособии рассматриваются вопросы организации связи в системах сотовой связи GSM.

Ил. 11, список лит. - 6 назв.

Введение.

Когда в 1991 г. появились первые сети GSM (Под аббревиатурой GSM будем подразумевать любые системы, основанные на технологии GSM, такие как GSM-900, DCS-1800 и PCS-1900.), главное внимание уделялось обеспечению ими услуг речевой связи на достойном уровне по сравнению с существовавшими тогда аналоговыми сотовыми системами. Однако уже с самого начала технология GSM была способна предложить несколько новых видов услуг, которые незамедлительно привлекли внимание определенной категории пользователей. Наиболее существенными нововведениями стали возможности шифрования передаваемой информации и роуминга по всей Европе.

Шифрование привлекло к GSM многих бизнесменов, которые впервые смогли активно использовать сотовую связь. Роуминг же заинтересовал тех, кому приходилось часто путешествовать, и кто хотел пользоваться одной-единственной телефонной трубкой в любой точке Европы. В то же время в базовой области голосовой связи GSM предложила две группы дополнительных услуг: перенаправление и запрещение звонков.

Следующим шагом развития GSM было введение услуг пересылки коротких сообщений (Short Message Service - SMS) и передачи данных. Сначала возможности услуг SMS ограничивались уведомлением о поступлении сообщения в ящик голосовой почты. И только недавно, начиная с 1995 г., сервис SMS стал расширяться. Сегодня пользователи систем GSM имеют возможность посылать друг другу короткие сообщения непосредственно с телефонной трубки или через компьютерные сети. Период с конца 1994 г. до начала 1995 г. - время бурного развития услуг передачи данных. Это было обусловлено появлением привлекательных радиотелефонов и тем, что значительное число сетей GSM стали способны поддерживать такие услуги.

Сегодня абоненты сетей GSM могут воспользоваться услугами мобильного модема/факса со скоростью передачи данных до 9,6 Кбит/с. Широкое распространение портативных ПК позволяет абонентам сетей GSM получать доступ к компьютерным системам их офисов, а также посылать и принимать сообщения электронной почты через сети GSM.

Изначально развитие GSM планировалось таким образом, что любая новая услуга или техническое новшество должны были вводиться одновременно во всех сетях GSM. Это привело к так называемому поэтапному развитию GSM. Введение в строй сетей GSM в 1991 г. было, фактически, первым этапом (phase 1). Второй этап (phase 2) развития GSM обеспечил такие дополнительные услуги, как, скажем, определение номера вызывающего абонента, удержание линии, групповой вызов, определение закрытой группы абонентов, выдача информации о плате за разговор. Этот этап также предполагает расширение полосы пропускания для систем GSM-900. Другое важное новшество, которое будет реализовано вскоре после завершения второго этапа, - кодирование речи с половинной скоростью. Этот шаг направлен на увеличение пропускной способности систем GSM. Но, несмотря на планируемое поэтапное введение новых услуг, некоторые предусматриваемые вторым этапом услуги, скажем определение номера, уже стали доступны пользователям.

Следующий после второго этапа - этап 2+ (phase 2+), характеризующийся тем, что новые функциональные возможности будут стандартизироваться и внедряться сразу же после подготовки их технических описаний. В Европейском институте стандартизации электросвязи (ETSI) сейчас ведется работа над 60 предложениями для GSM этапа 2+, среди которых:

1. улучшенное полноскоростное кодирование речи;
2. высокоскоростная передача данных по коммутируемым каналам (High Speed Circuit Switched Data - HSCSD);

3. пакетная передача данных (General Packet Radio Service - GPRS);
4. сжатие данных; групповые и широковещательные вызовы; взаимодействие между системами GSM и DECT.

1. Общие характеристики стандарта GSM.

В соответствии с рекомендацией CEPT 1980 г., касающейся использования спектра частот подвижной связи в диапазоне частот 862-960 МГц, стандарт GSM на цифровую общеевропейскую (глобальную) сотовую систему наземной подвижной связи предусматривает работу передатчиков в двух диапазонах частот: 890-915 МГц (для передатчиков подвижных станций - MS), 935-960 МГц (для передатчиков базовых станций - BTS) [1.1, 1.2].

В стандарте GSM используется узкополосный многостанционный доступ с временным разделением каналов (NB TDMA). В структуре TDMA кадра содержится 8 временных позиций в каждой из 124 несущих частот.

Для защиты от ошибок в радиоканалах при передаче информационных сообщений применяется блочное и сверточное кодирование с перемежением. Повышение эффективности кодирования и перемежения при малой скорости перемещения подвижных станций достигается медленным переключением рабочих частот (SFH) в процессе сеанса связи со скоростью 217 скачков в секунду.

Для борьбы с интерференционными замираниями принимаемых сигналов, вызванными многолучевым распространением радиоволн в условиях города, в аппаратуре связи используются эквалайзеры, обеспечивающие выравнивание импульсных сигналов со среднеквадратическим отклонением времени задержки до 16 мкс.

Система синхронизации рассчитана на компенсацию абсолютного времени задержки сигналов до 233 мкс, что соответствует максимальной дальности связи или максимальному радиусу ячейки (соты) 35 км.

В стандарте GSM выбрана гауссовская частотная модуляция с минимальным частотным сдвигом (GMSK). Обработка речи осуществляется в рамках принятой системы прерывистой передачи речи (DTX), которая обеспечивает включение передатчика только при наличии речевого сигнала и отключение передатчика в паузах и в конце разговора.

В качестве речепреобразующего устройства выбран речевой кодек с долговременным предсказанием и линейным предикативным кодированием с предсказанием (RPE/LTR-LTP-кодек). Общая скорость преобразования речевого сигнала - 13 кбит/с.

В стандарте GSM достигается высокая степень безопасности передачи сообщенийза счет их шифрования.

В целом система связи, действующая в стандарте GSM, рассчитана на ее использование в различных сферах. Она предоставляет пользователям широкий диапазон услуг и возможность применять разнообразное оборудование для передачи речевых сообщений и данных, вызывных и аварийных сигналов, а также подключаться к телефонным сетям общего пользования (PSTN), сетям передачи данных (PDN) и цифровым сетям с интеграцией служб (ISDN).

Приведем основные характеристики стандарта GSM:

1. частоты передачи подвижной станции - 890-915 МГц;
2. частоты приема подвижной станции - 935-960 МГц;
3. дуплексный разнос частот приема и передачи - 45 МГц;
4. скорость передачи сообщений в радиоканале - 270 833 кбит/с;
5. скорость преобразования речевого кодека - 13 кбит/с;
6. ширина полосы канала связи - 200 кГц;
7. максимальное количество каналов связи – 124;

8. вид модуляции – GMSK;
9. вид речевого кодека - RPE/LTP;
10. максимальный радиус соты – до 35 км;
11. схема организации каналов - комбинированная TDMA/FDMA.

2. Функциональная схема системы сотовой связи и ее элементы.

Система сотовой связи сроится в виде совокупности ячеек, или сот, покрывающих обслуживающую территорию (город и пригород). Ячейки обычно схематически изображаются в виде равновеликих правильных 6-угольников, что очень напоминает структуру пчелиных сот (рис. 1).

Сотовая структура системы непосредственно связана с принципом повторного использования частот, на основании которого и строится иерархическая структура всей системы. В центре каждой соты находится базовая станция, которая обслуживает все подвижные (мобильные) абонентские станции. При перемещении абонента из одной соты в другую происходит передача его обслуживания от одной базовой станции к другой. Все базовые станции системы замыкаются на центр коммутации, через который можно коммутироваться с наземными службами, такими как обычная городская телефонная сеть.

Следует отметить, что данная структура слегка абстрактна, т.к. в реальном мире соты никогда не бывают строгой геометрической формы, а имеют вид неправильных кривых, зависящих от условий распространения и затухания радиоволн. Также границы сот вообще не являются четко определенными. Точно также и положение базовой станции лишь приблизительно совпадает с геометрическим центром соты.

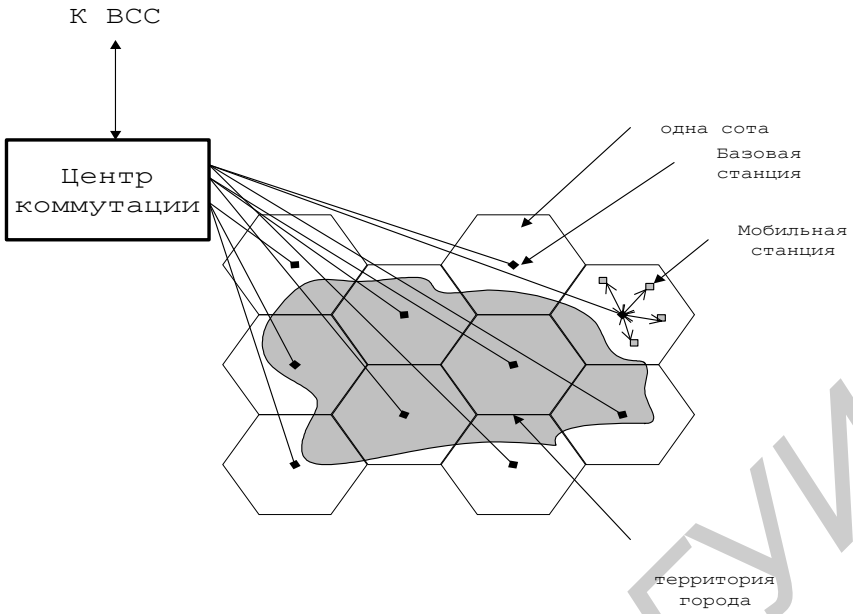


Рис. 1. Организация сотовой связи

В простейшем случае система сотовой связи содержит один центр коммутации, при котором имеется домашний регистр, и система связи обслуживает относительно небольшую замкнутую территорию (город), с которой не граничат территории, обслуживаемые другими системами. Территорию города также может покрывать не один, а несколько центров коммутации, из которых только при головном центре имеется домашний регистр, но обслуживаемая система по-прежнему не граничит с территориями других систем.

При перемещении абонента между сотами одной системы происходит передача обслуживания, а при перемещении на территории других систем - роуминг. Если на покрываемой территории находится несколько систем, и каждая система со своим домашним регистром, то при перемещении абонента из одной системы в другую может иметь место так называемая межсистемная передача обслуживания. Как для роумигна, так и для межсистемной передачи обслуживания необходима аппаратура совместимости систем (принадлежность их к общему стандарту сотовой связи).

В стандарте GSM используется понятие система базовой станции (СБС), в которую входит контроллер базовой станции (КБС) и несколько базовых приемопередающих станций (БППС). В частности, три БППС, расположенные в одном месте и замыкающиеся на один КБС, могут обслуживать каждая свой 120-градусный азимутальный сектор в пределах своей соты и т.п. (рис. 2).

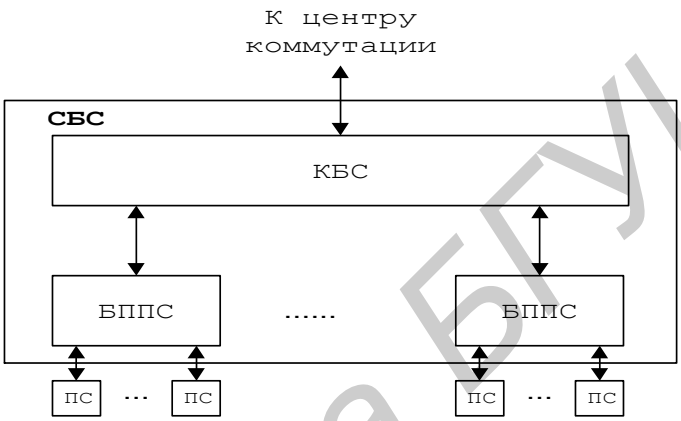


Рис. 2. Система базовой станции

Блок-схема подвижной станции приведена на рис. 3. В ее состав входят: блок управления, приемопередающий блок, антенный блок. Приемопередающий блок в свою очередь включает передатчик, приемник, синтезатор частот и логический блок.

Антенный блок - включает в себя антенну - в простейшем случае четвертьволновой штырь, и коммутатор прием-передача, который может представлять собой электронный коммутатор, подключающий антенну либо на выход передатчика, либо на вход приемника, поскольку подвижная станция цифровой системы никогда не работает на прием и передачу одновременно.

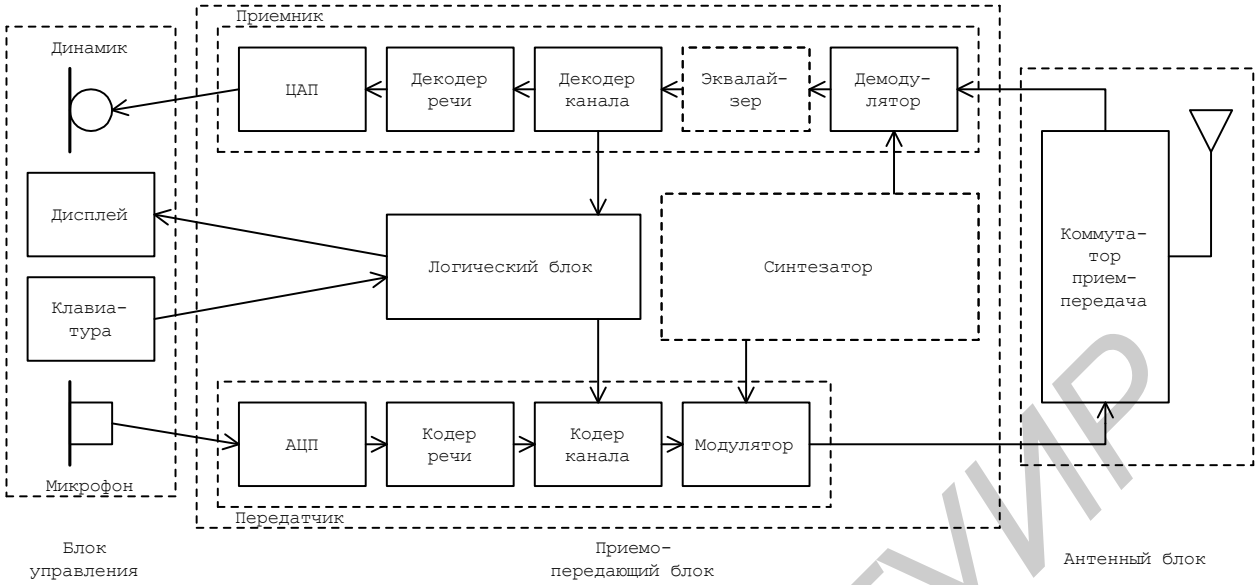


Рис. 3. Блок-схема подвижной станции

Блок управления: он включает в себя микротелефонную трубку – микрофон и динамик, клавиатуру и дисплей. Клавиатура служит для набора номера телефона вызываемого абонента, а также команд, определяющих режим работы подвижной станции. Дисплей служит для отображения различной информации.

Приемопередающий блок: состоит из приемника и передатчика.

Передатчик: в состав входят АЦП, преобразующий в цифровую форму сигнал с выхода микрофона, и вся последующая обработка и передача речи производится в цифровой форме, вплоть до обратного ЦА преобразования. **Кодер речи** осуществляет кодирование сигнала речи – преобразование сигнала, имеющего цифровую форму, по определенным законам с целью сокращения его избыточности, т.е. целью сокращения объема информации, передаваемой по каналу связи. **Кодер канала** – добавляет в цифровой сигнал, получаемый с выхода кодера речи, дополнительную (избыточную) информацию, предназначенную для защиты от ошибок при передаче сигнала по линии связи; с той же целью информация подвергается определенной переупаковке

(перемежению); кроме того, кодер канала вводит в состав передаваемого сигнала информацию управления, поступающую от логического блока. **Модулятор** – осуществляет перенос информации кодированного сигнала на несущую частоту. **Демодулятор** выделяет из модулированного радиосигнала кодированный сигнал, несущий информацию. **Декодер канала** выделяет из входного потока управляющую информацию и направляет ее на логический блок; принятая информация проверяется на наличие ошибок, и выявленные ошибки по возможности исправляются; до последующей обработки принятая информация подвергается обратной по отношению к кодеру переупаковке. **Декодер речи** – восстанавливает поступающий на него с кодера канала сигнал речи, переводя его в естественную форму, со свойственной ему избыточностью, но в цифровом виде. **ЦАП** – преобразует принятый сигнал речи в аналоговую форму и подает его на вход динамика. **Эквалайзер** – служит для частичной компенсации искажений сигнала вследствие многолучевого распространения; по существу, он является адаптивным фильтром, настраиваемым по обучающей последовательности символов, входящей в состав передаваемой информации; блок эквалайзера не является, вообще говоря, функционально необходимым и в некоторых случаях может отсутствовать. Для сочетания кодера и декодера иногда применяют термин **кодек**.

Помимо собственно передатчика и приемника, в приемопередающий блок входят логический блок и синтезатор частот. **Логический блок** – это, по сути, микрокомпьютер со своей оперативной и постоянной памятью, осуществляющий управление работой подвижной станции. **Синтезатор частот** является источником колебаний несущей частоты, используемой для передачи информации по радиоканалу.

Приведенная схема достаточно проста и абстрактна, так на ней не приведены усилители, генераторы сигналов синхрочастот, и т.п. Для обеспечения конфиденциальности передачи информации в некоторых системах

возможно использование режима шифрования: в этих случаях передатчик и приемник подвижной станции включают соответственно блоки шифрования и дешифрования сообщений. В подвижной станции системы GSM предусмотрен специальный съемный модуль идентификации абонента (Subscriber Identity Module - SIM). Подвижная станция системы GSM включает так называемый детектор речевой активности (Voice Activity Detector), который в интересах экономного расходования энергии источника питания, а также снижения уровня помех, неизбежно создаваемых для других станций при работающем передатчике, включает работу передатчика на излучение только на те интервалы времени, когда абонент говорит. На время паузы в работе передатчика в приемный тракт дополнительно вводится так называемый комфортный шум. В необходимых случаях в состав подвижной станции могут входить отдельные терминальные устройства, подключаемые через специальные адаптеры с использованием соответствующих интерфейсов.

Блок-схема базовой станции (БС) представлена на рис. 4.

Первая особенность базовой станции – это использование разнесенного приема, для чего станция должна иметь 2 приемные антенны (использование разнесенного приема). БС может иметь раздельные антенны на передачу и на прием. Еще одна особенность – наличие нескольких приемников и такого же числа передатчиков, позволяющих вести одновременную работу на нескольких каналах с различными частотами.

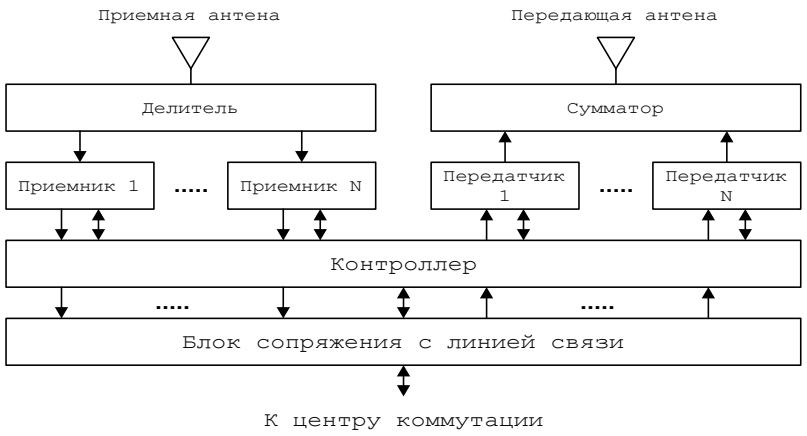


Рис. 4. Блок-схема базовой станции

Одноименные приемники и передатчики имеют общие перестраиваемые опорные генераторы, обеспечивающие их согласованную перестройку при переходе с одного канала на другой; конкретное число N приемопередатчиков зависит от конструкции и комплектации базовой станции. Для обеспечения одновременной работы N приемников на одну приемную и N передатчиков на одну передающую антенну между приемной антенной и приемниками устанавливается делитель мощности на N выходов, а между передатчиками и передающей антенной -–сумматор мощности на N входов.

Приемник и передатчик имеют, в общем, ту же структуру, что и в подвижной станции, за исключением того, что здесь в них отсутствуют блоки ЦАП и АЦП, поскольку и входной сигнал передатчика, и выходной сигнал приемника имеют цифровую форму. Возможны варианты, когда кодеки – либо только кодек речи, либо и кодек речи, и канальный кодек – конструктивно реализуются в составе центра коммутации, а не в составе приемопередатчиков базовой станции, хотя функционально они остаются элементами приемопередатчиков.

Блок сопряжения с линией связи осуществляет упаковку информации, передаваемой по линии связи на центр коммутации, и распаковку принимаемой от него информации. В качестве линии связи базовой станции с центром коммутации обычно используется радиорелейная или волоконно-оптическая линия, если базовая станция и центр коммутации не располагаются территориально в одном месте.

Контроллер БС, представляющий собой достаточно мощный и совершенный компьютер, обеспечивает управление работой станции, а также контроль работоспособности всех входящих в нее блоков и узлов.

Для обеспечения достаточной степени надежности многие блоки и узлы базовой станции резервируются, в состав станции включаются автономные источники бесперебойного питания. Поскольку аппаратура базовой станции потребляет значительную мощность, и соответственно выделяет заметное количество теплоты, в ней предусматриваются специальные устройства охлаждения.

Центр коммутации (ЦК) является «мозговым центром» и одновременно диспетчерским пунктом системы сотовой связи, на который замыкаются потоки информации со всех базовых станций и через который осуществляется выход на другие сети связи – стационарную телефонную сеть, сети междугородной связи, спутниковой связи, другие сотовые сети. В состав центра коммутации входит несколько процессоров (контроллеров), и он является типичным примером многопроцессорных систем.

Блок-схема центра коммутации представлена на рис. 5. Собственно коммутатор осуществляет переключение потоков информации между соответствующими линиями связи. Он может направить поток информации от одной базовой станции к другой, или от базовой станции к стационарной сети связи, или наоборот - от стационарной сети связи к нужной базовой станции.

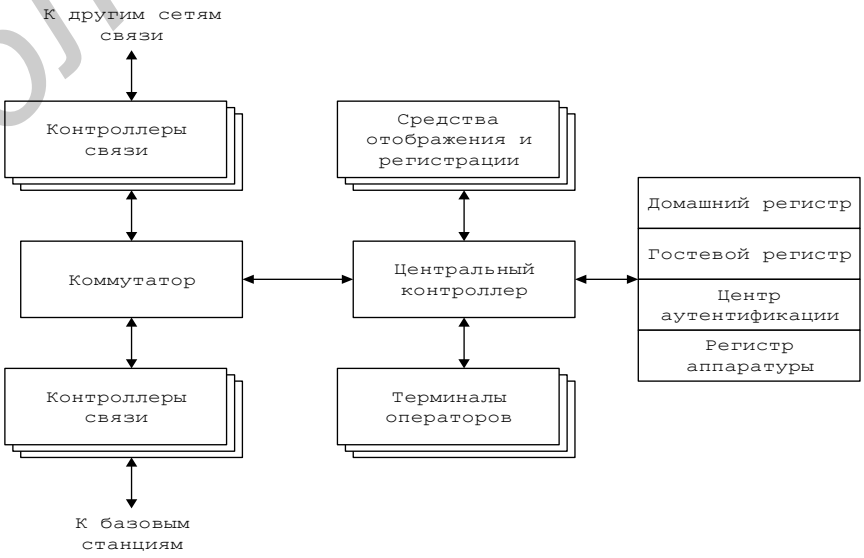


Рис. 5. Блок-схема центра коммутации

Коммутатор подключается к линиям связи через соответствующие контроллеры связи, осуществляющие промежуточную обработку (упаковку/распаковку, буферное хранение) потоков информации. Общее управление работой центра коммутации и системы в целом производится от центрального контроллера, который имеет мощное математическое обеспечение, включающее перепрограммируемую часть. Работа центра коммутации предполагает активное участие операторов, поэтому в состав центра входят соответствующие терминалы, а также средства отображения и регистрации информации. В частности, оператором вводятся данные об абонентах и условиях их обслуживания, исходные данные по режимам работы системы, в необходимых случаях оператор выдает требующиеся по ходу работы команды.

Важными элементами системы являются домашний регистр, гостевой регистр, центр аутентификации, регистр аппаратуры. Домашний регистр (домашний регистр местоположения - Home Location Register (HLR)), содержит сведения обо всех абонентах, зарегистрированных в данной системе, и о видах услуг, которые могут быть им оказаны. Здесь же фиксируется местоположение абонента для организации его вызова, и регистрируются фактически оказанные услуги. Гостевой регистр (гостевой регистр местоположения - Visitor Location Register (VLR)), содержит примерно такие же сведения об абонентах-гостях (роумерах), т.е. об абонентах, зарегистрированных в другой системе, но пользующихся в настоящее время услугами сотовой связи в данной системе. Центр аутентификации (Authentication Center) обеспечивает процедуры аутентификации абонентов и шифрования сообщений. Регистр аппаратуры (регистр идентификации аппаратуры - Equipment Identity Register (EIR)),

содержит сведения об эксплуатируемых подвижных станциях на предмет исправности и санкционированного использования. В частности, в нем могут отмечаться украденные абонентские аппараты, а также аппараты, имеющие технические дефекты.

Как и в базовой станции, в центре коммутации предусматривается резервирование основных элементов аппаратуры.

3. Структура TDMA.

В результате анализа различных вариантов построения цифровых сотовых систем подвижной связи (ССПС) в стандарте GSM принят многостанционный доступ с временным разделением каналов (TDMA). Общая структура временных кадров показана на рис. 6. Длина периода последовательности в этой структуре, которая называется гиперкадром, равна Тг = 3 ч 28 мин 53 с 760 мс (12533,76 с). Гиперкадр делится на 2048 суперкадров, каждый из которых имеет длительность Те = 12533,76/2048 = 6,12 с.

Рис. 6. Структура TDMA кадра

Суперкадр состоит из мультикадров. Для организации различных каналов связи и управления в стандарте GSM используются два вида мультикадров:

1) 26-позиционные TDMA кадры мультикадра;

2) 51-позиционные TDMA кадры мультикадра.

Суперкадр может содержать в себе 51 мультикадр первого типа или 26 мультикадров второго типа. Длительности мультикадров соответственно:

1) Тм= 6120/51 = 120 мс;

2) Тм = 6120/26 = 235,385 мс (3060/13 мс).

Длительность каждого TDMA кадра

Тк = 120/26 = 235,385/51 = 4,615 мс (60/13 мс).

В периоде последовательности каждый TDMA кадр имеет свой порядковый номер (NF) от О до NFmax, где NFmax = (26x51x2048) -1 = 2715647.

Таким образом, гиперкадр состоит из 2715647 TDMA кадров. Необходимость такого большого периода гиперкадра объясняется требованиями применяемого процесса криптографической защиты, в котором номер кадра NF используется как входной параметр.

TDMA кадр делится на восемь временных позиций с периодом

То = 60/13:8 = 576,9 мкс (15/26 мс)

Каждая временная позиция обозначается TN с номером от 0 до 7. Физический смысл временных позиций, которые иначе называются окнами, - время, в течение которого осуществляется модуляция несущей цифровым информационным потоком, соответствующим речевому сообщению или данным.

Цифровой информационный поток представляет собой последовательность пакетов, размещаемых в этих временных интервалах (окнах). Пакеты формируются немного короче, чем интервалы, их длительность составляет 0,546 мс, что необходимо для приема сообщения при наличии временной дисперсии в канале распространения.

Информационное сообщение передается по радиоканалу со скоростью 270,833 кбит/с.

Это означает, что временной интервал TDMA кадра содержит 156,25 бит. Длительность одного информационного бита 576,9 мкс/156,25 = 3,69 мкс.

Каждый временной интервал, соответствующий длительности бита, обозначается BN с номером от 0 до 155; последнему интервалу длительностью 1/4 бита присвоен номер 156. Для передачи информации по каналам связи и управления, подстройки несущих частот, обеспечения временной

синхронизации и доступа к каналу связи в структуре TDMA кадра используются пять видов временных интервалов (окон):

NB (Normal Burst – Нормальный временной интервал) используется для передачи информации по каналам связи и управления, за исключением канала доступа RACH. Он состоит из 114 бит зашифрованного сообщения и включает защитный интервал (GP) в 8,25 бит длительностью 30,46 мкс. Информационный блок 114 бит разбит на два самостоятельных блока по 57 бит, разделенных между собой обучающей последовательностью в 26 бит, которая используется для установки эквалайзера в приемнике в соответствии с характеристиками канала связи в данный момент времени.

В состав NB включены два контрольных бита (Steeling Flag), которые служат признаком того, содержит ли передаваемая группа речевую информацию или информацию сигнализации. В последнем случае информационный канал (Traffic Channel) "украден" для обеспечения сигнализации.

Между двумя группами зашифрованных бит в составе NB находится обучающая последовательность из 26 бит, известная в приемнике. С помощью этой последовательности обеспечивается:

- оценка частоты появления ошибок в двоичных разрядах по результатам сравнения принятой и эталонной последовательностей. В процессе сравнения вычисляется параметр RXQUAL, принятый для оценки качества связи. Конечно, речь идет только об оценке связи, а не о точных измерениях, так как проверяется только часть передаваемой информации. Параметр RXQUAL используется при вхождении в связь, при выполнении процедуры "эстафетной передачи" (Handover) и при оценке зоны покрытия радиосвязью;

- оценка импульсной характеристики радиоканала на интервале передачи NB для последующей коррекции тракта приема сигнала за счет использования адаптивного эквалайзера в тракте приема;

- определение задержек распространения сигнала между базовой и подвижной станциями для оценки дальности связи. Эта информация необходима для того, чтобы пакеты данных от разных подвижных станций не накладывались при приеме на базовой станции. Поэтому удаленные на большее расстояние подвижные станции должны передавать свои пакеты раньше станций, находящихся в непосредственной близости от базовой станции.

FB (Frequency Correction Burst – Временной интервал подстройки частоты) предназначен для синхронизации по частоте подвижной станции. Все 142 бита в этом временном интервале - нулевые, что соответствует немодулированной несущей со сдвигом 1625/24 кГц выше номинального значения частоты несущей. Это необходимо для проверки работы своего передатчика и приемника при небольшом частотном разносе каналов (200 кГц), что составляет около 0,022% от номинального значения полосы частот 900 МГц. FB содержит защитный интервал 8,25 бит так же, как и нормальный временной интервал. Повторяющиеся временные интервалы подстройки частоты (FB) образуют канал установки частоты (FCCH).

SB (Synchronization Burst – Интервал временной синхронизации) используется для синхронизации по времени базовой и подвижной станций. Он состоит из синхропоследовательности длительностью 64 бита, несет информацию о номере ТОМА кадра и идентификационный код базовой станции. Этот интервал передается вместе с интервалом установки частоты. Повторяющиеся интервалы синхронизации образуют так называемый канал синхронизации (SCH).

DB (Dummy Burst – Установочный интервал) обеспечивает установление и тестирование канала связи. По своей структуре DB совпадает с NB (рис. 1.7) и содержит установочную последовательность длиной 26 бит. В DB отсутствуют контрольные биты и не передается никакой информации. DB лишь информирует о том, что передатчик функционирует.

AB (Access Burst – Интервал доступа) обеспечивает разрешение доступа подвижной станции к новой базовой станции. AB передается подвижной станцией при запросе канала сигнализации. Это первый передаваемый подвижной станцией пакет, следовательно, время прохождения сигнала еще не измерено. Поэтому пакет имеет специфическую структуру. Сначала передается концевая комбинация 8 бит, затем - последовательность синхронизации для базовой станции (41 бит), что позволяет базовой станции обеспечить правильный прием последующих 36 зашифрованных бит. Интервал содержит большой защитный интервал (68,25 бит, длительностью 252 мкс), что обеспечивает (независимо от времени прохождения сигнала) достаточное временное разнесение от пакетов других подвижных станций.

Этот защитный интервал соответствует двойному значению наибольшей возможной задержки сигнала в рамках одной соты и тем самым устанавливает максимально допустимые размеры соты. Особенность стандарта GSM - возможность обеспечения связью подвижных абонентов в сотах с радиусом около 35 км. Время распространения радиосигнала в прямом и обратном направлениях составляет при этом 233,3 мкс.

Принятая структура TDMA кадров и принципы формирования сигналов в стандарте GSM в совокупности с методами капельного кодирования позволили снизить требуемое для приема отношение сигнал/помеха до 9 дБ, тогда как в стандартах аналоговых сотовых сетей связи оно составляет 17-18 дБ.

4. Организация физических и логических каналов в стандарте GSM.

Стандарт GSM разработан для создания сотовых систем подвижной связи (ССПС) в следующих полосах частот: 890-915 МГц - для передачи подвижными станциями (линия "вверх"); 935-960 МГц - для передачи базовыми станциями (линия "вниз").

Сети GSM функционируют параллельно с существующими европейскими национальными сетями аналоговых ССПС стандартов NMT-900, TAGS, ETACS.

Каждая из полос, выделенных для сетей GSM, разделяется на частотные каналы. Разнос каналов составляет 200 кГц, что позволяет организовать в сетях GSM 124 частотных канала. Частоты, выделенные для передачи сообщений подвижной станцией на базовую и в обратном направлении, группируются парами, организуя дуплексный канал с разносом 45 МГц. Эти пары частот сохраняются и при перескоках частоты. Каждая сота характеризуется фиксированным присвоением определенного количества пар частот.

Если обозначить FI(n) - номер несущей частоты в полосе 890-915 МГц, Fu(n) - номер несущей частоты в полосе 935-960 МГц, то частоты каналов определяются по следующим формулам:

$FI(n) = 890{,}2 + 0{,}2\,(n-1)$, МГц; $Fu(n) = FI(n) + 45$, МГц; $1 < n < 124$.

Каждая частотная несущая содержит 8 физических каналов, размещенных в 8 временных окнах в пределах TDMA кадра и в последовательности кадров. Каждый физический канал использует одно и то же временное окно в каждом временном TDMA кадре.

До формирования физического канала сообщения и данные, представленные в цифровой форме, группируются и объединяются в логические каналы двух типов: каналы связи - для передачи кодированной речи или данных (ТСН); каналы управления - для передачи сигналов управления и синхронизации (ССН).

Более чем один тип логического канала может быть размещен на одном и том же физическом канале, но только при их соответствующей комбинации.

Физический канал в системе с множественным доступом на основе временного разделения (TDMA) - это временной слот с определенным номером (или пара слотов с номерами, отличающимися на 3 при полноскоростном кодировании в стандарте D-AMPS) в последовательности кадров эфирного

интерфейса. Таким образом, в одном частотном канале в стандарте D-AMPS при полноскоростном кодировании передается информация трех физических каналов, при полускоростном кодировании - информация шести физических каналов, а в стандарте GSM всегда передается информация восьми физических каналов, но при полускоростном кодировании один физический канал содержит два канала трафика, информация которых передается по очереди, через кадр. Иными словами, при этом реализуется временное уплотнение каналов в 3 или 8 раз соответственно при полноскоростном кодировании и в 6 или 16 раз - при полускоростном. В этом и заключается одно из основных преимуществ цифрового поколения сотовой связи по сравнению с аналоговым.

Логические каналы различаются по виду (составу) информации, передаваемой в физическом канале. В принципе в физическом канале может быть реализован один из двух видов логических каналов - канал т*рафика* или канал *управления;* каждый из них, в свою очередь, может в общем случае существовать в одном из нескольких вариантов (типов).

С понятием канала управления мы по существу уже познакомились в начале данного раздела. Логический канал трафика - это канал передачи речи или данных (компьютерных данных, факсимильных сообщений), т.е. той информации, ради которой, собственно, и создается сотовая связь. Термин т*рафик* происходит от английского *traffic* (информационный поток, поток транспорта) и в применении к связи определяется как совокупность сообщений, передаваемых по линии связи, или как совокупность требований абонентов, обслуживаемых сетью связи. Коль скоро мы договорились, что в рамках данной книги ограничиваемся в основном передачей речи, то канал трафика оказывается для нас тождественным каналу передачи речи.

В стандарте D-AMPS версии IS-54, с его относительно простым эфирным интерфейсом, понятие «логические каналы» обычно не используется. Логический канал управления здесь по существу представлен укороченной

пачкой, используемой на этапе установления связи, и быстрым совмещенным каналом управления FACCH (Fast Associated Control Channel). Информация канала FACCH передается вместо информации речи, т.е. структура слота логического канала управления отличается от структуры слота логического канала трафика заменой поля Data на поле FACCH. Сегмент речи продолжительностью 40 мс при этом просто пропускается (теряется). Допустимая частота замены канала трафика каналом управления не регламентирована, но из общих соображений очевидно, что чем чаще это будет происходить, тем сильнее будет снижаться качество передачи речи. Замена информации речи информацией канала FACCH никак не помечается внутри слота, и характер информации выясняется лишь при ее декодировании.

Кроме того, в стандарте IS-54 используются так называемые выделенные каналы управления, доставшиеся цифровой (или цифро-аналоговой) системе в наследство от аналоговой AMPS с небольшими дополнениями в части состава передаваемой информации. Эти частотные каналы всегда используются только как каналы управления, т.е. они никогда не бывают каналами трафика. Первичные выделенные каналы управления используются как в аналоговом, так и в цифровом стандарте. Вторичные выделенные каналы управления используются только в цифровом стандарте; в аналоговом стандарте соответствующие частотные каналы использовались как каналы трафика. Обычно для каждой базовой станции назначается один выделенный канал управления.

Информация в выделенных каналах управления передается в цифровой форме с использованием частотной манипуляции (Frequency Shift Keying - FSK) со скоростью 10 кбит/с. Передача информации организуется в виде кадров, длительность и структура которых различна в прямом и обратном каналах (рис. 7).

Dot – пунктир (Dotting) - последовательность чередующихся единиц и нулей (дает хорошо обнаруживаемую частотную составляющую 5 кГц); Sync - синхронизирующая последовательность; DCC - цифровой код цвета (Digital Color Code); A1…A5 - информационные слова для подвижных станций с четными номерами; B1...B5 - информационные слова для подвижных станций с нечетными номерами; W1…W5 - информационные слова.

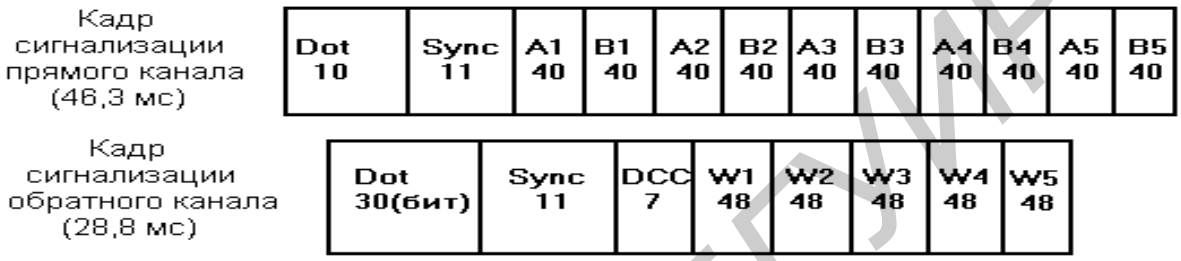


Рис. 7. Структура кадров сигнализации выделенных каналов управления

В обоих случаях кадр начинается с пунктирной последовательности, означающей начало кадра, и синхронизирующей последовательности известной структуры. Затем следуют информационные слова, которые повторяются пятикратно для исключения слов с искажениями по мажоритарному принципу («3 из 5»). Для защиты от ошибок информационные слова дополнительно кодируются (код BCH): из 40 бит слова прямого канала - 28 бит информационных и 12 контрольных; из 48 бит слова обратного канала - 36 информационных и 12 контрольных. В прямом канале информация передается синхронно (с жесткой привязкой ко времени), в обратном - асинхронно. Информационные поля кадра прямого канала содержат также так называемые биты «занято/свободно» - Busy/Idle (B/I) bits, по одному - в полях пунктира и синхронизации и по четыре - в каждом информационном слове; этими битами определяется временная привязка кадров сигнализации обратного канала (т.е. данная подвижная станция выдает свою информацию тогда, когда по состоянию бита «занято/свободно», канал не занят информацией, передаваемой

другой подвижной станцией). Передаваемое сообщение может занимать более одного кадра.

В стандарте IS-136 выделенных каналов управления нет, т.е. все частотные каналы равноправны в отношении состава передаваемой информации, но в явном виде возникает необходимость в использовании понятия логических каналов - каналов трафика и каналов управления. Каналы трафика в стандарте IS-136 не претерпели изменений по сравнению с IS-54.

Для передачи информации логических каналов управления выделяется один физический канал, т.е. два слота в пределах одного кадра эфирного интерфейса при полноскоростном кодировании, по одному слоту в пределах каждого из двух блоков.

В обратном направлении (от подвижной станции к базовой) передается информация только одного логического канала управления - канала случайного доступа RACH (Random Access Channel). Информация этого канала используется для организации доступа в систему сотовой связи со стороны подвижной станции и передается во всех слотах соответствующего физического канала.

В прямом направлении (от базовой станции к подвижной) передается информация нескольких логических каналов управления:

- вещательного канала управления BCCH (Broadcast Control Channel) с подканалами быстрого вещательного управления F-BCCH (Fast BCCH), расширенного вещательного управления E-BCCH (Extended BCCH) и вещательной передачи сообщений S-BCCH (Broadcast messaging);

- канала SPACH с подканалами вызова PCH (Paging Channel), ответа на вызов ARCH (Access Response Channel) и передачи коротких сообщений по определенному адресу SMSCH («от точки к точке» - point-to-point Short Message Service Channel);

- общего канала обратной связи SCF (Shared Channel Feedback).

Канал RACH (канал случайного доступа) используется при установлении связи по инициативе подвижной станции или, иными словами, для организации доступа в сеть со стороны подвижной станции. Канал SCF используется для передачи ответной информации в процессе организации этого доступа.

В канале BCCH передается информация, предназначенная для всех подвижных станций (*вещательный* режим передачи информации): это информация о состоянии сети (подканалы F-BCCH и E-BCCH), а также вещательные короткие сообщения (подканал S-BCCH). Быстро изменяющаяся информация о состоянии сети, требующая частого обновления (параметры каналов управления и информация, существенная для организации доступа в сеть), передается в подканале F-BCCH, вся информация которого обновляется с частотой суперкадров. Менее срочная информация передается в подканале E-BCCH, передача одного сообщения в котором может растягиваться на несколько суперкадров.

Канал SPACH используется для передачи адресных сообщений, т.е. сообщений, адресованных конкретным подвижным станциям. В подканале PCH передается информация вызова, а также команды для подвижной станции. Подканал ARCH используется на завершающем этапе установления соединения подвижной станции с сетью. Подканал SMSCH предназначен для адресной передачи коротких сообщений.

Передача информации в прямых цифровых каналах управления организуется следующим образом. Информация канала SCF передается в соответствующем поле каждого слота канала управления. Информация остальных каналов размещается в полях Data и имеет определенную последовательность в пределах слотов суперкадра и гиперкадра. Всего в суперкадре при полноскоростном кодировании 32 слота канала управления. Первые слоты отводятся для подканала F-BCCH (от 3 до 10 слотов), следующие слоты - для E-BCCH (от 1 до 8 слотов), затем - для S-BCCH (от 0 до 16 слотов) и

в конце - для информации канала SPACH (от 2 до 28 слотов). Информация подканалов F-BCCH и PCH одинакова в обоих суперкадрах одного гиперкадра (дублирование информации с целью повышения достоверности ее приема); информация других подканалов в суперкадрах одного гиперкадра различна.

Принятая структура каналов управления предусматривает такую организацию вызова подвижной станции, которая поддерживает *режим засыпания (sleep mode)* последней. Для этого вызов повторяется с периодичностью кадра вызова, а длительность кадра вызова в зависимости от его класса составляет от 1,28 секунды до 123 секунд. Если говорить более конкретно, то длительность кадра вызова для классов 1...8 составляет соответственно 1, 2, 3, 6, 12, 24, 48 и 96 гиперкадров, и в обоих суперкадрах первого гиперкадра в пределах кадра вызова передается информация вызова. Подвижная станция принимает (декодирует) информацию в первом (первичном) из двух указанных суперкадров, и если вызова в ее адрес нет, то «засыпает», т.е. отключается даже на прием до конца кадра вызова. Если декодировать информацию в первичном суперкадре не удается, например, из-за искажений сигналов, вызванных помехами, то предпринимается попытка декодировать вторичный суперкадр, несущий ту же информацию подканалов F-BCCH и PCH, после чего подвижная станция также получает возможность «заснуть» до конца кадра вызова. По умолчанию, т.е. до первой регистрации в системе, подвижная станция использует кадр вызова класса 1, т.е. кадр вызова минимальной длительности (один гиперкадр). В дальнейшем длительность кадра вызова назначается сетью.

Логические каналы стандарта GSM делятся на каналы трафика и каналы управления.

Каналы трафика TCH (Traffic Channels), в свою очередь, делятся на полноскоростные TCH/FS (с полноскоростным кодированием; F - сокращение

от Full - полный; S - Speech - речь) и полускоростные TCH/HS (H - сокращение от Half - половина); в обоих случаях имеется в виду передача речи.

Каналы управления CCH (Control Channels) делятся на 4 типа: вещательные каналы управления BCCH (Broadcast Control Channels), общие каналы управления CCCH (Common Control Channels), выделенные закрепленные каналы управления SDCCH (Standalone Dedicated Control Channels), совмещенные каналы управления ACCH (Associated Control Channels).

Вещательные каналы управления BCCH предназначены для передачи информации от базовой станции к подвижным в вещательном режиме, т.е. без адресования к какой-либо конкретной подвижной станции. В число вещательных каналов управления входят: канал коррекции частоты FCCH (Frequency Correction Channel) - для подстройки частоты подвижной станции под частоту базовой, канал синхронизации SCH (Synchronization Channel) - для кадровой синхронизации подвижных станций, а также канал общей информации, не имеющий отдельного наименования.

Общие каналы управления CCCH включают: канал вызова PCH (Paging Channel), используемый для вызова подвижной станции базовой; канал разрешения доступа AGCH (Access Grant Channel) - для назначения закрепленного канала управления, которое также передается от базовой станции на подвижную; канал случайного доступа RACH (Random Access Channel) - для выхода с подвижной станции на базовую с запросом о назначении выделенного канала управления. При передаче информации по общим каналам управления прием информации не сопровождается подтверждением.

Совмещенные каналы управления ACCH, также используемые для передачи информации в обоих направлениях (от базовой станции к подвижным и от подвижных к базовой), включают: медленный совмещенный канал

управления SACCH (Slow Associated Control Channel) - объединяется с каналом трафика (кадр 13 мультикадра канала трафика) или с каналом SDCCH; быстрый совмещенный канал управления FACCH (Fast Associated Control Channel) - совмещается с каналом трафика, заменяя в соответствующем слоте информацию речи, причем эта замена помечается скрытым флажком.

В отличие от дуплексных каналов - трафика и совмещенных каналов управления, размещаемых в канале трафика эфирного интерфейса, - симплексные каналы управления BCCH и CCCH размещаются в нулевом слоте кадров канала управления эфирного интерфейса на так называемых несущих BCCH, имеющихся в ячейке.

Сообщения канала RACH могут быть переданы в нулевом слоте любого кадра в пределах 51-кадрового мультикадра канала управления (рис. 8). Сообщение RACH передается подвижной станцией раз в 235 мс, т.е. только в одном из кадров мультикадра, при этом используется структура слота, соответствующая пачке доступа.

Рис. 8. Структура мультикадра канала управления

Сообщения каналов BCCH и CCCH, передаваемые от базовой станции к подвижным (прямой канал), размещаются в нулевых слотах 50 кадров мультикадра канала управления эфирного интерфейса; последний, 51-й, кадр мультикадра остается свободным. Первые 50 кадров делятся на 5 блоков по 10

кадров: в начале каждого блока передается сообщение канала FCCH (структура слота - пачка коррекции частоты), далее - сообщение канала SCH (структура слота - пачка синхронизации), затем в первом блоке передается четыре сообщения канала BCCH и четыре сообщения канала AGCH или канала PCH, а в остальных четырех блоках все восемь сообщений отводятся под канал AGCH или PCH. Сообщения логических каналов управления в большинстве случаев кодируются со значительной избыточностью с целью защиты от ошибок при передаче информации.

И в заключение еще раз отметим, что изложенные сведения о структуре и организации работы логических каналов управления весьма схематичны и не претендуют на исчерпывающую полноту. Более того, такие сложные и ответственные разделы, как организация каналов управления, имеют тенденцию совершенствоваться со временем, так что детальное знакомство с их работой требует изучения новейших версий стандартов, содержащих последние изменения.

5. Кодирование и перемежение в каналах связи и управления стандарта GSM.

Для защиты от ошибок в радиоканалах подвижной связи GSM PLMN используются сверточное и блочное кодирование с перемежением. Перемежение обеспечивает преобразование пакетов ошибок в одиночные. Сверточное кодирование является мощным средством борьбы с одиночными ошибками. Блочное кодирование, главным образом, используется для обнаружения нескорректированных ошибок.

Блочный код (n, k, t) преобразует k информационных символов в n символов путем добавления символов четности (n-k), а также может корректировать t ошибок символов.

Сверточные коды (СК) относятся к классу непрерывных помехоустойчивых кодов. Одной из основных характеристик СК является величина K, которая называется длиной кодового ограничения, и показывает, на какое максимальное число выходных символов влияет данный информационный символ. Так как сложность декодирования СК по наиболее выгодному, с точки зрения реализации, алгоритму Витерби возрастает экспоненциально с увеличением длины кодового ограничения, то типовые значения K малы и лежат в интервале 3-10. Другой недостаток СК заключается в том, что они не могут обнаруживать ошибки. Поэтому в стандарте GSM для внешнего обнаружения ошибок используется блочный код на основе сверточного кода (2, 1, 5) со скоростью r=1/2.

В соответствии с общей структурой кадров в стандарте GSM (рис. 9) передача информационных сообщений и сигналов управления осуществляется в нормальном временном интервале (NB) TDMA кадра. Структура NB (два пакета по 57 информационных бит каждый) требует, чтобы количество кодированных бит m, соответствующих n - некодированным битам в общей схеме кодирования и перемежении, равнялась бы целому числу, кратному 19. Затем эти биты зашифровываются и объединяются в I групп. Количество бит в этих группах также должно равняться 19, i групп переходят в i временных интервалов. Номер l называется степенью перемежения.

В различных логических каналах используются различные сверточные коды, поскольку скорости передачи и требования по защите от ошибок также различны. Для упрощения механизмов кодирования и декодирования для формирования кодов используются только несколько полиномов. Это позволяет использовать сверточный код с одной скоростью r=1/2. Однако, чтобы выполнить требования формирования полноскоростного канала связи, а также привести в соответствие структуру размещения бит со структурой кадров необходима скорость r=244/456=0,535.

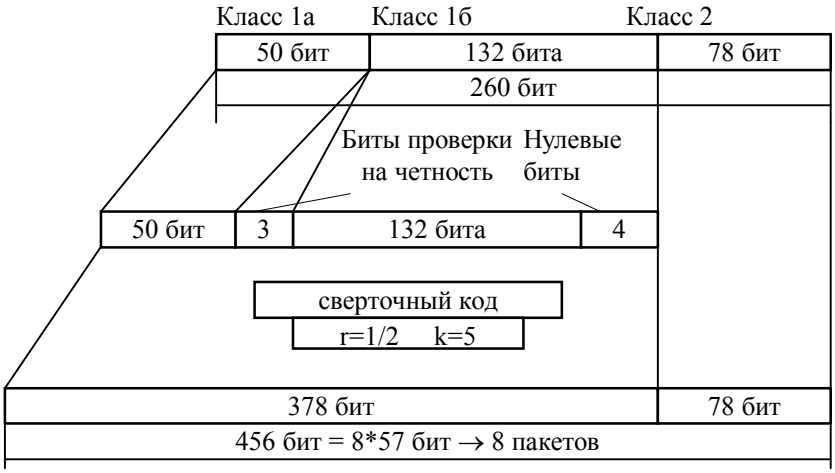
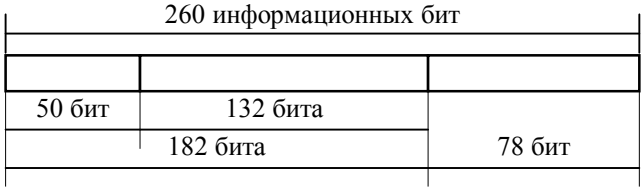


Рис. 9. Общая структура кадров

Для выравнивания скорости в речевом канале до r=1/2 применяют прореживание, то есть периодический пропуск некоторых кодированных символов. Такая операция называется перфорированием, а формируемые таким образом коды называются перфорированными. При приеме декодер, зная алгоритм прореживания, интерполирует принимаемые данные.

Кодирование осуществляется следующим образом: биты класса 1 разделяются дополнительно на 50 бит класса 1а и 132 бита класса 16 (рис. 10 а). Биты класса 1а дополняются тремя битами проверки на четкость (рис. 10 б). Блочный код представляет собой укороченный систематический циклический код (53, 50) с формирующим полиномом вида g (D)=D3+D+1.

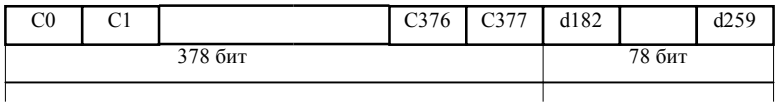
а) Первоначальный речевой кадр 260 бит/кадр Полноскоростной речевой канал



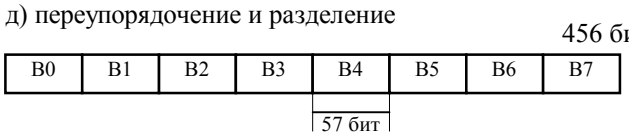
б) циклический код класса 1 (обнаружение ошибок)

в) переупорядочение и концевая комбинация

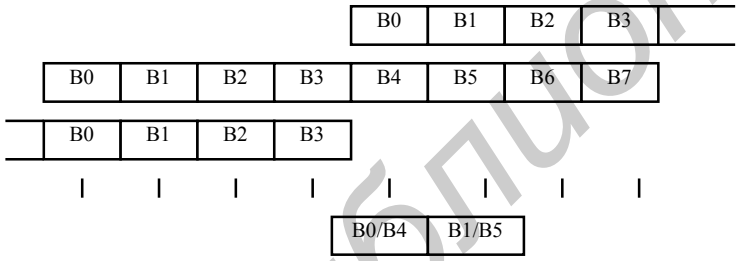
г) сверточный код r=1/2, класс 1 (исправление ошибок)



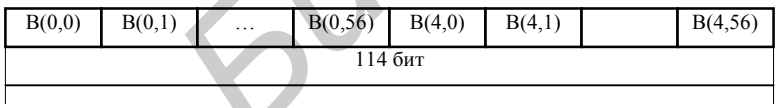
д) переупорядочение и разделение



е) блочно-диагональное перемежение



ж) разбиение на пакеты 114 бит/пакет



з) перемежение пакетов

Рис. 10. Общая структура кадра

В соответствии с принятым правилом формирования систематического кода, ключ Sw закрыт на время первых пятидесяти тактовых импульсов, а информационные биты, поступающие на вход кодирующего устройства, одновременно поступают на блок переупорядочения и формирования бит проверки на четность. После пятидесяти тактовых импульсов переключатель Sw срабатывает и биты проверки на четность поступают из кодирующего устройства. Сформированный в результате кадр показан на рис. 10. На этой стадии проводится первый шаг перемежения. Биты с четными индексами собираются в первой части информационного слова, за которыми следуют три бита проверки на четность. Затем биты с нечетными индексами запоминаются в буферной памяти и переставляются так, как показано на рис. 10 в. Далее следуют четыре нулевых бита, которые необходимы для работы кодера, формирующего код, исправляющий случайные ошибки в канале. После чего 189 бит класса 1 кодируются сверточным кодом (2,1,5) со скоростью r=1/2.

Как показано на рис. 10 г, после сверточного кодирования общая длина кадра составляет 2x189+78=456 бит. После этого кадр из 456 бит делится на восемь 57 битовых подблоков (рис. 10 д), которые подвергаются диагональному и внутрикадровому перемежению (рис. 10). Результаты перемежения показаны на рис. 10 ж, з. Более точно подблоки B0 и B4 формируются в пакеты по 114 бит, которые являются результатом блочно-диагонального перемежения (DI/B). На рис. 10 е биты B0 и B4 подблоков попарно перемежаются, образуя процесс внутрикадрового битового перемежения (|B|/B). В результирующий пакет (рис. 10 з) включены два опережающих флага h1, h0, которые используются для классификации различных пакетов передачи.

Для повышения эффективности применения сверточного кодирования в полноскоростных каналах передачи данных необходим длительный период перемежения. В этих каналах внутрикадровое перемежение (|B|/B) реализуется для степени перемежения l=19, что приводит к задержке передачи данных на

19x116=2204 бит. Если биты 1-го пакета (временного интервала) до перемежения обозначить как C (Km), m=1 ...116, то схема перемежения, то есть позиции бит после перемежения, определяются следующей формулой:

l(K+j, j+19t) = C(K, m) для всех K; j = m mod 19, t = m mod 6.

6. Аспекты безопасности в стандарте GSM

Сотовые системы подвижной связи нового поколения в состоянии принять всех потенциальных пользователей, если будут гарантированы безопасность связи: секретность и аутентификация. Секретность должна исключить возможность извлечения информации из каналов связи кому-либо, кроме санкционированного получателя. Проблема аутентификации заключается в том, чтобы помешать кому-либо, кроме санкционированного пользователя (отправителя), изменить канал, то есть получатель должен быть уверен, что в настоящий момент он принимает сообщение от санкционированного пользователя. Основным способом обеспечения секретности является шифрование. Относительно новая концепция - использование шифрования как способа аутентификации сообщений.

Аутентификация сообщений через шифрование осуществляется за счет включения в текст так называемого кода идентификации (то есть фиксированного или зависящего от передаваемых данных слова, которое знают отправитель и получатель или которое они могут выделить в процессе передачи). Получатель расшифровывает сообщение, путем сравнения получает удостоверение, что принимаемые данные являются именно данными санкционированного отправителя.

К системе шифрования предъявляются следующие основные требования:

1) нелинейные связи между исходным текстом и зашифрованным текстом;

2) изменение параметров шифрования во времени.

Если алгоритмы шифрования отвечают первому требованию, то, не зная ключа, исключается возможность изменить код идентификации, чтобы избежать обнаружения факта несанкционированного доступа. Второе требование исключает возможность нарушения работы системы за счет воспроизведения "обнаружителем" принятого ранее и записанного в память сообщения.

Один из путей обеспечения этих требований - применение синхронных систем передачи, но при этом необходимы системы тактовой инхронизации, что во многих случаях неприемлемо.

Второй путь - включение в информационную последовательность (каждое сообщение) временных меток так, чтобы зашифрованные данные были бы однозначно с ними связаны. Алгоритмы шифрования делятся на два класса:

- классические алгоритмы;

- алгоритмы с открытым ключом.

Классические алгоритмы используют один ключ для шифрования-дешифрования. Алгоритмы с открытым ключом используют два ключа: первый - для перехода от нешифрованного текста к шифрованному; второй - для обратного перехода от шифрованного к нешифрованному. Причем знание одного ключа не должно обеспечить обнаружение второго ключа. В этих алгоритмах один из ключей, обычно используемый для шифрования, можно сделать общим, и только ключ, используемый для расшифровки, должен быть засекречен. Эта особенность очень полезна для снижения сложности протокола и интеграции структур шифрования в сетях связи.

Алгоритмы шифрования с открытым ключом построены на определении односторонней функции, то есть некоторой функции f, такой, что для любого x из ее области определения f(x) легко вычислима, однако практически для всех y из ее области значений нахождение x, для которого y=f(x), вычислительно не

осуществимо. То есть, односторонняя функция является отдельной функцией, которая легко рассчитывается ЭВМ в приемлемом объеме времени, но время расчета обратной функции в существующих условиях недопустимо большое.

Первый алгоритм шифрования с общим ключом был назван RSA (первые буквы фамилий авторов Rivest, Shamir, Adleman). Алгоритм базируется на двух функциях E и D, связанных соотношением: D (E(*)) = E (D(*)).

Одна из этих функций используется для шифрования сообщений, другая - для дешифрования. Секретность алгоритма основана на том, что знание функции E (или D) не открывает легкого способа вычисления D (или E). Каждый пользователь делает общей функцию E и хранит в секрете функцию D, то есть для пользователя X есть открытый ключ Ex и секретный Dx.

Два пользователя A и B могут использовать алгоритм RSA, чтобы передать любое зашифрованное сообщение. Если абонент A хочет отправить сообщение M абоненту B, то он может сделать это следующим образом:

- зашифровать сообщение M;
- подписать сообщение M;
- зашифровать и подписать M.

В первом случае: A обеспечивает преобразование M, используя открытый ключ C = Eв (M) и посылает его абоненту B. B принимает C и вычисляет

Dв (c) = Dв (Eв (M)) = M.

Во втором случае: A подписывает M посредством вычисления F = Da (M)

и посылает F абоненту B (эти операции может осуществлять только пользователь A, которому известен секретный ключ Da). B получает F и вычисляет

Ea (F) = Ea (Da (M)) = M.

B теперь известно, что сообщение M действительно послано пользователем A. В этом случае секретность сообщения M не гарантируется,

так как все могут осуществить такую же операцию с использованием общего ключа Ea.

В третьем случае: A вычисляет F = Da (M) и C = Eв (F) = Eв (Da(M));

A посылает C к B. B получает C и вычисляет Dв (c) = Dв (Eв(F)) = Da (M);

B может теперь легко получить M, вычислив Ea (Da (M)) = M.

До операции шифрования и подписи каждое сообщение M должно разделяться на блоки фиксированной длины, затем каждый блок кодируется как совокупность фиксированного числа цифр. RSA кодер оперирует такими отдельными блоками в каждом цикле кодирования.

Алгоритм шифрования с открытым ключом RSA обеспечивает высокую степень безопасности передачи речевых сообщений и рекомендован к использованию в цифровых системах подвижной радиосвязи нового поколения.

В стандарте GSM термин "безопасность" понимается как исключение несанкционированного использования системы и обеспечение секретности переговоров подвижных абонентов. Определены следующие механизмы безопасности в стандарте GSM:

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

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

Рассмотрим последовательно механизмы безопасности в стандарте GSM, общий состав секретной информации, а также ее распределение в аппаратных средствах GSM системы. При этом будем использовать термины и обозначения, принятые в рекомендациях GSM.

Для исключения несанкционированного использования ресурсов системы связи вводятся и определяются механизмы аутентификации - удостоверения подлинности абонента. Каждый подвижный абонент на время пользования системой связи получает стандартный модуль подлинности абонента (SIM-карту), который содержит:

- международный идентификационный номер подвижного абонента (IMSI);

- свой индивидуальный ключ аутентификации (Ki);

- алгоритм аутентификации (A3).

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

Процедура проверки сетью подлинности абонента реализуется следующим образом.

Сеть передает случайный номер (RAND) на подвижную станцию. Подвижная станция определяет значение отклика (SRES), используя RAND, Ki и алгоритм A3:

$SRES = A3_{Ki}[RAND]$.

Подвижная станция посылает вычисленное значение SRES в сеть, которая сверяет значение принятого SRES со значением SRES, вычисленным сетью. Если оба значения совпадают, подвижная станция может осуществлять передачу сообщений. В противном случае связь прерывается, и индикатор подвижной станции должен показать, что опознавание не состоялось.

По причине секретности вычисление SRES происходит *в* рамках SIM. Несекретная информация (такая как Ki) не подвергается обработке в модуле SIM.

Для обеспечения секретности 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 подвижная станция вычисляет, кроме отклика SRES, также и ключ шифрования (Кс), используя RAND, Ki и алгоритм A8: $Кс = A8_{Ki}$ [RAND].

Ключ шифрования Кс не передается по радиоканалу. Как подвижная станция, так и сеть вычисляют ключ шифрования, который используется другими подвижными абонентами. По причине секретности вычисление Кс происходит в SIM.

Кроме случайного числа RAND сеть посылает подвижной станции числовую последовательность ключа шифрования. Это число связано с действительным значением Кс и позволяет избежать формирования неправильного ключа. Число хранится подвижной станцией и содержится в каждом первом сообщении, передаваемом в сеть. Некоторые сети принимают решение о наличии числовой последовательности действующего ключа шифрования в случае, если необходимо приступить *к* опознаванию или, если выполняется предварительное опознавание, используя правильный ключ шифрования. В некоторых случаях это допущение реально не обеспечивается.

Для установки режима шифрования сеть передает подвижной станции команду CMC (Ciphering Mode Command) на переход в режим шифрования. После получения команды CMC подвижная станция, используя имеющийся у нее ключ, приступает к шифрованию и дешифрованию сообщений. Поток передаваемых данных шифруется используя потоковый алгоритм шифрования A5 и ключ шифрования Кс.

Для исключения определения (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 новый TMSI. Если абоненту еще не присвоен временный номер (например, при первом включении подвижной станции), идентификация проводится через международный идентификационный номер (IMSI). После окончания процедуры аутентификации и начала режима шифрования временный идентификационный номер TMSI передается на подвижную станцию только в зашифрованном виде. Этот TMSI будет использоваться при всех последующих доступах к системе. Если подвижная станция переходит в новую область расположения, то ее TMSI должен передаваться вместе с идентификационным номером зоны (LAI), в которой TMSI был присвоен абоненту.

При выполнении процедуры корректировки местоположения по каналам управления осуществляется двухсторонний обмен между мобильной и базовой станциями служебными сообщениями, содержащими временные номера абонентов TMSI. В этом случае в радиоканале необходимо обеспечить секретность переименования TMSI и их принадлежность конкретному абоненту.

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

В этом случае подвижная станция уже зарегистрирована в регистре перемещения VLR с временным номером TMSI, соответствующим прежней зоне расположения. При входе в новую зону расположения осуществляется процедура опознавания, которая проводится по старому, зашифрованному в радиоканале TMSI, передаваемому одновременно с идентификатором зоны расположения LAI. LAI дает информацию центру коммутации и центру управления о направлении перемещения подвижной 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 передаётся как зашифрованный информационный текст с прерыванием сообщения в процессе “эстафетной передачи” на 100 – 150 мс. Процедура корректировки местоположения, включающая характеристики секретности, показана на рис. 11.

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).

Как управлять AUC будет решать тот, кому будет поручена эксплуатация сети. Интерфейс GSM с AUC не определен. AUC может решать следующие задачи:

Рис. 11. Процедура корректировки местоположения

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

- формирование набора RAND/SRES/Kc для каждого IMSI и раскрытие этих групп для HLR при необходимости.

Если подвижная станция переходит в новую зону расположения с новым VLR, новый VLR должен получить секретную информацию об этой подвижной станции. Это может быть обеспечено следующими двумя способами:

- подвижная станция проводит процедуру идентификации по своему международному номеру IMSI. При этом VLR запрашивает у регистра местоположения HLR группы данных RAND/SRES/Kc, принадлежащих данному IMSI;

- подвижная станция проводит процедуру аутентификации, используя временный прежний номер TMSI с наименованием зоны расположения LAI. Новый VLR запрашивает прежний VLR для посылки международного номера IMSI и оставшихся групп из RAND/SRES/Kc, принадлежащих этим TMSI/LAI.

Если подвижный абонент остается на более длительный период в VLR, тогда после некоторого количества доступов с аутентификацией VLR из соображений секретности потребует новые группы RAND/SRES/Kc от HLR.

Все эти процедуры определены в рекомендации GSM 09.02.

Проверка аутентификации выполняется в VLR. VLR 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). Эти же процедуры определяются в рекомендации GSM 09.02.

Введение режима шифрования в стандарте GSM выдвигает особые требования к подвижным станциям, В частности, индивидуальный ключ аутентификации пользователя Ki, связанный с международным идентификационным номером абонента IMSI, требует высокой степени защиты. Он также используется в процедуре аутентификации.

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

Основные характеристики модуля SIM определены в Рекомендации GSM 02.17.

В заключение следует отметить, что выбранные в стандарте GSM механизмы секретности и методы их реализации определили основные элементы передаваемых информационных блоков и направления передачи, на которых должно осуществляться шифрование: (RAND/SRES/Kc от HLR к VLR; RAND и SRES - в радиоканале). Для обеспечения режима секретности в стандарте GSM решены вопросы минимизации времени соединения абонентов. При организации систем сотовой радиосвязи по стандарту GSM имеется некоторая свобода в применении аспектов безопасности. В частности, не стандартизованы вопросы использования центра аутентификации AUC (интерфейс с сетью, структурное размещение AUC в аппаратных средствах). Нет строгих рекомендаций на формирование закрытых групп пользователей и системы приоритетов, принятых в GSM. В этой связи в каждой системе связи, использующей стандарт GSM, эти вопросы решаются самостоятельно.

Литература

1. M.Mouly, M.B.Pautet. The GSM System for Mobile Communications. 1992.
2. М.В. Ратынский "Основы сотовой связи", Москва, "Радио и связь", 2000.
3. Громаков Ю.А. Стандарты и системы подвижной радиосвязи. Мобильные ТелеСистемы – Эко - Трендз. Москва. 1997.
4. Р. Блейхут. Теория и практика кодов, контролирующих ошибки. Мир. 1986.
5. Дж. Кларк, Дж. Кейн. Кодирование с исправлением ошибок в системах цифровой связи. Москва. “Радио и связь”, 1987.
6. У. Диффи. Н. Хелман. Защищенность и имитостойкость: введение в криптографию. ТИИЭР.1979, т. 67. N 3. с. 71-109.

СОДЕРЖАНИЕ

Введение..... 4
1. Общие характеристики стандарта GSM……..... 6
2. Функциональная схема системы сотовой связи и ее элементы..... 8
3. Структура TDMA…… 17
4. Организация физических и логических каналов в стандарте GSM…… 23
5. Кодирование и перемежение в каналах связи и управления стандарта GSM…….. 33
6. Аспекты безопасности в стандарте GSM..... 38
Литература..... 49
..