УДК 621.382

ОЦЕНКА ОБЩИХ СИГНАЛЬНЫХ ОСОБЕННОСТЕЙ БЛОКИРОВАНИЯ МОБИЛЬНЫХ ТЕРМИНАЛОВ В СЕТЯХ GSM, GPRS И EDGE

А.Г. ГАЛКИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 14 марта 2007

Произведена оценка функциональных свойств сигнального обмена стандартов сотовой связи семейства GSM поколения 2G+ (GSM, GPRS, EDGE). Показана общность подхода при реализации сигнального обеспечения и выявлены общие особенности, позволяющие говорить о возможности реализации системного блокиратора, работающего в этих стандартах.

Ключевые слова: сотовая связь, GSM, GPRS, EDGE, системный блокиратор, сигнальный обмен.

Введение

В настоящей работе произведен анализ функциональных свойств радиообмена стандарта GSM для оценки возможности применения метода системного блокирования сотовых терминалов. Системное блокирование можно рассматривать, как применение имитационного сигнального обмена (помехи), генерируемого особой аппаратурой и приводящего к невозможности установления входящих/исходящих соединений для мобильных терминалов [1, 2]. Для этой же цели рассмотрены модификации стандарта GSM GPRS и EDGE.

Построение сети GSM, GPRS и EDGE

Для оценки общих сигнальных особенностей систем GSM и GPRS/EDGE рассмотрим построение сетей указанных систем. Структура сетей приведена на рис. 1. Из рисунка видно, что сеть GPRS/EDGE является фактически самостоятельной структурой, наложенной на базовую сеть стандарта GSM. Разделение сетей происходит в блоке контроллера-транскодера, где вводится модуль управления пакетами PCU (Packet Control Unit), направляющий пакетированные данные далее в сеть GPRS/EDGE. При этом речевые сигналы направляются на мобильный коммутатор базовой сети GSM.

Кроме того, в отличие от GSM и GPRS, где в радиоинтерфейсе $\mathbf{U}_m$ применяется модуляция GMSK с использованием 1-го бита на символ, в технологии EDGE применяется спектрально-эффективная 8-PSK модуляция с использованием 3 бит на символ. Применяется также адаптивная настройка канала в зависимости от требований и реальной помеховой обстановки. В результате, используя те же полосы частот, что GSM и GPRS, системы EDGE используют спектр эффективнее в три раза, чем GSM/GPRS-сети [3].

Для построения аппаратуры, блокирующей на общих принципах работу мобильных терминалов (МТ) всех трех систем, необходимо выбрать наиболее подходящее для этого место в сети. Можно утверждать, что это будет участок между МТ и базой (радиоинтерфейс $\mathbf{U}_m$), а также участок между базой и контроллером-транскодером (Abis интерфейс). Именно на этих

участках все три системы используют одинаковые полосы частот, близкие по логике команды управления, совпадающие каналы передачи.

Если ставится задача блокирования мобильных терминалов без внедрения соответствующей аппаратуры в инфраструктуру сети, то для этих целей остается лишь участок радиоинтерфейса $\mathbf{U}_m$.

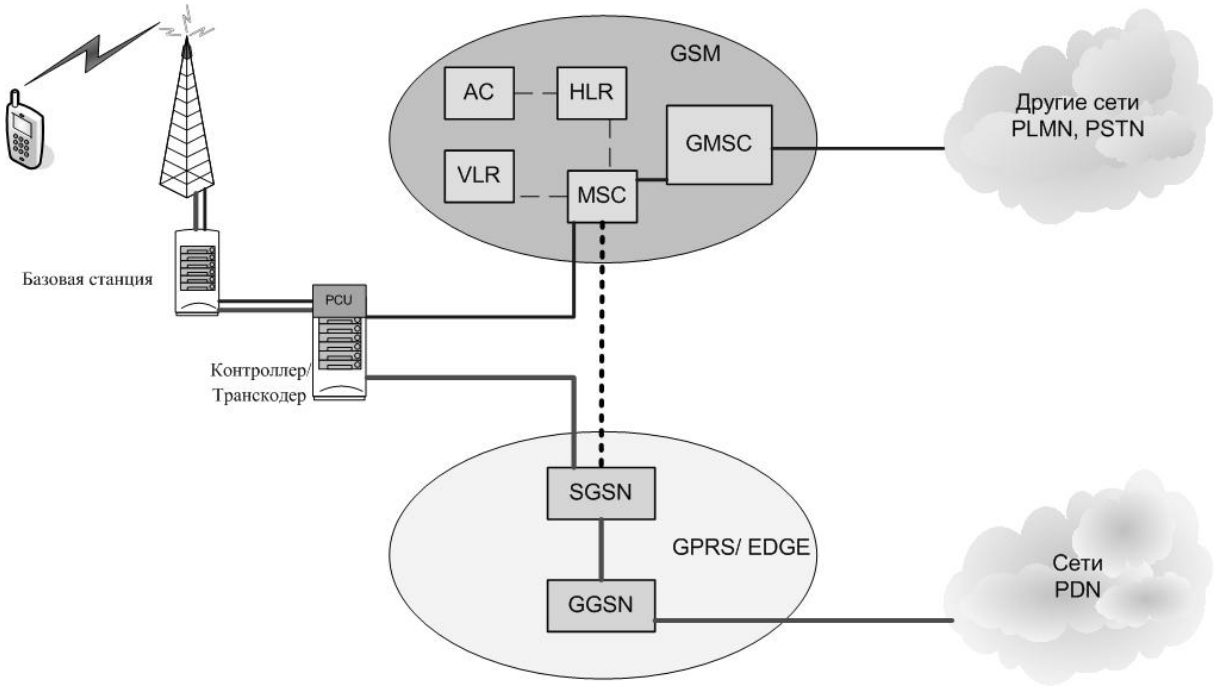

Рис. 1 Структура сети GSM, GPRS, EDGE: PCU (Packet Control Unit) — модуль управления пакетами; PDN (Packet Data Networks) — сети с коммутацией пакетов; LMN (Public Land Mobile Network) — наземная мобильная сеть общего пользования; PSTN (Public Switched Telephone Network) — телефонная коммутируемая сеть общего пользования; MSC (Mobile Services Switching Centre) — центр коммутации подвижной связи; GMSC (Gateway MSC) — межсетевой (шлюзовой) центр MSC; SGSN (Serving GPRS Support Node) — обслуживающий узел поддержки GPRS; GGSN (Gateway GPRS Support Node) — межсетевой (шлюзовой) узел поддержки услуг GPRS; AC (Authentication Centre) — центр аутентификации; VLR (Visitor location register) — регистр перемещения; HLR (Home location register) — регистр положения

Анализ функциональных свойств радиообмена базового стандарта GSM

На рис. 2 приведены диаграммы, поясняющие взаимодействие МТ с базовой станцией. Из диаграммы видно, что инициализация взаимодействия неподвижного терминала происходит согласно только двум различным сценариям — регистрации (перерегистрации) и установлению соединения. Сценарий перерегистрации не отличается по сигнальному взаимодействию от сценария регистрации. Разница заключается только в условности его запуска, в случае если терминал неподвижен — по истечению таймера. Для подвижных МТ в эти сценарии добавляется дополнительное условие перерегистрации (ч. В, п. 4 на рис. 2), когда в ходе движения МТ теряет сеть (уровень принимаемого терминалом сигнала ниже порогового значения), или меняет LA (Location Area), т.е. условно выбранную оператором область, внутри которой применяется один идентификационный номер LAC (Local Area Code). Если при перестройке с одной частоты на другую значение этого параметра меняется, инициализируется процедура перерегистрации. Сама процедура остается прежней. Логика схем взаимодействия не изменяется вне зависимости от типа соединения и протокола. Это обстоятельство позволяет говорить о возможной реализации общего логического подхода в реализации блокирования МТ.

Рис. 2. Взаимодействие неподвижного мобильного терминала и базовой станции

На рис. 3 представлена логическая модель уровней $\mathbf{U}_m$ и Abis интерфейсов в рамках описания BOC/OSI [7].

Первый уровень — это физический, второй — канальный уровень. Для интерфейсов $\mathbf{U}_m$ и Abis эти уровни идентичны. Канальный уровень представляет модифицированную версию LAPD протокола, используемого ISDN — так называемый LAPDm. В случае A-интерфейса используется MTP-протокол. Третий уровень протокола обмена сигналами GSM подразделяется на три подуровня:

подуровень управления радиоресурсами (Radio Resources Management). Отвечает за начальную установку, поддержание жизнедеятельности и организацию радиоканалов и фиксированных каналов, включая процедуры смены соты и канала (handover). Часть RR, которая передается по радиоинтерфейсу, обозначается RR;

подуровень управления мобильностью (Mobility Management). Отвечает за процедуры смены зоны (location updating) и регистрации (registration) абонента. Управляет секретностью доступа и процедурами авторизации абонента;

подуровень управления соединением (Connection Management). Отвечает за общую процедуру управления вызовом, управляет дополнительными сервисами и SMS.

В результате анализа особенностей радиоинтерфейса $\mathbf{U}_m$ может быть предложен следующий алгоритм блокирования МТ.

В зоне блокирования необходимо на задействованных рабочих частотах передавать имитацию сигналов базовой станции с уровнями, превышающими уровни настоящих сигналов.

Цель данной процедуры — подавить исходные сигналы.

Одновременно с этим необходимо генерировать несущую на новой частоте с абсолютно лучшим для блокируемого периметра уровнем, из списка тех частот, которые не присутствуют в данном месте. Зарегистрировавшись на ней, МТ не смогут общаться с домашней сетью.

Для имитации процедуры аутентификации МТ достаточно во время этой процедуры высылать мобильному терминалу подтверждения на сгенерированные им ключи.

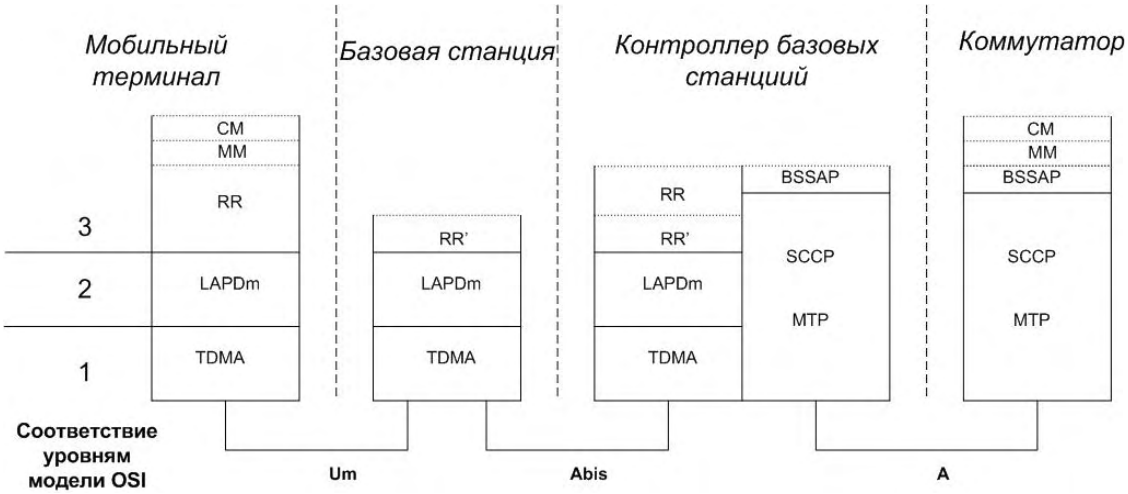

Рис. 3. Логическая модель $\mathbf{U}_m$ интерфейса и его окружение применительно к стандарту GSM

Анализ функциональных свойств радиообмена стандартов GPRS и EDGE

GPRS/EDGE — это модификация стандарта GSM с использованием существующей структуры (рис. 1). Поэтому общий подход к реализации блокиратора остается без изменений. Для GPRS/EDGE сетей интерфейсы на выше описанных участках остаются такими же, как и для GSM. Однако логическая модель уровней интерфейсов GPRS отличается от GSM, как показано на рис. 4. GSM RF (Radio Frequency) — это физический уровень (общий для GSM/GPRS/EDGE), MAC — (Medium Access Control) — канальный, RLC (Radio Link Control) — сетевой. RLC и MAC тесно связаны между собой и служат для обеспечения высоконадежной передачи данных по радиоинтерфейсу. RLC уровень при передаче сегментирует LLC (Logical Link Control) фреймы ни RLC/MAC блоки, которые затем поступают на MAC уровень. При

приеме RLC восстанавливает LLC-фреймы из RLC/MAC блоков. RLC также выполняет функции мультиплексирования, для того чтобы более одной MT могли использовать один физический канал, а одна MT могла занять до 8 TS. При передаче с подтверждением RLC уровень обеспечивает повторную передачу RLC/MAC блоков. Функции MAC уровня заключаются в управлении сигнальными процедурами через $\mathbf{U}_m$ интерфейс, необходимыми для получения доступа к сети по радиоинтерфейсу (запрос и выделение радиоканала), включая постановку пакетов в очередь в соответствии с их приоритетом. SNDCP (Subnetwork Dependent Convergence Protocol) — промежуточный протокол, устанавливающий точки входа к протоколам более высокого уровня и точки доступа к более низкому LLC уровню. Обеспечивает компрессию, сегментацию и десегментацию, мультиплексирование и демультиплексирование пакетов данных. Компрессии подвергаются абонентские данные и заголовки пакетов (опционально). Сегментация необходима для ограничения размеров пакетов, транспортируемых нижестоящим LLC уровнем по радиоинтерфейсу. Необходимая для реализации блокиратора процедура принудительной перерегистрации в GPRS, как было сказано ранее, практически не отличается от GSM. Называется эта операция RA Update (Области регистрации в GPRS могут отличаться от GSM. Если минимальная область регистрации в GSM называется Location Area, то в GPRS минимальная область называется — Routing Area.). Как и в GSM, таймер принудительной перерегистрации устанавливает оператор. Информацию о нем MT получает, принимая вещательный канал BCCH или PBCCH. Таймер периодического RA Update обнуляется и запускается вновь при возврате MT в состояние STANDBY. При переходе в состояние READY таймер останавливается. Фактически это означает, что посылка LLC-фреймов вызывает остановку таймера, так как при посылке LLC-фреймов MT переходит в состояние READY. Чтобы определить, как этого можно избежать, рассмотрим возможные состояния MT.

Мобильная станция с точки зрения радиоресурса (Radio Resource — RR) может использовать два различных режима работы. Packet Idle Mode (PIM) — когда MT свободна, и Packet Transfer Mode (PTM) — режим передачи пакетов. Каждый режим характеризуют определенные функциональные возможности. MT, находясь в PIM, анализирует PBCCH и канал пейджинга. Если каналы PBCCH и PCCCH отсутствуют в соте, то MT слушает BCCH и PCH. В PIM невозможна передача данных между MT и BSS. Если у LLC уровня возникает необходимость передачи пакетов (LLC-фреймов), то это вызывает переход в Packet Transfer Mode. В PTM мобильной станции выделяется радиоресурс для организации передачи на одном или нескольких физических каналах. Возможна последовательная передача одного или нескольких LLC-фреймов. Передача может быть установлена в противоположных направлениях. Трансфер LLC-фреймов может происходить как с подтверждением на уровне RLC, так и без подтверждения. Нахождение MT в Packet Transfer Mode контролируется таймером RLC протокола. Этот таймер запускается после окончания транзакции. Если до его истечения активность не наблюдается, мобильный терминал переводится в состояние Packet Idle Mode. Необходимо отметить, что в зависимости от класса MT одновременно с передачей данных может осуществляться контроль за GSM запросами. Так MT класса A, находясь в PIM или PTM, может одновременно осуществить соединение для услуг с коммутацией каналов. MT класса B, должен покинуть Packet Idle Mode или Packet Transfer Mode перед переходом в такой режим. Работа MT в PTM возможна только, когда MT находится в состоянии READY. Режим Packet Idle Mode возможен при нахождении MT как о состоянии READY, так и в состоянии STANDBY. В состоянии IDLE мобильная станция с точки зрения радиоросурса является недоступной и не поддерживает ни Packet Idle Mode, ни Packet Transfer Mode [13].

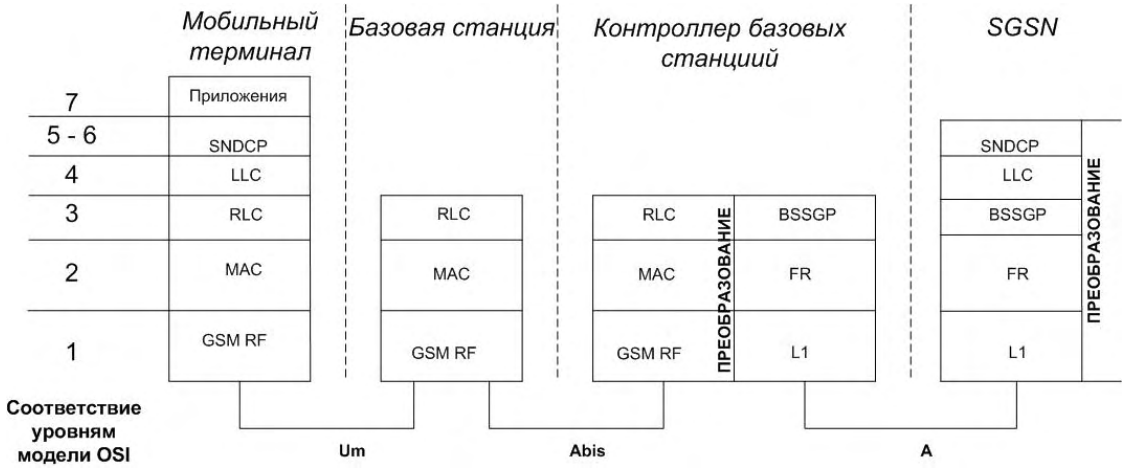

Рис. 4. Логическая модель $\mathbf{U}_m$ интерфейса и его сигнальное окружение применительно к стандарту GPRS, EDGE

Таким образом, для реализации функционирования блокиратора в GPRS сетях необходимо:

1. Используя имитационный модулированный сигнальный канал, передавать минимальное значение таймера RLC протокола. Это приведет к тому, что терминалы, которые находились в состоянии передачи пакетов в минимальный интервал, перейдут в состояние Packet Idle Mode; соответственно изменится статус MT с READY на STANDBY.
2. Поскольку в модулированном канале LLC-фреймы не передаются, все терминалы в состоянии STANDBY запустят таймер периодического RA Update, данные о значении которого передает блокиратор.
3. По истечении таймера все терминалы начнут поиск сети, и в результате выполнения алгоритма анализа несущих предпримут попытку регистрации на частоте, генерируемой блокиратором;. блокиратор беспрепятственно даст возможность зарегистрироваться всем MT, предпринявшим такую попытку.

Так как технология EDGE отличается от GPRS только способом кодирования канальной информации, все вышесказанное в полной мере будет работать и в EDGE сетях.

Заключение

Таким образом, на основе анализа сигнального обмена стандартов GSM, GPRS и EDGE показана возможность применения системного блокирования мобильных терминалов.

Для стандарта GSM предложен алгоритм принудительной регистрации мобильных терминалов на генерируемой блокиратором фиктивной частоте.

Для реализации блокиратора в GPRS/EDGE сетях предлагается передавать минимальное значение таймера RLC протокола с дальнейшей регистрацией терминалов на фиктивной несущей.

ESTIMATION OF COMMON A SIGNAL FEATURES FOR BLOCKING OF MOBILE TERMINALS IN NETWORKS GSM, GPRS AND EDGE

A.G. GALKIN

Abstract

The estimation of functional properties of a signal exchange of standards of a cellular transmission of family GSM, generation 2G+ (GSM, GPRS, EDGE) is made. The generality of the approach is shown at realization of signal provision and the common features are revealed, allowing to speak about an opportunity of realization system-jammer operating in these standards.

Литература

1. *Хореев А.А.* // Специальная техника 2006. № 5. С. 55–64.
2. *Галкин А.Г., Конопелько В.К.* //Докл. БГУИР. 2005. № 6. С. 56–61
3. Anders Furusk.r, Jonas N.slund and H.kan Olofsson // 136 Evolution Ericsson Review. 1999. No. 1. P. 28–37.
4. Siemens Information System Description D900/D1800, Network System Concept, A50016-D1109-V10-4-7618 Siemens AG 2000.
5. Huawei Training center. 2001-10 "M900/M1800 BSS principle part training multimedia materials (Engineer)".
6. Bernd F. GSM Network Management.
7. ETSI TC-SMG. "Digital cellular telecommunications system; Base Station Controller – Base Transceiver Station (BSC - BTS) interface principles" (GSM 08.52).
8. ETSI TC-SMG. "Digital cellular telecommunications system; Security Aspects" (GSM 02.09).
9. ETSI TC-SMG. "Digital cellular telecommunications system; Subscriber Identity Modules" (GSM 02.17).
10. ETSI TC-SMG. "Digital cellular telecommunications system; Security Related Network Functions" (GSM 03.20).
11. ETSI TC-SMG. "Digital cellular telecommunications system; Security Related Algorithms" (GSM 03.21).
12. Siemens, MN2712EU21MN_0001 "PLMN GPRS/UMTS CN standard maintenance tasks"
13. *Кузнецов М.А., Абатуров П.С., Никодимов И.Ю. и др.* GPRS-технология пакетной передачи данных в сетях GSM СПб., 2002.