УДК 621.395.34

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ СОРМ В СЕТЯХ LTE

В.О. Тихвинский, заместитель генерального директора ОАО «Гипросвязь» по инновационным технологиям, д.э.н., проф.; vtniir@mail.ru
С.В. Терентьев, руководитель центра инновационных технологий и услуг ОАО «Гипросвязь», к.т.н.
В.П. Высочин, вице-председатель ИТТ РАЕН, к.т.н.

Ключевые слова: *система технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ), сеть мобильного беспроводного доступа, функциональный модуль СОРМ, контроль и перехват сообщений, контентные сообщения, служебная сетевая информация, интерфейс хендовера, функциональная модель СОРМ.*

В ожидании появления на телекоммуникационном рынке России сетей мобильного беспроводного доступа на базе технологий LTE (Release 8, 9) [1] и LTE Advanced (Release 10), поддерживающих стандарты МСЭ (скорость передачи данных в каналах радиоинтерфейса до 1 Гбит/с в линиях «вниз» и «вверх»), необходимо сформулировать соответствующие требования к системе технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ) для этих сетей [2].

В настоящее время существует нормативно-техническая база обеспечения СОРМ для LTE и LTE Advanced, разработанная Техническим комитетом Lawful Interception («Законный перехват») Европейского института стандартизации электросвязи (ETSI) [3–10]. Однако СОРМ сети LTE в России должна удовлетворять не только европейским, но и национальным требованиям к СОРМ в сетях передачи данных [2].

В уже развернутых сегодня сетях LTE реализованы функции высокоскоростной передачи речи на основе технологии All-IP, и контролируемая СОРМ информация контентных сообщений (Content of Communication, CC) относится к IP-уровню сети LTE [10], поэтому ниже рассматриваются функциональные особенности СОРМ этих сетей при передаче данных в режиме пакетной коммутации. В дополнение к контентным данным решения СОРМ сети LTE (EPS) позволяют генерировать файлы служебной сетевой информации контроля и перехвата данных (Intercept Related Information, IRI) с сообщениями плоскости управления сетью, относящимися к уровню сигнализации.

Сообщения IRI включают собираемые в интересах СОРМ данные, которые связаны с телекоммуникационными услугами, используют целевые идентификаторы со специальными связями, ассоциированными с информацией и данными абонента (включая неудачные попытки присоединений и вызовов), с услугами, имеющими отношение к передаваемой информации и данным (например, управление профилем услуг абонентом), а также информацию о расположении абонента.

Контентные сообщения (CC) представляют собой информацию, передаваемую в сети между двумя или большим числом пользователей, за исключением сообщений IRI. CC могут быть частью телекоммуникационных услуг и сохраняются для каждого пользователя с целью их восстановления.

Услуги присоединения IP-уровня сети LTE поддерживают услуги уровня приложений для абонентов этой сети: прием/передачу e-mail, веб-поиск, услуги FTP, речевые аудиоуслуги (VoIP, PoC), другие мультимедийные услуги (MBMS, видеотелефония).

Особенности архитектуры СОРМ для режима пакетной коммутации. Логическая конфигурация СОРМ сети LTE, определяемая техническими спецификациями 3GPP и используемая для решения задач контроля и перехвата сообщений, может не соответствовать делению на физические функциональные модули, реализуемые различными разработчиками СОРМ для сетей LTE. Эта система обычно содержит логические функциональные модули администрирования (ADMinistrative Function, ADMF), передачи (Delivery Function, DF), сопряжения (Mediation Function, MF), мониторинга (Law Enforcement Monitoring Facilities, LEMF) и интерфейсы типа X и HI (Handover Interface).

Функциональная модель СОРМ, используемая для активации/дезактивации СОРМ и формирования запросов при контроле и перехвате сообщений в сети LTE, показана на рис. 1. Она включает модули ADMF, DF2 и DF3, а также традиционных сетевых функций LTE, контролируемых СОРМ: LTE ICE, реализуемых домашним сервером абонентских данных (Home Subscriber Server, HSS), модулем управления мобильностью (MME), сервисным (S-GW) и пакетным (P-GW) шлюзами.

Таким образом, в функциональной модели СОРМ сети LTE дополнительно к типовым сетевым модулям (MME, S-GW, P-GW, HSS), контролируемым СОРМ, используется еще ряд специализированных функциональных модулей. Рассмотрим более детально их функции и задачи.

Модуль администрирования (ADMF) обеспечивает [5–8]:

- взаимодействие со всеми субъектами правоохранительных органов, которым необходим доступ к информации СОРМ соответствующей сети LTE;
- поддержку деятельности СОРМ на основе индивидуального разделения информации СОРМ между различными субъектами правоохранительных органов;
- взаимодействие с контролируемой сетью.

В сети LTE используется только один модуль ADMF.

Модули функции передачи (DF) системы СОРМ используются для распределения:

- служебной сетевой информации контроля и перехвата данных (IRI) по соответствующим уровню доступа субъектам правоохранительных органов посредством интерфейса хендовера HI2 на основе назначенных географических зон (IA) контроля и перехвата сообщений;
- информации контентных сообщений по соответствующим уровню доступа субъектам правоохранительных органов посредством интерфейса хендовера HI3 на основе назначенных географических зон (IA) контроля и перехвата сообщений.

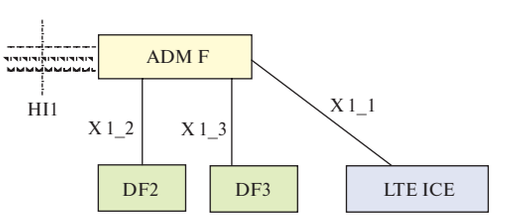

Рис. 1

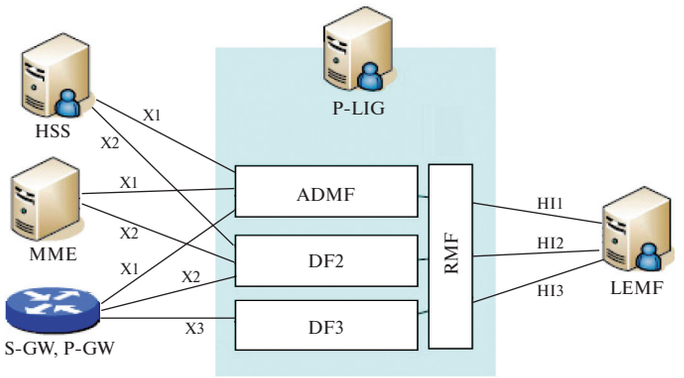

Рис. 2

Функциональные модули RMF (Regional Mediation Function) или MF являются модулями сопряжения, или модулями-посредниками. Они выполняют частично функции администрирования и доставки информации СОРМ, а также используются для преобразования информации СОРМ, передаваемой по интерфейсам хендовера HI1, HI2 и HI3, в форматы, основанные на национальных и региональных стандартах. Например, при использовании в СОРМ требований технических спецификаций ETSI TS 101 671 [10] или ANSI J-STD-025 [11] интерфейсы HI1, HI2 и HI3 будут адаптированы к этим спецификациям. (Стандарт ETSI ES 201 671 [12] является более ранней версией TS 101 671 и не содержит последних изменений.)

Для объединения функциональных модулей сети LTE, относящихся к СОРМ, используется специальный пакетный шлюз P-LIG (Packet Lawful Interception Gateway). В него (рис. 2) включена вся совокупность служебных модулей:

ADMF – обеспечивает контроль сообщений правоохранительными органами внутри сетевых элементов LTE;

DF2 – собирает контролируемую СОРМ сигнальную информацию от элементов сети LTE (например, команду Attach);

DF3 – собирает контролируемую СОРМ информацию обмена служебными данными от элементов сети LTE и выполняет две важнейшие функции: контроля вызовов (сигнализации) и транспорта служебной информации для контентных сообщений;

RMF – обеспечивает возврат контролируемой СОРМ информации к модулю мониторинга LEMF в воспринимаемом правоохранительными органами формате данных;

LEMF – собирает контролируемую СОРМ информацию от лица соответствующего субъекта национального правоохранительного органа.

Каждый физический модуль сети LTE, подлежащий контролю СОРМ: MME, S-GW, P-GW, HSS, – соединен собственным X1-интерфейсом с модулем ADMF.

Спецификациями 3GPP определяются следующие интерфейсы, обеспечивающие СОРМ для модулей HSS, MME, S-GW и P-GW:

- интерфейсы X1_1, X1_2 и X1_3 – переносят обеспечивающую СОРМ сетевую информацию;
- интерфейс X2 – переносит информацию сигнализации, собираемую для СОРМ;
- интерфейс X3 – переносит СОРМ информацию служб обмена сети LTE;
- интерфейсы хендовера HI1, HI2 и HI3 – обеспечивают взаимодействие модулей СОРМ сети LTE с оборудованием мониторинга для законного прослушивания (LEMF).

Каждый физический модуль из входящих в совокупность модулей LTE ICE (MME, S-GW, P-GW, HSS) соединен собственным интерфейсом X1_1 с модулем администрирования ADMF. Соответственно каждый модуль из LTE ICE выполняет функции СОРМ (активацию, деактивацию, опрос, запуск вызываемого модуля) независимо от остальных модулей.

Целевые идентификаторы (параметры сети, подлежащие контролю со стороны СОРМ) могут быть представлены одним из следующих параметров сети LTE [1, 13]: IMSI, MSISDN (СОРМ только пакетных данных) или IMEI (СОРМ при передаче пакетных данных), возможности использования которых в интересах СОРМ детально рассмотрены в технических спецификациях TS 23.060.

Некоторые виды передаваемого контента в процессе обеспечения процедуры мобильности не могут быть подвергнуты контролю и перехвату, если они основаны на параметре MSISDN или IMEI. Использование в качестве целевого идентификатора параметра IMSI не приводит к ограничениям в обеспечении СОРМ.

Целевые идентификаторы, контролируемые СОРМ при передаче мультимедийных услуг с использованием модуля подсистемы IMS CSCF (Call Session Control Function – функция управления сеансами вызовов), могут быть следующими: SIP URI или TEL URL.

Для обеспечения СОРМ в сети LTE в режиме пакетной коммутации (PS interception) использована функциональная архитектура, которая реализует законный контроль и перехват сообщений применительно к основным узлам LTE (EPS): MME, S-GW, P-GW, HSS. На рис. 3 показана конфигурация СОРМ для модуля управления мобильностью MME (*а*), HSS (*б*) и для шлюзов S-GW, P-GW (*в*).

Сетевые интерфейсы, обеспечивающие СОРМ в сети LTE. Интерфейс X1_1 используется для передачи сообщений от модуля управления ADMF к модулям, охваченным СОРМ в сети LTE (ICE), таких как:

- целевые идентификаторы (MSISDN, IMSI, IMEI, SIP URI или TEL URL, NAI);
- информация о содержании предоставляемого контента;
- адрес модуля передачи DF2 для контроля и перехвата соответствующей служебной информации IRI;
- адрес модуля передачи DF3 для контроля и перехвата контентных сообщений;
- значение параметра географической зоны (IA) СОРМ сети LTE в случае географически зависимой СОРМ.

Пример информационного обмена по интерфейсу X1_1 для активации СОРМ приведен на рис. 4.

После активации командой Activation change request изменений в передаче сообщений CC или IRI они также могут быть переданы для идентификации.

Задача перехвата сообщений активируется по запросу от различных субъектов правоохранительных органов, каждый из которых может запросить перехват посредством различных идентификаторов. В этом случае контролируемый целевой идентификатор объекта перехвата необходимо передавать при помощи раздельных сообщений активации от модуля ADMF к модулям LTE ICE по интерфейсу X1_1. Каждая активация может быть выполнена как для IRI, так и для CC и IRI.

Когда несколько субъектов правоохранительных органов запрашивают активацию СОРМ на основе одного и того же идентификатора, ADMF сначала определяет, существует ли уже активация этого идентификатора, а затем этот модуль (как внедренная опция) может передать дополнительное со-

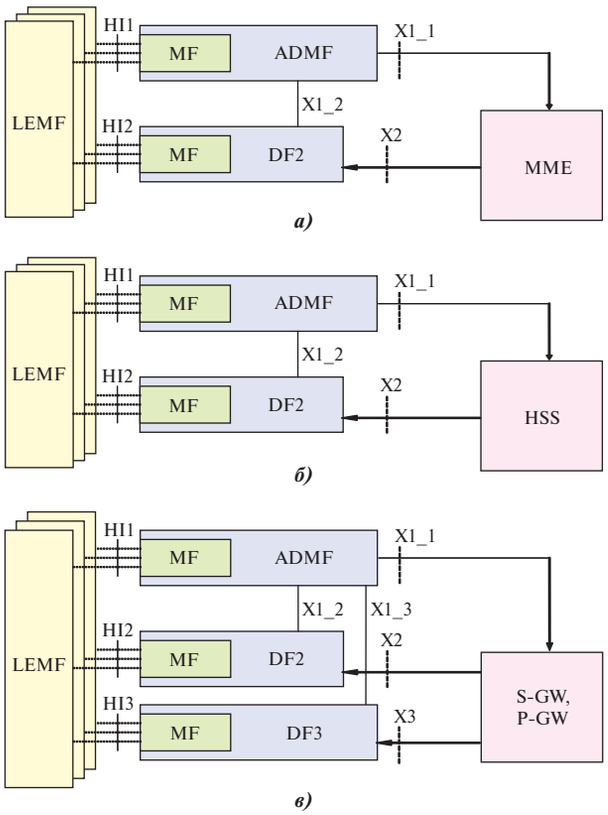

Рис. 3

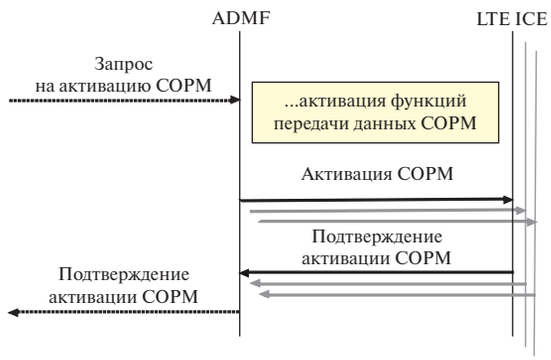

Рис. 4

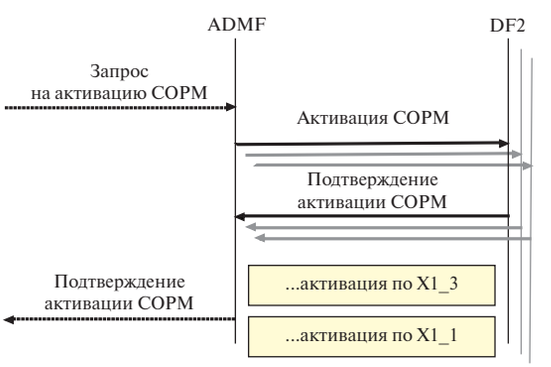

Рис. 5

общение активации модулям LTE ICE. Когда активация необходима, чтобы произвести изменения в целях перехода от данных IRI только к CC или только к IRI, в модули LTE ICE должна быть отправлена команда Activation change message.

В случае повторной активации COPM только вызывавшие ее субъекты правоохранительных органов получат соответствующие данные IRI.

Интерфейс X1_2 (IRI) предназначен для активации сообщений IRI и передачи команд от ADMF к DF2, которые содержат:

- целевые идентификаторы объекта перехвата;
- адрес доставки сообщений IRI, соответствующих адресу LEMF;
- идентификатор активации модуля передачи DF2, который уникальным образом идентифицирует его процедуру активации и используется для дальнейшего запуска вызываемого модуля или его деактивации;
- зону охвата IA в случае использования географически зависимой COPM;
- гарантированный номер ссылки, если он требуется в национальной опции COPM.

Пример информационного обмена по интерфейсу X1_2 для активации COPM приведен на рис. 5.

Если целью контроля и перехвата сообщений является COPM для нескольких субъектов правоохранительных органов по нескольким идентификаторам одновременно, передача соответствующей команды активации COPM потребуется для каждой комбинации субъектов правоохранительных органов (Law Enforcement Agency, LEA) и параметра идентификации.

Интерфейс X2 позволяет передавать от сетевых модулей MME, S-GW, P-GW, HSS к модулю передачи DF2 следующую информацию:

- целевые идентификаторы объекта перехвата (MSISDN, IMSI и IMEI);
- идентификаторы IA в случае использования географически зависимой COPM;
- данные о состоянии абонентского терминала-объекта перехвата (команды: Mobile Station Attach; Mobile Station Detach; активация PDP-контекста; начало выполнения перехвата с присоединения мобильной станции (национальная опция); начало выполнения перехвата с активации PDP-контекста; модификация PDP-контекста; деактивации PDP-контекста; обновление зоны RA Routing Aria); передача SMS и др.);
- идентификатор QoS;
- коррелированный номер объекта перехвата;
- параметры кодирования (ключи и соответствующие параметры для декодирования CC).

Сообщения IRI передаются в модуль DF2 с использованием определенного механизма передачи данных.

Интерфейс X3 при контроле и перехвате CC передает от модулей MME, S-GW, P-GW, HSS к DF3 следующую информацию:

- целевые индикаторы объекта перехвата;
- коррелированный номер объекта перехвата;
- временной ярлык файла (time stamp);
- направление потока данных (TPDU инициирует сессию (MO) или терминирует ее (MT));
- размещение абонента-объекта перехвата или параметры IA в случае использования географически зависимой COPM.

Процедура управления COPM для контентных сообщений в соответствии с роуминговыми соглашениями и функционирование COPM могут изменяться с учетом национальных особенностей управления сетью LTE.

Интерфейсы хендовера HI1, HI2 и *HI3*, определяемые как интерфейсы между субъектами LEA и модулем админис-

трирования, обеспечивают взаимодействие с оборудованием мониторинга для законного прослушивания [10]. Интерфейсы хендовера, используемые COPM, представляют собой физические и логические интерфейсы внутри сети, предназначенные для контроля и перехвата сообщений, запрашиваемых от оператора сети/ провайдера доступа/ провайдера услуг (NwO/AP/SvP). Их результаты доставляются оборудованию мониторинга для законного прослушивания (LEMF).

HI1, двунаправленный интерфейс между оператором сети LTE и субъектом LEA, обеспечивает оператора сети LTE детальной информацией об объекте перехвата и контроля для осуществления процедуры COPM, обычно в форме гарантии правоохранительного органа, содержащей детальную информацию об объекте COPM. Разрешение на проведение законного прослушивания и перехват сообщений спецслужба по интерфейсу HI1 доводит до оператора сети/ провайдера доступа/ провайдера услуг (NwO/AP/SvP) [14].

HI2 и HI3, однонаправленные интерфейсы от оператора сети LTE к субъекту LEA сообщений IRI и CC при проведении COPM, соединяют соответствующие модули передачи DF2 и DF3 COPM сети LTE и субъекты правоохранительных органов. Являясь интерфейсом к оборудованию мониторинга для законного прослушивания (LEMF), HI3 обеспечивает управление сигнализацией и транспортировкой служебных данных для контентных сообщений. На рис. 3 HI2 представлен как интерфейс между LEA и DF2 (модулем передачи сообщений IRI).

Сценарии обеспечения COPM сети LTE. Можно рассмотреть три сценария обеспечения COPM сети LTE, которая при общей глобальной базе абонентов HSS имеет внутреннее деление на несколько федеральных округов, где сети соседних округов по отношению к собственной сети являются визитными.

Все три сценария имеют общие условия: абонентский терминал (User Equipment – UE) запрограммирован на обеспечение COPM при взаимодействии с модулями S-GW, P-GW и MME собственной сети и общей глобальной базой абонентов оператора сети LTE. Особенности сценариев:

В сценарии 1 процедура COPM не обеспечивается в других активированных для COPM сетевых модулях (S-GW, P-GW и MME) за пределами собственной сети LTE. Абонентский терминал UE инициирует сессию в собственной сети, которая маршрутизируется на собственный шлюз P-GW.

Шлюз COPM P-LIG собственной сети перехватывает следующие сообщения:

- сигнализацию модуля HSS (Update Location и др.);
- сигнализацию модуля MME собственной сети (Attaches, Bearer requests и др.), информацию Cell ID;
- сигнализацию (Bearer setup и др.) и служебный трафик сервисного узла S-GW собственной сети;
- сигнализацию (Bearer setup и др.) и служебный трафик пакетного узла P-GW собственной сети.

В сценарии 2 COPM не активирована для других визитных соседних сетей. Абонентский терминал UE инициирует сессию в визитной сети, и инициированная сессия маршрутизируется в собственную сеть через шлюз PGW.

Шлюз COPM P-LIG собственной сети перехватывает следующие сообщения:

- сигнализацию модуля HSS (Update Location и др.);
- сигнализацию (Bearer setup и др.) и служебный трафик пакетного узла P-GW собственной сети.

В сценарии 3 COPM не активирована для других визитных соседних сетей. Абонентский терминал UE инициирует сессию в визитной сети, и инициированная сессия маршрутизируется в собственную сеть через шлюз PGW.

Шлюз COPM P-LIG перехватывает сигнализацию только модуля HSS (Update Location и др.).

Таким образом, посещение абонентом визитных сетей других федеральных округов потребует создания COPM сети LTE и в этих федеральных округах.

Заключение. Обозначим основные особенности построения COPM сети LTE:

- точками перехвата сообщений являются типовые сетевые модули сети LTE: MME, S-GW, P-GW, HSS на уровне собственной сети;
- для реализации COPM следует использовать специальный пакетный шлюз P-LIG, объединяющий функциональные модули сети LTE, относящиеся к COPM: ADMF, DF, MF, LEMF и интерфейсы типа X, HI;
- перемещение абонентского терминала внутри других регионов обслуживания сети потребует обеспечения COPM внутри визитного региона.
- COPM сети LTE, реализованная в виде шлюза P-LIG, кроме основных задач COPM, также обеспечивает:
- взаимодействие с субъектами нескольких правоохранительных органов;
- использование географически зависимой COPM и фильтрацию размещения абонента в зоне местоположения (Tracking Area, TA) или соте (субрегионе);
- ограничение передачи управления COPM в сети LTE через регионы обслуживания.

Особенности построения ЕСС России потребуют системного дизайна при создании COPM сети LTE на основе национальных процедур, проводимых в ходе оперативно-розыскных мероприятий.

ЛИТЕРАТУРА

1. **Тихвинский В.О., Терентьев С.В., Юрчук А.Б.** Сети мобильной связи LTE: технологии и архитектура // М.: Эко-Трендз, 2010.
2. Приказ от 27 мая 2010 г. № 73 Минкомсвязи РФ «Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Ч. II. Требования к сетям передачи данных» (Зарегистрирован в Минюсте РФ 07.07.2010 № 17748).
3. **Гольдштейн Б.С., Елагин В.С.** Законный перехват сообщений: подходы ETSI, CALEA И COPM// Вестник связи/ - 2007. - №3.
4. ETSI TS 101 331: «Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies».
5. ETSI ES 201 158: «Lawful Interception; Requirements for network functions».
6. ETSI ES 201 671: «Handover Interface for the lawful interception of telecommunications traffic».
7. 3GPP TS 33.106: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements.
8. 3GPP TS 33.107: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 10).
9. 3GPP TS 23.008: 3rd Generation Partnership Project; Technical Specification Group Core Network; Organization of subscriber data.
10. ETSI TS 101 671: Handover Interface for the lawful interception of telecommunications traffic (step 3).
11. ANSI J-STD-025-A: Lawfully Authorized Electronic Surveillance.
12. ETSI ES 201 671: Handover Interface for the lawful interception of telecommunications traffic.
13. 3GPP TS 23.060: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description.
14. **Гольдштейн Б.С., Крюков Ф.Ю., Хегай И.П.** Инженерные аспекты COPM //Вестник связи. – 2005. – № 9.

Получено 17.01.11