электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 02, февраль 2016

УДК 004.057.4+621.395.74

Разработка системы декодирования стека протоколов ОКС-7 в подсистеме коммутации сети сотовой связи

***Батусов П. В.**, студент*
кафедра «Теоретическая информатика и компьютерные технологии»
Россия, 1050005, г. Москва, МГТУ им. Н.Э. Баумана

Научный руководитель: Вишняков И.Э., ст. преподаватель
Россия, 1050005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Теоретическая информатика и компьютерные технологии»
vishnyakov@bmstu.ru

Введение. В настоящее время в мире широко используется технология мобильной сотовой связи для общения и передачи информации между людьми. Основные составляющие сотовой сети — это сотовые телефоны и базовые станции, которые поддерживают постоянный радиоконтакт, периодически обмениваясь сообщениями. Сотовый (мобильный) телефон позволяет абоненту пользоваться всеми услугами оператора связи посредством отправки данных в сеть через базовые станции. Если телефон выходит из поля действия одной базовой станции (или качество радиосигнала сервисной соты ухудшается), он налаживает связь с другой. Кроме того, операторы различных сотовых сетей могут заключать между собой договоры роуминга, благодаря которым абонент, находясь вне зоны покрытия своей сети, может совершать и принимать звонки через «чужую» сеть, а операторы получают возможность совместно использовать инфраструктуру сети, сокращая затраты на её развертывание.

Современные GSM-сети имеют сложную структуру, состоящую из подсистем, ответственных за хранение и обеспечение доступа к данным абонентов, установку и поддержку соединения, а также предоставление различных дополнительных услуг. Для выполнения вышеперечисленных функций активно используются базы данных, в которых хранится вся необходимая информация об абонентах сети: их текущее местоположение, тарифный план, данные необходимые для коммутации вызова и отправки текстовых сообщений. [1].

При мониторинге сотовых сетей возникает задача разбора большого объема данных, имеющих разное представление и структуру, с возможностью сохранения

декодированных результатов в базу. В данной работе описана разработанная модель данных, которую можно легко расширить для хранения новых типов сообщений, а также рассмотрена реализация системы, решающей вышеописанную задачу.

Структура сети GSM. GSM core network (базовая сеть) является центром сотовых сетей стандарта GSM. В её задачи входит предоставление GSM-сервисов, таких как голосовые звонки, SMS, и передача данных по коммутируемым линиям. На рисунке 1 показана структура подсистем базовых станций и коммутации. GSM состоит из трёх основных подсистем: подсистемы базовых станций (BSS — Base Station Subsystem), подсистемы коммутации (NSS — Network Switching Subsystem) и центра технического обслуживания (OMC — Operation and Maintenance Centre). В отдельный класс оборудования GSM выделены терминальные устройства — подвижные станции (MS — Mobile Station), также известные как сотовые телефоны.

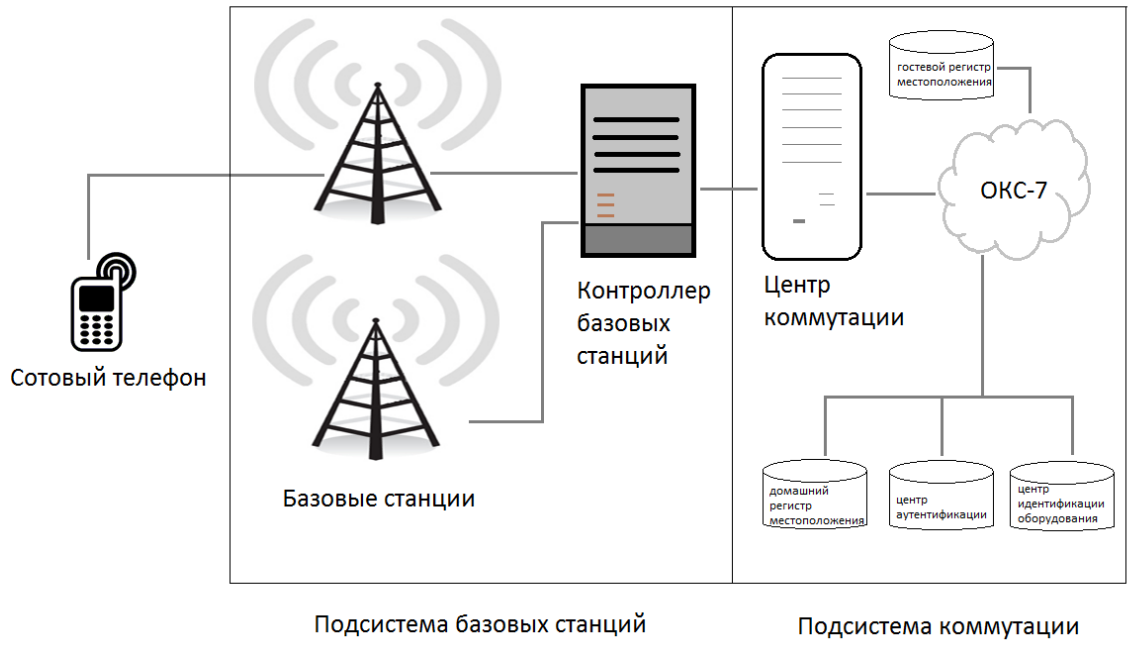

Рис. 1. Структура подсистем базовых станций и коммутации

Главным элементом подсистемы коммутации и всей сети является центр коммутации (MSC – Mobile Switching Center). Он отвечает за установку соединения, выполняет функции маршрутизации вызовов, занимается эстафетной передачей обслуживания при перемещении абонента из одной соты в другую и многим другим, включая сбор статистических данных на конкретной географической территории. Кроме

этого, MSC постоянно отслеживает местоположение пользователей, чтобы быстро установить соединение при вызове.

Для хранения информации о местоположении абонентов используются домашний регистр местоположения (HLR – Home Location Registry) и гостевой регистр местоположения (VLR – Visitor Location Registry). Каждый пользователь сети приписан к определенному домашнему регистру местоположения, в чью базу данных попадает информация о предоставляемых услугах, международный идентификатор мобильного абонента (IMSI – International Mobile Subscriber Identity) и данные, необходимые в случае вызова. Гостевой регистр местоположения содержит абонентскую базу данных со всей информацией о подвижных абонентах, в том числе роумерах – абонентах другой системы GSM, временно использующих услуги данной системы в рамках процедуры роуминга.

При регистрации мобильного телефона в сети происходит также аутентификация модуля идентификации абонента (SIM – Subscriber Identification Module). Этим занимается центр аутентификации (AUC – Authentification Center) – защищенная база данных, которая накапливает копии ключей шифрования, хранящихся в SIM-карте каждого абонента. Операторы сотовой связи сами определяют, в какой момент будет происходить аутентификация абонента.

При передаче данных между узлами сети используется набор сигнальных телефонных протоколов ОКС-7 (общеканальная сигнализация №7) [2], а также его расширение – протокол SIGTRAN, поддерживающий те же приложения и парадигмы управления вызовами, но использующий Интернет-протокол (IP) [3]. ОКС-7 обеспечивает процедуры установления, поддержки и завершения соединения, а также согласования различных параметров, связанных с отправкой и получением информации для абонентов [4]. Так, например, через систему сигнализации реализуется процедура хэндовер (Handover) – смена абонентом канала связи во время разговора без потери соединения [5]. При декодировании сообщений этой процедуры можно получить информацию о перемещении абонента (его старое и текущее местоположение).

Одними из основных уровней ОКС-7 являются: прикладная часть средств транзакций (TCAP – Transaction Capabilities Application Part) и часть мобильных приложений (MAP – Mobile Application Part), которые вместе составляют прикладную часть сообщения сети. Уровень TCAP необходим для поддержания диалогов между элементами сети. Все TCAP сообщения имеют номера – идентификаторы транзакций, которые используются для отделения одного диалога от другого.

Часть мобильных приложений, вложена в TCAP, и именно в MAP содержится прикладная часть транзакций. Вся информация представлена в виде сообщений, каждое из которых имеет заголовок, содержащий длину и тэг, а также данные, которые в свою очередь могут быть сообщением или массивом сообщений. Иногда длина сообщения не указывается явно, а концом служит специальный маркер – EOC (End of Contents). Все сообщения делятся на два класса: конструкторы, состоящие из других сообщений, и примитивы, чьи данные сообщением не являются.

Разработка системы декодирования и сохранения результатов. Для приложения-декодировщика обязательным критерием является возможность разбора сетевого трафика в режиме «реального времени»: обработка данных должна производиться быстрее, чем будет получена новая порция для разбора. Вся система разделена на два модуля: декодирования сообщений сети и загрузки полученных результатов в базу (рис. 2).

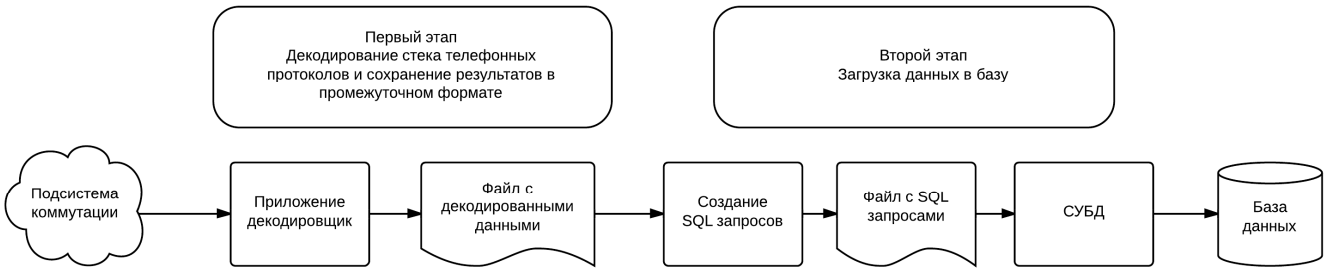

Рис. 2. Схема обработки данных

На рисунке 3 представлена схема работы системы декодирования. При получении очередного сетевого пакета, производится попытка его разбора, в результате которой могут возникнуть ошибки (например, если данные пакета были повреждены при передаче в сети). Информация о пакетах, и причины, по которым их не получилось декодировать, сохраняются в журналах событий. Если разбор произошел удачно, то начинается обработка полученных данных, после которой происходит разбор следующего пакета.

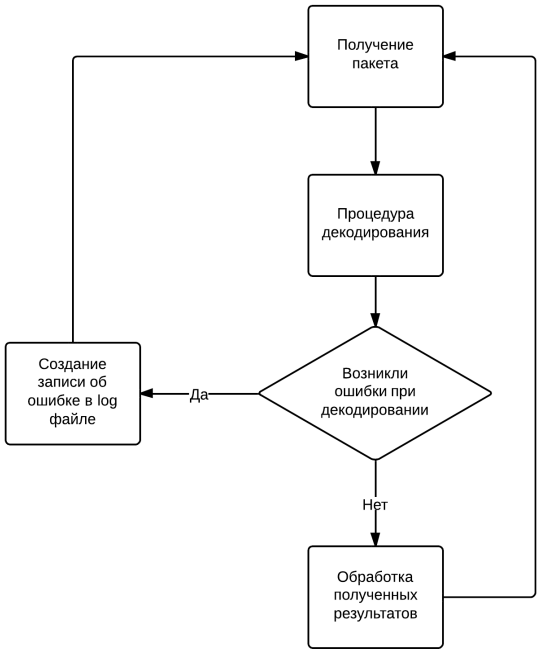

Рис. 3. Схема работы системы декодирования

При декодировании TCAP сообщений определяются их типы, идентификаторы транзакций и количество вложенных MAP-компонент. Эта информация используется для дальнейшего разбора и обработки результатов. Для каждого MAP сообщения создается своя функция для его декодирования. На рисунке 4 показан пример возможного TCAP сообщения, содержащего ошибку в одном из вложенных MAP сообщений. В данном случае возможно частичное декодирование, так как заголовок сообщения не повреждён, в нём указана длина, а значит, его можно пропустить и перейти к декодированию следующего MAP сообщения. Такая операция невозможна, если используется маркер EOC для пометки окончания блока данных и длина вложенного сообщения неизвестна.

После декодирования пакета, полученные результаты нельзя сразу поместить в базу данных, так как один пакет может содержать в себе лишь часть диалога (за исключением MAP-сообщений, которые переносят в себе сразу все необходимые данные, например, SMS-сообщения, состоящие только из одной части). Разобранные данные помещаются в программный буфер сообщений, а после того как будут получены недостающие части диалога – записаны в базу данных. Возможны случаи, когда из-за аппаратных ошибок некоторые сообщения диалога не попадут на обработку программы и для того, чтобы они не засоряли программный буфер, создана процедура очистки, обеспечивающая удаление сообщений по истечении некоторого таймаута.

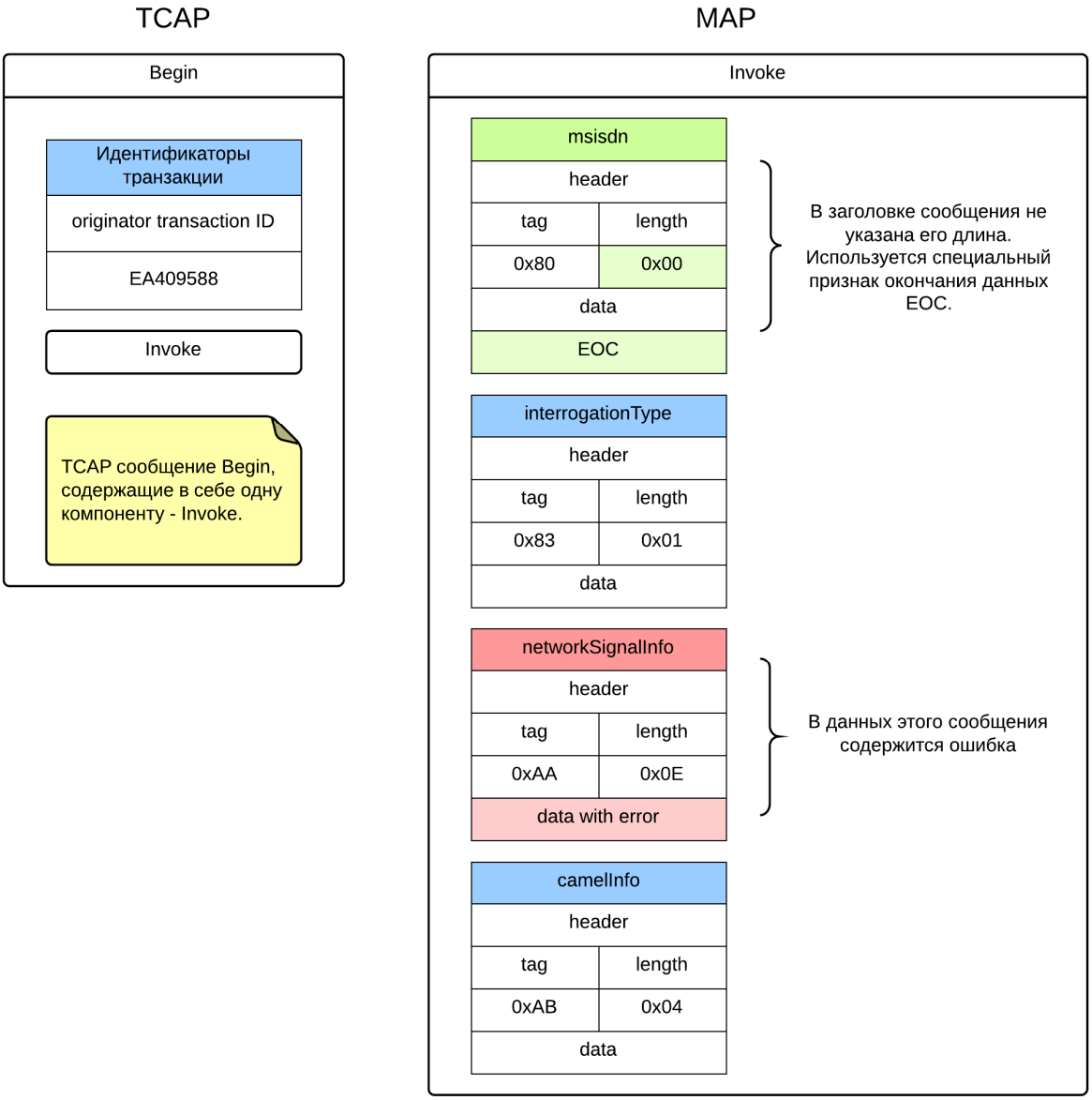

Рис. 4. Пример TCAP-сообщения

Модуль загрузки данных в базу обеспечивает формирование SQL-запросов для сохранения декодированных результатов. Чтобы исключить возможность SQL-инъекций через текстовые сообщения (например, такое: «'); COMMIT; DROP TABLE SMS;»), все символы «'» заменяются на «`» еще на первом этапе разбора сетевых пакетов. Выполнением сформированных SQL-запросов занимается СУБД SQLite, тем самым обеспечивая загрузку данных в базу. Загрузка данных из каждого файла происходит как отдельная транзакция, поэтому, если по каким-то причинам при её выполнении возникнет ошибка, то в базу не вставится ничего лишнего. Информация об ошибке сохранится и, если проблема не в сгенерированных командах, то запрос на вставку можно будет повторить вручную.

База данных. Чтобы представить множество различных телефонных сообщений в реляционной базе данных, удобно применить шаблон проектирования «категория-подтип» (рис. 5).

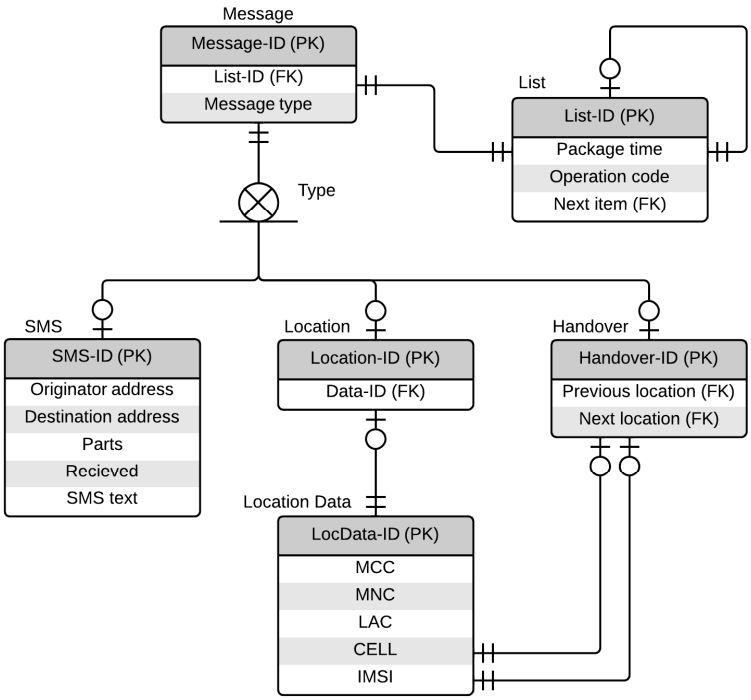

Рис. 5. Схема данных для хранения обработанных результатов

В данной работе был произведен разбор трех типов сообщений, и под каждый из них создана своя таблица: сообщения хэндовер (таблица Handover), SMS с одноименной таблицей и информация о местоположении (таблица Location). В таблице Message хранится тип полученного при разборе диалога сообщения. Поле List-ID содержит идентификатор записи в таблице List, отвечающей за головной элемент цепочки пакетов, составляющих данное сообщение. Тип сообщения является дискриминатором, по нему всегда однозначно определяется, в какой таблице содержатся декодированные данные.

В таблице List содержится информация, общая для всех MAP-сообщений, – это дата отправки сообщения и код MAP-операции, а также идентификатор следующего пакета. Так как используется образец проектирования «категория-подтип», то значение поля Message-ID совпадает со значением соответствующего первичного ключа в конкретной таблице, определяемой дискриминатором, благодаря чему удобно использовать операцию соединения (JOIN) для получения информации из базы.

Тестирование. Задачей тестирования является оценка производительности каждого из модулей системы. Необходимо оценить объем сетевого трафика, который сможет обработать приложение-декодировщик в режиме «реального времени». Тестирование системы производилось на компьютере с процессором Intel(R) Core(TM) i3 CPU M 370 (2.40GHz) под управлением операционной системы Linux Mint 16 Petra. Каждый из модулей запускался на трех различных наборах данных.

Первый тестовый набор состоит из 40000 пакетов, объемом 11,4 Мбайт. Из них 4,5% пакетов содержат сообщения типа Handover, а остальные – сообщения, разбор которых система декодирования не производит. Во втором наборе из 100000 пакетов, объемом 20,5 Мбайт, содержится 1200 сообщений SMS, все другие сообщения игнорируются. Эти тестовые наборы нужны, чтобы оценить влияние типов сообщений на быстродействие каждого модуля. Третий тестовый набор содержит в себе все типы сообщений, которые разбираются декодером. В него входят 205000 пакетов, объемом 50 Мбайт из которых 2% – информация о местоположении абонентов, 0,5% – сообщения Handover и 2,75% – SMS. Результаты тестирования представлены в таблице.

Описание входных данных	Время выполнения, с		
	модуль декодирования	создание SQL-запросов	занесение данных в базу
Первый тестовый набор	0,296	3,251	1,243
Второй тестовый набор	0,572	1,755	0,311
Третий тестовый набор	2,392	8,694	5,767

Из результатов тестирования видно, что на производительность модуля декодирования, в основном, влияет только количество обрабатываемых пакетов, а не тип декодируемых сообщений. Объем сетевого трафика в 50 МБ система сможет декодировать за 2,4 с. Для модуля загрузки в базу данных наблюдается противоположная ситуация: в первом наборе данных пакетов было меньше чем во втором, однако и процесс создания SQL-запросов и их выполнение потребовали большего количества времени, чем для второго набора.

Заключение. В данной работе рассмотрена одна из подсистем сети оператора сотовой связи, а также структура и работа общеканальной сигнализации №7. В результате

была реализована и протестирована система декодирования стека телефонных протоколов с возможностью сохранения результатов декодирования в реляционную базу данных, позволяющую легко получать информацию об обработанном сетевом трафике.

Список литературы

[1]. GSM Network Switching Subsystem Engineering. U.S.A. Lexington: Booksurge, 2013. 644 p.

[2]. Signaling System No. 7 (SS7/C7): Protocol, Architecture and Services. U.S.A. San Jose: Cisco Press, 2004. 744 p.

[3]. SIGnalling TRANsport. Available at: http://www.openss7.org/sigtran.html, accessed 18.09.2014.

[4]. Основные принципы построения и работы сети GSM. Available at: http://www.utran1980.com/gsm/content/, accessed 18.09.2014.

[5]. Handover procedure. Available at: http://www.scribd.com/doc/127028502/Handover-pdf, accessed 18.09.2014.