УДК 004.7

Адаптивный алгоритм управления служебной нагрузкой при безопасной выгрузке мобильного трафика в сети Wi-Fi

© Н.Е. Богомолова, М.С. Панфилова

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Представлены первые результаты работы, посвященной исследованию процесса выгрузки трафика мобильных сетей через повсеместно развернутые сети Wi-Fi. Предложены варианты оптимизации этого процесса путем управления служебной нагрузкой. Разработан адаптивный алгоритм снижения объема служебной информации, учитывающий поведение абонента.

Ключевые слова: *беспроводные сети, выгрузка мобильного трафика, хэндовер, бесшовность, мобильность, служебная нагрузка.*

Введение. Необходимость выгружать трафик возникает у операторов мобильной связи по двум основным причинам. Во-первых, согласно исследованиям Tellabs, политика предоставления безлимитного доступа к мобильному Интернету, характерная для крупных операторов мобильной связи, способна сделать их бизнес нерентабельным, поскольку стоимость обслуживания оборудования оказывается выше стоимости передаваемого трафика, а переход на сторону гибкой тарификации мобильного Интернета потребует от оператора аккуратной классификации и распределения IP-потоков абонентов. Во-вторых, требования пользователей к мобильному Интернету начинают превышать возможности развернутых сотовых сетей: трафик растет в геометрической прогрессии, а дальнейшая эволюция сетей радиодоступа ограничена законами физики. Оптимальным решением проблемы на данный момент является развертывание так называемых «маленьких сот» (small cells) на базе стандарта Wi-Fi в местах большого скопления мобильных абонентов (торговые и бизнес-центры, вокзалы и аэропорты, университеты и т. п.).

Сети Wi-Fi сегодня максимально подходят для разгрузки операторов мобильной связи как экономически выгодное и широко распространенное средство для выгрузки большого количества мобильных данных, при этом они обеспечивают целый ряд новых услуг [1]. Консорциум 3GPP (3rd Generation Partnership Project) разработал ряд спецификаций, посвященных вопросу освобождения ресурсов сетей сотовой связи и выгрузки трафика в сети WLAN. Однако эти специ-

фикации в большинстве своем являются рекомендациями общего характера, и ряд задач остаются нерешенными.

Целью работы является исследование процесса безопасной выгрузки мобильных данных в сети Wi-Fi и возможностей его оптимизации.

Концепция I-WLAN. Концепция Interworked Wireless LAN (I-WLAN) — это 3GPP-спецификация, позволяющая мобильным устройствам (смартфонам, планшетам, ноутбукам и др.) получать доступ к услугам мобильной сети через соединение Wi-Fi/IP. Важным аспектом данной концепции является внедрение технологий Mobile IP, разработанных IETF для реализации бесшовного хэндовера между сетями 3GPP и WLAN с сохранением пользовательских сессий. Основная цель этого решения — сохранение IP-адреса абонента при его переходе между сетями.

Другим принципиальным аспектом является обеспечение должного уровня безопасности при переходе в сеть Wi-Fi. Спецификация 3GPP TS 33.402 определяет два типа Wi-Fi-доступа (именуемого также non-3GPP):

• *trusted — доверенный доступ*, который возможен при использовании специально настроенных (как правило, операторских) точек доступа, поддерживающих режим безопасности WPA/WPA2 Enterprise со специальными методами аутентификации;

• *untrusted — недоверенный режим*, позволяющий использовать любые точки доступа, включая открытые hotspot, не контролируемые оператором и не обеспечивающие надлежащего уровня безопасности соединения.

Во втором случае безопасность должна обеспечиваться дополнительными средствами, речь о которых пойдет далее. В рамках данной статьи будет рассмотрен только режим untrusted, поскольку он представляет существенно больший интерес с точки зрения трудоемкости организации безопасной выгрузки трафика.

Архитектура сети Wi-Fi. В общем случае структура гетерогенной сети, состоящей из сети сотового оператора (2G/3G) и местных высокоскоростных локальных сетей (WLAN), может быть представлена как совокупность двух типов сетей:

• *информационной*, по которой то с низкими, то с высокими скоростями передается информация пользователей;

• *служебной*, осуществляющей взаимодействие элементов информационной сети.

При этом для обеспечения безопасного Wi-Fi-соединения и организации бесшовного хэндовера по служебной сети передается значительный объем сигнальной информации.

Концепция I-WLAN вводит в привычную 3GPP-архитектуру новую функциональную единицу — домашний агент HA (Home Agent) (рис. 1).

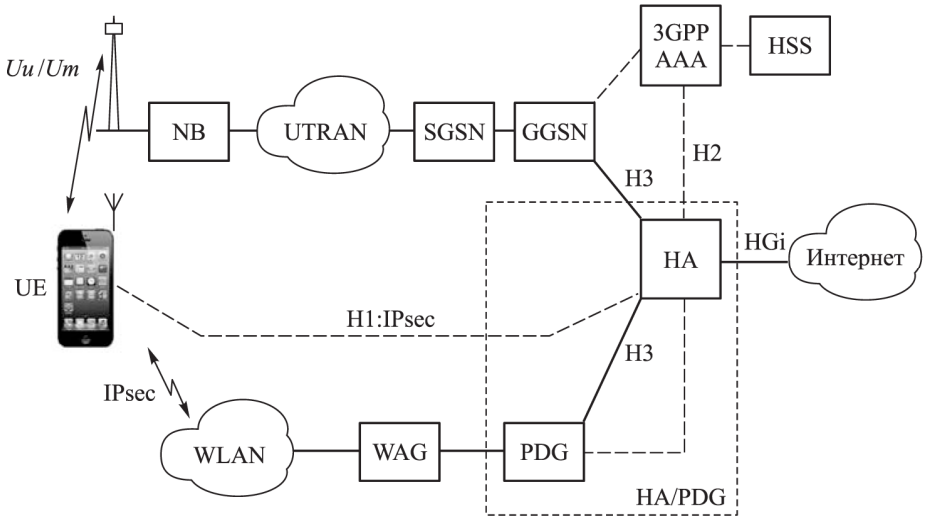

Рис. 1. Интеграция сети Wi-Fi с UMTS-инфраструктурой

Рассмотрим кратко назначение основных участников процесса выгрузки:

• HA (Home Agent) — ключевой элемент для организации бесшовного переключения между сетями, имеет двойной стек IPv4/IPv6;

• PDG (Packet Data Gateway) — входная точка для трафика в операторскую сеть, отвечает за построение IPsec-туннеля, проводит аутентификацию и авторизацию абонента, назначает абоненту IP-адрес;

• UE (User Equipment) — мобильный терминал абонента (смартфон, планшет, ноутбук с 3G-модемом и т. п.), на котором установлено специальное программное обеспечение, управляющее переключением между сетями на клиентской стороне;

• AAA-сервер — сервер, поддерживающий аутентификацию для сессий между UE и PDG, а также между UE и HA;

• SGSN (Serving GPRS Support Node), GGSN (GPRS Gateway Service Node) — два узла поддержки услуг GPRS.

Оптимизация процесса управления мобильностью абонента. Все манипуляции по переключению абонента между сетями относятся к служебным взаимодействиям, минимизация которых всегда является актуальной задачей в сетях любых типов: сначала при осуществлении роуминга в сетях GSM 2G [2], затем в гетерогенных сетях, осуществляющих передачу трафика реального времени, и т. д.

Для задачи выгрузки мобильного трафика эта проблема становится еще более острой, поскольку помимо задачи снижения служебной нагрузки возникают жесткие ограничения по времени, отведенному на взаимодействия, для обеспечения бесшовного хэндовера.

Чтобы минимизировать задержку при настройке защищенного соединения UE с PDG и HA, можно было бы разрешить абоненту выполнять некоторую предварительную установку сессии IPsec с соответствующими узлами в сети. Однако недостатком такой оптимизации может быть увеличение сигнальной нагрузки, а также рост накладных расходов на обслуживание сессии.

В результате предложен другой путь оптимизации — объединение PDG и HA. Это позволит использовать одну сессию IPsec между абонентским терминалом UE и сетью, что существенно упрощает схему взаимодействия, уменьшает сигнальную нагрузку, а также способствует снижению капитальных и эксплуатационных затрат.

При такой архитектуре абонент устанавливает одно защищенное соединение с объединенным HA/PDG (см. рис. 1).

Оба пути оптимизации включают неоднократное обращение к домашнему регистру мобильного оператора HSS. Если абонент достаточно мобилен и часто появляется в зоне действия сетей Wi-Fi, целесообразно включить для него режим быстрой повторной аутентификации (fast reauthentication), чтобы не обращаться к HSS при каждом переключении.

Алгоритм динамического управления статусом абонента. Включать режим быстрой повторной аутентификации для всех абонентов не имеет смысла, так как это избыточно. В связи с этим предлагается ввести дополнительный модуль, который будет хранить информацию об абонентах, выходящих на связь в зонах Wi-Fi, и осуществлять динамическое управление их статусом [3]. Например, при каждом выходе абонента в зону высокоскоростной передачи данных его статус повышается. Служебная информация об абонентах, не выходящих на связь в течение долгого времени, стирается.

Устройства динамического управления статусом представляются в виде коллектива автоматов с переменной структурой, действующих в случайной среде с двумя входами [4]. Состояние первого входа, соответствующее отсутствию попыток абонента установить соединение в течение заданного периода, назовем *штрафом*. При поступлении штрафа информация о данном абоненте получает более низкий статус и в конце концов стирается. Состояние второго входа, соответствующее успешным выходам абонента в сеть, назовем *поощрением*. При поощрении статус абонента повышается. Рассматриваемая модель также позволяет вводить различные приоритеты для абонентов, т. е. усложнять алгоритм работы.

Для исследования работы дополнительного модуля была также построена имитационная модель, с помощью которой можно получить характеристики качества обслуживания различных сервисных классов одновременно. Модель позволяет отражать динамический характер поведения пользователей при перегрузках как в информационной, так и в сигнальной сети.

Для классификации абонентов по приоритетам следует учитывать поведение абонента: динамику его перемещений между сетями, требуемое качество запрашиваемых услуг и т. п.

Для проведения моделирования была реализована предварительная упрощенная имитационная модель на языке Java, определяющая в буфере границы обслуживания абонентов различных категорий. Динамическое управление этими границами осуществляется с помощью коллектива стохастических автоматов, которые настраивают эти границы в зависимости от динамики поведения абонентов.

На рис. 2 показан график, отражающий результаты проведенного моделирования для тысячи подключений. Здесь по оси абсцисс откладывается длина списка, а по оси ординат — количество обращений к HSS.

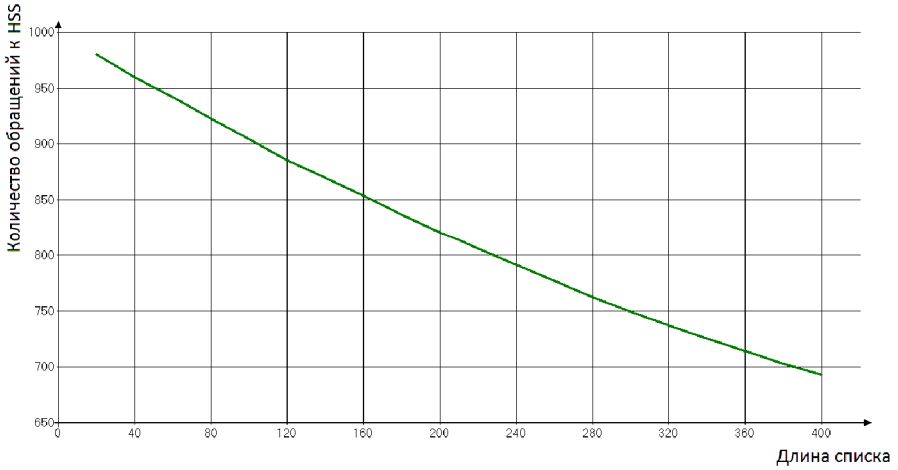

Рис. 2. Зависимость количества обращений HSS от длины списка пользователей

Как видно из графика, при росте длины списка количество обращений к HSS уменьшается, соответственно, уменьшается и сигнальная нагрузка.

Заключение. На основе проведенных предварительных исследований и изучения процесса защищенной выгрузки мобильного трафика в сети Wi-Fi были выделены задачи снижения служебной нагрузки и временной задержки при хэндовере и предложены вари-

анты оптимизации процесса выгрузки. Разработана упрощенная модель управления служебной нагрузкой в гетерогенной сети. В качестве обратной связи в этой модели выступает степень мобильности абонента, т. е. частота его переходов между сетями 3GPP и Wi-Fi. Модель требует дальнейшего развития и доработки, в частности необходимо исследовать величину штрафов и поощрений автоматов, управляющих границами ее параметров.

В данной статье рассматривались в основном сети 2G/3G, однако следует отметить, что концепция выгрузки мобильного трафика остается актуальной и для сетей LTE с незначительными и больше формальными изменениями.

ЛИТЕРАТУРА

[1] Сакалема Д.Ж. *Подвижная радиосвязь.* Москва, Горячая линия — Телеком, 2012, 511 с.

[2] Богомолова Н.Е. Влияние дополнительных услуг на пропускную способность ОКС № 7 в мобильных сетях. *Мобильные системы*, 2003, № 3, с. 14–17.

[3] Богомолова Н.Е., Панфилова М.С. Исследование передачи данных в гетерогенных мобильных сетях. *Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем. Материалы Всерос. конф. с междунар. участием*. Москва, 22–26 апреля 2013 г. Москва, РУДН, 2013, с. 70–71.

[4] Лазарев В.Г., Гончаров Е.В. Метод адаптивной маршрутизации с учетом задержек передачи управляющих сообщений. *Тр. VI Междунар. конф. по информационным сетям и системам ISINAS-2000.* Санкт-Петербург, 2–7 октября 2000 г. Санкт-Петербург, 2000, с. 320–330.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Богомолова Н.Е., Панфилова М.С. Адаптивный алгоритм управления служебной нагрузкой при безопасной выгрузке мобильного трафика в сети Wi-Fi. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/network/1014.html

Богомолова Наталья Егоровна родилась в 1955 г., окончила Московский электротехнический институт связи в 1977 г. Канд. техн. наук, доцент МГТУ им. Н.Э. Баумана. Автор более 40 научных работ в области телекоммуникаций. e-mail: nbogomolova09@ gmail.com

Панфилова Мария Сергеевна — магистр техники и технологии по направлению «Информатика и вычислительная техника», ассистент кафедры «Защита информации» МГТУ им. Н.Э. Баумана, главный инженер-программист компании «SM Solutions». Более пяти лет работает в области информационной безопасности и мобильных телекоммуникаций, автор нескольких публикаций в данной области. e-mail: mpanfilova@sm-sol.com