УДК 621.391

АСПЕКТЫ БЕЗОПАСНОСТИ ПРИ УПРАВЛЕНИИ HeNB LTE

Пудалев Т.О., Пронькин Л.А.

Научный руководитель: ***Черников Дмитрий Юрьевич***

Институт инженерной физики и радиоэлектроники СФУ

В данной статье рассматриваются основные аспекты безопасности функционирования домашних базовых станций LTE.Приведены различные способы защиты каналов связи между элементами системыи особенности обеспечения безопасности при первоначальном запуске базовых станций.

Ключевые слова: мобильные сети, LTE, фемтосоты, HeNB,IPSec,TLS.

This article discusses the main aspects of the safety of home base stations LTE’s functioning. There are different ways to protect communications between system components and security features in the initial launch of base stations.

Keywords: mobile network, LTE, femtocells, HeNB, IPSec, TLS.

HeNB(Homee-NodeBase) – домашняя базовая станцияв технологии LTE, представляющая собой маломощную и миниатюрную станцию сотовой связи (фемтосоту), предназначенную для обслуживания небольшой территории (одного офиса или квартиры). HeNB являются первым мобильными сетевыми элементами, которые операторы разворачивают в помещениях клиента. Соединяется они с сетью сотового оператора через канал связи, подведенный к пользователю, обслуживает обычно не более нескольких телефонов.

Фемтосоты, пикосоты, метросоты, и микросоты относятся к категории так называемых «малых сот» (smallcells) — маломощных беспроводных точек доступа, работающих в лицензируемом частотном спектре и управляемых оператором.

Благодаря фемтосотам, покрытие сотовой сети резко улучшается именно в тех точках, где это необходимо. Фемтосоты предоставляют все те же функции, что и «большая» сотовая ячейка, но в одном удобном для установки контейнере.

До недавнего времени основное внимание уделялось развитию UMTS-фемтосот, однако они могут создаваться и для других стандартов, в том числе и для LTE.

Для сотового оператора это даёт возможность улучшить покрытие и ёмкость сети, особенно внутри зданий. Появляется возможность предоставлять дополнительные услуги по сниженным ценам и экономить на оборудовании.

Однако, ввиду многих причин, для HeNBвопрос безопасности передачи данных имеет особую важность. В связи с этим впервые в 3GPPспецификациихарактеристики безопасности для управления сетевыми элементами рассматриваются настолько детально. Руководствуясь ожиданиями на массовый спрос в развертывании HeNB, интерфейс управления был полностью стандартизован, чтобы системы управления HeNB и сами HeNB от различных вендоров могли неограниченно взаимодействовать друг с другом.

Архитектура безопасности управления HeNB основывается 3GPP спецификации. Эти спецификации описывают интерфейс «Type 1», который определен, какинтерфейс между управляющими и управляемыми элементами сети.Этот протокол обеспечивает связь в режиме реального времени между HeMS (Homee-ManagementSystem) иHeNB, и определяет команды и форматы данных, которые будут использоваться. Кроме того, данный протокол позволяет использоватьмеханизм передачи файлов для загрузки программного обеспечения, общих конфигурационных данных, а также различных статистических сведений.

На рисунке 1 показанабазовая архитектура управления для HeNB. HeMS может быть расположена как в сети оператора, так и в Интернете.Если HeMS расположена в домене оператора, трафик управления направляется через SeGW, поскольку трафик из Интернета никогда не должен иметь доступа к домену безопасности оператора напрямую. Если HeMS расположена в Интернете, тогда реализуется прямое соединениечерез Интернет между HeNB и HeMS.

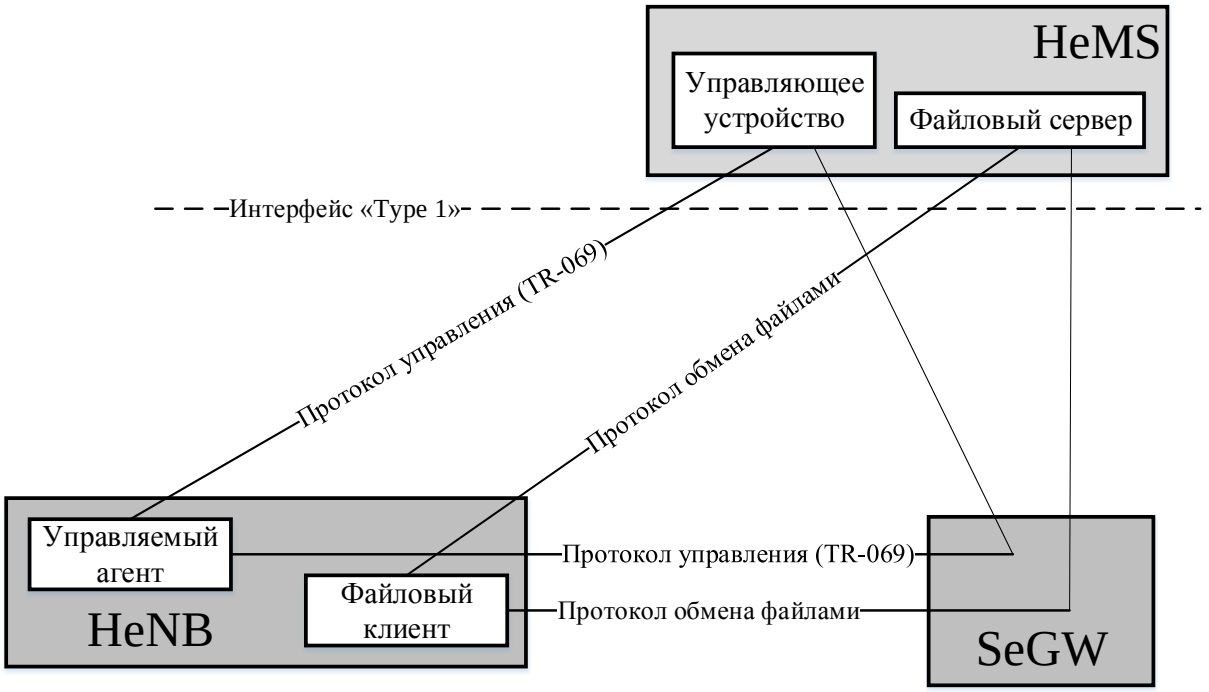

Рисунок 1 – Архитектура управления HeNBи HeMS

В зависимости от расположения HeMS требуются различные механизмы безопасности. Вдополнение, необходимо иметь в виду, что HeMS можетявлятьсягеографически распределенной системой; например, сервер автоматической конфигурации и файловый сервер могут быбыть физически разделенными. Это может произойти, если существующая инфраструктура файлового сервера, которая являетсяобщедоступной через Интернет, используется для поддержки существующих шлюзов; например,HeNBи файловый сервер разделены DSLроутером.

Когда HeMS расположены в домене безопасности оператора, трафик управления туннелируется через тот же туннель IPsec, который используется для сигнализациии пользовательского трафика между HeNB и базовой сетью. Кроме того, в случае если требуется сквозная безопасность между HeNB и HeMS, оператор может дополнительно развернуть определенные механизмы безопасностидля доступа к HeMS, расположенной в общедоступном сегменте Интернета.

Когда HeMS доступна через Интернет, HeNB должна установить защищенный туннель к этим HeMS для трафика управления.Такой защищенный туннель, с использованием протокола TLS,не является обязательным.

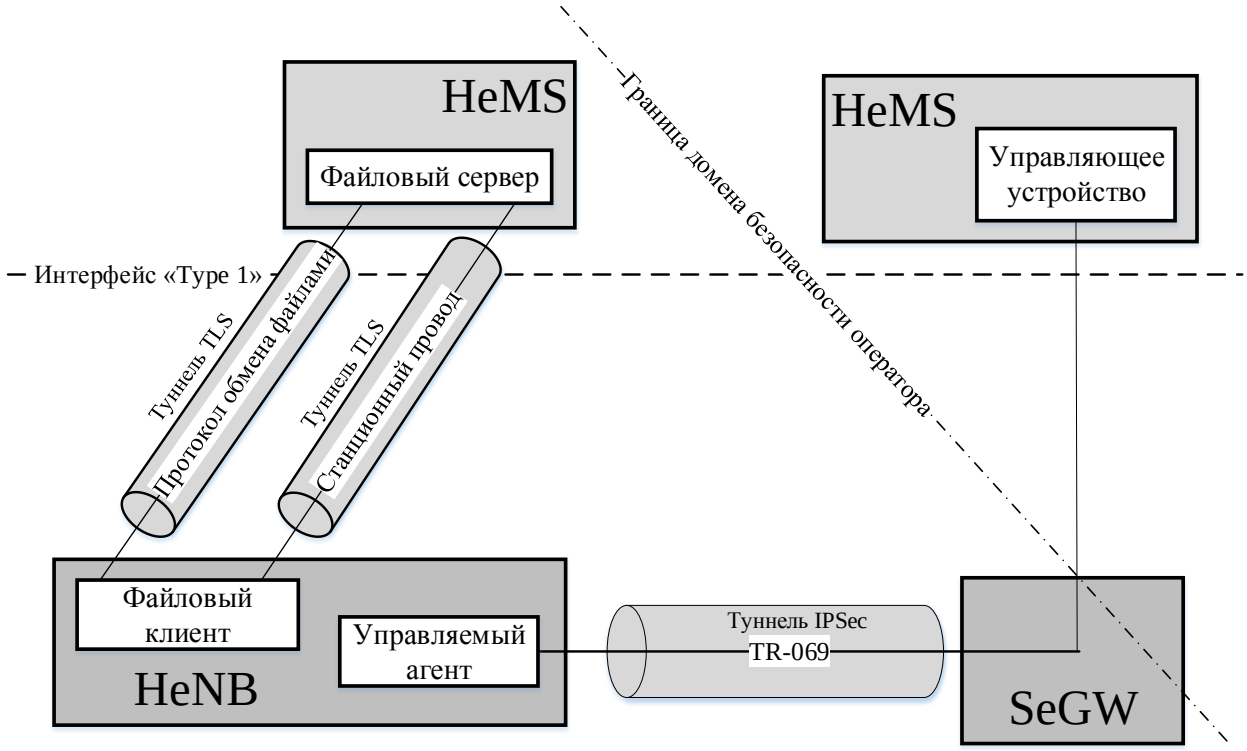

Рисунок 2 – Используемые механизмы безопасности в зависимости от расположения HeMS

На рисунке 2 показана архитектура управления в случае с распределенной HeMS.Также на рисунке отмеченыобязательные для данного случая механизмы безопасности и основные типы соединений. Трафик управления между агентом вHeNB и менеджеромвHeMS защищены туннелем IPsec. В соответствии с политикой оператора, интерфейс между SeGW и HeMS и другими внутренними сетевыми интерфейсами может быть защищен с помощью интегрированных средств интерфейса Zb. Для загрузки программного обеспечения или любой другой передачи файлов, HeNB должен установить туннель TLSc файловым менеджером в HeMS, до того, как какие-либо данные будут загружены или скачены.

Важным аспектом безопасности является обеспечение инициализации оборудования HeNB.HeMS являетсяглавным управляющим элементом для HeNBпосле первого включения питания, или после сброса HeNB к заводским настройкам. URL-адрес для доступа к данной HeMS может храниться в зашифрованном виде в HeNB. 3GPP спецификации не определяют, принадлежит ли начальный адресHeMSпроизводителюHeNB, провайдеру или третьей стороне. Таким образом, допускается гибкая процедураподключенияHeNB к сетям оператора, не требующая настройки оператором определенных параметров в HeNB для всехHeNBs во время производства или доставки с производственных предприятий. В соответствии с этим ясно, что начальный HeMS, обычно будет располагаться в общедоступном сегменте интернета, поскольку в противном случае адрес SeGW должен быть также предварительно запрограммированHeNB.

Начальная HeMS предоставляет HeNB операционные адреса и параметры для последующей работы в сети определённого оператора. Выбор адресов и параметров может основываться на географическом расположении, которое определяются в самой HeNB, или согласно глобальным уникальным идентификационным данным. Кроме того,первичнаязагрузка программного обеспечения может быть произведена, если начальная HeMS обнаруживает устаревшую или несоответствующую версию программного обеспечения HeNB.Механизмы безопасности, используемые для защитыHeNB, применяются также и к начальной HeMS. Если начальная HeMS расположена в сети оператора позади SeGW, этот SeGW вызывают «начальным SeGW», и адрес этого SeGW должен быть также преднастроен в HeNB.

Таким образом мы рассмотрели лишь самые основные моменты, на которые следовало бы обратить внимание при обеспечении безопасности управления HeNBLTE. Однако даже короткое перечисление потенциально уязвимых мест технологии даёт повод самым серьёзным образом задуматься над обеспечением безопасности представленной технологии доступа. И конечно

следует отметить, что, со временем, распространение сетей четвёртого поколения и рост числа абонентовтолько усилят актуальность использования маломощных беспроводных точек доступа, а соответственно и требований к обеспечениюих безопасности.

Библиографический список

1 Тихвинский В.О., Терентьев С.В., Юрчук А.Б.Сети мобильной связи LTE: технологии и архитектура: учеб. пособие–М.:Эко-Трендз, 2010. – 224 с.

2 Гельгор А.Л. Технология LTE мобильной передачи данных: учеб. пособие. — СПб.: Изд-во Политехн. ун-та, 2011. — 204 с.

3HassaneinH. LTE, LTE-AdvancedandWiMAX. Chichester, UK: JohnWiley&Sons, 2012, – 275pp.

4ForsbergD., Günther H. LTESecurity. Chichester, UK: John Wiley & Sons, 2010, – 284 pp.