Глава 3

Уроки, извлеченные из раннего внедрения M2M-технологий

Samia Benrachi-Maassam

*Bouygues Telecom, Париж, Франция*

**3.1 Введение**

Современный активный рост внедрения M2M-технологий (*прим.: M2M – межмашинное взаимодействие*) привел к появлению различных рабочих задач. В настоящее время с ними сталкиваются поставщики сетевых услуг, установленная инфраструктура которых изначально разрабатывалась и оптимизировалась для предоставления услуг личной связи. Цель настоящей главы – рассказать о некоторых наиболее важных открытиях и извлеченных уроках, а также описать наилучшие современные методики, касающиеся сетевой архитектуры, чтобы помочь справиться с текущим ростом внедрения M2M-технологий.

Хотя M2M-устройства используют различные типы коммуникационных технологий, включая радиосвязь ближнего действия, кабельную связь и сотовые сети 2G/3G/4G, данная глава уделяет большее внимание устройствам, использующим модули связи 2G и 3G для подключения к операторам сотовой связи (ОСС). Сотовые технологии имеют несколько характеристик, удовлетворяющих требованиям различных сегментов рынка межмашинного взаимодействия. Среди них – доступность и географический охват, малая задержка и высокий уровень безопасности. К тому же, операторы сетей (и в частности ОСС) постепенно становятся надежными партнерами для внедрения M2M-технологий. Они предоставляют все больше и больше новых услуг с добавленной стоимостью помимо стандартных возможностей подключения и активации, тем самым принимая стратегию, делающую их поставщиками M2M-услуг.

Одной из первых проблем, с которой сталкиваются ОСС при внедрении M2M-технологий, является возможность управления большим количеством M2M-устройств с разными характеристиками трафика без ущерба для услуг личной связи. Бесспорно, при таком внедрении должна использоваться существующая инфраструктура и технологии, и лишь затем должны использоваться инвестиции ОСС на капитальные и эксплуатационные расходы. Вследствие этого необходимо четкое понимание требований к услугам, а также характеристик трафика в каждом целевом сегменте рынка. Остаток этой главы имеет следующую структуру. Во-первых, предлагается вниманию обзор оперативного внедрения M2M наряду с техническими решениями в области архитектуры для удовлетворения различных требований M2M-приложений. Во-вторых, предлагается краткое описание некоторых проблем, связанных с M2M, а также некоторые начальные механизмы архитектурной оптимизации. Наконец, в этой главе приводится описание основного опыта и уроков, извлеченных при раннем внедрении M2M-сервисов.

**3.2 Раннее оперативное внедрение M2M-технологий**

**3.2.1 Введение**

В данном разделе описываются несколько примеров оперативного внедрения M2M, при котором использовались существующие сети ОСС. Данные примеры приведены для того, чтобы продемонстрировать различные возможные современные технологические решения для сбора данных (или обмена данными), а также для запуска устройств. Термин «запуск устройств» относится к механизмам, используемым M2M-сервером[1](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03-note-0001) для запуска аппаратного комплекса канала передачи данных[2](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03-note-0002) с помощью M2M-устройства. Хотя и может быть желательно, чтобы каждое устройство было постоянно включено и имело присвоенный IP-адрес, такой вариант является очень затратным в том, что касается использования ресурсов сети и потребления электроэнергии. По существу, для устройств, передающих очень малые объемы данных, использование сервисов CS-доменов (доменов с коммутацией каналов), таких как SMS, может быть в целом более эффективным решением. Следующие примеры внедрения выделяют различные технологические решения, иллюстрации к которым также приводятся в этом разделе:

**Сбор и обмен данными** может осуществляться посредством:

**сервисов CS-доменов, таких** как домены SMS и данных, передаваемых по коммутируемому каналу (CSD).[3](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03-note-0003) Использование CS-доменов является наиболее желаемым в случае внедрения таких M2M-приложений, которые время от времени передают очень небольшие объемы данных.

**каналов с пакетной коммутацией** (**PS**). Использование PS-доменов наиболее подходит для приложений, передающих относительно большие объемы данных или требующих низкой задержки сети. Канал пакетной радиосвязи общего пользования (GPRS) может работать в постоянном режиме (всегда включен) или включаться по команде M2M-устройства, периодически или на основании пускового сигнала, такого как доступность данных или сигнал тревоги.

**Запуск устройств M2M-сервером** может осуществляться посредством:

**отправки специального SMS-сообщения на устройство** – устройство реагирует посредством включения канала GPRS, что также называется активацией контекста протокола пакетных данных (PDP-контекста).

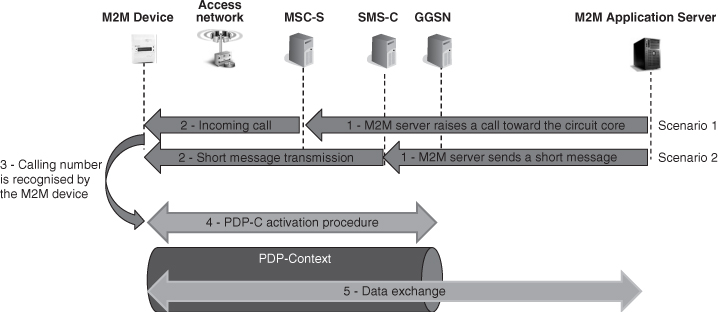
**непринятого голосового вызова** – как правило, M2M-сервер запускает создание голосового вызова на M2M-устройство. M2M-устройство распознает номер вызывающей стороны и инициирует создание PDP-контекста, не отвечая на голосовой вызов.

**Активация PDP-контекста по сетевому запросу (NRPCA)**: Это решение позволяет сети (от имени M2M-сервера) активировать PDP-контекст. Подобная опция устраняет необходимость отправки SMS или непринятого голосового вызова. Однако она нечасто внедряется в рабочие сети в связи с присущими ей техническими ограничениями. Работа современных стандартов 3GPP направлена на оптимизацию механизмов NRPCA (см. Главу 6).

[На Рисунке 3.1](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_0001) приведен обзор процедуры запуска устройств с помощью SMS-сообщений или непринятых голосовых вызовов.

[**Рисунок 3.1**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_anc_0001) Коммуникационная модель при запуске устройств.

M2M Device – M2M-устройство; Access network – Сеть доступа; MSC-S – MSC-сервер; SMS-C - СМС-центр; GGSN - Узел поддержки шлюза GPRS; M2M Application Server – Сервер M2M-приложений; Scenario 1/2 – Сценарий 1/2; 1 - M2M server raises a call toward the circuit core – M2M-сервер совершает вызов в адрес канала связи; 2 - Incoming call – Входящий вызов; 1 – M2M server sends a short message - M2M-сервер отправляет короткое сообщение; 2—Short message transmission – Передача короткого сообщения; 3 – Calling number is recognized by the M2M device – номер вызывающей стороны распознается M2M-устройством; 4 – PDP-C activation procedure – процедура активации PDP-контекста; PDP-context – PDP-контект; 5—Data exchange – Обмен данными



**Шаги 1 и 2**: M2M-сервер создает голосовой вызов через MSC-сервер (MSC-S)[4](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03-note-0004) или отправляет SMS-сообщение на M2M-устройство через SMS-центр (SMS-C). Затем запрос (голосовой вызов или SMS-сообщение) передается на M2M-устройство

**Шаг 3**: M2M-устройство распознает команду о необходимости активации PDP-контекста

**Шаг 4**: Активируется PDP-контекст. В результате M2M-устройству присваивается IP-адрес, и оно получает возможность обмена данными с M2M-сервером по протоколам TCP-IP

**Шаг 5**: M2M-устройство совершает обмен данными с M2M-сервером

Следует учесть, что процедура запуск устройств может использоваться в сочетании с периодической активацией канала PDP-контекста. Устройство настраивается так, чтобы периодически создавать возможность связи (периодичность устанавливается в M2M-устройстве посредством изменения конфигурации). В таком качестве процедура запуска устройств используется в случаях, когда M2M-серверу необходимо вызывать M2M-устройство, в то время как, например, периодическая отчетность по зарегистрированным данным происходит по инициативе M2M-устройства.

Перед развертыванием GPRS-сети обычно внедряется CSD в качестве технологии обмена данными для M2M-приложений. Технология CSD – это первоначальная форма передачи данных, разработанная для GSM-систем. Технология CSD обеспечивает исходящую и входящую скорость передачи 9,6 кбит/сек, что достаточно для ранних/некоторых M2M-приложений (отправка данных счетчика, информация о расположении резервуаров для газа, и т.д.).

Далее в главе приводятся примеры того, как вышеупомянутый набор механизмов может быть использован для отклика на потребности M2M-приложений.

**3.2.2 Примеры раннего оперативного внедрения M2M-технологий**

**3.2.2.1 Слежение за автотранспортными средствами**

M2M-приложения на основе систем слежения за автотранспортом (таких, как система контроля транспортных средств или система автострахования по принципу pay-as-you-drive) полагаются на способность ОСС рассчитывать и обеспечивать доступ серверов M2M-приложений к сведениям о местонахождении отслеживаемого транспортного средства. В иных случаях сведения о местонахождении отправляются с M2M-терминала на сервер M2M-приложений посредством каналов сети передачи данных. В данном конкретном случае существуют два типа данных о местоположении, подлежащих обмену:

**местоположение по GPS** – предоставляет более точные данные о местонахождении, но требует использования GPS-антенны и может не работать при любых условиях.

**местоположение в сети** – данные либо предоставляются на основе соты базовой станции, обслуживающей конкретный терминал (менее точное местоположение), либо вычисляются с помощью триангуляции с учетом силы сигналов, измеренных с различных базовых станций.

Как показано на Рисунке 3.2, M2M-сервер запрашивает сведения о географическом местоположении M2M-устройства с локационной станции (Шаг 1). Локационная станция обращается к регистру местонахождения (HLR), чтобы связаться с сервером MSC, управляющим M2M-устройством (Шаг 2). В шагах 3-6 геолокационный сервер запрашивает с сервера MSC список всех сот, рядом с которыми может располагаться M2M-устройство, чтобы затем предоставить сведения об идентификаторах 2G/3G-сот. Затем локационная станция переводит идентификаторы 2G/3G-сот в географическую точку в соответствии с заранее настроенными таблицами преобразования. Затем сведения о местоположении передаются на M2M-сервер посредством заранее созданного безопасного VPN-туннеля (Шаг 8) во избежание утечки данных. Следует учесть, что локационная станция может предоставить доступ к сведениям о местоположении нескольким M2M-серверам, имеющим необходимые права в отношении M2M-устройства (Шаг 9).

**Рисунок 3.2** Базовый принцип M2M-приложений для отслеживания автотранспорта

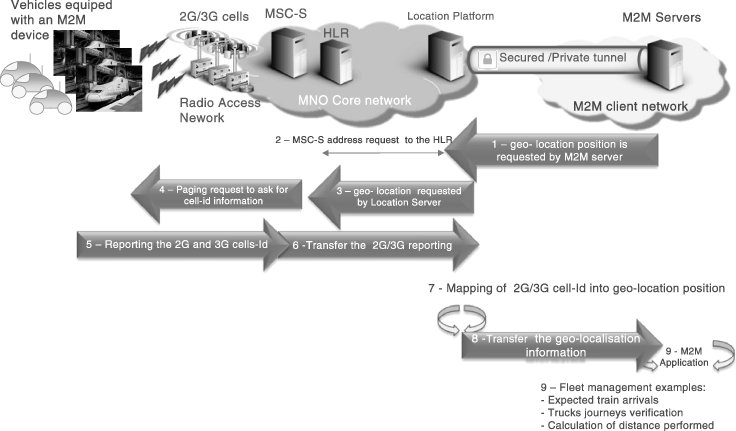
Vehicles equipped with an M2M device – Автотранспортные средства, снабженные M2M-устройством; 2G/3G cells – соты 2G/3G; Radio Access Network – сеть радиодоступа; MSC-S – сервер MSC; HLR – регистр местонахождения; MNO Core Network – опорная сеть ОСС; Location platform – локационная станция; Secured/Private tunnel – безопасный/частный туннель; M2M-servers – M2M-сервера; M2M client network – клиентская M2M-сеть; 1 – сведения о географическом местоположении запрашиваются M2M-сервером; 2 – сервер MSC отправляет запрос в регистр местонахождения; 3 – сведения о местоположении запрашиваются локационным сервером; 4 – запрос списка идентификаторов сот; 5 – отправка списка идентификаторов 2G/3G-сот; 6 – отправка отчета о 2G/3G-сотах; 7 – преобразование идентификаторов 2G/3G-сот в географическую точку; 8 – передача сведений о местонахождении; 9 – M2M-приложение;

9 – примеры систем контроля транспортных средств:

- ожидаемое время прибытия поезда

- верификация перемещения грузового транспорта

- расчет пройденного расстояния



Сведения о местоположении по GPS и в сети могут быть дополнительно использованы для предоставления информации о местоположении сервером M2M-приложений, когда это необходимо. Сведения о местоположении по GPS могут, к примеру, быть использованы в случае автокатастрофы или других чрезвычайных ситуаций для обеспечения спасательных служб точной информацией.

**3.2.2.2 Интеллектуальная телеметрия**

Технология интеллектуальной телеметрии позволяет осуществлять в реальном времени сбор различных данных со счетчиков, предоставляющих сведения о температуре, потреблении энергии или уровне загрязнения. В данном разделе описаны сценарии внедрения следующих технологий: интеллектуальный учет электричества и мониторинг уровня газа в резервуаре.

В примере с интеллектуальным учетом M2M-устройство настроено на управление графиком периодической отчетности о данных со счетчиков, например, каждые 3 часа интеллектуальный счетчик будет передавать отчет о данных измерений на M2M-сервер. При современном внедрении используются два возможных решения для периодической отчетности:

**SMS-решение** – данные измерений отправляются посредством SMS-сообщения

**GPRS-решение solution** – для передачи данных измерений по протоколу TCP/IP устанавливается и используется GPRS-канал

Выбор между SMS и GPRS-решением зачастую обусловлен требованиями поставщика M2M-приложения, включая ограничения, связанные с внедренными коммуникационными модулями.

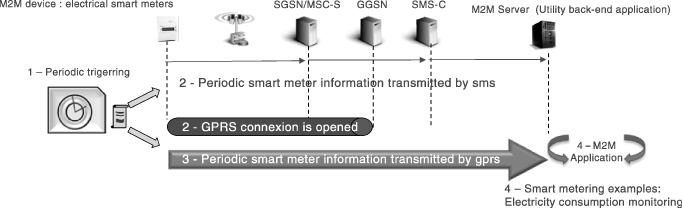
Помимо периодической отчетности о данных измерений система интеллектуального учета электричества (Рисунок 3.3) зачастую требует, чтобы M2M-сервер отправлял срочные команды на интеллектуальные счетчики. Этот как раз тот случай, когда есть необходимость в вызове операций «запрос-ответ», таких как, например, временное отключение какой-либо единицы оборудования. В данном случае M2M-сервер обычно инициирует отправку специального SMS-сообщения, чтобы запустить интеллектуальный счетчик, который играет роль целевой единицы оборудования. Интеллектуальный счетчик распознает этот сигнал и вызывает соответствующие операции «запрос-ответ».

[**Рисунок 3.3**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_anc_0003) Автоматический запуск в системе интеллектуального учета электричества

M2M device: electrical smart meters – M2M-устройство: интеллектуальные счетчики электричества; SGSN/MSC-S – Узел поддержки обслуживания GPRS/MSC-сервер; GGSN – Узел поддержки шлюза GPRS; SMS-C – SMS-центр; M2M Server (Utility back-end application) – M2M-сервер (Серверное приложение для учета энергии); 1 – Периодический запуск; 2 – Периодические отчеты о данных с интеллектуального счетчика, передаваемые через SMS; 2 – открыто GPRS-подключение; 3 – Периодические отчеты о данных с интеллектуального счетчика, передаваемые через GPRS; 4 – M2M-приложение;

4 – Примеры интеллектуального учета:

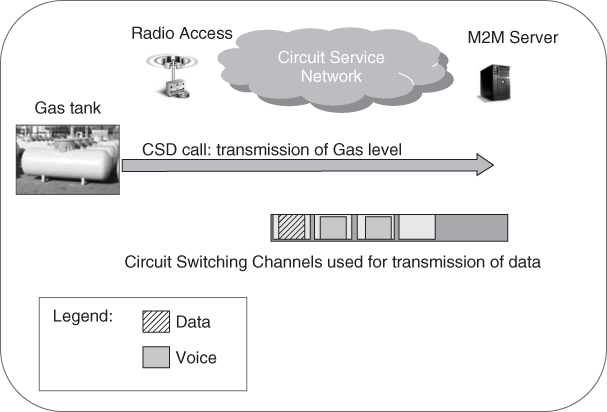
Мониторинг потребления электроэнергии



Другой пример интеллектуальной телеметрии связан с мониторингом уровня газа в резервуаре (Рисунок 3.4), применяемом некоторыми энергетическими компаниями. Использование сети ОСС обеспечивает дополнительную безопасность рабочего персонала, а также высокую степень рабочей эффективности. Мониторинг уровней газа в резервуарах в реальном времени осуществляется удаленно при помощи коммуникационного SIM-модуля, устанавливаемого на счетчик уровня газа. В данном случае данные об уровнях отправляются посредством CSD в центральное приложение, которое при необходимости вызывает уместные операции.

[**Рисунок 3.4**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_anc_0004) Использование CSD для мониторинга уровней газа в резервуарах.

Radio Access – Радиодоступ; Circuit Service Network – Сеть коммутации; M2M Server – M2M-сервер; Gas tank – газовый резервуар; CSD call: transmission of Gas level – CSD-вызов: передача данных об уровне газа; Circuit Switching Channels used for transmission of data – Коммутируемые каналы, используемые для передачи данных; Legend – Обозначения; Data – данные; Voice – Голос



Хотя технология CSD может расцениваться читателем как утратившая актуальность, ее применение обусловлено потребностями конечных пользователей, которые зачастую предпочитают избегать масштабных перестроек в существующем программном обеспечении или затрат на интеграцию коммуникационных GPRS-модулей.

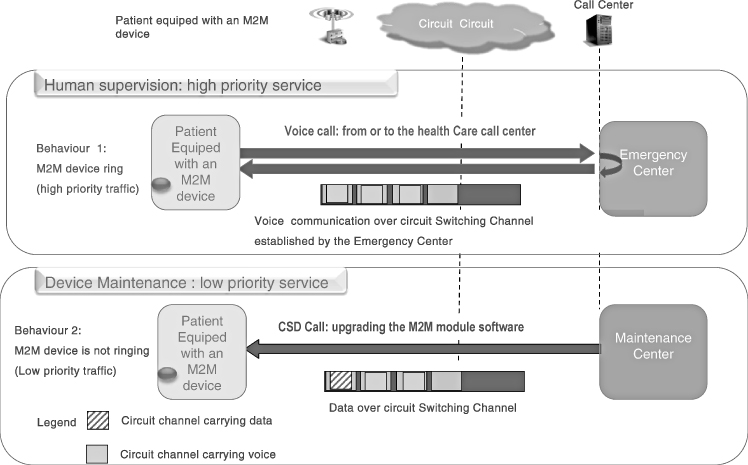
**3.2.2.3 Медицинский мониторинг**

M2M-приложения eHealth (такие как удаленный контроль за пациентом, отслеживание независимого старения и физической формы, управление течением заболевания) составляют крупный сегмент рынка M2M-технологий. В данном разделе речь пойдет о приложении для здорового старения, нацеленного на стареющее население западных стран. Данный сервис зачастую использует M2M-устройства, встроенные в носимый браслет или ожерелье. Он позволяет пациенту связаться с центром экстренной помощи нажатием всего одной клавиши на M2M-устройстве. M2M-сервер распознает номер звонящего (без ответа) и автоматически инициирует вызов в адрес M2M-устройства пациента. Затем пациент получает помощь специалиста (по оказанию неотложной помощи). Данная процедура была введена, чтобы удостовериться том, что все понесенные расходы и соответствующие счета будут исполнены для M2M-сервера.

Кроме того, при данном сценарии внедрения другой M2M-сервер (технический центр) периодически выполняет обновление программного обеспечения и прошивки посредством CSD-сервиса. Оба сценария изображены на Рисунке 3.5, показаны оба типа поведения системы.

[**Figure 3.5**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_anc_0005) Удаленная медицинская помощь

Patient equipped with an M2M device – пациент, снабженный M2M-устройством; Circuit circuit – сеть коммутации; Call center – центр обработки звонков; Human supervision: high priority service – Надзор за пациентом: сервис с высоким приоритетом; Behaviour 1: M2M device ring (high priority traffic) – Тип поведения системы 1: Звонок с M2M-устройства (высокоприоритетный трафик); Voice call: from or to the health care call center – Голосовой вызов: в адрес или от центра обработки звонков; Emergency Center – Центр экстренной помощи; Voice communication over circuit-switching channel established by the emergency center – Голосовая связь по коммутационному каналу, установленному центром экстренной помощи; Device Maintenance: low priority service – Техническое обслуживание устройства: сервис с низким приоритетом; Behaviour 2: M2M device is not ringing (Low priority traffic) – Тип поведения системы 2: M2M-устройство не звонит (низкоприоритетный трафик); CSD Call: upgrading the M2M module software – CSD-вызов: обновление программного обеспечения M2M-модуля; Maintenance Center – Технический центр; Data over circuit switching channel – Данные, передаваемые по коммутационному каналу; Legend – Обозначения; Circuit channel carrying data – Коммутационный канал передачи данные; Circuit channel carrying voice – Коммутационный канал голосовой связи



**Тип поведения M2M-устройства 1**: При получении звонка (который остается без ответа), центр экстренной помощи инициирует высокоприоритетный вызов в адрес M2M-устройства и устанавливает связь со специалистом по оказанию неотложной помощи, используя при этом высокоприоритетный номер MSISDN (номер мобильного абонента цифровой сети с интеграцией служб) M2M-устройства. Устройство снабжено двумя номерами MSISDN, один - для высокоприоритетных сервисов, другой – для всех остальных сервисов.

При таком типе поведения система надзора за пациентом задействует критически важную и высокоприоритетную услугу ОСС. Использование специального номера MSISDN позволяет предоставлять высокий приоритет всем таким вызовам.

**Тип поведения M2M-устройства 2**: Поскольку M2M-устройство нуждается в регулярном обновлении ПО и прошивки, со вторым MSISDN-номером используется CSD-канал, что позволяет системе задать низкий приоритет такому обслуживанию.

В данном примере раннего внедрения M2M-устройству присваивается 2 номера MSISDN, чтобы обеспечить возможность различных форм сетевого поведения, в зависимости от срочности ситуации:

Первый номер MSISDN используется для инициации или получения высокоприоритетного вызова в случае срочной необходимости в установке канала связи. Сеть будет использовать данный номер MSISDN для обеспечения быстрого обслуживания высокоприоритетных звонков. Кроме того, данный номер MSISDN используется для того, чтобы убедиться, что при высокоприоритетном звонке используется свободный номер MSISDN, не используемый для низкоприоритетной CSD-связи.

Второй номер MSISDN используется для CSD-связи, которая расценивается как низкоприоритетная.

Как бы то ни было, главным недостатком является возможное повышение объема используемых ресурсов MSISDN. Поскольку в настоящее время существует дефицит таких ресурсов как MSISDN, разработка стандартного решения, при котором не требуется использование нескольких номеров MSISDN, является критически важным аспектом для будущих M2M-технологий.

**3.2.2.4 Наблюдение и безопасность**

M2M-устройства для наблюдения и безопасности применяются в жилых и офисных помещениях, таких как школы, общественные учреждения, магазины, для предоставления сведений о контроле данных, фото- и видеонаблюдении в приложения охранной сигнализации. Сотовые сети часто используются для основного или вспомогательного доступа, чтобы обеспечить связь с приложениями мониторинга безопасности или владельцами помещений.

Передаваемые сведения в основном содержат информацию о сигналах тревоги и, время от времени, видеосигналы низкого и среднего разрешения.

Приложения для наблюдения и безопасности нуждаются в сетях с очень низкой задержкой и высокой скоростью, когда дело доходит до передачи фото- и видео-файлов. Такие требования сразу подчеркивают важность использования каналов с пакетной коммутацией (PS-каналов). Во избежание долгих периодов задержки, связанных с активацией PDP-контекстов, должно поддерживаться постоянное подключение с присвоением постоянного IP-адреса. Кроме того, приложения наблюдения и безопасности имеют и другие требования, например:

Аутентификация M2M-устройства проводится сервером M2M-приложений (вдобавок к механизму аутентификации ОСС) с использованием протокола RADIUS. Такой тип аутентификации является необходимым для M2M-устройств с активацией PDP-контекста.

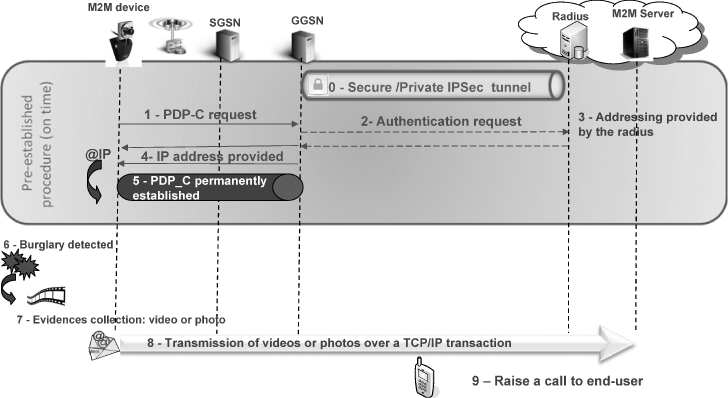
IP-адрес присваивается M2M-устройству сервером M2M-приложений, находящимся в той же подсети, или объектом, действующим от его имени. Такой механизм позволяет избежать необходимости использования общедоступной IP-адресации, что удобно для постоянно включенных каналов.

Чтобы обезопасить процедуру аутентификации M2M-устройств и избежать утечки данных, которыми обмениваются ОСС и сервер M2M-приложений, между ОСС и сетью компании, содержащей сервер M2M-приложений, устанавливается зашифрованный безопасный IP-туннель (IPSec).

Иллюстрация установки сети, используемой для приложений наблюдения и безопасности, представлена на Рисунке 3.6.

[**Рисунок 3.6**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_anc_0006) Постоянная защита и удаленное наблюдение.

M2M Device – M2M-устройство; SGSN – Узел поддержки обслуживания GPRS; GGSN – Узел поддержки шлюза GPRS; RADIUS – протокол RADIUS; M2M Server – M2M-сервер; Pre-established procedure (on time) – заранее заданная процедура (по расписанию); 0 – безопасный/частный туннель IPSec; 1 – Запрос PDP-контекста; 2 – Запрос аутентификации; 3 – Адресация, обеспечиваемая RADIUS; 4 – Предоставление IP-адреса; 5 – Постоянный PDP-контекст; 6 – обнаружено противоправное проникновение; 7 – Сбор улик: видео и фото; 8 – передача видео и фото через TCP/IP; 9 – создание звонка конечному пользователю



Шаги 1–5 изображают установку PDP-контекста. После удачной аутентификации с использованием протокола RADIUS M2M-устройству присваивается IP-адрес. В случае обнаружения актов вандализма или незаконного проникновения (Шаг 6), M2M-устройство автоматически соберет улики (Шаг 7) с камер, установленных в здании (фото и видео). В шаге 8 улики передаются по протоколу TCP/IP через постоянно включенный PDP-контекст, иначе говоря, без необходимости создания сетевого канала передачи данных и с использованием заранее установленного туннеля IpSec. В шаге 8 улики передаются по TCP/IP соединениям через постоянно включенный PDP-context, иначе говоря, без необходимости установки сетевого канала передачи данных и с использованием заранее установленного туннеля IPSec (Шаг 0). Оператор может провести начальную проверку перед тем, как отправлять команду в помещения. Оператор может также позвонить конечному пользователю и подтвердить факт вандализма/проникновения фотографией или видеозаписью (Шаг 9).

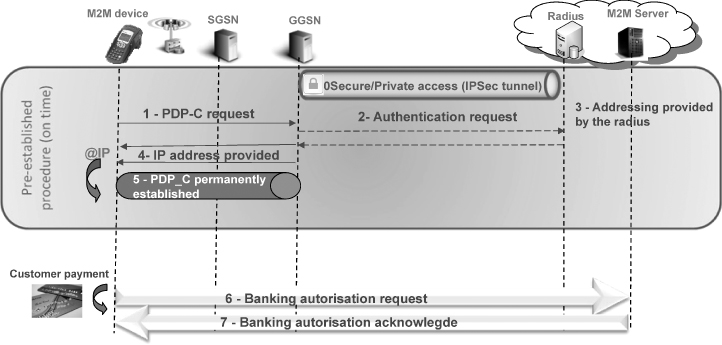
**3.2.2.5 Торговые автоматы и автоматизированные кассовые аппараты (банкоматы)**

Торговые автоматы и автоматизированные кассовые аппараты (банкоматы) широко используются для совершения финансовых транзакций и выдачи наличных. В основном, терминалы торговых автоматов и банкоматов подключены к глобальным сетям (беспроводным или проводным), чтобы иметь возможность обмена данными с центральным сервером и обработки транзакций по платежам/выдаче наличных. Помимо усиленных требований по безопасности и целостности данных одной из главных проблем, с которыми сталкиваются приложения для торговых автоматов/банкоматов, является необходимость предоставления услуг в режиме, близком к реальному времени, что требуется вследствие высокой степени интерактивности для конечного пользователя. Такие нужды удовлетворяются использованием постоянного подключения, чтобы избежать возможных задержек при установке PDP-контекста (в случае с ОСС).

[Рисунок 3.7](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_0007) описывает внедрение M2M в системы электронных платежей. После успешной аутентификации с использованием туннеля IPSec M2M-устройству присваивается IP-адрес.

[**Рисунок 3.7**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_anc_0007) Постоянная система электронных платежей, иллюстрация.

M2M device – M2M-устройство; SGSN – Узел поддержки обслуживания GPRS; GGSN – Узел поддержки шлюза GPRS; RADIUS – протокол RADIUS; M2M Server – M2M-сервер; Pre-established procedure (on time) - заранее заданная процедура (по расписанию); Customer payment – Клиентский платеж; 0 – безопасный/частный доступ (туннель IPSec); 1 – Запрос PDP-контекста; 2—Запрос аутентификации; 3 – Адресация, обеспечиваемая RADIUS; 4 – Предоставление IP-адреса; 5 – Установка постоянного PDP-контекста; 6 – Запрос банковской авторизации; 7 - Подтверждение банковской авторизации



Как только клиент запускает процедуру оплаты счета, терминал выполняет обмен данными с M2M-сервером в соответствии с требованиями платежной транзакции (Шаги 6 и 7).

**3.2.2.6 Основные выводы относительно примеров раннего внедрения M2M**

Один из выводов, которые можно сделать на основании ранних оперативных внедрений, состоит в том, что выбор решений в основном зависит от характеристик требований целевого приложения. В целом, следует учитывать следующие требования приложений:

требования к сквозной задержке сети и интерактивности;

объемы данных;

частота обмена данными;

коммуникация «клиент-сервер»;

возможности коммуникационных модулей.

[Таблица 3.1](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_tbl_0001) предоставляет общую сводку используемых сетевых решений, исходя из требований приложений. Хотя в Таблице 3.1 предоставлены общие правила, при принятии конечного решения зачастую следует принимать в расчет другие ограничения, такие как требования конечного пользователя, а также установленные унаследованные приложения и коммуникационные модули.

[**Таблица 3.1**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_tbl_anc_0001) Перечень M2M-решений и примеры вариантов использования

Дополнительная нагрузка на ресурсы CS-домена

Необходимо два номера MSISDN

Отсутствие затрат от использования сигналов PS-домена; только для передачи небольших объемов данных

Срочные вызовы направляются с высоким приоритетом

Вызывается CSD-вызов выделенного номера MSISDN

CSD передача данных с несколькими номерами MSISDN

Услуги передачи данных высокой доступности

Для передачи небольшого объема сведений создается голосовой вызов или SMS-сообщение

Голосовая или SMS-связь

PS-домен

Объем данных от среднего до высокого (без необходимости обслуживания в реальном времени)

Низкий объем данных и низкая периодичность

Все еще используется CS-домен, несмотря на то, что фактический обмен данными осуществляется через PS-домен

Нет необходимости поддерживать PDP-контекст для всех устройств постоянно

Когда коммуникация инициируется сервером, производится запуск устройства. В адрес M2M-устройства, требующего создания PDP-контекста, отправляется SMS или вызов без ответа. Как вариант, M2M-устройство инициирует PDP-контекст, например, при необходимости отправки отчета

PDP-контекст устанавливается на период передачи данных

PS-домен

Постоянное

Интерактивность/ данные в реальном времени

Поддержка контекста на сетевых устройствах для каждого канала (дополнительные капитальные и эксплуатационные расходы)

Отсутствие задержек (относительно канала передачи данных)

M2M-устройство имеет постоянно активный PDP-контекст, обеспечивающий постоянное подключение

Минусы

Описание

CS-домен

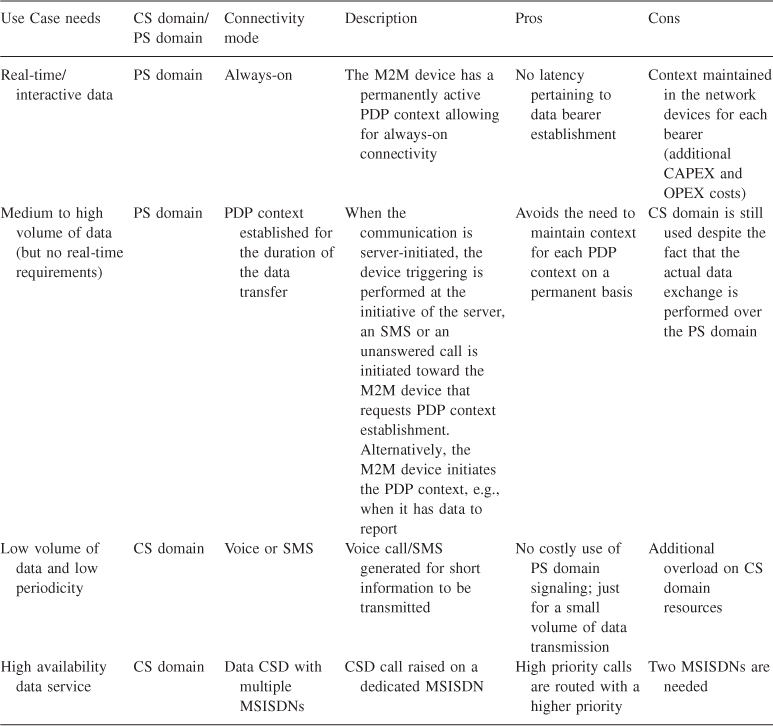
CS-домен

Плюсы

Режим подключения

CS-домен/ PS-домен

Нужды варианта использования Use case needs



**3.2.3 Частые вопросы касательно раннего внедрения M2M**

В данном разделе приводится обзор некоторых[5](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03-note-0005) проблем, встречающихся при ранних внедрениях M2M. Разрешение этих проблем посредством надлежащей настройки сети и новых опций, которые определяются современными стандартами является ключевым фактором успеха в массовом распространении M2M-технологий.

**3.2.3.1 Переполнение и перегрузка**

Будучи иллюстрацией мест, в которых может произойти переполнение, Рисунок 3.8 предоставляет обозначения сетевых устройств, могущих служить причиной переполнения и перегрузки.

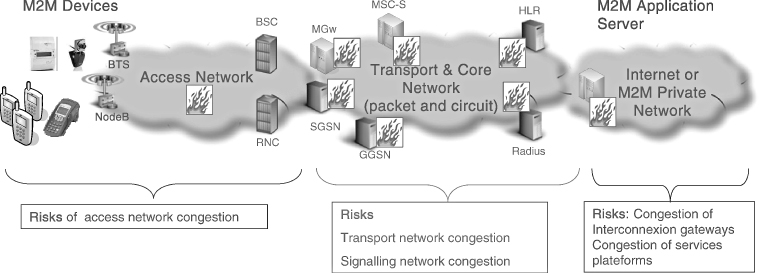
[**Рисунок 3.8**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_anc_0008) Переполнение M2M-устройств.

M2M Devices – M2M-устройства; BTS – базовая приемопередающая станция; NodeB – Узел B; Access network – Сеть доступа; BSC – Контроллер базовых станций; RNC – Дистанционный сетевой контроллер; MGw – Шлюз мобильной связи; SGSN – Узел поддержки обслуживания GPRS; MSC-S – Сервер MSC; GGSN – Узел поддержки шлюза GPRS; Transport & Core Network (packet and circuit) – Транспортная и опорная сеть (пакетно-коммутационная); HLR – Регистр местонахождения; Radius – протокол Radius; M2M Application Server – Сервер M2M-приложений; Internet or M2M Private Network – Интернет или частная сеть M2M;

Risks of access network congestion – Риски переполнения сети доступа;

Risks / Transport network congestion / Signaling network congestion – Риски / переполнение транспортной сети / переполнение сигнальной сети;

Risks: Congestion of Interconnexion gateways/Congestion of services platforms – Риски: Переполнение шлюзов двустороннего подключения/Переполнение сервисных платформ



Typically, the issue of congestion occurs when the M2M device requests the establishment of a PDP context. In the event of the establishment of the PDP context failing, the M2M devices keep constantly trying until they establish a connection.

В связи с аномально высоким числом запросов серверы аутентификации (RADIUS) могут перегружаться на ранних этапах процесса внедрения. Когда в опорную пакетную сеть приходит запрос на PDP-соединение «человек-человек», сервер аутентификации не может ответить и выдает ошибку превышения времени ожидания ответа. Перегрузка распространяется в обратном направлении через интерфейсы узла поддержки шлюза GPRS (GGSN) и в результате на более поздних этапах встает вся опорная пакетная сеть.

Зачастую сетевым администраторам необходимо будет на мгновение приостановить M2M-трафик в качестве меры для идентификации и изоляции дефектных или неисправных коммуникационных модулей. Однако выполнить такую операцию может быть нелегко в связи с недостатком средств для распознавания M2M-трафика как такового.

Для предварительного анализа отличий M2M-трафика от H2H-трафика (последний тип наиболее часто передается по сетям телекоммуникаций) могут быть приведены следующие характеристики трафика:

**Синхронность**: M2M-устройства зачастую программируются так, чтобы предоставлять отчеты по данных через определенный промежуток времени, например, каждый час, без какой-либо рандомизации в установленных каналах подключения. Такое поведение приводит к синхронизации в том, что касается использования ресурсов сети, и зачастую приводит к переполнению.

**Непредсказуемость**: В иных случаях M2M-модули внедряются оператором, не знающим, подходит ли такое внедрение для M2M. В этом случае оператор не может предсказать поведение трафика и конфигурировать сеть в соответствии с ним.

**Резкое повышение объема передачи**: Некоторые устройства (например, устройства наблюдения и безопасности) обычно генерируют малые объемы данных, за исключением случаев, когда включается тревога. К примеру, видеокамера может начать генерировать большой объем данных при включении тревоги.

**Неконтролируемость**: Некоторое множество устройств подключается к сети без какого-либо определенного порядка. Взять, к примеру, набор роуминговых устройств: когда пропадает покрытие сети оператора А (из-за проблем радиосвязи), устройства будут одновременно пытаться подключиться к оператору B.

**3.2.3.2 Недостаток ресурсов распознавания и адресации**

Для идентификации мобильных терминалов используются номера MSISDN. Они также предоставляют удобные средства для того, чтобы связаться с терминалом конкретного абонента. В современных внедрениях ОСС, предназначены ли они для M2M или H2H коммуникации, каждому абоненту присваивается номер MSISDN. Формат MSISDN подробно описан в Рекомендации ITU-T E.164. Хотя он позволяет внедрять большое количество устройств, национальными номерными планами разных стран ограничены возможности MSISDN до нескольких цифр (на основании прогнозов касательно персональной связи). Возьмем, к примеру, Францию, где мобильным операторам присвоены следующие блоки номеров: 06 XX XX XX XX и 07 XX XX XX XX. Такие номерные планы предполагают наличие максимум 200 миллионов абонентов, что может быть достаточно для 65 миллионов жителей, однако этот предел будет быстро достигнут при масштабном внедрении технологий межмашинного взаимодействия. В периоды раннего внедрения одним из вариантов оптимизации этого ресурса может стать использование частных планов MSISDN. К сожалению, это решение накладывает определенные ограничения, касающиеся, например, оперативной совместимости при роуминге. В силу этого, такое решение может не подойти для подключения автомобиля, совершающего поездки за границу и требующего возможности подключения в роуминге для дальнейшего использования M2M-сервиса.

Когда M2M-устройства создают каналы передачи данных, используется IP-адресация. В зависимости от сценария и требований внедрения может использоваться и общественная, и частная IP-адресация. Для оптимизации ресурсов IP-адресации ОСС может быть использована частная IP-адресация, однако для этого необходима особая установка сети либо для постройки специальных частных сетей для M2M-серверов и подчиненных им M2M-устройств, либо для развертывания транслятора сетевых адресов (NAT), когда M2M-сервер располагается в сети Интернет. Частная IP-адресация имеет следующие ограничения:

дополнительные расходы, связанные с развертыванием NAT;

Существует возможность, что M2M-сервер не сможет связаться с M2M-устройством в случае коммуникации по инициативе сервера, если не будет внедрена четкая методология образования проколов NAT. Следовательно, все еще будет необходим запуск устройств через SMS, даже если M2M-устройство имеет установленный PDP-контекст.

**3.2.3.3 Использование контекста CS-домена для сервисов только данных**

Хотя можно поспорить с тем, что M2M-устройство, настроенное на использование услуг только PS-домена не требует наличия присвоенного номера MSISDN, на практике, тем не менее, стандарт 3GPP считает обязательным наличие MSISDN, поскольку некоторые процедуры, такие как выставление счетов, проводятся с использованием MSISDN в качестве идентификатора. Кроме того, использование SMS-сообщений в качестве механизма для запуска устройств подразумевает необходимость наличия MSISDN, а также подписки на CS-домен в дополнение к подписке на PS-домен. Подписка на CS-домен связана с определенными затратами, связанными с необходимостью поддержки контекста CS-домена.

В нынешнем стандарте 3GPP о SMS номера MSISDN используются для отправки SMS-сообщений. Продолжающаяся работа 3GPP направлена на решение этого ограничения, чтобы появилась возможность появления «только-PS» подписки и отправки SMS на идентификатор IMSI (международный идентификатор мобильного абонента), то есть, без необходимости использования MSISDN.

**3.2.3.4 Выводы касательно проблем раннего внедрения**

Хотя существует несколько проблем, связанных с внедрениями M2M-технологий, самыми важными вопросами остаются те, что касаются перегрузки и переполнения, а также недостатка ресурсов нумерации и адресации. Стандарты и управляющие органы работают в направлении решения этих двух типов проблем с целью предоставления долгосрочного закрепления, которое обеспечит беспрепятственное и экономичное распространение M2M. В том, что касается адресации, хотя текущая динамика роста технологии IPv6 может предоставить конкретные прогнозы на ближайшее будущее, ее широкомасштабное внедрение зачастую затрудняется конечными пользователями.

В том, что касается перегрузки и переполнения, становится совершенно ясно, что хотя усовершенствование стандартов и должно обеспечить долгосрочное закрепление, для текущего роста внедрения M2M-сетей необходимо краткосрочное решение, не влияющее на стабильность сети. Элементы такого решения представлены в следующем разделе.

**3.2.4 Возможная оптимизация внедрений M2M**

В данном разделе приводится обзор лучших современных практик, касающихся сетевого планирования и архитектуры и обеспечивающих рост внедрений M2M, в то время как новые стандарты разрабатываются с целью долгосрочного закрепления. В другой части раздела рассказывается о необходимости распознавания трафика. Распознавание трафика – это базовый фактор, позволяющий создавать оптимизированную архитектуру M2M-сетей.

**3.2.4.1 Распознавание трафика**

Распознавание M2M-трафика как таковое является основным методом, позволяющим:

оптимизировать рабочую сеть так, чтобы она лучше управлялась с M2M-внедрениями. В дальнейшем в этом разделе мы продемонстрируем, как определенные устройства опорной сети могут быть настроены и оптимизированы для обработки M2M-запросов.

создать M2M-специфические функции эксплуатации, администрирования и обслуживания (OAM). К примеру, в случае переполнения, связанного со сбоем некоторого множества устройств, зачастую будет желательно полностью отключить устройства, вызывающие переполнение, например, устройства, относящиеся к основам M2M-сервисов. Как вариант, можно перенаправлять соответствующих абонентов на другое сетевое устройство так, чтобы не оказывать влияния на наиболее важные сервисы. При этом сетевой администратор имеет средства для прекращения сопряженного ущерба и оперативной поддержки других сервисов. Как только основная причина проблемы будет устранена (например, новая версия прошивки M2M-устройства вызывает слишком частое подключение к сети), трафик может быть снова направлен в сеть.

**3.2.4.2 Использование диапазона IMSI**

Распознавание трафика может выполняться путем использования выделенных диапазонов IMSI. Эти выделенные диапазоны будут организованы по категориям использования и встроены в регистр местонахождения (HLR) / HSS-сервер абонентов и в шлюзовый коммутационный центр мобильной связи (GMSC) с тем, чтобы определять регулярную маршрутизацию M2M-трафика. Идентификатор IMSI состоит из 15 цифр: первые пять цифр используются для мобильного кода страны и кода сети мобильной связи. Следующие две цифры могут использоваться для маршрутизации к определенным регистрам местонахождения для M2M, в то время как подмножество оставшихся цифр может быть использовано для распознавания определенного конечного пользователя, например, основных коммунальных предприятий, или определенного сегмента рынка M2M, например, eHealth.

**3.2.4.3 Выделенное центральное оборудование опорной сети**

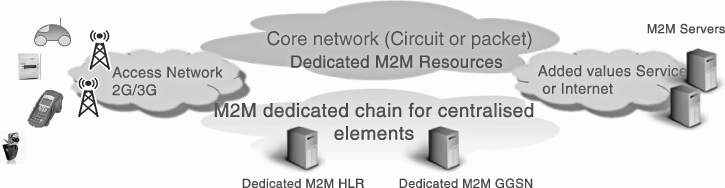
Чтобы беспрепятственно управиться с любым вариантом применения M2M, здесь мы продемонстрируем важность распознавания M2M-трафика. Данный параграф призывает к использованию сетевых архитектур, в которых определенные сетевые устройства предназначены специально для обработки M2M-трафика. Для их обозначения мы используем термин «выделенные M2M-сети».

[На рисунке 3.9](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_0009) показаны два устройства опорной сети из которых состоит выделенная M2M-сеть:

**регистр местонахождения (HLR)** – это центральная база данных абонентов сети. При использовании определенных диапазонов IMSI для M2M появляется возможность направления всех запросов на регистрацию в сети на определенный регистр HLR. При этом оператор сети может избежать переполнения и перегрузки вследствие большого количества одновременных запросов от M2M-устройств на регистрацию в сети, к примеру, роуминговых устройств, теряющих покрытие оператора А и пытающихся подключиться к оператору B. Вдобавок, при выделении определенного регистра HLR под M2M его конфигурация и обслуживание может быть оптимизирована для работы с M2M. Например, объем памяти регистра HLR для M2M-абонентов может быть оптимизирован благодаря тому, что для абонентов с определенной категорией устройств обычно наличествует большой объем абонентских данных. Также, поскольку некоторые M2M-устройства являются стационарными, регистр HLR можно оптимизировать путем снижения частоты проведения процедур управления мобильностью и, таким образом, улучшить производительность HLR-устройств.

**узел поддержки шлюза GPRS (GGSN)** – это сетевое устройство, выполняющее помимо всего прочего функцию шлюза для IP-сетей или, выражаясь точнее, для сетей компаний или Интернета, где обычно располагается M2M-сервер. Техническая конфигурация этого устройства может быть настроена специально на работу с M2M. Для примера можно взять случаи, когда определенные M2M приложения требовали использования постоянных каналов передачи данных, хотя генерировали малые объемы трафика. В этом случае узел GGSN может быть настроен и устроен так, чтобы обрабатывать бесконечно большее количество PDP-контекстов при использовании меньшего объема памяти для передачи данных.

[**Рисунок 3.9**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_fig_anc_0009) Оптимизированная сетевая архитектура для M2M.



Core network (circuit or packet) – Опорная сеть (коммутационная или пакетная); Dedicated M2M Resources – Выделенные ресурсы M2M; Access Network 2G/3G – Сеть доступа 2G/3G; Added values service or Internet – Дополнительные сервисы или Интернет; M2M Servers – M2M-серверы; M2M dedicated chain for centralized elements – Выделенная M2M-сеть для централизованных элементов; Dedicated M2M HLR – Выделенный регистр HLR для M2M; Dedicated M2M GGSN – Выделенный узел GGSN для M2M

**3.2.4.4 Детальная настройка элементов опорной сети: APN-специфическая конфигурация GGSN для M2M**

В дополнение к использованию выделенной M2M-сети для опорной сети, определенная конфигурация и оптимизация опорной сети поможет обеспечить дальнейшую эффективность в управлении M2M. В данном разделе приводится пример конфигурации имен точек доступа (APN) узла GGSN для M2M. Такая конфигурация определенных точек доступа позволяет *более тонким образом* управлять M2M-трафиком. Например, мы можем выбрать особое имя APN для трафика eHealth в связи с необходимостью обеспечения низкой задержки и вибраций. Такая необходимость будет отражена в соответствующей маркировке пакетов и создании высокого приоритета для такого трафика.

Имя точки доступа (APN) – это параметр GPRS, обеспечивающий направление трафика в IP-сети. Каждому абоненту регистра HLR может быть присвоено особый APN, активируемый при создании PDP-контекста.

Параметр APN может быть настроен с несколькими параметрами, чтобы создать особую форму поведения, которая обычно основывается на текущем соглашении с конечным пользователем:

**Режим подключения** может быть постоянным и непостоянным. В случаях с непостоянным подключением узел GGSN может быть настроен так, чтобы закрывать PDP-контекст по истечении определенного времени.

**Параметры IP-адресации** могут быть настроены на использование общественной или частной IP-адресации.

**Лимит времени для точки доступа** указывает время, по истечении которого PDP-контекст закрывается сетью. Этот механизм используется для того, чтобы избежать необходимости поддержки контекстов для каналов, которые больше не используются.

В таблице 3.2 путем иллюстрации определенных возможных типов категоризации создается 4 различных APN, которые затем разделяются на категории по режиму подключения (постоянный/непостоянный), либо по плану IP-адресации (общественный/частный). Каждый параметр APN может быть впоследствии отрегулирован в соответствии с типом трафика, которым он управляет: например, частные APN «M2M\_Al\_On-Private.com» и «M2M\_Non\_Perm-Private.com» используют NAT-маршрутизацию, в то время как публичные APN «M2M\_Al\_On-Public.com» и «M2M\_Non\_Perm-Public.com» используют маршрутизацию непосредственно через Интернет. При таком типе категоризации APN трафик M2M может быть не только отделен посредством выделенной M2M-сети, ему могут быть присвоены разные приоритеты/механизмы управления в зависимости от нужд клиента/сегмента рынка.

[**Таблица 3.2**](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_tbl_anc_0002) Категоризация и настройка APN

Имя точки доступа

M2M\_Al\_On-Private.com

M2M\_Al\_On-Public.com

M2M\_Non\_Perm-Private.com

M2M\_Non\_Perm-Public.com

План

IP-адресации

Частный

Публичный

Частный

Публичный

Лимит времени для точки доступа

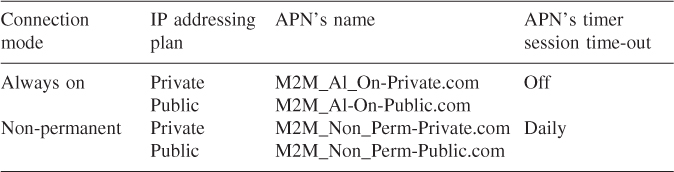
Отсутствует

Ежедневно

Режим подключения

Постоянный

Непостоянный



**3.3 Заключение**

Хотя M2M-приложения уже нашли свое место в рабочих сетях, невероятно важным остается тот факт, что M2M-технологии не могут считаться просто очередным сервисом персональной коммуникации. Сетевые операторы (и в частности, ОСС) придерживаются двухэтапного подхода:

Этап 1 заключается в оптимизации текущих используемых сетей M2M. При такой оптимизации в расчет принимаются некоторые фундаментальные характеристики M2M, такие как синхронность, неравномерность трафика и стационарные устройства. Множество лучших из существующих практик продолжают неуклонно развиваться вокруг:

**выделенных M2M-сетей** – суть таких сетей заключается в создании определенного набора сетевых элементов, управляющих M2M-трафиком. Эти элементы конфигурируются таким образом, чтобы справляться с нуждами M2M-трафика, в отличие от обычных конфигураций, предназначенных для персональной связи.

**распознавание трафика** – заключается в том, чтобы отличать M2M-трафик как для CS-, так и для PS- доменов с использованием специальных диапазонов IMSI и выделенных APN.

**оптимизация сетевого оборудования** – заключается в оптимизации оборудования специально для работы с M2M. В качестве примера в этой главе приведено использование оптимизированного регистра HLR, в котором, к примеру, используются меньшие контексты для каждого абонента, и реже запускаются процедуры управления мобильностью для стационарных M2M-устройств.

Перечень возможных процедур оптимизации, попадающих под Этап 1 можно продолжить. В данной главе не представлен обзор всех возможных процедур оптимизации, поскольку они могут отличаться в зависимости от различий операторов и в большей степени зависят от M2M-приложений, с которыми планируется работать.

Этап 2 заключается в обеспечении долгосрочного закрепления развернутых сетей ОСС путем введения новых возможностей и опций, изначально разработанных специально для M2M. Стандарт 3GPP TR 23.888 (-NIL-) служит отправной точкой для таких оптимизаций. Ожидается, что такие возможности поспособствуют более масштабному и экономичному внедрению M2M-технологий в будущем и станут применимы посредством обновления программного обеспечения или внедрения нового оборудования при необходимости. Примеры полезной сетевой оптимизации включают:

Возможность абонентской подписки типа «только PS»/без использования MSISDN: при наличии такой возможности операторам сотовой связи больше не нужно будет содержать абонентский контекст в CS-домене или присваивать M2M-устройствам, использующим исключительно пакетные сервисы, номера MSISDN.

Онлайн-запуск устройств: заключается в предоставлении эффективных механизмов для инициации установки каналов передачи данных.

[1](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_enote_anc_0001) В дальнейшей части главы термины «M2M-сервер» и «сервер M2M-приложений» используются взаимозаменяемо.

[2](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_enote_anc_0002) Канал передачи данных определяется структурой коммутации сети, позволяющей осуществлять передачу данных. Зачастую для ОСС используются следующие термины: PDP-контекст, канал пакетной радиосвязи общего пользования (GPRS), подключение сети пакетной передачи данных (PDN).

[3](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_enote_anc_0003) Пояснения касательно CSD-сервиса приведены на следующей странице.

[4](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_enote_anc_0004) Термин «MSC-S» означает сервер центра коммутации мобильной связи, а термин «SMS-C» означает центр передачи коротких сообщений (SMS-центр).

[5](file:///C:\Users\user\AppData\Local\Temp\AVSTemp325273488\AvsTmpDll15045\AvsTmpDll15045\OEBPS\#c03_enote_anc_0005) На одно лишь перечисление всех возможных проблем, возникающих при внедрении, может уйти целая глава.

**Источники**

3GPP TR 23.888 (2011). Системные усовершенствования для машинных коммуникаций.