№5
февраль 2017

MSK IX

Интернет изнутри

Интернет вещей

Умные и опасные? Вопросы безопасности IoT

Вместе с ростом числа и типа устройств, подключённых к Интернету, растут и риски, связанные с безопасностью и защитой частной жизни.

с. 46

Содержание:

Журнал «Интернет изнутри»
По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №5, дата выхода: январь 2017 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
Эл № ФС77-63308

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Редакционная коллегия:
Воронина Елена
Платонов Алексей

Дизайн:
Чернега Наталья

Корректор:
Рябова Наталья

Интернет вещей

главный редактор,
Андрей Робачевский

Многие вещи нам непонятны не потому, что наши понятия слабы; но потому, что сии вещи не входят в круг наших понятий.

Козьма Прутков «Плоды раздумья»

Дорогой читатель!

Хотя сама концепция вещи, подключенной к Интернету, не нова, очевидно, что сегодня мы наблюдаем новый виток эволюции Сети. Миниатюризация сенсорных, исполнительных и вычислительных элементов вкупе с неуклонным уменьшением стоимости привела к тому, что практически любой физический объект можно "подключить" к Интернету, любой механизм автоматизировать и управлять им удаленно.

Это, конечно, открывает новые возможности. Это и автоматизированные системы освещения, энергосбережения, управления транспортом, производственными процессами, распределения и доставки продукции, позволяющие в реальном времени контролировать состояние вплоть до мельчайших компонентов этих систем и принимать оптимальные решения. Это и автоматизация домашних систем освещения, отопления и безопасности. Это и беспилотные транспортные средства...

Количество переходит в новое качество.

В этом номере мы постарались подобрать статьи, более детально рассматривающие этот качественный переход - от архитектурных решений системы до отдельных технологических элементов IoT, от вопросов безопасности до перспектив развития IoT в России.

Вопросам безопасности посвящено несколько статей, поскольку тема эта является чрезвычайно актуальной. Отчасти это связано с тем, что решение этих вопросов осложняется отсутствием четкой формулировки самой проблемы, отчасти потому, что IoT связывает виртуальный мир с физическим, перенося киберпроблемы в реальную жизнь.

В этом номере мы прощаемся с авторами двух популярных рубрик, которые они начали и вели на протяжении жизни журнала. Это "Мультистейкхолдерские кунштюки" Леонида Тодорова и "Путевые заметки" Ольги Александровой-Мясиной. Мне, как и многим читателям, будет не хватать этих публикаций.

Перед вами пятый выпуск. Надеемся, что он оправдает ваши ожидания. Расскажите нам, что вам понравилось, а что – нет, о чем бы вы хотели прочитать в следующих номерах. Ждем ваших отзывов и предложений по адресу info@internetinside.ru.

Интернет вещей: сетевая архитектура и архитектура безопасности

Уильям Стеллингс (William Stallings)*

Интернет вещей (Internet of Things, IoT) – новейший этап длительной и еще не закончившейся революции в области вычислительных систем и средств связи. IoT - это термин, которым обозначается все разрастающийся комплекс подключенных друг к другу интеллектуальных устройств, от бытовой техники до крошечных датчиков. В этой статье мы приведем обзор IoT, а затем рассмотрим сетевую архитектуру и архитектуру безопасности IoT, которые помогут в разработке, реализации и развертывании IoT.

Интернет вещей (Internet of Things, IoT) – новейший этап длительной и еще не закончившейся революции в области вычислительных систем и средств связи. Его размер, многообразие и влияние на повседневную жизнь, коммерческую деятельность и государственное управление затмевают предыдущую историю технического прогресса. IoT - это термин, которым обозначается все разрастающийся комплекс подключенных друг к другу интеллектуальных устройств, от бытовой техники до крошечных датчиков. Доминантной темой является встраивание мобильных приемопередатчиков малого радиуса действия в разнообразные гаджеты и предметы повседневного быта, что открывает новые формы коммуникации между людьми и вещами, а также между разными вещами. Сегодня Интернет обеспечивает соединение между собой миллиардов промышленных и бытовых предметов, как правило, с помощью облачных систем. Такие предметы передают информацию датчиков, действуют в соответствии со своим окружением, а иногда могут самомодифицироваться, создавая общую среду управления более крупной системой, такой как завод или даже город.

"Вещами" в интернете вещей являются, главным образом, глубоко встроенные устройства с такими отличительными особенностями, как узкая полоса пропускания, сбор данных с низкой повторяемостью и малый объем используемых данных. Эти устройства обмениваются данными друг с другом и предоставляют данные через пользовательские интерфейсы. Некоторые встроенные устройства IoT, такие как охранные видеокамеры высокого разрешения, видеотелефоны VoIP и немногие другие, требуют для работы широкополосного стриминга. Но бесчисленное число других продуктов требует передачи пакетов данных всего лишь время от времени.

В этой статье мы приведем обзор IoT, а затем рассмотрим сетевую архитектуру и архитектуру безопасности IoT, которые помогут в разработке, реализации и развертывании IoT.

Контекст

Развивающийся Интернет охватывает миллиарды объектов, использующих стандартные архитектуры коммуникации для предоставления услуг конечным пользователям. Эта эволюция создает новые взаимодействия между физическим миром и миром вычислений, цифрового контента, анализа, приложений и услуг. Возникший в результате интернет вещей (IoT) открывает беспрецедентные возможности пользователям, изготовителям устройств и поставщикам услуг в самых разных секторах. В числе направлений, которым пойдут на пользу возможности сбора данных, автоматизации и анализа, предоставляемые IoT, - здравоохранение и фитнес-индустрия, мониторинг и автоматизация жилых домов, энергосбережение и "интеллектуальная электросеть", сельское хозяйство, транспорт, экологический мониторинг, инвентаризация и управление продукцией, безопасность, видеонаблюдение, образование и многие другие.

Технологическое развитие происходит во многих областях. Неудивительно, что исследования беспроводных сетей проводятся и сейчас, и уже достаточно длительное время, правда, раньше они назывались иначе: мобильные вычисления, всепроникающий компьютинг, беспроводные сенсорные сети и киберфизические системы.

Разработано множество предложений и продуктов в области энергоэффективных протоколов, безопасности и конфиденциальности, адресации, экономичных радио, энергосберегающих схем для продления срока службы батареек, надежности сетей, составленных из ненадежных и бессистемно "засыпающих" узлов. Подобный прогресс в области беспроводных технологий жизненно важен для роста IoT. Кроме того, имеют место такие направления разработки, как придание IoT-устройствам возможности взаимодействия с социальными сетями, использование межмашинного взаимодействия, хранение и обработка больших объемов информации в реальном времени, программирование приложений, предоставляющих конечным пользователям интеллектуальные и полезные интерфейсы с этими устройствами и данными.

Многие делились своим видением IoT. Stankovic говорит о преимуществах для людей, таких как перевод повседневной деятельности

в цифровую сферу; использование фрагментов бионической кожи для коммуникации с окружающими интеллектуальными объектами для большего комфорта, здоровья и безопасности; интеллектуальные часы и нательные устройства, оптимизирующие доступ к городским услугам. Среди преимуществ для города можно назвать отсутствие задержек на транспорте за счет отказа от светофоров и использования 3D-транспортных устройств. Интеллектуальные здания могут не только контролировать энергопотребление и безопасность, но и поддерживать деятельность для укрепления здоровья. Так же, как люди получили новые способы доступа к окружающему миру посредством смартфонов, IoT создаст новую парадигму в том плане, что предоставит нам непрерывный доступ к необходимой информации и услугам.

По оценкам Cisco, за следующее десятилетие чистая прибыль экономики IoT составит $14,4 трлн. Согласно исследованиям компании, в этом играют роль пять основных движущих сил:

- Использование активов ($2,5 трлн): IoT сокращает расходы на продажи, общие и административные расходы и стоимость проданных товаров, оптимизируя выполнение и эффективность бизнес-процессов.
- Производительность труда ($2,5 трлн): IoT повышает производительность труда за счет эффективного использования человеко-часов.
- Цепочки поставок и логистика ($2,7 трлн): IoT снижает количество отходов и повышает эффективность процессов.
- Удовлетворенность клиентов ($3,7 трлн): IoT повышает ценность для заказчика и увеличивает долю рынка, добавляя новых клиентов.
- Инновации, включая снижение времени выхода на рынок ($3,0 трлн): IoT повышает отдачу от вложений в НИОКР, снижает время выхода на рынок и создает дополнительные потоки доходов за счет новых бизнес-моделей и возможностей.

Аналогично опубликованный в 2015 году отчет McKinsey Global Institute констатирует, что прогнозируемый общий экономический эффект IoT сейчас составляет $3,9 трлн, а к 2025 году достигнет 11,1 трлн. По самой верхней оценке объем этого эффекта - включая дополнительные доходы от потребителей - к 2025 году будет эквивалентен 11% мировой экономики.

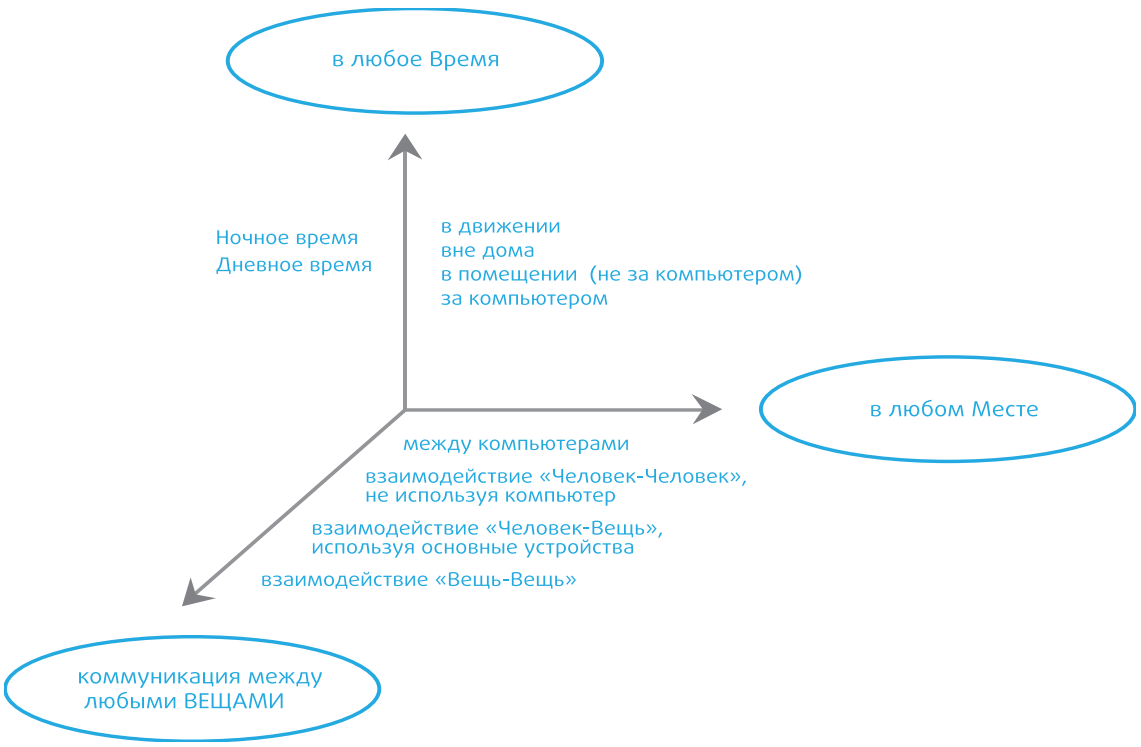
Масштаб интернета вещей

Отдел стандартов связи МСЭ (Международный союз электросвязи, International Telecommunication Union) опубликовал Рекомендацию Y.2060, озаглавленную "Обзор интернета вещей" (Overview of the Internet of Things). В этом документе содержатся следующие определения, описывающие охват IoT:

- Интернет вещей (IoT): Глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий.
- Вещь: Применительно к интернету вещей означает предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи.
- Устройство: Применительно к интернету вещей означает элемент оборудования, который обладает обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также ввода, хранения и обработки данных.

В большинстве литературы IoT считается связанным с коммуникацией между интеллектуальными предметами. Рекомендация Y.2060 распространяет эту концепцию на виртуальные вещи - ниже мы рассмотрим это подробнее. Согласно Рекомендации Y.2060, IoT характеризуется добавлением измерения “коммуникация между любыми ВЕЩАМИ” к технологиям информации и связи, которые уже обеспечивают коммуникацию “в любое ВРЕМЯ” и “в любом МЕСТЕ” (рис. 1).

Рис.1. Новое измерение, появившееся в интернете вещей.



В книге Designing the Internet of Things элементы IoT сведены в простую формулу:

Физические объекты + контроллеры, сенсоры, исполнительные механизмы + Интернет = IoT

Эта формула четко описывает саму суть интернета вещей. Экземпляр IoT состоит из набора физических объектов, каждый из которых:

- содержит микроконтроллер, обеспечивающий интеллектуальность;
- содержит датчик, измеряющий какой-либо физический параметр, и/или исполнительный механизм, срабатывающий от какого-либо физического параметра;
- имеет возможность коммуникации по Интернету или какой-либо другой сети.

Элементом, не входящим в эту формулу и охваченным определением по Y.2060, является способ идентификации отдельной вещи, обычно называемый тегом.

Обратите внимание, что хотя в литературе всегда используется термин "интернет вещей", точнее было бы назвать его сетью вещей, поскольку речь идет не о "большом" Интернете (потому "интернет вещей" и пишется по-русски с маленькой буквы - перев.). Например, инсталляция "умного дома" состоит из набора вещей в доме, обменивающихся информацией по Wi-Fi или Bluetooth с центральным контроллером. На заводе или ферме интернет вещей может поддерживать корпоративные приложения, которые будут взаимодействовать со средой и запускать приложения, использующие интернет вещей. В этих примерах удаленный доступ по Интернету обычно имеется, но его может и не быть. Независимо от того, есть ли такое подключение к Интернету или нет, набор "умных" объектов на площадке, в комплекте с любыми другими вычислительными устройствами и устройствами хранения, можно охарактеризовать как "сеть вещей" или "интернет вещей" (с маленькой буквы).

Таблица 1, в основу которой лег график Beecham Research, дает представление об области охвата IoT.

Стандарты совместимости IoT

В ближайшее время разнородные "островки" решений, скорее всего, будут обгонять в своем развитии развертывание IoT-решений, основанных на функционально-совместимых стандартах. Так обстоят дела с любой новой технологией на этапе ее зарождения. Например, Sutaria and Govindachari отмечают, что две характеристики сетевых IoT-устройств, вызывающие наибольшие проблемы, - это наличие устройств с низким энергопотреблением (рассчитанных на работу месяцами и годами без подзарядки) и частый обмен данными по сетям с потерей пакетов. Нынешние стандартные протоколы Интернета в этих условиях неоптимальны. В более широком смысле имеет место дисбаланс между огромным количеством устройств, генерирующих данные с бешеной скоростью в разных местах, и использованием сетевых технологий и облачных систем, которые хранят огромные объемы данных в небольшом количестве локаций при относительно низкой скорости обновления данных. Интеграция этих двух классов систем для удовлетворения потребностей пользователей требует определенных возможностей от сетевых протоколов во всей архитектуре сети и протоколов, от физического уровня к прикладному.

Над решением этих вопросов работает несколько организаций и стандартизационных форумов, стремясь расширить или адаптировать протоколы Интернета для устройств IoT. Для создания единой структуры и классификации необходимых функций по их месту в стеке протоколов ряд этих групп также занимается вопросом формальной архитектуры для IoT. В то время как существующие стандарты и Интернет сделали IoT возможным, в ближайшем будущем вряд ли возможно появление стека новых стандартов, которые дополнят или модифицируют существующие для сферы IoT. Как и многие другие достижения, ставшие возможными благодаря Интернету, IoT будет какое-то время стихийно развиваться и проходить через процессы естественного отбора, пока постепенно не выявятся жизнеспособные технологии и механизмы протоколов. В настоящей статье мы рассмотрим два направления работы по созданию общих концепций, которые могут оказаться полезными в уже идущем процессе стандартизации.

Эталонная модель IoT от МСЭ-Т

С учетом сложности IoT имеет смысл создание архитектуры, которая бы специфицировала основные компоненты и их взаимосвязь. Архитектура IoT может предоставить следующие преимущества:

- дать администратору сети или IT-менеджеру полезный контрольный список для оценки функциональности и полноты предложений от разных поставщиков;
- служить ориентиром для разработчиков в плане того, какие функции нужны в IoT и как они взаимодействуют;
- служить основой для стандартизации, стимулируя совместимость и сокращение расходов.

В настоящем разделе мы приведем обзор архитектуры IoT, разрабатываемой сектором стандартизации Международного союза электросвязи (МСЭ-Т или ITU-T). В следующем разделе мы обсудим архитектуру, разрабатываемую Всемирным форумом IoT (IoT World Forum). Последняя, создаваемая индустриальной группой, использует полезный альтернативный подход для понимания масштаба и функциональности IoT.

Эталонная модель IoT от МСЭ-Т описана в Рекомендации Y.2060. В отличие от большинства других эталонных моделей и архитектурных моделей, описанных в литературе, модель МСЭ-Т детализирует фактические физические компоненты экосистемы IoT. Это полезно, так как высвечивает элементы экосистемы IoT, которые должны быть соединены, интегрированы, управляемы и предоставлены приложениям. Детальная спецификация экосистемы описывает требования к возможностям IoT.

Один из важных аспектов, который заостряет модель, - тот факт, что IoT на деле не является сетью физических вещей. Это скорее сеть устройств, взаимодействующих с физическими вещами, вместе с прикладными платформами - такими как компьютеры, планшеты и смартфоны, - которые взаимодействуют с этими устройствами. Поэтому обзор модели МСЭ-Т мы начнем с обсуждения устройств.

Терминология

Ниже приведен список определений ключевых терминов из Рекомендации Y.2060:

Сеть связи (Communication Network): инфраструктурная сеть, соединяющая устройства и приложения, такая как сеть на основе стека протоколов IP или Интернет.

Вещь (Thing): предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи.

Устройство (Device): элемент оборудования, который обладает обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также ввода, хранения и обработки данных.

Устройство переноса данных (Data-carrying Device): устройство переноса данных подключается к физической вещи и непрямым образом соединяет эту физическую вещь с сетями связи. Примерами могут служить ак-

Таблица 1 Интернет вещей

Сектор услуг	Прикладные группы	Расположения	Примеры устройств
IT и сети	Публичные	Услуги, e-коммерция, центры данных, мобильная связь, проводная связь, ISP	Серверы, хранилища, PC, маршрутизаторы, коммутаторы, PBX
	Корпоративные	IT/центры данных, офисы, частные сети	
Безопасность, охрана	Оборудование слежения, контроль	Радары/спутники, военная безопасность, беспилотники, оружие, транспорт, корабли, самолеты, снаряжение	Танки, истребители, боевые комплекты связи, джипы
	Общественная инфраструктура	Люди, животные, почта, пища/здоровье, упаковка, багаж, подготовка воды, экология зданий, общая экология	Автомобили, дорожные рабочие, службы безопасности, пожарные, экологический мониторинг
	Аварийные службы	Оборудование и персонал, полиция, пожарные, регуляторы	Машины скорой помощи, машины аварийных служб
Розничная торговля	Специализированные	АЗС, игровые клубы, боулинг, кино, дискотеки, спецмероприятия	Кассовые терминалы, бирки, знаки, торговые автоматы
	Туризм и общепит	Гостиницы, рестораны, бары, кафе, клубы	
	Магазины	Супермаркеты, торговые центры, единичные магазины, центры дистрибуции	
Транспорт	Неавтомобильный	Воздушный, железнодорожный, морской	Машины, освещение, корабли, самолеты, знаки, таможня
	Автомобильный	Легковые, грузовые, строительная техника, внедорожники	
	Транспортные системы	Система оплаты, управление трафиком, навигация	
Промышленность	Распределение	Трубопроводы, конвейеры, обработка материалов	Насосы, клапаны, чаны, конвейеры, двигатели, приводы, преобразование, производство, сборка/упаковка, емкости, танки
	Преобразование, дискретное	Металл, бумага, резина, пластик, металлоизделия, электронные платы, тестирование	Сектор услуг
	Процессы	Нефтехимия, углеводороды, еда, напитки	
	Автоматизация ресурсов	Горное дело, ирригация, сельское хозяйство, лесное хозяйство	
Здравоохранение и науки о жизни	Здравоохранение	Больницы, реанимации, мобильные станции, клиники, лаборатории, кабинеты врачей	MRI, КПК, импланты, хирургическое оборудование, насосы, мониторы, телемедицина
	Ин-виво, домашние системы	Импланты, домашние системы мониторинга	
	Исследования	Разработка лекарств, диагностика, лаборатории	
Потребительский сектор и дом	Инфраструктура	Проводка, сетевой доступ, управление энергопотреблением	Цифровые камеры, энергосистемы, посудомойки, электронные книги, настольные компьютеры, стиральные машины, датчики, лампочки, телевизоры, MP3, игровые приставки, освещение, сигнализация
	Безопасность	Охранные системы/сигнализации, пожарная безопасность, экобезопасность, для стариков, для детей, защита энергоснабжения	
	Комфорт и развлечения	Кондиционеры, освещение, приставки, развлекательные системы	
Энергия	Спрос/предложение	Производство энергии, передача и распределение, низковольтные сети, качество энергии, управление энергией	Турбины, ветряки, UPS, батарейки, генераторы, датчики, аккумуляторы
	Альтернативные источники	Солнечная, ветровая, когенерация, электрохимическая	
	Нефть и газ	Платформы, буровые, устьевое оборудование, насосы, трубопроводы	
Здания	Коммерческие, организаций	Офисы, образование, торговля, общепит, здравоохранение, аэропорты, стадионы	ОВКВ, транспорт, пожарная безопасность, освещение, охрана, доступ
	Промышленные	Производственные, чистые, кампусы	

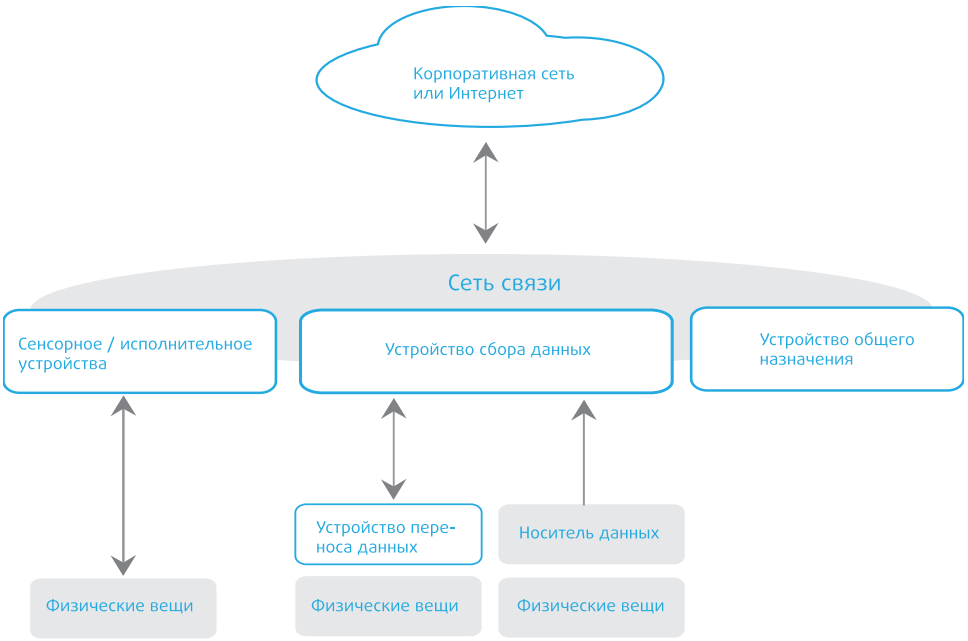
тивные бирки RFID.

Устройство сбора данных (Data-capturing Device): под устройством сбора данных понимается считывающее/записывающее устройство, имеющее возможность взаимодействия с физическими вещами. Взаимодействие может осуществляться непрямым образом с помощью устройств переноса данных или напрямую с помощью носителей данных, подключенных к физическим вещам.

обработки и связи и может обмениваться данными с сетями связи с использованием проводных или беспроводных технологий. Устройства общего назначения включают оборудование и приборы, относящиеся к различным областям применения IoT, например, станки, бытовые электроприборы и смартфоны.

Шлюз (Gateway): элемент IoT, соединяющий устройства с сетями связи. Он выполняет необходимую трансляцию между протоколами, используемыми в сетях связи и в устройствах.

Рис.2. Типы устройств и их взаимосвязь с физическими вещами.



Носитель данных (Data Carrier): безбатарейный объект переноса данных, подключенный к физической вещи и имеющий возможность предоставлять информацию пригодному для этого устройству сбора данных. Эта категория включает штрих-коды и QR-коды, наклеенные на физические вещи.

Сенсорное устройство (Sensing Device): устройство, которое может обнаруживать или измерять информацию, относящуюся к окружающей среде, и преобразовывать ее в цифровые электрические сигналы.

Исполнительное устройство (Actuating Device): устройство, которое может преобразовывать цифровые электрические сигналы, поступающие от информационных сетей, в действия.

Устройство общего назначения (General Device): устройство общего назначения обладает встроенными возможностями

Уникальным аспектом IoT, по сравнению с другими сетевыми системами, очевидно является наличие множества физических вещей и устройств, отличных от вычислительных устройств и устройств обработки данных. На рис. 2, адаптированном из Рекомендации Y.2060, изображены типы устройств в модели МСЭ-Т. Модель рассматривает IoT как сеть устройств, тесно связанных с вещами. Сенсорные и исполнительные устройства взаимодействуют с физическими вещами в окружающей среде. Устройства сбора данных считывают данные из физических вещей или записывают данные на физические вещи путем взаимодействия с устройствами переноса данных или носителями данных, подключенными или связанными с физическим объектом тем или иным образом.

Эта модель проводит различие между устройствами переноса данных и носителями данных. Устройство переноса данных является устройством в смысле Рекомендации Y.2060. Как минимум, устройство всегда обладает возможностями связи и может обладать другими электронными возможностями. Примером устройства переноса данных является RFID-бирка. В то же время носитель данных - это элемент, присоединенный к физической вещи с целью идентификации или информирования.

В Рекомендации Y.2060 отмечается, что технологии, используемые для взаимодействия между устройствами сбора данных и устройствами переноса данных или носителями данных, включают радиочастотное, инфракрасное, оптическое и гальваническое возбуждение. Примеры каждой из них:

- Радиочастотные: радиочастотные идентификационные (RFID)-бирки, или радиометки.

- Инфракрасные: инфракрасные метки, используемые в Вооруженных Силах, больницах и других средах, где нужно отслеживать расположение и перемещение персонала. Это и отражающие инфракрасные нашивки на военной форме, и работающие от батареек бейджи, излучающие идентификационную информацию. Последние могут содержать кнопку, при нажатии которой бейдж может использоваться для прохода через портал, и бейджи, автоматически повторяющие сигнал для контроля за перемещениями персонала. Пульты дистанционного управления, используемые в быту или в других средах для управления электронными устройствами, тоже можно легко интегрировать в IoT.

- Оптические: штрих-коды и QR-коды могут служить примерами идентификационных носителей данных, которые считываются оптически.

- Гальваническое возбуждение: примером могут служить медицинские импланты, использующие электропроводящие свойства человеческого тела[9]. В ходе коммуникации между имплантом и поверхностью гальваническая пара передает сигналы с импланта на электроды, выведенные на кожу. Эта схема использует очень мало энергии, что позволяет снизить размер и сложность имплантированного устройства.

Последним типом устройств с рисунка 2 являются устройства общего назначения. Они обладают возможностями обработки данных и связи, которые могут быть инте-

грированы в IoT. Хорошим примером является технология "умного дома", которая может интегрировать практически любое устройство в доме в сеть для централизованного или дистанционного управления.

На рис. 3 приведен обзор элементов, задействованных в IoT. В левой части рисунка приведены различные способы связи с физическими устройствами. Предполагается, что одна или несколько сетей поддерживают связь между устройствами.

На рис. 3 появляется еще одно устройство, связанное с IoT: шлюз. Как минимум шлюз работает транслятором между протоколами. Шлюзы решают одну из главных проблем при проектировании IoT, а именно проблему совместимости, как между разными устройствами, так и между устройствами и Интернетом либо корпоративной сетью. "Умные" устройства поддерживают широкий спектр беспроводных и проводных технологий передачи данных и сетевых протоколов. Кроме того, возможности обработки данных у таких устройств, как правило, ограничены.

Рекомендация Y.2067 закрепляет требования к шлюзам IoT, которые обычно распадаются на три категории:

- Шлюз поддерживает различные технологии доступа к устройствам, позволяя устройствам обмениваться данными друг с другом и с сетью - Интернетом или корпоративной сетью, содержащей приложения IoT. Такие схемы доступа могут, например, включать ZigBee, Bluetooth и Wi-Fi.
- Шлюз поддерживает необходимые сетевые технологии как для локальных, так и для глобальных сетей. Эти технологии могут включать в себя Ethernet и Wi-Fi на территории организации, а также сотовую связь, Ethernet, DSL и кабельный доступ к Интернету и глобальным корпоративным сетям.
- Шлюз поддерживает взаимодействие с приложениями, управление сетью и функции безопасности.

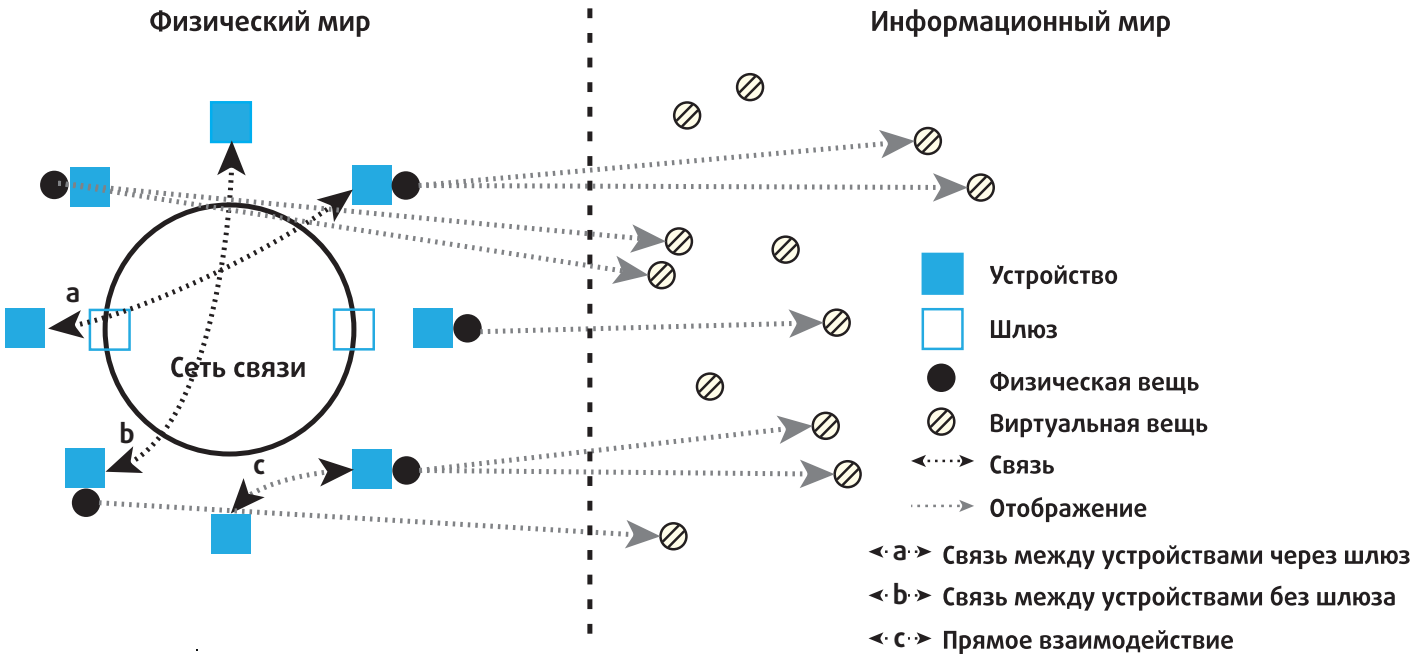
Два первых требования включают в себя трансляцию протоколов между различными сетевыми технологиями и стеками протоколов. Третье требование обычно называется функцией IoT-агента. В сущности, IoT-агент предоставляет функциональность высокого уровня от имени IoT-устройств, такую как организация или резюмирование данных из нескольких устройств для передачи в IoT-приложения, обеспечение протоколов и функций безопасности и взаимодействие с системами управления сетью.

Здесь следует отметить, что термин "сеть связи" прямо не определяется в серии IoT-стандартов Y.206x. Сеть (или сети) связи поддерживает связь между устройствами и может непосредственно поддерживать прикладные платформы. Она может иметь размеры небольшого IoT, такого как домашняя сеть "умных" устройств. В более общем смысле сеть (или сети) устройств соединяется с корпоративными сетями или Интернетом для связи с системами приложений и серверами, на которых расположены базы данных, связанные с IoT.

Теперь можно вернуться к левой части рисунка 3, иллюстрирующей возможности связи устройств между собой. Первая возможность - связь между устройствами через шлюз. Например, с помощью шлюза сенсорное или исполнительное устройство с поддержкой Bluetooth может осуществлять связь с устройством сбора данных или устройством общего назначения, использующим Wi-Fi. Вторая возможность - связь по сети связи без шлюза. Например, если все устройства в сети "умного дома" поддерживают Bluetooth, они могут управляться с компьютера, планшета или смартфона с поддержкой Bluetooth. Третья возможность - прямая связь устройств между собой по отдельной локальной сети, в то время как связь с внешней сетью (на рисунке не показана) осуществляется через шлюз LAN. Приведем пример такой возможности. Представьте себе, что на большой территории, например, на ферме или заводе, находится большое число датчиков с низким энергопотреблением. Эти устройства взаимодействуют между собой для последовательной передачи данных на устройство, подключенное к шлюзу в сеть связи.

В правой части рисунка 3 подчеркивается, что каждая физическая вещь в интернете

Рис.3. Технический обзор IoT (Рекомендация Y.2060).



вещей может быть представлена в информационном мире одной или несколькими виртуальными вещами, но при этом виртуальная вещь может существовать без соответствующей физической вещи. Физические вещи сопоставлены виртуальным вещам, хранящимся в БД и других структурах данных. Приложения обрабатывают виртуальные вещи и работают с ними.

На рис. 4 изображена эталонная модель IoT от МСЭ-Т, состоящая из четырех уровней плюс возможности управления и безопасности, действующие между уровнями. До сих пор мы говорили об уровне устройства. В терминах функциональности связи уровень устройства включает в себя, грубо говоря, физический и канальный уровни OSI. Теперь перейдем к другим уровням.

Уровень сети выполняет две базовых функции. Возможности сети относятся к взаимодействию устройств и шлюзов. Транспортные возможности относятся к транспорту информации служб и приложений IoT, а также информации управления и контроля IoT. Грубо говоря, эти возможности соответствуют сетевому и транспортному уровням OSI.

Уровень поддержки услуг и поддержки приложений предоставляет возможности, которые используются приложениями. Многие разнообразные приложения могут использовать общие возможности поддержки. К примерам относятся общая обработка данных и управление БД. Специализированные возможности поддержки - это конкретные возможности, которые предназначены для удовлетворения потребностей конкретного подмножества приложений IoT.

Уровень приложения состоит из всех приложений, взаимодействующих с IoT-устройствами.

Уровень возможностей управления охватывает традиционные функции управления сетью, т.е. управление неисправностями, управление конфигурацией, управление учетом, управление показателями работы и управление безопасностью.

В Рекомендации Y.2060 в качестве примеров общих возможностей управления перечислены:

- управление устройствами: примеры включают обнаружение устройств, аутентификацию, дистанционную активацию и деактивацию устройств, конфигурацию, диагностику, обновление прошивки и/или ПО, управление рабочим статусом устройства;
- управление топологией локальной сети: примером является управление конфигурацией сети;
- управление трафиком и перегрузками: например, обнаружение условий перегруженности сети и реализация резервирования ресурсов для срочных и/или жизненно важных потоков трафика.

Специализированные возможности управления тесно связаны с требованиями приложений, например, требованиями по контролю линии передачи электроэнергии в "умной" электросети.

Уровень возможностей обеспечения безопасности включает общие возможности обеспечения безопасности, которые не зависят от приложений. В Рекомендации Y.2060 примеры общих возможностей обеспечения безопасности включают:

- на уровне приложения: авторизацию, аутентификацию, защиту конфиденциальности и целостности данных приложения, защиту неприкосновенности частной жизни, аудит безопасности и антивирусную защиту;
- на уровне сети: авторизацию, аутентификацию, конфиденциальность данных об использовании и данных сигнализации, а также защиту целостности данных сигнализации;
- на уровне устройства: аутентификацию, авторизацию, проверку целостности устройства, управление доступом, защиту конфиденциальности и целостности данных.

Специализированные возможности обеспечения безопасности тесно связаны с требованиями приложений, например, требованиями безопасности мобильных платежей.

Рис.4. Эталонная модель IoT по Рекомендации Y.2060.

Эталонная модель Всемирного форума IoT

Всемирный форум IoT (IoT World Forum, IWF) - спонсируемое отраслью ежегодное событие, объединяющее представителей бизнеса, госструктур и вузовской науки с целью продвижения IoT на рынок. Комитет по архитектуре Всемирного форума IoT, составленный из лидеров индустрии, включая IBM, Intel и Cisco, в октябре 2014 года опубликовал эталонную модель IoT. Эта модель служит общей структурой, призванной помочь отрасли ускорить развертывание IoT. Модель предназначена для того, чтобы стимулировать сотрудничество и способствовать созданию повторяемых моделей внедрения.

Эта эталонная модель является полезным дополнением к модели МСЭ-Т. Документы МСЭ-Т делают упор на уровнях устройства и шлюза, описывая верхние уровни лишь в общих чертах. И действительно, в Рекомендации Y.2060 все описание уровня приложения уместилось в одну фразу. Наибольшее внимание рекомендации серии Y.206x уделяют определению концепции для поддержки разработки стандартов взаимодействия с устройствами IoT.

IWF озабочен более масштабным вопросом разработки приложений, промежуточного ПО и функций поддержки для корпоративного интернета вещей. Предложенная семиуровневая модель изображена на рис. 5.

Документальное описание модели IWF, опубликованное Cisco, указывает, что разработанная модель отличается следующими характеристиками:

- упрощает: помогает разбить сложные системы на части так, чтобы каждая из этих частей стала понятнее;
- проясняет: предоставляет дополнительные сведения для точной идентификации уровней IoT и выработки общей терминологии;
- идентифицирует: идентифицирует аспекты, в которых те или иные типы обработки оптимизированы в различных частях системы;
- стандартизирует: представляет собой первый шаг к тому, чтобы поставщики могли создавать продукты IoT, способные взаимодействовать друг с другом;
- организует: делает IoT реальным и доступным, а не просто абстрактной концепцией.

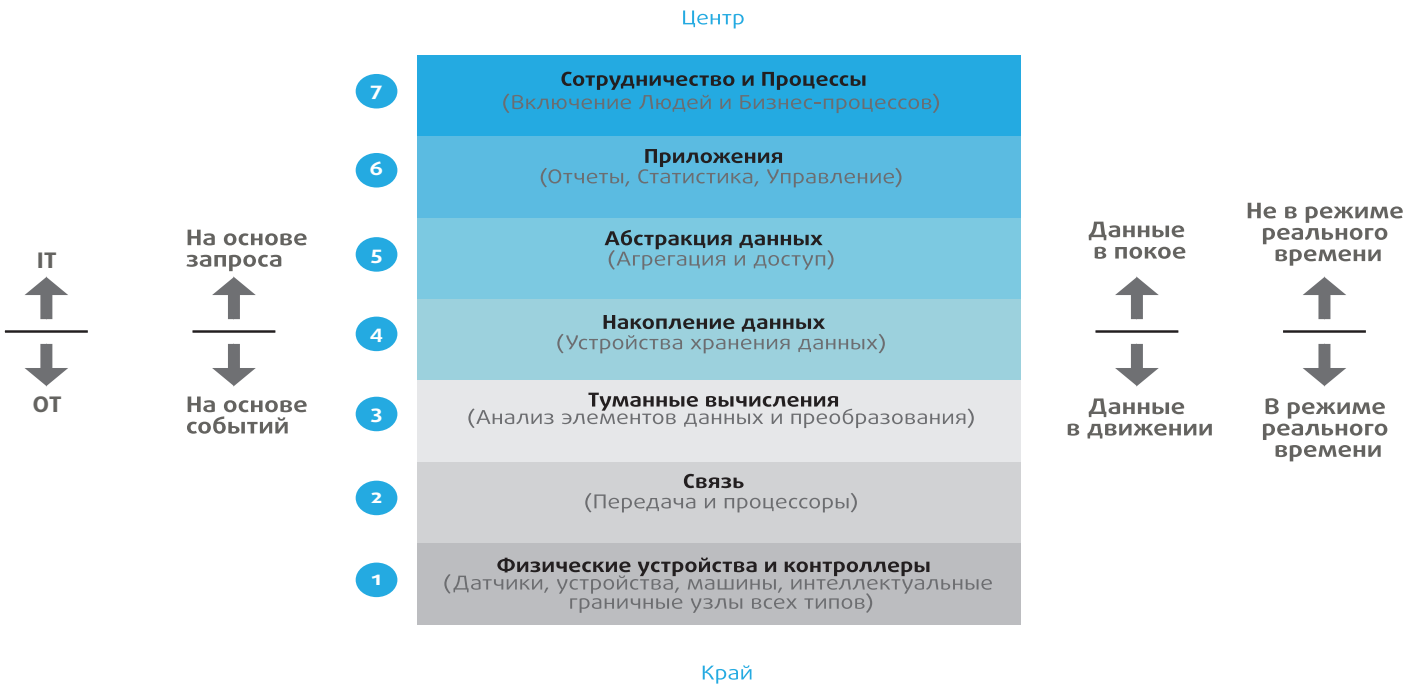
Уровень 1 образуют физические устройства и контроллеры, которые могут управлять несколькими устройствами. Уровень 1 модели IWF примерно соответствует уровню устройства в модели МСЭ-Т (рис. 4). Как и в модели МСЭ-Т, элементы на этом уровне - не физические вещи как таковые, а устройства, взаимодействующие с физическими вещами, такие как сенсорные и исполнительные устройства. Среди прочих возможностей эти устройства могут уметь осуществлять аналого-цифровое и цифро-аналоговое преобразование, генерацию данных, а также поддерживать дистанционный опрос и/или дистанционное управление.

С логической точки зрения этот уровень реализует связь устройств между собой и между устройствами и низкоуровневой обработкой на уровне 3. С физической точки зрения этот уровень состоит из сетевых устройств, таких как маршрутизаторы, коммутаторы, шлюзы и брандмауэры, используемых для создания локальных и глобальных сетей и подключения к Интернету. Этот уровень позволяет устройствам осуществлять связь друг с другом и посредством более высоких логических уровней обмениваться данными с прикладными платформами, такими как компьютеры, устройства дистанционного управления и смартфоны.

Уровень 2 модели IWF примерно соответствует уровню сети в модели МСЭ-Т. Основное отличие в том, что модель IWF относит шлюзы к уровню 2, в то время как в модели МСЭ-Т они относятся к уровню 1. Поскольку шлюз является сетевым устройством и устройством связи, отнесение его к уровню 2 имеет больше смысла.

Во многих внедряемых системах IoT распределенная сеть датчиков может генерировать большие объемы данных. Например, офшорные нефтяные месторождения и нефтеперерабатывающие заводы могут генерировать до терабайта данных ежедневно. Самолет может генерировать несколько терабайт данных в час. Вместо того, чтобы хранить все эти данные постоянно (или хотя бы долгое время) в централизованном хранилище, доступном для приложений IoT, часто более целесообразно выполнять как можно большую часть обработки данных как можно ближе к датчикам. Поэтому задачей уровня периферийных вычислений (edge computing level) является преобразование сетевых потоков данных в информацию, пригодную для хранения и более высокоуровневой обработки. Элементы обработки на этом уровне могут иметь дело с большими объемами данных и выполнять операции преобразования данных, в результате которых хранить приходится уже гораздо меньший объем. Опубликованный Cisco документ по модели IWF содержит следующие примеры операций на уровне периферий-

Рис.5. Эталонная модель Всемирного форума IoT.



ных вычислений:

- анализ: анализ данных по критериям того, подлежат ли они обработке на более высоком уровне;
- форматирование: переформатирование данных для единообразной высокоуровневой обработки;
- разархивирование/декодирование: обработка криптографических данных с дополнительным контекстом (таким как происхождение);
- дистилляция/сокращение: сокращение и/или резюмирование данных для того, чтобы минимизировать эффект на объем данных и трафик в сети и в высокоуровневых системах обработки;
- оценка: определение того, представляют ли данные пороговое значение или аварийный сигнал; этот процесс должен включать перенаправление данных дополнительным получателям.

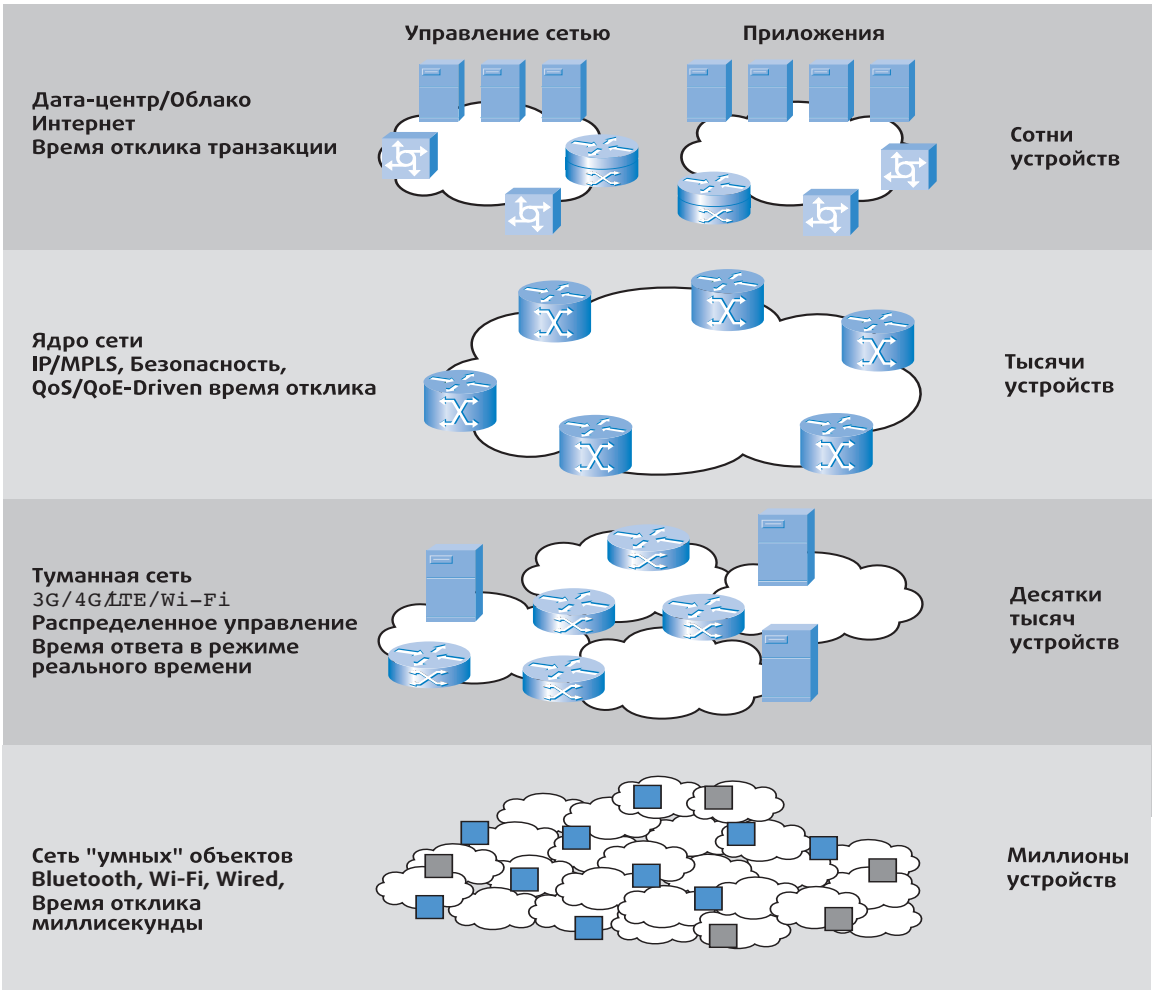
Элементы обработки на этом уровне соответствуют устройствам общего назначения в модели МСЭ-Т (рис. 2). Как правило, они развертываются физически на краю сети IoT, т.е. рядом с сенсорами и другими устройствами генерации данных. Таким образом, часть базовой обработки больших объемов генерируемых данных снимается с прикладных программ IoT, расположенных центрально.

Обработка на уровне периферийных вычислений иногда называется туманными вычислениями (Fog Computing). Туманные вычисления и туманные службы, как ожидается, станут отличительной характеристикой IoT. Этот принцип проиллюстрирован на рис. 6. Туманные вычисления представляют в современных сетевых технологиях тренд, противоположный облачным вычислениям. В облачных вычислениях большой объем централизованных ресурсов хранения и обработки данных доступен распределенным потребителям посредством облачных сетевых структур для относительно небольшого числа пользователей. В туманных вычислениях большое число отдельных интеллектуальных объектов осуществляют связь с туманными сетевыми структурами, которые осуществляют вычисления и хранят ресурсы рядом с периферийными устройствами в IoT. Туманные вычисления решают проблемы, возникшие вследствие деятельности тысяч или миллионов "умных" устройств, включая проблемы безопасности, конфиденциальности, ограниченных возможностей сети и задержки. Термин "туманные вычисления" выбран потому, что туман стелется по земле, в то время как облака находятся высоко в небе.

Сравнение облачных и туманных вычислений приведено в таблице 2, составленной на основе данных.

На уровне 4, уровне накопления данных, данные, поступившие с различных устройств, профильтрованные и обработанные уровнем периферийных вычислений, помещаются в хранилище, где будут доступны для более высоких уровней. Этот уровень разительно отличается и от низкоуровневых (туманных), и от высокоуровневых (облачных) вычислений по особенностям конструкции, требованиям и методам обработки.

Рис.6. Туманные вычисления.



Данные, проходящие сквозь сеть, называются «данными в движении». Скорость и организация данных в движении определяется устройствами, генерирующими данные. Генерация данных происходит по событиям, либо периодически, либо по возникновении какого-либо события в среде. Для сбора данных и их обработки необходимо реагировать на их появление в реальном времени. Напротив, многим приложениям не требуется обрабатывать данные со скоростью сетевой передачи. На практике ни облачная сеть, ни прикладные платформы не смогли бы успевать за объемами данных, генерируемых гигантским количеством IoT-устройств. Вместо этого приложения имеют

дело с «данными в покое», т.е. данными в том или ином легкодоступном хранилище. Приложения могут обращаться к данным по мере необходимости либо вне режима реального времени. Таким образом, высокие уровни функционируют по принципу транзакций, в то время как три нижних уровня работают по событиям.

Ниже перечислены операции, выполняемые на уровне накопления данных:

- преобразование «данных в движении» в «данные в покое»;
- преобразование формата из сетевых пакетов в реляционные таблицы БД;
- переход от вычислений по событиям к вычислениям по запросу;
- значительное снижение объема данных за счет фильтрации и выборочного хранения.

Еще один взгляд на уровень накопления данных заключается в том, что он представляет собой границу между информационными технологиями (IT), под которыми понимается целый спектр технологий обработки информации, включая ПО, оборудование, технологии связи и сопутствующие службы, и операционными технологиями (Operational Technology, OT), представляющими собой оборудование и ПО, обнаруживающие или вызывающие изменения путем прямого мониторинга и/или контроля физических устройств, процессов и событий на предприятии.

Уровень накопления данных впитывает большое количество данных и помещает их в хранилище, практически не приспосабливая к потребностям конкретных приложений или групп приложений. С уровня периферийных вычислений в хранилище может поступать множество разных видов данных в разных форматах и от разнородных обработчиков. Уровень абстракции данных может агрегировать и форматировать такие данные способами, которые делают доступ приложений более управляемым и эффективным. В числе связанных задач могут быть следующие:

- Комбинирование данных из различных источников, включая выверку нескольких форматов данных.
- Выполнение необходимых преобразований для обеспечения единообразной семантики данных из разных источников.

Таблица 2 Сравнение облачных и туманных вычислений

	Облако	Туман
Расположение ресурсов хранения/обработки	Центр	Край
Задержка	От низкой до высокой	Низкая
Доступ	Фиксированный или беспроводной	Главным образом беспроводной
Поддержка мобильности	Неприменимо	Да
Контроль	Централизованный/иерархический (полный контроль)	Распределенный/иерархический (частичный контроль)
Доступ к службам	Через ядро	На краю/с наладонника
Доступность	99,99%	Высокая нестабильность/высокий уровень резервирования
Число пользователей/устройств	Десятки и сотни миллионов	Десятки миллиардов
Основной генератор контента	Люди и устройства	Устройства/сенсоры
Генерация контента	В центральном расположении	Везде
Потребление контента	На конечных устройствах	Везде
Виртуальная программная инфраструктура	Центральные корпоративные серверы	Пользовательские устройства

- Помещение отформатированных данных в соответствующую базу данных, например, большие объемы повторяющихся данных помещаются в систему больших данных, такую как Hadoop. Данные событий направляются в реляционную СУБД, отличающуюся более быстрым временем реакции и адекватным интерфейсом для таких типов данных.
- Оповещение приложений более высокого уровня о том, что данные заполнены или достигнут определенный уровень данных.
- Консолидация данных в одном месте (с помощью ETL (extract, transform, load), ELT (extract, load, transform) или репликации данных) либо предоставление доступа к нескольким источникам данных путем виртуализации данных.
- Защита данных путем соответствующей аутентификации и авторизации.
- Нормализация/денормализация и индексация данных для быстрого доступа приложений.

Уровень приложения содержит приложения любого типа, использующие данные IoT на входе или управляющие IoT-устройствами. Как правило, приложения взаимодействуют с уровнем 5 и с данными в покое, поэтому им необязательно функционировать на скоростях сети. Следует предусмотреть упрощенный режим работы, который позволит приложениям миновать промежуточные уровни и напрямую взаимодействовать с уровнем 3 или даже уровнем 2. Модель IWF не определяет приложения по всей строгости, считая этот аспект выходящим за рамки дискуссии о модели IWT.

Уровень взаимодействия и процесса появился в результате признания того, что IoT будет полезен лишь тогда, когда с ним смогут взаимодействовать люди. Этот уровень может включать несколько приложений и обмен данными и/или управляющей информацией по Интернету или корпоративной сети.

IWF считает эталонную модель IoT принятой в отрасли базовой структурой, направленной на стандартизацию концепций и терминологии, связанных с IoT. Что еще более важно, модель IWF определяет необходимый функционал и проблемы, которые требуется решить до того, как отрасль сможет реализовать ценность IoT. Эта модель полезна как для поставщиков, разрабатывающих функциональные элементы внутри модели, так и для заказчиков, помогая им выработать свои требования и оценивать предложения поставщиков.

Фреймворк безопасности IoT

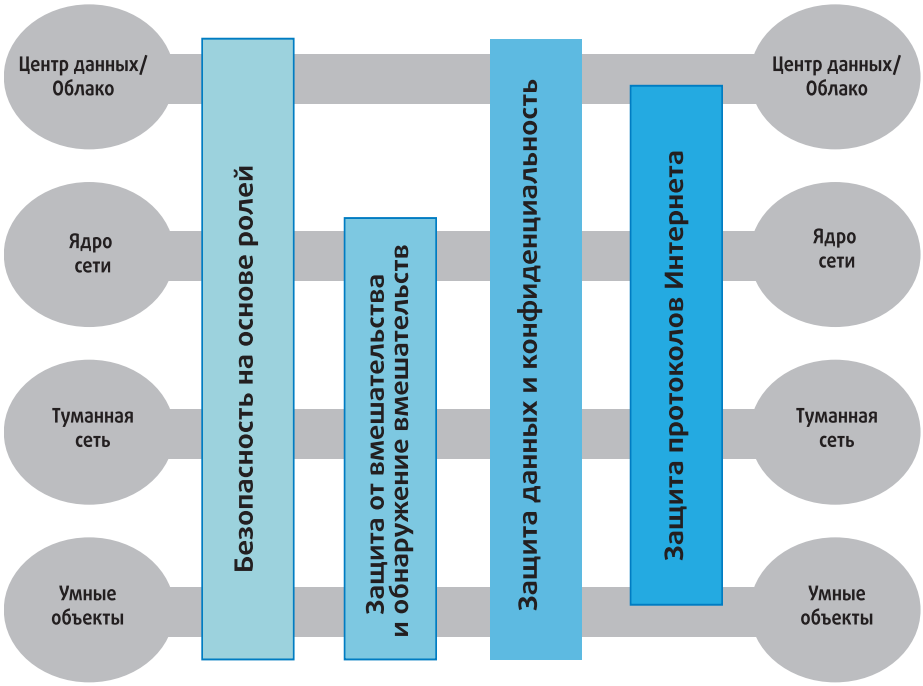
Компания Cisco Systems, сыгравшая ведущую роль в разработке модели Всемир-

ного форума IoT, разработала фреймворк безопасности IoT, ставший полезным дополнением к эталонной модели Всемирного форума IoT. На рисунке 7 показана среда безопасности, связанная с логической структурой IoT.

Модель Cisco IoT представляет собой упрощенную версию модели Всемирного форума IoT. Она состоит из следующих уровней:

- "Умные" объекты/встроенные системы: этот уровень включает в себя сенсорные/исполнительные устройства и другие встроенные системы на границе сети. Эта часть IoT наиболее уязвима. Устройства могут находиться в среде, не защищенной физически, и от них может требоваться функционирование в течение нескольких лет. Доступность тоже является важной проблемой. Кроме того, менеджерам сети необходимо заботиться об аутентичности и целостности данных, генерируемых сенсорами, и о защите исполнительных устройств и других "умных" устройств от несанкционированного использования. Также могут присутствовать такие требования, как конфиденциальность и защита от подслушивания.
- Туманная/периферийная сеть: этот уровень представляет проводные и беспроводные соединения устройств IoT. Кроме того, на этом уровне может осуществляться определенный объем обработки и консолидации данных. Ключевой проблемой является большая вариативность сетевых технологий и протоколов, используемых различными устройствами IoT, и необходимость выработки и воплощения единой политики безопасности.
- Ядро сети: уровень ядра сети предоставляет пути для передачи данных между платформами в центре сети и устройствами IoT. Здесь проблемы безопасности те же, что в традиционных сетях. Однако огромное количество оконечных узлов, с которыми надо взаимодействовать и управлять ими, создает значительную проблему для безопасности.
- Центр данных/облако: этот уровень содержит платформы для приложений, хранения данных и управления сетью. IoT не привносит на этот уровень никаких новых проблем безопасности, кроме необходимости иметь дело с гигантским количеством отдельных оконечных узлов.

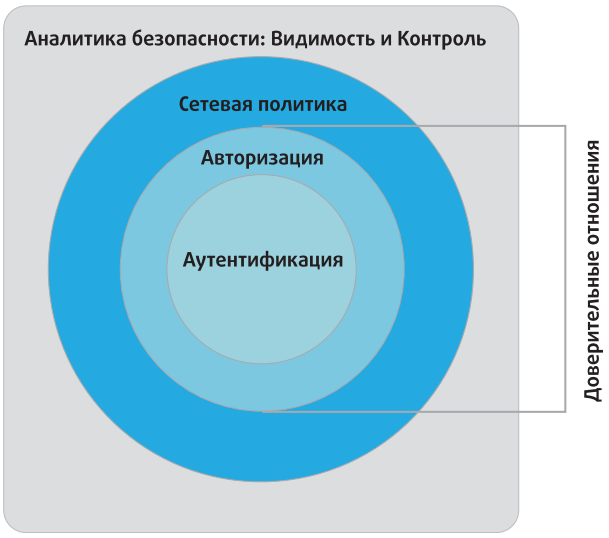
Рис.7. Среда безопасности IoT.



С помощью этой четырехуровневой архитектуры модель Cisco определяет четыре общих возможности безопасности, охватывающих несколько уровней:

- Безопасность на основе ролей: системы управления доступом на основе ролей (Role-Based Access Control, RBAC) назначают права доступа ролям, а не отдельным пользователям. Пользователям, в свою очередь, сопоставляются различные роли, либо статически, либо динамически, соответственно обязанностям. RBAC широко используется в коммерческих облачных и корпоративных системах. Этот инструмент, понятный администраторам, может использоваться для управления доступом к IoT-устройствам и генерируемым ими данным.

Рис.8. Безопасный фреймворк IoT.



- Защита от вмешательства и обнаружение вмешательств: эта функция особенно важна на уровне устройств и туманной сети, но распространяется также и на уровень ядра сети. Все эти уровни могут использовать компоненты, физически находящиеся вне физически охраняемой территории предприятия.
- Защита данных и конфиденциальность: эти функции охватывают все уровни архитектуры.

Защита протоколов Интернета: защита «данных в движении» от подслушивания и перехвата важна для всех уровней.

На рисунке 7 отмечены конкретные функциональные области безопасности поверх четырех уровней модели IoT. В документе Cisco также предлагается концепция безопасности IoT, определяющая компоненты функции безопасности для IoT, охватывающей все уровни, как показано на рис. 8. Перечислим четыре компонента:

- Аутентификация: этот компонент охватывает элементы, инициирующие доступ, и первым делом идентифицирует устройства IoT. В отличие от типичных корпоративных сетевых устройств, для которых

идентификация может осуществляться по идентификационным признакам человека (таким как имя/пароль или бейдж), оконечные устройства IoT должны оснащаться такими методами аутентификации, которые не требуют вмешательства человека. К таким методам относятся радиочастотные метки, сертификаты x.509 или MAC-адреса оконечных устройств.

- Авторизация: авторизация управляет доступом к устройству через структуру сети. Этот элемент включает в себя контроль доступа. Вместе с уровнем аутентификации он вырабатывает необходимые параметры для того, чтобы разрешить обмен информацией между устройствами и между устройствами и прикладными платформами, тем самым обеспечивая работу IoT-служб.

- Сетевая политика: этот компонент охватывает все элементы, осуществляющие маршрутизацию и транспортировку трафика с оконечных устройств по инфраструктуре, будь то контроль, управление или собственно трафик данных.

- Аналитика безопасности, включая видимость и контроль: этот компонент включает все функции, необходимые для централизованного управления устройствами IoT. В первую очередь он охватывает видимость IoT устройств, означающую попросту то, что центральные функции управления безопасно оповещены о парке распределенных устройств IoT, включая идентичность и атрибуты каждого устройства. На основе такой видимости возникает способность осуществлять контроль, включая конфигурацию, патчи и обновления, а также контрмеры для пресечения угроз.

Важным элементом этой концепции являются доверительные отношения. В этом контексте доверительные отношения означают способность двух партнеров по обмену быть уверенными в идентичности и правах доступа друг друга. Аутентификационный компонент концепции доверия реализует базовый уровень доверия, дополняемый авторизационным компонентом.

В документе Cisco приведен пример того, что автомобиль может установить доверительные отношения с другой машиной того же изготовителя. Такие доверительные отношения, однако, могут позволить машинам обмениваться только сведениями о безопасности. При установлении доверительных отношений между той же самой машиной и дилерской сетью машина может передавать и получать дополнительную информацию, такую как показания одометра и результаты последнего техобслуживания.

Выводы

Согласно процитированному выше отчету McKinsey, примерно 40% общей экономической ценности IoT приходится на способность всех физических устройств "разговаривать" друг с другом посредством компьютеров, т.е. на совместимость. Если совместимость ограничена, то ценность IoT может составить всего $7 трлн, в то время как развитая совместимость способна довести ценность IoT для глобальной экономики до $11 трлн к 2025 году. Примерно 40% всей возможной ценности зависит от способности различных систем IoT взаимодействовать друг с другом. В таблице 3, основанной на отчете McKinsey, приведена оценка экономической ценности (в процентах), требующей совместимости между IoT-системами для разных секторов.

Чтобы добиться такого типа совместимости, который необходим для раскрытия этих преимуществ, необходимо выработать стандарты для всех уровней функционала IoT, от уровня устройства до уровня приложения (рис. 4). Хотя эти стандарты пока еще пребывают в зачаточном состоянии, описанные в настоящей статье архитектурные модели являются полезным базисом для будущих усилий.

Таблица 3 Добавленная ценность благодаря совместимости IoT

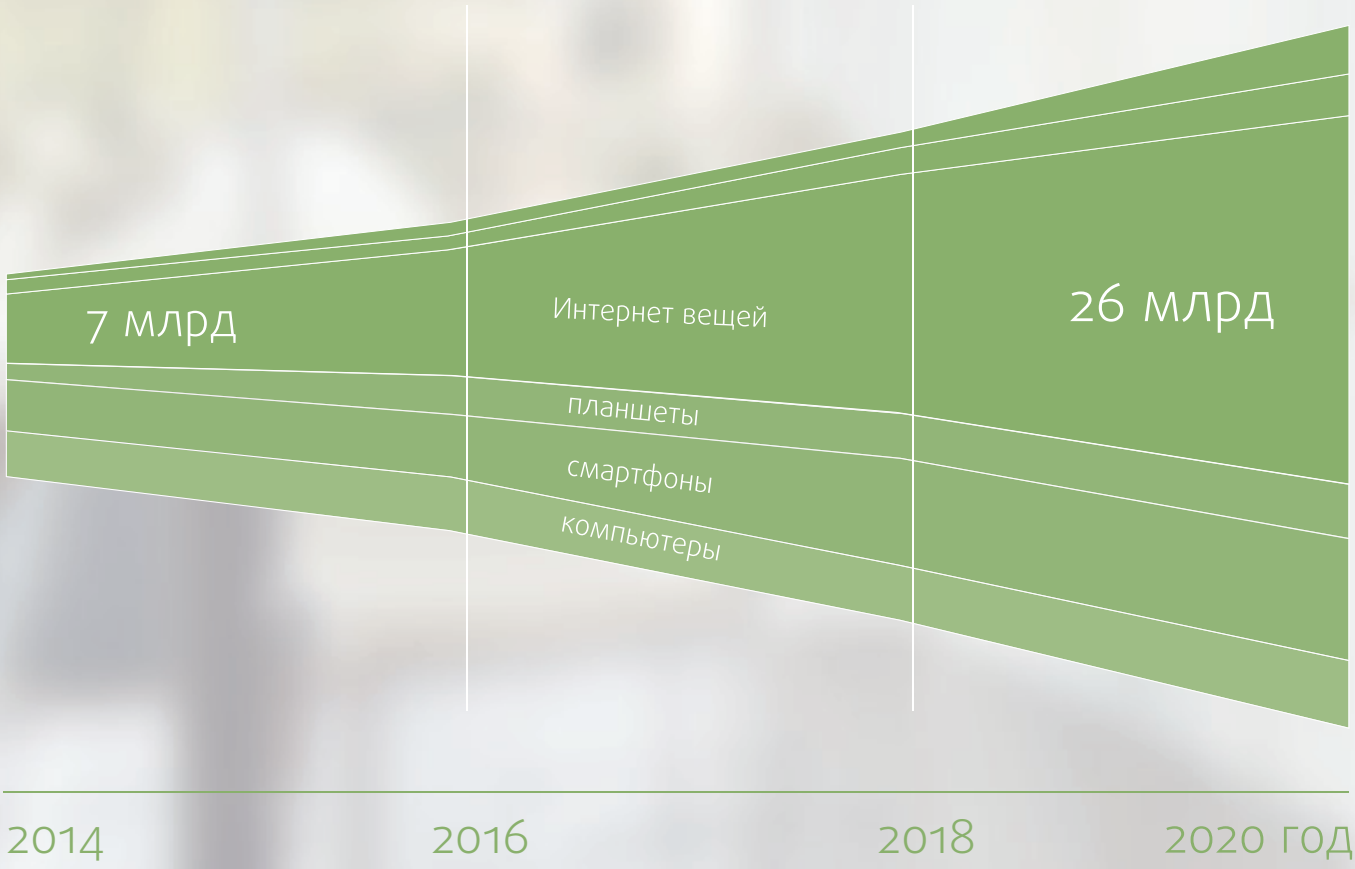
Ситуация	Потенциальная ценность, требующая совместимости (трлн долл.)	% общей ценности	Примеры того, как совместимость повышает ценность
Заводы и фабрики	1,3	36	Данные с различных типов оборудования повышают эффективность конвейера
Города	0,7	43	Видео, данные сотовых телефонов и автомобильные датчики отслеживают трафик и оптимизируют поток машин
Розничная торговля	0,7	57	Связь между системами оплаты и обнаружения предметов обеспечивает автоматическую оплату
Рабочие места	0,5	56	Связь между данными о расположении работника и механизмов поможет избежать несчастных случаев и попадания под воздействие химикатов
Автомобили	0,4	44	Данные об износе оборудования для страховки, техобслуживания и предпродажного анализа
Сельское хозяйство	0,3	20	Многочисленные системы датчиков для совершенствования управления фермой
Открытые пространства	0,3	29	Обмен навигационными данными между разными машинами и между машинами и GPS/контролем движения
Дом	0,1	17	Взаимодействие устройств для автоматизации домашних дел с безопасностью и энергосистемой
Офисы	>0,1	30	Данные из различных систем здания и других зданий повысят безопасность

Источник: The Internet of Things: Network and Security Architecture, The Internet Protocol Journal Vol 18, No 4

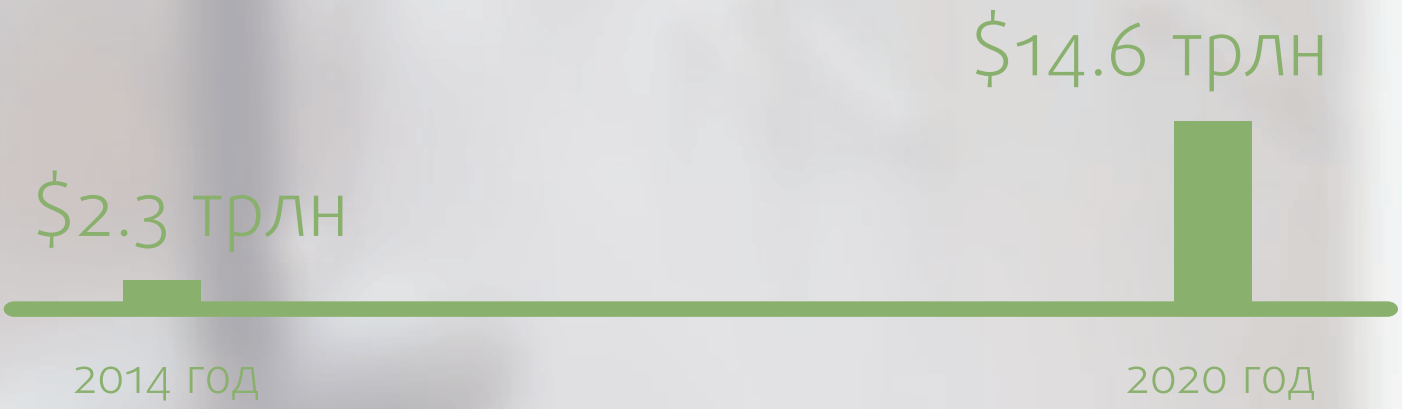
*Уильям Стеллингс (William Stallings) - независимый консультант и автор нескольких книг по безопасности, компьютерным сетям и компьютерной архитектуре. Его последняя книга озаглавлена: Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud (Pearson, 2016). Он держит сайт на ComputerScienceStudent.com с ресурсами для студентов в области компьютерных наук и профессионалов, а также входит в редакторский совет по криптологии. Имеет ученую степень Ph.D. по компьютерным наукам, присужденную Массачусетским технологическим институтом. Его электронный адрес: ws@shore.net

СТАТИСТИКА ПОДКЛЮЧЕННЫХ К ИНТЕРНЕТУ УСТРОЙСТВ И ВЕЩЕЙ

УСТРОЙСТВА



РЫНОЧНАЯ СТОИМОСТЬ IOT



Источник:
http://www.informationisbeautiful.net/visualizations/the-internet-of-things-a-primer/

МАШИНЫ

сейчас 2020

23 — 253

МИЛЛИОНОВ

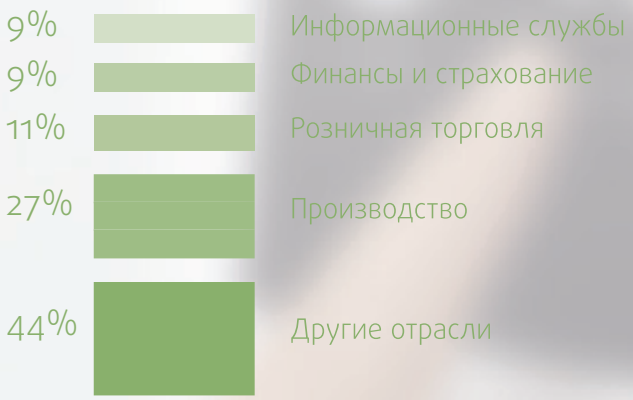
ЛАМПОЧКИ

сейчас 2020

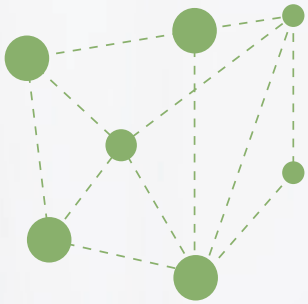
2 — 100

МИЛЛИОНОВ

ОБЛАСТИ



BIZ



1.7 МЛН

поключенных компаний в 2014 году

ЛЮДИ

2 из 3

купят умную технику для дома

1 из 2

планируют купить переносимые устройства

TECH

Стек IP-протоколов ZigBee

Дуглас Коумер (Douglas Comer)*

Эта статья начинается с нескольких примеров интеллектуальных встроенных систем и способов, с помощью которых они обмениваются информацией. Затем идет подробное обсуждение одной из технологий: стека протоколов для беспроводных полносвязных сетей, разработанных для приложений, управляющих интеллектуальными сетями электроснабжения (Smart Grid). Статья анализирует этот стек протоколов, использование IPv6 и некоторые последствия таких конструктивных решений.

Рождается огромная область сетевых технологий: коммуникация среди интеллектуальных встроенных систем. Идея заключается в том, что вычислительные системы могут быть встроены во множество устройств, и эти системы смогут использовать Интернет для коммуникации с другими устройствами. Конечно, некоторые устройства будут предоставлять информацию для людей, и люди могут пользоваться приложениями, контролирующими встроенные устройства. Следовательно, новая сетевая парадигма частично включает взаимодействие с человеком. Однако основной акцент при этом делается на системы, которые могут взаимодействовать с окружающей средой и друг с другом, а не на традиционные компьютеры, которые хранят данные и выполняют приложения. Исследователи и специалисты ввели в употребление термины «интернет вещей» (Internet of Things, IoT или iThings) и «M2M (межмашинные) приложения» (Machine-to-Machine Applications), которые отражают смысл этой идеи. Несмотря на довольно неуклюжую формулировку, термин «интернет вещей» стал общепринятым.

Эта статья начинается с нескольких примеров интеллектуальных встроенных систем и способов, с помощью которых они обмениваются информацией. Затем идет подробное обсуждение одной из технологий: стека протоколов для беспроводных полносвязных сетей, разработанных для приложений, управляющих интеллектуальными сетями электроснабжения (Smart Grid). Статья анализирует этот стек протоколов, использование IPv6 и некоторые последствия таких конструктивных решений.

Приложения для зондирования, мониторинга и контроля

Мы используем термин «встроенные системы» в отношении вычислительных систем, которые являются составной частью другого механизма или устройства. Главное различие между встроенной системой и обычной компьютерной системой следует из их внешних соединений. Обычная компьютерная система имеет дело с информацией: компьютер способен хранить и преобразовывать данные, а также обеспечивать к ним доступ. В отличие от этого, встроенная система способна воспринимать и контролировать физический мир вокруг себя. В качестве примера можно рассмотреть термостат, используемый для управления системой отопления и кондиционирования. Современный термостат (называемый «умным» термостатом) представляет собой встроенную систему: такой термостат содержит встроенный процессор, работающий под управлением программного обеспечения и выполняющий все необходимые функции.

Пользователь может сконфигурировать термостат таким образом, чтобы параметры настройки менялись в зависимости от времени дня. Термостат подключен к целому набору датчиков, который может включать датчик температуры помещения, датчик, обнаруживающий потоки воздуха (т.е. работает ли вентилятор), и датчик, подключенный к нажимным кнопкам (кнопкам-переключателям), который позволяет пользователю задать требуемую температуру. Более совершенные системы имеют в своем составе датчики относительной влажности воздуха. Кроме того, термостат подключен к элементам управления, которые позволяют процессору включать и выключать нагреватель или кондиционер, регулировать скорость вращения вентилятора, а также управлять функциями увлажнителя и влагопоглотителя.

Большинство компьютерных пользователей уже знакомы со встроенными системами. Например, подключенный к компьютеру принтер имеет в своем составе встроенную систему. После отправки компьютером документа на печать встроенная система принтера управляет двигателями и механизмами принтера, заставляя их подавать листы бумаги, перемещать механизм струйной печати и распылять капельки чернил (тонера).

Принтер также имеет в своем составе датчики, которые способны обнаруживать заторы при подаче бумаги и низкий уровень тонера.

General Electric (GE) – крупнейшая промышленная компания США – производит продукты, которые выходят далеко за пределы потребительского рынка. GE производит двигатели для самолетов, турбины для электростанций, локомотивы для железных дорог, медицинское оборудование для создания изображений и рассчитанные

для тяжелых условий работы машины, которые обеспечивают транспортировку людей, обогрев домов и электроснабжение заводов. Используя термин «Промышленный интернет» (Industrial Internet), компания GE ввела в действие крупную инициативу, направленную на объединение обменивающихся данными встроенных систем для использования как на заводах, так и в продуктах компании.

Сбережение и сбор энергии

Некоторые встроенные системы, например, встроенная система управления принтера, подключены к надежному источнику питания. Однако многие встроенные системы полагаются на временные источники энергии и сконструированы таким образом, чтобы ее сберегать. Например, сотовые телефоны работают от батарей (аккумуляторов), а датчики состояния окружающей среды, размещенные в удаленных местах (например, в пустыне), могут использовать фотоэлементы.

Как особый случай, некоторые встроенные системы способны собирать энергию из окружающей среды вокруг них. Например, размещенный в океане датчик может использовать движение волн для генерации электроэнергии, а датчик, расположенный рядом с горячим источником, использовать тепловую энергию. Сбор энергии даже включает использование кинетической энергии, которую генерируют люди при открывании двери или при нажатии на выключатель освещения. Возможна ситуация, когда встроенная система, использующая сбор энергии, вынуждена работать периодически – для аккумулирования достаточного заряда (например, при эксплуатации радиопередатчика).

Мир интеллектуальных встроенных систем

Для того, чтобы понять будущее интернета вещей, мы должны представить, что мощные встроенные системы появятся везде – дома, в офисе, в автомобиле, в торговом центре и на улице. Например, рассмотрим автомобили. В дополнение к навигационным и развлекательным системам конструкторы работают над системами, которые позволят автомобилю вычислять расстояние до соседних машин, обнаруживать объекты на дороге, предупреждать об изменении дорожного покрытия (например, в результате строительства), а также обнаруживать дорожные полосы и предупреждать водителя о заносе автомобиля. Автомобиль с интеллектуальной встроенной системой может обмениваться данными с соседними автомобилями и координировать торможение. Интеллектуальная встроенная система может использовать средства для распознавания лиц с целью идентификации водителя при посадке в автомобиль, регулировки параметров настройки в соответствии с предпочтениями водителя, отслеживания индивидуальных привычек управления автомобилем и наблюдения за необычной манерой вождения, адаптации предупреждений в соответствии со временем реакции конкретного водителя.

В офисных зданиях встроенные системы уже обнаруживают присутствие людей и соответствующим образом регулируют освещение и отопление/кондиционирование. Система может использовать датчики для изменения режима работы систем отопления и кондиционирования при открытых окнах. Что более важно, интеллектуальные встроенные системы смогут использовать алгоритмы обучения для накопления закономерностей. Например, если некоторые сотрудники часто входят и выходят из своего офиса в течение рабочего дня, то система может научиться не выключать отопление до тех пор, пока эти сотрудники не будут отсутствовать в течение более длительного времени. Аналогично, если сотрудник имеет обыкновение работать спозаранку, система может изучить эту закономерность и соответствующим образом управлять офисной средой. Таким образом, если сотрудник обычно приходит на работу рано и каждый день уходит домой в 15.00, то интеллектуальная система может выучить эту закономерность и ожидать прибытия и отбытия сотрудника в соответствующее время.

Важность коммуникации

Почему же акцент смещается на интеллектуальные системы, способные обмениваться между собой данными? Они имеют множество преимуществ. Например, в дополнение к локальной координации, коммуникация позволяет системам использовать облачные вычисления[10, 11] для анализа данных, полученных от набора встроенных устройств. Коммуникация означает, что встроенные системы могут иметь меньший объем памяти и менее мощные процессоры, что ведет к снижению энергопотребления. Короче говоря, небольшие встроенные системы могут выполнять сложные функции благодаря совместной работе с соседними встроенными системами либо за счет доступа к удаленной информации.

В качестве примера можно рассмотреть набор датчиков, используемых для оценки механического напряжения в таких объектах гражданской инфраструктуры, как мосты. Измерение напряжения важно для того, чтобы понять, сможет ли мост выдержать определенную нагрузку, требуется ли его укрепить и когда его необходимо заменить. Для измерения механического напряжения инженеры размещают небольшие, питающиеся от батареи датчики в различных точках по всему мосту. Без возможности обмена данными каждый датчик должен располагать собственным локальным хранилищем для хранения измерений вместе с соответствующей отметкой времени для каждого из них. Если каждый датчик имеет в своем составе средства радиосвязи, то набор датчиков способен сформировать беспроводную сеть, по которой данные измерений передаются в точку сбора, а сама эта точка может располагаться где-то в Интернете, далеко от моста. В контексте измерений это важное различие обусловлено координацией и быстротой анализа. Коммуникация позволяет сенсорным узлам использовать протокол, который снимает показания одновременно. Сбор данных в реальном времени делает возможным быстрое обнаружение опасных ситуаций и принятие мер до того, как произойдет авария.

Кроме того, коммуникация позволяет снизить издержки. Возьмем для примера умные счетчики, которые используются компаниями, предоставляющими коммунальные услуги. Традиционный подход к оценке расхода заключается в размещении счетчика за пределами того места, где располагается клиент, и в ежемесячной отправке сотрудника для снятия показаний счетчика. Умный счетчик имеет в своем составе средства беспроводной коммуникации, а это означает, что коммунальная компания может считывать его показания удаленно. Даже если умный счетчик использует радиопередатчик, диапазон действия которого охватывает только ближайшую улицу, его показания можно снять с помощью проезжающего по этой улице автомобиля, а не посредством прямого обхода сотрудником компании, что позволяет резко сократить расходы на снятие показаний счетчиков.

Встроенные системы в торговых центрах

В дополнение к вышеописанным сенсорным системам интернет вещей включает весьма неожиданные области применения. Например, многие торговые центры теперь располагают крупными видеоэкранами,

показывающими рекламные ролики. Магазины используют эти экраны для рекламы продуктов и услуг, а также скидок и специальных акций. Коммуникация необходима для динамической загрузки этих рекламных роликов, поскольку их контент и графики показа могут измениться в любой момент – менеджменту требуется способность контролировать, какая реклама показывается на данном экране и как долго она остается видимой.

Где расположена система управления видеоэкранами и какие сетевые технологии необходимы для подключения этой системы управления к отдельным экранам? Ответ на этот вопрос довольно интересен и немного удивителен: в рамках современной реализации каждый экран имеет в своем составе стек протоколов TCP/IP и подключение к глобальной сети Интернет. Интернет-соединение позволяет размещать систему управления в любом месте. В частности, торговый центр может прибегнуть к аутсорсингу IT-функций, разместив систему управления в «облаке». Что более важно, оснащение каждого экрана интернет-соединением и программным обеспечением протоколов означает, что контент не обязательно должен размещаться на том же физическом хосте, что и управляющая система.

Возможность отделить контент от управляющей системы очень важна, поскольку это позволяет отделить информацию, которой владеет розничный торговец, от системы управления конкретного торгового центра. В результате, розничная торговая компания может направлять свой контент сразу в несколько торговых центров. Например, такой торговец, как Apple, может разместить видеоконтент для рекламных роликов в облачном сервере и затем передавать команды котроллерам каждого торгового центра, задавая график показа вместе с URL-ссылкой на каждый ролик. Поскольку они имеют доступ к Интернету, отдельные экранные системы способны загрузить копию запланированного к показу ролика (возможно, через локальный кэш для повышения производительности).

Сбор данных из интернета вещей

Экраны в торговых центрах иллюстрируют еще одно важное преимущество сетевых систем – их способность передавать данные для сбора. Хотя клиенты это не всегда замечают, но размещенные в торговых центрах экраны оснащены камерами. При приближении человека к экрану система использует камеру для обнаружения его присутствия. Система идентифицирует человеческие лица и применяет алгоритмы анализа, которые используют такие особенности, как расстояние между глазами, для того, чтобы охарактеризовать человека. Программное обеспечение такого экрана способно с высокой точностью определить, является ли стоящий перед камерой человек мужчиной или женщиной, а также приблизительно оценить возрастную группу человека. Таким образом, вместо того, чтобы просто следовать предопределенному графику показа рекламных роликов, система может использовать эти характеристики человека для выбора соответствующей рекламы. Например, мужчине среднего возраста можно показать рекламу спортивного автомобиля вместо рекламы женской одежды.

В дополнение к использованию видеоинформации для выбора рекламных роликов системы торговых центров также собирают и передают данные о взаимодействии. Например, система предоставляет статистику о том, сколько людей наблюдали определенную рекламу, их пол и возраст, а также сколько времени каждый человек или группа людей оставались перед экраном при показе определенного набора рекламных роликов. Продуктовые магазины используют точно такой же подход: они устанавливают камеры со встроенными средствами обработки данных над холодильниками и в других местах магазина. Эти камеры записывают, останавливались ли клиенты у данного прилавка с продуктами, сколько времени каждый покупатель смотрел на прилавок и сколько клиентов, в конечном счете, выбрали продукт или просто двинулись дальше. После передачи данных на сервер информация с конкретного места может быть объединена с данными из других точек. Ключевая идея заключается в том, что объединение данных из нескольких мест обеспечивает повышение точности анализа.

Беспроводная сетевая коммуникация и IEEE 802.15.4

Каким образом следует подключать устройства к Интернету? Беспроводные сетевые технологии являются популярным выбором даже в случае полупостоянных развертываний в рамках небольшой области. Рассмотрим для примера электронные экраны в торговых центрах. Хотя они являются полупостоянными (т.е. экраны размещаются стационарно на несколько недель), беспроводная сеть означает, что экран можно перемещать без создания нового сетевого соединения.

Какие беспроводные сетевые технологии следует использовать для подключения интеллектуальной встроенной системы? Ответ зависит от нескольких факторов, включая физическое расстояние между узлами сети, необходимые скорости передачи данных и требования к электропитанию. Электропитание влияет двумя способами. В случае встроенных сенсорных систем, которые работают от батарей, общее энергопотребление должно быть сведено к минимуму с целью максимального увеличения времени работы батарей. Хотя мощность, потребляемая радиопередатчиком, занимает львиную долю в расходе энергии батареи, использование меньшего объема памяти или снижение частоты процессора может также понизить требования к общей мощности. В случае встроенных систем, которые обладают постоянным источником электропитания (например, подключены к сетевой розетке), может возникнуть необходимость в ограничении передачи радиосигналов с тем, чтобы избежать помех, связанных с работой других устройств или передачей иных радиосигналов.

В настоящее время стандартизированы несколько беспроводных сетевых технологий с низким энергопотреблением. Данная статья рассматривает сетевую технологию, определенную стандартом IEEE 802.15.4[1]. Существуют различные версии 802.15.4; они отличаются между собой по используемым частотным диапазонам и методам модуляции, а также по максимальному передаваемому размеру данных (MTU, Maximum Transmission Unit). Стандарт IEEE определяет физический уровень сети и уровень управления доступом к среде передачи (MAC, MediaAccess Control), при этом другие группы определили протоколы верхнего уровня для использования в беспроводных сетях с низким энергопотреблением. Для целей настоящей статьи необходимо знать только общие характеристики технологии 802.15.4:

- относительно низкая скорость передачи данных (максимум 250 кбит/с);
- чрезвычайно малый размер MTU (127 октетов);
- ограниченное расстояние (максимум 10

метров с обычной антенной и питанием от батареи).

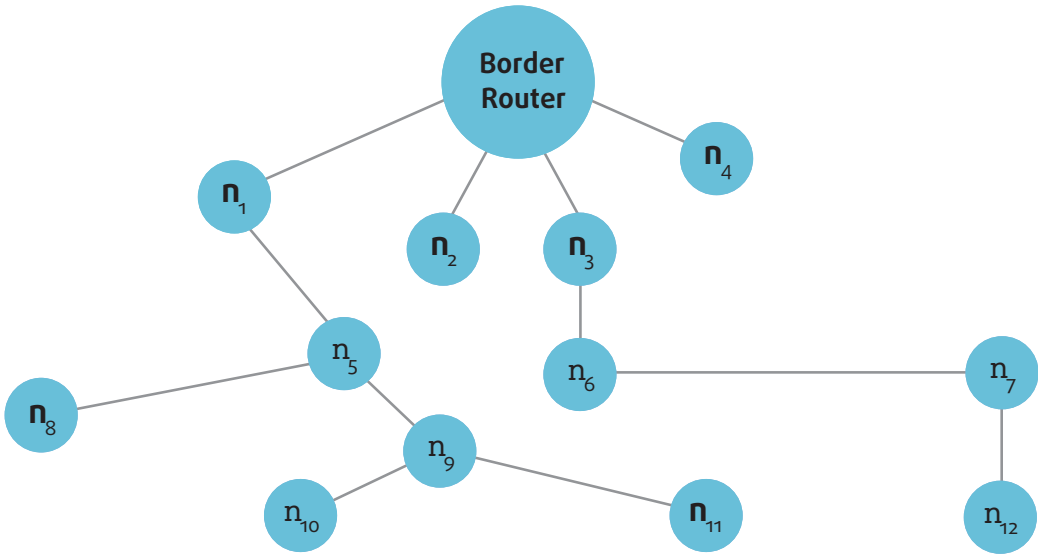
Многосвязная сеть (mesh network) для датчиков интеллектуальной энергосистемы

Одна из областей применения беспроводной технологии 802.15.4 является результатом инициативы по внедрению интеллектуального компьютерного управления в системы распределения электроэнергии. Известный под названием «интеллектуальная сеть электроснабжения» (Smart Grid), подход включает размещение датчиков во всех устройствах, использующих электроэнергию. В дополнение к крупным системам, используемым для отопления и охлаждения, конструкторы предусмотрели установку датчиков в кухонных бытовых приборах (например, электропечи, холодильники, посудомоечные машины и даже тостеры), компьютерных и развлекательных системах (например, телевизоры и стереосистемы), в небольших портативных приборах. Компании, предоставляющие коммунальные услуги, хотят взимать более высокую плату в часы пиковых нагрузок, и датчики будут обмениваться данными с такой компанией с целью определения ценовых условий и предупреждения пользователей о времени дня, когда взимается более высокая плата. Как альтернативный вариант, датчики будут способны заблокировать определенные варианты использования в течение пиковых часов.

Наиболее очевидная конструкция системы датчиков для жилища включает размещение базовой станции в жилом помещении и использование беспроводной технологии, позволяющей базовой станции обмениваться данными с каждым датчиком. Этот подход известен как «звездообразная» топология. Например, системы Wi-Fi (802.11) используют звездообразную топологию. Однако такой подход недостаточно хорошо работает во всех ситуациях. В частности, металлические трубы и другие находящиеся внутри здания препятствия могут помешать распространению беспроводных сигналов и сделать невозможным охват всего жилища из одной точки, особенно в случае портативных приборов, которые могут быть перемещены из одной комнаты в другую. Поэтому разработчики интеллектуальных электросетей предусмотрели адаптивную систему, в рамках которой набор сенсорных узлов автоматически формирует самоорганизованную многосвязную сеть или просто меш. Каждый узел такой сети выполняет две задачи: обмен данными для устройства, к которому он прикреплен, и переадресация для других узлов.

В жилище будет установлен граничный маршрутизатор, который соединит между собой многосвязную сеть и внешний мир. При инициализации узла он присоединяется к мешу и пытается установить соединение с граничным маршрутизатором. Если узел может напрямую «дотянуться» до граничного маршрутизатора, то он обменивается данными непосредственно с граничным маршрутизатором. Если узел не может напрямую «дотянуться» до граничного маршрутизатора, то он ищет ближайший соседний узел, имеющий путь к граничному маршрутизатору. По сути, соседний узел соглашается действовать в качестве маршрутизатора и перенаправлять пакеты. Если путь к граничному маршрутизатору существует у нескольких соседних узлов, то первоначальный узел выбирает один из них с помощью алгоритма выбора. Алгоритм выбора может принимать во внимание несколько показателей, включая качество радиосигнала (т.е. уровень помех), задержку, пропускную способность узла и пропускную способность промежуточных узлов. После того, как узел выберет путь до граничного маршрутизатора, он информирует соседние узлы и соглашается передавать их пакеты. Таким образом, если существует возможность создать сеть, которая обеспечивает связность для каждого узла, то узлы автоматически сформируют такую многосвязную сеть. Позднее в данной статье мы вернемся к вопросу о том, каким образом соседний узел делает свой выбор.

Рис. 1. Пример дерева переадресации, накладываемого на набор сенсорных узлов. Дерево будет образовано в том случае, если каждый узел - один путь до граничного маршрутизатора.



Дерево переадресации для многосвязной сети

Данное выше описание превращает выбор пути в меше в нечто тривиальное. На самом деле, меш может предлагать большое количество возможных путей. Различие между маршрутизацией (выбор пути среди сетей) и переадресацией (выбор пути внутри сети) довольно расплывчато, поскольку каждое радиосоединение можно представить в виде сети. Что более важно, путь с наименьшим количеством хопов (промежуточных сегментов) может оказаться неоптимальным, поскольку связность между узлами является попарной, и низкая мощность сигнала между конкретной парой узлов может сделать этот путь ненадежным. Более того, если узлы меша являются мобильными (портативными), либо если среда затрудняет прохождение сигнала (например, люди движутся через комнату), то переадресация должна динамически изменяться. Несмотря на потенциальную сложность маршрутизации в

меше, уже созданы решения, способные справиться с базовыми случаями. В частности, были созданы протоколы, обрабатывающие переадресацию между граничным маршрутизатором и отдельными узлами в топологии полустатического меша.

Ключевая идея, которая позволяет упростить переадресацию в меше, заключается в следующем наблюдении: если главной целью является установление коммуникации датчиков с удаленным сервером, то каждому сенсорному узлу требуется выбрать только один способ для соединения с граничным маршрутизатором. Трафик от удаленного сервера до узла меша может передаваться по тому же пути, но в обратном направлении. Иными словами, пути переадресации в сети формируют дерево в графо-теоретическом смысле (т.е. граф без циклов), при этом граничный маршрутизатор является корнем такого дерева. Рис. 1 показывает набор сенсорных узлов и одно возможное дерево переадресации.

Как показывает приведенный выше рисунок, граничный маршрутизатор обычно крупнее других узлов сети (т.е. имеет больший объем памяти и вычислительную мощность). Позже мы увидим, что граничный маршрутизатор выполняет функции маршрутизации и также предоставляет услуги переадресации для всего меша.

Использование интернет-протоколов в меше

С точки зрения интернет-протоколов вопрос стоит следующим образом: использовать традиционную парадигму присвоения IP-префикса всему мешу либо использовать парадигму, которая предполагает обращение с каждым радиосоединением как с отдельной сетью с двухточечным соединением.

Эти два подхода известны под следующими названиями:

- Mesh-under: меш действует как единая сеть, протоколы уровня 2 управляют широковещательной и групповой адресацией;
- Route-over: меш действует как набор двухточечных соединений, протоколы уровня 3 управляют всей переадресацией.

В рамках подхода mesh-under, в пользу которого склоняется IEEE, узел использует протоколы уровня 2 для формирования дерева переадресации. Идея аналогична мосту и протоколам связующих деревьев, используемых в Ethernet. Например, узел использует широковещательную адресацию уровня 2 для того, чтобы обнаружить, какие соседние узлы находятся в пределах досягаемости радиосвязи. Каждый соседний узел отвечает, позволяя паре узлов узнать, что они находятся в пределах досягаемости, а также определить качество сигнала. Граничный маршрутизатор также использует широковещательную трансляцию уровня 2 для объявления о себе. Узлы меша передают друг другу информацию о том, какие узлы находятся в пределах их досягаемости. В конечном счете каждому узлу меша станет известно о других узлах и о том, как до них добраться, а также каким образом переадресовывать широковещательные пакеты. Таким образом, задавшись адресом уровня 2 граничного маршрутизатора, узлы меша узнают, куда следует направлять пакеты (т.е. они сформируют дерево переадресации).

В рамках подхода route-over, в пользу которого склоняется IETF (Internet Engineering Task Force), узел использует протоколы уровня 3 для идентификации соседних узлов и формирования дерева переадресации. Конечно, базовое аппаратное обеспечение не понимает IP-адресов или формата IP-датаграмм. Таким образом, пакеты уровня 3 переносятся внутри фреймов (кадров) уровня 2. Например, для того, чтобы найти соседние узлы, программное обеспечение уровня 3 генерирует датаграмму IPv4 с локальным широковещательным адресом (broadcast address) или датаграмму IPv6 с локальным для соединения групповым адресом (link-local multicast address). Такая датаграмма отправляется посредством аппаратного широковещания.

В рамках любого из этих подходов при вводе в меш нового узла он должен выбрать, каким образом подключить себя к дереву. Используются два шага. На первом шаге узел должен обнаружить набор соседних узлов, которые находятся в пределах его прямой досягаемости, и оценить качество радиосоединения с каждым соседним узлом. На втором этапе узел должен выбрать, будет ли он осуществлять коммуникацию с граничным маршрутизатором напрямую, либо он будет использовать один из соседних узлов при переадресации пакетов. Обратите внимание, что качество сигнала имеет важнейшее значение – даже если узел способен напрямую «дотянуться» до граничного маршрутизатора, он может выбрать непрямой путь, если качество сигнала при прямом соединении достаточно низкое.

В контексте стека IP-протоколов основное различие между подходами mesh-under и route-over проявляется в IP-пересылке (IP forwarding). Подход mesh-under следует традиционной парадигме, обращаясь со всем мешем как с отдельной сетью со знакомыми характеристиками единого широковещательного домена и способностью произвольной пары узлов осуществлять коммуникацию.

IP присваивает единый префикс всему мешу, и любая датаграмма, адресованная узлу сети, будет сначала передана базовому аппаратному интерфейсу для осуществления доставки. После принятия исходящей датаграммы от IP-уровня сетевой интерфейс использует информацию, собранную протоколами маршрутизации уровня 2, для выбора следующего хопа (промежуточного сегмента), в который будет направлена датаграмма. По мере того, как пакет перемещается по мешу, в каждом промежуточном узле он обрабатывается только средствами уровня 2. После прибытия в пункт назначения датаграмма передается на уровень 3. Таким образом, вся детальная информация меша остается скрытой от уровня 3.

Подход route-over требует знания топологии меша на уровне IP. Другими словами, IP известно, что некоторых узлов сети можно достичь напрямую, а других нет. В частности, использование подхода route-over нарушает стандартное допущение IP-протоколов о том, что если два хоста коллективно используют один IP-префикс, то они подключены к сети, которая позволяет им напрямую обмениваться пакетами. В рамках меша route-over все узлы меша коллективно используют один префикс, несмотря на то, что конкретный узел способен напрямую обмениваться данными только с ближайшими соседями. Используя терминологию IPv6, мы говорим, что узел либо «на соединении» (on link), либо «вне соединения» (off link). Для работы с узлами, до которых нельзя добраться напрямую, IP использует маршрутизацию по источнику (source routing). IP должен понимать топологию меша и быть способен задать путь через меш до пункта назначения (например, перейти к узлу 9, затем к узлу 5, затем к узлу 1 и, наконец, к граничному маршрутизатору). Приведенные ниже разделы описывают

стек протоколов ZigBee, который использует подход route-over, а следующие за ними разделы анализируют некоторые возникающие проблемы.

Стек протоколов IPv6 для ZigBee

Альянс ZigBee[2] и IETF[3] сотрудничают между собой с тем, чтобы определить методы использования IPv6 в многосвязных топологиях, реализующих подход route-over. Альянс ZigBee определил открытый стандарт, известный под названием ZigBee IP[4]. В таблице 1 перечислены три ключевые рабочие группы IETF, связанные с инициативой ZigBee. Последующие разделы описывают разрабатываемые протоколы.

Таблица 1 Рабочие группы IETF, связанные с инициативой ZigBee Effort

Название	Основной вклад
6LoWPAN	IP-over-802.15.4 Shim Layer
ROLL RPL	протокол маршрутизации для многосвязных сетей
CoRE CoAP	CoRE CoAP

Основная идея конфигурации route-over для ZigBee заключается в использовании IPv6 во всех возможных случаях и во внесении изменений по мере необходимости. Для сжатия датаграмм IPv6 и отправки их по радиоканалу 802.15.4 был создан специальный протокол. Для обнаружения соседних узлов, находящихся в пределах прямой досягаемости, используется модифицированная форма технологии IPv6 Neighbor Discovery (Обнаружение соседей). Кроме того, особый протокол был разработан для обмена характеристиками между соседними узлами.

В дополнение к этому для сбора информации о возможности соединения (связности) в рамках всего меша и расчета данных пересылки используется новый протокол маршрутизации. И наконец, заголовок исходного маршрута IPv6 используется для «похоповой» (посегментной) пересылки каждой датаграммы через весь меш. Следующие разделы содержат описание некоторых базовых протоколов.

Протокол IPv6 over Low-Power Wireless Networks

Протокол IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) определяет транспортировку IPv6 через радиоканал 802.15.4. Главная проблема заключается в конфликте между требованием IPv6 к длине MTU – не менее 1280 октетов[5] - и особенностями протокола 802.15.4, который требует, чтобы максимальная длина не превышала 127 октетов. Фактически, если используется шифрование AES-CCM-128, то доступная полезная нагрузка снижается до 81 октета. Для того, чтобы отправить датаграмму IPv6 через такой канал, протокол 6LoWPAN вводит дополнительный «промежуточный» уровень, который осуществляет сжатие и передачу данных. Промежуточный уровень принимает исходящую датаграмму IPv6, сжимает заголовок, разделяет датаграмму на ряд сегментов, называемых «фраглетами» (fraglet), и отправляет каждый фраглет внутри отдельного пакета. На приеме промежуточный уровень 6LoWPAN принимает входящие фраглеты, объединяет и восстанавливает их в единую датаграмму, распаковывает заголовок и передает результат уровню IP. Это значит, что IPv6 конфигурируется таким образом, чтобы отправлять и получать законченные датаграммы, не зная о том, что промежуточный уровень разбивает датаграмму на фраглеты для последующей передачи. Существуют две причины, по которым 6LoWPAN не использует обычную фрагментацию IPv6. Первая причина: протокол 6LoWPAN работает только через единичный канал. В результате этот протокол гораздо проще, поскольку все фраглеты датаграммы должны прибывать в определенном порядке. Вторая причина: фрагментация IPv6 не способна обрабатывать MTU, состоящие из 127 октетов.

Протокол 6LoWPAN Neighbor Discovery

Традиционный протокол IPv6 Neighbor Discovery (IPv6-ND) предоставляет механизм определения адресов, который можно использовать, помимо прочего, для обнаружения дублирования адреса (DAD, Duplicate Address Detection). К сожалению, IPv6-ND содержит фундаментальное допущение о том, что префикс IPv6 устанавливает соответствие с широковещательным доменом. Поэтому узел может использовать широковещание IPv6, преобразуемое в аппаратное широковещание, для охвата всех узлов, которые имеют один и тот же префикс. Однако в рамках многосвязной топологии широковещательная передача может достигнуть только некоторых узлов меша, оставляя часть узлов вне соединения. В результате обычная функция DAD будет работать неправильно.

Протокол 6LoWPAN Neighbor Discovery (6LoWPAN-ND) вносит в IPv6-ND несколько изменений и оптимизаций, которые специально предназначены для маломощных беспроводных сетей с потерями, имеющих ограниченный диапазон. В общем случае 6LoWPAN-ND исключает все механизмы, которые «наводняют» меш пакетами. Вместо того, чтобы требовать от отдельных узлов участия в DAD, 6LoWPAN-ND использует регистрационный подход, в рамках которого каждый узел меша регистрирует свой адрес на граничном маршрутизаторе.

По мере того, как узлы регистрируют свои адреса, программное обеспечение, работающее на граничном маршрутизаторе, помечает все адрес-дубликаты (напоминаем, что граничный маршрутизатор располагает вычислительной мощностью и памятью, которые необходимы для работы с такими общесетевыми сервисами, как регистрация адресов). И наконец, 6LoWPAN-ND позволяет узлам спать (т.е. переходить в состояние покоя для экономии энергии). После пробуждения такой узел должен возобновить регистрацию своего адреса на случай, если некий другой узел зарегистрировал адрес-дубликат в течение его сна.

Протокол MLE (Mesh Link Establishment)

При разработке IPv6 было принято допущение о том, что базовые аппаратные соединения сконфигурированы до выполнения программного обеспечения IP. В частности, IPv6 ожидает, что обмен данными был аутентифицирован, т.е. соединения уже должны существовать. Для меша 802.15.4 узел должен выбрать, каким образом следует подключиться к дереву пересылки. Конфигурирование соединений является довольно сложным делом, поскольку передача радиосигналов может быть асимметричной. Узел не может просто «прослушать» передаваемые соседями сигналы и выбрать из них узел с самым сильным сигналом, поскольку возникает вопрос о том, насколько хорошо его сигнал принимается этим соседним узлом. Давайте рассмотрим случай граничного маршрутизатора, обладающего мощным передатчиком и большой антенной. Возможна ситуация, когда узел получает сильный сигнал от граничного маршрутизатора, даже если его передатчик слишком слаб, чтобы «дотянуться» до граничного марш-

рутизатора. Таким образом, перед тем, как использовать IPv6 в меше route-over, необходимо добавить низкоуровневый протокол, который позволит узлу узнать уровень сигналов, наблюдаемых соседями при получении данных от этого узла.

ZigBee использует протокол Mesh Link Establishment (MLE) для конфигурирования соединений. MLE прибегает к помощи двустороннего обмена пакетами: один узел передает сообщение, а принимающий узел отправляет ответ. В ответе содержится информация о наблюдаемом качестве сигнала. После получения узлом MLE-ответа от каждого соседнего узла этот узел будет знать о том, насколько хорошо каждый из его соседей может принимать передаваемые данные. Конечно, сила сигнала может меняться по прошествии времени, если происходит перемещение узлов или появляются электрические помехи (например, начинает работать мощный электродвигатель). Поэтому такие измерения необходимо периодически повторять.

MLE включает не только средства, которые оценивают силу сигнала. В ходе передачи пакета MLE позволяет узлам обмениваться конфигурационной информацией. Два узла обмениваются адресной информацией и выбирают тип защиты для своего соединения. Самое важное, MLE позволяет узлу информировать соседа о том, что он может «дотянуться» до граничного маршрутизатора. Таким образом, после присоединения к мешу новый узел запускает MLE, собирает информацию о том, какие из его соседей имеют путь до граничного маршрутизатора, и использует силу сигнала для выбора одного из таких соседей в качестве родительского узла в дереве пересылки.

Интересно отметить, что не все протоколы ZigBee учитывают асимметричную силу сигнала. В частности, при построении дерева пересылки протокол RPL (Routing Protocol for Low-Power and Lossy Networks) выбирает соединения, которые являются двунаправленными; если коммуникация может осуществляться только от узла А к узлу Б, то RPL не включает такое соединение.

Однако способность осуществлять обмен данными не означает, что его качество одинаково в обоих направлениях. В случае граничного маршрутизатора, обменивающегося данными с другим узлом, кажется разумным допустить, что сигнал, отправленный граничным маршрутизатором, может быть сильнее, чем сигнал, отправленный узлом. Даже в случае двух узлов, ни один из которых не является граничным маршрутизатором, возможна ситуация, когда сигнал, полученный в одном направлении, гораздо сильнее, чем сигнал, полученный в обратном направлении. Несмотря на это, после завершения выбора пути RPL отправляет по нему трафик в обоих направлениях.

Пересылка данных в меше ZigBee Route-Over

Обычная IP-пересылка использует префикс IP при выборе следующего хопа. Однако, как это уже указывалось ранее, некоторые узлы сети будут «на соединении» (т.е. их можно достичь напрямую), а остальные «вне соединения» (т.е. их можно достичь только опосредованно). Поэтому при решении вопроса о том, каким образом переслать датаграмму, IP должен иметь в своем распоряжении больше информации, чем только префикс сети. Проблема может быть решена двумя способами, и ZigBee IP использует термины «режим с хранением» (storing mode) и «режим без хранения» (non-storing mode) для того, чтобы охарактеризовать эти два подхода.

Как это подразумевает термин «режим с хранением», каждый узел сети хранит значительный объем информации. В дополнение к хранению адреса родительского узла (т.е. адреса следующего хопа по направлению к граничному маршрутизатору) каждый узел узнает и сохраняет адрес следующего хопа для каждого узла, расположенного «ниже по течению». В терминах теории графов это значит, что узел дерева хранит следующий хоп для каждого узла в своем поддереве. Наихудший сценарий возможен в сети, в которой единственный узел N соединяет все другие узлы с граничным маршрутизатором. В таком случае узел N хранит следующий хоп для всех остальных узлов сети.

Если возникает необходимость в отправке датаграммы, то работающее на узле программное обеспечение IP запрашивает информацию о пересылке, которая хранится локально (на том же узле). Если место назначения расположено в нисходящем направлении, то эта информация указывает следующий хоп, который нужно использовать. Если место назначения не расположено в нисходящем направлении, то узел направляет датаграмму вдоль пути, ведущего к граничному маршрутизатору.

Требования к памяти для режима с хранением превышают те, которые подразумевает предыдущее описание. После того, как RPL рассчитает маршруты, узел должен хранить в памяти только следующий хоп для мест назначения, расположенных в его поддереве (в худшем случае N – 1 пунктов назначения). Однако в ходе расчета маршрутов необходима дополнительная память, RPL использует алгоритм маршрутизации с учётом состояния каналов. Поэтому узел должен собрать попарные анонсы соединений для всех каналов поддерева, а затем запустить и выполнить алгоритм поиска кратчайшего пути для расчета следующих хопов. Требуемый объем памяти по-прежнему пропорционален количеству узлов в поддереве, однако расчет может потребовать вдвое больше памяти, чем необходимо для хранения информации о следующих хопах.

Хотя режим с хранением и решает задачу по передаче данных вдоль границ дерева пересылки, он не обеспечивает оптимальную маршрутизацию во всех случаях. Рассмотрим для примера два узла, которые расположены близко друг от друга, но не на одном и том же поддереве пересылки.

Если один из этих узлов отправляет данные другому, то пакет направляется вверх по дереву в направлении граничного маршрутизатора. Когда пакет достигнет узла, который является общим для обоих поддеревьев маршрутизации, направление его движения изменится на нисходящее вдоль по другому поддереву до пункта назначения. Худший сценарий реализуется в том случае, когда единственным общим узлом обоих поддеревьев является граничный маршрутизатор: пакет должен быть транспортирован на максимальное расстояние вверх вдоль одного из поддеревьев до граничного маршрутизатора, после чего он перемещается вниз вдоль другого поддерева до пункта назначения. IETF разрабатывает протокол, который сможет обнаруживать и использовать маршруты, расположенные вне дерева пересылки.

Концепция дерева пересылки и протокола маршрутизации, такого как RPL, который рассчитывает и обслуживает дерево, обусловлена тремя допущениями: топология остается относительно статичной, узлы часто обмениваются данными между собой и задержка при коммуникации должна быть минимизирована. Благодаря предварительному расчету дерева пересылки узлы меша готовы к перенаправлению любого пакета в любое время. В ситуациях, когда топология меняется либо трафик становится редким (например, сенсорный меш, в котором показания датчиков собираются раз в неде-

лю), накладные расходы на поддержание маршрутов могут быть неоправданными. Вместо этого более эффективным способом может оказаться использование подхода «по запросу», в рамках которого узлы меша ждут получения пакета, осуществляют поиск маршрута, отправляют пакет и затем удаляют маршрут.

Режим без хранения предназначен для сетей, в которых узлы имеют ограниченный объем памяти и процессорных ресурсов. Для того, чтобы минимизировать локальное хранение и обработку данных, каждый узел должен знать только две вещи: набор соседних узлов в пределах его прямой досягаемости и идентификатор того соседнего узла, который ведет к граничному маршрутизатору. Предполагается, что граничный маршрутизатор располагает существенными объемами памяти и большой процессорной мощностью, которые позволяют ему выполнять все необходимые расчеты пути. Граничный маршрутизатор знает полную топологию меша и обрабатывает всю маршрутизацию по источнику. Когда у узла появляется датаграмма для отправки, он направляет ее граничному маршрутизатору. Если датаграмма предназначена для сайта в Интернете, то граничный маршрутизатор перешлет ее. Если датаграмма предназначена другому узлу меша, то граничный маршрутизатор «инкапсулирует» ее во внешней датаграмме, использует копию топологической информации для вставки заголовка исходного маршрута во внешнюю датаграмму и направляет инкапсулированную датаграмму через меш. На каждом шаге узел меша находит адрес соседнего узла в заголовке исходного маршрута и использует этот адрес для отправки датаграммы указанному соседу. Пожалуй, наиболее серьезное последствие использования IPv6 для реализации меша route-over проистекает из требования к маршрутизации по источнику для режима без хранения и требования к размеру заголовка исходного маршрута IPv6.

Может показаться, что режим без хранения напрасно растрачивает сетевые ресурсы, поскольку датаграмма, отправленная от одного узла другому, приходит сначала в граничный маршрутизатор и только затем в пункт назначения. Наихудший сценарий реализуется в том случае, когда пакет отправляется между парой узлов, которые находятся на расстоянии двух хопов, но деревья пересылки которых пересекаются только в граничном маршрутизаторе – вместо двух хопов пакет может быть транспортирован через N хопов, где N – количество узлов.

Несмотря на это, Альянс ZigBee выбрал режим без хранения с тем, чтобы позволить отдельным узлам иметь чрезвычайно малый объем памяти и низкую частоту процессора, сводя к минимуму как издержки, так и энергопотребление.

Важное соображение относительно режима с хранением является результатом ограничений на масштабирование: в наихудшем случае для хранения информации о связности меша требуется объем памяти пропорциональный N – количеству узлов в сети. Хотя большинство многосвязных сетей ZigBee имеют меньше 24 узлов, некоторые такие сети содержат тысячи узлов. Следовательно, режим с хранением для крупного меша означает, что каждый узел должен хранить таблицы, которые довольно велики по сравнению с объемом памяти, доступным в небольших устройствах (например, 64 или 128 килобайт ОЗУ). Использование режима без хранения позволяет узлам, работающим от небольшой батареи, хранить в памяти лишь следующую информацию:

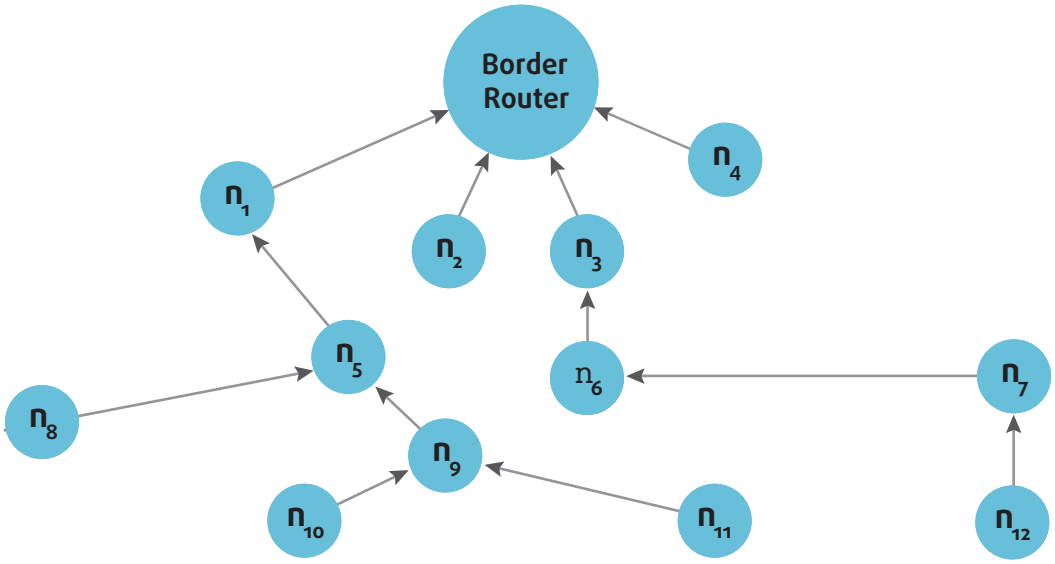
- список соседних узлов в пределах прямой досягаемости и MAC-адрес каждого из таких узлов;
- идентификатор соседнего узла, который в настоящее время служит в качестве пути к граничному маршрутизатору.

Следует отметить, что объем памяти, требуемый для использования режима без хранения, пропорционален количеству соседних узлов, находящихся в пределах прямой досягаемости, и это число обычно значительно меньше, чем количество узлов меша. Фактически, даже находясь в плотном меше, узел может ограничить этот список верхними K узлами (т.е. K соседей, которые сообщили о самом сильном сигнале).

Протокол RPL

В IETF был разработан протокол маршрутизации, который может использоваться вместе с IPv6 в многосвязных сетях route-over. Этот протокол, известный под именем Routing Protocol for Low-Power and Lossy Networks (RPL), позволяет узлам объявлять прямые соединения и узнавать о других соединениях в меше. RPL определяет заголовок IPv6, позволяя датаграмме переносить информацию RPL в дополнение к полезной нагрузке. Стандарт ZigBee IP определяет использование режима без хранения. В рамках режима без хранения RPL распространяет информацию о соединениях вверх до граничного маршрутизатора. На граничном маршрутизаторе выполняется специальная версия программного обеспечения RPL, которая собирает информацию, т.е. оно строит топологию всего меша.

Рис. 2. Граф DODAG, определенный протоколом RPL для дерева на рис. 1.



После построения топологии граничный маршрутизатор вычисляет дерево пересылки. Вме-

сто наложения дерева на ненаправленный граф, RPL делает каждое соединение направленным – в сторону корня (т.е. в сторону граничного маршрутизатора). Граф топологии меша, создаваемый RPL, называется DODAG (Destination-Oriented Directed Acyclic Graph). Рис. 2 показывает DODAG в форме дерева, представленного на рис. 1.

Хотя соединения в DODAG направлены в сторону корня, такое представление является лишь особенностью протокола, оно не навязывает направление потока пакетов. В частности, в тех случаях, когда граничному маршрутизатору требуется отправить датаграмму одному из узлов, он использует DODAG в обратном направлении, создав заголовок исходного маршрута, в котором узлы перечислены вниз по дереву (т.е. в обратном порядке относительно стрелок на рисунке).

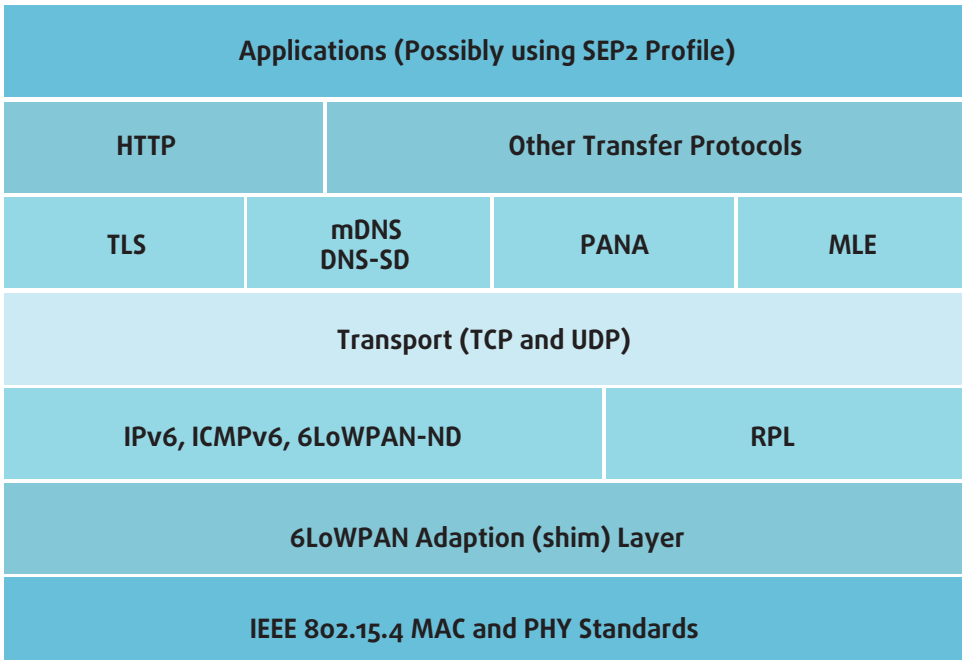
RPL разделяет узлы дерева на три типа: корень (граничный маршрутизатор действует в качестве корня DODAG), лист (т.е. узел, который имеет только одно соединение) и промежуточный узел (узел, который имеет не менее двух соединений, и который пересылает датаграммы). Поскольку промежуточные узлы перенаправляют пакеты, стандарт ZigBee IP использует термин «маршрутизатор ZigBee IP» или более коротко «маршрутизатор ZIP». Узлы-листья не выполняют протокол RPL. Вместо этого каждый узел-лист подключен к маршрутизатору ZIP, который выполняет все его функции по пересылке. Т.е. маршрутизатор ZIP информирует граничный маршрутизатор о каждом узле-листе, с которым он соединен.

Протокол RPL устроен гораздо сложнее, чем это здесь описывается. Например, RPL можно использовать вместе с режимом «с хранением»; сообщения должны задавать используемый режим. Кроме того, RPL способен распространять информацию вниз по дереву. Например, существует возможность использовать RPL для информирования узлов об используемых IP-префиксах.

Другие протоколы в спецификации ZigBee IP

Помимо основных протоколов, которые были определены выше, спецификация ZigBee IP включает многие другие протоколы. ZigBee IP использует IPv6, Internet Control Message Protocol Version 6 (ICMPv6), TCP, User Datagram Protocol (UDP), Protocol for carrying Authenticationfor Network Access (PANA), multicast DNS (mDNS), DNS Service Discovery (DNS-SD) и Transport Layer Security (TLS), который используется в сочетании с PANA, Extensible Authentication Protocol (EAP) и Extensible Authentication Protocol Transport Layer Security (EAP-TLS) для аутентификации. Приложения, соответствующие требованиям Smart Energy Profile 2.0[6], используют в качестве коммуникационного протокола традиционный HTTP. В качестве альтернативы группа IETF разрабатывает новый протокол, известный как Constrained Application Protocol (CoAP)[7], который предназначен для ограниченных сетей, включая меш 802.15.4. На рис. 3 представлены основные протоколы.

Рис. 3. Поуровневое представление основных протоколов, используемых в многосвязных сетях ZigBee.



Анализ использования IPv6 Route-Over для меша

Существует много вопросов относительно использования IPv6 и подхода route-over в меше, состоящем из энергосберегающих, беспроводных сенсорных узлов. Какой подход лучше - route-over или mesh-under? Как много дополнительных протокольных накладных расходов требуется для route-over? Будет ли реализация route-over требовать больше памяти, чем mesh-under? Если да, то насколько? Имеет ли смысл использовать IPv6 в многосвязной сети, которая имеет очень малый размер MTU и чрезвычайно медленные соединения? Если RPL использует режим без хранения, то каковы накладные расходы в контексте дополнительной пересылки пакетов? Насколько необходимо изменить IPv6 и протоколы поддержки IPv6 для того, чтобы они работали в многосвязной топологии?

Как отмечалось выше, стандарт IPv6 определяет, что протокол IPv6 нельзя использовать в сети с размером MTU меньше, чем 1280. Таким образом, 6LoWPAN добавляет промежуточный уровень, который делит датаграмму на фраглеты для последующей передачи. Транспортировка фраглетов имеет преимущество по сравнению с обычной фрагментацией: все фраглеты должны прибывать последовательно и в определенном порядке. Т.е. после того, как первый фраглет достигнет получателя, последующие фреймы (кадры), поступающие от отправителя, должны содержать остальные фраглеты – без присутствия фраглетов из других датаграмм. Таким образом, если входящий фрейм не содержит ожидаемого фраглета, то получатель отбрасывает всю датаграмму. Преимущество фраглетов по сравнению с традиционной фрагментацией заключается в пониженном использовании памяти: получателю не требуется хранить буферы для набора частичных датаграмм.

Главный недостаток фраглетов является результатом комбинации трех факторов: большой размер датаграммы, чрезвычайно малый размер MTU и более высокая вероятность потери. Особенно большим размером отличаются датаграммы, отправляемые из граничного маршрутизатора в адрес отдельного узла меша, поскольку дополнительный уровень инкапсуляции приводит

к добавлению базового заголовка IPv6 и заголовка исходного маршрута.

В результате датаграмма минимального размера (1280 октетов) будет разделена на 11 фраглетов. Если вероятность потери конкретного пакета равна p ($0 < p \leq 1$), то вероятность потери всей датаграммы гораздо выше, чем p. Хотя спецификация 6LoWPAN распознает поведение с потерями, активное использование транспортировки фраглетов увеличивает повторную передачу данных (и задержку).

Еще одна проблема, связанная с MTU, возникает из-за того, что граничный маршрутизатор должен выбрать MTU для датаграмм, поступающих извне меша. Стандарт IPv6 определяет MTU для соединения равным 1280 октетов. Если граничный маршрутизатор принудительно использует MTU размером 1280 октетов для внешних соединений, то прибывающая извне датаграмма должна быть дополнительно инкапсулирована перед ее последующей передачей в меш. К сожалению, дополнительный заголовок увеличивает размер датаграммы до $1280 + \delta$, что делает ее размер больше, чем 1280 октетов MTU протокола 6LoWPAN. Одно из решений определяет размер MTU протокола 6LoWPAN как $1280 + \delta$, но требует от граничного маршрутизатора принудительного ограничения на размер MTU (1280 октетов) для внешних источников. К сожалению, введение такого специального ограничения в код IPv6 ведет к снижению универсальности протокола – применение нестандартных методов для работы с мешем делает стек протоколов неустойчивым. Например, если кто-нибудь изобретет новый механизм обнаружения MTU для пути, то этот новый механизм нельзя интегрировать в граничный маршрутизатор до тех пор, пока он не будет адаптирован в соответствии со специальными правилами MTU.

Разработчикам было понятно, что обычные протоколы IPv6 нельзя использовать для конфигурирования радиоканала либо для двусторонней оценки сигнала. Поэтому они создали протокол MLE. Кроме того, им пришлось заменить протокол IPv6 Neighbor Discovery, поскольку хотя узлы меша используют единый IP-префикс, они не принадлежат к единому широковещательному домену. На первый взгляд, кажется, что MLE и IPv6-ND могут быть модифицированы для совместной работы: MLE обнаруживает соседние узлы, а IPv6-ND использует информацию, полученную от MLE, для ведения списка MAC-адресов соседей. Однако IPv6-ND также решает другие задачи. Например, IPv6-ND использует сообщения ICMPv6 для распространения сетевой информации, включая сетевые префиксы. К сожалению, RPL также предоставляет способ для распространения сетевого префикса вниз (по дереву) от граничного маршрутизатора до узлов меша. Следует ли использовать IPv6-ND или RPL? Каков бы ни был выбор, один из этих двух протоколов должен быть изменен с тем, чтобы избежать «гонки», в рамках которой оба протокола пытаются одновременно распространять префиксы адресов. ZigBee IP решает эту проблему, определив, что только 6LoWPAN-ND следует использовать для распространения информации о конфигурации сети.

В статье утверждалось, что для экономии электроэнергии узлы меша ZigBee могут переходить в режим сна. Интересно отметить, что механизм обнаружения адреса может потребовать, чтобы узел потратил дополнительную энергию. Для того, чтобы увидеть, почему это происходит, необходимо знать два факта. Первое, при регистрации адреса присваивается интервал времени действия, в течение которого эта регистрация остается действительной. Второе, ради экономии энергии режим сна останавливает работу максимального количества аппаратных средств. Таким образом, возможна ситуация, когда часы (тактовый генератор) энергосберегающего узла не работают в течение цикла сна.

А теперь представьте, что произойдет при пробуждении узла. Если цикл сна был достаточно длительным, либо если часы (тактовый генератор) не работали, то узел не может знать о возможном прибытии нового узла и о возможной регистрации дублирующего IP-адреса в граничном маршрутизаторе. Таким образом, после пробуждения узел должен отправить сообщение о перерегистрации и получить ответ до того, как он сможет использовать свой адрес. В рамках обычной сети использование протоколом IPv6 адресного префикса /64 и встроенных MAC-адресов делает маловероятным дублирование адресов. Однако стандарт 802.15.4 включает 16-битовый MAC-адрес, и это означает, что узлы должны выполнять требования протокола во избежание дублирования адресов.

Другое неожиданное осложнение является результатом маршрутизации в меше. Используемые в обычных сетях протоколы маршрутизации выбирают кратчайшие пути (за исключением случаев, когда политика определяет иное). Протоколы маршрутизации меша должны иметь дело с несколькими независимыми переменными: сила радиосигнала вдоль пути, длина пути и вероятность помех. Таким образом, кратчайший путь через меш может быть неоптимальным. Что более важно, не существует простого способа оценить вероятность помех или количественно оценить обратную зависимость между длиной пути и качеством сигнала. На самом деле возможны трудности даже при расчете зависимости эффективной пропускной способности от качества сигнала. Источники электропитания могут еще больше усложнить маршрутизацию. Например, можно представить систему маршрутизации, которая предпочитает узлы, получающие питание от непрерывного источника, узлам, получающим питание от батареи. В результате того, что приходится осуществлять оптимизацию по многим параметрам и без очевидной целевой функции, протоколы маршрутизации меша могут оказаться более сложными и менее поддающимися настройке, чем обычные протоколы маршрутизации.

Частично неэффективность меша ZigBee является результатом фундаментального решения, принятого при разработке IPv6: заголовок датаграммы IPv6 нельзя изменять после того, как датаграмма окажется в пути. Для того, чтобы перемещаться по мешу, датаграмма должна включать заголовок исходного маршрута и заголовок RPL. Однако эти дополнительные заголовки имеют смысл только внутри меша и должны быть удалены после выхода из него. Если разрешить дополнительным заголовкам остаться, то датаграмма может пересечь еще один меш ZigBee, в котором его информация может быть неправильно интерпретирована, что приведет к ошибочному перенаправлению датаграммы. Аналогичным образом, если датаграмма поступает в меш извне, то к ней необходимо добавить соответствующие заголовки. В результате решений, принятых при разработке IPv6, заголовки нельзя удалять или добавлять. Поэтому единственной приемлемой опцией остается инкапсуляция: каждая датаграмма IPv6, пересылаемая через меш, должна быть инкапсулирована внутри другой датаграммы IPv6, имеющей соответствующие заголовки. Для сети с MTU большого размера инкапсуляция IP-in-IP добавляет лишь небольшой объем служебной информации. Однако для сети 802.15.4 размер аппаратного MTU составляет только 127 октетов. Таким образом, единственная пара адресов IPv6 (источник и пункт назначения) занимает более 25% объема MTU. Для сравнения, пара адресов IPv4 занимает немногим более 6% MTU. В

отличие от протокола IPv4, который разрешает вставлять опции в существующий заголовок, IPv6 требует инкапсуляции заголовка для вставки опции исходного маршрута. Такой подход требует добавления нескольких IPv6-адресов, что легко приводит к генерированию одного или нескольких дополнительных фраглетов. В результате выбор IPv6 вместо IPv4 ведет к значительному увеличению накладных расходов и делает получившуюся сеть менее эффективной.

На основе вышеприведенного обсуждения мы делаем следующий вывод:

Хотя использование парадигмы route-over и стандарта IPv6 для меша ZigBee 802.15.4 и является возможным, реализация такого подхода потребует разработки альтернативных протоколов, создания специальных исключений и значительных дополнительных расходов.

Резюме

Новая тенденция концентрирует внимание на интернете вещей, в рамках которого интеллектуальные встроенные системы, воспринимающие и контролирующие свою среду, используют IT для обмена информацией. Примеры таких встроенных систем включают датчики в автомобилях, офисах, торговых центрах и гражданской инфраструктуре.

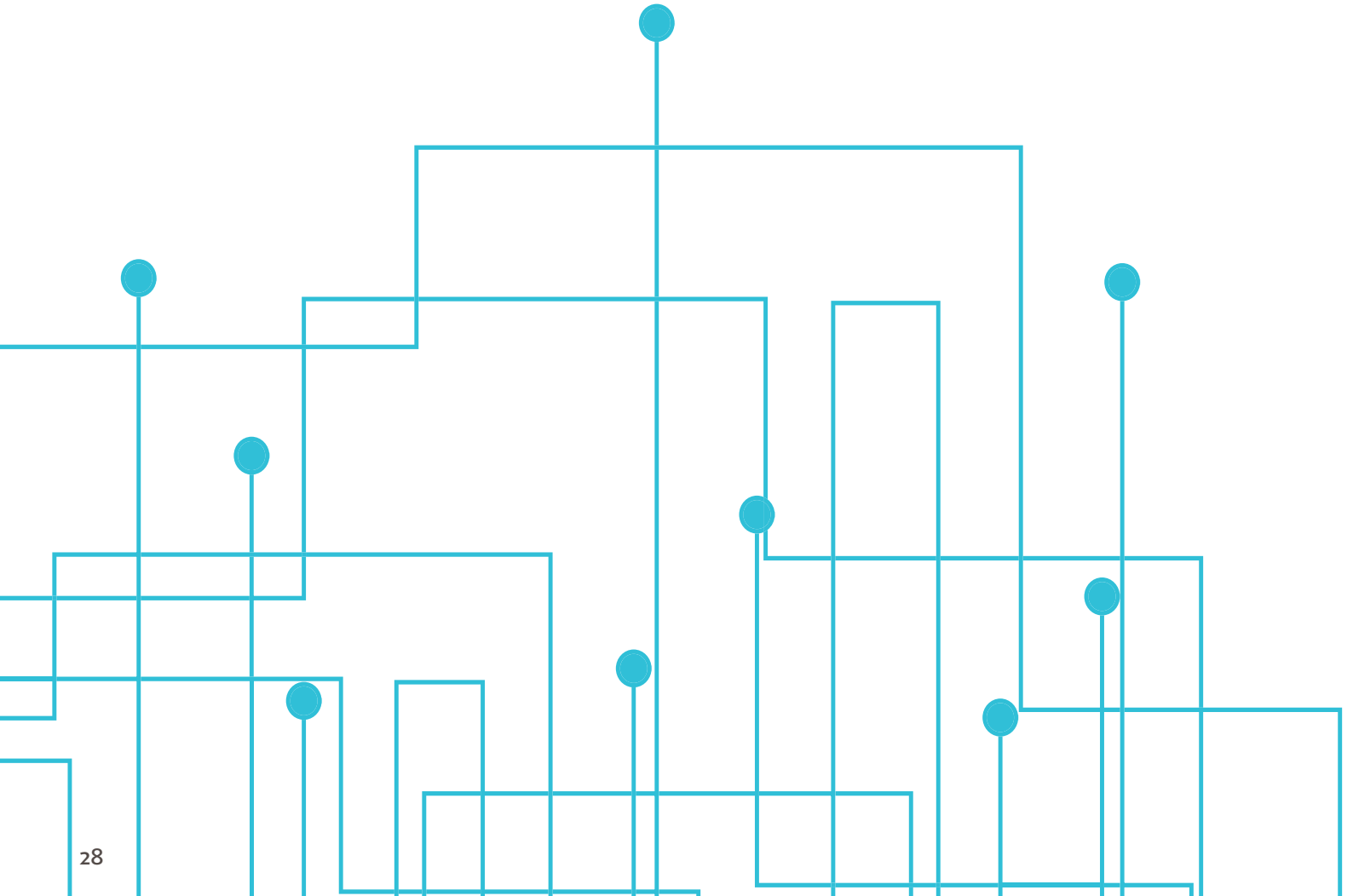
Консорциум производителей, известный как Альянс ZigBee, определяет стандарты для сетевых технологий, использующих беспроводное сетевое аппаратное обеспечение IEEE 802.15.4 для создания многосвязной сети (меша) датчиков интеллектуальной энергосистемы. Сеть ZigBee имеет в своем составе граничный маршрутизатор, который соединяет ее с внешним миром; другие узлы меша самоорганизовываются для формирования соединений и пересылки.

В контексте протоколов Альянс ZigBee работает совместно с IETF над реализацией подхода route-over, который использует IPv6. По сути дела, система route-over использует IP для любой переадресации. На практике IPv6 и стандартных протоколов поддержки IPv6 недостаточно для реализации энергосберегающей, беспроводной технологии меша с потерями, которая имеет небольшой размер MTU и низкую скорость передачи данных. Из этого следует, что работа была сконцентрирована на замене многих элементов IPv6, на добавлении промежуточного уровня, адаптирующего к небольшому размеру MTU, на разработке нового протокола, который тестирует силу сигнала и устанавливает соединения, и на построении нового протокола маршрутизации, формирующего дерево переадресации. Даже с учетом этих изменений конструктивные элементы IPv6 не очень хорошо вписываются в технологию IEEE 802.15.4.

Благодарность

Содержащиеся в настоящей статье материалы были взяты с разрешения [8].

Источник: ZigBee IP Protocol Stack, The Internet Protocol Journal Vol 17, No 2



Перечень ссылочных документов

[1] Стандарт IEEE 802.15.4 можно пробрести по адресу:

http://webstore.ansi.org/RecordDetail.aspx?sku=IEEE%20802.15.4-2011

[2] Информацию об Альянсе ZigBee можно найти на сайте:

http://www.zigbee.org/

[3] Информацию о группе IETF (Internet Engineering Task Force) можно найти на сайте: http://www.ietf.org/

[4] Информация о спецификации ZigBee IP:

http://zigbee.org/zigbee-for-developers/networkspecifications/zigbeeip/

[5] Stephen E. Deering and Robert M. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, December 1998.

[6] Полный список спецификаций ZigBee можно найти по адресу:

http://zigbee.org/zigbee-for-developers/applicationstandards/ и:

http://zigbee.org/zigbee-for-developers/networkspecifications/

[7] Спецификацию протокола CoAP (Constrained Application Protocol) можно найти по адресу:

http://datatracker.ietf.org/doc/draft-ietf-corecoap/

[8] Douglas E. Comer, Internet working with TCP/IP Volume 1: Principles, Protocols, and Architecture, sixth edition, Prentice Hall, ISBN 0-13-608530-X.

[9] David Lake, Ammar Rayes, and Monique Morrow, “The Internet of Things”, The Internet Protocol Journal, Volume 15, No. 3, September 2012.

[10] T. Sridhar, “Cloud Computing — A Primer: Part One”, The Internet Protocol Journal, Volume 12, No. 3, September 2009.

[11] T. Sridhar, “Cloud Computing — A Primer: Part Two”, The Internet Protocol Journal, Volume 12, No. 4, December 2009.

*Дуглас Коумер является заслуженным профессором компьютерных наук в университете Пердью. Ранее он работал в качестве вице-президента по исследованиям и совместным исследованиям в компании Cisco Systems. Являясь участником первоначального состава группы IAB, он участвовал в ранних разработках в области Интернета. Он получил международную известность как один из авторов протоколов TCP/IP и интернет-технологий. Дуглас Коумер написал целый ряд бестселлеров в области технической литературы, его трехтомная серия Internet working признана как авторитетная работа по интернет-технологиям. Его книги, которые были переведены на 16 языков, широко используются в отрасли и в академических кругах многих стран. Коумер консультирует отраслевые организации, его лекции прослушали тысячи профессиональных инженеров и студентов со всего мира. В течение 20 лет он был главным редактором журнала Software-Practice and Experience. Он является членом ассоциации ACM (Ассоциация по вычислительной технике США) и обладателем многочисленных наград за преподавательскую деятельность. Электронная почта: comer@cs.purdue.edu

Сети LPWAN в IETF

Александр Пелов, Паскаль Тюбо, Суреш Кришнан
(Alexander Pelov, Pascal Thubert, Suresh Krishnan)

Новый класс беспроводных технологий под общим названием «сети с низким энергопотреблением и большим покрытием» (Low-Power, Wide-Area, или LPWA) обладает рядом общих характеристик, которые идеально подходят для приложений интернета вещей (Internet of Things, IoT). Функции сетей LPWA хорошо подходят для многих приложений IoT, где не требуется передавать данные с датчиков на сколько-нибудь высокой скорости, и где невозможно обеспечить питание от электросети или частую замену батареек.

Новый класс беспроводных технологий под общим названием «сети с низким энергопотреблением и большим покрытием» (Low-Power, Wide-Area, или LPWA) обладает рядом общих характеристик, которые идеально подходят для приложений интернета вещей (Internet of Things, IoT). Эти характеристики включают оптимизацию энергопотребления радиопередачи, упрощенную сетевую топологию, пакеты размером в несколько десятков байт, передающиеся несколько раз в день с очень маленькой скоростью, и, в основном, восходящий трафик, благодаря чему устройства основную часть времени могут находиться в режиме глубокого сна с пониженным энергопотреблением. Эти характеристики позволяют вести передачу на расстоянии до нескольких километров, обеспечивают долгий срок работы от батарейки (до десяти лет работы от одной батарейки-«таблетки»), а также простое и масштабируемое развертывание с применением дешевых устройств и простых инфраструктур. Функции сетей LPWA хорошо подходят для многих приложений IoT, где не требуется передавать данные с датчиков на сколько-нибудь высокой скорости, и где невозможно обеспечить питание от электросети или частую замену батареек.

В отличие от привычных сетей, где требуется все возрастающая пропускная способность и надежность, у сетей LPWA есть целый ряд интересных приложений, где высокая пропускная способность вовсе не требуется, мало того - некритичны потери пакетов или большие задержки, например:

- измерение влажности почвы;
- мониторинг коррозии в танках и бункерах;
- отслеживание уровня снега или воды на улице;
- наличие и/или примерное расположение товара (например, автомобилей на стоянке автозавода);
- обнаружение вибраций двигателя (например, для оценки риска выхода его из строя в ближайшие часы/дни).

В подобных приложениях показания каждого отдельного датчика не имеют большой ценности, будучи, как правило, очень короткими и редко изменяющимися – например, могут сводиться к одному биту «ОК». Из-за этой особенности такие данные редко собирались эффективным образом (за исключением лишь малого числа отраслей, таких как нефтегазовая), поскольку стоимость прокладки проводов намного превосходит ценность показаний датчиков. Поэтому маловероятный останов технологических процессов из-за таких нештатных ситуаций, как неисправность клапана или потери воды в оросительной системе, считался неустранимым риском. Но пусть ценность отдельных данных и незначительна, сейчас общая ценность всех этих - до сих пор не измерявшихся - данных считается новой золотой жилой для оптимизации технологических процессов во всех отраслях и дает стимулы для внедрения Интернета в промышленности.

В типовом сценарии применения технологий LPWA стоимость датчиков должна быть как можно ниже, процедура их монтажа – как можно проще, а затраты на обслуживание устройств в течение их жизненного цикла – минимальными. Еще одна проблема связана с большим числом контролируемых объектов (одна система может контролировать тысячи или десятки тысяч «вещей») и масшта-

Рис. 1. Технологии 3GPP LPWA.

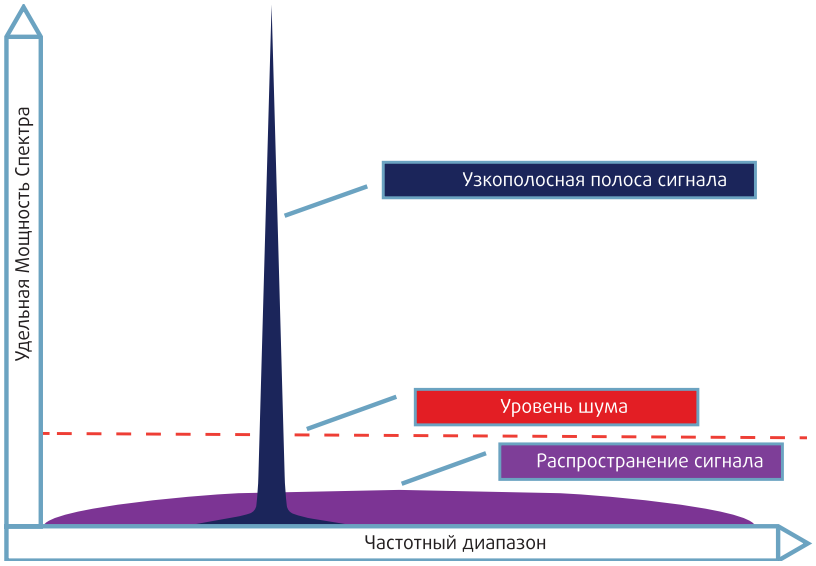
LTE-M (aka LTE-MTC, Cat-M1)
NB-IOT (aka Cat-NB1)
EC-GSM-IOT (aka EC-GPRS)

бом развертывания сети, которая часто охватывает огромные площади, значительно превышающие дальность технологий локальных беспроводных сетей (WLAN) и беспроводных персональных сетей с низким энергопотреблением (LoWPAN), приближаясь к масштабам районных беспроводных сетей (Wireless Neighborhood Area Network, Wi-NAN) и сотовой связи.

При проектировании сетей LPWA (также называемых LPWAN) можно использовать оба напрашивающихся подхода, т.е. увеличивать покрытие беспроводных сетей с низким энергопотреблением или уменьшать стоимость и энергопотребление сотовых сетей. В реальности используются все возможные варианты решения описанных выше проблем, порождая целый спектр новых технологий с рядом уникальных возможностей (см. рис. 1).

Для работы в лицензируемом диапазоне частот 3GPP стандартизировала новую узкополосную технологию радиопередачи NB-IOT, особенностями которой являются простота, низкое энергопотребление и большое покрытие. Кроме того, для быстроты развертывания NB-IOT может использовать имеющуюся инфраструктуру LTE или старую сетевую инфраструктуру и сосуществовать с ними в том же частотном диапазоне. 3GPP также стандартизировала для LTE категорию простого пользовательского оборудования с низкой полосой пропускания под названием Cat-M1 и усовершенствования сетей GSM/GPRS для IoT, получившие название EC-GSM-IoT.

Рис. 2. Подходы LPWA к использованию частотного диапазона.



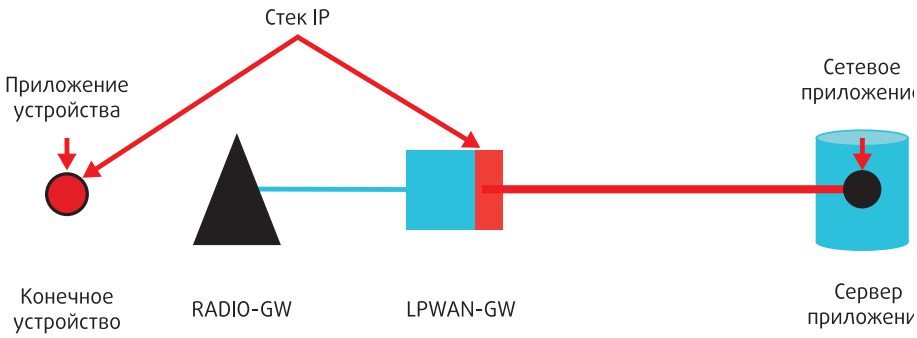
Еще один тип технологий LPWA (например, LoRa, SIGFOX, INGENU) предназначен для работы в нелицензируемых диапазонах промышленных, научных и медицинских частот (ISM = Industrial, Scientific and Medical), позволяя передавать данные на десятки километров со скоростью на уровне десятков кбит/с, используя самые разнообразные технологии радиосвязи, от SIGFOX Ultra Narrow Band (UNB), использующей тонкий пик спектра, и до LoRa Chirp Spread Spectrum (CSS), распределенной по всей доступной полосе пропускания. Оказалось, что комбинирование различных методов дает конечному пользователю дополнительную свободу выбора, а также свободу от привязки лишь к одной части спектра, за которую конкурировали бы все устройства и системы. Эти новые технологии дополняют возможности диапазона ISM, заложенные в стандартеIEEE802.15.4 для таких приложений, как Smart Grid (Wi-SUN) (рис. 2).

Таблица 1 Сравнение технологий LPWA

	Wi-SUN	SIGFOX	LoRa	EC-GSM	CAT-M1	CAT-NB1
Внедрены	Да	Да (EC, США и Канада)	Да	Да	4 кв. 2016	4 кв. 2016
Инсталляции	Частные	SIGFOX	Частные / моб. оп.	Мобильные операторы / обновление ПО		
(SDO) Стандарт	IEEE 802 IETF	(ETSI) LTN	LoRaWAN (ETSI) LTN	3GPP		
Спецификация доступна бесплатно для IETF	Да	Объявлено о беспл. доступности в конце 2017 г.	Да	Да		
Сертификация	Wi-SUN Alliance	SIGFOX	LoRa Alliance	Региональные участники 3GPP (ETSI, ATIS...)		
Макс. мощность передачи, dBm	8-14	14	14	23/33	20/23	23
Макс. полоса пропускания	200-400-600 кГц	100/600 Гц (EC/США, Канада)	125-500 кГц	200 кГц	1,08 МГц	200 кГц
Модулирование	FSK	DBPSK вверх, GFSK вниз	Chirp Spread Spectrum	GMSK	QPSK QAM	QPSK
Скорость передачи данных, до	50-300 кбит/с	100 бит/с (EC) 600 бит/с (США, Канада)	0,3-50 кбит/с	70 кбит/с	375 кбит/с	65 кбит/с
Полоса частот	Не лицензируется, полоса Sub-GHz ISM (433 и 868 МГц в EC, 928 МГц в США/Канаде)			2G	LTE	2G & LTE

Необходимость поиска компромисса между затратами, бюджетом энергопотребления, гарантией бесперебойной работы и управляемостью указывает, что требуется добиваться оптимизации для каждого индивидуального приложения, и что разные технологии радиосвязи с разными возмож-

Рис. 3. Общие компоненты технологий LPWAN.



ностями и сервисами будут сосуществовать и в дальнейшем: для каждого конкретного приложения будет применяться та технология, которая является для нее оптимальной.

Такая свобода выбора, а также возможность адаптировать новые типы радиосвязи и сервисов по мере развития технологий и возникновения новых потребностей, создают условия для появления различных новых экосистем и приложений, что является одним из главных преимуществ подхода LPWA (см. таблицу 1).

Однако такое разнообразие должно контролироваться, иначе возникнет несовместимость: например, если в каждой технологии будет реализована своя модель приложений, идентификации, безопасности и управления сервисами, то нельзя будет мигрировать приложение по мере изменения потребностей пользователя на другую технологию, либо если архитектура приложения на стороне облака у разных технологий будет сильно отличаться, то невозможно будет использовать один и тот же набор ПО, утилит и навыков.

Чтобы не получить в результате комбинаторный взрыв сложности, необходимо обеспечить конвергенцию технологий по модели «песочных часов» с помощью дополнительного уровня поверх радиоканала, аналогично протоколу IP для Интернета.

Таким уровнем конвергенции для LPWAN могут стать IPv6 и CoAP, обеспечивая доступность устройств и в то же время их относительную изоляцию с абстрагированием от технологий беспроводной передачи более низкого уровня. На берлинской конференции IETF 96 после успешного установочного семинара была образована рабочая группа LPWAN, которая впервые собралась на IETF 97 в Сеуле. Эта рабочая группа будет заниматься передачей пакетов IPv6 по сетям LPWA и "взаимовыгодной" реализацией подключения сетей LPWAN к Интернету.

Общая архитектура LPWAN

На первый взгляд спектр технологий LPWA может показаться слишком разнообразным для стандартизации силами IETF. Например, Wi-SUN уже поддерживает IPv6 посредством 6LoWPAN, поэтому тут дополнительно работать над поддержкой не нужно. Тем не менее, в Wi-SUN можно совершенствовать другие компоненты, например, безопасность и управление идентификационными данными, что, возможно, заинтересует другие стороны, уже поддерживающие эту технологию.

При более тщательном рассмотрении выясняется, что технологии LPWAN обычно используют похожие структуры для шлюзов уровня радиоканала (RADIO-GW) с оконечными устройствами и для шлюзов сетевого уровня (LPWAN-GW), которые агрегируют трафик нескольких RADIO-GW и осуществляют соединение с внешним миром. Для технологий LPWAN также очень желательно реализовать поддержку IP-связи между сетевыми приложениями и приложениями оконечных устройств, с целью улучшения портируемости сервисов и универсализации инструментария (рис. 3).

Для IETF крайне важно создание общей архитектуры, которая обеспечит совместимость технологий. Одна из главных задач IETF - это выявить общие функциональные потребности для шлюзов LPWAN (GW) и стандартизировать реализующие этот функционал протоколы. Новая архитектура должна по-максимуму использовать основные общие черты технологий LPWAN,

Рис. 4. Потенциальная архитектура LPWAN.

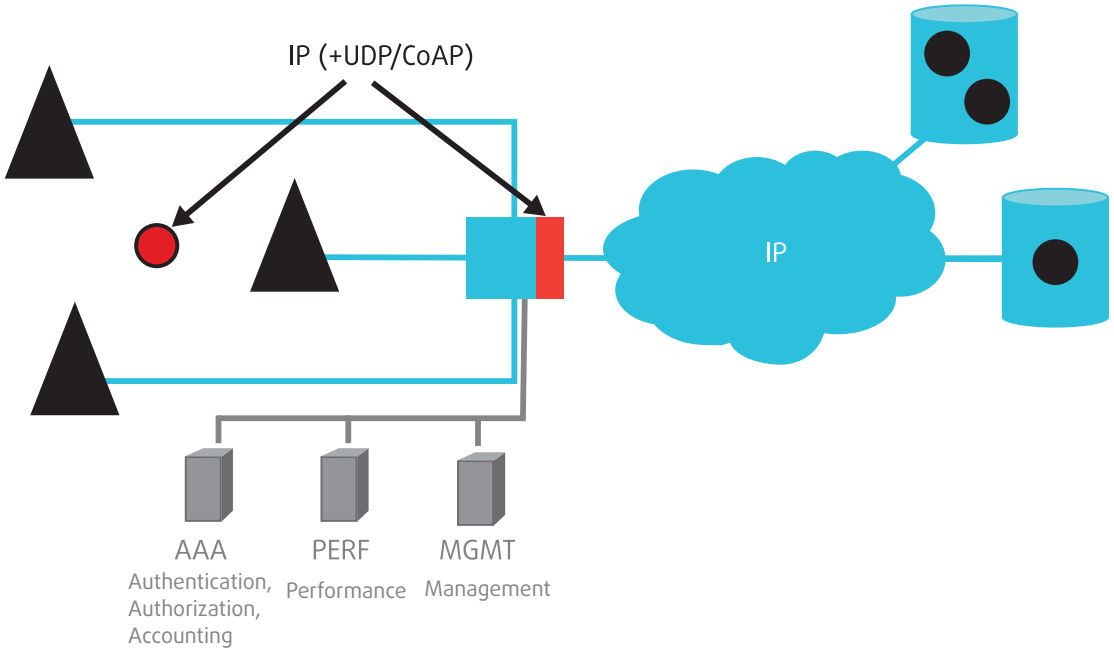
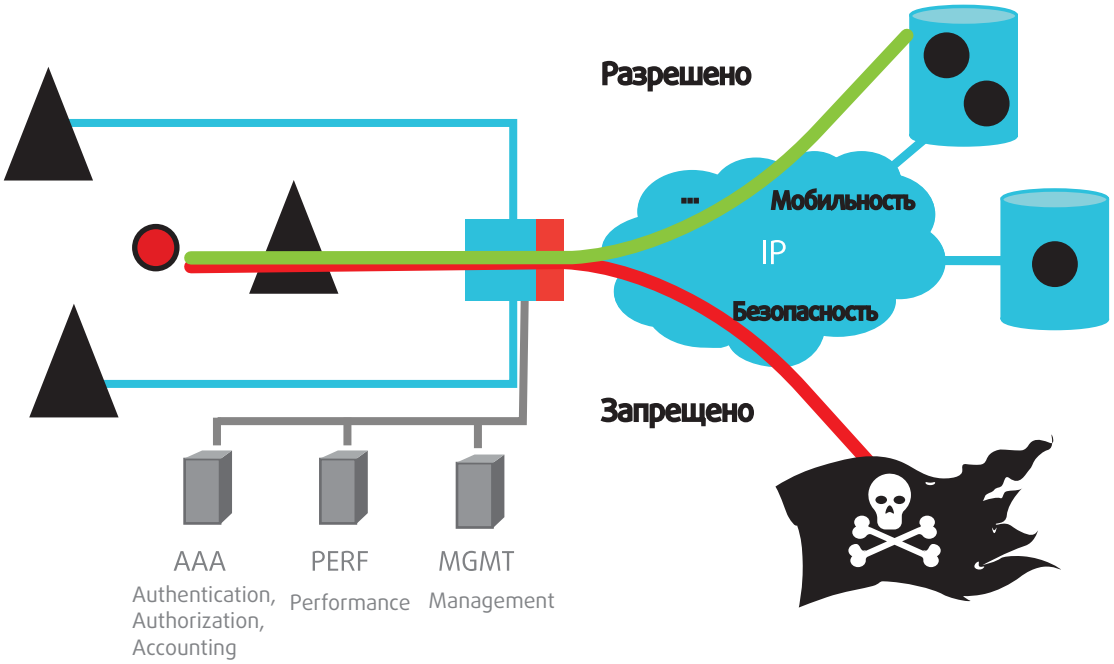


Рис. 5. IoT-инсталляции должны быть безопасными.



такие как оптимизация времени работы от батарейки, крайне нерегулярный характер трафика и низкая пропускная способность. Такие экстремальные требования далеко выходят за пределы возможностей 6LoWPAN, предназначенного для беспроводных технологий с низким энергопотреблением и малым покрытием.

Используя эту архитектуру, IETF предлагает конвергировать разные технологии радиосвязи в единые «песочные часы» с очень высоким сжатием трафика IPv6 и CoAP между оконечным устройством и сетевым шлюзом с тем, чтобы и добиться общего управления шлюзом, и предоставить приложениям безопасные интернет-сервисы.

Нужны новые алгоритмы

Некоторые технологии LPWA из-за черепашьей скорости передачи данных очень чувствительны к размеру пакета. Поэтому классические методы сжатия плохо подходят для технологий, где на передачу IP и CoAP остается всего один-два октета. Такой уровень сжатия может дать RoHC (Robust Header Compression), но в своем нынешнем виде ее нецелесообразно использовать из-за разнообразия потоков данных и прогнозируемого сильного изменения характера трафика в будущем.

В IETF необходимо больше работать над этой проблемой, возможно, взять лучшее из обеих технологий сжатия и обеспечить экстремальное сжатие, необходимое для поддержки IP и CoAP устройствами, в то же время обеспечив функционирование LPWAN-GW для терминирования потоков трафика IP - так, чтобы шлюз «считал» оконечное устройство устройством удаленного ввода-вывода (подобно USB-устройствам для ПК).

Новые протоколы должны учитывать сжатие на уровне приложений (например, CoAP) и применять для оптимизации сжатия все возможные механизмы и особенности LPWAN (прежде всего топологию «звезда» и ограниченный и заранее известный трафик для каждого оконечного устройства).

Не только сжатие

Если бы единственной целью нового направления работ IETF была возможность обмениваться данными с устройствами по IP, не нужно было бы создавать для LPWAN отдельную рабочую группу. Добавим, что реализация поддержки CoAP на оконечном устройстве позволяет использовать модель взаимодействия IETF, разработанную группами CoRE WG и T2T RG и недавно принятую Open Connectivity Foundation и другими организациями. Но для того, чтобы реализовать безопасные и доступные интернет-сервисы для устройств IoT с низким энергопотреблением, требуется сделать очень много для самого Интернета. Недавняя атака на блог Кребса «On Security» показала, что безопасность и обслуживание устройств IoT невозможно реализовать исходя из практики, выработанной для обычных ПК. Нужны гарантии долговременной защиты устройств от взлома – этого, возможно, удастся достичь путем автоматического управления положением и рассылки патчей, закрывающих уязвимости по мере их обнаружения, а также путем изоляции устройств и от возможных атак, и от возможных целей таких атак.

Кроме традиционных практик, необходимо обеспечить надежную защиту IoT-устройств от злоумышленников, пытающихся собрать с них информацию либо поставить их под контроль и использовать в своих интересах. С одной стороны, обмен данными между устройством IoT и его приложением должен быть возможен в любой момент, вне зависимости от того, развертывается ли приложение, работает в штатном режиме или выводится из эксплуатации. С другой стороны, несанкционированный обмен данными с IoT-устройствами должен всегда быть надежно перекрыт, чтобы в случае компрометации одного устройства локализовать ущерб для всей сети и пресечь возможность компрометации других устройств.

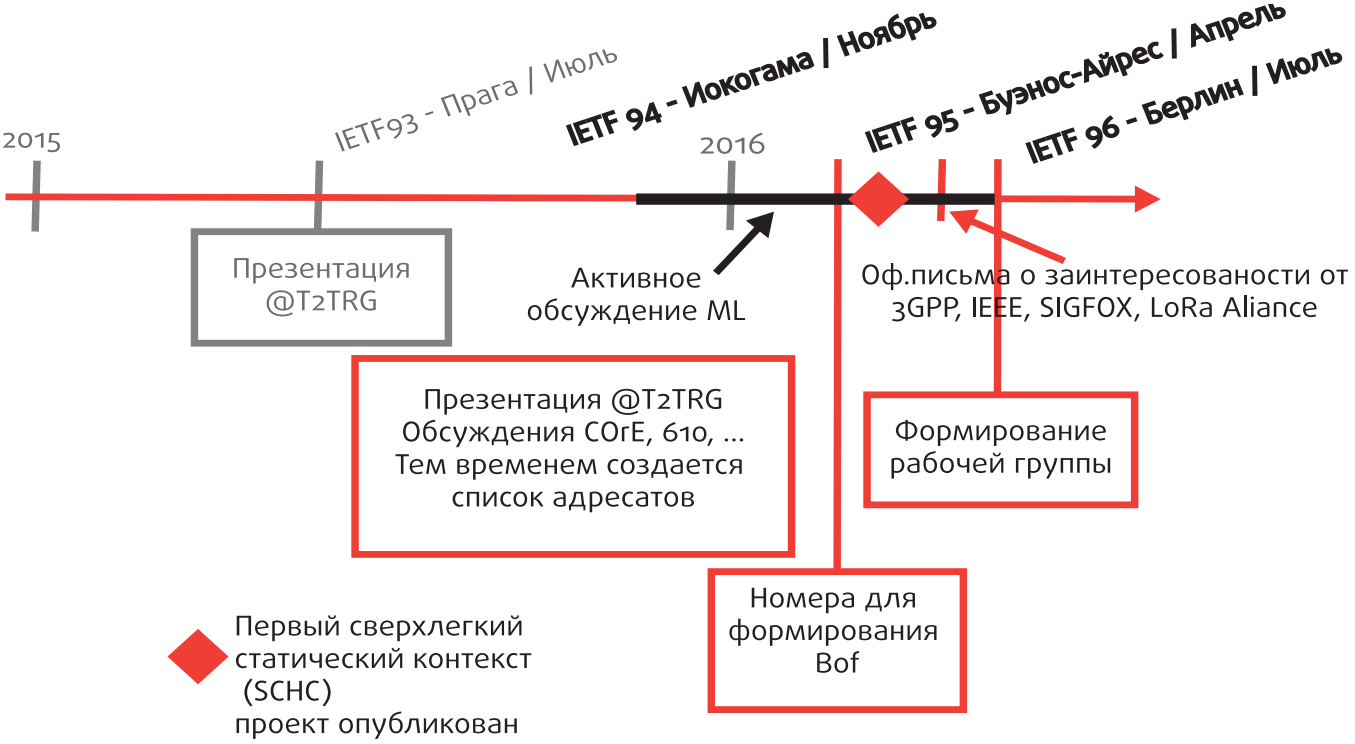
Самый простой и надежный способ защиты - это изоляция устройства и его приложений в оверлейной сети, использующей уникальные локальные адреса, которые недоступны извне. Но доступные по требованию и масштабируемые оверлеи - не единственная потребность IoT, которую может помочь реализовать IETF. Сейчас, когда к Интернету начали подключаться автомобили, а квартирные переезды осуществляются вместе с миграцией всей домашней сети, необходимо обеспечить мобильность IoT-устройств на уровне протокола IP.

Технологии оверлейных сетей IETF, например, NEMO и LISP, реализуют мобильность путем изоляции трафика, но подходы к безопасности и масштабируемости у них различны. Для того, чтобы выбирать решения, соответствующие фактическим потребностям ситуации и реальным сценариям, требуется комбинация практического опыта в области LPWA с опытом в области интернет-технологий.

Работа по IPv6 на сегодняшний момент

Проект спецификации, представленный исследовательской группой T2T RG на IETF 93,

Рис. 6. График деятельности LPWAN.



был всего лишь первым наброском. В нем в общих чертах описывались потенциальные возможности применения и возможные ограничения сетей с низким энергопотреблением и большим покрытием, а также то, как IETF может доработать эти сети, в том числе повысить их безопасность, мобильность, улучшить управление устройствами, обнаружение сетей и сервисов.

Основными задачами этого документа были изложение актуальных проблем LPWAN и организация работ по этим проблемам в уже существующих рабочих группах. Многочисленные обсуждения этих вопросов на IETF 93 и 94, а также дискуссии с другими игроками в этой отрасли показали, что для решения этих задач необходимы либо отдельная площадка, если они не вписываются в направление работ уже существующих рабочих групп, либо специальный механизм координации, если посвященные этим проблемам группы уже есть.

Правильность этого подхода еще более подтвердили разносторонние дискуссии в списке рассылки вне рабочих групп, а также большой интерес к негруппообразующей BoF на IETF 95 в Буэнос-Айресе. Поворотным пунктом стал проект спецификации Static Context Header Compression, который впервые показал на практике возможность реализации стека IETF в таких сетях с очень сильными ограничениями. Это событие, вкупе с мощным процессом стандартизации IETF, мотивировало разработчиков четырех основных технологий LPWAN (SIGFOX, LoRa, Wi-SUN и 3GPP) поддержать создание рабочей группы LPWAN и поручить IETF реализацию своего стека для этих LPWAN. Рабочая группа LPWAN также играет важную роль в том, чтобы объединить усилия разных сообществ, лишь немногие участники которых ранее имели дело с IETF.

Задачи и дорожная карта

Первым делом рабочая группа займется разработкой новых способов сжатия трафика IP/UDP/CoAP, которые заложат основу дальнейшей работы в этом направлении. График работ очень напряженный (мы планируем подготовить окончательную версию к середине 2017 года), так как спрос на четыре базовые технологии уже сейчас крайне высок. На первом этапе мы также поможем структурировать сообщество LPWAN и заложить фундамент для последующего расширения деятельности, в том числе на протоколы управления Radio-GW и LPWAN-GW, обеспечение мобильности оконечных устройств и AAA-процедуры, оверлеи, безопасность и использование DNS в ядре сетей LPWAN.

Источник: Low-Power Wide-Area Networks at the IETF, http://www.ietfjournal.org/low-power-wide-area-networks-at-the-ietf/

Интернет вещей: Стандарты и рекомендации IETF

Ари Керанен, Карстен Борман
(Ari Keränen, Carsten Bormann)

К настоящему моменту IETF уже больше десятилетия трудится над выработкой спецификаций и документированием ключевых стандартов и рекомендаций по IoT, и сегодня активность этой организации в этом направлении больше, чем когда-либо. Другие организации и консорциумы, работающие в области IoT, приняли стек протоколов Интернета в качестве основы для своих решений. IP и в частности IPv6 являются очевидным выбором для построения сетей, но широко используется и остальная часть стека IETF IoT, включая CoAP и DTLS.

Для истинного интернета вещей (IoT) необходимо, чтобы эти «вещи» могли использовать протоколы Интернета. В Интернете всегда существовали те или иные «вещи», а неспециализированные компьютеры в домах и центрах обработки данных обычно без проблем работают с протоколами Интернета, так как они для этих устройств и предназначены. Тем не менее, подключение к Интернету устройств более узкого назначения, которым часто нужны оптимизированные версии или специальные условия использования для этих протоколов, имеет значительные достоинства.

Предыстория

За последнее десятилетие в IETF было инициировано несколько разнообразных работ, направленных на то, чтобы предоставить широкому диапазону вещей возможность использовать совместимые технологии для взаимодействия друг с другом: от миниатюрных датчиков, управляемых микроконтроллерами, до больших компьютеров в центрах обработки данных.

Когда мы писали об IoT в журнале IETF в 2010 году, в IETF имелось три рабочих группы, чья деятельность была направлена на IoT для устройств и сетей с ограниченными возможностями: группа 6LoWPAN, определившая уровень адаптации IPv6 и сжатие заголовков, пригодные для ограниченных радиоканалов; группа ROLL, сосредоточившая свою деятельность на протоколах маршрутизации для сетей с ограниченными узлами; и группа CoRE, целью которой является распространение архитектуры Web на большинство ограниченных сетей и встроенных устройств. Деятельность в направлении IoT с 2010 года только расширилась, и сегодня у нас насчитывается семь рабочих групп, активно разрабатывающих различные аспекты IoT (плюс еще две, завершивших работу), а также исследовательская группа Internet Research Task Force (IRTF), посвященная открытым исследовательским вопросам, связанным с IoT.

Деятельность IETF в области IoT

Первая рабочая группа IETF IoT, получившая название 6LoWPAN (IPv6 over Low-Power WPAN), была образована в марте 2005 года. Она определила методы адаптации IPv6 для сетей IEEE 802.15.4 (WPAN), отличающихся крайне малым размером пакета, путем сжатия заголовков и оптимизации обнаружения соседей (Neighbor Discovery). 6LoWPAN завершила свою работу в 2014 году, и пришедшая ей на смену рабочая группа 6Lo занимается разработкой аналогичных механизмов адаптации к более широкому спектру технологий радиосвязи, включая Bluetooth Low Energy (RFC 7668), ITU-T G.9959 (как используется в Z-Wave, RFC 7428) и стандарт беспроводных телефонов Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE), а также экономичную технологию проводных сетей Master-Slave/Token-Passing (MS/TP), широко используемую в сетях RS-485 при создании систем автоматизированного управления.

Рабочая группа ROLL (Routing Over Low-Power and Lossy Networks) создала спецификации как для RPL-протокола IPv6 Routing Protocol for Low-Power and Lossy Networks (RFC 6550), так и для набора связанных расширений для различных метрик маршрутизации, объективных функций и малтикаста. Еще одним результатом деятельности ROLL стал комплект требований и заявлений о применимости, терминологический документ и анализ угроз безопасности.

Рабочая группа CoRE (Constrained RESTful Environments) до сих пор является одной из самых активных IoT-групп. Основным результатом ее работы является Constrained Application Protocol (CoAP, RFC 7252), радикально упрощенный аналог HTTP, основанный на UDP. Расширения CoAP позволяют осуществлять групповую коммуникацию (RFC 7390) и несложную серверную рассылку для наблюдения за ресурсами (RFC 7641). Все это дополняется механизмом обнаружения и самоописания, основанном на формате веб-ссылок, пригодном для ограниченных устройств (RFC 6690). Нынешняя деятельность группы направлена на разработку расширений, которые будут поддерживать передачу больших ресурсов, использование каталогов ресурсов для координации обнаружения, готовых к использованию описаний интерфейсов и транспортировку CoAP поверх TCP и TLS. Рабочая группа CoRE сейчас переформируется: в ее область работы включаются RESTCONF-подобные функции управления и коммуникация типа "публикация-подписка" по CoAP. CoRE также разрабатывает формат данных для представления измерений,

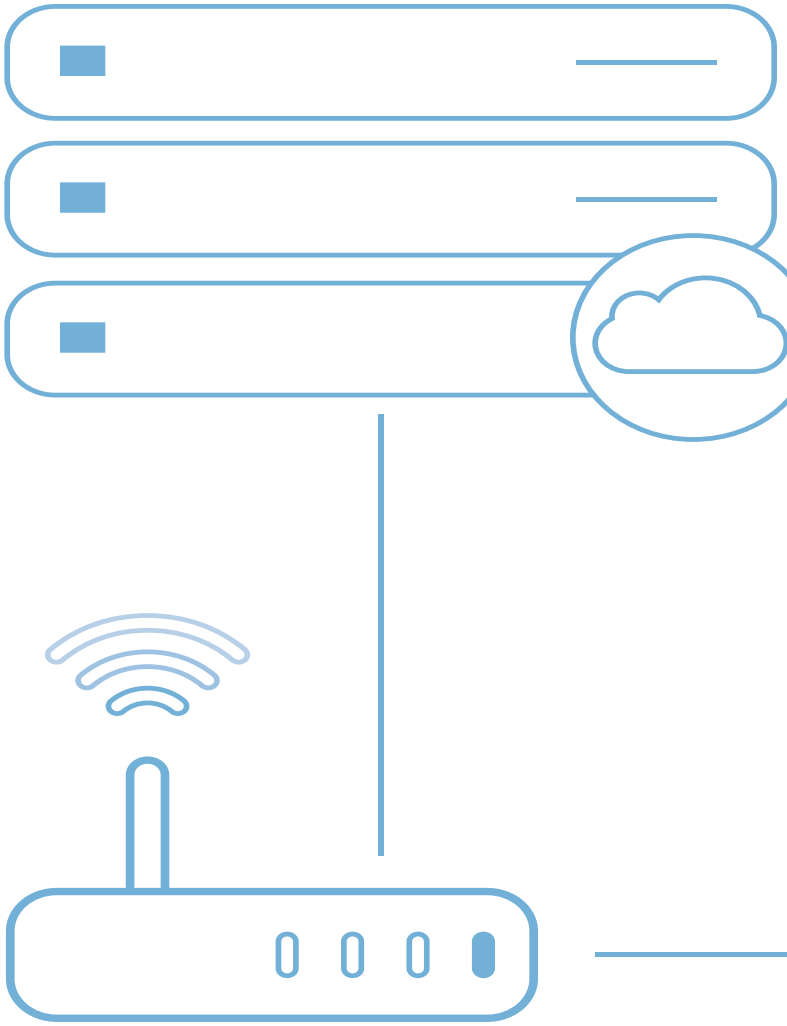
снятых с датчиков, который будет использовать стандарт Concise Binary Object Representation (CBOR) (RFC 7049), аналог JSON, оптимизированный для двоичных данных и устройств с ограниченными ресурсами.

С 2010 года стало ясно, что IoT невозможен без надежной системы безопасности. Поэтому большинство новых рабочих групп по IoT были сформированы в сфере безопасности. Рабочая группа DICE (DTLS In Constrained Environments), уже завершившая работу, создала профиль TLS/DTLS, пригодный для ограниченных IoT-устройств. Рабочая группа ACE (Authentication and Authorization for Constrained Environments) трудится над механизмами аутентификации для доступа к ресурсам, размещенным на серверах в ограниченных средах, и недавно подготовила всеобъемлющий документ RFC 7744. Работу в этом направлении поддерживает недавно образованная рабочая группа COSE, создающая упрощенные аналоги CBOR для методов подписания и шифрования объектов JSON, разрабатываемых в группе JOSE.

Группа 6TiSCH (IPv6 Over the TSCH Mode of IEEE 802.15.4e), ставшая своеобразным дополнением к 6Lo, была образована в 2014 году и работает над реализацией IPv6 для Time-Slotted Channel Hopping (TSCH), недавно добавленного в сети IEEE 802.15.4. Эта работа направлена на использование детерминированных функций реального времени TSCH и включает в себя архитектуру, информационную модель и вопросы конфигурации. Обзорный документ 6TiSCH с изложением проблемы (RFC 7554) был опубликован в 2015 году; следующей будет спецификация для интерфейса с минимальной конфигурацией.

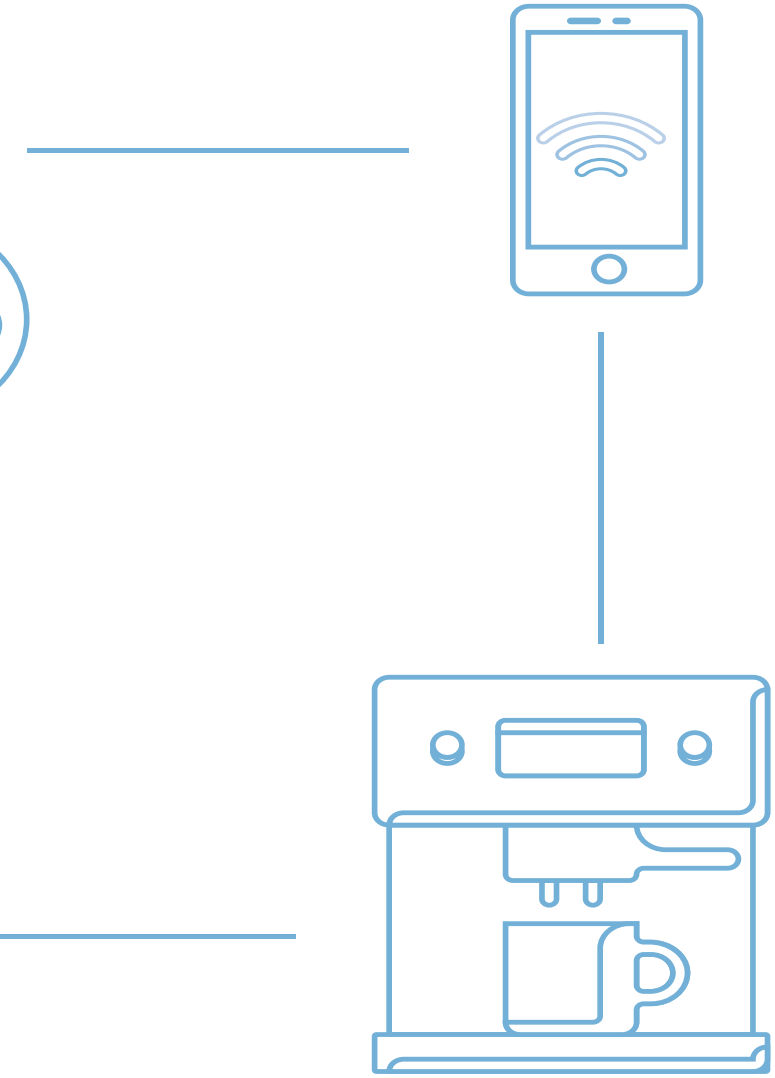
Кроме новых протоколов и других механизмов, разрабатываемых рабочими группами IETF, также важной является разработки рекомендаций по эффективным методам внедрения и другим аспектам. Рабочая группа LWIG (Lightweight Implementation Guidance) WG работает над такими документами, включая рекомендации для протоколов CoAP и IKEv2, асимметричной криптографии и CoAP в сотовых сетях. LWIG опубликовала RFC 7228, определяющий общую терминологию для сетей с ограниченными узлами.

Даже если оставить за скобками деятельность IETF, направленную конкретно на сценарии IoT, весь стек протоколов Web стремительно развивается, и многие из новых технологий, созданных другими рабочими группами IETF, скорее всего, будут использоваться также и для IoT. Рабочая группа HTTPbis недавно завершила создание спецификации для протокола HTTP/2, которая более пригодна для IoT-сценариев, чем ранние версии HTTP, благодаря более компактному формату и упрощенным правилам обработки. Рабочая группа TLS разрабатывает протокол TLS версии 1.3, включая DTLS 1.3, который может устанавливать безопасные транспортные сеансы более эффективно и поэтому лучше подойдет для IoT. Рабочая группа Homenet занята разработкой автоматической конфигурации сетей IPv6 в домашних сетях. Параллельно деятельности IETF по стандартизации следует отметить две исследовательские группы IRTF:



ICNRG (Information-Centric Networking), исследующую применимость своих технологий для сценариев IoT, и CFRG (Crypto Forum), развивающую фундаментальные методы шифрования, такие как новые кривые эллиптической криптографии (ECC), которые бу-

дут более пригодны для IoT. И, наконец, IAB (Internet Architecture Board) организовывал несколько связанных семинаров (например, по безопасности, архитектуре, семантической совместимости) и опубликовал информационные документы, такие как Architectural Considerations in Smart Object Networking (RFC 7452).



В то время как IoT-ориентированные рабочие группы IETF уже выработали первые зрелые стандарты для IoT, возникают все новые вопросы для исследования, связанные с внедрением этих стандартов. Рабочая группа IRTF T2TRG (Thing-to-Thing Research Group) была образована в 2015 году для исследования открытых вопросов IoT, в первую очередь проблем с возможностью выработки стандартов IETF. В числе изучаемых тем - управление и эксплуатация сетей с ограниченными узлами, управление безопасностью и жизненным циклом, способы использования парадигмы REST в сценариях IoT и семантическая совместимость. Кроме того, имеется значительный интерес к отслеживанию и вкладу в работу других групп, работающих в области IoT. Например, недавно начала работу группа WoT (Web of Things) в составе W3C, и две группы тесно сотрудничают, изучая совместное будущее IoT и Web-технологий.

Заключение

К настоящему моменту IETF уже больше десятилетия работает над выработкой спецификаций и документированием ключевых стандартов и рекомендаций по IoT, и сегодня активность этой организации в этом направлении больше, чем когда-либо. Другие организации и консорциумы, работающие в области IoT, приняли стек протоколов Интернета в качестве основы для своих решений. IP и в частности IPv6 являются очевидным выбором для построения сетей, но широко используется и остальная часть стека IETF IoT, включая CoAP и DTLS. Базовый стек протоколов IETF IoT, как он определен сейчас в спецификациях RFC, является зрелым и пригодным для внедрения. Появляются дополнительные потребности в стандартизации, и активные группы в составе IETF и IRTF не покладая рук работают над выявлением и удовлетворением этих потребностей.

Источник: Internet of Things: Standards and Guidance from the IETF

Нечеловеческие вещи

Андрей Колесников

— Давай развернем инфраструктуру LORA в Москве и области.

— А сколько это стоит?

— Ерунда, базовая станция в районе 700 евро накрывает несколько километров.

— А какие услуги будем предлагать?

— ??...

(Типичный диалог специалистов ЙОТ 2015 года)

Термин «интернет вещей» предложил Кевин Аштон (Kevin Ashton) в 1999 году во время презентации технологий RFID для логистики компании Procter & Gamble. В том же 1999 году он изрек краткое функциональное описание:

Если бы у нас были компьютеры, которые бы знали об окружающих нас вещах на основе данных, которые бы они собирали без нашей помощи, мы смогли бы посчитать и отследить вообще все вокруг и это снизило бы уровень отходов, потерь и затрат. Мы бы знали, когда и какие вещи нуждаются в замене, ремонте или апгрейде и знали бы, откуда они взялись.

Тотальный контроль окружающего мира - это тот идеал, к которому стремится человечество в силу своей природной любознательности и алчности. Сегодня, в начале 2017 года, ремесло контроля над вещами и процессами стало системным общемировым явлением. В этом не очень много науки, все технологии, которые используются для интернета вещей, известны и используются много лет. Скорее, речь идет о том, что люди "распробовали" экономические эффекты и удобство контроля над вещами и через это пришли к выводу о том, что вещи могут взаимодействовать друг с другом без участия человека, тем самым повышая эффективность работы тех или иных систем. Сегодня мы наблюдаем два процесса: конкуренция идей и соперничество технологий.

При любой активно развивающейся технологии мы проходим через период турбуленции в стандартах и параметрах протоколов. В мире Интернета это занимает несколько лет, до тех пор, пока основные технологические игроки не договорятся друг с другом. Поэтому вопросы стандартизации можно отнести к фактору времени: количество используемых протоколов снизится, но останется существенным. Стандарты непосредственно влияют на бизнес-риски, но об этом ниже.

Как и у религии, у технологии должны быть Главная Книга и торговцы Книгой. Интернет вещей (для простоты ЙОТ) является прекрасным примером.

Главной книгой интернета вещей стал отчет McKinsey Global Institute "Интернет вещей: рассчитывая ценность за пределами надувательства"[1]. Этот отчет по сути установил ключевые драйверы развития интернета вещей как самостоятельной индустрии в применении к вертикалям хозяйственной деятельности человечества. Финансовые оценки McKinsey бизнеса интернета вещей мгновенно перекочевали в PowerPoint-презентации и аналитические записки различных по размеру технологических компаний. Я тоже торговец Книгой и люблю жонглировать цифрами и вставить между делом десятка два миллиарда долларов, придавая убедительности словам. Прекрасно то, что когда лет через пять станет понятен объем ЙОТ, всем будет до лампочки, что предрекали нам McKinsey или Deloitte в 2015 году. Сегодня понятна суть интернета вещей (плюс - минус миллиард - не принципиально) - технологии и модели интернета вещей уже здесь, и они позволяют либо снижать издержки бизнеса, либо повышать доходность, либо и то, и другое.

Так что же случается, когда прекрасные идеи и технологии падают на почву российской действительности? Начинается информационное бурление и постепенное внедрение ЙОТ. Проблема, с которой мне приходится постоянно сталкиваться, - это малое количество специалистов, которые понимают ЙОТ в комплексе: и технологии, и бизнес-процессы, и важность контроля всего жизненного цикла производства или сервиса, включая всех участников описываемой модели. Поэтому при работе с клиентом действенной моделью повествования является путь от простого к сложному: Как снизить уровень воровства материалов? Как вычислить приписки при загрузке руды? Как выстроить и контролировать логистику передвижения транспорта? Как оптимизировать жизненный цикл производства, внедряя датчики и управляющие элементы, и обмениваться информацией с поставщиками и сбытом?

Со времени проведения первых конференций ЙОТ в России прошло всего два года, а мы имеем дело с полномасштабным сдвигом в понимании технологии и концепций ЙОТ на самых различных уровнях государственного и муниципального управления и

в бизнесе. Появились дорожные карты развития интернета вещей, Москва (по моим оценкам) вошла в тройку столиц мира по уровню внедрения систем и вещей Интернета. Мне представляется, что ЙОТ - это не совсем про технологии, а про возможность увидеть систему в комплексе со всеми внешними интерфейсами, вычислить проблемы и предложить решение. Подсмотренные чужие примеры тоже вполне годятся. Интернет пришел к нам из США. Интернет вещей приходит к нам из многих стран мира. Россия - один из глобальных участников процессов становления экономики интернета вещей, поэтому схема give and take вполне справедлива.

Сегментируя это

Опираясь на отчет McKinsey, можно разделить применение технологий интернета вещей по вертикальным сегментам:

- Жилье: функционирование, автоматизация и безопасность.
- Офис: безопасность и энергетика.
- Заводы и фабрики: управление оборудованием и функционирование.
- Торговля: автоматизация, кассы.
- Промышленные объекты: оптимизация, функционирование, здоровье сотрудников и безопасность.
- Человек: здоровье и образ жизни
- В мире: логистика, доставка, навигация.
- Города: безопасность и транспорт.
- Автотранспорт: автономные машины и предиктивное обслуживание.

Также необходимо добавить данных из отчета специфики глобального рынка:

- Интероперабельность добавит 40% к ценности систем интернета вещей. Это непосредственно связано с унификацией стандартов и протоколов.
- Сегодня используется не более 1% для “майнинга” ценностей из собираемых ЙОТ данных. К этому можно добавить ощущение (рассчитать сложно), что наличие открытых данных и возможность их микширования в поисках закономерностей существенно добавят стоимости и значимости собранным и обработанным данным.
- Индустриальный интернет вещей (B2B, IIoT) даст в два раза больше денег, чем использование на рынке консьюмеров.
- Россия и другие экономики третьих стран дадут вклад порядка 40%, при этом развитые экономики обеспечат 60%.

С чем мы имеем дело в России?

Не существует целостного понимания прогнозов роста бизнеса ЙОТ в России по предложенным McKensey лекалам. Данные разрознены, система оценки отсутствует, во многих сегментах хозяйственной деятельности информации просто не существует.

Однако кое-какие данные есть, как и общее ожидание от перспектив реализации проектов ЙОТ в России. Начнем с простого утверждения о том, что при дефиците внешних и внутренних инвестиций, общем спаде производства и в экономике, технологии и системы ЙОТ помогают сократить расходы. Говоря проще, когда нет новых денег, нужно внимательно посмотреть на расходную часть бюджета и продумать инструменты по реализации схемы “инвестиции с издержек” с применением ЙОТ-технологий.

ЙОТ можно условно разделить на два сегмента: весь ЙОТ и “индустриальный интернет”.

Индустриальный (промышленный) интернет вещей (Industrial Internet of Things, IIoT) – интернет вещей для корпоративного применения - система объединенных компьютерных сетей и подключенных промышленных объектов со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека. Граница индустриального интернета весьма размыта, но это разделение нам пригодится при рассмотрении вертикальных сегментов рынка применения ЙОТ-технологий. При оценке объема рынка в России можно использовать существующие клише, доступные в различных отчетах:

по количеству устройств (убывание): энергетика и коммунальные службы, транспорт, промышленность, здравоохранение, торговля, госсектор, финансы, бизнес-услуги, образование;

по доходам (убывание): транспорт, промышленность, коммунальные службы, здравоохранение, умный дом, торговля, безопасность, умный город, IT[2].

Мы рассмотрим несколько конкретных примеров, исходя исключительно из доступности информации, не принимая во внимание ни космические цифры по количеству устройств, ни финансовые прогнозы.

Жилой сектор

Цели внедрения ЙОТ в жилом секторе и муниципальных услугах понятны и просты: комфорт, контроль издержек и потерь. Для муниципалитетов существенной функцией является пресечение воровства и создание энергетических “гридов” для управления отказами в энергообеспечении. “Умный дом” тоже можно отнести к этой группе, так как внедрение умных и даже хипстерских функций управления домашней инженерией влечет за собой серьезный выигрыш за счет снижения энергетических затрат.

Энергия = деньги, общая формула для энергетического и жилого секторов.

Умный дом (smart house, также building automation и intelligent building, АСУЗ) - жилое пространство (дом, квартира), организованное для комфортного проживания людей с использованием автоматизации и высокотехнологичных устройств. Две главные функции умного дома - это безопасность и ресурсосбережение для всех пользователей (комфортное проживание). Алгоритмы систем умного дома понятны и просты в использовании: следить за температурой, не включать кондиционер, если работает отопление, выключать свет, если в комнате никого нет, и так далее. Можно считать, что это наиболее прогрессивная концепция взаимодействия человека с жилым пространством — когда в автоматизированном режиме в соответствии с внешними и внутренними условиями задаются и отслеживаются режимы работы всех инженерных систем и электроприборов.

Гражданам концепция “умного дома” или “умного холодильника” наиболее понятна и близка. Но с точки зрения объема рынка и потенциала бизнеса, эта ниша занимает последнее место.

Внедрение ЙОТ в муниципальных услугах жилого и офисного сектора сулит большие перспективы. Для контроля энергетики жилого и офисного пространства используются интеллектуальные измерительные приборы (счетчики). Эти приборы следят за потреблением электроэнергии, газа, воды и тепла в любых предустановленных интервалах. Они определяют показатели потребления более детально, нежели традиционные

средства измерения, и дополнительно снабжены коммуникационными средствами для передачи накопленной информации посредством сетевых технологий с целью мониторинга и осуществления расчётов за коммунальные услуги.

Одной из отличительных черт некоторых приборов являются контроллеры с автономным питанием на 5-10 лет и радиоканалы, используемые как для однонаправленной передачи информации, так и для двунаправленной. Кроме того, умные счетчики имеют функцию дистанционного управления с помощью сети Интернет. Интеллектуальные счётчики являются экономичным средством для получения детальной информации о потреблении энергоресурсов, позволяя ценообразующим организациям вводить дифференцированные тарифы на потребление в зависимости от времени суток и времени года и проводить мониторинг потребления и, следовательно, управлять им, снижая излишний расход ресурсов.

Возвращаясь к идее “инвестиции с издержек”, стоит отметить, что снижение потребления на 1 кВт.ч у конечного потребителя экономит до 4-5 кВт.ч энергии у производителя. В жилом и офисном секторах России потребление горячей воды и энергии отопления составляет до 80-90% от общего энергопотребления муниципальных территорий. Поэтому переход на “умные” технологии быстро окупается в многоквартирных жилых домах. Учитывая климатические условия России, мы не будем развивать тему умного грида, солнечных панелей, возврата энергии генерирующим компаниям и другие крутые вещи, позволяющие экономить еще больше.

На российском рынке представлены несколько отечественных компаний, предоставляющих решения и сервисы в области муниципальной энергетики. Все они предоставляют схожие сервисы, которые можно описать набором услуг АО «Электротехнические заводы «Энергомера».

«Энергомера» предоставляет комплексные решения по автоматизации учета электроэнергии для бытовых потребителей и ЖКХ и предоставляет полный перечень услуг по автоматизации учета - от проектирования до внедрения:

- автоматический сбор данных с приборов учета электроэнергии (опционно - счетчиков воды, газа, тепла);
- хранение параметров учета в базе данных;
- возможность установки многотарифного учета;
- полное снятие воровства электричества;
- возможность без монтажа отключить абонента за неуплату.
- данные со всех счетчиков, установленных в квартирах, автоматически собираются устройством сбора и передачи данных;
- показания приборов учета передает на пользовательский терминал, например, в управляющую компанию, где эти данные хранятся, обрабатываются, а также по этим данным выставляются «платежки» на оплату электроэнергии.

Технические параметры приборов учета, устройств сбора данных и радиомодулей можно посмотреть на сайте компании. Компания также активно работает на рынке энергообеспечения промышленных предприятий.

Другие компании, представленные на этом рынке:

ОАО "Нижегородское НПО им. М. В. Фрунзе" - разработчик и производитель автоматизированных систем мониторинга и учета энергоресурсов.

Информационно-измерительная система "Теплоком" - позволяет организовать автоматизированный коммерческий учет тепловой энергии и других ресурсов (электроэнергия, вода, газ) и решать проблемы энергосбережения в различных масштабах. Возможна организация как домового, так и квартирного учета.

«СТРИЖ Телематика», пожалуй, самая “раскрученная” российская компания, предоставляющая автоматизированные услуги по учету энергоресурсов на базе собственной LPWAN-технологии.

Интересные решения в области учета потребления воды предоставляет ЗАО "Тепловодомер", реализуя системы диспетчеризации показаний водосчетчиков по радиоканалу с применением технологии Wireless M-Bus (WMBUS). Ими разработано несколько способов считывания показаний приборов:

- Инкассаторский способ (обходной). Заключается в том, что инкассатор, оснащенный специализированным PDA, перемещается от объекта к объекту, которые оборудованы счетчиками воды с радиомодулями.
- Стационарный способ. Сбор данных осуществляется с радиомодулей счетчиков ретрансмиттером и далее передается на концентраторы. Они в свою очередь передают данные через GSM/GPRS или Ethernet на сервер.

Еще одна гибкая беспроводная система "Водоприбор учет" изготавливается ОАО "Завод «Водоприбор". Обеспечивает сбор и обработку данных комплексного учета потребления энергоносителей (как общедомового, так и поквартирного) и позволяет решать разные задачи по организации учёта потреблённых ресурсов; в систему включены первичные приборы учета со встроенными или внешними радиомодулями для передачи данных, различные ретрансляторы, концентраторы и программное обеспечение сбора и обработки данных.

Подводя итог описанию систем и услуг по учету энергоресурсов, можно сказать, что все системы построены по классической схеме ЙОТ: датчики, среда передачи данных, обработка информации в облаке и приложения, позволяющие осуществлять биллинг и реализовывать другие функции. Используются частоты диапазона 868 МГц, модемы 3G/GPRS.

Ожидается, что в процессе реализации дорожной карты интернета вещей в энергетике[3] количество “исполняемых” системных функций существенно вырастет. И мы перейдем от “удаленного отключения за неуплату” к смарт-гриду, позволяющему экономить до 20% от текущих затрат.

Транспорт

Крупнейшим российским рынком, относящимся к ЙОТ/M2M, можно смело назвать рынок систем мониторинга коммерческого автотранспорта (см. таблицу 1).

В настоящее время уровень проникновения систем мониторинга транспорта в коммерческий автопарк в России близок к 50%, при количестве подключенных грузовых автомобилей и автобусов около трех миллионов. При этом у крупных автоперевозчиков проникновение (доля подключенных автомобилей) достигает 100%.

В 2015 году отмечен разовый рост подключений, связанный с введением системы «Платон». Внедрение этой системы, в рамках которой был план установить около

миллиона устройств в 2016 году, на самом деле является сдерживающим фактором. «Платон» - типичный пример цифрового феодализма[4]. Весь функционал «Платона» мог быть реализован, например, с использованием уже существующей системы ЭРА-ГЛОНАСС. Это не потребовало бы установки на грузовой транспорт дорогостоящих специализированных устройств (тахографов), отнимающей у транспортных компаний средства, заложенные на развитие систем управления транспортом, ничего не давая с точки зрения повышения эффективности бизнеса.

В силу своей проприетарности и дороговизны существующий рынок мониторинга транспорта незначительно охватывает частных перевозчиков, которые могут стать основной точкой роста, поскольку на них приходится не менее половины из имеющегося в России автопарка коммерческих автомобилей – это более двух миллионов грузовиков и около 0,7 миллиона автобусов. В этом сегменте активно используются китайские поделки, широко представленные на «Алибабе». Но назвать это полноценным ЙОТ весьма сложно. Так как трекинг автомобиля “в облаке” является исключительно сервисом мониторинга и не подразумевает приложения каких-либо функциональных действий к объекту мониторинга.

Хороший потенциал роста применения ЙОТ на автотранспорте имеется в так называемом умном страховании. Причем как в корпоративном, так и в частном сегменте рынка. Первые результаты внедрения умного страхования в России и мире показывают, что базирующийся на данных телеметрии анализ стиля вождения и расчет связанного с ним индивидуального уровня риска, результаты которого становятся доступными в режиме реального времени не только страховой компании, но и водителю, позволяет снизить смертность от ДТП.

По прогнозу J’son & Partners Consulting, по состоянию на конец 2018 года в России будет подключено к сервисам “умного страхования” более одного миллиона автомобилей против 30 тысяч в 2015 году.

Точками роста на этом рынке выступают страховые компании, сервисные компании (например, ЭРА ГЛОНАСС), мобильные операторы и автомобильные концерны, которые уже устанавливают устройства телеметрии в автомобили на этапе производства (естественно, в модели “цифрового феодализма” данными автопроизводители делиться не собираются). Но предстоит решить ряд серьезных проблем.

Розничная стоимость телеметрического устройства, подключаемого к диагностическому разъему страхуемого автомобиля, превышает 5 тысяч рублей. Такая стоимость неприемлема для клиента вне сегмента “лакшери”. Необходимы законодательные меры, которые позволят использовать универсальные устройства, построенные на идеологии открытости, данные которых смогут быть использованы в различных приложениях. В этом случае массовость продаж таких универсальных устройств может решить проблему их дороговизны.

Наш путь развития ЙОТ

Рассмотрев два сегмента применения технологий ЙОТ, время перейти к задачам так называемых дорожных карт внедрения интернета вещей в России. Общую задачу дорожных карт можно представить как набор мероприятий, призванных облегчить внедрение методов и технологий интернета вещей в российскую действительность. С описанным выше примером использования ЙОТ на транспорте мы можем смело фанта-

Таблица 1 Мониторинг коммерческого автотранспорта, источник: J’son & Partners Consulting, 2015

	2010A	2011A	2012A	2013A	2014A	2015F	2016F	2017F	2018F
Бортовые устройства систем fleet management	350 000	700 000	1 100 000	1 971 154	2 365 000	2 880 000	3 250 750	4 028 510	5 098 611
Бортовые устройства охранных систем с подключением через сотовую связь	117 300	154 800	203 400	265 770	315 666	360 572	392 974	426 653	485 909
Контроль большегрузов (бортовые устройства)	0	0	0	0	0	300 000	1 000 000	1 800 000	2 200 000
Контроль большегрузов (стационарные и мобильные терминалы)	0	0	0	0	0	1847	1900	2000	2100
Автострахование (устройства телеметрии)	0	0	0	0	3000	30 000	135 465	459 000	1 090 000
Платные дороги (терминалы оплаты)	0	0	20	80	150	210	250	300	350
Платные дороги (бортовые устройства)	0	0	0	10 000	20 000	40 000	70 000	100 000	125 000
Медиа-системы (Connected Infotainment)	0	0	22080	67 800	159 068	249 060	342 742	461 302	616 380
Прочие(Connected-PDN, подключенные светофоры, информационные табло и т. п.	5000	5 500	6 050	6655	7321	8053	8858	9744	10718
Всего	472 300	860 300	1 331 550	2 321 459	2 870 197	3 869 742	5 202 938	7 287 509	9 629 067

зировать и накидать драфт дорожной карты “интернет вещей на транспорте”:

- Ведомству 1 обязать производителей автотранспортных средств передавать параметры автомобиля в “универсальный интерфейс”, допускающий установку устройств телеметрии сторонних производителей.
- Ведомству 2 обеспечить исполнение обязательного требования об обеспечении всех автотранспортных средств начиная с 201X года устройствами, позволяющими подключать средства сбора, передачи и приема телеметрии (перечень параметров).
- Ведомствам 3 и 4 обязать страховые компании и авторизованные технические центры подключаться к системам предиктивной диагностики автотранспортных средств начиная с 201Y года.
- Ведомству 5 начиная с 201Z года обеспечить пакетную трансляцию следующих параметров (градус, покрытие, осадки, видимость) в привязке к геопозиции;
- Ведомству 6 обеспечить бродкаст сигналов управления дорожным движением (параметры) в привязке к геопозиции.
- Ведомству 7 согласовать с Евросоюзом использование частотных диапазонов (перечень) для применения в системах телеметрии автотранспорта.

У дорожной карты также должны быть измеряемые параметры. Например:

- снизить количество ДТП на % к такому-то году;
- снизить затраты на эксплуатацию государственных информационных систем на автотранспорте на % путем внедрения открытых интерфейсов и протоколов… и так далее.

Дорожные карты - это понятный для чиновников и функционеров способ развития той или иной индустрии. Но схема начинает рассыпаться, когда необходимо осуществлять межотраслевое взаимодействие, исходя из того, что чиновник всегда отвечает только за свою “вертикаль”. С интернетом вещей роль “клея” играют негосударственные организации и бизнес. Например, «Яндекс» в дорожной карте «Интернет+медицина», Национальная ассоциации промышленного интернета (НАПИ) в дорожной карте по энергетике и Ассоциация интернета вещей с интернетом вещей в агропромышленном комплексе.

Дорожная карта «Интернет+город»

Дорожная карта была разработана чиновниками Минпромторга, Минкомсвязи, экспертами НАПИ, Ассоциации интернета вещей, представителями различных компаний телекоммуникационной индустрии и ЙОТ-провайдеров, специалистами в области юриспруденции. Всего в работе над текстом дорожной карты в различное время работали почти 100 человек. В частности, дорожная карта нацелена на исправление законодательных барьеров в использовании ЙОТ в муниципальном хозяйстве и энергетике. Например:

- Внесение изменений в Статью 12 Федерального закона №256-ФЗ “О безопасности объектов топливно-энергетического комплекса” в части установления требований к организациям, осуществляющим эксплуатацию и сервисное обслуживание объектов ТЭК, которые отнесены к объектам высокой и средней категории опасности, с учетом необходимости осуществлять сбор, хранение и обработку технологических данных с использованием технических средств, размещенных на территории Российской Федерации”.
- Проведение анализа положений отраслевого законодательства (№126-ФЗ “О связи”, №35-ФЗ “Об электроэнергетике”, №189-ФЗ “Жилищный кодекс”, и т.д.) и общегражданского законодательства (в частности, Трудовой Кодекс), препятствующих внедрению технологий интернета вещей и индустриального интернета;
- Внесение изменений в №115-ФЗ “О концессионных соглашениях” и №224-ФЗ “О государственно-частном, муниципально-частном партнерстве в РФ и внесении изменений в отдельные законодательные акты РФ в части дополнения перечней объектов концессионного соглашения и объектов соглашения (объекты информационно-телекоммуникационной инфраструктуры)».
- Разработка изменений в №261-ФЗ “Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты РФ в части создания условий и стимулирования перехода к дистанционному сбору данных о потреблении».
- Разработка нормативного регулирования в части перевода индивидуальных приборов учета в общедолевую собственность, требования к форматам и стандартам передачи и представления данных о потреблении электроэнергии из локальных систем учета в ГИС ЖКХ…

И это только малая часть дорожной карты. Переход на ЙОТ цепляет за собой каскад изменений в законах и подзаконных актах, меняет привычные способы осуществления хозяйственной деятельности.

Дорожная карта «Интернет+медицина»

Целью дорожной карты «Интернет+медицина» является развитие системы электронного здравоохранения в РФ. Задачи, которые решает дорожная карта: повышение доступности, качества и эффективности медуслуг за счет информационных и интернет-технологий, мобильного и облачных сервисов; устранение регуляторных барьеров для широкого применения информационных технологий и перехода к электронному юридически значимому электронному документообороту.

Задача, непосредственно связанная с применением ЙОТ, - телемедицина. В рамках дорожной карты необходимо разработать и принять нормативно-правовую базу для развития и применения в процессе оказания медицинской помощи телемедицинских технологий, стимулировать процесс внедрения новейших методов диагностики и лечения, использование технологий дистанционного мониторинга состояния здоровья человека.

Возвращаясь к перечню вертикалей внедрения ЙОТ, медицина является одной из наиболее перспективных областей применения методов и технологий интернета вещей в России. А результат этого внедрения непосредственно влияет на здоровье и продолжительность жизни граждан. В дорожной карте есть два блока, непосредственно связанных с ЙОТ.

Проведение НИР, содержащей анализ странового и международного опыта регулирования и стимулирования развития системы персонализированной медицины (включая применение носимых медицинских и фитнес-устройств) и предложений по мерам, необходимым для развития в РФ персонализированной медицины, в том числе в целях регулярного мониторинга состояния здоровья граждан и оказания

доврачебной помощи. Внесение изменений в №323-ФЗ "Об основах охраны здоровья граждан в РФ", для того, чтобы создать правовые основы применения телемедицинских технологий в сфере охраны здоровья граждан. Телемедицина включает в себя огромный круг вопросов, например:

- сертификация телемедицинских технологий;
- пределы и порядок наступления ответственности участников телемедицинской деятельности, медицинские организации, персонал, операторы информационных систем, операторы связи и передачи данных и т.д.;
- вопросы обеспечения безопасной передачи данных.

Дорожная карта ЙОТ в агропромышленном комплексе

Ожидается, что к марту 2017 года будет создана и согласована дорожная карта по применению технологий интернета вещей в сельском хозяйстве. Причем там не одна дорожная карта, а целых две. Первый документ служит цели повышения производительности сельского хозяйства в целом. Второй документ должен обеспечить внедрение меток идентификации животных с целью обеспечения мониторинга жизненного цикла продуктов мясной промышленности.

Над дорожной картой работают представители Минпромторга, Минсельхоза, Минкомсвязи, эксперты Открытого правительства и Ассоциации интернета вещей. Привлечены эксперты из телекоммуникационных компаний, интеграторов и операторов ЙОТ-услуг.

Применение технологий и процессов интернета вещей в сельском хозяйстве дает очень быстрый эффект, а главное – более-менее понятно, что нужно делать. Входящие условия для дорожной карты уже определены:

- сокращение расходов и потерь: ГСМ, транспорт, техника, удобрения, хранение продукции, логистика, мониторинг;
- повышение результатов: точное земледелие, корма, сбыт, эффективная энергетика теплиц и полей;
- информационное обеспечение: глобальные и локальные прогнозы погоды, контроль жизненного цикла продукции.

Перспективы развития ЙОТ в России

Существует несколько перспективных областей развития интернета вещей в России, определяемых сложившейся инфраструктурой производства и предоставления услуг.

Для отечественных компаний, работающих в сфере информационно-коммуникационных технологий, можно рассматривать следующие области:

- Для операторов связи и провайдеров услуг дата-центров - локализация платформ ЙОТ на территории России и развитие собственных ЙОТ-платформ для существующей клиентской базы.
- Для системных интеграторов и разработчиков программных приложений - реализация функционала отечественных систем телеметрии и телеуправления в виде приложений для глобальных платформ ЙОТ.
- Для разработчиков и производителей электронной аппаратуры - разработка и локализация производства устройств для подключения объектов телеметрии и телеуправления к платформам ЙОТ[5].
- Интеграторам – видимо, тренд на создание проприетарных государственных информационных систем будет сломлен в ближайшее время и будут востребованы системы, позволяющие обмениваться большими массивами данных для обеспечения контроля услуг ЙОТ, жизненного цикла продуктов и услуг.
- Для самоделкиных и небольших технологических компаний намечается большая область применения своих умений в агропромышленном комплексе, небольших муниципалитетах, гражданских объектах народного хозяйства.
- Отдельно необходимо отметить большой потенциал ЙОТ в закрытых областях: ВПК, инфраструктура ФСИН, силовые ведомства.
- Телемедицина - это огромный, пока не сформировавшийся рынок ЙОТ.
- Умное страхование и применение ЙОТ на автотранспорте. Можно принимать ставки на то, когда «Платон» перестанет быть проприетарным.

Также ожидается серия покупок небольших инфраструктурных ЙОТ-компаний, эксплуатирующих LPWAN, мобильными операторами, которые будут опаздывать на дележ пирога ЙОТ в связи с задержкой внедрения nb-LTE. При этом традиционные услуги M2M с SIM-картами будут продолжать расти для вещей и объектов, не требующих автономного энергоснабжения.

Традиционно поделенные придворными IT-компаниями индустрии также будут активно развиваться в сторону ЙОТ-технологий. В первую очередь, энергетика (электроэнергия, газ, нефть), РЖД, космос.

В целом, если государство не примет очередной Yarovoi-compatible-закон, обязывающий регистрировать каждое ЙОТ-устройство, хранить данные в государственном мега-облаке и применять проприетарную и не совместимую с тысячами доступных и дешевых устройств криптографию, можно с умеренным оптимизмом говорить о том, что интернет вещей в России будет активно развиваться и принесет дивиденды тысячам компаний, которые будут вкладывать в ЙОТ время, ресурсы и деньги.

Примечания

1. McKinsey Global Institute 2015, The Internet of Things: Mapping the Value Beyond the Hype.

2. Ovnum, Machina Research, Nokia, 2016.

3. Минэнерго: «Создание типовой доверенной системы оперативно-технологического, ситуационного и производственного управления объектами электроэнергетики с использованием цифровых технологий индустриального интернета».

4. Цифровой феодализм - построение проприетарных информационных систем в рамках ведомственной вертикали без возможности использования таких систем для других целей и/или с отсутствием побудительных причин отдавать данные во внешние системы.

5. Несмотря на множество государственных программ, отечественная микроэлектроника пока не предлагает ничего сравнимого, например, с контроллерами Ti.

Уроки мультистейк-холдеризма

Леонид Тодоров

Война миров, или Как правильно выбрать лицо

Мне сразу понравились его носки в разноцветную полосочку. Сбросив модные блестящие туфли с кисточками на подъеме (т.н. loafers, рекомендую Florsheim на Пятой Авеню, там к ним в комплекте идет еще специальная бархотка и средство для очистки, и все вместе всего за..., любезный читатель, ты не одеваешься на Пятой Авеню? Н-да... Ну, тогда просто представь мужские туфли черного цвета с лаковым отливом), он закинул ноги в тех самых радужных носках на широкую приборную доску Mercedes-Benz Sprinter и произнес сакраментальную фразу первооткрывателя России вообще и Москвы в частности: «Мог ли я думать, что в один прекрасный день...» Но давайте по порядку...

Обеспечив в 2009 году при помощи гремучей смеси невообразимого нахальства и примитивного, но действенного шантажа делегирование России кириллического домена .рф, мы в Координационном центре решили отметить это судьбоносное событие проведением в 2010 году Первого Российского форума по управлению Интернетом и пригласить на него весь мировой интернет-бомонд, включая и тогдашнего президента интернет-корпорации ICANN Рода Бекстрома. Разумеется, охота на такого рода птиц - дело тонкое, деликатное, и рецепт успеха непрост (наживка - коктейль из 1/4 сиропа в виде обещаний встреч с представителями российской бизнес-элиты, 2 столовых ложки умеренного оптимизма относительно неформальных бесед «на полях» мероприятия с руководством Минкомсвязи и «российским руководством», щепотка приправы в виде выступления на открытии Форума, соль, перец по вкусу, но при правильном соотношении ингредиентов эффект дает стопроцентный). Добавьте к этому гарантию присутствия на сцене для вручения КЦ памятной таблички об эпохальном событии, и Род был наш в течение того же времени, что требуется электромагнитному импульсу для покрытия расстояния между Центром агрессивного блока НАТО по вопросам кибербезопасности в Таллине и мирным почтовым сервером средней руки петербуржского провайдера.

Вот почему теплым майским деньком 2010 года от Р.Х. я отправился в Домодедово встречать Рода и его помощницу по связям с общественностью Барбару. Учитывая мой богатый опыт в подобного рода делах, торжественная встреча в аэропорту прошла на высоком уровне. Про носки и приборную доску Спринтера я уже поведал, так что перейдем прямо к делу.

В комьюнити поговаривали, что страсть Рода к публичным выступлениям в стиле проповедников Дальнего Запада далеко не случайна – то ли дед, то ли отец нашего героя окормлял паству где-то в Небраске или Оклахоме. В любом случае, Род не подкачал. Камлал он на славу. Здесь было все: и вздетые к небу руки, и перст указующий, и выя смиренно-скорбно склоненная, и голосовые модуляции от шепота до громозвучного хорала. При таком исполнении суть не важна, но что-то там было про кибербезопасность, мультистейкхолдеризм, далее везде.

Были и судьбоносные встречи, что «на полях», и неформальный обмен мнениями по широкому спектру представляющих взаимный интерес вопросов... Барбара цвела, Род выступал величаво, как четвертый из трех великих теноров, но при этом деловито, и улыбка не сходила с его лица.

Два дня пролетели незаметно (типовая фраза из школьного сочинения на все времена) и вот усталые, но довольные (оттуда же), мы катим в «Шарик», откуда Род улетает в... куда там улетают президенты ICANN (бог весть какие дали, но всегда по делу с «оконцовкой» в Лос-Анджелесе).

В Вип-зале Шереметьево полумрак и прохлада, и после дежурной чашки кофе я собираюсь откланяться, но Род останавливает меня властным движением руки.

- Леонид, - звучным, хорошо поставленным голосом, начинает он, - ты был с нами все эти дни («Ну, на самом деле, неполных два», - механически поправляю я его про себя), и твоя помощь была неоценима для успеха нашей миссии (президенты ICANN всегда разговаривают так – я даже знавал одного, который вместо слов «Я знаю» употреблял исключительно выражение «Я осведомлен»), которую я лично считаю настоящим прорывом и о которой будет в полной мере осведомлено (я же говорил!) наше глобальное комьюнити, - Барбара механически кивает головой в такт речи, - и потому в знак нашей благодарности я прошу тебя принять вот ЭТО.

С этими словами он лезет в карман и достает – честное слово! - рулончик туго скатанных купюр зеленого цвета, в которых и слепой бы безошибочно признал доллары.

За недостатком места в этой колонке для описания моих эмоций предлагаю читателю обратиться к той главе «Мастера и Маргариты», где представлены незабвенный Н. И. Босой и сверток баксов в вентиляции. Краем глаза я увидел, как побледневшая Барбара тихонько сползает по стенке. И не скажешь же: «Что вы себе позволяете?! Я же советский человек, комсомолец!» - или что-то в этом роде. Мысль металась лихорадочно, но чу! Вот оно спасение: со сгиба банкноты на меня искоса поглядывал Александр Гамильтон! И вот тут-то и пришло озарение: я гордо взглянул в лицо Роду и отчеканил твердо: «Род, в нашей стране ценят и берут как чаевые только Франклина!»

Изящный выпад достиг цели: Род вспыхнул, а скольжение Барбары вдоль стены замедлилось и краски начали возвращаться на ее лицо. Бросив взгляд на Барбару, Род как-то быстро и неразборчиво попрощался и исчез в глубине вип-зала, а за ним утицей проплыла и Барбара.

Ехал я домой победителем, хотя, признаться, и мелькала подленькая мыслишка: «А чего было и не взять?»

Вот так я преподнес достойный урок миру чистогана, двойных стандартов и сомнительных духовных ценностей, ибо мультистейкхолдеризм, любезный читатель, это не про деньги, а добровольное и бескорыстное служение комьюнити. Хотя рулончика того все равно жалко, честное слово...

P.S. Судьба нас снова свела с Родом спустя многие годы на одном интернет-саммите в далеком китайском городе Учжэне. Встретились как родные, даже обнялись, и с лукавым ленинским прищуром Род вдруг завел такую речь: «Леонид, я все вспоминаю, как ты тогда помог мне в Москве – до сих пор признателен тебе, и есть у меня для тебя особый подарок!» С этими словами он достает из кармана пиджака... раритетный серебряный доллар! Признаюсь, хоть и не нумизмат, но я был покорен – эта огромная монета всколыхнула что-то том-сойеровское в душе, и я взял ее с благодарностью (благо и мы с Родом уже не те, да и мир другой стал).

Вот она, эта монета. Любуйся, читатель, на профиль Статуи свободы и всякое там эгалите и либерте . А тем временем этим стуломмастер Гамбсэтой поучительной былью я заканчиваю свои интернет-повести Белкина. «Прощай, господинъ читатель; чрезъ сіи строки мы довольно спознались» ((с) Екатерина II).

Умные и опасные? (Вопросы безопасности IoT)

Андрей Робачевский

Вместе с ростом числа и типа устройств, подключённых к Интернету, растут и риски, связанные с безопасностью и защитой частной жизни. Это особенно справедливо для IoT – окружающие нас вещи могут быть использованы не по назначению и в преступных целях, их функциональность может быть изменена вплоть до отказа работы. В то время как умные объекты все теснее вплетаются в нашу жизнь, делая нас все более зависимыми от них, вопросы обеспечения защищённости систем IoT, персональных данных становятся как никогда актуальными и составляют важный элемент нашей собственной безопасности и защищённости частной жизни.

Недавние массированные атаки на сайт KrebsOnSecuirty и компанию Dyn вызвали шквал публикаций в прессе и опять привлекли внимание к IoT, на сей раз - к проблеме безопасности, связанной с использованием этих устройств. Эти распределённые атаки отказа в обслуживании (DDoS) сгенерировали трафик в несколько сотен гигабит в секунду (на сайт KrebsOnSecuirty был направлен поток в 660 Гбит/с) и включали около 1,5 миллионов устройств, в большинстве своём DVR и IP-камеры. Этот ботнет был рекрутирован и управлялся вредоносом под именем Mirai.

Хотя это далеко не первый случай такого рода, он позволяет увидеть новые тенденции и особенности новой стратегии массированных DDoS. В частности:

- В ботнет были рекрутированы не компьютеры, а специализированные устройства, такие как домашние маршрутизаторы, ресиверы цифрового телевидения, IP-камеры. Существенным преимуществом их использования для атакующих является режим постоянной работы, недостаточно зрелое программное обеспечение и отсутствие цикла его обновления.

- Существенный масштаб внедрения однотипных устройств. Это означает, что найденная уязвимость может сразу поразить миллионы объектов. До недавнего времени рекорды атакующего трафика ставились так называемым рефлекторными атаками с усилением. Упомянутые же атаки не использовали ни рефлекторов, ни усилителей и не нуждались в возможности спуфинга. Несколько миллионов устройств просто посылали трафик в одно и то же место.

Учитывая, что IoT является областью бурной инновации, когда функциональность и время выхода на рынок являются абсолютными приоритетами, можно предположить, что число уязвимостей «умных объектов» будет только расти. А принимая во внимание все растущий масштаб внедрения контроллеров, сенсоров и других автономных устройств, имеющих связь с Интернетом, поверхность атаки становится угрожающе обширной.

В чем же решение? Как предотвратить развитие негативной тенденции, когда объекты представляют опасность не только для их обладателя, но и для окружающей среды?

Не претендуя на знание ответов на эти вопросы, давайте начнем с того, что попробуем взглянуть на суть этих вещей. Начнем с вопроса – что такое IoT?

Что такое IoT?

Несмотря на то, что сегодня термин «интернет вещей» или IoT (Internet of Things) материализовался в коммерческих устройствах и системах и используется повсеместно, не существует общепринятого определения.

Например, некоторые определяют IoT как систему связанных между собой и подключенных к Интернету физических объектов с помощью миниатюрных встроенных сенсоров и проводных и беспроводных технологий для создания экосистемы всепроникающего компьютинга. Другие делают упор на встроенный интеллект в материальных объектах, позволяющий регистрировать и соответствующим образом реагировать на изменение их состояния и состояния окружающей среды.

Во многом это объясняется тем, что эта область нова и изменчива; отчасти же тем, что эта тема затрагивает социальные аспекты и имеет во многом как технический, так и философский характер. Иногда под IoT понимают любое специализированное компьютерное устройство, как, например, домашний маршрутизатор или камеру наблюдения.

Однако можно попробовать выделить несколько существенных элементов, общих для IoT.

Сенсоры и контроллеры. Звук, движение, наблюдаемые и окружающие объекты, освещенность, температура – эти и другие параметры определяют состояние «вещи» и ее взаимодействие с окружающей средой. Если от «вещи» предполагается действие - она также содержит контроллер – регулятор или управляющее устройство. Так, например, дверь может распознать визитера по биометрическим параметрам и открыть

замок, если они соответствуют хозяину жилища.

Отсутствующий пользовательский интерфейс. Большинство «вещей» получают информацию от сенсоров и управляющих серверов. Взаимодействие с пользователем часто происходит опосредованно, через управляющие серверы с интерфейсом порталов, или используя приложения, с помощью которых пользователь может получить информацию о статусе объектов и задать определенные установки. Умная лампочка осветительной системы Hue компании Philips управляется не привычным диммером или выключателем, а с помощью приложения, установленного на вашем смартфоне или планшете.

Программируемый интеллект. По существу, «вещь», подключенная к Интернету, – это материализованное приложение. И как для обычного приложения, ее функциональность может быть улучшена и расширена. Например, для осветительной система Hue существует более сотни различных приложений, позволяющих управлять освещением в доме с учетом времени дня, года, музыкой, текущей телевизионной программой и т.п. Подключив термостат Nest к Интернету вы получите доступ к дополнительной функциональности, например, определение оптимального режима в зависимости от прогноза погоды. Проще говоря – границами возможностей является ваше воображение.

Связность. Использование Интернета для обеспечения связности «вещей» позволяет им не только обмениваться информацией друг с другом или центральной системой. Интернет обеспечивает доступность вещей вне зависимости от вашего расположения. Вы можете управлять отопительной системой вашего дома из салона автомобиля, а климатической системой автомобиля – перед выходом из дома. Открытая коммуникационная инфраструктура Интернета позволяет таким системам обмениваться информацией с другими системами и информационными источниками. Так, система отопления может использовать данные прогноза погоды для выбора оптимального режима.

Автоматизация. Индустриальные сенсорные управляющие системы появились задолго до «интернета вещей». Уникальность сегодняшнего явления заключается в том, что оно принесло автоматизацию в массы, позволяя автоматизировать повседневные бытовые задачи. С другой стороны, благодаря открытой коммуникационной инфраструктуре, с помощью этих систем путем автоматизации могут быть решены широкомасштабные задачи – от интеллектуальной транспортной системы до интеллектуального городского освещения.

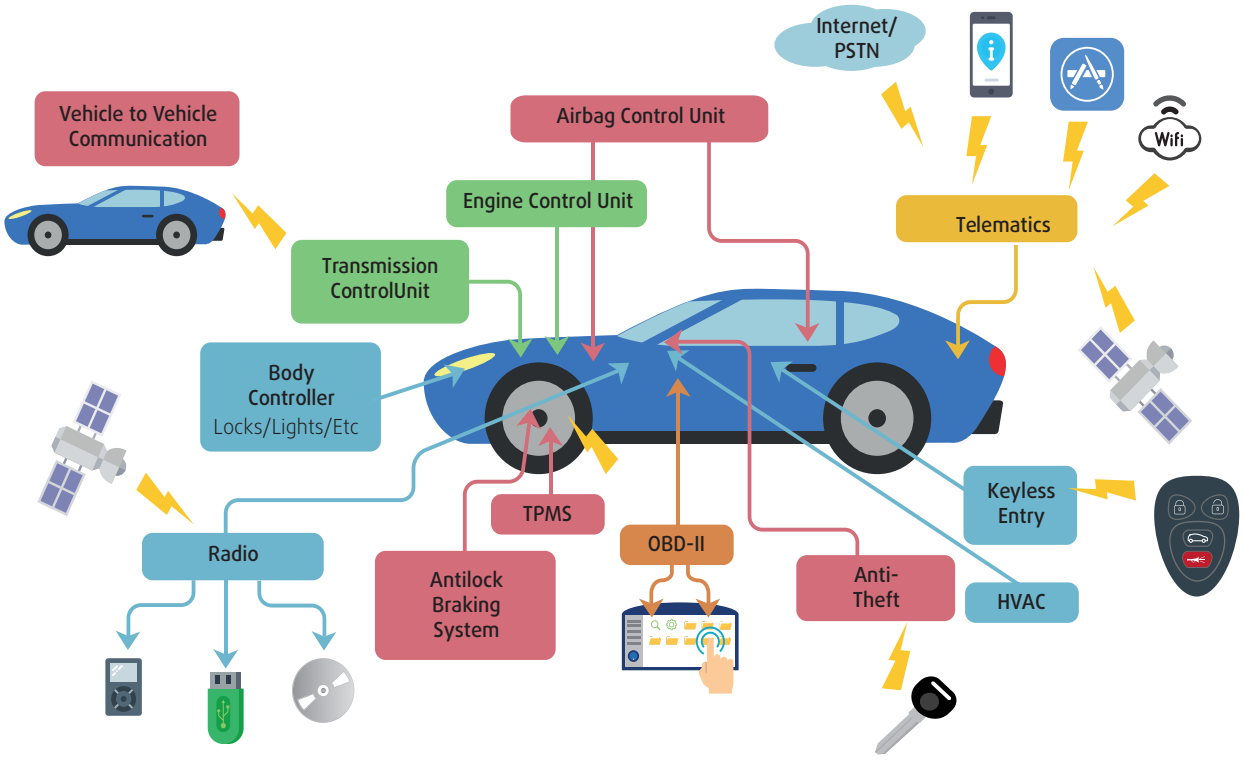
Умные системы: автомобиль, производство, дом

Для того, чтобы лучше увидеть типичные уязвимые места систем IoT и таким образом предложить общие рекомендации по безопасности, давайте рассмотрим несколько различных классов систем: системы автоматизации автомобилей, индустриальные системы и, наконец, системы домашней автоматизации.

Системы автоматизации автомобиля

Компьютеризация современного автомобиля происходит стремительными темпами. Цифровые контроллеры позволяют реализовать гораздо более широкий спектр функциональности, с большей эффективностью и гибкостью, чем механические системы. Однако интеграция новых технологий с многообещающими возможностями с коммуникационной архитектурой прошлого века представляет серьезные проблемы безопасности.

Рис. 1. Цифровые каналы ввода-вывода в современном автомобиле (Источник: Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S. et al. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces, http://www.autosec.org/pubs/carsusenixsec2011.pdf).



Дело в том, что взаимодействие между различными компонентами в автомобиле происходит с помощью так называемой

шины CAN (Controller Area Network). Эта архитектура была разработана в 1990 году и заменила километры проводов. К сожалению, архитектура шины не обеспечивает достаточной безопасности, в частности, сегментации и изоляции между подключенными к ней устройствами. Это означает, что переключатель фар потенциально имеет доступ к контроллеру тормозов, а развлекательная система – к топливной системе. С точки зрения безопасности, устройства развлекательных систем и систем поддержки не должны иметь возможность напрямую обмениваться данными с устройствами, обеспечивающими критические функции автомобиля.

Другим уязвимым местом CAN является отсутствие аутентификации подключенных устройств. Учитывая, что CAN является широковещательной средой, неавторизованное устройство, подключенное к шине, сможет передавать данные, которые могут быть восприняты другими устройствами. Например, модуль управления двигателем регулярно посылает в шину показания скорости вращения коленвала. Эти данные «слышат» все устройства CAN, но только тахометр реально их обрабатывает, обновляя показания. Тем не менее, шина не помешает другому устройству послать модифицированные данные скорости вращения, тем самым искажая показания тахометра.

Наконец, шина не поддерживает шифрования – все данные передаются открыто. Хотя протокол CAN и является проприетарным, это вряд ли является убедительным аргументом в пользу безопасности.

Очевидно, что сегодняшний анализ рисков фундаментально отличается от видения 80-х годов прошлого века. Тридцать лет назад для использования перечисленных уязвимых мест атакующему требовалось бы физически подключиться к шине и потратить некоторое время на декодирование проприетарного протокола обмена данными между устройствами. Сегодня ситуация фундаментально отличается. Появление телематических устройств, поддерживающих протоколы Wi-Fi, Bluetooth, 3G/4G и широко используемых в современных развлекательных и навигационных системах, ключей зажигания с удаленным управлением, различных устройств, отслеживающих окружающую среду (например, парковочный ассистент, адаптивный круиз-контроль), существенно увеличивают поверхность атаки. Насколько «открыта» система управления современного автомобиля, показано на рис. 1.

Сегодня атакующему достаточно обнаружить уязвимое место в одном из перечисленных устройств, чтобы получить неограниченный доступ к CAN со всеми вытекающими отсюда возможностями. Например, группа исследователей CAESS (Center for Automotive Embedded Systems Security) убедительно показала, что получив доступ к CAN, атакующий сможет отключить тормоза, включить тормоза на отдельных колесах, выключить двигатель, фальсифицировать показания спидометра и т.п. (см. http://www.autosec.org/pubs/cars-oakland2010.pdf).

Насколько реальны эти угрозы, свидетельствуют случаи атак на серийные автомобили, например, удаленная атака на Jeep Cherokee, продемонстрированная исследователями Miller и Valasek и широко освещенная в печати. Кстати, этот случай является иллюстрацией еще одной особенности рождающегося IoT. Зачастую устройства IoT не имеют **возможности автоматического обновления программного обеспечения** с целью закрытия уязвимых мест. Учитывая продолжительный срок жизни многих устройств, отсутствие такой функциональности представляет существенный риск. Компания Fiat Chrysler вынуждена была отозвать 1,4 миллиона машин для обновления программного обеспечения. Учитывая неудобства такой операции для владельцев, можно предположить, что для значительной части автомобилей уязвимость осталась незакрытой.

Индустриальные системы

Эволюция автоматизированных систем управления (АСУ) прошла путь от закрытых систем с проприетарными устройствами и протоколами к многоуровневой архитектуре со все большим использованием стандартных IT-компонентов и, наконец, к новой растущей тенденции внедрения технологий IoT.

Стоимость и расширенная функциональность являлись основными побудительными причинами перехода к более стандартной IT-архитектуре и компонентам. Этот переход имел последствия для безопасности – система уже не могла рассматриваться как полностью изолированная, уязвимые места стандартных компонентов были более явными. Однако для АСУ этого поколения было возможно обеспечить достаточную изоляцию от окружающей среды, включая физическую защиту. Количество компонентов было относительно ограниченным, а связь с внешней коммуникационной инфраструктурой, в частности, с Интернетом, не являлась требованием и либо хорошо контролировалась, либо полностью отсутствовала.

Возможность внедрения миниатюрных датчиков и контроллеров практически во все компоненты физического производственного процесса таит в себе выгоды, от которых трудно отказаться. В первую очередь – это существенное усиление надежности системы и обеспечение превентивного обслуживания. Сбор показателей состояния различных компонентов системы в реальном времени, сравнение данных от идентичных устройств, пороговые индикаторы износа – все это позволяет удешевить производственный процесс и значительно повысить его качество.

Однако применение IoT в АСУ часто несет в себе серьезные проблемы безопасности. Во-первых, вся **система становится более открытой**. Требования производительности и объема трафика зачастую превышают возможности корпоративной VPN, для раскрытия полного потенциала во многих случаях необходимо обеспечить связь со внешними службами и т.п. Во-вторых, эти проблемы усугубляются тем, что традиционные компоненты АСУ не защищены по определению, будучи разработаны для предполагаемой полностью закрытой и контролируемой среды.

Домашняя автоматизация

Появление IoT в домашней сети началось собственно с момента появления самой домашней сети. Домашний маршрутизатор можно считать первой домашней вещью, следуя наиболее общему определению: устройство, автономно выполняющее свои функции и подключенное к Интернету. И именно домашние маршрутизаторы сразу стали (и до сих пор являются) легкой добычей для рекрутёров ботнетов.

Однако истинный IoT многие связывают с компьютеризацией существующих окружающих вещей, таких как осветительные приборы, термостаты, дверные замки и т.п. Эта область развивается стремительно и довольно хаотично. В отличие от систем автомобильной автоматизации и АСУ, где имеет большее место отраслевое регулирование и стандартизация, область домашней автоматизации – это поистине «дикий запад". Неуклонно уменьшающаяся цена и размеры сенсорных и исполнительных устройств позволяют компьютеризировать и подсоединить практически любую вещь. Есте-

ственно, инновационный потенциал в этой среде огромен. За умными термостатами и лампочками следуют дверные замки, сенсоры движения и детекторы дыма. Однако для раскрытия возможностей домашних IoT необходимо, чтобы устройства не только могли общаться с «удаленным мозгом» - облачными услугами и управляющим приложением, - но и между собой, образуя скоординированную систему умного дома. Такой совместимости у умных вещей пока нет.

В то же время, наряду с появлением единичных умных устройств, можно наблюдать формирование «экосистем», интегрирующих операционные системы устройств, коммуникационные протоколы и облачные услуги приложений. Большинство этих экосистем центрированы вокруг ведущих производителей или консорциумов. Например, Google продвигает операционную систему для умных объектов Brillo и коммуникационную платформу Weave, Apple занята разработкой платформы HomeKit, Qualcomm – Alljoyn, а Samsung рекламирует платформу SmartThings.

Эти платформы являются своего рода виртуальными операционными системами для умных объектов, позволяя централизовать предоставление в том числе функций безопасности (таких, как аутентификация, контроль доступа, изоляция и т.п.). В отсутствие таких платформ производителям умных объектов приходится самостоятельно обеспечивать требуемую защищенность устройств и реализовывать облачные приложения. К сожалению, чаще всего эти вопросы не решаются на должном уровне, уступая место требованиям функциональности и стоимости.

В среде домашней автоматизации несколько факторов усугубляют проблему безопасности:

- «Умный дом» является **открытой системой**. Более того, несмотря на развитие упомянутых платформ, внедрение IoT в домашнем хозяйстве как правило производится неспециалистами, без долгосрочного планирования, приводя к созданию эклектичной системы с компонентами и архитектурой различных производителей и **отсутствием единой политики безопасности**.

- Основной упор делается на функциональность устройств и системы в целом. Учитывая желание минимизировать стоимость устройств, это зачастую приводит **к недостаточному вниманию к вопросам безопасности**. Рядовой потребитель просто не может оценить степень защищенности устройств и связанные с его использованием риски и вынужден закрыть на эти аспекты глаза для получения желаемого функционального результата.

- Все больше окружающих нас вещей используют Интернет для расширения своей функциональности. Становиться все сложнее приобрести «вещь», которая бы не подключалась к Интернету.

- Масштаб внедряемых устройств IoT существенен. Более того, **однотипность этих устройств значительно усиливает эффект обнаружения уязвимости** в одном из них.

- Многие сенсоры производят **сбор весьма конфиденциальных данных**, предоставляющих информацию о наших привычках, поведении, нахождении, могут прослушивать наши разговоры и делать видеозаписи. Например, телевизор SmartTV компании Samsung имеет возможность управляться голосовыми командами. Проблема заключается в том, что для этого телевизор пересылает услышанную речь в Sasmung для анализа на предмет возможных команд. Разумеется, эти данные зачастую содержат не только команды, но и просто подслушанный разговор. Насколько хорошо защищены эти данные и кто имеет к ним доступ?

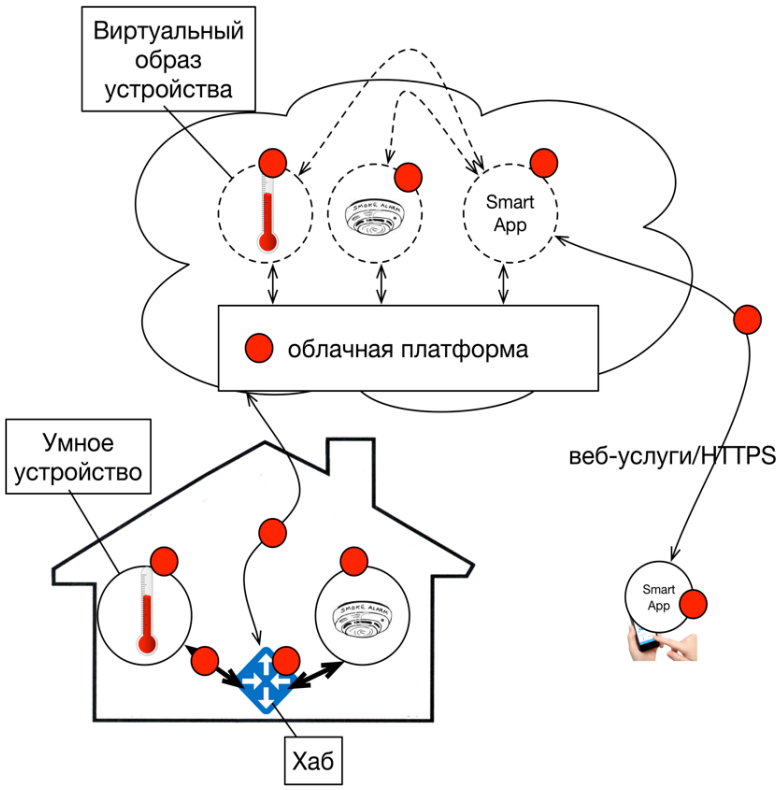
Модель угроз

Чтобы понять риски, связанные с IoT, давайте рассмотрим архитектуру такой системы. В качестве примера возьмем наиболее общий вариант домашней автоматизации. Уязвимые места системы показаны на рис. 2 красными кругами.

Рассмотрим каждый из компонентов системы в отдельности.

- «Умное» устройство. Устройства IoT значительно различаются как по своей функциональности, так и по доступным ресурсам - от специализированного компьютера до миниатюрного сенсора или контроллера. Первая категория устройств является наиболее привлекательной для рекрутёров ботнетов благодаря следующим свойствам: широкая функциональность и значительные вычислительные возможности, непосредственное подключение к домашней сети и Интернету с широкой полосой пропускания, работа в режиме постоянного включения и отсутствие взаимодействия с пользователем. Для этой категории наиболее часто

Рис. 2. Уязвимые места экосистемы домашней автоматизации IoT.



используются операционные системы общего назначения – преимущественно Linux - с известными и постоянно обнаруживающимися новыми уязвимыми местами. Широко известны случаи использования "умных" холодильников для рассылки спама или медиаресиверов для создания мощной атаки отказа в обслуживании. Для второй категории используются специализированные ОС (RIOT OS, Tizen, Windows 10 for IoT, Mbed OS). Скомпрометированные устройства этой категории могут использоваться для атаки на самого владельца – сбор данных, изменение функциональности, а также для атаки на другие устройства сети. Наряду с низким качеством программного обеспечения некоторых устройств, особенно в области безопасности, основными проблемами являются **недостаточно сильная защита доступа и отсутствие механизма автоматического обновления программного обеспечения**.

- Коммуникационные протоколы. Устройства IoT по определению непосредственно или опосредованно (например, через шлюзы) подключены к Интернету. При этом имеет смысл выделить беспроводную связь в качестве отдельного компонента.

  - Беспроводная связь. Радиосвязь может являться уязвимым местом, когда атакующий находится на небольшом расстоянии от устройств. Это может быть и атака отказа в обслуживании путем глушения сигнала или атака посредника (Man-in-the-middle, MITM), если атакующему удается подключиться к беспроводной сети.

  - Протоколы верхних уровней (транспорт и приложение). Недостаточная защита на этом уровне, например, отсутствие надежной аутентификации и защиты данных, может быть использована для атаки MITM, со всеми вытекающими последствиями. Наиболее уязвимыми местами коммуникационных протоколов являются **отсутствие надежной аутентификации и шифрования данных**.

- Шлюз или хаб. Шлюз обеспечивает обмен данными между устройствами, использующими различные протоколы, например, ZigBee и Bluetooth. Также шлюз обычно обеспечивает опосредованное подключение этих устройств к Интернету и доступ к облачным услугам. Проблемы, которые я перечислил относительно устройств с достаточными ресурсами, существуют и для шлюзов. В некоторых архитектурных решениях, как, например, HomeKit, шлюз берет на себя также расширенные функции, обычно предоставляемые облачными услугами – сбор, анализ и хранение данных, программы автоматизации, а также обеспечивает удаленный доступ к функциям домашнего IoT. Также шлюз зачастую обеспечивает защиту подключенных к нему устройств, поэтому **обеспечение безопасности для этого элемента чрезвычайно важно**.

- Облачные услуги. Поскольку возможности большинства «умных» объектов ограничены, вычислительные ресурсы для поддержки процессов автоматизации и управления устройствами, сбора и хранения данных, а также предоставление удаленного доступа обеспечиваются удаленными серверами, наиболее типично размещенными в облаке. Такой подход позволяет также управлять не изолированными устройствами, а их ансамблем – например, координируя работу осветительной и отопительной системы, системы безопасности, датчиков движения и т.п.

  - Программное обеспечение платформы. Облачная платформа обеспечивает создание (регистрацию) и управление устройствами IoT. После регистрации устройства платформа создает виртуальный образ физического объекта IoT, обеспечивая вычислительные ресурсы и память, необходимые для его работы и автоматизации. Облачная платформа является своего рода виртуальной операционной системой для приложений IoT. Она обеспечивает необходимый уровень абстракции, предоставляя стандартный API взаимодействия с устройствами, независимо от их физической реализации и производителя. Разумеется, физические объекты или шлюзы должны поддерживать протоколы платформы.
    Платформа играет критическую роль в обеспечении безопасности, так же, как мобильная ОС определяет уровень безопасности смартфона. **Регистрация устройства и приложения, контроль доступа к различным функциям устройства – от реализации этих функций зависит защищенность всей системы**. Если приложение может получить большие привилегии, чем было задекларировано, например, к дополнительным функциям или другим устройствам системы (см., например, «Security Analysis of Emerging Smart Home Applications» Earlence Fernandes, Jaeyeon Jung, and Atul Prakash, https://iotsecurity.eecs.umich.edu/), это может иметь существенные последствия для безопасности самих владельцев IoT-систем.

  - Пользовательские облачные приложения. Так же, как и в мире смартфонов, пользователь имеет возможность установить приложения различных разработчиков для управления своими «умными» устройствами. Как и в случае со смартфонами, существует **риск установки вредоносных приложений**. Аутентификация программного обеспечения от разработчиков с репутацией, а также возможное сканирование на предмет вредоносных функций могут помочь в уменьшении этих рисков.

- Приложения удаленного доступа. Эти приложения предоставляют пользовательский интерфейс взаимодействия с облачными пользовательскими приложениями для управления объектами IoT. Наиболее типичным является использование веб-API. При этом клиентом является приложение, установленное на смартфоне или планшете (или даже на компьютере), а сервисная часть обслуживается облачным приложением. **Использование незащищенных протоколов**, например, HTTP вместо HTTPS, и **недостаточно прочная система аутентификации** являются наиболее уязвимыми элементами этого компонента.

В поисках решений

Как хорошо видно из анализа угроз системы IoT, проблема безопасности требует комплексного решения. Не существует магической технологии или практики, которые бы надежно защитили всю систему. Чем открытее система, тем больше игроков должны быть вовлечены в решение проблемы – от производителей оборудования IoT, разработчиков программного обеспечения до провайдеров облачных структур и самих владельцев «умных» устройств. Более того, недостаточная защищенность хотя бы одного из элементов может существенно ослабить безопасность системы в целом.

Принимая во внимание анализ угроз и уязвимости системы, показанные на рис. 1, можно сформулировать ряд комплексных мер, направленных на усиление защищенности системы в целом.

Защищенность устройств IoT

Начнем с собственно устройств IoT – с умных замков, термостатов, лампочек, видеокамер и т.п. Хотя, как я уже отмечал, возможности таких систем сильно различаются, все же можно сформулировать несколько общих рекомендаций:

1. Надежная система доступа и аутентификации, основанная на криптографии.

Требование удобства подключения устройства зачастую берет верх над требованиями безопасности и нередки случаи использования стандартных логинов/паролей типа admin/admin, даже без требования их изменения после первоначальной инициализации устройства в сети. В процессе инициализации устройства и его аутентификации во многих случаях играют важную роль локальные шлюзы или облачные платформы.

2. Криптографическая защищенность программного обеспечения (ПО).

Хорошей практикой является использование системы PKI для подписания кода и проверки его аутентичности. Эта функциональность также является основой для защищенного обновления ПО.

3. Обновление ПО на протяжении всего жизненного цикла устройств.

Как известно, практически не существует ПО без ошибок. Это значит, что рано или поздно в устройстве могут быть обнаружены новые уязвимые места. Единственным способом уменьшения этого риска является возможность обновления ПО версией с закрытыми найденными уязвимыми местами. Разумеется, при условии, что разработчик ПО реагирует на найденные уязвимости созданием необходимых заплаток и своевременно выпускает обновленную версию ПО. Чрезвычайно важно, чтобы обновление могло осуществляться автоматически, без участия владельца устройств. Критическим является защищенность всего процесса.

Этот вопрос является непростым, а его решение таит множество подводных камней. Более подробное обсуждение проблем и дополнительных рекомендаций в этой области можно найти в отчете семинара Internet of Things (IoT) Software Update (IoTSU) (https://tools.ietf.org/html/draft-farrell-iotsu-workshop), организованного IAB.

Защита передаваемых данных и коммуникационной инфраструктуры

1. Криптографическая защита данных.

Эта мера является общепринятым способом решения проблемы защиты данных. Она является критической для исключения прослушивания и спуфинга другими скомпрометированными устройствами, а также атак проигрывания (replay attack). Особенно для беспроводных сетей важно обеспечение шифрования также и на канальном уровне.

2. Отсутствие критических зависимостей от связности.

Защиту коммуникационной инфраструктуры зачастую трудно обеспечить. Например, связь в беспроводной сети может быть прервана с использованием радиоглушения. Важным здесь является сохранение системой критической функциональности даже при отсутствии связи. Например, владелец должен иметь возможность открыть дверь, а термостат должен продолжать выполнять базовую температурную программу.

Защита системы

Как обсуждалось выше, в общем случае объекты IoT формируют своего рода “ансамбль” и являются частью сложной системы с внешними компонентами. Хотя наиболее простые формы, как например, фитнес-гаджет – смартфон, будут продолжать существовать, автоматизация окружающей среды – дома, офиса, города или производственного процесса – подразумевает все более тесную интеграцию отдельных компонентов и умных объектов.

В «системном» аспекте можно выделить две основных области, играющие существенную роль в обеспечении безопасности, - локальная сеть IoT и облачная платформа. Замечу, что в ряде случаев услуги приложений предоставляет локальный хаб. В этом случае рекомендации для платформы относятся к нему.

Защита локальной сети

Фундаментальный принцип сквозной связности (end-to-end principle) в Интернете предполагает, что интеллект сосредоточен на оконечных устройствах, а основной функцией сетей является пересылка пакетов от источника к получателю, невзирая на их природу, тип адресатов и т.п. Нарушение этого принципа вводит невидимые зависимости, разъедающие совместимость и прозрачное взаимодействие сетей, тем самым уменьшая инновационный потенциал Интернета в целом.

Однако в случае IoT мы вряд ли можем продолжать рассматривать локальную сеть в качестве прозрачной нейтральной среды. Принцип сквозной связности по-прежнему применим, но сегодня это скорее действует между локальной сетью и облаком. Появление облачных услуг и IoT существенно меняет наше представление об оконечном устройстве в контексте этого принципа.

В отношении локальной сети, помимо перечисленных рекомендаций по защищенности коммуникационной инфраструктуры, главным вопросом является **возможность определения политики безопасности и обеспечение ее соблюдения**. Проблемой является то, что обычный пользователь вряд ли может и хочет самостоятельно определить эту политику, поэтому эта задача должна по возможности быть решена без его участия.

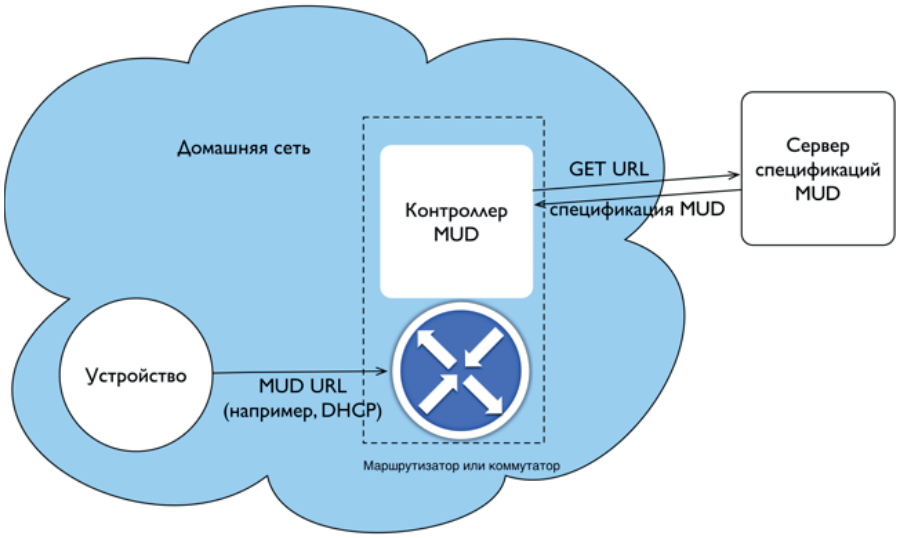
Сегодня типичной политикой безопасности в домашней сети является блокирование входящих соединений и пакетов с подложными адресами. Последнее обычно является положительным последствием использования NAT, а не сознательным использованием практики BCP38 (https://datatracker.ietf.org/doc/rfc2827/), и известны случаи, когда ПО NAT позволяет отдельные случаи спуфинга.

Однако устройства, подключаемые к домашней сети, должны иметь возможность общения со внешним миром, что зачастую требует разрешения определенных внешних соединений и открытия соответствующих портов на домашнем маршрутизаторе. Для автоматизации этой задачи широко используется технология UPnP (https://ru.wikipedia.org/wiki/UPnP). К сожалению, протокол UPnP не обладает необходимыми функциями безопасности, и позволяет вредоносному ПО открыть порты на домашнем маршрутизаторе для входящего трафика. Протокол UPnP не обеспечивает, в частности, аутентификацию устройств и предоставляет ограниченные возможности спецификации трафика устройства.

Одним из возможных решений данной проблемы является создание дополнительной спецификации устройства, детально

описывающей требуемую политику безопасности для конкретного устройства – перенаправление портов, допустимые источники трафика и его характеристики. Эта спецификация может быть использована для реализации этой политики на устройствах безопасности или домашних маршрутизаторах. Проект этого решения под названием Manufacturer Usage Description (Спецификация использования от производителя) или MUD (https://tools.ietf.org/html/draft-ietf-opsawg-mud) в настоящее время обсуждается в IETF.

Рис. 3. Архитектура MUD (Источник: «Manufacturer Usage Description Specification», https://tools.ietf.org/html/draft-ietf-opsawg-mud).



Суть его заключается в следующем. В процессе инициализации устройство передает URL, где расположен соответствующий файл MUD. Контроллер MUD, который может являться частью домашнего маршрутизатора или экрана безопасности, скачивает файл с сервера и соответствующим образом конфигурирует списки доступа и т.п. Предполагается, что файл MUD предоставляется производителем устройства и защищен электронной подписью, позволяющей контроллеру проверить подлинность спецификации. Принцип работы этого подхода схематично показан на рис. 3.

Безопасность облачной платформы

Облачная платформа является виртуальной операционной системой системы IoT. Она обеспечивает программный интерфейс доступа и управления "умными" объектами, создавая и обслуживая их виртуальные копии. Поэтому от того, насколько защищены эти функции, зависит безопасность системы в целом. В этой области можно выделить несколько важных моментов.

1. Контроль доступа к ресурсам устройств.

Подобно мобильным приложениям для смартфонов, приложение объявляет набор ресурсов, к которым оно хотело бы получить доступ. Платформа же предоставляет список устройств с этими ресурсами. Соответственно, пользователь получает возможность выбрать, к каким устройствам и их возможностям данное приложение может иметь доступ, тем самым авторизуя приложение. Однако зачастую система доступа, обеспечиваемая платформой, недостаточно детальна. Например, исследователи Мичиганского университета и Miscrosoft Research обнаружили, что в платформе SmartThings, когда пользователь авторизует приложение для доступа к устройству, он тем самым предоставляет доступ ко всем возможностям этого устройства (https://iotsecurity.eecs.umich.edu/). Для иллюстрации уязвимости такого подхода они использовали приложение для мониторинга статуса зарядки батареи для автономных устройств, в частности, замка входной двери. Авторизуя это, с виду невинное и полезное приложение, пользователь открывает ему доступ также к другим возможностям, как, например, открытие и закрытие замка. Злоумышленники могут использовать эту возможность для маскировки вредоносного ПО под видом безобидных утилит. Однако, как отмечают исследователи, создание более детальной системы может сделать пользование системой более сложной, требуя от пользователя дополнительных операций по авторизации. Как известно, желание поскорее установить понравившееся приложение зачастую пересиливает требования безопасности, и пользователь игнорирует все предосторожности. Здесь важно найти правильный баланс.

2. Надежная идентификация приложений, защищенная система распределения событий.

Использование системы событий довольно распространённый подход во многих платформах. Во многом здесь применима аналогия шины CAN, используемой в автомобильной индустрии. Аутентификация приложений для избегания спуфинга и изоляция событий для предотвращения доступа неавторизованными приложениями – два необходимых элемента защищенности платформы.

3. Верификация приложений «магазинами приложений» (app stores).

Так же, как и в экосистеме мобильных приложений, возможность предварительной проверки приложений на предмет наличия вредоносного кода, как, например, атак внедрения кода (code injection), превышения привилегий и т.п., позволит создать более защищенную экосистему.

Заключение

Значительный рост рисков, связанных с проблемами безопасности и защиты частной жизни, связан не с IoT как таковым, а с тем, что цифровой мир и Интернет все плотнее вплетается в нашу жизнь. Все больше персональных и конфиденциальных данных хранятся в "облаках", все более зависимы мы от умных полезных устройств, приложений, Интернета. IoT безусловно делает рассмотренные выше проблемы более значительными.

Защищенность системы - не бинарное состояние. Степень безопасности представляет собой широкий спектр. Насколько хорошо защищена система, также зависит от характера угроз. Все эти факторы меняются во времени. Будем надеяться, что по мере того, как отрасль становится более зрелой, безопасность IoT будет обеспечиваться на адекватном уровне.

Интернет бесконтрольных вещей

Дэвид Плонка (David Plonka)

Недавно на интернет вещей (Internet of Things, IoT) обрушился вал критики в связи с рядом серьезных инцидентов. Интеллектуальные телевизоры, DVR и веб-камеры были названы источниками одних из самых масштабных DDoS-атак за всю историю Интернета. Но что же собой представляют те самые вещи, то есть класс устройств, образующих интернет вещей? Наконец, говоря об измерениях IoT, следует не забывать об операционных последствиях и соображениях приватности. Могут ли требования приватности или анонимности защитить пользователей IoT от вредных воздействий?

Недавно на интернет вещей (Internet of Things, IoT) обрушился вал критики в связи с рядом серьезных инцидентов[1]. Интеллектуальные телевизоры, DVR и веб-камеры были названы источниками одних из самых масштабных DDoS-атак за всю историю Интернета[2]. Но что же собой представляют те самые вещи, то есть класс устройств, образующих интернет вещей? Эти «вещи» – устройства, которые (1) спроектированы с зависимостью от Интернета, причем раньше подобное устройство от него не зависело, и (2) быстро изготовлены, однотипно сконфигурированы и установлены по всему Интернету. Оба эти аспекта важны как с инженерной, так и с операционной точки зрения. IoT-устройства – это не просто потребительская электроника. Сама их конструкция предполагает работу с ресурсами Интернета. Мало того, обычно нас не информируют о появлении в Интернете хостов нового типа. Поскольку очень быстро появилось и продолжает появляться множество однотипных устройств, связанные с IoT проблемы быстродействия, надежности и безопасности разрастаются крупнее и быстрее, чем когда-либо раньше.

IoT поднимает ряд вопросов для нашего сообщества: Насколько велик интернет вещей? Каков его охват? Как можно это проверить?

В настоящее время IoT нам неизвестен в двух аспектах. Во-первых, практически отсутствуют измерения IoT. Сколько имеется устройств и какого типа? С какой скоростью разрастается IoT? Сколько могут прослужить IoT-устройства? А во-вторых, какие стандартные методы конструирования и эксплуатации могли бы ограничить негативное воздействие на быстродействие, надежность и безопасность?

Мы только начали отвечать на некоторые из этих вопросов и вплотную заниматься насущными проблемами IoT.

13-летнее исследование IoT: 2003-2016 годы

Проблемы, связанные с IoT-устройствами, в общем, не новы — в 2003 году произошла случайная DDoS-атака, связанная с IoT, конкретно с сотнями тысяч изделий компании Netgear, подключенными к разным фрагментам Интернета. Эти устройства являлись устройствами IoT в двух аспектах:

- Хотя ранее коммутаторы и маршрутизаторы сами по себе не зависели от Интернета, эти устройства были сконструированы так, чтобы синхронизировать свои часы с сервером NTP (Network Time Protocol), расположенным в Университете штата Висконсин в Мэдисоне. IP-адрес этого сервера NTP был жестко запрограммирован в прошивке.
- Всего за несколько месяцев было изготовлено и продано несколько сот тысяч таких устройств, распространившихся по всему миру.

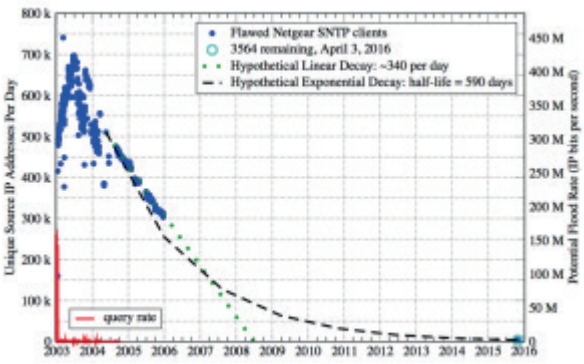
На рис. 1 изображен роутер Netgear модели MR814, выпущенный около 2003 года. Это и еще три вида устройств Netgear считают «виновниками» случайного всплеска трафика.

Реализация клиента SNTP на этих устройствах содержала ошибку, из-за которой они опрашивали сервер NTP раз в секунду, пока не получали ответ, что в результате время от времени приводило к внезапным потокам трафика в сотни тысяч пакетов в секунду. Поскольку проблему обнаружили до того, как количество подключенных к Интернету устройств достигло пика, а некоторые из дефектных устройств используются и по сей день, возникла уникальная возможность измерить некоторые аспекты IoT. С помощью моих коллег по университету мы построили график примерного количества дефектных SNTP-клиентов, наблюдавшихся с использованием NTP-сервера Университета штата Висконсин с 2003 по 2016 год.

Рис. 1. Беспроводной маршрутизатор netgear mr814 для кабельных/dSl сетей 802.11b.

На рис. 2 показано появление (2003–2004) и (последующее) исчезновение SMTP-клиентов за 13-летний период, очевидно показывающие рождение и смерть этих IoT-устройств. Всего было изготовлено около 700 тысяч дефектных изделий, пока в том же 2003 году дефект не устранили.

Рис. 2. Число дефектных SNTP-клиентов Netgear, 2003–2016 г.



Эти измерения показывают, что некоторые IoT-устройства служат очень долго, и что ни линейная, ни простая экспоненциальная модель не соответствует эмпирическим наблюдениям с удовлетворительной точностью. Некоторые устройства IoT остаются в эксплуатации больше десятилетия, обременяя своими дефектами многие тысячи пользователей и сетей.

Результатом этого инцидента стал ряд инженерных и эксплуатационных рекомендаций [3], закрепленных в нынешнем виде в RFC 4085 (BCP 105) [4]. Для получения дополнительной информации об инциденте с Netgear посетите сайт http://pages.cs.wisc.edu/~plonka/netgear-sntp/ или прочтите статью «Интернет старых и неуправляемых вещей» (The Internet of Things Old and Unmanaged) [5].

Контроль за IoT в наши дни

Сегодня свои инициативы в области IoT есть у IAB (Internet Architecture Board), IETF и IRTF (Internet Research Task Force). Например, семинар Internet of Things Software Update (IoTSU) 2016 рассматривал вопрос, как лучше всего подойти к изменению кода и конфигурации устройств IoT, изложив свои выводы в отдельной статье [6].

Что до измерения IoT, то исследовательская группа IRTF MAPRG (Measurement and Analysis for Protocols Research Group) запросила любые измерения IoT, прошлые и нынешние. И то исследование, которое мы обсуждали выше, было представлено и записано [7] на собрании MAPRG в ходе IETF 96 в Берлине, по итогам чего произошла дискуссия о требованиях, которые могли бы стимулировать измерения IoT.

В связи с выработкой измерений IoT возникает ряд вопросов. Какие имеются реальные счетчики или иные метрики для устройств IoT? Кто в этом заинтересован? Какие возможны виды измерений? Как быть с соображениями приватности? И как в этом участвует IPv6?

Заинтересованных лиц на самом деле много. Изготовителям наверняка хочется знать, как их изделия распространяются по цепочке поставок, вводятся в эксплуатацию и затем выводятся из нее. Провайдерам услуг требуется управление IoT-устройствами и оценка рисков. Пользователям устройств, владельцам и заказчикам наверняка потребуется обнаружение или поиск утерянных устройств и аудит, возможно, с целью информирования страховщиков или следующих покупателей об IoT-устройствах, которые, например, управляют жилым домом.

Что касается видов измерений IoT и того, что возможно и что нет, есть строки World Wide Web User-Agent и адреса управления доступом к медиа в Ethernet, которые помогают выявлять некоторые устройства IoT, но их можно маскировать или фальсифицировать. Поэтому остаются вопросы: возможна ли аутентификация IoT-устройств и какие есть реалистичные возможности для измерения времени работы IoT-устройств или определения их времени жизни?

Наконец, говоря об измерениях IoT, следует не забывать об операционных последствиях и соображениях приватности. Могут ли требования приватности или анонимности защитить пользователей IoT от вредных воздействий? Если IoT-устройства живут долго и (как сейчас) далеко не всегда используют IPv6, то они представляют собой очень серьезную и все осложняющуюся проблему исчерпания адресного пространства в IPv4, решить которую можно, например, через IPv6.

Нежелательный трафик и уязвимости, вызванные дефектами IoT-устройств, требуют особого внимания и сконцентрированных усилий в сообществах для исследования, стандартизации и эксплуатации. Если оставить интернет вещей бесконтрольным (в прямом и переносном смысле), то Интернету грозят беспрецедентные проблемы производительности, надежности и безопасности, которые были предсказаны еще десятилетие назад, но до сих пор не обезврежены.

Источник: The Internet of Things Unchecked, http://www.ietfjournal.org/the-internet-of-things-unchecked/

Сноски

1. http://thehackernews.com/2016/09/ddos-attack-iot.html

2. http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

3. https://tools.ietf.org/html/rfc4085#page-4

4. https://tools.ietf.org/html/rfc4085

5. http://pages.cs.wisc.edu/%7Eplonka/iotsu/IoTSU_2016_paper_25.pdf

6. https://tools.ietf.org/html/draft-farrell-iotsu-workshop-01

7. https://www.youtube.com/watch?v=DkAS_Ht6J6U#t=38m50s

IT-конференции

Ольга Александрова-Мясина

Этот выпуск посвящен интернету вещей. Модная тема! Скоро каждый из нас, сидя на кухне, сможет в период одиночества и тоски поговорить со своей микроволновкой о жизни. Раньше, до начала эпохи интернета вещей, поговорить по душам можно было только с телевизором, а теперь диапазон собеседников явно расширяется. И тема «общительной кофеварки» поднималась чуть ли не на каждой отраслевой конференции, форуме или семинаре, которые проводились в 2016 году. Охватить все, конечно же, не удалось, но получилось побывать на нескольких мероприятиях, на мой взгляд, самых интересных и насыщенных.

Сентябрь выдался холодным и мерзким, поговаривали, что бабье лето отменили, и пришлось распределять рабочий график так, чтобы было тепло и сухо, как в известной рекламе. Чтобы не тосковать из-за вечно плохой погоды, сходила на большой форум, который был назван просто и незатейливо – «Интернет вещей». Сюда собрались представители государства, крупнейших интернет-компаний, эксперты в области IT. Обсудили и цифровую экономику, и кибербезопасность, и многое другое. Но все же посвящен он был, в первую очередь, стратегии развития российского проекта операционной системы для интернета вещей, разработкой этой ОС занимается ассоциация «Тайзен.Ру», которая и организовала форум. Поэтому разговор здесь получился довольно узкопрофессиональный, для специалистов.

Для не-специалиста в области ОС, которым я являюсь, было скучно. Знаете, это как раз тот самый случай, когда в диалогах понимаешь одни предлоги. Еще я себя так чувствую на ENOG, оказываясь рядом с группой бородатых программистов, и (иногда) на Пиринговом форуме MSK-IX. Радует одно: я в команде организаторов, и всегда есть, чем заняться. Но обо всем по порядку.

Второй форум, связанный с интернетом вещей, на котором мне удалось побывать, прошел 15 октября на площадке Digital October в Москве. Это был первый в России мультиотраслевой Форум индустриального интернета, куда приехали не только представители IT и интернет-компаний, но и те, кто работает в отраслях, далеких от информационных технологий. Но мы же все понимаем, что интернет вещей – это то, чем люди пользуются и будут пользоваться в повседневной жизни, поэтому и интересно было бы узнать, как на него смотрят люди из других отраслей.

К сожалению, на форуме индустриального интернета этого не получилось – в основном выступали и рассказывали о перспективах развития интернета вещей все те же интернет-гуру. Так что можно сделать вывод, что пока что о том, что такое интернет вещей и зачем он нужен, знают лишь специалисты из нашей информационно-коммуникационной среды. Как будто это я уже где-то писала, да? А всё потому, что любые новинки на рынке на первом этапе всегда начинают продвигаться узкой группой единомышленников. В 2000 году я работала в платежной системе. Как-то мы пришли с президентом нашей компании к одному директору банка и предложили установить в отделениях его банка платежные терминалы. И знаете, что он нам ответил? Ответ был таким: «Вы какие-то сказки мне рассказываете, а надо делать проекты для реальной жизни...» Через семь лет платежные терминалы стояли в каждом подземном переходе. Потому что идея была на поверхности, и думающие люди подхватили ее и сделали. Здесь же как: кто первый встал, того и тапки. И кому-то тогда повезло.

Потом наступил ноябрь, и ФРИИ провел Форум перспективных технологий, где наконец-то (!) можно было услышать голоса не только айтишников, но и практиков, занимающихся внедрением и (главное!) применением интернета вещей на местах. В форуме приняли участие представители Минкомсвязи, Минпромторга, Минэнерго, руководители предприятий различных отраслей промышленности, малый и средний бизнес. Ну и, разумеется, IT-компании, вендоры, разработчики ПО и операторы связи, системные интеграторы.

Участникам форума было представлено исследование «Индустриальный (промышленный) интернет вещей. Мировой опыт и перспективы развития в России. Оценка влияния на качество жизни граждан и экономическое развитие страны», проведенное аналитиками J'son & Partners Consulting. В исследовании были проанализированы мировые тенденции и потенциал развития индустриального интернета вещей в России, роли участников экосистемы IoT, рассмотрены аспекты организационно-технологической трансформации бизнеса, приведены примеры реализации промышленного интернета. А после исследования участники стали делиться реальным опытом применения интернета вещей в повседневной жизни. Оказалось, что интернет вещей уже вокруг нас, хотя мы об этом еще не догадываемся. Тут и «умные» мусорные баки, и «разумные» лампочки, и интеллектуальные кофеварки – обо всем этом рассказали участники конференции. Как отмечали все, разговор на форуме получился живой и интересный, со множеством практических кейсов.

Обратно я ехала на метро и думала об умных вагонах в скором будущем! И еще представляла, как мы все будем расплачиваться через сетчатку глаза, куда будет встроен чип, и летать на космолетах, как в советском детском фильме «Гостья из будущего».

- У вас говорящий заяц? – вдруг услышала я голос рядом и не сразу поняла, о чём речь. Сзади стоял нетрезвый дяденька и тыкал пальцем в мой меховой брелок, который болтался на рюкзаке.

Кстати, да, он попал в точку! И все игрушки скоро будут разговаривать и развлекать наших детей, да и нас самих. Вот тогда-то они скажут всё, что о нас думают, и нам будет стыдно.

Но вернемся к конференционной жизни нашей отрасли. В самом начале декабря нас ожидал Пиринговый форум – моё любимое отраслевое мероприятие. Форум традиционный и традиционно очень приятный. В очередной раз убедилась, что выбор площадки – это 90% успеха любого мероприятия. И Центр международной торговли на Пресне как всегда был на высоте. Кроме того, в этом году была очень насыщенная программа – пришлось даже с утра, до официального открытия форума, делать два параллельных потока по темам, которые особенно интересовали многих участников: медиалогистика и сетевые технологии. Кстати, программа форума готовилась на основе мнений постоянных участников сообщества MSK-IX. Члены программного комитета обсуждали возможные темы на встречах с инициативной группой, общались с российскими и зарубежными коллегами, а итоговый рейтинг тем сформировали на основе голосования в сообществе Пирингового форума в социальных сетях.

Официальное открытие началось с выступления генерального директора MSK-IX Елены Ворониной, которая поприветствовала участников и представила динамику деятельности компании в цифрах. «Большие данные – повседневная реальность для нашей компании», – отметила Елена Воронина. За уходящий год сеть MSK-IX передала 4,5 эксабайт трафика, а количество запросов к платформе DNS MSK-IX, поддерживающей более шести миллионов доменных имён, достигло 1,8 триллиона.

Технический директор MSK-IX Александр Ильин рассказал о развитии сети и сервисных платформ компании. «Наряду с внедрением услуг обмена телесигналами, расширением магистралей и модернизацией роут-сервера, MSK-IX уделяет большое внимание удобству пользования сервисами. Новый клиентский кабинет – наглядная иллюстрация этой стратегии», – отметил Александр Ильин.

Коммерческий директор MSK-IX Евгений Морозов анонсировал новый зал MSK-IX на ММТС-9, вводимый в эксплуатацию в апреле 2017 года, а также узел доступа к MSK-IX в Риге. Затем состоялось награждение партнёров года MSK-IX: награды получили операторы "Мегафон", "Раском" и RETN.

Ежегодно на Пиринговый форум приглашаются представители зарубежных точек обмена трафиком. Винсент Райс (NL-IX) представил доклад о стратегии распределённого IXP, направленной на организацию связности для бизнес-клиентов, а Ричард

Петри (LINX) поделился опытом разделения программных и аппаратных плоскостей в сложной сети IXP.

Александр Котов (Vodafone Group) в своем выступлении рассказал о том, как устроена фильтрация контента и как эволюционируют практики ограничения Интернета в разных странах. В качестве примеров в сравнении с Россией докладчик привел Китай, Иран, США и некоторые европейские страны.

Тема сетевой безопасности и противодействия DDoS-атакам стала финальной темой форума. Сессия началась докладом Михаила Суконника (Radware) о разнице между публичным восприятием и реальной технической подоплёкой инцидентов безопасности в Интернете. На круглом столе «Безопасность в киберпространстве», который провел Андрей Колесников (Ассоциация интернета вещей), ведущие российские эксперты поделились практическим опытом противодействия кибертерроризму. «Профильные сетевые компании должны помочь широкому кругу владельцев интернет-сетей понять проблематику защиты от DDoS», – отметил Кирилл Малеванов (Selectel). Муслим Меджлумов ("Ростелеком") обратил внимание на ответственность производителей CPE-устройств за создание потенциальных угроз. «В защите от атак нужно переходить от защиты отдельных клиентов к защите Интернета в целом. Для этого сообщество операторов связи должно взаимодействовать теснее», – подчеркнул Александр Лямин (Qrator Labs).

А потом официальная, научная, техническая и практическая части закончились, и мы пошли пробовать вкусные закуски под звуки скрипки. И было у меня ощущение приятной легкости – когда позади что-то такое, о чем сильно беспокоишься. Я стояла за фуршетным столиком, ковыряла изящной вилочкой в салате и думала о том, что это предновогоднее мероприятие, где подводились итоги прошедшего года, стало и для меня неким рубежом, где я сама подводила итоги последних семи лет - потому что я готовилась покинуть доменный рынок и изменить ему с другим. «Пойдемте, графиня, нас ждут великие дела!» - сказал мне коллега. Он еще не знал, как был близок к истине!

Календарь событий: 2017 год

Международные события

6-8 февраля
NANOG 69,
Вашингтон, США

Североамериканская группа сетевых операторов (The North American Network Operators Group, NANOG) является одной из самых активных профессиональных ассоциаций в области сетевой архитектуры, конфигурации и технического администрирования сетей в Интернете. NANOG имеет активный список рассылки и проводит конференции три раза в год. http://nanog.org

20 февраля - 2 марта
APRICOT 2017,
ХоШиМин, Вьетнам

APRICOT - крупнейшая ежегодная конференция по интернет-технологиям, собирающая более 800 участников азиатского региона и Океании. Здесь обсуждаются вопросы внедрения и использования интернет-технологий, технического администрирования сетей и инфраструктурных услуг Интернета. Особое внимание уделяется образовательной деятельности – конференция начинается неделей "мастерских" по администрированию различных компонентов инфраструктуры Интернета. Совместно с APRICOT проводится встреча APNIC, организуемая региональной интернет-регистратурой, отвечающей за этот регион. Здесь помимо технических вопросов обсуждаются политики администрирования адресного пространства. https://2017.apricot.net/

26 февраля - 1 марта
NDSS,
Сан-Диего, США

Симпозиум NDSS - это ежегодная конференция, организуемая ISOC с целью способствования обмену информацией между исследователями и практиками по безопасности сетей и распределенных систем. Целевая аудитория включает в себя тех, кто заинтересован в практических аспектах компьютерной безопасности, с акцентом на реальные разработки и внедрения.
https://www.internetsociety.org/events/ndss-symposium/ndss-symposium-2017

11-16 марта
ICANN 58,
Копенгаген, Дания

Встречи ICANN проводятся три раза в год в различных регионах земного шара для того, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. https://meetings.icann.org/en/copenhagen58

26-31 марта
IETF 98,
Чикаго, США

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов в области Интернета. В основном работа в IETF проходит в многочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100). Три раза в год IETF проводит недельные совещания, на которые приезжают разработчики протоколов, инженеры и операторы со всего мира (в среднем около 1200 участников из более 50 стран мира).
https://www.ietf.org/meeting/upcoming.html

8-12 мая
RIPE 74,
Будапешт, Венгрия

Встречи RIPE проводятся два раза в год и собирают более 500 участников для обсуждения вопросов политики распределения номерных ресурсов (IP-адресов и номеров автономных систем) в зоне обслуживания RIPE NCC, сотрудничества, а также технических вопросов, связанных с маршрутизацией, DNS, связностью, измерениями и инструментарием. Встреча длится 5 дней и начинается с двухдневной пленарной программы, за которой следуют несколько параллельных сессий заседаний рабочих групп. https://ripe74.ripe.net/

В России

4 апреля,
Новосибирск

JBreak 2017
Единственная сибирская технологическая Java-конференция для опытных разработчиков. 4 апреля 2017 состоится второй JBreak, который соберет под своей крышей более 400 разработчиков. Конференция объединяет не только Java-экспертов со всей России, но и привлекает спикеров со всего мира. https://2017.jbreak.ru/

5-7 апреля,
Сочи

IT Summit 2017
Ежегодная встреча лидеров IT-индустрии - владельцев и первых лиц крупнейших российских и мировых IT-компаний, руководителей инфраструктурных организаций (аналитических компаний, фондов, кластеров), госструктур, влияющих на условия бизнеса. http://it-summit.ru/

6-7 апреля,
Нижний Новгород

Digital Оттепель 2017
Ежегодное мероприятие областной отрасли интернет-технологий, включающее в себя две параллельные конференции: для руководителей и заказчиков с одной стороны, и для специалистов Digital-сферы с другой. http://digitalnn.ru/

14-15 апреля,
Ульяновск

Стачка 2017
«Стачка» – международная профессиональная IT-конференция, которая уже пятый год подряд собирает в Поволжье лучших российских и западных экспертов из мира информационных технологий. https://expomap.ru/conference/stachka-2017/

В Москве

9 февраля,
Москва

Рынок облаков в России 2017
Тенденции российского облачного рынка, IaaS, PaaS или SaaS, какой должна быть облачная стратегия компании, IT-инфраструктура в облаке и перспективы виртуализации рабочих мест, помогают ли облака реально экономить затраты? http://events.cnews.ru/events/rynok_oblakov_v_rossii.shtml

23 марта,
Центр Digital October

Cloud & Digital Transformation 2017
Международная конференция в области IT и бизнеса для руководителей IT-департаментов, менеджеров по развитию бизнес-направлений и представителей финансовых департаментов крупнейших российских предприятий, ведущих мировых и отечественных экспертов и аналитиков. http://www.cloudmobility.ru/

12 апреля,
Москва

Data Centers, Cloud & IT 2017
Цифровая трансформация – можно ли к ней подготовиться, сколько нужно ЦОД, чтобы Россия могла идти в ногу с цифровой революцией, инициативы по импортозамещению IT-технологий, где и в какие сроки будут строить новые дата-центры, варианты трансформации ИТ для дата-центров. http://www.iotclouddata.center/

19-21 апреля,
Пансионат «Лесные дали»

Российский интернет-форум (РИФ+КИБ 2017)
Традиционно мероприятие проходит в формате выездного подмосковного трехдневного мероприятия, состоящего из конференции, выставки и внепрограммных активностей. В программе представлены секционные заседания, круглые столы, а также мастер-классы и мини-секции. http://2017.russianinternetforum.ru/

20 апреля,
Москва

Большие данные в России 2017
Как развивается мировой рынок больших данных, удалось ли большим данным покорить российскую промышленность, транспорт и государственный сектор, как решить проблему кадрового голода в этой сфере и каковы перспективы развития рынка больших данных в России в 2017 году? https://expomap.ru/conference/bol-shie-dannyie-v-rossii-2017/


MSK
IX
WWW.MSK-IX.RU
+7 (495) 737-9295
«Московский Internet Exchange» — крупнейшая
в России точка обмена интернет-трафиком (IX)

Интернет изнутри

2017