«Умные» коровы,

или Как создавать устройства для «Интернета вещей», которые будут работать без отказов

Никто не пытается создать продукт для «Интернета вещей» (IoT), заранее обреченный на неудачу, но провалы порой случаются. История IoT изобилует такими случаями, начиная с «умных» замков, которые очень быстро взламывались хакерами, и заканчивая историей об отзыве 440 000 «умных» датчиков дыма и CO.

Черил Аджулини (Cheryl Ajluni)

Когда такой провал единичен и легко устраняем заменой одного продукта другим, его влияние на имидж и доходы компании может быть минимальным. Но картина меняется, если неудачные продукты IoT установлены в местах, куда доступ затруднен, или используются в суровых условиях. Если с такими устройствами возникают проблемы, прежние успехи компании уже не спасут ее репутацию.

И сегодня это очень реальный сценарий, поскольку распространение IoT набирает обороты, а устройства «Интернет вещей» находят применение в ряде очень интересных приложений в местах с ограниченным доступом. Идеальным примером является «умное» сельское хозяйство, в котором датчики IoT используются в различных приложениях, предназначенных для повышения продуктивности и устойчивости сельскохозяйственного производства. Они предназначены для контроля уровня влаги в почве и отслеживания роста сорняков, поддержания оптимальных условий в инкубаторе и даже контроля здоровья коров мясных пород.

Рис. 1. В «умную» корову имплантировано устройство IoT для контроля ее поведения и мониторинга ряда важных параметров, например температуры тела. Активные IoT-метки используются круглые сутки для отслеживания активности и здоровья животных

В «умном» животноводстве датчики IoT вживляются под кожу коровы в нескольких местах. Эта операция требует минимального хирургического вмешательства и проводится под анестезией (рис. 1). После вживления ожидаемый срок службы датчиков составляет три года. В течение этого срока они отслеживают поведение животного и ряд показателей жизнедеятельности, причем важнейшим из них является температура, по которой можно судить о здоровье коровы.

На словах это просто, но, поскольку датчики находятся внутри животного, их нелегко извлечь, если что-то пойдет не так. Большой вес коров и их привычка чесаться боками о различные предметы создают еще одну проблему. Что случится, когда 800-килограммовая корова решит почесаться тем местом, где находится датчик? Не будет ли он поврежден?

Правильное решение этого вопроса отличает удачный IoT-продукт от неудачного. Успешные продукты IoT рассчитаны на безотказную работу не только во время испытаний в идеальных лабораторных условиях, но и в реальном мире со всеми его сложностями.

Ниже перечислены пять факторов, способных вызвать отказы устройств IoT, а также некоторые советы о том, как их избежать.

Перегруженность сети и колебания нагрузки

После включения нового устройства IoT может оказаться, что в непосредственной близости работают сотни подобных приборов. На одной «умной» ферме может находиться стадо крупного рогатого скота (с несколькими датчиками в каждом животном), датчики для измерения параметров почвы, растений и окружающей среды, дистанционного мониторинга животных и сбора статистики, а также фермерские

дроны, не говоря об устройствах IoT, которые фермер может носить с собой. Перегруженность информационной сети способна повлиять на работу устройств. В результате резкого увеличения сетевого трафика устройства IoT будут все время передавать данные повторно. Это может вызвать их отказ или ускоренную разрядку батарей.

Во избежание этих проблем производители должны испытывать IoT-устройства в сетях с трафиком, который ожидается в реальных условиях. Подобное тестирование следует проводить с имитацией различных типов передаваемых данных, таких как потоковая передача видео или голоса.

Помехи

На «умной» ферме возможна большая плотность установки устройств IoT, функционирующих в одних и тех же переполненных диапазонах частот. Это значительно увеличивает вероятность перекрестных помех. Многие из данных устройств неспособны обнаруживать друг друга, не говоря о совместном использовании частотных каналов, что может привести к непредсказуемым последствиям.

Во избежание этого необходимо протестировать их взаимную совместимость. Это поможет производителям определить помехоустойчивость устройств и обеспечить их работоспособность в сложной радиоэлектронной обстановке (РЭО). Устройства IoT следует протестировать на способность работы с реально используемыми уровнями сигналов, скоростями передачи и протоколами.

Сложности роуминга

Беспроводные устройства IoT часто меняют свое местоположение. Это может превратиться в проблему, если в них не реализованы надежные алгоритмы роуминга, позволяющие избежать задержек и сбоев передачи данных. Отключение всего на несколько секунд может привести к потере ценной информации. Перегруженность и помехи оказывают значительное влияние на то, насколько хорошо работают алгоритмы роуминга, что делает испытание в условиях реальной сети критическим для предотвращения отказа устройства. В сценарии с «умной» фермой имплантация устройств IoT обретает смысл, только если фермер имеет непрерывный доступ к данным.

Одним из способов предотвращения сбоев является проверка поведения устройств IoT при роуминге в сложных условиях. Также рекомендуется разработать антенну устройства таким образом, чтобы оно могло справляться с объемом и контентом реального трафика.

Функциональная совместимость с сетевой инфраструктурой

Сегодня устройство IoT действует исправно. А на следующий день оно начинает сбоить или вообще прекращает работать. Скорее всего, проблема заключается не в самом устройстве, а в том, что пользователь обновил прошивку точек беспроводного доступа. Небольшое изменение в сетевой инфраструктуре превращает прекрасно функционирующее устройство IoT, например имплантированный датчик, в нечто не распознаваемое целевой средой. К счастью, эффективную защиту от таких сбоев может обеспечить набор тестов на соответствие всем функциям протокола беспроводной передачи данных, а не определенной их части.

Нарушения безопасности

Любое устройство IoT может быть уязвимым для атаки, даже если оно вживлено в корову (рис. 2). Иногда хакеров интересуют собираемые данные. В других случаях они пытаются использовать уязвимость устройства для проникновения в сеть. Это может произойти, когда устройство находится в роуминге или под воздействием помехи. Помеха может вызвать перегрузку устройства и возникновение состояний отказа, что приведет к длительным задержкам соединения и сделает его уязвимым для взлома. Остановить подобный сценарий можно с помощью набора тестов с возможностью имитации поведения при роуминге в сложной РЭО.

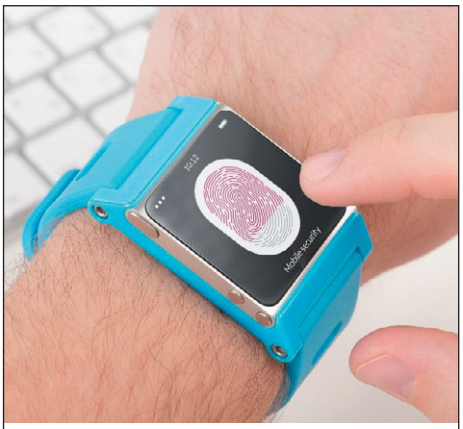

Рис. 2. Хакеры могут взломать любое конечное устройство IoT, такое как смарт-часы, прибор медицинского мониторинга или даже имплантированный в корову датчик

Увеличение спроса на технологии IoT заставляет производителей уделять все большее внимание надежности предлагаемой продукции. Для компаний, стремящихся к созданию безотказных продуктов IoT, крайне важно полностью понять условия эксплуатации своих изделий и организовать правильные испытания для оценки их способности противостоять всем возможным вредным факторам. И, будь то датчики для «умных» коров, приборы медицинского мониторинга или что бы то ни было еще, компании, для которых главным является надежность их продукции, обязательно выйдут в лидеры растущего рынка IoT. ■