Катастрофы и их последствия:

возможности IoT

«Интернет вещей» (IoT) — технология, потенциально представляющая собой новый виток технологической революции, обещающая громадные выгоды в экономической сфере и способная поднять жизненный уровень человечества на новую ступень. Однако IoT также несет в себе угрозу для частной жизни и должен обеспечивать беспрецедентно высокий уровень безопасности. Стандартизация устройств IoT и протоколов их взаимодействия между собой — это ключевое условие, позволяющее реализовать наметившиеся экономические выгоды и обеспечить надежное и безопасное взаимодействие всех компонентов возникающей нео-информационной среды.

Филип А. Лаплант (Phillip A. Laplante)

Джеффри Воас (Jeffrey Voas)

Нэнси Лаплант (Nancy Laplante)

Первод: Алексей Гречишников

В настоящее время уже существуют сотни тысяч, если не миллионы, приложений и устройств IoT. Некоторые из них способны взаимодействовать друг с другом, другие — нет, а в каких-то случаях попытка установить такое взаимодействие может закончиться самым непредсказуемым образом. Таким образом, выработка и соблюдение единого стандарта «Интернета вещей» крайне важна. Однако встает вопрос: что же именно такое IoT и какие стандарты являются определяющими для него? Чтобы проиллюстрировать те сложности, которые возникают при работе IoT, мы рассмотрим конкретные примеры, а также предложим пути преодоления возникающих при этом проблем.

IoT и стандарты: терминология

В настоящее время понятие IoT трактуется по-разному, и единого четкого определения на этот счет не существует.

Например, Европейский исследовательский кластер дает следующее определение IoT: «Динамическая глобальная инфраструктура, способная к самоконфигурации, основанная на стандартных протоколах взаимодействия, физические и виртуальные устройства (вещи) которой персонифицированы, используют интеллектуальный интерфейс и бесшовно интегрированы в информационную сеть» [1].

Определение ITU (агентство ООН по информации и технологиям связи) звучит так: «Глобальная инфраструктура информационного сообщества с усовершенствованными службами взаимодействия между совместимыми между собой компонентами (физическими и виртуальными) и основанная на существующих и еще разрабатываемых информационных и коммуникационных технологиях» [2].

В соответствии с определением Консорциума Всемирной Сети (Worldwide Web Consortium), IoT «включает в себя датчики и исполнительные механизмы, физические объекты, их местоположение, и даже людей. В своей основе это ролевая функция веб-технологий по содействию в разработке приложений и услуг для различных устройств и их виртуального представления» [3].

В «Википедии», «Технопедии», «Вебопедии» и других подобных справочных ресурсах Интернета можно найти и иные определения. Однако следует отметить, что во всех них будет присутствовать следующее: «различные системы, взаимодействующие между собой определенным образом и подключающиеся к другим подобным системам, находящимся в пределах радиуса действия».

Типичными приложениями, относящимися к IoT, являются, к примеру, «умный дом», «умный город», транспортная система, здравоохранение, объекты критической инфраструктуры, такие как системы генерации и передачи энергии. Элементы IoT могут быть найдены повсюду — в промышленных объектах и правительственных учреждениях, в обычном доме. OASIS (Organization for the Advancement of Structured Information Standards) предсказывает, что датчики IoT будут присутствовать в «каждом мобильном устройстве, каждом автомобиле, каждой двери, каждой комнате, в любой части любого устройства — в каждой кровати, каждом стуле, каждом браслете, каждом доме, офисе, больнице, служебном помещении, в каждом городе и деревне — повсюду на Земле» [4]. Но все это в будущем. В настоящее время IoT — это, по сути, множество разобщенных систем, некоторые из которых являются экспериментальными, довольно мелких по сравнению с теми задачами

и надеждами, которые на них возлагаются, и, в основном, предназначенных для контроля за различными системами функционирования зданий («умный дом»).

Роль IoT в сценарии ликвидации последствий катастрофы

Несмотря на отсутствие согласованного определения, в настоящее время разрабатываются различные стандарты для самых разнообразных устройств IoT, связи, сетей, приложений. Вследствие этого возникает острый вопрос о совместимости данных стандартов. Важность этого можно продемонстрировать на примере гипотетической системы аварийного реагирования на чрезвычайные ситуации. Например, в США, по замыслу, такая система будет представлять единый центр обработки данных, которые должны быть совместимы не только с действующими стандартами IoT, но также со стандартами Национального института стандартов и технологий (NIST), Управления по охране труда (OSHA), Федерального агентства по управлению в чрезвычайных ситуациях (FEMA), требованиями Закона об охране и ответственности за информацию, полученную в результате медицинского страхования (HIPAA), и др.

Катастрофы и стихийные бедствия могут быть вызваны погодой, являться результатом несчастных случаев, а также преднамеренных действий людей, например таких, как физический и биологический терроризм. Одним из самых печально известных таких случаев является катастрофа 11 сентября 2001 г., когда действия террористов привели к захвату самолетов и последующему разрушению башен Всемирного торгового центра в Нью-Йорке и атаке здания Пентагона (Вашингтон, округ Колумбия). Эта трагедия произошла сравнительно недавно, и существует множество документов, фотографий, видео, интервью непосредственных участников этих событий — выживших и тех, кто принимал участие в спасении людей и ликвидации последствий этой страшной катастрофы.

В Нью-Йорке столкновение первого захваченного террористами самолета с Северной башней привело к пожару, сопровождавшемуся сильным задымлением. Многие из тех, кто в это время находился в здании, пострадали: часть людей погибла, кто-то выжил, получив ранения различной степени тяжести. Вскоре последовало столкновение второго самолета с Южной башней, повлекшее за собой новые человеческие жертвы. С момента первой атаки и в течение последующих дней службы спасения эвакуировали раненых, разыскивали тела погибших в развалинах. В те дни множество людей пытались найти своих родных и близких в больницах и моргах, искали хоть какой-нибудь их след в новостных репортажах или рассказах очевидцев. К сожалению, многим помочь не удалось. В результате этой террористической атаки погибли более 2700 человек и почти 7000 были госпитализированы [5].

Посмотрим, что могло бы быть, если бы средствами IoT было возможно четко определить местонахождение людей в башнях и развалинах и установить, может ли человек самостоятельно покинуть место катастрофы или же ему требуется срочная эвакуация на транспортном средстве. Если бы такое было возможно, это кардинально улучшило бы положение. Пострадавшие были бы уверенно идентифицированы, скорее получили бы необходимую помощь, их эвакуация происходила бы значительно быстрее, и привлеченные силы и средства применялись бы более эффективно. Прибывшие в пункт сортировки получали бы, например, браслет с бар-кодом или иное активное или пассивное средство идентификации, регистрировались бы в системе, и все дальнейшие перемещения пострадавшего могли бы быть с легкостью отслежены. Данные о жертвах и их перемещениях, поступившие в систему, были бы доступны на специальном сайте. Также в системе фиксировались бы данные о тех, кто скончался от полученных травм.

Описанное выше не является чистой фантастикой: такие системы уже существуют. Тиа Гао (Tia Gao) и ее коллеги разработали прототип системы мониторинга пациентов в реальном времени. Такая система «интегрирует жизненно важные признаки, датчики местоположения, AdHoc-сети, электронные записи пациентов, а также использует технологии веб-портала для удаленного мониторинга состояния пациентов, в том числе тех, кто еще не был эвакуирован с места катастрофы» [6].

Наличие устройств слежения и мониторинга крайне положительно сказалось бы на скорости принятия решений и эффективности оказания помощи жертвам теракта в Нью-Йорке. Они были бы полезны как для тех, кто оказывал помощь, так и для пострадавших, причем не только на месте совершения теракта, но и на всех последующих стадиях операции. Такого рода системы и устройства также уже были разработаны. Например, более 10 лет назад командой во главе с Конрадом Лоринцем (Konrad Lorincz) была создана система, названная CodeBlue, которая при произошедшей катастрофе осуществляет динамическую интеграцию сенсоров датчиков и иных беспроводных устройств [7]. Этой командой также была разработана MoteTrack — технология на основе радиосвязи, позволяющая определять местоположение находящихся в зданиях спасателей и жертв катастрофы.

При проведении спасательных операций также важным является наличие оборудования и устройств для отслеживания перемещений. Локальные сети больниц уже осуществляют между собой обмен информацией о наличии, например, запасов крови для переливания. Применение IoT позволит улучшить и расширить возможности такого обмена. Единый центр помощи будет координировать перемещение пострадавших и распределение средств оказания помощи и медикаментов. В настоящее время разрабатывается единый стандарт по обмену такой информацией. В качестве одного из прототипов рассматривается IEEE's Big Data New Initiative [8]. В нем предполагается использование семейства стандартов для портативных медицинских устройств IoT IEEE 11073 [9].

Однако все предполагаемые преимущества при использовании IoT могут быть реализованы только при условии полной и надежной совместимости всех используемых устройств, включая персональные устройства слежения, которые могут быть у пострадавших, — например, мобильные телефоны или другие носимые гаджеты, подключающиеся к системам IoT.

Согласование стандартов

Помимо стандартизации определения IoT и процессов взаимодействия входящих в него систем и компонентов, также необходимо создать стандарты, на основе которых устройства IoT будут объединяться между собой в различные конфигурации. Такие проекты также разрабатываются в настоящее время. К примеру, LPWAN (Low Power Wide Area Network — энергоэффективная сеть дальнего радиуса действия). Данная спецификация объединяет беспроводные устройства с питанием от аккумуляторов в региональные, национальные и глобальные сети и предусматривает наличие безопасной двунаправленной связи, мобильность и локализацию услуг для обеспечения непрерывного взаимодействия между входящими в сеть смарт-устройствами. Существуют и иные, стандарты, например Sigfox или LTE [10]. Они также необходимы, однако весьма важным является совместимость друг с другом и способность к совместной работе различных стандартов, особенно в тех условиях, когда это является критически важным, например при катастрофах и стихийных бедствиях.

NIST (Национальный институт стандартов и технологий) распространил черновой вариант межведомственных рекомендаций — Interagency Report (IR) 8063 [11], в которых описываются основные понятия для IoT и согласовываются стандарты работы. В нем говорится, что ключевыми особенностями систем IoT являются связь, вычисления и обработка сигналов датчиков, а также даются определения базовых компонентов распределенной сети, называемых примитивами, и описываются классы элементов как базис для всех систем IoT. Предполагаются следующие примитивы [11]:

- сенсоры (датчики): электронные устройства по оцифровыванию физических показателей (например, температуры, ускорения, веса, звука и так далее);
- агрегаторы (преобразователи): программные компоненты, которые на основании заложенных математических алгоритмов осуществляют преобразование и группировку поступающих «сырых» данных в промежуточные данные, пригодные для дальнейшей обработки;
- каналы связи: среда, в которой осуществляется передача данных (например, прямое соединение по USB, беспроводное, проводное, акустическое между сенсорами, агрегаторами, каналами связи, триггерами принятия решения или внешними утилитами;
- внешние утилиты (eUtility): программные или аппаратные обработчики и сервисы, предоставляющие вычислительные мощности, которые могут потребоваться агрегаторам IoT;

- триггеры принятия решений: правила, работающие по принципу «Что, если» и выдающие конечные результаты, необходимые для успешной работы в соответствии с требованиями и спецификациями конкретной системы IoT.

Элементами, играющими главную роль в повышении степени совместимости и совместной работе IoT, будут являться:

- среда функционирования: «вселенная» (рабочее пространство) всех примитивов данной сети, в которую объединены все устройства и которая, по существу, является рабочим профилем IoT;
- цена: затраты денежные и временные (скорость реагирования системы), которые будут присущи данной IoT с точки зрения повышения надежности и безопасности работы;
- географическое расположение: место, где физически расположены и работают сенсоры и внешние утилиты, или место, где они были произведены;
- пользователь: человек или организация, которым принадлежат конкретные сенсоры, каналы связи, агрегаторы, триггеры принятия решения или внешние утилиты;
- идентификаторы устройства (device ID): уникальные идентификаторы конкретного сенсора, канала связи, агрегатора, триггера принятия решения или внешней утилиты;
- мгновенный снимок (snapshot): кратчайший временной интервал, используемый для синхронизации событий, вызванных сенсором, каналом связи, агрегатором, триггером принятия решения или внешней утилитой.

Системы IoT, разработанные и построенные с учетом данных рекомендаций, обеспечат надежную совместную работу, при этом они могут быть сформированы из различных компонентов, служб и коммерческих продуктов IoT.

Смешанный стандарт

Итак, согласование стандартов — это поиск пути для уменьшения или даже исключения различия в работе двух или даже большего количества «разношерстных» систем и приведение их к некоему единому целому. В то же время существует другой подход к проблеме совместимости: так называемый смешанный стандарт. Он предполагает выбор для работы только тех компонентов из разных стандартов, комбинация которых наилучшим образом совместима в конкретной системе IoT [12]. Поскольку NIST IR 8063 определяет базовые компоненты для любой IoT, это может быть использовано как основа для нового (смешанного) стандарта, являющегося комбинацией двух (или более) других (рисунок).

Например, предположим, что A и B являются стандартами IoT, включающими в себя устройства и системы, подобные тем, которые рассматриваются в сценарии преодоления последствий катастрофы. Примитивы и элементы, соответствующие NIST IR 8063, могут быть извлечены из A и B, преобразованы в промежуточное представление и затем транслированы в смешанный стандарт, который можно назвать A/B.

Нерешенные проблемы

Стандартизация необходима для всех устройств и систем IoT, особенно тех из них, которые работают в критически важных условиях, таких как ликвидация последствий катастрофы. Согласованная работа поможет скоординировать работу спасательных бригад, пожарных, медперсонала, которые прибывают к месту происшествия из разных точек. Объединение их усилий с помощью устройств IoT позволит наиболее эффективно использовать людские и материальные ресурсы. Однако остается нерешенной масса вопросов.

Рассмотрим, к примеру, что может получиться, если работа каких-либо из систем IoT (принадлежащих службе перевозки пострадавших, расположенных в соседних зданиях и сооружениях или даже тех, которыми располагает служба предупреждения об опасных ситуациях) будет не согласована с другими устройствами и службами глобальной сети, вызывая сбой в их функционировании. С одной стороны, это может оказаться даже полезным (изолированная система может сработать быстрее: например, пострадавший — сотрудник ФБР, и доступ к его личным данным может быть ограничен системой безопасности этого учреждения; а изолированная система просто не знает о таком ограничении — ***прим. перев.***), но, с другой стороны, такое положение дел может привести к дополнительным проблемам (например, службы обеспечения безопасности могут блокировать информацию от других источников). Что произойдет, если какая-либо второстепенная система окажет непреднамеренное воздействие на критически важную, и это приведет к катастрофической ошибке? А как быть со стандартами безопасности?

Вероятно, лучше, если некритические системы не будут требовать специализированных протоколов для совместной работы с критическими системами IoT, и информация, поступающая от них, будет доступна даже в самое тяжелое время — в момент катастрофы.

* * *

Таким образом, для IoT, особенно в жизненно важных структурах, подобных системе реагирования на стихийные бедствия, важнейшую роль будут играть как совместимые, так и смешанные стандарты. ■

Оригинал статьи опубликован на сайте www.computer.org/computer

Литература

1. www.internet-of-things-research.eu/about_iot.htm
2. www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
3. www.w3.org/WoT
4. C. Cosgrove-Sacks. Open Protocols for an Open, Interoperable Internet of Things. Org. for Advancement of Structured Information Standards. 18 Feb. 2014. www.oasis-open.org/presentations/open-protocols-and-internet-of-things-oasis.ppt.
5. J. R. Lawson and R. Vettori. Emergency Response Operations // NIST NCSTAR 1-8, Nat'l Inst. Standards and Technology. 1 Dec. 2005; www.nist.gov/customcf/get_pdf.cfm?pub_id=101049.
6. T. Gao et al. Vital Signs Monitoring and Patient Tracking over a Wireless Network // 27th Ann. IEEE Conf. Engineering in Medicine and Biology Society (EMBS 05). 2006.
7. K. Lorincz et al. Sensor Networks for Emergency Response: Challenges and Opportunities // IEEE Pervasive Computing. 2004. Vol. 3. № 4.
8. http://bigdata.ieee.org/standards
9. A. F. Martins et al. IEEE 11073 and Connected Health: Preparing Personal Health Devices for the Internet // IEEE Int'l Conf. Consumer Electronics (ICCE 14). 2014.
10. K. Tassin. LTE and the Internet of Things. 3GPP, 2016. www.3gpp.org/news-events/3gpp-news/1607-iot.
11. J. Voas. Draft: Primitives and Elements of Internet of Things (IoT) Trustworthiness. NIST IR 8063 Nat'l Inst. Standards and Technology, 16 Feb. 2016. http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8063.
12. J. M. Voas and P. A. Laplante. Standards Confusion and Harmonization // Computer. 2007. Vol. 40, № 7.

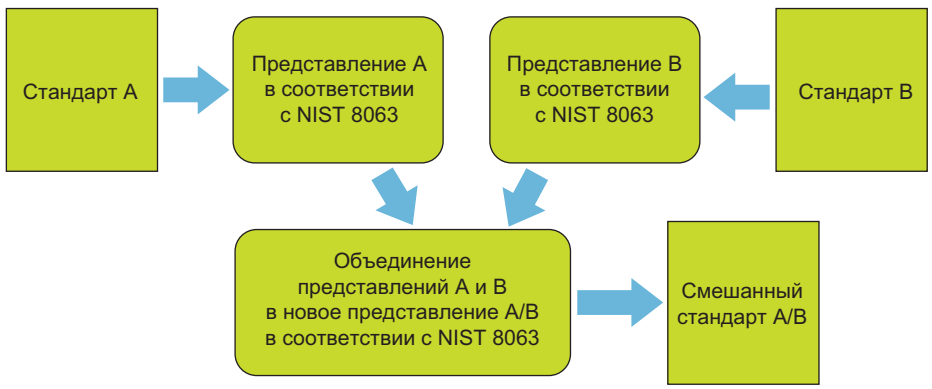

Рисунок. Предполагаемая схема образования смешанного стандарта. Примитивы и элементы, определенные в черновой версии рекомендаций NIST 8063, могут быть извлечены из стандартов A и B, преобразованы в промежуточное представление и затем объединены в смешанный стандарт A/B