

# Дотянуться до «вещей»



**Александр ГОЛЫШКО,**  
ведущий аналитик,  
АО «НПО РусБИТех», к. т. н.

Концепция Интернета вещей (Internet of Things – IoT), которой сегодня вряд ли кого-нибудь удивить, впервые была сформулирована в 1999 г. основателем исследовательской группы Auto-ID при Массачусетском технологическом институте Кевином Эштоном на презентации для руководства компании Procter & Gamble. В презентации рассказывалось о том, как всеобъемлющее внедрение радиочастотных меток (Radio Frequency Identification – RFID) сможет видоизменить систему управления логистическими цепями в корпорации. В том же году был создан Центр автоматической идентификации (Auto-ID Center), занимающийся радиочастотной идентификацией и сенсорными технологиями, благодаря которому эта концепция и получила широкое распространение.

Официальное определение IoT приведено в Рекомендации

В 1926 г. Никола Тесла в интервью для журнала Collier's сказал, что в будущем радио будет преобразовано в «большой мозг», все вещи станут частью единого целого, а инструменты, благодаря которым это станет возможным, будут легко помещаться в кармане. Собственно, это время пришло, и все упомянутое помещается отнюдь не только в кармане.

Международного союза электросвязи МСЭ-Т Y.2060, согласно которому это глобальная инфраструктура информационного общества (GIS), обеспечивающая передовые услуги за счет организации связи между вещами (физическими или виртуальными) на основе существующих и развивающихся совместимых информационных и коммуникационных технологий. Собственно, теперь вещью является абсолютно все – от каких-либо датчиков вплоть до человеческих тел, а коммуникационные технологии для передачи данных стали ключевым элементом всей конструкции IoT, что бы о ней ни говорили ИТ-корпорации или простые «айтишники».

С развитием технологий автоматизации и существенным удешевлением микроэлектроники датчики все чаще обретают дополнительный функционал за счет применения микроконтроллеров в своей конструкции, что обеспечивает возможность обмена цифровой информацией с устройствами сбора данных и/или иными датчиками, в том числе с использованием шлюза/маршрутизатора.

МСЭ-Т предусматривает использование для IoT множества сетевых технологий – глобальных сетей, локальных сетей, беспроводных самоорганизующихся (ad-hoc) и ячеистых (mesh) сетей. Указанные сети связи переносят

данные, собранные устройствами, к соответствующим программам приложениям, а также передают команды от программных приложений к устройствам.

Часто IoT противопоставляют технологии M2M (Machine-to-Machine – межмашинное взаимодействие) либо считают, будто IoT – исключительно беспроводной доступ, тогда как M2M может работать и по эфиру, и по проводам. Однако в общем виде M2M – это просто соединение и связь между двумя или более устройствами, которые могут осуществляться не обязательно через Интернет. По факту IoT базируется на технологии M2M, которая появилась раньше, чем IoT, и обе технологии очень похожи. Можно также сказать, что IoT – это общая сеть вещей, которая объединяет и устройства, и M2M-взаимодействия между ними.

Иногда говорят, что IoT – следующий уровень развития устройств, которые могут объединяться в сеть через Интернет или с помощью беспроводных технологий. Впрочем, если вы в Интернете, то вы и так уже в сети, объединившись со всеми остальными. Что же касается беспроводных технологий, то на самом деле у них нет никакого приоритета на IoT, поскольку проводные соединения замечательно работают на благо IoT, являясь к тому же наиболее

защищенными от всякого рода помех и нехороших людей, потому что для вмешательства необходимо получить физический доступ к кабелю.

Самое простое объяснение того, что такое IoT, следующее: это сеть, в которой общаются между собой не пользователи, а устройства. И если раньше к Интернету подключались компьютеры, ноутбуки, смартфоны и планшеты, то теперь к нему можно подсоединить практически любое устройство, куда вставлен, к примеру, процессор: smart-часы, «умные» бытовые приборы и даже «умные» кроссовки с носками.

Теперь посмотрим, каким образом «умные» носки могут продемонстрировать нам свой «ум».

## Доступ по проводам

Итак, издавна самый надежный, безопасный и простой способ передачи данных между устройствами – это физическое соединение кабельным/проводным каналом связи. Зачастую датчики штатно имеют в своей конструкции разъемы Ethernet, обеспечивающие подключение, в частности, по оптическому каналу. Современные проводные сети используют, как правило, витую пару и порты стандарта RJ-45, а также стандарты:

- IEEE 802.3u с максимальной пропускной способностью 0,1 Гбит/с;
- IEEE 802.3ab с максимальной пропускной способностью 1 Гбит/с и др.;
- IEEE 802.3ap с максимальной пропускной способностью 10 Гбит/с, разъем SFP+.

Указанные выше стандарты сохраняют свои характеристики при длине медного кабеля до 100 м, а с оптическим кабелем расстояния могут быть гораздо больше.

В 1990 г. выпускник MIT, один из отцов протокола TCP/IP Джон Ронки создал первую в мире интернет-вещь, подключив к сети свой тостер.

Ну а в технологичном доме Билла Гейтса, как писали в СМИ, через Интернет работала кофеварка.

## PLC

Провода бывают не только телекоммуникационные, что давно привлекало внимание связистов. Возможность передачи данных по линиям электропередачи обеспечивает постоянно совершенствующаяся технология PLC (Power Line Communication). Здесь электропитание берется не из аккумуляторов или батареек, а непосредственно из физической среды. В общем, кое-что из семейства PLC может пригодиться и для IoT.

Существует несколько вариантов классификации PLC-систем. Во-первых, технологии передачи данных по электросетям принято разделять на широкополосные (Broadband over Power Lines – BPL) и узкополосные (Narrowband over Power Lines – NPL). Широкополосные системы (со скоростями до 1 Гбит/с) ориентированы на системы высокоскоростного доступа к Интернету, создание домашних компьютерных сетей, а также на приложения, требующие высокоскоростного обмена данными: потоковое видео, системы видеоконференцсвязи, цифровой телефонии и т. д. Узкополосные (низкоскоростные) системы ориентированы на использование в средствах домашней автоматизации, в управлении простейшими бытовыми приборами и т. п. В этом случае достаточно значительно меньшей пропускной способности канала (0,1–100 кбит/с). Для конечного пользователя более близка классификация по назначению, по сути, по области применения. Используется также классификация PLC-систем по типу используемых линий электропередачи.

## X-10

Технология X-10 была разработана еще в 1978 г. с участием одноименной компании

и предназначалась для реализации дистанционного управления простейшими бытовыми приборами. Для передачи цифровых данных в этой технологии используется амплитудно-частотная манипуляция. Предусматривается передача радиоимпульсов с частотой заполнения 120 кГц, генерируемых в моменты перехода переменного напряжения частотой 50/60 Гц через нуль (при этом скорость передачи данных на физическом уровне составляет 50/60 бит/с). Такая схема кодирования выбрана не случайно, поскольку при нулевом значении напряжения, как правило, уровень помех уменьшается, при этом снижается влияние других устройств, подключенных к электросети.

До сих пор контроллеры и адаптеры, использующие эту технологию для управления бытовыми приборами, выпускаются многими компаниями США и Европы.

## CEBus

Стандарт CEBus (Consumer Electronic Bus – шина потребительской электроники) был утвержден в сентябре 1992 г. и продвигается Альянсом электронной промышленности EIA (Electronic Industries Alliance), объединяющим производителей электронного оборудования в целях разработки единых электрических и функциональных спецификаций интерфейсного оборудования. В стандарте предусмотрена передача данных с использованием проводов бытовой электросети, витой пары или коаксиального кабеля, а также беспроводная передача в радио- или инфракрасном диапазоне частот. Скорость обмена данными не зависит от выбранной среды передачи данных и составляет в среднем 7,5 Кбит/с. В стандарте CEBus был использован метод передачи данных с расширением спектра (Spread Spectrum – SS).

## LonWorks

Стандарт LonWorks, принятый институтом ANSI (American

National Standards Institute) в 1999 г., ориентирован на использование в распределенных системах автоматизации зданий, транспортных сетях, системах автоматизации промышленных предприятий. В качестве физической среды передачи в технологии LonWorks предусмотрено использование электропроводки, витой пары, коаксиального кабеля или радиоканала. LonWorks базируется на применении технологии узкополосной передачи данных. В ней реализованы улучшенная цифровая обработка сигналов, эффективный механизм коррекции ошибок и оригинальный алгоритм выбора альтернативных несущих частот. Максимальная скорость передачи данных в сети LonWorks составляет 1,25 Мбит/с. Протокол LonTalk, лежащий в основе технологии LonWorks, обеспечивает возможность создания сетей с практически неограниченным количеством узлов и ориентирован на решение задач автоматизации, когда необходимы высокие надежность и скорость передачи данных.

Впрочем, вернемся к Кевину Эштону и концепции IoT, которая началась-таки с RFID и с тех пор успела серьезно расплодиться.

## RFID

RFID подразумевает, что снабженные этой технологией объекты распознаются с помощью радиосигналов. Специальные RFID-метки (транспондеры или теги) появились в 40-х гг. XX в., запатентованы были в 80-х и состоят из микрочипа для записи и хранения информации, а также антенны для связи между транспондером и внешним RFID-оборудованием. RFID-метка защищена от внешних воздействий специальной оболочкой и заключена в миниатюрный пластиковый корпус с креплениями к объекту.

На транспондер записываются:

- уникальный номер – EPC (Electronic Product Code) или UUI (Unique Item

Identifier – уникальный идентификатор объекта по различным стандартам ISO/IEC), по которому идентифицируется объект;

- дополнительные сведения – аналоги штрих-кодов символика EAN-128 или стандарта ANSI MH 10.8.2;
- пароль для доступа к транспондеру или его обнуления.

EPC – это еще и электронный код продукта, и способ нумерации каждого изделия, упаковки, документов или ячеек для их хранения по стандарту ISO/IEC 18000-6. Его использует EPCglobal GS1 – организация, которая занимается стандартизацией и продвижением маркировки TMLC (торгово-материальных ценностей).

Работает RFID-технология по следующему алгоритму:

- с помощью специализированного оборудования на радиометку записываются идентификационные данные;
- радиометка крепится к объекту;
- RFID-считыватель связывается с транспондером, при передаче сигнала устройство генерирует электромагнитное поле, которое через антенну наводит электропитание на микрочип радиометки;
- радиометка «просыпается» и отвечает на запрос, посылая через антенну радиосигнал с записанными в ней данными на приемопередатчик (этот процесс называется обратным рассеиванием – backscatter);
- RFID-считыватель принимает отправленный радиометкой сигнал, принятые данные обрабатываются предустановленным программным обеспечением;
- полученная информация передается на компьютер, оснащенный специализированным софтом («товароучеткой»).

Радиометка не обязательно должна находиться в границах прямой видимости RFID-считывателя. RFID-системы классифицируются по размеру зон считывания данных: ближней – до 20 см, средней – от 20 см до 5 м, дальней – от 5 до 300 м. Все транспондеры, которые

используются в системах RFID, работают на определенных частотах по регламентируемым протоколам – в соответствии с едиными международными стандартами, содержащими их описание.

Широко распространенная группа стандартов RFID – ISO/IEC 18000 – охватывает радиочастотные полосы в диапазонах от 125 кГц до 2,45 ГГц. Поддерживаются как пассивными (в основном) – без собственного источника питания, так и активными (реже) – с миниатюрной батареей – радиометками, транслирующими сигнал на дистанции от 20 см до нескольких десятков метров. Есть еще ряд стандартов для радиометок, размещаемых на животных, в банковских и транспортных картах и пр. Существуют и фанаты данного направления, вживившие подобные чипы (к примеру, для животных) в свое тело, что очень помогает им бесконтактным образом открывать двери, включать свет и в целом считать себя киборгами из будущего. Ну а теперь о ближайших родственниках RFID, которые часто берут на себя решение задач для радиометок.

## NFC

NFC (Near Field Communications или ISO 14443) – технология беспроводной передачи данных малого радиуса действия, предоставляющая возможность обмена данными между устройствами, находящимися на расстоянии около 10 см, анонсирована в 2004 г. Особенность этой технологии – отсутствие постоянного соединения.

NFC полностью совместим с системой меток RFID и применяется в основном для считывания данных со смарт-карт, смартфонов, смарт-часов и прочих носимых с собой устройств для выполнения бесконтактных платежей, идентификации и прочих задач, требующих краткосрочного соединения. Считыватель NFC одновременно может работать только с одним источником

данных на расстоянии не более 0,2 м. Скорость установки соединения – менее 0,1 секунды.

## Bluetooth

Bluetooth (IEEE 802.15.1) – всем известный распространенный стандарт, обеспечивающий обмен информацией между периферийными устройствами ПК (POS-терминалы, клавиатуры, принтеры и пр.), мобильными (мобильные телефоны, планшеты и пр.) и носимыми устройствами (смарт-часы, трекеры, гарнитуры) в диапазоне 2,402–2,48 ГГц. Протокол относится к беспроводным персональным сетям (Wireless Personal Area Network – WPAN).

Изначально Bluetooth позволял устройствам осуществлять обмен данными, когда они находились в радиусе до 10 м друг от друга (что сильно зависит от преград и помех). Скорость установки соединения – от 5 секунд.

В последней версии стандарта Bluetooth 5.0, разработанной специально для IoT-устройств и представленной в 2016 г., скорость передачи данных увеличивается до 6,25 Мбит/с, а расстояние – до 240 м (в идеальных условиях, с отсутствием явных препятствий) и, что важно, при большей энергоэффективности по сравнению с предыдущими версиями стандарта. Технически «вещи» могут выбирать между увеличенной скоростью или увеличенной дальностью, причем оба варианта обеспечивают низкое энергопотребление. Что касается большой дальности, то в этом у IoT объективно существует самая высокая потребность.

Все приведенные усовершенствования Bluetooth относятся к спецификации Bluetooth Low Energy (BLE), которая была введена начиная с Bluetooth 4.0. Технология BLE предназначена для снижения энергопотребления периферийных устройств.

## ZigBee

Когда не требуется какой-либо значительной дальности связи,

спецификация ZigBee, пожалуй, наиболее продвинутая надстройка к стандарту IEEE 802.15.4. В частности, сети ZigBee IEEE 802.15.4-2006 обладают рядом преимуществ:

- благодаря ячеистой (mesh) топологии и специальным алгоритмам маршрутизации сеть ZigBee обеспечивает самовосстановление и гарантированную доставку пакетов в случаях обрыва связи между отдельными узлами (появления препятствия), перегрузки или отказа какого-то элемента;
- предусматривает криптографическую защиту данных, передаваемых по беспроводным каналам, и гибкую политику безопасности;
- устройства ZigBee отличаются низким электропотреблением, особенно конечные устройства, для которых предусмотрен режим «сна», что позволяет им работать до трех лет от одной обычной батарейки AA и даже AAA;
- сеть ZigBee – самоорганизующаяся, ее структура задается параметрами профиля стека конфигурирования и формируется автоматически путем присоединения (повторного присоединения) к сети образующих ее устройств, что обеспечивает простоту развертывания и легкость масштабирования путем обычного присоединения дополнительных устройств;
- устройства ZigBee компактные, имеют относительно невысокую стоимость (стоимость модуля ZigBee на порядок ниже, чем модема Wi-Fi).

Связь в сети ZigBee осуществляется путем последовательной ретрансляции пакетов от узла источника до узла адресата. В сети ZigBee предусмотрено несколько альтернативных алгоритмов маршрутизации, выбор которых происходит автоматически.

Стандарт предусматривает возможность использования каналов в нескольких частотных диапазонах. Наибольшая скорость передачи и наилучшая помехоустойчивость достигаются

в диапазоне от 2,4 до 2,48 ГГц. В этом диапазоне предусмотрено 16 каналов по 5 МГц. Максимальная скорость передачи данных – 250 кбит/с (средняя – от 5 до 40 кбит/с).

Расстояние между рабочими станциями сети составляет десятки метров внутри помещений и сотни метров на открытом воздухе. За счет ретрансляции покрываемая сетью зона может быть весьма значительной: до нескольких тысяч квадратных метров в помещении и до нескольких гектар на открытом пространстве. К тому же сеть ZigBee в любой момент может быть расширена добавлением новых элементов или, наоборот, разбита на несколько зон.

Период задержки передачи сигнала ZigBee намного меньше, чем у Bluetooth (несколько секунд), и составляет 30 мс, что примерно равно времени от нажатия выключателя до возникновения света в люстре. Говорят, что в связи с этим Bluetooth стал меньше использоваться в системах «Умный дом».

## Z-wave

Z-Wave – распространенный радиопrotocol передачи данных, предназначенный для домашней автоматизации. Характерной особенностью Z-Wave является стандартизация от уровня физического до уровня приложения. То есть протокол покрывает все уровни OSI классификации, что позволяет обеспечивать совместимость устройств разных производителей при создании гетерогенных сетей.

Протокол Z-Wave был разработан для квартир и небольших домов. Обычно такие системы содержат от пяти до 100 устройств. Основная особенность Z-Wave состоит в том, что он относится к формату «сделай сам» (DIY), т. е. установку и настройку системы владелец жилья может осуществить самостоятельно. Поддерживает до 232 устройств в одной сети,

что более чем достаточно для любого «умного дома».

Передача данных осуществляется на частоте 869,0 МГц (Россия), 868,42 МГц (Европа, страны СЕРТ, Китай, Сингапур, ОАЭ, ЮАР), 908,42 МГц (США, Мексика), 921,42 МГц (Австралия, Бразилия, Новая Зеландия), 919,8 МГц (Гонконг), 865,2 МГц (Индия), 868,2 МГц (Малайзия), Япония (951–956 и 922–926 МГц). Модуляция FSK (частотная манипуляция). Скорость передачи: 42 кбит/с, 100 кбит/с и 9,6 кбит/с (для совместимости со старыми устройствами). Сквозность – не более 1%. Предельная мощность передачи – 1 мВт.

Сигналы Z-Wave могут распространяться на расстояние до 100 м на открытом воздухе, но в многоэтажных домах этот показатель снижается до 15 м (с препятствиями) или до 30 м (без препятствий).

Семейство технологий для домашней автоматизации старше, чем IoT, причем весьма обширно (X10, Insteon, UPB, Tread и пр.), и, дабы оно не увело нас куда-то в сторону, ограничимся сказанным.

## LPWAN

Логично предположить, что беспроводное подключение «вещей», распределенных по обширной территории, будет также осуществляться посредством сетей с низким энергопотреблением, потому как энергию все равно нужно где-то брать, скорее всего, от батарейки или аккумулятора. Собственно, зачем нужны LPWAN (Low Power Wide Area Network), если у нас уже есть готовые и обкатанные решения вроде Wi-Fi или LTE?

Допустим, на один жилой дом из 350 квартир придется 1000 счетчиков-пользователей с копеечным трафиком в многомегабитных каналах связи. Если все счетчики будут подключены к ближайшей базовой станции LTE, то займут все ее ресурсы пропускной способности – счетчики-то подключены

постоянно. Поскольку таких домов вокруг базовой станции будет много, то такой IoT больше похож на «диверсию» против мобильной связи. А еще есть вопросы энергопотребления, потому что батарейка в счетчике обойдется дешевле, чем электрокабель.

В отличие от классических систем мобильной связи огромное семейство сетей LPWAN специально разрабатывалось в расчете на обслуживание IoT, большинство устройств которого являются простыми сенсорами с низким уровнем генерируемого трафика (10–50 бит в день, преимущественно в сторону базовой станции), с обеспечением низкой стоимости сетевого оборудования и малого энергопотребления (время автономной работы от аккумуляторов до десяти лет и более). С помощью подобных сетей следят за работой предприятий, контролируют качество воды, добычу нефти, газа, полезных ископаемых. Сети указанного типа используют как точки доступа для сбора и передачи информации, собранной датчиками, которые объединены в сетевые кластеры.

Для построения сетей LPWAN разработано немало технологий, в том числе в России, однако в глобальном масштабе их следует разделить на две большие группы по характеру используемых радиочастот – лицензируемых и нелицензируемых. Последние представляют собой: 40 МГц, 169 МГц, 433 МГц, 863–876 МГц, 915–921 МГц, 2,4 ГГц, полосы в 5 ГГц, а также полосы CRS (системы когнитивного радио) в диапазоне ТВ-вещания). Часто для описания нелицензированных диапазонов применяется термин ISM (Industrial, Scientific and Medical band) – диапазон частот для промышленной, научной и медицинской аппаратуры.

В РФ к нелицензируемому диапазону частот, которые могут быть использованы без оформления разрешения ГРЧ при условии соблюдения требований по ширине полосы,

излучаемой мощности и назначению готового изделия, относят: 433,075–434,750 МГц; 868,0–868,2 МГц; 868,7–869,2 МГц; 2400,0–2483,5 МГц. При этом для 434 МГц мощность передатчика должна составлять не более 10 мВт, для 868,0–868,2 МГц – до 10 мВт, для 868,7–869,2 МГц – до 25 мВт, для 2,4 ГГц – не более 100 мВт.

Соответственно в лицензируемых могут работать только обладатели разрешений на работу в конкретных радиочастотных диапазонах, а в остальных – кто угодно. При этом полосы частот в нелицензируемых диапазонах имеют свои ограничения как по ширине, так и по наличию помех от других пользователей.

К наиболее известным технологиям из безлицензионного пула относятся LoRa/LoRaWAN, SigFox, Neil/Weightless, On-Ramp и др., включая отечественную систему «Стриж».

## LoRa

Технология LoRa была представлена в начале 2015 г. компанией Semtech и исследовательским центром IBM Research с дальнейшим созданием LoRa Alliance для поддержки технологии и ее дальнейшего развития. LoRa опирается на метод модуляции LoRa, запатентованный компанией Semtech, а также на открытый сетевой протокол Long Range Wide Area Networks (LoRaWAN). Тут есть свои особенности. В целом LoRa относится к физическому уровню (PHY), и эта технология принадлежит компании Semtech Corporation. В свою очередь, LoRaWAN относится к подуровню управления доступом к среде (MAC) и развивается консорциумом LoRa Alliance. Спецификация LoRaWAN находится в свободном доступе, а LoRa является проприетарной технологией, и компания Semtech собирает лицензионные отчисления с поставщиков микросхем, которые продают модули LoRa.

Модуляция LoRa основана на технологии расширения спектра (Spread Spectrum Modulation) и вариации линейной частотной модуляции (Chirp Spread Spectrum – CSS). Такое решение обеспечивает высокую устойчивость связи на значительных расстояниях и позволяет увеличить дальность связи почти в десять раз по сравнению с обычными системами прямой радиосвязи при тех же характеристиках передатчиков.

Сеть может иметь различные топологии: ячеистую (mesh), звезда, «точка – точка» и др. Рабочие частоты: 915 МГц (США), 868 МГц (Европа), 433 МГц (Азия). Полоса рабочих частот – до 500 кГц.

Зона охвата базовой станции (шлюза LoRa) в сети LoRaWAN – до 2,5 км в городе и 20–45 км вне города, скорость передачи данных – 0,3–50 Кбит/с. Продолжительность автономной работы конечного устройства с аккумулятором емкостью 2000 мА·ч – почти девять лет.

Радиоинтерфейс физического уровня LoRa определяет все аспекты передачи радиосигналов между различными узлами сети (шлюзами LoRa) и оконечными устройствами (сенсорами и датчиками IoT). Он основан на использовании широкополосных радиосигналов с крупной базой, много больше единицы.

Радиоинтерфейс LoRa устанавливает рабочие частоты, виды модуляции, уровни мощности, сигнализацию и обмен сигналами между передающими и приемными устройствами в сети LoRa.

Сетевая архитектура LoRa включает абонентские устройства IoT, шлюзы LoRa (базовые станции), сетевые серверы, подключенные по транспортной сети к сети Интернет, и серверы приложений. Абонентские устройства IoT сети LoRa являются, как правило, устройствами, включающими кроме модема датчики или сенсоры, которые передают данные лишь в короткие промежутки времени по заданному графику.

Центральный сервер сети LoRaWAN адресно управляет устройствами (End-Node), шлюзами сети и соединяет сеть доступа LoRaWAN с сервером приложений.

Шлюзы LoRa, как правило, представляют собой многоканальные мультимодемные трансиверы, способные выполнять демодуляцию нескольких каналов одновременно и даже одновременную демодуляцию множества сигналов на одном и том же радиоканале.

Шлюзы служат для организации передачи данных между устройствами LoRa (End-Node) и центральным сервером, не внося изменений в сами сообщения («прозрачный мост») и прежде всего играя роль концентраторов трафика и его инкапсуляции в транспортный I-трафик.

Связь шлюзов и центрального сервера LoRaWAN обеспечивается транспортной сетью оператора (backhaul) на основе стандартных технологий (Ethernet, Wi-Fi, GPRS) по протоколу TCP/IP. Все устройства LoRa (End-Node), как правило, являются двунаправленными, но они поддерживают и функционирование в режиме, обеспечивающем групповое обновление ПО или передачу иных массовых сообщений (Broadcast), что позволяет сократить время на их передачу.

В настоящее время в мире работает более 60 операторов LoRaWAN, в том числе и в РФ. В России утвержден национальный стандарт LoRaWAN Ru.

## Symphony Link

LoRaWAN – не единственный стандарт LPWAN, который использует физический уровень LoRa.

Компания Link Labs разработала конкурирующее решение LPWAN на основе LoRa, называемое Symphony Link, которое, по заявлениям Link Labs, способно превзойти LoRaWAN посредством гарантированного получения сообщений, увеличенной абонентской емкости,

использования ретрансляторов и более простого обновления встроеного ПО.

С учетом того, что за стандартом LoRaWAN стоит консорциум LoRa Alliance, вряд ли Symphony Link станет серьезным конкурентом на рынке обслуживания IoT.

## «Стриж»

Отечественная разработка для LPWAN – «Стриж» – является недорогой и экономичной альтернативой многим другим технологиям. Сети на ее базе развернуты в РФ и ближнем зарубежье. Она обеспечивает быстрое развертывание сети, большой радиус действия (10–50 км), срок автономной работы – до десяти лет, низкие затраты на внедрение – одна станция опрашивает все устройства без концентраторов и ретрансляторов (экономию на промежуточном оборудовании), низкую стоимость решения (в три-четыре раза ниже, чем у аналогов), высокую надежность – сеть работает по топологии «звезда» (устройства опрашиваются напрямую базовой станцией без промежуточного оборудования или mesh).

Устройства и модемы «Стриж» передают восьмибайтные пакеты данных по беспроводному протоколу XNB (Extended Narrowband). Это беспроводной узкополосный LPWAN-протокол, разработанный командой «Стриж» для обмена данными с абонентских устройств на больших распределенных территориях с минимальными затратами энергии. Работает там, где не ловит GSM/GPRS. Базовые станции передают данные на сервер. Сервер осуществляет обработку данных, мониторинг и управление устройствами.

Предусмотрена двусторонняя связь для отправки управляющих команд на устройства. Частота передачи Uplink – 868,8 МГц, частота передачи Downlink – 446,0 МГц. Альтернативные рабочие частоты – до 1 ГГц (по запросу). Ширина полосы канала передающего устройства – 100 Гц.

Технология обработки радиочастотного спектра – программно-определяемая радиосистема. Модуляция сигнала – DBPSK. Мощность передачи – 25 мВт (в 80 раз ниже, чем у мобильного телефона, что безопасно для людей и животных).

Подключение к транспортной сети Ethernet – WAN или 2 SIM-карты GPRS/3G/LTE, VSAT. Скорость передачи – 50/100/1000 бит/с. Образует 5 тыс. доступных каналов для одновременной передачи без коллизий. Суточная емкость базовой станции – 5 млн сообщений с 2 млн абонентских устройств. Множественный доступ – интеллектуальное распределение каналов. Шифрование данных алгоритмами – AES-128, XTEA-256, ГОСТ Р34.12-2015. Защита от помех – FEC, CRC32, псевдослучайная перестройка частоты. Потребление на отправку пакета данных – 35–40 мА в течение 10 секунд. Удаленное обновление ПО абонентских устройств.

## SigFox

Технология SigFox была изобретена и запатентована в 2009 г. одноименной французской компанией. Первая сеть SigFox (868 МГц) была возвращена в 2012 г. во Франции, в 2014 г. обеспечено общенациональное покрытие страны. Следующими в плане были США, но разрешенный там диапазон 902 МГц оказался слишком подвержен помехам. Тогда SigFox пошла в Азию и сегодня присутствует более чем в 60 странах мира (но не в РФ). В США Федеральная комиссия по связи (FCC) выделила SigFox диапазон 915 МГц.

Для передачи данных SigFox использует сверхузкую полосу частот (Ultra-Narrow Band – UNB) с двоично-фазовой манипуляцией (BPSK), а для кодирования данных меняет фазу несущей, что позволяет снизить уровень шума на принимающей стороне (приемники при этом дешевле). Радиус действия – 30–50 км (при помехах – 3–10 км).

Срок службы устройств без замены батареи (две штуки AA) – 20 лет. Топология сети – «звезда» вокруг базовой станции.

Стандартом SigFox определено максимальное количество сообщений от базовой станции до конечного устройства – 140 в день размером не более 12 байт (без служебной информации). В обратном направлении – четыре сообщения в день размером 8 байт.

В SigFox узлы могут использоваться в двух конфигурациях:

- режим P2P – прямая связь между узлами (интерфейс LAN);
- гибридный режим – SigFox/P2P (P2P + шлюз в сети SigFox) – позволяет передавать через сеть только определенные сообщения.

## Weightless

Семейство «невесомых» технологий Weightless – открытый стандарт для сетей LPWAN повышенной мощности в целях увеличения сетевой производительности. В специальной группе интересов Weightless SIG (Special Interest Group) предлагается семейство следующих протоколов.

Weightless-W – открытый стандарт технологии, предназначенный для работы на частотах ТВ-диапазона 470–790 МГц (TV White Space – TVWS). Там, где это разрешено, конечно. Радиус зоны покрытия – 5 км (подходит для использования в приложениях для нефтяной и газовой отраслей).

Weightless-N предназначен для создания широких зон покрытия при невысоких скоростях передачи данных – до 500 бит/с. Обеспечивает однонаправленную связь до 10 км. Поддерживает широкий диапазон ISM-частот и низкое энергопотребление. Weightless-N подходит для сенсорных сетей измерений температуры, контроля уровня жидкости в резервуаре и пр.

Похоже, Weightless SIG уже отказалась от стандартов Weightless N и W и теперь продвигает единственный

Weightless P, который иногда называют просто Weightless.

Weightless-P – стандарт, предназначенный для узкополосных IoT-решений, требующих высокой плотности устройств, долгосрочной службы батареи и двунаправленной связи. Особенностями являются высокая масштабируемость, возможность оптимизации линий связи Uplink или Downlink, создания широких зон покрытия, длительный срок службы батареи и безопасная сеть.

Weightless-P использует узкополосные 12,5 кГц каналы, что дает возможность передавать в семь раз больше данных, чем SigFox, и в 98 раз больше данных, чем LoRaWAN в городских условиях. Другие технические характеристики: мощность передатчика абонентского устройства – 14 dBm; использование синхронизированных каналов связи (в стандарте TDMA/FDMA); спектрально-эффективная модуляция OQPSK; использование любых ISM-полос частот для разветвления: 169 / 433 / 470 / 780 / 868 / 915 / 923 МГц (ключевая особенность); роуминг; дальность связи – 2 км в городе; адаптивная скорость передачи данных – 0,2–100 кбит/с; контроль мощности передачи в линиях Uplink и Downlink для уменьшения помех и увеличения пропускной способности сети.

Weightless также является открытым стандартом, направляемым организацией Weightless SIG, который, казалось бы, лучше, чем проприетарные стандарты, подобные LoRa, подходит и для разработки инноваций, и для конкуренции на рынке. Однако, как отмечают специалисты, нехватка доступного аппаратного обеспечения и редкие обновления спецификации не свидетельствуют о каком-либо серьезном развитии.

## IEEE 802.11ah

Учитывая все основные исходные данные для радиointерфейса IoT, разработчики порадовали потребителей новым

протоколом Wi-Fi специально для IoT/WLAN на базе стандарта IEEE 802.11ah – Wi-Fi HaLow (опубликован в 2017 г.). Впрочем, в этом случае не стоит обольщаться по части специализации для IoT, поскольку одной из целей разработки Wi-Fi HaLow было получение разрешения на использование семейства IEEE 802.11 в субгигагерцовом диапазоне радиочастот. Хотя и для IoT Wi-Fi HaLow, как говорят, – отличное решение.

От остальных представителей семейства Wi-Fi IEEE 802.11ah отличается тем, что работает в диапазоне до 1 ГГц, имеет меньшую мощность передатчика и значительно большую дальность, чем в традиционных сетях Wi-Fi (в том числе во многом благодаря низкой рабочей частоте).

Важные аспекты IEEE 802.11ah – поведение базовых станций, сгруппированных для сведения к минимуму коллизий в эфире, использование ретранслятора для увеличения радиуса действия, небольшого энергопотребления (конкурирует с Bluetooth) благодаря оптимальным периодам пробуждения/сна и применению секторных антенн. Стандарт использует спецификацию IEEE 802.11a/g с пониженной дискретизацией для обслуживания 26 каналов, каждый из которых способен обеспечить пропускную способность 100 Кбит/с, а все вместе – подключение к тысячам устройств в зоне обслуживания базовой станции.

Стандарт обеспечивает скорость соединения от 150 кбит/с в дальней зоне (до 1 км) и до 347 Мбит/с – в ближней. Скорость передачи данных до 347 Мбит/с достигается только при максимальном использовании четырех пространственных потоков, использующих один канал шириной 16 МГц. Стандартом определяются различные схемы модуляции и скорости кодирования.

## IEEE 802.11af

Другим стандартом WLAN для полос ниже 1 ГГц является

IEEE 802.11af, который, в отличие от 802.11ah, работает в лицензированных полосах радиочастот – в телевизионном радиоспектре в диапазонах VHF и UHF между 54 и 790 МГц, используя технологию когнитивного радио (организации гибкого доступа к радиочастотному спектру с правом работы на первичной или вторичной основе).

## Ingenu

В отличие от LoRa и Sigfox, которые используют ISM диапазон 915 МГц, стандарт Ingenu работает в нелицензируемом ISM диапазоне 2,4 ГГц, где работают Wi-Fi и Bluetooth. К тому же у диапазона 2,4 ГГц гораздо большая ширина, чем, к примеру, у диапазона 915 МГц.

Ядром стандарта Ingenu для сетей LPWAN является технология RPMA (множественный доступ со случайной фазой – Random Phase Multiple Access), которая представляет собой физический уровень PHY и подуровень управления доступом к среде MAC, разработанные компанией Ingenu специально для удовлетворения требований к сетям LPWAN: глобально доступный диапазон (2,4 ГГц), широкое покрытие (одна точка доступа RPMA может покрыть до 455 км<sup>2</sup>), огромная производительность (одна точка доступа RPMA способна принять 535 117 сообщений в час), долгая работа от батареи (10–20+ лет) и устойчивость к радиопомехам.

Стандарт RPMA также подразумевает двунаправленный поток данных, подтверждение доставки, изменяемые размеры пакета, отзывчивость сети, возможность аутентификации и широкополосной передачи.

Помимо разработки стандарта LPWAN компания Ingenu управляет Machine Network, общедоступной сетью стандарта RPMA, которая покрывает свыше 259 тыс. км<sup>2</sup> более чем в 30 странах в США, а также около 30 стран.

Не так давно Ingenu анонсировала переориентацию своей корпоративной стратегии на предоставление услуг RPMA в рамках модели PaaS (Platform as a Service – платформа как услуга).

## Мобильная связь IoT/M2M

Технология M2M актуальна для компаний любых разновидностей бизнеса, использующих SIM-карты операторов мобильной связи в своих устройствах и оборудовании. Одним из основных преимуществ услуги является простота ее подключения, которое можно осуществить быстро, без дорогостоящей прокладки инфраструктуры и практически где угодно, включая места, куда почти невозможно провести кабель (было бы радиопокрытие). Но главное преимущество, точнее, суть услуги – это возможность беспроводного удаленного управления сетью устройств с установленной SIM-картой.

Разумеется, работа осуществляется в лицензированных диапазонах, что, кстати, абсолютно не волнует владельца устройств IoT/M2M, потому что его сеть является наложенной на работающую сеть мобильной связи.

О недостатках решения IoT/M2M говорилось выше, но стоит повторить: использование значительных ресурсов пропускной способности сети мобильной связи для относительно небольших потребностей каждого подключенного устройства может превратиться в довольно дорогое удовольствие как для одной, так и для другой стороны. Тем не менее, если ваши «вещи» находятся, к примеру, на разных континентах, M2M будет для вас хорошим решением. Впрочем, есть и проблемы.

Если речь идет о какой-то более массовой истории либо о серийном оборудовании, то использование «обычной SIM-карты» имеет ряд недостатков. Со временем контакты в SIM-слоте окисляются, а установка,



обслуживание и замена SIM-карт при большом количестве устройств становятся затруднительными и затратными.

Проблемы с надежностью SIM-карты решают путем использования SIM-чипа стандарта MFF2 (его роль аналогична роли стандартной SIM-карты), который впаивается при производстве в оборудование и вместе с иными элементами для защиты от агрессивной внешней среды может покрываться защитным слоем лака. В дополнение SIM-чип позволяет уменьшить габариты оборудования и повысить надежность и отказоустойчивость.

Впрочем, и тут не без проблем: в соответствии с законодательством РФ операторы связи передают своим абонентам SIM-карты/чипы только после заключения договора на оказание услуг связи. При перепродаже IoT/M2M оборудования с впаиваемым SIM-чипом его нельзя изъять и установить новый, поэтому требуется корректное перезаключение указанного договора на каждый SIM-чип с новым пользователем оборудования или корректное заявление в ЕСИА (Федеральную государственную информационную систему «Единая система идентификации и аутентификации»).

Поскольку обычная SIM-карта и SIM-чип не позволяют изменить владельца без похода к оператору связи и замены физического носителя, появилась технология eSIM, которая дает возможность удаленно «перепрошить» устройство и загрузить туда новый абонентский профиль. Это упрощает процедуру тестирования устройств Интернета вещей, снижает себестоимость и затраты на логистику и обслуживание SIM-карт, повышая надежность оборудования. На текущий момент в мире есть две технологии eSIM от GSMA (Всемирная ассоциация GSM) – eSIM Consumer и eSIM M2M.

Технология eSIM Consumer – технология для смартфонов, когда для «загрузки SIM-карты» требуется сканировать QR-код.

Технология eSIM M2M подразумевает под собой экосистему, которая состоит из нескольких составляющих:

- eUICC-чипы для IoT/M2M, установленные в IoT/M2M-оборудование на заводе-изготовителе;
- система RSP (Remote SIM Provisioning), установленная у оператора связи, – для организации загрузки «по воздуху» цифровой SIM-карты в eSIM-чип.

eUICC (чип/карта) выглядит как обычная SIM-карта/чип, но внутри имеет другую аппаратную и программную начинку, которая работает по стандарту SGP.02 (Remote Sim Provisioning для eSIM M2M), т. е. поддерживает технологию eSIM M2M. В соответствии со стандартом SGP.02 eSIM-чип позволяет удаленно выполнять операцию, аналогичную установке новой SIM-карты на оборудование.

Впрочем, индустрия мобильной связи не забыла об экономии сетевых ресурсов при обслуживании IoT и заготовила соответствующий пакет изменений в стандартах 3GPP.

## EC GSM IoT

Интернет вещей с расширенным покрытием на базе стандарта GSM (EC GSM IoT – Extended Coverage Global System for Mobile IoT – EC-GPRS) – один из стандартов LPWAN консорциума 3GPP, который работает в лицензируемом диапазоне.

Данный пакет изменений предусматривает сравнительно небольшие изменения относительно базовой технологии GSM/GPRS/EDGE, что позволяет использовать подавляющее большинство установленных базовых станций GSM без замены или модернизации аппаратного обеспечения, а только с программным обновлением.

Фактически используется стандартная несущая GSM/GPRS/EDGE с изменениями, позволяющими увеличить бюджет линии и количество подключенных устройств, снизить стоимость

реализации технологии в конечном устройстве. Основные дополнения:

- Extended DRX (eDRX, Extended Discontinuous Reception) и Power Saving Mode (PSM) – снижение периодичности обязательных сигнальных сообщений, оптимизация интервалов приема и получения информации, поддержка длительных, до 52 минут, периодов молчания, в течение которых устройство остается подключенным к сети, не передавая и не получая информацию;
- Extended coverage – адаптация канального уровня сети, использующая, в частности, многократное повторение передаваемой информации для улучшения покрытия на 20 dB по сравнению с традиционными системами;
- упрощение сетевой сигнализации (отказ от поддержки той части сигнализации, которая обеспечивает совместную работу с WCDMA/LTE-сетями);
- расширение механизмов аутентификации и безопасности соединения и др.

Ключевые преимущества EC-GSM – готовность сетевой инфраструктуры (в большинстве случаев требуется только обновление программного обеспечения на узлах сети), распространенность сетей стандарта GSM и их охват.

Впрочем, из вариантов обслуживания IoT с помощью сетей мобильной связи стандарт EC GSM IoT имеет наименьшее количество преимуществ.

## eMTC

Технология eMTC называется также LTE M/LTE MTC (Machine Type Communication – машинная связь) или LTE Cat.M1.

Помимо полной совместимости с существующими сетями LTE основное преимущество, выделяющее технологию eMTC и определяющее ее рыночную нишу, – это высокая пропускная способность, составляющая до 1 Мбит/с в направлении

Uplink и Downlink. eMTC призван обеспечить снижение стоимости конечного IoT устройства за счет отказа от множества функциональностей стандарта LTE, которые востребованы и широко применяются в сетях мобильного широкополосного доступа (МШПД), но становятся избыточными при массовом подключении IoT-устройств. В общем, надо быть проще.

Стандартизация eMTC началась в Release 12 3GPP и продолжилась в Release 13 и 14. По сравнению с классическими LTE-системами в eMTC определены:

- механизмы Extended DRX и PSM для LTE, которые должны решить задачу снижения энергопотребления;
- TTI bundling (улучшает покрытие в Uplink) и множественные повторения пакетов, обеспечивающие повышение помехоустойчивости;
- новая категория LTE Cat.0 для IoT-устройств и новый класс мощности 20dBm;
- позиционирование (E-CID и OTDOA);
- групповое вещание (Multicast SC-PTM);
- межчастотная (inter-frequency) мобильность;
- увеличение скорости передачи данных и пр.

eMTC имеет высокую степень готовности сетевой инфраструктуры (современные базовые станции выполняются по технологии SDR – Software Define Radio – программно-определяемое радио, позволяя работать в разных стандартах и различных радиочастотных диапазонах), благодаря чему может быть развернута на существующих сетях LTE путем простого обновления ПО. Более того, сети LTE для мобильного ШПД и IoT могут сосуществовать и динамически перераспределять используемые ресурсы (частотный спектр, вычислительную мощность базовой станции и др.) в зависимости от типа и количества подключенных устройств и создаваемого ими трафика.

## NB-IoT

Narrowband IoT (NB IoT – «узкополосный Интернет вещей»), называемый еще LTE Cat.M2 – третий стандарт LPWAN, выпущенный консорциумом 3GPP, имеет несколько кардинальных отличий от LTE M. NB-IoT относится к так называемому CIoT, Cellular IoT (по терминологии 3GPP) или MIoT, Mobile IoT (по терминологии GSMA) и продвигается операторами сотовой связи и производителями соответствующего оборудования. Узкополосным (Narrow Band) этот вид связи назвали по сравнению с «традиционным» LTE, где используются существенно более широкие полосы частот (3, 5, 10, 15, 20 МГц), что позволяет разделить общий ресурс пропускной способности базовой станции между гораздо большим количеством абонентских устройств.

NB IoT предполагает меньшую пропускную способность – 250 кбит/с против 1 Мбит/с LTE M. Сам принцип функционирования IoT не предполагает значительного обмена информацией с устройствами, соответственно приводимые значения весьма условны и достигаются при высоком качестве радиосигнала. Другое отличие заключается в том, что стандарт NB IoT основан на модуляции с расширением спектра методом прямой последовательности (DSSS), так что он не связан с LTE, как LTE M. К тому же стандарт не ограничивает используемые полосы диапазоном LTE.

Самое важное в NB-IoT – возможность работы при более низких уровнях сигнала и при высоком уровне шумов, а также экономия батареи. Предназначен он для передачи коротких сообщений, и от него не требуется передача аудиовидеоконтента, больших файлов и пр. На физическом уровне есть определенные особенности, которые помогают обеспечить необходимые характеристики:

- общая полоса для NB-IoT ограничена шириной в 180 кГц;

- радиотракт пользовательского устройства имеет всего одну антенну, приемник и передатчик;
- передача и прием разнесены по времени, т. е. по сути это полудуплексный режим;
- возможность передавать в направлении Uplink на одной поднесущей;
- используемые типы модуляции ограничены BPSK и QPSK;
- повторения передаваемого сигнала (coverage enhancement).

Для NB-IoT могут использоваться практически те же диапазоны частот, что и для 2G/3G/4G – 800 МГц, 900 МГц, 1800 МГц. Смысла использовать более высокие частоты нет из-за большего затухания сигнала.

Если сравнивать возможности NB-IoT с другими технологиями построения глобальных сетей Интернета вещей, такими как eMTC, SigFox и LoRa, то NB-IoT обеспечивает более высокую производительность. Кроме того, когда все технологии рассматриваются с точки зрения инвестиций в сеть, обеспечения радиопокрытия, емкости и надежности сети, видно, что NB-IoT является наиболее подходящей технологией.

3GPP определил три сценария развертывания радиоканалов NB-IoT:

- в защитной полосе между каналами – Guard Band;
- внутри существующих каналов – In Band;
- автономное развертывание – Standalone.

Standalone использует в основном отдельный диапазон частот; разворачивание в режиме Guard Band осуществляется в полосе частот, зарезервированной в качестве защитной полосы между существующими каналами сети LTE; разворачивание в режиме In Band реализуется в тех же ресурсных блоках, что и существующая LTE-сеть.

Стандартизация NB-IoT началась с Release 13 3GPP и продолжилась в последующих, включая:

- позиционирование (OTDOA и UTDOA);
- групповое вещание (Multicast SC-PTM);
- новый класс мощности (14dBm);
- мобильность;
- новые механизмы, направленные на дополнительное уменьшение энергопотребления.

NB-IoT ориентирован скорее на неподвижные (стационарные) устройства, так как в этом режиме не поддерживается автоматическое переключение между сотами (handover). При перемещении в другую соту устройству NB-IoT придется снова регистрироваться в сети. Таким образом, NB-IoT предназначается в первую очередь для таких приложений, как автоматический сбор показаний со счетчиков, датчиков, дистанционное управление уличным освещением и т. п. В отличие от NB-IoT другая ветка CIoT – LTE-M – поддерживает переключение между сотами и обеспечивает в несколько раз более высокие скорости приема/передачи.

В NB-IoT возможны большие задержки связи при использовании режимов энергосбережения. Дело в том, что окончательное устройство, находясь в режимах энергосбережения, оказывается недоступным со стороны сети (сервера приложений).

В целом считается, что NB-IoT – самый эффективный протокол IoT для «более быстрых» приложений. Сеть на базе NB-IoT также может быть развернута на существующих сетях LTE путем простого обновления ПО. Если этого еще не сделано, значит, операторы мобильной связи пока не наблюдают большого количества потенциальных клиентов, оставляя нишу IoT на откуп операторам LPWAN из нелицензируемого радиочастотного пула. Там, где они увидят выгоду, оперативно внедрят новые технологии, предоставив лучшие условия и лучшее качество. Не стоит забывать, что нелицензируемые диапазоны имеют относительно узкие полосы частот, что подчас приводит их пользователей к взаимным

помехам (не только случайным) и различным коллизиям, причем без претензий к источникам последних.

Кстати, на рубеже 2008–2009 гг. произошел переход от «Интернета людей» к «Интернету вещей», когда количество подключенных к сети предметов превысило количество людей, как в Интернете, так и на планете.

## 5G

Сети мобильной связи 5-го поколения (5G) впервые были изначально спроектированы в том числе и для обслуживания экосистемы IoT. При этом они обеспечивают более чем 100-кратное увеличение пропускной способности сети, попутно решая задачи значительного увеличения скорости передачи данных (от 50 Мбит/с до 1 Гбит/с), значительного увеличения емкости сети с возможностью подключить гораздо больше устройств (в том числе устройств IoT, не требующих каких-либо огромных скоростей передачи данных) и значительного сокращения времени отклика. Оборудование 5G может использовать любые неиспользованные полосы радиоспектра, объединяя их ресурсы благодаря технологии агрегации несущих (Carrier Aggregation).

В сетях 5G используются два основных диапазона частот: от 400 МГц до 6 ГГц и от 24 до 50 ГГц. Одна базовая станция 5G, работающая на частоте 400 МГц, сможет охватывать связью многие десятки километров территории. Посредством технологии Massive MIMO одна базовая станция также может обслуживать гораздо большее количество одновременно подключенных устройств благодаря возможности управлять диаграммой направленности антенн, фокусируя радиоволны на конкретном устройстве.

Для быстрого развертывания сетей 5G во многих странах операторы используют более низкие частоты и покрывают сразу огромные территории,

что составляет серьезную конкуренцию остальным членам семейства LPWAN.

## 6G

В следующем поколении мобильной связи, работы над которым уже начались, скорости увеличатся, а пропускные способности расширятся. В целом экосистема 6G будет использовать широкий набор частотных диапазонов от менее 6 ГГц до 1 ТГц.

И люди, и машины чувствительны к задержкам в доставке информации (хотя и в разной степени). Своевременность доставки информации будет иметь решающее значение для сильно взаимосвязанного общества будущего.

Предыдущие поколения беспроводных сетей в основном фокусировались на пропускной способности канала, то есть того, какой объем данных можно через него пропустить в единицу времени. В 6G, наоборот, больше внимания будет уделено задержкам сигнала, что выливается в то, сколько времени надо на реакцию и обучение сети. Типичное применение – аналитика на границе сети для Индустрии 4.0, например, граничные устройства Интернета Вещей (IoT), взаимодействующие с дополненной реальностью. Но это дело будущего, которое нам обещают примерно к 2030 году.

А пока в заключение отметим, что, несмотря на все приведенное выше, развитие IoT лишь ускорило в направлении IoB (Internet of Bodies – Интернет тел), IoNT (Internet of Nano-Things – Интернет нановещей), MIoT (Military Internet of Things – военный Интернет вещей), IoBT (Internet of Battle Things – Интернет боевых вещей), IoMT (Internet of Military Things – Интернет военных вещей), которым тоже будут нужны стандарты, радиointерфейсы и соответствующие экосистемы, чтобы обслужить тот самый «огромный мозг», предсказанный Н. Тесла. ■