Низкоскоростной Интернет вещей в Украине: LoRaWAN и NB-IoT

О преимуществах линейной частотной модуляции LoRa, возможностях и перспективах NB-IoT, а также настоящем и ближайшем будущем технологий Интернета вещей в нашей стране.

В широком смысле Интернет вещей — это концепция сети передачи данных, предусматривающая взаимодействие между физическими объектами, оснащенными встроенными средствами и технологиями для обмена информацией друг с другом или с внешней средой.

Поскольку спектр представленных в настоящее время решений достаточно широк, есть смысл рассмотреть низкоскоростные LPWAN-системы передачи данных, представленные, в частности, в нашей стране. Прежде всего это LoRaWAN и NB-IoT. Именно эти IoT-системы внедряются буквально на наших глазах в различных отраслях экономики.

О терминах и определениях

За время развития Интернета вещей создано огромное количество (свыше 150) инструментов, технологий и протоколов различного уровня для обеспечения передачи телеметрической информации и межмашинного обмена по радиоканалам. Однако в настоящее время, говоря об IoT, подразумевают несколько технологий, как высоко-, так и низкоскоростных, среди которых видное место занимают системы ***низкоскоростной передачи данных*** LPWAN (Low-power Wide-area Network) с ***низким энергопотреблением*** и, как правило, редким выходом в сеть для передачи необходимых показаний от многочисленных терминальных устройств и IoT-датчиков.

При этом в таких системах вовсе не предполагается наличие высоких скоростей, а тем более непрерывной работы (хотя таковая для систем IoT и не исключается). Поэтому когда говорят, что появление высокоскоростной мобильной связи стандарта 5G будет стимулировать внедрение систем промышленного Интернета вещей (Industrial IoT) и обеспечивать новые возможности для различного вида охранных систем, к этим заявлениям следует относиться весьма осторожно. Это утверждение справедливо далеко не для всех IoT-систем.

В целом же перспективы внедрения Интернета вещей во многом связаны с несколькими факторами, прежде всего с наличием и доступностью на рынке соответствующего оборудования — т.н. «интеллектуальных» счетчиков воды, электроэнергии, газа, а также датчиков, позволяющих фиксировать параметры окружающей среды (температуру, влажность, др.), а также строить охранные системы.

Так сложилось, что в настоящее время для производства конечного оборудования LPWAN чаще всего используются технологии LoRaWAN и NB-IoT. В мире налажен массовый выпуск терминальных устройств, поддерживающих упомянутые технологии. В Украине также все реализованные IoT-проекты, пусть и небольшие по объему (или даже тестовые), используют указанные протоколы.

В статье представлен сегмент низкоскоростных энергосберегающих IoT-систем (LPWAN), которые пока что рассматриваются в нашей стране как безальтернативные решения.

EcoStruxure™
Innovation At Every Level

Рішення для периферійних обчислень

УПЕВНЕНО

керуйте переходом на цифрові технології з мікро-ЦОДами **EcoStruxure™**

Мікро-ЦОД **EcoStruxure™** для настінного монтажу на 6 монтажних одиниць виробництва Schneider Electric™ з можливістю дистанційного керування за допомогою EcoStruxure IT Expert є ідеальним рішенням для невеликих приміщень із жорсткими вимогами щодо економії простору.

#CertaintyInAConnectedWorld

se.com/ua

APC

EcoStruxure
IT Expert

6U Wall Mount
EcoStruxure
Micro Data Center

Life Is On | Schneider Electric

Построение IoT — подходы и концепции

Интернет вещей — технология, позволяющая решать задачи, связанные, в первую очередь, со сбором информации от различных датчиков с целью ее последующей обработки и анализа. Базовыми особенностями существующих и проектируемых сетей IoT является работа с низкими скоростями передачи данных на больших расстояниях, низкое потребление клиентских IoT-устройств, что обеспечивает возможность их длительного функционирования от стандартных элементов (батареек).

Работа низкоскоростных IoT-систем обеспечивается за счет использования ограниченной полосы пропускания каналов связи — 120–180 кГц, что характерно как для систем LoRaWAN, так и для NB-IoT, которые в настоящее время нашли применение в нашей стране. Собственно говоря, обе упомянутые технологии содержат в своих названиях уточняющие аббревиатуры, а именно LoRa (Long Range — «длинная дистанция») и NB (Narrow Band — «узкая полоса»).

На первый взгляд, это вроде бы синонимы. Но анализ показывает, что это не совсем так, и при сравнимых полосах пропускания и мощности сигнала в радиоканале технология LoRa обеспечивает существенно более высокую помехозащищенность, а значит, большую дальность при прочих равных условиях, расходуя меньше энергии аккумуляторных батарей для передачи тех же объемов информации.

Связано это, прежде всего, с используемой в LoRaWAN непривычной для связистов широкополосной линейно-частотной модуляцией (ЛЧМ, Chirp Spread Spectrum, CSS), которая базируется на идее передачи элементарных сигналов в виде несущей, частота которой линейно нарастает. Использовать такой сигнал для передачи информации предложила компания Semtech в процессе разработки способа модуляции для технологии LoRa. Такие сигналы ранее использовались в радиолокации, где задача передачи информации вовсе не стоит, а частота сигнала f(t) в процессе передачи зондирующих радиоимпульсов меняется во времени единожды заданным способом — от минимальной f_{min} до максимальной f_{max}:

$$f(t) = f_0 + \mu \cdot t, \quad (1)$$

где $f_0 = (f_{max} + f_{min})/2$ — центральная частота диапазона; $\mu = (f_{max} - f_{min})/T_c$ — скорость изменения частоты радиосигнала; T_c — длительность радиоимпульса; $-T_c/2 \leqslant t \leqslant T_c/2$ – время.

О том, как выполняется модуляция сигнала и какие его параметры при этом меняются, мы рассмотрим далее в разделе «Модуляция LoRa».

Сейчас же для нас важно констатировать тот факт, что разработчики упомянутых стандартов и технологий ставят перед собой общую цель — обеспечить низкоскоростную передачу данных (по сути телеметрии) на сравнительно большие расстояния с минимальными затратами сетевых ресурсов. Причем даже в системе NB-IoT реализована возможность повышения мощности IoT-поднесущих диапазона LTE (используемых для передачи данных) на 6 дБ по сравнению с обычными LTE-каналами только с одной целью — расширить дальность работы системы.

Что касается производительности той или иной технологии, то утверждается, что скорость передачи данных в NB-IoT достигает 58,8 кбит/с, при этом имеются решения, которые позволяют увеличить это значение до 100 кбит/с. Отечественные операторы утверждают, что данные от абонента в сеть могут передаваться со скоростью до 250 кбит/с, а к абоненту — 226,7 кбит/с.

В то же время известно, что максимальная битовая скорость передачи в LoRa при использовании ЛЧМ не превышает 6,8 кбит/с (и это без кодирования). Отличия разительные. Кроме того, при ухудшении помеховой обстановки LoRa может снизить скорость до 366 бит/с, а с учетом кодирования — еще в два раза. Однако в LoRa заложены и возможности перехода на обычную частотную манипуляцию (FSK или GFSK), которая может обеспечить более скоростную передачу данных — в районе 50 кбит/с.

При создании системы удаленной телеметрии заказчик, прежде всего, выбирает технологию физического уровня, определяющую структуру сети, скорость ее развертывания и возможности. В настоящее время в Украине ведется проработка и создание IoT-систем на базе технологий NB-IoT и LoRaWAN. Первый вариант предполагает использование уже существующих сетей сотовой связи мобильных операторов. При этом задействуется существующая сетевая инфраструктура (как правило, LTE, хотя не исключается и GSM). Второй способ обеспечивает коммерческое применение для решений локальных задач, в том числе и на территориях, не охваченных системами мобильной связи.

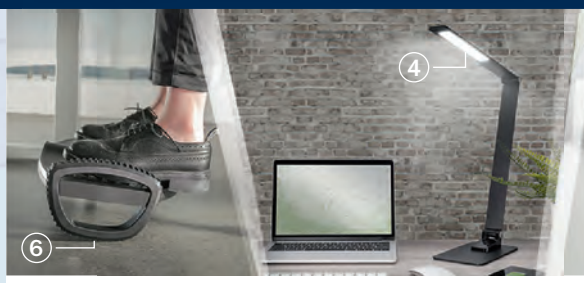
Для продвижение протокола LoRaWAN в качестве стандарта для глобальных сетей с низким энергопотреблением в январе 2015 г. была создана некоммерческая организация LoRa Alliance (https://lora-alliance.org), которая насчитывает около 500 членов.

Модуляция LoRa

Спецификация LoRa определяет физический уровень передачи сигналов от оконечных устройств к шлюзу и использует весьма специфическую линейно-частотную модуляцию (ЛЧМ). До времени появления этого способа передачи сигналов на практике использовали известные традиционные виды модуляции (в применении к дискретной передаче данных чаще используется термин «манипуляция») — амплитудная, частотная, фазовая, амплитудно-фазовая (она же квадратурная).

DIGITUS®
by ASSMANN

ЕРГОНОМІЧНЕ ОБЛАДНАННЯ НА БУДЬ-ЯКУ ВИМОГУ



Здорові умови праці дуже важливі для успіху всієї компанії в повсякденному офісному житті. Але працівники часто страждають від болю в спині, викликаної тривалим і неправильним сидінням. Це має прямі наслідки для здоров'я та ефективності.

Пропонуємо рішення: більша продуктивність внаслідок покращеної ергономіці в роботі. Завдяки ергономічним рішенням від DIGITUS® ви отримуєте професійні робочі місця, адаптовані до потреб співробітників та вимог компанії. Ідеально підходить для дому та офісу!

Електрично регульовані по висоті рами та столи дозволяють створити оптимальну позу, зручну для спини, і забезпечують різноманітність. Крім того, підйомник робочої поверхні створює практичне рішення для швидкого перетворення звичайного письмового столу на ергономічну робочу станцію.

ІДЕАЛЬНЕ ДОПОВНЕННЯ ДО ЕРГОНОМІЧНОГО РОБОЧОГО МІСЦЯ:

- ✓ Регульовані стільці для гнучкої роботи сидячи, ритулившись і стоячи
- ✓ Правильні умови освітлення в будь-якій ситуації завдяки світлодіодним настільним світильникам з практичною функцією зарядки USB для мобільних пристроїв
- ✓ Ергономічні підніжки з функцією перекочування для активних рухів ногами та покращення кровообігу

Відкрийте для себе широкий асортимент ергономічного обладнання, щоб зробити роботу в офісі успішною.

ELECTRIC HEIGHT-ADJUSTABLE
DESK WITH USB-CHARGER: DA-90406
TABLE FRAME: DA-90390 (1)
3-LEG TABLE FRAME: DA-90392 (2)

ERGONOMIC WORKSPACE RISER
BLACK: DA-90380-1
WHITE: DA-90380-2 (3)

LED MONITOR LIGHT WITH CLAMP MOUNT
DA-90415

ERGONOMIC STAND/SIT/LEAN CHAIR, HEIGHT ADJUSTABLE
DA-90391

ACTIVE ERGONOMIC FOOTREST WITH ROCKER FUNCTION
DA-90412

СКАНУЙТЕ QR-КОД ЗАРАЗ ...
... і знайдіть продукти

Компанія ERC
Tel. +44 230 34 74;
+44 390 55 10
network@erc.ua
www.erc.ua

IoT + «УМНЫЙ ДОМ»

Хотя так называемым технологиям межмашинного обмена находят все больше применений, ряд их особенностей остаются за пределами внимания потенциальных разработчиков локальных IoT-систем. Что здесь имеется в виду? В первую очередь, IoT рассматриваются как комплексы, предназначенные для учета расхода воды, газа, электроэнергии в городских условиях, а также для предоставления иных централизованных услуг с единым мощным потребителем результатов. Это будут различные «водоканалы», «облэнерго», «облгазы» – организации, которые работают с большими массивами оконечных устройств, показания с которых необходимо снимать и обрабатывать. Эта группа потребителей будет рассматривать не только вопросы монетизации внедрения новых услуг, но и их экономическую целесообразность.

Тем не менее, есть другая группа потенциальных потребителей, которые вполне могут решать локальные задачи – обеспечение безопасности определенной территории (заводы, фабрики, дачные поселки, склады, школы, и т.д.). Важным фактором здесь является платежеспособность клиентов. Но если речь идет об охранных системах, то необходимо обеспечить мгновенную передачу информации о срабатывании датчиков с терминальных устройств на центральный узел. В этом случае работа по расписанию неуместна.

Мы не будем анализировать, какой из двух вариантов решения (LoRaWAN или NB-IoT) имеет лучшие экономические показатели внедрения и эксплуатации. Но то, что обе системы в принципе могут обеспечить решение охранных задач, не вызывает сомнений.

То же самое можно сказать о системах безопасности зданий и сооружений, где незаметная установка множества датчиков движения с последующей активизацией камер видеонаблюдения может принести определенные плоды. Ведь датчики движения и сами терминальные устройства имеют небольшие размеры, а их количество практически ограничено лишь разумной целесообразностью.

Даже для домашнего применения такие решения могут обладать определенным смыслом, ведь такие терминальные устройства не требуют внешнего питания, их наличие и место установки трудно обнаружить. Срабатывание датчика в критической ситуации будет мгновенным, что не позволит злоумышленнику оперативно произвести какие-то неправомерные действия или отключить систему безопасности, поскольку она будет распределенной и иметь автономную систему электропитания. Любые критические срабатывания датчиков будут переданы хозяину микро-IoT-системы (или охранной структуре) с указанием, что именно сработало и где.

Но все описанное требует информированности ИТ-специалистов по безопасности о наличии таких возможностей.

Хотя при внедрении «умных» (IoT) счетчиков электроэнергии, воды и газа ничего не стоит подключить сразу же IoT-датчики охранной сигнализации. Было бы логично, если бы все это устанавливалось (пусть даже как опция) сразу же после ввода дома в эксплуатацию на все возможные системы.

И здесь уже вполне уместно говорить об интеграции систем «умного дома» с «интернетом вещей». Ведь системы «умного дома», как правило, используют проводные соединения для связи с локальным управляющим контроллером. А оборудование IoT рассматривает радиоканал как среду, по которой данные передаются в систему учета.

Объединение систем учета, управления домашними элементами и системами безопасности технологически вполне возможно именно на базе IoT.

Как видно из приведенной выше формулы (1), частота немодулированного сигнала при ЛЧМ линейно нарастает от минимального f_{min} до максимального значения f_{max}.

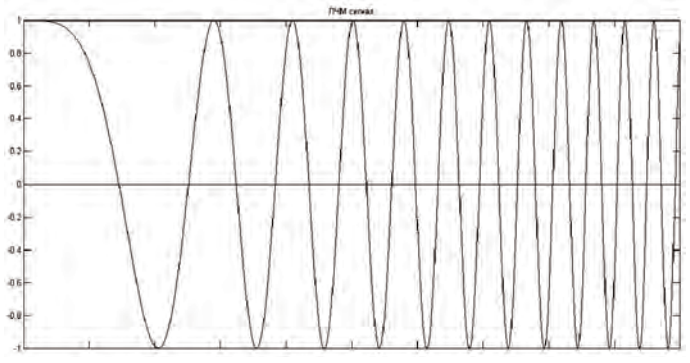


Рис. 1. Пример ЛЧМ-сигнала

Временная функция такого сигнала имеет вид, приведенный на **рис. 1**, а аналитическое выражение представляет из себя гармоническую функцию:

$$x(t) = A_0\cos[2\pi\cdot(f_0 t + t^2\mu/2)], \quad (2)$$

где f_0 — центральная частота радиосигнала;
$-T_c/2 \leqslant t \leqslant T_c/2$.

Перейдем теперь, собственно, к модуляции (манипуляции) ЛЧМ-сигнала. Если в амплитудной модуляции можно ступенчато менять амплитуду сигнала, в частотной — частоту, в квадратурной — амплитуду и знак синусной и косинусной составляющих, то в ЛЧМ этот простой способ вариации параметров сигнала уже не срабатывает, поскольку в процессе передачи непрерывно меняются как частота, так и фаза.

Для того, чтобы передать хотя бы один символ, нам следует обеспечить как минимум два хорошо различимых варианта сигнала. Это легко сделать. Например, символу «0» будет соответствовать посылка, в которой частота нарастает от минимума до максимума. А символу «1» — сигнал, в котором частота будет снижаться от f_{max} до f_{min}. В данном случае кратность модуляции будет равна единице — однократная модуляция. Под кратностью понимают количество двоичных символов, которые закодированы в сигнальном созвездии. Но такая кратность, как правило, недостаточна, ведь другие сигнальные созвездия, как, например, КАМ-16/32/64/128/256, обеспечивают передачу соответственно от 4 до 8 бит на посылку.

Решение задачи поиска эффективного сигнального созвездия было найдено и состоит оно в том, что при фиксированной длине посылки T_c и заданной величине скорости изменения частоты μ различные варианты сигнала формируются за счет сдвига начальной частоты на величину $k\cdot\Delta f$, где $k = 0,1,2,...(2^{SF}-1)$ (**рис. 2**). В данном случае SF — это кратность модуляции, которая определяет базу радиосигнала

$$B = (f_{max} - f_{min})T_c = 2^{SF}. \quad (3)$$

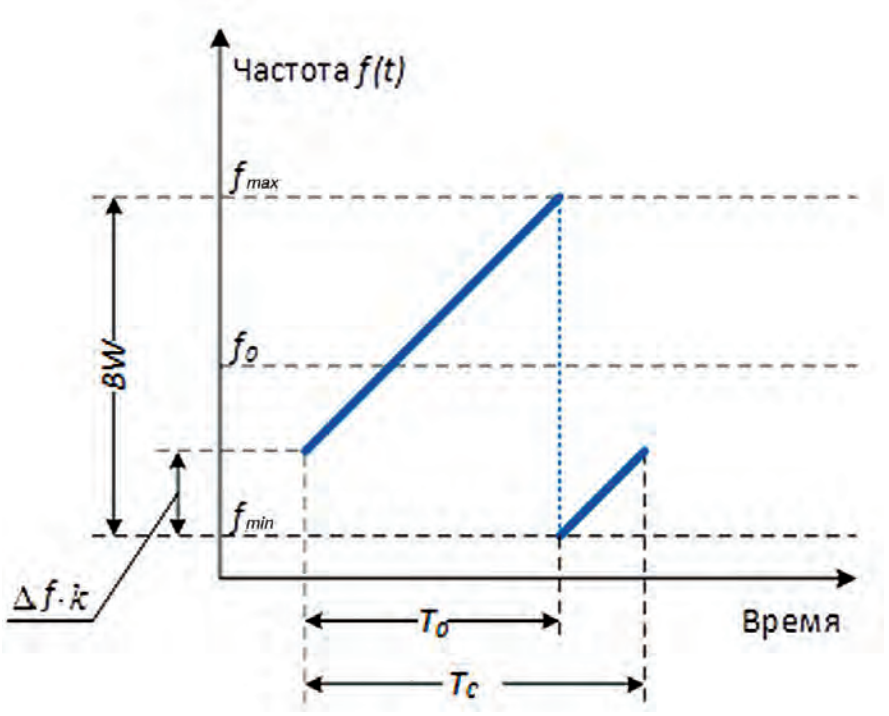


Рис. 2. Формирование сигнального созвездия за счет позиции начальной частоты $f_н = f_{min} + k \cdot \Delta f$

Другими словами, N-кратная модуляция предусматривает 2^N вариантов сигнального созвездия. Поэтому Δf можно определить как

$$\Delta f = (f_{max}-f_{min})/2^N. \quad (4)$$

При этом частота изменяется во времени линейно; угол наклона определяется фиксированной величиной μ. Поскольку в этом случае частота генерации f достигнет f_{max} быстрее, чем в базовой варианте, то после наступления события $f = f_{max}$ происходит «сброс» до $f = f_{min}$ и сигнал начинает снова вырабатываться, начиная с минимальной частоты. И это все продолжается до завершения длительности посылки T_c.

Формирование следующей посылки сигнала начинается с частоты $m \cdot \Delta f$, где значение m определяется очередной битовой группой.

В результате мы получим условное «созвездие» из 2^{SF} сигналов, первый из который (с номером 0) будет иметь нулевой сдвиг относительно исходного ЛЧМ-сигнала, второй — будет иметь начальный сдвиг, равный Δf, третий вариант — со сдвигом $2 \cdot \Delta f$ и т.д. Последняя модификация будет иметь сдвиг $(2^{SF}-1) \cdot \Delta f$, не достигнув всего лишь величины Δf от верхней частоты диапазона f_{max}.

Итак, задача формирования разновидностей модулированного сигнала решена. Хотя есть и нюансы, например, входную битовую последовательность желательно пропустить через скремблер, чтобы избавить модулятор от длинной последовательности нулевых или единичных символов. Ведь в этом случае фаза генерируемого сигнала меняться не будет, что может вызвать проблемы на приемной стороне.

Прием и распознавание сигналов с целью определения передаваемого варианта из последовательности $k = 0,1,2,...(2^{SF}-1)$ выполняется с помощью согласованного фильтра. Это стандартная процедура, которая используется в алгоритмах оптимального приема сигналов, когда находится максимум корреляционной функции путем сравнения принимаемого сигнала со всеми возможными существующими 2^{SF} вариантами. Детально останавливаться на этом вопросе мы не будем.

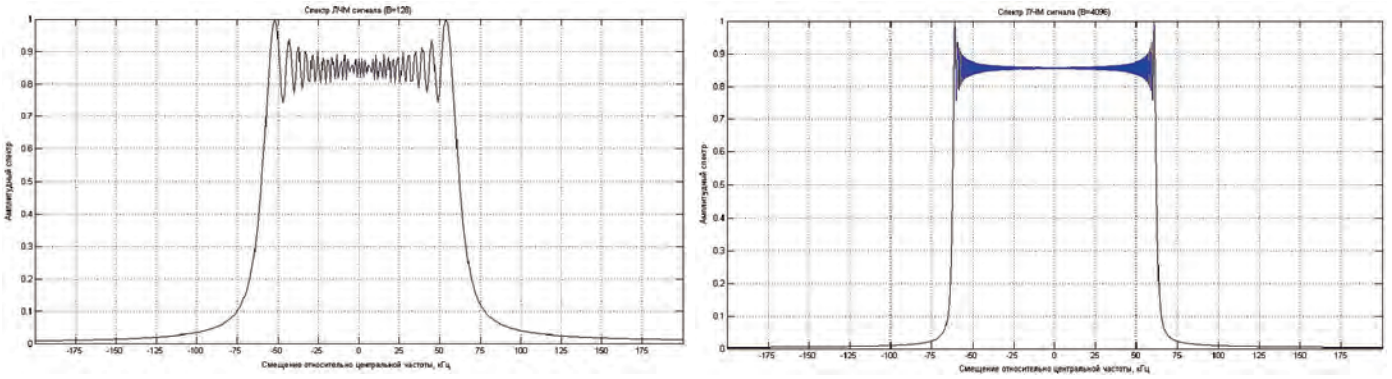


Рис. 3. Ширина спектра ЛЧМ-сигнала для варианта семикратной (B = 128, SF = 7) (слева) и двенадцатикратной модуляции (B = 4096, SF = 12) (справа) зависит только от ширины диапазона используемых частот

Отметим также, что в документации по технологии LoRa величина SF (Spreading Factor) переводится иногда как «коэффициент расширения спектра». Но как легко показать, ширина спектра ЛЧМ-сигнала практически зависит только от разности верхней и нижней частот (**рис. 3**), от кратности модуляции SF практически не зависит. Как видно из иллюстрации, основная энергия сигнала сосредоточена в диапазоне частот между f_{min} и f_{max}. Поэтому корректно все же об SF говорить как не о коэффициенте расширения спектра, а как о кратности манипуляции.

IoT: СКОРОСТЬ — НИЗКАЯ, ДАЛЬНОСТЬ — ВЫСОКАЯ

Когда говорят о том, что количество данных, передаваемых в системе IoT, незначительно, то это справедливо лишь для части приложений, например, при передаче показаний квартирных счетчиков. Но можно найти и такие варианты применения, когда данных будет много, и даже очень много. За примерами далеко ходить не нужно – подготовка к старту космического корабля, очевидно, требует передачи гигантского объема телеметрической информации. И здесь речь не идет о достаточной энергоемкости систем питания оконечного оборудования или об экономии пропускной способности канала связи – данных реально чрезвычайно большое количество и поступают они с невероятно высокой скоростью. В этом случае мы также можем говорить о системе IoT, но отличия от низкоскоростных систем съема показаний за оказанные коммунальные услуги будут принципиальными.

Но это предельный случай системы сбора данных, причем он не носит массовый характер. Тем не менее на заводах по выпуску сложной техники потоки данных могут оказаться практически непрерывными и носить явно выраженный двунаправленный характер. В этом случае использование универсальных технологий LoRaWAN и NB-IoT, являющихся по определению полудуплексными, может оказаться неприемлемым.

Это значит, что в каждом конкретном прикладном случае следует выполнить детальный анализ задачи и принять решение о том, какие из существующих систем подойдут наилучшим образом. А возможно, что в каких-то случаях это будут гибридные решения, или даже с компонентами, которые придется специально разрабатывать для конкретной системы.

Все это свидетельствует о том, что выбор той или иной системы IoT является отдельной задачей и универсального решения здесь просто может не оказаться.

Как установить скорость передачи

В процессе обмена сообщениями между шлюзом и оконечными устройствами для каждого конкретного канала связи (с учетом уровня сигнала и помеховой обстановки) выбираются оптимальные параметры модуляции (SF = 7,...12) и способ кодирования. Первый показатель задает количество бит, передаваемых на протяжении одной элементарной посылки сигнала. Простое кодирование с обнаружением и/или исправлением ошибок (доступны варианты, когда на 4 информационных символа приходится от 0 до 4 проверочных) несколько снижает скорость (до двух раз), тем не менее, позволяя повысить помехозащищенность.

Самую высокую скорость в канале обеспечивает 7-кратная модуляция со 128 вариантами ЛЧМ-сигнала (SF=7). При этом длительность посылки T_c определяется по формуле

$$T_c = 2^{SF}/(f_{max} - f_{min}). \quad (5)$$

Поскольку ширина спектра сигнала обычно является константой (для стран Европы и Украины она составляет 125 кГц), то длительность посылки зависит исключительно от выбранного способа манипуляции или, что то же самое, от ее кратности. Так, при SF = 7 легко найти, что T_c = 1,024 мс. Поскольку за указанное время передается 7 бит, то за одну секунду может быть передано 6836 бита, что, собственно говоря, и определяет битовую скорость передачи символов в 6836 бит/с (при SF = 7 и $f_{max} - f_{min}$ = 125 кГц).

Если мы повысим кратность манипуляции, например, до значения 8, то длительность посылки сигнала, как следует из формулы (3), вырастет в два раза и составит 2,048 мс, а скорость передачи упадет в два раза, до 3906 бит/с. Если качество канала связи недостаточно хорошее, то длительность посылки можно увеличивать и далее, вплоть до T_c = 32,768 мс, что соответствует 12-кратной манипуляции (SF = 12) и количеству вариантов сигнала на длительности посылки, равному 2^{SF} = 4096). В этом случае скорость передачи символов снизится до величины 366 бит/с, а с учетом кодирования CR = 4/8 этот показатель может уменьшиться еще в два раза — до 183,11 бит/с.

В результате мы видим, что модуляция LoRa является достаточно гибким инструментом, обеспечивающим при использовании ЛЧМ-сигналов передачу информации со скоростью от 186 бит/с до 6836 бит/с. К слову, стандарт LoRa предусматривает возможность перехода на частотную манипуляцию FSK (Frequency Shift Keying), при которой скорость можно поднять до 50 кбит/с. Но помехозащищенность такой передачи гораздо ниже и данный тип связи может использоваться в специальных случаях, например, при коротких расстояниях между оконечными устройствами и шлюзом.

Механизм синхронизации в LoRa

Для успешного функционирования любой системы обмена информацией необходима взаимная синхронизация приемника и передатчика, позволяющая определить временные границы приема-передачи как целого блока данных (или кадра), так и единичных символов.

Технология LoRa использует асинхронный режим приема-передачи, при котором передатчик может начать генерацию радиосигнала в любой момент времени. Это так называемый протокол ALOHA. В этом случае требуется механизм, обеспечивающий синхронизацию приемника по сигналу от передатчика. В качестве такового используется преамбула, предшествующая каждому сеансу связи. Она включает в себя последовательность символов, позволяющих приемнику обнаружить активность передатчика, определить используемую кратность модуляции (SF), длину посылки T_c и выполнить символьную синхронизацию.

Таким образом, когда оконечное устройство принимает решение о необходимости передать информацию в сторону шлюза, оно посылает в радиоканал преамбулу — по сути это посылки обычного ЛЧМ-сигнала с длительностью T_c, определяемой кратностью модуляции, частота которого линейно меняется от f_{min} до f_{max}. Количество таких посылок задается при настройке системы. После преамбулы следуют две стартовые посылки с ниспадающей частотой, которые необходимы для уведомления приемника о начале передачи символов (**рис. 4**).

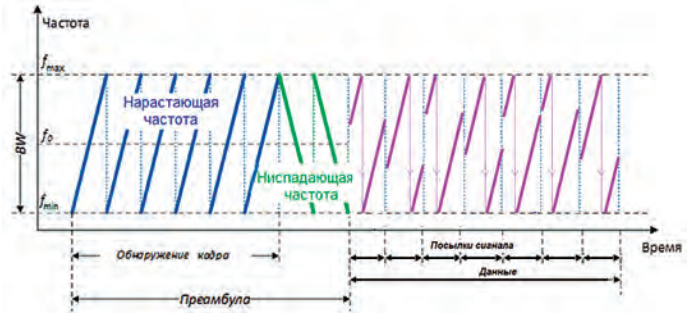


Рис 4. Преамбула, сигнал синхронизации и рабочие посылки LoRa при работе системы

И все вроде бы хорошо в асинхронной передаче и приеме. Особенно, когда в системе всего один передатчик. А вот когда их количество возрастает до сотен или тысяч, неминуемы коллизии, когда возможна накладка друг на друга сигналов, формируемых разными устройствами. В этом случае приемник (шлюз или базовая станция) демодулируют сигнал с ошибками. Эта ситуация коллизий отслеживается, и терминальное устройство отправляет пакет данных повторно через некоторое произвольное время задержки. Аналогичным образом поступает и устройство, за счет которого произошла коллизия. Если шлюз обнаруживает, что пакет данных принят неверно, он не отправляет подтверждающий сигнал, тем самым вынуждая оконечное оборудование повторять передачу.

Классы устройств LoRa

Длительное время работы батарей питания устройств LoRaWAN обеспечивается регламентом функционирования оконечного оборудования, в соответствии с которым передача данных выполняется по установленным в системе правилам. Поскольку работа со шлюзами осуществляется в полудуплексном режиме, то после инициации

ПРАВА ЛИ ВИКИПЕДИЯ?

Всемирная энциклопедия утверждает, что «Интернет вещей является частью более широкой концепции домашней автоматизации, которая может включать освещение, отопление и кондиционирование воздуха, медиа-системы и системы безопасности, а также системы видеонаблюдения». Но с этим утверждением весьма трудно согласиться. Возможно, все наоборот, а именно, «Различные домашние системы и пр. сами являются лишь подсистемами Интернета вещей». Как бы то ни было, но практика внедрения в Украине решений на базе технологий LoRaWAN и NB-IoT только подтверждает факт, что Интернет вещей не следует объединять с технологиями «умного дома». Хотя охранные системы, контроль доступа и периметра вполне могут использовать низкоскоростные радиоканалы IoT при создании охранных комплексов.

соединения и передачи данных на шлюз терминальное устройство автоматически переходит в режим приема, чтобы получить подтверждение данных от шлюза или обеспечить изменение настроек. Такой алгоритм работы характерен для устройств ***класса A***, которые не могут по своему желанию произвольно переключаться в режим приема информации от шлюзов, даже если вдруг такая необходимость возникнет.

Однако оборудование ***класса B*** такой возможностью уже обладают. Для этого зарезервированы дополнительные окна приема по расписанию. Чтобы начать прием данных, оконечное устройство синхронизируется по специальным сигналам от шлюза (по маякам). Очевидно, что наличие такой возможности снижает время автономной работы.

И, наконец, иногда бывает необходимо обеспечить возможность получения на стороне оконечного оборудования непрерывных или больших объемов данных и при этом не требуется длительная работа от автономного источника питания. В этом случае используется оборудование ***класса C*** (Class C) с максимальным приемным окном. Такие устройства могут получать данные от IoT-шлюзов практически в непрерывном режиме. Приемное окно закрывается лишь на время передачи данных.

NB-IoT

Столь детально рассказав об особенностях модуляции LoRa, хотелось бы также остановиться на другом LPWAN-решении — системе ***NB-IoT (Narrow Band Internet of Things)***. Этот стандарт разработан консорциумом 3GPP в июне 2016 года для организации низкоскоростной передачи данных по каналам мобильных сетей связи.

NB-IoT является одним из трех стандартов IoT, предложенных 3GPP для сотовых сетей связи: eMTC (enhanced Machine-Type Communication), NB-IoT и EC-GSM-IoT. При этом eMTC обладает наибольшей пропускной способностью и разворачивается на оборудовании LTE. Сеть NB-IoT может использовать как оборудование LTE, так и устанавливаться отдельно, в том числе поверх GSM. EC-GSM-IoT предоставляет наименьшую пропускную способность и разворачивается поверх сетей стандарта GSM.

Важно отметить, что NB-IoT обладает стандартными свойствами сетей LPWAN: оборудование работает в полудуплексном режиме, ширина полосы пропускания на прием — 180 кГц. Поскольку данная система может работать в частотных диапазонах, используемых для предоставления мобильных услуг LTE и GSM, этот вариант IoT рассчитан, прежде всего, на операторов связи. Ведь в этом случае не нужно приобретать специальные лицензии на частотные диапазоны, а развертывание сети выполняется в основном за счет модернизации базовых станций и установки необходимого программного обеспечения. Все сказанное означает, что сеть NB-IoT может быть построена достаточно оперативно на больших территориях, причем для крупных заказчиков по их требованию для создания IoT-сетей могут быть использованы более низкочастотные лицензионные диапазоны GMS (900 МГц), что позволяет увеличить дальность связи.

Принцип работы NB-IoT

По своей физической структуре и архитектуре сеть NB-IoT практически все унаследовала от LTE, поэтому построение инфраструктуры для IoT требует в основном лишь обновления программного обеспечения на имеющихся базовых станциях.

При формировании LTE-сигнала (**рис. 5**) используется принцип разделения каналов OFDM с разнесением поднесущих на 15 кГц. В DL (Downlink, направление от БС) используется OFDMA, а в UL (Uplink, направление на БС) — SC-FDMA. Весь диапазон LTE разделен на ресурсные блоки (Resource block, RB), каждый из которых состоит из 12 поднесущих с суммарной шириной занимаемой полосы в 12×15 кГц = 180 кГц. Каждый ресурсный блок в свою очередь разделен на 12×7 = 84 ресурсных элемента (Resource element, RE).

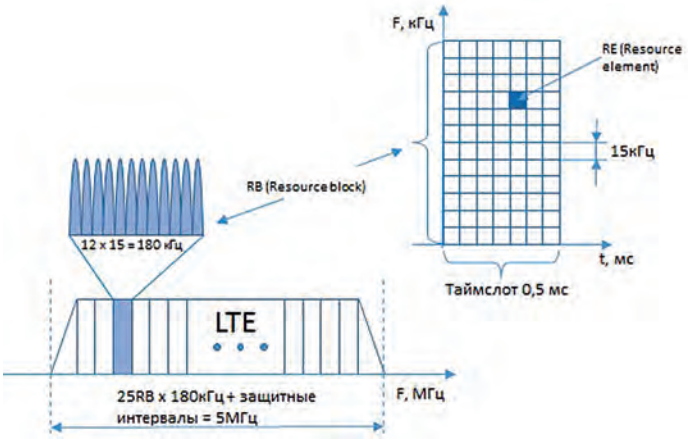


Рис. 5. Передача NB-IoT-сигнала в LTE-диапазоне

Для NB-IoT в полосе LTE задействуется один ресурсный блок с полосой пропускания 180 кГц. Для увеличения дальности передачи сигнал дополнительно усиливают на 6 дБ. Именно поэтому сеть IoT имеет более широкий охват территории, чем LTE.

Запуск сети может осуществляться тремя способами — в зависимости от места расположения ресурсного блока (**рис. 6**):

- внутри полосы пропускания LTE;
- в защитной полосе частот;
- на выделенном канале шириной 200 кГц, который также включает и защитный спектр 300–600 кГц, чтобы избежать помех. Такой способ требует дополнительного выделения частотного ресурса и дополнительных затрат.

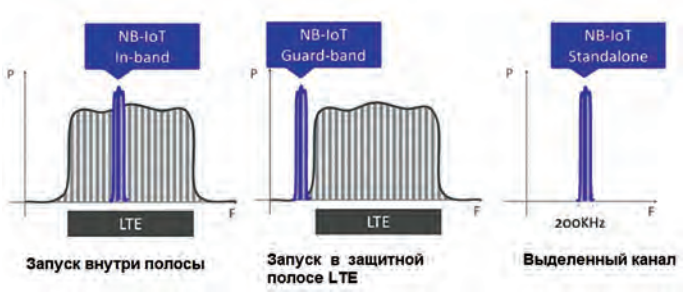


Рис. 6. Три способа организации канала NB-IoT

По информации из интернет-источников, скорость передачи данных в NB-IoT достигает 58,8 кбит/с. Хотя имеются решения, благодаря которым это значение можно повысить до 100 кбит/с. В то же время отечественные операторы мобильной связи настаивают на более высоких доступных скоростях в NB-IoT — 250 кбит/с (выгрузка данных, UL) и 226,7 кбит/с (загрузка, DL). В данном случае скорей всего речь идет о максимальных показателях. Хотя высокая скорость для систем LPWAN — не самоцель.

Пути IoT неисповедимы

Чтобы понять, что же происходит в Украине в части развертывания систем IoT, обратимся к искусству ведения войн. Обычно страны, которые ставили перед собой задачу остановить или замедлить движение противника вглубь своей территории, возводили особого рода системы инженерных защитных сооружений в виде так называемых укрепрайонов (УР), преодолеть которые было достаточно непросто.

Картину, аналогичную преодолению защитных полос, мы сейчас наблюдаем в стремлении IoT-систем найти свое место в современном ИТ-мире. На самом деле Интернет вещей хочет задействовать свободные территории под свои нужды, сформировав новые потребности, о которых раньше никто не задумывался, и тем самым расширить рынок сбыта соответствующих услуг и оборудования. Но все идет не совсем так, как того хотелось бы. Новым технологиям приходится преодолевать «укрепрайоны», которые мешают и замедляют движение вперед.

Итак, в настоящее время мы наблюдаем в нашей стране параллельное развитие двух низкоскоростных технологий передачи данных LoRaWAN и NB-IoT. Однако каких-то мощных схваток на поприще борьбы за крупные проекты пока не наблюдается.

Тройка операторов мобильной связи, обладающих лицензиями на использование LTE-сетей, активно внедряет технологию NB-IoT, обеспечивая возможность ее использования в будущем потенциальными корпоративными заказчиками. С другой стороны, определенные успехи демонстрируют сторонники LoRaWAN, которые реализуют небольшие проекты, часть из которых относится к пилотным, а другие — к ознакомительным. Сложно назвать крупными внедрения, на которых установлено всего несколько десятков терминальных устройств.

Рассмотрим более детально ситуацию, которая сложилась в отрасли IoT в нашей стране.

В 2018 году оператор сотовой связи ***lifecell*** в партнерстве с ТОВ ***«Интернет вещей Украина»*** (IoT Ukraine) начал разворачивать первую в Украине сеть национального масштаба для предоставления IoT-услуг. На первом этапе реализации проекта в коммерческую эксплуатацию была запущена сеть LoRaWAN, которая работает в выделенном для европейских стран диапазоне 868 МГц. Сообщается также о тестировании сети NB-IoT, которая построена на оборудовании Ericsson и Huawei.

При развертывании системы LoRaWAN было использовано оборудование Cisco, а также IoT-платформа Actility. Для продвижения IoT-решений создан веб-сайт *https://iot.lifecell.ua*, на котором размещается информация о реализованных проектах. Кстати, все из них выполнены по технологии LoRaWAN:

- «Умные» уличные светильники (Smart steet Lights);
- Smart Agriculture (Разумное сельское хозяйство);
- Smart Metering («Умный» учет для «Кировоградгаз», «Луцкводоканал», «Львовоблэнерго», «Водоканал Петропавловский»);
- Smart Environment (Мониторинг качества воздуха).

Информация о количестве подключенных на данный момент терминальных устройств для указанных внедрений отсутствует.

В начале 2020 года ***«Vodafone Украина»*** запустила сеть NB-IoT, которая представляет собой выделенный частотный канал для IoT-оборудования на существующей сети LTE (диапазон 1800 МГц). Тестирование было проведено на фрагментах сети оператора в Киеве с использованием клиентского оборудования, предоставленного компанией «Киевводоканал».

В сентябре 2021 года в коммерческую эксплуатацию запущена услуга «Умный учет воды». Данное решение позволяет клиентам развернуть систему по автоматизированному сбору и учету использования водных ресурсов. Оно включает в себя «умные счетчики» со встроенным модемом, которые могут передавать показания на сервер для их дальнейшего коммерческого и технологического учета. Наличие веб-интерфейса позволяет клиентам получать доступ к агрегированным и индивидуальным данным потребления ресурсов. Платформа позволяет также выгружать сведения во внутренние системы заказчика в различных форматах или по API. Решение рассчитано на коммунальные предприятия, ОСМД и другие заинтересованные структуры.

Работы по развертыванию сети NB-IoT проводит также ***«Киевстар»*** на базе существующей сети LTE путем обновления конфигураций базовых станций. Для развития сетей NB-IoT используются частотные диапазоны 900 МГц или 1800 МГц в зависимости от конкретной ситуации.

В частности, уже выполнено несколько пилотных проектов с городскими водоканалами — Smart Metering (мониторинг и учет показателей в коммунальных сетях); «Умное» освещение — партнерский проект с компаниями «Радий» и «Одис-W» по управлению тысячами городских светильников; «Электронный билет», который вместе со своими партнерами «Киевстар» реализовал в Мариуполе. Ожидается масштабирование аналогичных проектов в других городах Украины.

При этом серверы приложений могут размещаться у заказчика в специально оснащенных помещениях, или же в облачной инфраструктуре собственного дата-центра оператора. Для этого используются решения Microsoft Azure Cloud и Azure Stack. Если заказчик хочет получить решение «под ключ», то в этом случае ПО для сервера может предоставляться оператором.

Для работы устройств в сети NB-IoT используются USIM-карты, функционал которых предусматривает наличие мобильного номера (MSISDN). В приложениях такие устройства идентифицируются благодаря ключам и различным алгоритмам, что обеспечивает безопасность подключений.

В январе 2021 года украинский системный интегратор IoT-решений — ***iotji by DEPS*** — завершил первый этап построения LoRaWAN-системы для ПрАТ «А/Т Тютюнова компанія «В.А.Т.-Прилуки». Команда iotji (являющаяся подразделением компании DEPS), развернула сеть беспроводных IoT-устройств на территории фабрики. Несколько десятков точек учета были оборудованы датчиками с LoRa-модулями, которые каждый час предают информацию о потребляемых объемах воды в учетную систему предприятия.

Получив положительный опыт эксплуатации на первом этапе внедрения проекта, было решено приступить ко второму этапу, который на текущий момент также завершен. Существующая подсистема учета воды была расширена путем добавления нескольких десятков дополнительных счетчиков и импульсных датчиков к ним. А также реализована новая подсистема проекта — технический учет электричества. Для этого были выбраны электросчетчики Teletec украинской компании «Телекомунікаційні Технології», которые подходят для технического и коммерческого учета расхода электроэнергии. При этом они обеспечивают встроенную поддержку технологии LoRaWAN (класс C). Одной из их особенностей является режим работы «запрос-ответ». Чтобы узнать текущие показания, сервер приложений должен отправить на устройство предварительно сформированный запрос, что несколько отличается от традиционного режима ALOHA работы сетей LoRaWAN.

В настоящее время все три украинских оператора мобильной связи объявили о доступности коммерческих услуг NB-IoT на своих LTE-сетях. На самом деле данные сети обеспечивают скорее потенциальные возможности подключения терминального оборудования и корпоративных клиентов к низкоскоростной системе сбора данных. Но реальные проекты IoT под ключ предполагают также установку терминального оборудования на объектах, принадлежащих крупным заказчикам или абонентам коммунальных сетей. И здесь обойтись только выделением необходимых IoT-каналов в сети NB-IoT и предложением SIM-карт будет недостаточно. Несмотря на проведенные работы по модернизации LTE-сетей и предоставление сетевых возможностей по передаче данных, о количестве реализованных проектов и установленном абонентском оборудовании информацию получить не удалось. Большей частью сети IoT — это, пусть и апробированные на оборудовании потенциальных заказчиков, но все же пилотные или тестовые системы.

LoRaWAN против NB-IoT

Поскольку LoRaWAN и NB-IoT находятся в одной узкой нише LPWAN-систем, между ними не может не возникнуть конкуренция. Оборудование LoRaWAN не привязано к сотовым сетям мобильной связи и передача данных осуществляется асинхронно. За счет этого устройства LoRaWAN затрачивают на передачу информации в три-пять раз меньше времени, чем оборудование, работающее в других системах LPWAN, в частности, NB-IoT. Это значит, что ресурс батарей существенно экономится.

Скорость передачи данных в сетях NB-IoT — 50–200 кбит/с, в LoRaWAN — от 300 бит/с до 50 кбит/с. NB-IoT — это более эффективный протокол IoT для «более быстрых» приложений. Для большинства случаев устройствам LoRaWAN вполне достаточно имеющихся скоростей передачи данных.

Технологию NB-IoT реально могут развивать лишь операторы мобильной связи, уже имеющие развитую инфраструктуру. Т.е. NB-IoT — это решение преимущественно для операторов. Для внедрения новых сервисов им достаточно заменить в основном лишь ПО базовых станций, так что IoT для операторов на первый взгляд не выглядит сверхдорогим решениям. В то же время крупные предприятия могут создавать свои собственные локальные системы LoRaWAN, легко подключаемые к общественным сетям, как к мобильным, так и фиксированным.

LoRaWAN уже принят в качестве стандарта сети IoT во многих странах, включая США, Австралию, Новую Зеландию, Тайвань и Нидерланды. Экосистема LoRa намного шире экосистемы NB-IoT. Например, в LoRa Alliance входит более 500 компаний — разработчиков аппаратного и программного обеспечения, а также операторы связи LoRaWAN.

Но окончательные выводы о победе какой-либо технологии делать рано. Возможно, лавры вообще никому не достанутся. Ведь некоторые критики весьма серьезно сомневаются в реальной необходимости установки интеллектуальных счетчиков для удаленной передачи их показаний в центральные узлы соответствующих служб. Сейчас эти

показания снимают сами жильцы и передают их по назначению (опять же, очень часто — именно дистанционно) раз в месяц. Трудоемкость процедуры не очень высокая. А вот стоимость умных счетчиков для частных потребителей может оказаться неподъемной. Будут ли решение этой задачи брать на себя отечественные компании-монополисты, предоставляющие коммунальные услуги — это большой вопрос.

В то же время серьезные перспективы демонстрируют так называемые системы промышленного Интернета вещей (IIoT). В этом случае предприятия могут предпочесть разворачивание собственных IoT-сетей на базе технологии LoRaWAN, чтобы не оказаться в зависимости от конкретного оператора связи, предоставляющего неконтролируемые заказчиком каналы связи.

Интернет вещей, как технология низкоскоростной передачи данных на большие расстояния, имеет большие перспективы. С появлением новых разновидностей оконечного оборудования и решения вопросов его интеграции в существующие системы учета и контроля возможно произойдет объединение разнородных решений («умный дом», системы безопасности и др.). Хочется верить, что в ближайшем будущем будут созданы условия для внедрения как собственно технологий IoT, так и смежных решений.

Владимир СКЛЯР, **СиБ**

ХРОНИКА

Cloudflare пережила «крупнейшую DDoS-атаку в истории»

Компания Cloudflare, мировой провайдер услуг доставки контента, DNS и защиты от DDoS-атак, летом этого года сама столкнулась с масштабнейшей атакой такого типа. Компания сообщила, что в июле ее автономные краевые системы защиты от DDoS выявили и остановили атаку мощностью 17,2 млн запросов в секунду (rps). Для сравнения: Cloudflare в среднем обрабатывает за секунду 25 млн запросов HTTP. Таким образом, объем атаки составил 68% легитимного трафика (**рис.**).

Атака была запущена мощной бот-сетью и была нацелена на клиента Cloudflare из финансового сектора. Атака длилась меньше минуты, и за это время бот-сеть обрушила на краевую инфраструктуру Cloudflare 330 млн запросов. В течение 15 секунд нагрузка держалась на уровне 15 млн rps. Бот-сеть состояла из более чем 20 тыс. зараженных IoT-устройств из 125 стран, в том числе 15% атак шли из Индонезии и еще 17% приходилось на Индию плюс Бразилию.

По утверждению Cloudflare, это была самая крупная DDoS-атака, с которой компания когда-либо сталкивалась, и по объему она почти в 3 раза превосходила любую другую атаку, о которой сообщалось в прессе. Кроме того, данная бот-сеть с тех пор еще не раз давала о себе знать, а в августе она запустила против другого клиента Cloudflare (хостинг-провайдера) DDoS-атаку с пиковым объемом 8 млн rps.

Также Cloudflare фиксирует рост активности другой бот-сети, которая насчитывает 28 тыс. ботов и базируется на варианте известного вредоносного ПО Mirai (этот код впервые проявился в 2016 году и захватывал устройства под управлением Linux, такие как маршрутизаторы и камеры видеонаблюдения). Из проведенных бот-сетью DDoS-атак часть по объему превышала 1 Тбит/с. В некоторых случаях атаки длились всего несколько секунд.

Система защиты от DDoS, с помощью которой Cloudflare удалось остановить атаки, базируется на программном демоне собственной разработки. Эти демоны работают во всех ЦОД Cloudflare и асинхронно анализируют образцы трафика на предмет DDoS-атак. При выявлении атаки система в реальном времени вырабатывает правило ее блокировки.

Брайан Хонан, независимый консультант из Ирландии, в комментарии SANS Institute отметил: DDoS-атаки стали настолько распространены, что для хостинг-провайдера не иметь защиты

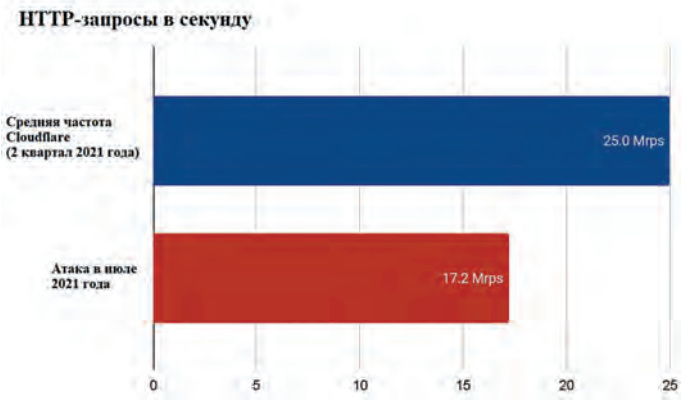


Рис. Объем июльской DDoS-атаки по сравнению с типичным числом запросов HTTP (данные Cloudflare)

от DDoS – это все равно, что пользоваться почтой без спам-фильтра. При этом преступники продолжают совершенствовать свои инструменты и в этой области, что требует постоянных инноваций со стороны защитников. Другой аналитик, Ли Нили из Ливерморской национальной лаборатории, полагает, что мощные и скоротечные DDoS-атаки становятся трендом. Команды мониторинга и реагирования, работающие в SOC, слабо приспособлены к отражению таких атак, а потому на первое место выходит автоматизация.

Между тем, как сообщало в июне аналитическое подразделение Nokia Deepfield, в период с января 2020 года по май 2021-го средний пиковый объем DDoS-атак вырос на 100%, достигнув 3 Тбит/с, причем большинство самых мощных атак генерируются из инфраструктуры менее чем 50 хостинг-провайдеров. В частности, DDoS-трафик подскочил на 50% в период с марта по июнь прошлого года, когда началась пандемия COVID-19 и компании по всему миру переходили на удаленную работу. Nokia Deepfield также считает, что растущее количество незащищенных IoT-устройств может потенциально вылиться в DDoS-атаки мощностью 10 Тбит/с и больше. Такие атаки способны «положить» компьютерные сети на уровне целой страны, как это произошло в Бельгии в мае этого года, и даже провайдеры 1 уровня, которые пропускают трафик намного более высокого уровня, могут столкнуться с проблемами.