Новый стандарт для проектов «Умный дом» – Connected Home over IP

Часть 1

Виктор Алексеев (victor.alexeev@telemetry.spb.ru)

Концепция «Умного дома» была впервые сформулирована в документе Building Management System (BMS). До настоящего времени основной проблемой этого направления было отсутствие единого международного стандарта. Учитывая это, крупнейшие мировые концерны Amazon, Apple, Google и Zigbee Alliance в декабре 2019 года создали рабочую группу, названную Project Connected Home over IP (CHIP). Основная цель этой рабочей группы заключается в разработке и продвижении единого стандарта протоколов беспроводной связи с открытым кодом, предназначенных для оборудования, используемого в проектах Smart Home. В 2020 году к проекту CHIP присоединились IKEA, Legrand, NXP Semiconductors, Resideo, Samsung SmartThings, Schneider Electric, Signify (ранее Philips Lighting), Silicon Labs, Somfy и Wulian. В данной статье рассмотрены основные базовые принципы, заложенные в основу проекта CHIP.

Общая структура «Умного дома»

Четвёртая промышленная революция всё больше меняет не только производство, но и всю нашу жизнь, включая жилищное строительство. Всё чаще нам встречается термин Smart Home («Умный дом»). Концепция «Умного дома», впервые сформулированная в документе Building Management System (BMS) в 1986 году [1], основана на использовании компьютерной системы, контролирующей всё энергетическое и бытовое оборудование дома.

Прежде всего, «Умный дом» обеспечивает безопасность и комфорт, а также предоставляет множество дополнительных опций, облегчающих повседневные рутинные работы по дому. Немаловажно и то, что современные проекты «Умного дома» способствуют значительной экономии затрат на электричество, воду и отопление.

В последнее время всё возрастающее значение приобретают проекты квартир и персональных домов, предназначенные для проживания людей с деменцией. Количество людей с этим недугом постоянно увеличивается и к 2050 году может достигнуть по всему миру 155 млн человек [2].

Проекты включают в себя интеллектуальные устройства, предназначенные для отслеживания из любой точки мира состояния и действий пожилых людей. Для этого используются камеры видеонаблюдения, дистанционные переговорные устройства, датчики движения и падения человека, автоматизированные тонометры с передачей информации по Интернету, дозаторы лекарств с голосовым напоминанием и другие аналогичные приборы. Для полноценной реализации в подобного рода проектах должно быть реализовано бытовое оборудование, облегчающее жизнь пожилого человека: умные кровати, инвалидные коляски с электрическим приводом, автоматизированное безопасное кухонное и сантехническое оборудование, роботы-пылесосы, голосовое управление освещением, климат-контролем, шторами и системами вентиляции (см. рис. 1).

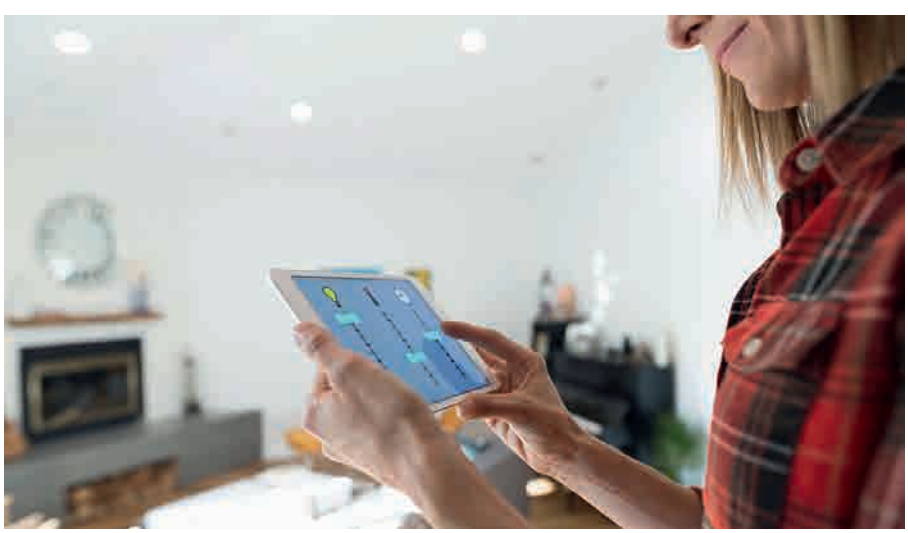

Рис. 1. Гаджеты с большим экраном и крупным шрифтом помогают пожилым людям управлять бытовыми приборами, не вставая с кресла [3]

Стремительно растущий рынок IoT будет вовлекать всё больше и больше новых продуктов в проекты «Умного дома». Рынок мгновенно реагирует на потребности потребителей. Хорошим примером тут служит фирма Intellias, которая в период пандемии COVID-19 разработала IoT-платформу для интеллектуальных холодильников, обеспечивающую поддержку систем корпоративного удалённого питания. За короткое время платформа стала популярной во многих странах мира, и к ней уже подключились сотни тысяч холодильных установок [4].

По данным Harbour Research, чуть меньше половины всех устройств IoT, которые будут установлены по всему миру в ближайшие 20 лет, придётся на проекты «Умного дома» [5]. Согласно оценкам [6], мировой объём рынка «Умного дома», составлявший в 2020 году примерно $80 млрд, увеличится к 2026 году до $314 млрд.

На первом этапе своего существования (1990-е годы) рост индустрии «Умного дома» сдерживался в основном из-за высокой общей стоимости проектов, сложности проводного монтажа оборудования, отсутствия единого стандарта и относительно низких цен на оплату ЖКХ.

Ситуация кардинально изменилась в начале 2000-х годов в связи с интенсивным развитием глобальных и локальных систем беспроводной связи, когда для коммуникации между датчиками, центральным процессором и исполнительными устройствами внутри дома широко стали использовать сети стандартов WLAN. При этом для удаленного контроля проектов «Умного дома» начали применять беспроводные GSM-модемы.

Современные системы «Умного дома»

В любом из предлагаемых сегодня на рынке вариантов «Умного дома» используется примерно одна и та же базовая схема, показанная на рисунке 2.

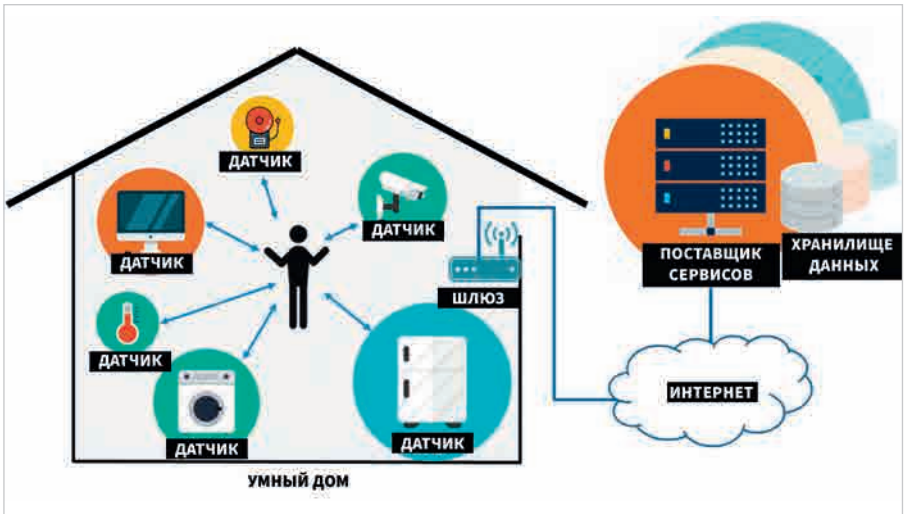

Рис. 2. Типовая базовая структурная схема «Умного дома» [7]

Основная особенность современных проектов «Умного дома», отличающих их от разработок предыдущих поколений, – использование системы беспроводной связи для коммуникации сенсоров и исполнительных устройств с центральным процессором. Интеллектуальные сенсоры и исполнительные устройства подключаются с помощью локальных беспроводных технологий WLAN к центральному контроллеру, который объединяет все устройства «Умного дома» в единую сеть и управляет ими в соответствии с заданной программой.

В структуре «Умного дома» сохраняются также и стандартные проводные интерфейсы электропитания и датчиков. Таким образом, можно пользоваться обычными выключателями, специальным пультом управления или переключать управление в автоматический режим. Связь «Умного дома» на глобальном уровне осуществляется с помощью сетей мобильной связи поколений 2G, 3G, 4G. Поэтому можно контролировать удалённо работу всех систем, находясь в любой точке мира, где есть мобильная связь.

Сегодня различные проекты «Умного дома» позволяют управлять всем оборудованием в трёх основных режимах – вручную, дистанционно и полностью автоматически. Кроме того, поддержка аудиоассистента позволяет также управлять всеми приборами с помощью обычных голосовых команд.

Современные сложные беспроводные системы «Умного дома» обладают множеством разнообразных функций, обеспечивающих управление таким оборудованием как, например:

- охранная и пожарная сигнализации;
- видеонаблюдение в контрольных точках с передачей информации по сети Интернет;
- контроль аварийной протечки водопровода и систем отопления;
- контроль систем электропитания с переключением на резервный источник;
- удалённое управление гаражными воротами, рольставнями, уличным освещением;
- автоматизированный климат-контроль по заданному графику;
- контроль содержания вредных веществ в воздухе помещений (окись и двуокись углерода, летучие органические соединения);
- удалённый контроль и автоматизированное управление кухонным оборудованием;
- робот-пылесос (автоматическая уборка по заданному графику);
- электронный секретарь (обработка телефонных вызовов, календарь запланированных дел и платежей, голосовые напоминания);
- удалённое управление телефоном с громкой связью, телевизором, домофоном, проигрывателем, проектором с помощью голосовых команд или смартфона;
- видеоняня – круглосуточный контроль за младенцем;
- системы климат-контроля в винном погребе;
- удалённый контроль минерального состава и влажности почвы в саду и цветниках (команды контроллера);
- оптимальный автоматизированный режим полива растений в саду и цветниках (команды контроллера);
- возможность масштабирования системы за счёт монтажа дополнительного оборудования.

Потенциал «Умного дома» привлекает огромное количество производителей, системных интеграторов и поставщиков услуг. В результате появляются новые продукты и решения, использующие традиционные технологии и комплектующие. Это, в свою очередь, приводит к невозможности совместной работы датчиков и управляющих устройств от разных брендов.

В простейших системах «Умного дома», таких как «Комплект умный дом Xiaomi Mi Smart Sensor Set», несколько датчиков одного стандартного интерфейса управляются непосредственно самим смартфоном [9].

В более сложных проектах «Умного дома» комплект оборудования может состоять из множества самых различных сенсоров и исполнительных устройств. В настоящее время на рынке доминируют три крупнейшие мировые экосистемы для «Умного дома»: Amazon Alexa, Google Home (Google Assistant) и Apple HomeKit.

Различные производители используют ранее принятую технологию связи между датчиками и управляющим процессором. Чаще всего используются Wi-Fi, Bluetooth (BLE), Zigbee и Z-Wave. Также существуют проекты с использованием LPWAN-технологий нелицензионного диапазона частот ISM: 802.15.4, Thread, LoRa, SIGFOX, Weightless, «ВАВИОТ».

Одним из интересных направлений в конкурентной борьбе за рынок «Умного дома» являются проекты, в которых всё оборудование разбивается на группы устройств, каждая из которых управляется собственным ведущим. Это даёт возможность мелким производителям и стартапам выйти на рынок с продукцией, предназначенной только

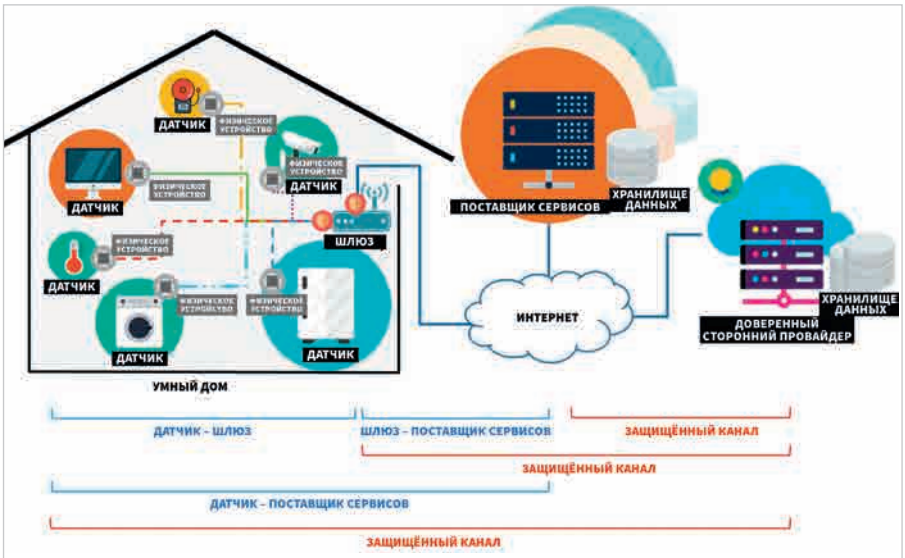

Рис. 3. Схема проекта «Умного дома» с иерархической топологией контроля оборудования [10]

для определённого сегмента. Например, такое бытовое оборудование, как системы отопления и климат-контроля, холодильники, кухонное оборудование, имеют один тип интеллектуальных сенсоров. В системах видеонаблюдения, телевизорах, охранных сигнализациях используются другие сложные автоматизированные датчики. Для управления освещением, замками, шторами и другими аналогичными устройствами используются простейшие датчики с микропотреблением электроэнергии. Для управления этими устройствами можно задействовать различные типы контроллеров.

На рисунке 3 показана схема проекта «Умного дома» с иерархической топологией контроля оборудования.

Сенсорные сети в этом проекте разделены на три класса в зависимости от назначения и технических возможностей: нижний, средний и высший. Интеллектуальный сенсор высшего уровня предназначен для выхода через точку доступа (AP) в сеть Интернет, а также для управления сенсорами среднего уровня. Интеллектуальные сенсоры среднего уровня управляют простейшими датчиками нижнего уровня. Сенсоры среднего класса взаимодействуют только с ближайшими датчиками низшего и высшего классов и не имеют выхода во внешние сети.

Датчик низшего класса общается только с ближайшим к нему сенсором среднего класса. Все сенсоры оснащены уникальными ключами, представляющим собой чип, который нельзя физически скопировать. Сеансы связи предполагают предварительную взаимную аутентификацию сенсоров и согласование ключей. Таким образом, указанная схема является безопасной и эффективной по сравнению с другими методами с одним центральным управляющим микрокомпьютером. Авторы этой работы считают, что предложенная ими схема соответствует требованиям, предъявляемым к нейронным эхо-сетям (ESN, echo state networks) [11], и может быть использована в смешанных сетях.

Нейронные сети ESN позволяют интегрировать в проектах «Умного дома» новые технологии IoT, например автономное управление сенсорами и исполнительными устройствами, киберфизические системы и мобильные узлы. В сетях подобного рода можно отказаться от мощного центрального процессора, поскольку в киберфизических системах (cyber-physical system) [12] вычислительные ресурсы распределены по всей физической системе. При этом вычислительные мощности распределяются по сети в иерархическом порядке в зависимости от назначения и сложности сенсоров. Развитие подобных экосистем, основанных на ESN-сетях, позволит подключать к проектам «Умного дома» отдельными блоками оборудование конкретного назначения, например блоки оборудования безопасности, кухонного оборудования, садово-огородный блок и другие подобные комплексные наборы оборудования.

С развитием IoT-технологий пропорционально увеличивается вероятность угроз безопасности. Поскольку современный «Умный дом» представляет собой сложный программно-аппаратный комплекс с большой базой данных, он в принципе уязвим для различного рода злонамеренных попыток взлома систем безопасности, которые могут причинить серьёзный ущерб и даже угрожать жизни людей, находящихся в доме.

Возможны несколько основных потенциальных вариантов утечки данных на следующих этапах передачи информации: «устройство–устройство» (интеллектуальный сенсор), «устройство–координатор», «координатор–шлюз», «устройство–контроллер для локальной сети», «контроллер поставщика услуг IoT и сервисные службы Интернет». Системы безопасности современных проектов «Умного дома» должны обеспечивать надёжную защиту на каждом из перечисленных этапов передачи информации. Основные хакерские технологии взлома систем IoT достаточно хорошо известны: Exploits, Password Attacks, IoT Worms, Unpatched Devices, Legacy Protocol, Cryptojacking и другие [13]. Методы борьбы с этими технологиями подробно описаны [14–17]. Поэтому в этой статье не будет детально рассмотрен этот вопрос.

Поскольку все проекты «Умного дома» предусматривают выход в глобальные внешние сети, перенасыщенные различными вирусами, проблемы безопасности, связанные с Интернет, также крайне важны для этого направления IoT. Даже опытные пользователи, не говоря уже о детях и пожилых людях, могут кликнуть на ссылку, которая запустит механизм заражения вирусами систем, управляющих оборудованием дома. Поэтому необходимо обеспечить комплексную локальную и облачную защиту от заражения вирусами и сетевых атак.

Проект «Умный дом с подключением по протоколу IP»

Отмеченные ранее глобальные проблемы, связанные с индустрией «Умного дома», признают все ведущие мировые производители, поставщики и интеграторы электроники.

Заметный отрыв трёх лидеров рынка от потенциальных конкурентов для Amazon, Google и Apple создаёт определённое преимущество. Однако для остальных компаний и для индустрии «Умного дома» в целом такая ситуация является крайне неприятной. Определённые нарекания, связанные с допол-

нительными неудобствами при выборе и монтаже оборудования, возникают у потребителей рынка.

Несовместимость технологий и оборудования для всех участников этого рынка, кроме трёх лидеров, создаёт дополнительные проблемы:

- необходимость дополнительных значительных затрат на выбор и использование проприетарных платформ, протоколов и согласующих шлюзов;
- поддержка складских запасов нескольких наименований изделий одного назначения, но от разных производителей для каждой из несовместимых платформ;
- возможное сокращение срока службы комплекта оборудования, обусловленное изменением базовых протоколов владельцами лицензий.

Наиболее ожесточённая конкурентная схватка наблюдалась между группировками, сложившимися вокруг Thread/Weave–Google/Nest, против их соперников, объединившихся под флагом Amazon+Apple. В проектах Amazon устройства Echo и Eero со встроенными концентраторами умного дома используются интеллектуальные устройства на базе ZigBee [18]. В экосистеме Google nest используются устройства, которые связываются между собой с помощью Thread, Weave и Bluetooth LE [19]. Широко распространённая экосистема HomeKit Apple's smart home platform базируется на технологиях Wi-Fi и Bluetooth LE [20].

Остальные поставщики технологий и комплектующих для «Умного дома» заметно отстают от лидеров по объёмам продаж. Они пытаются либо разрабатывать собственные протоколы, либо предлагают роутеры для связи с платформами Google, Amazon и Apple.

Thread и ZigBee (3.0/pro) используют один и тот же стандарт IEEE 802.15.4 на физическом (PHY) канальном подуровне (MAC) (см. рис. 4). Это значит, что можно, вообще говоря, использовать одинаковые устройства в конкурирующих технологиях. Понимая это и видя бесперспективность дальнейшей конкурентной борьбы, соперники решили объединиться и продолжить совместные разработки на благо потребителей всего мира. Таким образом, в декабре 2019 года Amazon, Apple, Google под руководством Zigbee Alliance создали рабочую группу, названную Project Connected Home over IP (CHIP – умный дом с подключением по протоколу IP). Основная цель этой рабочей группы заключается в разработке и продвижении единого стандарта протоколов беспроводной связи с открытым кодом, предназначенных для оборудования, используемого в проектах «Умного дома» [21].

В 2020 году к проекту CHIP присоединились: IKEA, Legrand, NXP Semiconductors, Resideo, Samsung SmartThings, Schneider Electric, Signify (ранее Philips Lighting), Silicon Labs, Somfy и Wulian. Предполагается, что основное руководство проектом будет осуществлять Zigbee Alliance.

В качестве двух основных задач проекта CHIP можно выделить, во-первых, унификацию блоков «Умного дома» различных производителей, а во-вторых, снижение затрат на разработку и монтаж оборудования.

Литература

1. https://memoori.com/evolution-building-management-system-data-connectivity/.
2. https://www.researchgate.net/publication/336325413_IoT_for_smart_homes/link/5e3e00b892851c7f7f25f96e/download.
3. https://www.aarp.org/caregiving/home-care/info-2017/best-buy-tech-gadgets-caregiving-fd.html.
4. https://www.iot-now.com/2021/03/09/108212-case-study-sophisticated-iot-platform-for-billions-of-connected-fridges/.
5. https://harborresearch.com/.
6. https://www.mordorintelligence.com/industry-reports/global-smart-homes-market-industry.
7. https://www.mdpi.com/1424-8220/16/7/1036/htm.
8. https://www.dreamstime.com/photos-images/smart-home.html.
9. https://www.paritet94.ru/gadzhety/umnyj-dom/komplekt-umnyj-dom-xiaomi-smart-home-security-kit-global-ver.
10. https://www.mdpi.com/2073-8994/9/8/143.
11. https://arxiv.org/abs/2012.02974.
12. https://www.researchgate.net/figure/Attack-surface-of-Cyber-Physical-System-CPS-24_fig1_332826219.
13. https://habr.com/ru/company/yota/blog/333850/.
14. https://researchers.mq.edu.au/en/publications/blockchain-for-iot-security-and-privacy-the-case-study-of-a-smart.
15. https://arxiv.org/pdf/1705.06805.pdf.
16. https://link.springer.com/chapter/10.1007/978-981-10-0281-6_70.
17. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/industries/home-automation.
18. https://www.amazon.com/b/ref=ods_aucc_dp_bp_wwytk2?node=17238426011.
19. https://support.google.com/googlenest/answer/7071794?hl=en&ref_topic=7195641.
20. https://developer.apple.com/support/homekit-accessory-protocol.
21. https://www.connectedhomeip.com/.

НОВОСТИ МИРА

Электроника 6G из дерева

Из наноцеллюлозы уже сделаны радиолинзы, которые фокусируют сигналы радиопередатчика.

В настоящее время исследователи разрабатывают радиоустройство 6G для демонстрации передачи данных с максимально возможной скоростью. В 6G частота сигнала составляет порядка 300 ГГц, а длина волны такова, что размер антенны не должен превышать 1мм.

Фокусировка сигнала на антенне приёмника является решающим моментом. Для этого необходимы радиообъективы. Наноцеллюлоза как материал для их изготовления имеет много преимуществ: это лёгкий, механически прочный материал с низкой структурой потерь электроэнергии, и она легко доступна. Лёгкость и низкие потери крайне важны. Потери сигнала в материале должны быть минимальными. Лучший из материалов может состоять на 99% из воздуха, и тогда доля потерь будет бесконечно мала. Из целлюлозы уже напечатан материал, похожий на воздух, а это означает, что он чрезвычайно лёгкий. Она хорошо подходит для 3D-печати и обеспечивает необходимую опорную структуру,

образующуюся из нанотрубок, что означает, что в них содержится много воздуха. Водорастворимый и хрупкий электронный компонент, мягко говоря, выглядит странно, но исследователи планируют разработать для линз защитную плёнку.

www.techxplore.com