Туманный Интернет вещей

Алексей Галицын (Москва)

В статье рассмотрены альтернативные (отличные от предлагаемых правительством и программой «Цифровая экономика») подходы к решению проблемы возрождения полупроводниковой индустрии страны и создания индустрии Интернета вещей, основанные на новой парадигме в архитектуре и обеспечении безопасности беспроводного Интернета вещей, ориентированных на конвергенцию Интернета вещей и концепции туманных вычислений.

Статья публикуется в авторской редакции. Мнение редакции не всегда совпадает с позицией автора. Но редакция открыта для диалога и предоставляет специалистам возможность донести свои идеи до аудитории журнала. Специализированный журнал – это информационная площадка, на которой порой встречаются самые невероятные проявления творческой мысли.

Введение

По данным всемирного исследования PwC Digital IQ® за 2017 год, Интернет вещей (IoT) занимает первое место среди восьми прорывных технологий, способных изменить бизнес-модели компаний или целых индустрий, опережая в этом рейтинге искусственный интеллект, дополненную реальность, технологию, связанную с созданием дронов и управлением ими, блокчейн и целый ряд других технологий [1].

В отличие от рынков большинства других технологий, рынок Интернета вещей практически безграничен, и, по прогнозам компаний Cisco и IBM, объём мирового IoT-рынка уже к 2020 году должен превысить $7 трлн (это практически четверть бюджета США или Китая). Однако эти амбициозные ожидания в настоящее время сдерживаются «из-за отсутствия стандартизации протоколов, отсутствия совместимости и однозначной идентификации IoT-устройств, отсутствия единых стандартов в сфере кибербезопасности Интернета вещей, а также в связи с уязвимостью IoT-устройств к внешним проникновениям и внешним воздействиям, которые могут привести к существенному репутационному и финансовому ущербу для компаний. Ещё одной, вполне очевидной проблемой является дороговизна существующих решений, ведь IoT – это не только сенсоры, но и сложная инфраструктура. Наконец, существенным сдерживающим фактором являются возможности канала передачи информации – в данном случае ограничения по дистанции использования датчиков, объёму передаваемой информации и помехозащищённости» [2].

Проблемы вертикальной интеграции IoT

Интернет вещей – это необъятное число подключённых датчиков, камер, смартфонов, компьютеров и устройств, которые взаимодействуют с другими устройствами, веб-сайтами, серверами и облаками [3]. Большинство приложений Интернета вещей, взаимодействующих с реальным миром, чувствительны к задержкам и требуют быстрой реакции. Для такого рода приложений, работающих в реальном времени, нужна новая распределённая модель вычислений, а также новая архитектура, в которой функционал облачных вычислений, сетевого взаимодействия и хранения критической информации должен быть опущен с «облаков на землю», т.е. на периферию бурно расширяющейся сети. При этом благодаря близости процесса вычислений нового туманного сегмента облака к вещам, производимые в «тумане» операции могут выполняться в реальном масштабе времени, без каких-либо задержек, потерь связи и т.п. Таким образом, для дальнейшего развития Интернета вещей необходимо создание и внедрение новой концепции – концепции туманных вычислений и новой парадигмы в архитектуре [4] расширяющейся сети Интернет.

Концепция туманных вычислений

Туманные вычисления (от англ. fog computing) – это подход к построению приложений, в которых обработка данных и серверные компоненты для обслуживания время чувствительных транзакций размещаются не в облаке, а ближе к периферии – на конечных устройствах (или рядом с ними): компьютерах, мобильных устройствах, датчиках, смарт-узлах и т.п., не теряя при этом связи с облачной инфраструктурой, решая основные проблемы и устраняя недостатки традиционной облачной модели (возможные задержки, необходимость в высокоскоростном «трансконтинентальном» соединении, непредвиденные сетевые заторы, сбои, потери связи, которые становятся критичными при расширении Интернета до уровня Интернета вещей). Таким образом, в туманных вычислениях дополнительная обработка данных и сервис должны быть размещены на конечных устройствах (end points), точках доступа или выделенных периферийных серверах. Классические облачные технологии очень хороши, но имеют один явный минус: облачная технология упирается в пропускную способность канала связи, которая небезгранична – уже сейчас каналы перегружены. И чем больше пользователей, тем сильнее эта перегрузка. Архитектура туманных вычислений снижает загруженность каналов связи путём подгрузки итоговых данных (вместо обеспечения постоянного соединения) от облаков, что требует новой (другой) организации прикладных процессов.

Туманные вычисления – следующий шаг в эволюции облаков, который открывает новые возможности для бизнеса за счёт поддержки локальной высокоскоростной обработки данных на узлах периферии сети, т.е. непосредственно на IoT-сенсорах и исполнительных механизмах, которые могут оперировать вместе со связанными облачными сервисами, чтобы обеспечить функции хранения, вычисления, сетевого взаимодействия и управления в зависимости от рабочей нагрузки. Это потребует другой организации приложений (которые должны будут уметь работать как в облачном, так и в частично автономном режиме) и новой архитектуры самой сети – распределённой горизонтальной архитектуры системно-

го уровня, которая будет распределять ресурсы и службы (такие как вычисления, хранение данных, управление и организация сети) между облачной вычислительной средой и конечными устройствами/узлами. В основе нижнего уровня этой архитектуры лежит концепция «капли». Что и роднит его с физическим воплощением тумана. «Капля» – это чип микроконтроллера со встроенной памятью и беспроводным интерфейсом передачи данных для соединения с такими же «каплями» тумана в локальном радиопространстве, имеющий интерфейсы для связи с глобальной транспортной инфраструктурой сети Интернет. Непосредственно к «капле» могут подключаться всевозможные датчики температуры, света, напряжения, излучения, положения в пространстве и т.п. Таким образом, «капля» может использоваться и для подключения датчиков, и для связи с другими «каплями», и для связи с транспортной инфраструктурой сети Интернет. Такая «капля» является своеобразной базовой технологией для туманных вычислений. С помощью таких микрочипов, допускающих возможность подключения к Интернету, можно создать действительно распределённую сеть устройств и развернуть её на всю планету [4].

Разновидности туманных вычислений

По существу, fog computing – это локальное облако более низкого уровня, как туман в низине. Туманные вычисления решают проблему задержки в облачных технологиях. Но остаётся и ещё один не менее важный, но нерешённый практический вопрос, связанный с потерями соединения и невозможностью гарантированного постоянного подключения к Интернету. Решение этой проблемы привело к созданию такой разновидности туманных вычислений, как росистые вычисления («роса» – буквальный перевод англ. dew), смысл которых состоит в том, что на локальном (конечном) устройстве сохраняется легковесная локальная копия процесса, что обеспечивает работу пользователя (устройства) даже в автономном режиме [5]. Как только становится доступным интернет-соединение, конечное устройство синхронизируется с облаком. Росистые вычисления работают на самом нижнем уровне архитектуры (на периферии) Сети, для которого характерно наличие связи непосредственно между конечными устройствами (end points) через различные каналы беспроводной связи: Wi-Fi, Bluetooth, ZigBee и ряд других [6]. Иногда это явление называется edge computing. Оно будет играть ключевую роль в будущих виртуализированных сетях и должно дать новый импульс их распространению. Применительно к мобильным сетям 5G эта концепция носит название Mobile edge computing (MEC). Появление и развитие MEC в международном масштабе потребует в последующие годы астрономических инвестиций в новое оборудование и разработку нового класса приложений [7].

Поддержка туманных вычислений государством и корпорациями

Администрация президента РФ поручила Минкомсвязи, Минпромторгу, Ростелекому и Агентству стратегических инициатив (АСИ) заняться подготовкой инфраструктуры для туманных вычислений. Об этом сообщил «Коммерсант» со ссылкой на собственные источники в правительстве [8].

В ноябре 2015 года Cisco, Microsoft, Dell, ARM, Intel и Princton University основали OpenFog Consortsium [9], поддерживающий создание открытой архитектуры для туманных вычислений. OpenFog Consortium опубликовал описание эталонной архитектуры OpenFog – универсальной технологической модели для проектов Интернета вещей (IoT) на основе мобильной связи 5G. В основу OpenFog легло применение туманных вычислений – специальной системы обработки и хранения данных, управления работой устройств и обслуживания сетевых коммуникаций, которая предусматривает расположение данных непосредственно вблизи источника их генерации и последующего использования с возможностью обслуживания через облачную инфраструктуру.

Google представил платформу для Интернета вещей – Android Things [10] с поддержкой микрокомпьютеров Intel Edison, Joule 570x, NXP Pico i.MX6UL, Argon i.MX6UL и Raspberry Pi 3. Fog-приложения разрабатываются на платформе Android Studio для любого из этих устройств. Android Things также обеспечивает интеграцию с Google Play и всей экосистемой Android, на которой сейчас работают 90% смартфонов в мире. Таким образом, система Android Things даёт возможность любому Android-смартфону или планшету работать в качестве fog-узла, который, в свою очередь, должен стать новой точкой доступа в Интернет для более простых устройств мира вещей.

Пользователям необходимы данные и приложения в любом месте и в любое время, в этом вся суть облачной модели предоставления услуг. Это означает, что будущее облаков лежит даже не в узкой области Интернета вещей (IoT), а в более широкой области – всеобъемлющего Интернета (Internet of Everything – IoE), который сохраняет преемственность с более ранними стадиями развития Глобальной сети. Обе эти модели (IoT+IoE) предполагают взаимодействие распределённых процессов с мобильными объектами взрывоопасного реального мира, причём взаимодействие через беспроводную среду, которая априори является ненадёжной (подвержена помехам) и легкодоступной (для взлома не требуется даже физического подключения к оборудованию сети). В связи с этим возникает и новая острейшая проблема, требующая решения, – проблема обеспечения безопасности всей системы (IoT + IoE + туманные вычисления) в целом [11].

Проблема обеспечения безопасности IoT+IIoT+IoE

Чем отличается безопасность классического Интернета от безопасности беспроводного Интернета будущего, расширенного до уровня вещей? Классический Интернет создавался на основе «первобытных» компьютеров, при проектировании которых разработчики даже подумать не могли о том, что надо обеспечивать их безопасность, и уж тем более аппаратными средствами. Поэтому безопасность классического Интернета обеспечивается программно – асимметричными алгоритмами криптокодирования, а защита открытых ключей от подмены обеспечивается довольно сложным (в плане практической реализации) механизмом доверенных серверов и цифровых сертификатов.

Последствия печальны, не говоря уж о нанесённом экономическом ущербе: борьба с уязвимостями программного обеспечения, вирусами и киберпреступностью превратилась в настоящую,

причём самодостаточную индустрию (которой при ином изначальном подходе могло и не быть).

Как известно, основным поставщиком угроз безопасности является периферия Сети, поэтому безопасность беспроводного соединения (а Интернет вещей будущего априори будет беспроводным), необходимого для подключения вещей к Интернету при его расширении, это наиважнейшая и в то же время сложнейшая проблема, острота и сложность которой во многом и отличает классический проводной Интернет от беспроводного Интернета, расширенного до уровня вещей. Обусловлено это тем, что криптокодирование по определению должно осуществляться в реальном источнике и реальном приёмнике информации, а если источниками или приёмниками информации становятся мобильные вещи, то и всю «тяжёлую» криптографию придётся переносить в вещи и как-то обеспечивать им доступ к доверенным серверам и цифровым сертификатам. Для подавляющего большинства простых вещей это физически нереально: ведь Интернет вещей будущего – это уже не только (и не столько) многократное увеличение количества подключённых устройств (или даже целых систем) с IP-адресами на душу населения, сколько возможность беспроводного взаимодействия с ними самими тысячекратно большего количества более простых предметов, не обладающих IP-адресами, которые тоже требуют защиты.

В связи с вышеизложенным механизмы безопасности классической сети Интернет «за браузером» работать не будут. Именно поэтому сейчас в локальной беспроводной среде используют «лёгкую» автономную криптографию, а системные транзакции в этой среде вообще ничем не защищены, что существенно снижает безопасность сети Интернет в целом, а по мере развития Интернета вещей неизбежно приведёт к катастрофе. Тем не менее даже эта «лёгкая» криптография не так уж и дешева, поскольку потребляет значительные вычислительные ресурсы. В подтверждение этому ниже перечислим некоторые протоколы передачи данных и протоколы безопасности, которые используют существующие наиболее массовые беспроводные технологии (Wi-Fi, Bluetooth, ZigBee).

Транспортные протоколы: уровень PHY&MAC Layer (WLAN: 802.11, WPAN: 802.15, PLC: PRIME, Automation: CIP); уровень Adaptation Layer (WLAN/WPAN: 6LowPAN, PLC: PRIME IPv6 SSCS, Automation: Ethernet/IP); уровень Transport/Network Layers (UDP over IPv6, TCP over IPv6, IPv6 Stack); уровень Application Layer (CoAP, MQTT, AMQP, RTPS); уровень Routing (RPL, PCEP, LISP(Cisco)).

Протоколы безопасности: 802.1AR – Secure Device Identity, 802.1AE – Media Access, Control (MAC) Security, 802.1X – Port-Based (Authenticated) Media Access Control, IPsec AH & ESP, Tunnel/Transport Modes, (D)TLS – (Datagram) Transport Layer Security.

Для элементарного использования этих протоколов недостаточно быть просто программистом-разработчиком прикладных систем, а нужно быть ещё и профессионалом в области компьютерной безопасности в части безопасности беспроводных систем и уметь использовать всю эту «криптотехнику» (причём на всех уровнях транспортной инфраструктуры) для организации каждого конкретного соединения. То есть, будучи весьма и весьма затратным, процесс создания безопасного Интернета вещей с использованием этих технологий является недоступным для массового разработчика. Если создавать Интернет вещей на основе уже существующих стандартов, то «в пылу борьбы» за выход на триллионный IoT-рынок первыми, при обилии платформ, сложности архитектуры и полном отсутствии экспертизы безопасности создаваемых продуктов, этот многотриллионный рынок будет полностью дискредитирован, ещё не «родившись».

Таким образом, при использовании существующего беспроводного оборудования в условиях аппаратного дефицита на периферии (в вещах) и увеличении количества вещей до сотен миллиардов, угрозы безопасности станут неприемлемыми. США и Англия уже ввели законы, предписывающие производителя обеспечивать безопасность устройств Интернета вещей, правда, не указали, как это сделать?

По мнению автора статьи, выход из создавшейся ситуации может быть только один: безопасность должна предоставляться массовому разработчику прикладных систем Интернета вещей не в виде непонятных ему стеков протоколов, а в виде той самой «капли» – готового беспроводного чипа (IP-блока – для систем на кристалле), гарантирующего и автоматически обеспечивающего безопасность любого и каждого беспроводного соединения на периферии сети («за браузером») [4].

Так как создавать российский, да и мировой Интернет вещей?

Использовать и копировать десятки чипов беспроводной связи или сенсорных сетей (созданных за рубежом в прошлом веке для совершенно других целей – покрытия сотен квадратных километров – и оказавшихся не у дел после создания и развёртывания сетей LTE и выхода сотовой телефонии на уровень 5G) и снова бороться за безопасность программными методами?

Или создать один универсальный чип (IP-блок), обеспечивающий безопасность беспроводного соединения аппаратно, причём чип не для «покрытия площадей» (это обеспечат LTE и 5G), а для создания самого крупного и самого массового сегмента рынка Интернета вещей (для создания безопасного локального мира умных вещей, непосредственно окружающих человека), позволяющего обеспечить взаимодействие человека с этим новым миром умных вещей через новый интерфейс (через смартфон) и безопасное подключение этого нового локального мира умных вещей к глобальной транспортной инфраструктуре?

Ответ прост: конечно же, при создании беспроводного Интернета вещей будущего не надо совершать тех же ошибок, что и при создании компьютеров. Безопасность и все остальные качества, необходимые системам беспроводного Интернета вещей, должны поставляться не в виде ресурсоёмких стеков программных протоколов, а как готовый безопасный аппаратный IP-блок (IoT-радиопроцессор), т.е. телекоммуникационный процессор (со-процессор), простой и понятный массовому разработчику, гарантирующий криптографическую уникальность и безопасность каждого беспроводного соединения.

Что, собственно, автор статьи и предлагает сделать, выпустив чип (IP-блок) универсального IoT-радиопроцесора с криптокодированием структуры радиосигнала для создания умных вещей (причём IP-блок будет интегрируем в системы на кристалле, создаваемые для новых вещей,

точек доступа, PC, планшетов, смартфонов и т.п.).

Тем самым в беспроводном соединении предлагается перенести процедуру криптокодирования с информации на структуру радиосигнала, что обеспечит её принципиальную недоступность для кибератак [12]. При этом в существующей сети Интернет не придётся ничего ломать: посредством стандартной техники Интернета (VPN-соединения, SSL-протоколы) будет обеспечено безопасное взаимодействие прикладных процессов новой точки доступа (I-Phone, I-PAD, PC и т.д.) с Интернетом (web-серверами, сайтами и облаками), а посредством нового информационно-прозрачного, но криптографически защищённого по структуре радиосигнала беспроводного соединения будет обеспечено безопасное взаимодействие этих прикладных процессов, собственно, с вещами (т.е. обеспечение следующего уровня расширения Сети). Соответственно, и прикладные процессы в рамках концепции fog computing должны будут строиться с учётом новой архитектуры нижнего уровня Сети и этих новых возможностей по обеспечению безопасности.

Такой подход позволит сохранить все существующие механизмы безопасности классической сети Интернет (т.е. всю её инфраструктуру), что называется «до браузера», т.е. сохранить все механизмы, обеспечивающие безопасное взаимодействие прикладных процессов, происходящих в компьютерах и смартфонах (fog-узлах) с сайтами, серверами и облаками, одновременно обеспечив простоту, прозрачность, а главное – высочайший уровень безопасности информационного взаимодействия этих процессов с вещами, а вещам – безопасное взаимодействие напрямую между собой.

Базовая радиочастотная технология

Для осуществления криптокодирования структуры радиосигнала может быть использована базирующаяся на псевдослучайных кодовых крипто последовательностях C-UWB RF-технология, использующая RF-спектр на вторичной основе, которая строится на корреляционной обработке сложного широкополосного радиосигнала и принципе кодового разделения каналов [6].

В свою очередь, корреляционная обработка радиосигнала позволяет (на основе принципа кодового разделения каналов) процесс адресации устройств тоже перенести с логического (адресация на основе информации, полученной после демодуляции радиосигнала) на физический уровень обработки самого радиосигнала (до его демодуляции) и обеспечить прямую, т.е. непосредственную адресацию устройств друг другом (с последующей передачей информации), фактически исключив из состава систем средства и устройства, выполнявшие эти функции в традиционных радиосистемах (контроллеры-координаторы, сетевые операционные системы и т.п.) [4].

Используя радиочастотный спектр на вторичной основе, C-UWB RF-технология на физическом уровне обработки радиосигнала (благодаря корреляционной обработке радиочастотного сигнала и кодовому разделению каналов) автоматически решает проблему коллизий, позволяя обеспечить взаимодействие смарт-коммуникаторов с вещами, а «домашних» вещей – напрямую между собой, без участия привязанных к инфраструктуре посредников – контроллеров-координаторов и сетевых ОС, и уж тем более не через облака и сайты в Америке, что удобно, надёжно, эргономично и безопасно.

Помехозащищённость

Кроме того, при расширении Интернета чрезвычайно актуальной с точки зрения безопасности становится проблема помехозащищённости локальных соединений этого нового «дважды беспроводного» Интернета вещей, где компьютеры и смартфоны становятся новыми беспроводными точками доступа в Интернет для более простых и тоже беспроводных устройств.

Ведь если на верхнем уровне беспроводной транспортной инфраструктуры (т.е. на уровне LTE) эта проблема как-то купируется лицензированием диапазона частот, контролем за эфиром, высокими мощностями радиосигнала и методами помехоустойчивого кодирования, то самый нижний уровень новой, едва существующей сегодня локальной транспортной инфраструктуры Интернета вещей работает в нелицензируемых диапазонах частот, а в плане помехозащищённости практически беззащитен, ведь помехозащищённость у существующих RF-стандартов (технологий) просто равна нулю.

Впрочем, для нашей российской C-UWB RF-технологии удалось предложить простые и эффективные методы подавления помех [13] и повысить помехозащищённость радиосистем ещё на два порядка по сравнению с самой «стойкой» технологией ZigBee.

Всё вышеперечисленное в корне меняет архитектуру, эргономику, уровень безопасности и себестоимость новых радиосистем. Фактически этот подход позволяет создать локальную радиосреду, недоступную для кибератак, и перейти к новой парадигме в архитектуре IoT, т.е. избавиться от уровня традиционных локальных радиосетей (принципиально необходимого во всех существующих RF-стандартах прошлого века) и устранить тот «разрыв» в системе безопасности Интернета, который вносит беспроводное соединение на самом нижнем уровне Сети. При этом повсеместность покрытия (вместо дальности действия локальной сети) обеспечат LTE и 5G.

Всё это приводит к повышению безопасности и многократному снижению себестоимости систем Интернета вещей в целом, поскольку для них уже не требуются ни сетевые операционные системы, ни контроллеры-координаторы локального радиопространства, осуществляющие адресацию устройств, распределение и назначение каналов для связи, борьбу с коллизиями, маршрутизацию пакетов и т.п., вышеперечисленное также освобождает от всех проблем и от вычислительных ресурсов, поддерживающих сложнейшие протоколы безопасности, используемые в существующих радиочастотных стандартах для организации каждого (!) соединения.

Причём это системное решение, названное «IoT-радиопроцессором», не будет ломать существующие базовые принципы работы системы безопасности классической сети Интернет, а будет использовать все уже существующие вышестоящие уровни безопасности сети и практически автоматически вписываться в эталонную архитектуру OpenFog на её нижнем уровне. Это решение и будет той самой «каплей», которая позволит создать действительно безопасную распределённую сеть устройств Интернета вещей и развернуть (масштабировать) эту сеть на всю планету.

Безальтернативность предлагаемого решения

Имплантировать в смартфон будущего (в смарт-коммуникатор) чипы или контроллеры-координаторы существующих RF-стандартов бесперспективно просто потому, что тогда непонятно, кто именно в конечном итоге будет контролировать нелицензируемый локальный эфир:

- смартфон? Но который из десяти в каждой квартире, в квартирах соседей и по какому стандарту – для каждой из функционально разных прикладных систем?
- может быть, некий стационарный контроллер-координатор? Но который из них – Bluetooth, ZigBee, Wi-Fi, LoRa, SigFox и т.д. – причём ваш или соседский?

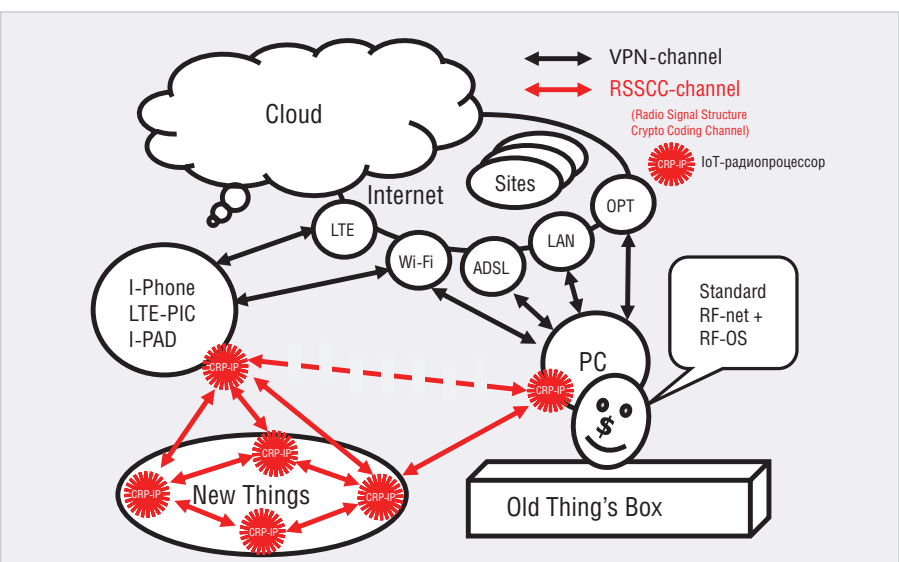
Этот вопрос в нелицензируемом радиопространстве для традиционных радиочастотных технологий всегда будет открытым, а проблемы коллизий, электромагнитной совместимости и безопасности будут только обостряться по мере «урбанизации» локального радиопространства, обусловленной развитием самого же Интернета вещей. В условиях конкурентной борьбы стандартов (со ставкой $10 трлн в год) эта проблема для нелицензируемого локального радиопространства всегда будет неразрешимой.

Открытость системных транзакций и полное отсутствие помехозащищённости (при высокой стоимости и сложности старой архитектуры и средств криптографии, которые им придётся «переносить» в вещи!) делает существующие RF-стандарты (при наличии авторского решения) совершенно бесперспективными для создания Интернета вещей будущего.

Суть инновации

Таким образом, наша инновация заключается в создании универсального информационно-безопасного элемента – IoT-радиопроцессора (IP-блок, SoC, Chip-set, +Soft) с криптокодированием структуры радиосигнала, инструмента создания локального (физического пространства в радиусе 100–200 м) радиопространства глобальной информационной среды будущего, базового элемента построения виртуального «мира умных вещей», позволяющего разместить «мир вещей» в локальном радиочастотном пространстве на вторичной основе без конфликтов с существующими радиочастотными стандартами и технологиями, обеспечив при этом непосредственную радиочастотную адресацию устройств друг другом, непревзойдённую информационную безопасность, высочайшую помехозащищённость и минимальную себестоимость подключения вещей к Интернету.

Универсальность IoT-радиопроцессора (при криптографической уникальности каждого формируемого беспроводного соединения) как в плане программируемости его функционального назначения, так и в плане программирования архитектуры, топологии и даже физического уровня локальной радиосреды обеспечит IoT-радиопроцессору выпуск многомиллиардными тиражами и, соответственно, себестоимость, несопоставимую с себестоимостью микросхем традиционных радиочастотных стандартов.



Место IoT-радиопроцессора в архитектуре систем

Предлагаемый чип изначально предназначен для создания горизонтальных туманных архитектур, имеющих доступ к облакам, в которых распределённые прикладные процессы будут гарантированно автономно работать каждый в своей локальной радиосреде («на своей земле», «на своём заводе», «в своей квартире»), имея возможность доступа и к облачным сервисам через новые стационарные (типа подключённых к Интернету PC) или мобильные (типа смартфонов) точки доступа, в которые, так же как и в вещи, будет имплантирован чип (или IP-блок – в системы на кристалле). На основе этого чипа (IP-блока) будет возможно построение как, собственно, безопасного мира умных вещей, подключённого к глобальному Интернету, так и непосредственное информационно-прозрачное (но в то же время безопасное) взаимодействие с ним человека посредством нового интерфейса – смартфона (в будущем смарт-коммуникатора), причём без «посредников» в виде традиционных, располагаемых на местности контроллеров-координаторов беспроводной локальной радиосети.

Простота и прозрачность построения безопасного локального «мира вещей» и его подключения к Интернету (т.е. доступность этого процесса для массового разработчика), эргономичность архитектуры систем, простота обеспечения безопасности уникальная помехозащищённость, при многократном снижении себестоимости радиосистем – всё это делает наш подход и технологию безальтернативными для создания Интернета вещей (IoT), индустриального Интернета (IIoT) и всеобъемлющего Интернета (IoE) будущего. Предлагаемый автором статьи IoT-радиопроцессор может сыграть такую же ключевую роль в создании мировой индустрии Интернета вещей, какую супергетеродин сыграл в создании радио, а микропроцессор – в создании компьютерной индустрии.

России производство этого чипа позволило бы (!) не только сохранить вымирающую полупроводниковую индустрию, но и кардинально решить проблему импортозамещения и безопасности в этом самом крупном и самом массовом сегменте электроники, т.к. на сегодня только импортозамещение может уберечь от «закладок» в

компьютерные технологии. При этом приборостроительным предприятиям и полупроводниковым фабрикам страны (за счёт наших интеллектуальных, а не их технологических преимуществ) был бы (!) открыт новый безграничный мировой рынок всеобъемлющего Интернета (IoT+IIoT+IoE) – самый быстрорастущий, самый крупный и самый массовый рынок электроники ближайшего и даже отдалённого будущего.

Выводы

К сожалению, данная разработка десятилетиями не интересовала ни полупроводниковые фабрики страны (прекрасно существовавшие за счёт дотаций от государства), ни само государство (в лице Минпромторга). У фабрик просто не было денег не только на развитие, но даже на поддержание собственной инфраструктуры, а уж тем более на дорогостоящие перспективные разработки. Минпромторг был занят более важными делами: реорганизацией предприятий отрасли, консолидацией активов предприятий отрасли (образование СП «Элемент»), реорганизацией (перестановкой кресел) Департамента радиоэлектронной промышленности и разработкой «Научных парадигм цивилизации» [14].

Вместе с тем полупроводниковая индустрия постоянно находится в поле зрения высшего руководства (правительства) нашей страны, констатирующего, что:

«Одно из ключевых предприятий отрасли – АО «Ангстрем-Т» в Зеленограде. Ранее были сделаны инвестиции в этот проект. Необходимо найти решение, которое позволит предприятию развиваться, сохранять высококвалифицированные рабочие места, осваивать новые технологии, которых в нашей стране просто нет» (Д. Медведев, из стенограммы заседания Наблюдательного совета ВЭБ РФ от 4 февраля 2019 года).

«Год начинаем с двух очень важных сделок. Первая сделка – это «Ангстрем-Т». Выполнено поручение президента: «ВЭБ.РФ» стал собственником предприятия. Мы сегодня на наблюдательном совете рассмотрели ответственность перед коллективом и поддержку деятельности предприятия в течение 2019 года. Определён бюджет для этих целей и план мероприятий. Вместе с тем были даны поручения уже по правительственной линии – готовить инвестиционную программу для развития «Ангстрем-Т». Этот вопрос будет рассмотрен на совещаниях в правительстве, и когда будет высокая готовность проекта, председатель правительства в том числе рассмотрит этот инвестиционный проект, который будет осуществлён чуть позже. Такой проект должен иметь бюджетное финансирование, ВЭБ здесь будет выполнять функцию агента правительства, помогая правительству осуществлять этот очень важный инвестиционный проект» (И. Шувалов, из заявления прессе после заседания наблюдательного совета ВЭБ.РФ 04.02.19).

Очень важно, что курирующий радиоэлектронную отрасль вице-премьер Ю. И. Борисов (непосредственно руководивший этой отраслью в течение 20 лет) выполнил поручение премьер-министра и 10 декабря 2019 года предложил-таки решение [15]: «Ещё одним направлением для госинвестиций должно стать развитие зеленоградского производителя чипов «Ангстрем-Т». В прошлом году он был объявлен банкротом, но теперь планируется восстановление производственных мощностей. Из бюджета уже выделено $300 млн (20 млрд рублей), а на расширение на 2020 год заложен ещё $1 млрд (около 67 млрд рублей). Рынок подсказал решение: для индустрии Интернета вещей стали снова востребованы технологии 250–90 нм, ей не требуются субмикронные технологии. На Западе даже стали восстанавливать устаревшие мощности – парадокс!»

Заключение

Приятно чувствовать заботу правительства о полупроводниковой индустрии страны. Приятно осознавать, что «невидимая рука рынка» подсказала наконец стране решение и выход из создавшейся в полупроводниковой индустрии страны ситуации. Однако не совсем понятно, почему профильный вице-премьер и в рамках программы «Цифровой экономики» решил, что все «умные» вещи в домах и квартирах жителей России, а также все станки в цехах российской Индустрии 4.0. должны общаться между собой через базовые станции «на районе», а безопасность индустрии Интернета вещей должна обеспечиваться весьма экзотическим способом: «посредством подключения к сетям IoT системы средств оперативно-розыскных мероприятий (СОРМ) и внесения изменений в закон «О связи» [16]?»

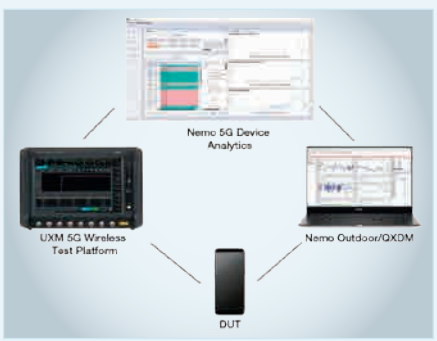
Литература

1. https://constanta.co/news/20180305-vsemirnoe-issledovanie-digital-iq-za-2017-god-pwc/.
2. https://iot.ru/promyshlennost/obzor-novostey-iot-pochemu-prognozy-po-kolichestvu-iot-ustroystv-stali-skromnee-i-kogda-v-rossii-bud.
3. *Зараменских Е. П.* Интернет вещей. Исследования и область применения. ИНФРА-М. 2016.
4. *Галицын А. А.* Интегральный радиопроцессор – перспективная техническая основа Интернета вещей. Датчики и Системы. 2015. №1.
5. https://shalaginov.com/2016/12/16/nfv-i-mec-v-chem-razlichiye/.
6. *Галицын А. А.* Технология C-UWB – основа для информационно-телекоммуникационных систем нового поколения. Электроника: наука, технология, бизнес. 2008. №5.
7. http://www.iksmedia.ru/articles/5491297-Edge-Computing-iz-oblakov-na-zemlyu.html.
8. https://www.kommersant.ru/doc/3026455.
9. https://en.wikipedia.org/wiki/OpenFog_Consortium.
10. https://en.wikipedia.org/wiki/Android_Things.
11. *Кринон Г.* Безопасность «Интернета Вещей»: существующие проблемы и их решение. Инноватор. 2017. №1.
12. *Галицын О. И.* Патент на изобретение № 2557451 RU «Способ динамической адресации корреспондентов мобильной радиосети и устройство для его реализации». Приоритет от 08.06.2012.
13. *Bobkov M., Galitsyn A., Kalugin V.* US Patent № 7.250.541 B2. Method for suppressing narrowband noise in a wideband communication system. Priority date 22.08.2002.
14. *Шпак В. В.* Микроэлектроника как двигатель четвертой технологической революции. Тезисы доклада на конференции «Научная парадигма цивилизации в XXI веке: капитализм, социализм и четвёртая технологическая революция». Челябинский государственный университет. Челябинск. 2018.
15. https://profile.ru/economy/industry/velichie-rossijskoj-elektronnoj-promyshlennosti-pokazushhestvuet-tolko-v-nesbytochnyx-proektax-173986/.
16. https://www.kommersant.ru/doc/3924324.

НОВОСТИ МИРА

Keysight представляет новое интегрированное решение для ускорения проверки эффективности устройств 5G

Компания Keysight Technologies сообщила о релизе новых инструментов устранения неисправностей и тестирования, которые помогут производителям устройств 5G и мобильным операторам автоматизировать процессы испытаний и формирования отчётов для различных конфигураций и моделей.



Набор инструментов для тестирования устройств 5G от компании Keysight позволяет ускорить проверку эффективности 5G-оборудования перед выходом продукта на рынок. В состав набора входит платформы UXM 5G и Nemo Outdoor для испытания беспроводных устройств, а также программный пакет Nemo 5G Device Analytics. Вместе эти программы представляют собой интегрированные лабораторные решения для тестирования, устранения неисправностей и повышения качества сетевых сервисов. Набор тестирования входит в комплект решений Keysight для эмуляции 5G-сетей и позволяет автоматически формировать стандартизированные отчёты для количественной оценки эффективности испытуемого оборудования.

Компания Keysight применила основные технологии тестирования, измерения и анализа данных, чтобы создать новое законченное пользовательское решение, обеспечивающее корреляцию результатов испытаний устройств. Это позволяет ускорить анализ первопричин проблем и оценить эффективность при разнообразных сценариях использования.

Набор инструментов Keysight для тестирования 5G-оборудования обеспечивает следующие преимущества для пользователей:

1. оценка эффективности устройств при различных сценариях эксплуатации, смоделированных с учётом реальных условий;

2. поддержка сценариев тестирования по ключевым показателям эффективности (КПЭ): скорость передачи данных, успешное распределение ресурсов в сетях LTE и 5G, производительность сети на границе зоны покрытия;

3. простое сравнение испытуемого продукта с эталонными девайсами, конкурирующими моделями и устройствами, в которых используются разные конфигурации модемов и программного обеспечения.

В наборе инструментов Keysight для тестирования устройств 5G используется единая программная среда, формирующая данные на основе решений в области эмуляции сетей 5G для любых испытуемых продуктов. Это первое законченное пользовательское решение для полностью автоматического тестирования устройств любых производителей, предназначенное в том числе для испытания изделий, в которых работают модемы от разных производителей микросхем. В настоящее время продолжается расширение экосистемы, которая сегодня объединяет более 76 поставщиков устройств 5G, предлагающих 16 вариантов конструктивных решений для оборудования, совместимого с сетями 5G new radio (NR).

Пресс-релиз Keysight Technologies

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
ЭЛЕКОНД

КОНДЕНСАТОРЫ
разработка и производство

оксидно-электролитические алюминиевые конденсаторы
К50-15, К50-17, К50-27, К50-37, К50-68, К50-74, К50-76, К50-77, К50-80, К50-81, К50-83, К50-84, К50-85, К50-86, К50-87, К50-88, К50-89, К50-90, К50-91, К50-92, К50-93, К50-94, К50-95(чип), К50-96, К50-97(чип), К50-98

объемно-пористые танталовые конденсаторы
К52-1, К52-1М, К52-1БМ, К52-1Б, К52-9, К52-11, К52-17, К52-18, К52-19, К52-20, К52-21, К52-24, К52-26(чип), К52-27(чип), К52-28

оксидно-полупроводниковые танталовые конденсаторы
К53-1А, К53-7, К53-65(чип), К53-66, К53-68(чип), К53-71(чип), К53-72(чип), К53-74(чип), К53-77(чип), К53-78(чип)

ионисторы (суперконденсаторы)
К58-26, К58-27

накопители электрической энергии на основе модульной сборки суперконденсаторов

Россия, 427968, Удмуртская Республика,г. Сарапул, ул. Калинина, 3
Тел.: (34147) 2-99-53, 2-99-89, 2-99-77, факс: (34147) 4-32-48, 4-27-53
e-mail: elecond-market@elcudm.ru, http://www.elecond.ru

Реклама

ЭЛЕКТРО

МИНПРОМТОРГ РОССИИ

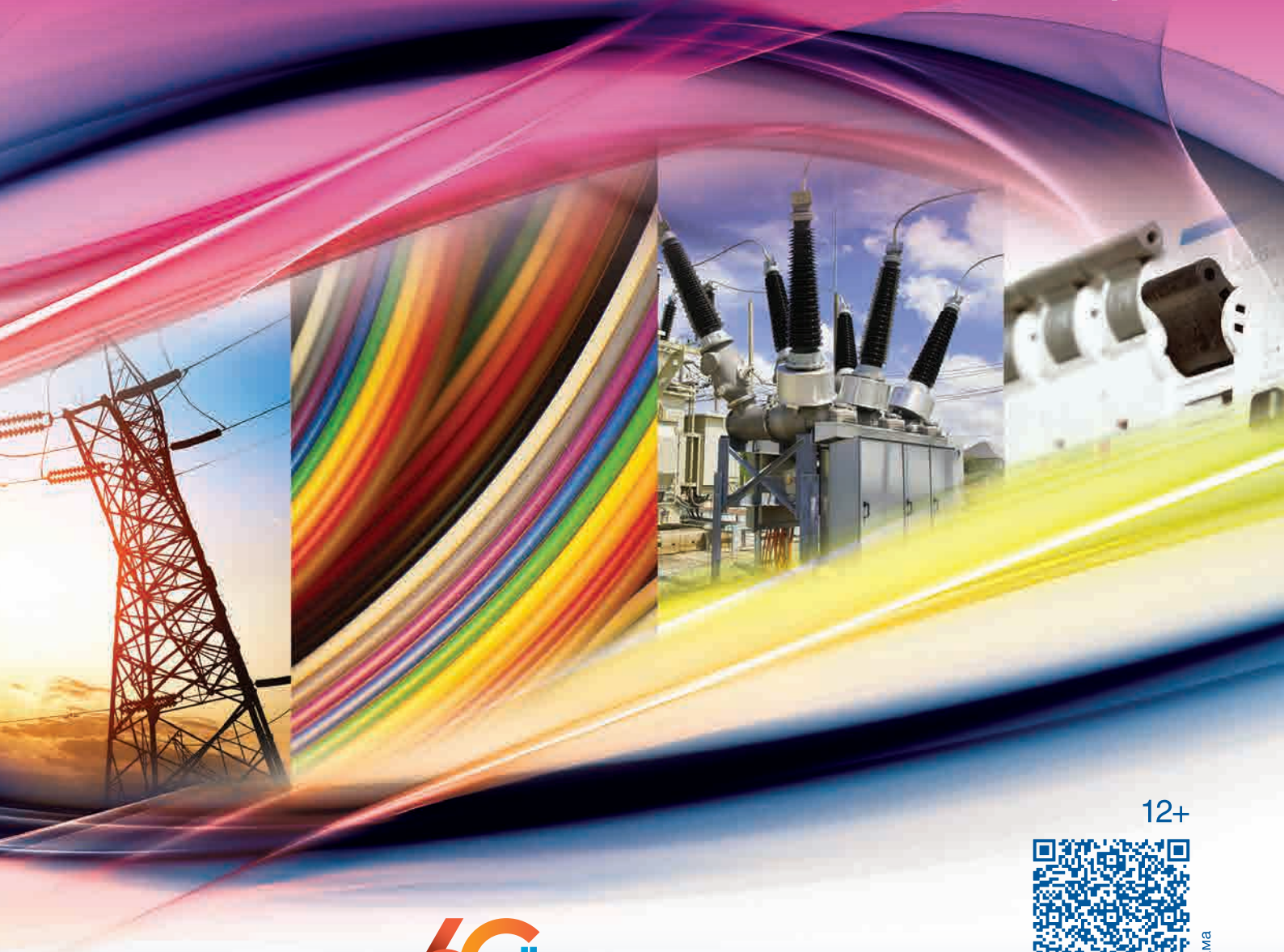
ТПП РФ

29-я международная выставка «Электрооборудование. Светотехника. Автоматизация зданий и сооружений»

8–11.06.2020

Россия, Москва | ЦВК «ЭКСПОЦЕНТР», Краснопресненская наб., 14 | Павильон №2 (залы 1, 2)

www.elektro-expo.ru



12+

ЭКСПОЦЕНТР

Реклама

ЭЛЕКТРО МАРКЕТ
ВАЖНЫЕ СВЯЗИ ДЛЯ ВАЖНЫХ ДЕЛ

ЭЛЕКТРО TALK
РАЗГОВОРЫ С ТОЛКОМ

ЭЛЕКТРО SKILLS
ПРОКАЧАЙ НАВЫКИ И КОМПЕТЕНЦИИ