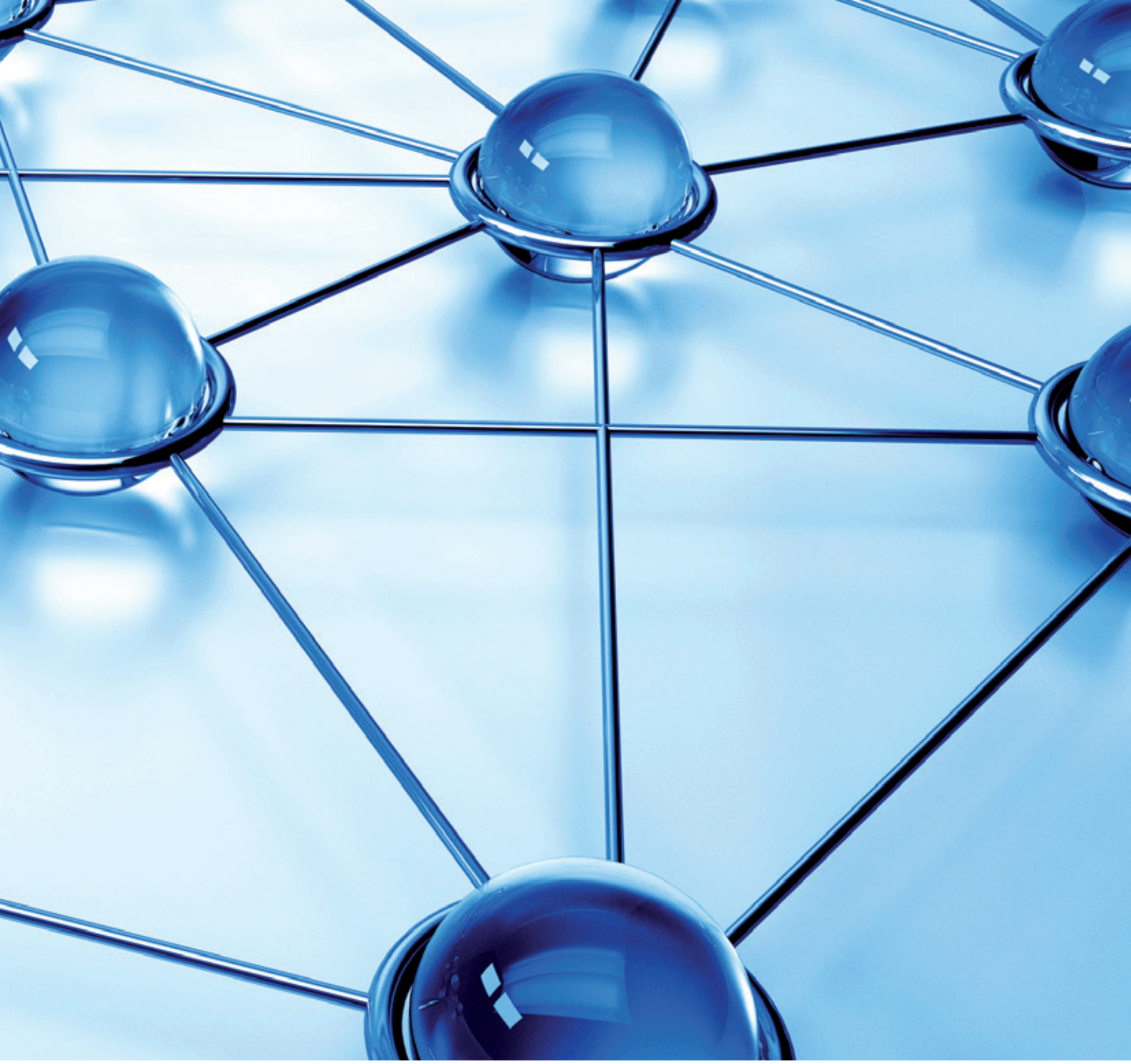


Белая книга

«Интернет вещей»: Беспроводные сенсорные сети

Краткое содержание

В настоящее время, умные электросети, умные дома, умные системы водоснабжения и умные транспортные системы представляют собой инфраструктуру, связывающую воедино наш мир намного теснее, чем когда-либо раньше. Эти системы, как правило, связаны единой концепцией – интернетом вещей (IoT), где при помощи датчиков вся физическая инфраструктура тесно связана с информационно-коммуникационными технологиями; а интеллектуальный контроль и управление осуществляется при помощи встроенных сетевых устройств. В такой сложной динамической системе устройства взаимосвязаны для передачи измеряемых данных и команд управления по сетям распределенных датчиков.

Беспроводная сенсорная сеть (WSN) представляет собой сеть, образованную большим количеством узлов датчиков, где каждый узел оснащен датчиком для обнаружения физических явлений, таких как свет, тепло, давление и т.д. Сети WSN - революционный метод сбора информации с целью создания информационно-коммуникационной системы, которая значительно улучшит надежность и эффективность инфраструктуры. В отличие от проводных решений установка WSN является более простой, при этом сама сеть отличается большей гибкостью устройств. Благодаря быстрому технологическому развитию датчиков WSN станет ключевой технологией IoT.

В настоящей Белой книге описано использование и эволюция WSN в более широком контексте IoT, а также представлен обзор возможностей использования WSN с учетом инфраструктурных технологий, приложений и стандартов, представленных в WSN-проектах. Это шестая по счету Белая книга, обобщающая опыт МЭК в рамках ее Международных стандартов и Услуг по оценке соответствия для решений проблем в глобальном масштабе в области электротехники.

В разделе 2 описана история появления IoT и WSN, а также приведены примеры из сферы электроэнергетики, в которой в настоящее время проходит модернизация электросетей. Технологии WSN играют важную роль в осуществлении контроля безопасности оборудования преобразования и передачи электроэнергии, а также установки миллиардов умных датчиков.

В разделе 3 представлена оценка технологической составляющей и характеристикам WSN, а также мировому спросу в данной области, в том числе аспектам группирования данных и безопасности.

В разделе 4 описаны проблемы и будущие тенденции WSN по широкому спектру их практического применения в различных отраслях, в том числе сверхбольшие измерительные устройства, обеспечение безопасности и конфиденциальности, а также сервисная архитектура.

В разделе 5 описаны возможности практического использования данных сетей. Возможности по практическому использованию WSN в современном мире являются воистину безграничными. С одной стороны, WSN заключают в себе множество новых практических возможностей и, следовательно, обуславливают появление новых рынков; с другой стороны, проекты в данной области имеют ряд ограничений, которые требуют новых парадигм. В данном разделе описаны возможности практического использования WSN в системах умных электросетей, умного водоснабжения, умных транспортных систем, а также умных домов.

В разделе 6 представлен анализ стандартизации, которая является главным предварительным условием для достижения операционной совместимости WSN между продуктами различных поставщиков, а также между различными решениями, возможностями практического применения и сферами.

В разделе 7 приведен ряд основных рекомендаций для производителей, регуляторов, МЭК, а также замечания общего характера в контексте вопросов безопасности и данных WSN.

Благодарность

Настоящая Белая книга была подготовлена проектной группой Wireless Sensor Networks, Бюро по рыночной стратегии МЭК. Состав проектной группы:

Dr. Shu Yinbiao, Project Leader, MSB Member, SGCC

Dr. Kang Lee, Project Partner, NIST

Mr. Peter Lanctot, IEC

Dr. Fan Jianbin, SGCC

Dr. Hu Hao, SGCC

Dr. Bruce Chow, Corning Incorporated

Mr. Jean-Pierre Desbenoit, Schneider Electric

Mr. Guido Stephan, Siemens

Mr. Li Hui, Siemens

Mr. Xue Guodong, Haier

Mr. Simon Chen, SAP

Mr. Daniel Faulk, SAP

Mr. Tomas Kaiser, SAP

Mr. Hiroki Satoh, Hitachi

Prof. Ouyang Jinsong, ITEI China

Mr. Wang Linkun, ITEI China

Ms. Wang Shou, ITEI China

Dr. Zhen Yan, Nari Group Corporation

Dr. Sun Junping, China-EPRI

Prof. Yu Haibin, SIA

Dr. Zeng Peng, SIA

Dr. Li Dong, SIA

Dr. Wang Qin, University of Science and Technology, Beijing

Содержание

Аббревиатуры

Технические и научные термины

ABS	антиблокировочная тормозная система
AMI	инфраструктура интеллектуальных счетчиков
CAPEX	капитальные расходы
CoAP	Протокол приложения с ограниченным доступом
COSEM	Сопутствующая спецификация измерения электрической энергии
CPU	Управляющий процессор
DLMS	Спецификация языка устройства
DSN	Сеть распределенных датчиков
ESC	Электронная система безопасности
FCD	Переменные данные транспортных средств
FDM	мультиплексная передача с частотным разделением
FH	Скачкообразное переключение частоты
GHG	Парниковые газы
GPS	Глобальная система позиционирования
ICT	Информационно-коммуникационные технологии
IoT	Интернет вещей
KPI	Ключевые показатели эффективности
M2M	Межмашинный интерфейс
MAC	Управление доступом к среде передачи данных
MEMS	Микроэлектромеханические системы
MIMO	Многоканальный вход – многоканальный выход
OEM	Производитель оригинального оборудования
OFDM	мультиплексирование с ортогональным частотным разделением
OPEX	Эксплуатационные расходы
PHY	Физический уровень
PV	Фотоэлектрический
QoS	Качество обслуживания
RES	Источник возобновляемой энергии

RFID	Радиочастотная идентификация
SOA	Сервис-ориентированная архитектура
SOAP	Протокол сервис-ориентированной архитектуры
TDMA	Многостанционный доступ с временным разделением каналов
TSMP	Синхронизованный временной mesh-протокол
TSP	Защита, безопасность и конфиденциальность
UCC	Городской центр консолидации
USN	Универсальная сенсорная сеть
WIA-FA	беспроводные сети для промышленной автоматизации - автоматизация производства
WIA-PA	беспроводные сети для промышленной автоматизации - автоматизация процессов
WISA	беспроводной интерфейс для датчиков и приводных механизмов
WLAN	Беспроводная локальная сеть
WMAN	Беспроводная городская сеть
WPAN	Беспроводная персональная сеть
WSN	Беспроводная сенсорная сеть
WWAN	Беспроводная глобальная сеть
XFCD	Расширенные переменные данные транспортных средств

Организации, институты и коммерческие компании

ABB	Группа компаний ABB
ARPANET	Сеть Агентства перспективных исследовательских разработок
BBF	Форум широкополосных сетей
CAB	Бюро по оценке соответствия (МЭК)
China-EPRI	Китайский научно-исследовательский институт электроэнергетики
DARPA	Управление перспективных исследований и разработок Министерства обороны (США)
ETSI	Европейский институт стандартов электросвязи
IEC	Международная электротехническая комиссия
IEEE	Институт инженеров по электронике и электротехнике
IETF	Инженерная рабочая группа Интернета

ISO	Международная организация по стандартизации
ITEI	Институт технологии и экономики (Китай)
ITU-T	Международный союз электросвязи – Сектор стандартизации электросвязи (МСЭ-Т)
MSB	Бюро по рыночной стратегии (МЭК)
NIST	Национальный институт стандартов и технологий
OGC	Открытый геопространственный консорциум
OMA	Открытый Мобильный Альянс
SGCC	Государственная сетевая компания Китая
SIA	Шеньянский институт автоматизации (Китай)
SMB	Совет по стандартизации (МЭК)
UCB	Калифорнийский университет в Беркли (США)
W3C	Консорциум всемирной паутины

Глоссарий

Интернет вещей
IoT

Объединение уникально идентифицируемых встроенных вычислительных устройств в рамках развернутой интернет инфраструктуры

Уровень управления доступом к среде передачи данных
MAC-уровень
часть протокола передачи данных, которая контролирует доступ к физической среде передачи в сетях IEEE 802 (LAN)

Система на чипе
SoC
интегральная схема (ИС), которая объединяет все компоненты компьютера или другой электронной системы в один чип

Синхронизованный временной mesh-протокол
TSMP
сетевой протокол, являющийся центральным элементом беспроводной сенсорной сети с низким энергопотреблением

Беспроводная локальная сеть
WLAN
локальная сеть, в которой данные передаются без использования проводов

Беспроводная городская сеть
WMAN
Другое название – беспроводной абонентский доступ (WLL). В основу WMAN положен стандарт IEEE 802.16. Эффективная скорость беспроводного абонентского доступа составляет от 1 до 10 Мбит /секунду на удалении от 4 до 10 километров

Беспроводная персональная сеть
WPAN
беспроводная сеть малого радиуса действия, которая занимает площадь всего несколько десятков метров

Беспроводная сенсорная сеть
WSN
Самоорганизующиеся сети с множеством переходов беспроводных сенсорных узлов, используемых для мониторинга и управления физическими явлениями

Беспроводная глобальная сеть
WWAN
Беспроводная сеть, обеспечивающая коммуникационные услуги в пределах географической области большей, чем территория одного города. Этот вид сетей является наиболее распространенным из всех беспроводных сетей.

Раздел 1
Введение

1.1 Краткий обзор

В современном мире датчики находятся повсюду. Мы стали воспринимать это явление как должное, поскольку датчики находятся в наших автомобилях, смартфонах, на предприятиях, осуществляя контроль выбросов угарного газа в атмосферу, и даже в почве, контролируя грунтовые условия в виноградниках. Хотя, как нам может показаться, присутствие датчиков стало ощущаться совсем недавно, исследования по беспроводным сенсорным сетям (WSN) начались еще в 1980-х годах, а только с 2001 года к WSN появился повышенный интерес с точки зрения использования в промышленных целях и проведения научных исследований. Причиной этого стала доступность недорогих и низкомощных миниатюрных компонентов, таких как процессоры, радио и датчики, которые зачастую были интегрированы в один чип (система на чипе (SoC)).

Концепция интернета вещей (IoT) была разработана параллельно с WSN. Понятие «интернет вещей» было впервые использовано Кэвином Аштоном в 1999 году [1] и относится к уникально идентифицируемым объектам и их виртуальном представлении в «подобной интернету» структуре. Этими объектами могут быть любые объекты от крупных зданий, промышленных предприятий, самолетов, автомобилей, машин, любых видов товаров, конкретных частей больших систем до людей, животных и растений, и даже конкретных частей их тел.

Сам по себе IoT не является технологией связи, тем не менее, технологии беспроводной связи будут играть главную роль, в частности, WSN будут иметь множество вариантов практического использования и охватывать многие отрасли экономики. Небольшие, прочные, недорогие и маломощные WSN-датчики позволят IoT проникнуть в самые маленькие по размеру предметы, установленные в любой среде, по разумным ценам. Интеграция этих объектов в IoT станет важной вехой эволюции WSN.

В целом, WSN можно охарактеризовать как сеть взаимодействующих узлов, которые могут управлять окружающей средой, обеспечивая взаимодействие между людьми или компьютерами и окружающей средой [2]. Фактически, активность восприятия, обработки и связи при ограниченном количестве энергии является прекрасным стимулом для использования перекрестного дизайна, как правило, требующего комплексной обработки распределенного сигнала/обработки данных, управления доступом к среде передачи данных, а также протоколы связи [3].

Синтез существующих приложений WSN в качестве неотъемлемой части системной инфраструктуры позволяет выявить и разработать новые возможности по практическому их применению, которые будут соответствовать будущим тенденциям на рынке и в мире технологий. Например, технологические приложения WSN для умных электросетей, систем умного водоснабжения, интеллектуальных транспортных систем, а также умных домов генерируют огромное количество данных, которые можно использовать в различных целях.

По мере перехода современного мира в новую эпоху WSN в рамках IoT, появляется ряд правовых последствий, которые со временем необходимо будет урегулировать. Одной из наиболее актуальных проблем является право собственности и использование данных, которые были собраны, консолидированы, соотнесены для получения дополнительной ценности. Ожидается, что деятельность брокеров данных станет очень прибыльным бизнесом, поскольку обобщение информации, полученной из различных источников, приведет к появлению новых и не совсем понятных бизнес возможностей, а также, возможно, к гражданско-правовой ответственности в данной

сфере. Недавний скандал, в котором была замешана администрация национальной безопасности США и другие органы, указал на наличие значительного интереса по сбору данных для использования в различных целях.

Одной из наиболее сложных проблем в этом новом мире является мышление машин, принимающих независимые решения, что является фактором непредсказуемого влияния на окружающую среду или общество, в рамках которого эти.

машины функционируют. Это может оказаться несущественным по своей сути, например, холодильник, подающий сигнал своему владельцу о необходимости покупки молока или масла в магазине неподалеку; или весьма сложным в ситуации с роботом, который был запрограммирован для «выживания» в сложной среде, в которой изначально не предусмотрено взаимодействие с людьми. Все может показаться простым в контексте транспортного средства, которое документирует свое использование подобно черному ящику в аэрокосмической промышленности. Однако, таким не является, если такая информация будет использоваться не только для того, чтобы понять причину аварии, но и в ее представлении в качестве доказательства против владельца или оператора. Например, машина, которая будет уведомлять правоохранительные органы о своем незаконном использовании.

Мы приходим в мир, когда машина может действовать, как будто являясь юридическим лицом. Рамки и сама категория ответственности становится размытой, а вопрос ответственности «владельца» и «оператора» машины сильно усложняется в условиях незначительного вмешательства человека или его полного отсутствия в действия робота или машины. Безусловно, это является самым наихудшим сценарием, однако, возникает вопрос сбалансированности стоимости возможной ответственности и преимуществами решений IoT. Эта проблема быстро перерастает в общественную плоскость или плоскость этики, порождая дискуссии в области морали. Это то, что обычно называется сдвигами ценностей поколений, однако, тенденции IoT не будут ждать новых поколений.

1.2 Область применения данной Белой книги

Это шестая по счету Белая книга, обобщающая опыт МЭК в рамках ее Международных стандартов и Услуг по оценке соответствия для решений проблем в глобальном масштабе в области электротехники. Такие аналитические доклады разрабатываются Бюро по рыночной стратегии МЭК, который отвечает за анализ и понимание рынка с целью описания тенденций будущего для принятия стратегических решений.

Раздел 2

История и промышленные стимулы развития WSN

Толчком для развития WSN послужили военные технологии, в частности, системы наблюдения в горячих точках. Сегодня эти сети состоят из распределенных независимых устройств, оснащенные датчиками для мониторинга физических условий, и применяются в промышленной инфраструктуре, автоматике, здравоохранении, транспорте и многих пользовательских сферах.

Первые исследования в области WSN начались в начале 1980-х годов, когда Управление перспективных исследований и разработок Министерства обороны США (DARPA) внедрило программу распределенных сенсорных сетей (DSN) для целей американских вооруженных сил. На тот момент Сеть Агентства перспективных исследовательских разработок (ARPANET) использовалась уже в течение нескольких лет и насчитывала около 200 центральных ЭВМ в университетах и исследовательских институтах [4]. Предполагалось, что DSN будут иметь множество пространственно распределенных недорогих чувствительных узлов, взаимодействующих друг с другом, но управляемых автономно, при этом информация направляется в любой узел, где она может использоваться наилучшим образом. Несмотря на то, что первые исследователи сенсорных сетей имели четкое представление о DSN, сама по себе технология не представляла готовый продукт. Если более конкретно, то датчики были довольно объемными (т.е. по размеру были равны коробке для обуви или даже больше), а возможности практического применения были весьма ограничены. Более того, первые DSN не были тесно связаны с беспроводной связью.

Последние достижения в области вычислительной техники, связи и микроэлектромеханических систем привели к значительным подвижкам в исследованиях в области WSN и приблизили его к достижению изначальной задумки. Новая волна исследований в области WSN началась в 1998 году и стала привлекать все больше внимания и исследователей с различных стран. Основной задачей новой волны исследований новых сенсорных сетей стали сетевые технологии и обработка сетевой информации для беспроводных самоорганизующихся сред с высокой динамикой, а также сенсорных узлов с ограниченными ресурсами.

Кроме того, сенсорные узлы стали намного меньшими по размеру (т.е. от колоды карт до частиц пыли) и более дешевыми, что, в свою очередь, стало причиной появления многих возможностей практического применения сенсорных сетей, таких как мониторинг окружающей среды, сеть автомобильных датчиков и сети датчиков тела.

Следует подчеркнуть, что DARPA стала пионером в рамках новой волны исследований сенсорных сетей, начав исследовательскую программу SensIT [5], которая позволила современным сенсорным сетям получить такие новые возможности как беспроводные самоорганизующиеся сети, динамические запросы и постановка задач, перепрограммирование и многозадачность. В настоящее время WSN считаются одной из наиболее важных технологий 21 века [6]. Например, Китай включил WSN в свои национальные программы по стратегическим исследованиям [7]. В результате, стала набирать обороты коммерциализация WSN, появляется много новых технологичных компаний, таких как Crossbow Technology (подключение физического мира к цифровому миру) и Dust Networks.

Сегодня промышленная автоматизация является одной из наиболее важных областей применения WSN. По данным Freedonia Group, доля мирового рынка датчиков для промышленного использования составляет 11 миллиардов долларов США, а стоимость установки (в ос-

новном, затраты на кабельную связь) и ее использование составляет более 100 миллиардов долларов США. Такая высокая стоимость является основной проблемой, препятствующей развитию промышленных коммуникационных технологий. Технология WSN, позволяющая осуществлять «повсеместно доступное считывание» в рамках всего промышленного процесса, может обеспечить достижение и поддержание важных параметров, недоступных при онлайн-мониторинге по причине указанных выше издержек. Эти параметры являются важными для внедрения оптимального управления для достижения цели повышения качества продукции и снижения потребления энергии.

По данным ON World [8] количество беспроводных устройств, которые будут установлены в промышленных регионах, увеличится на 553 % в период между 2011 по 2016 годами, когда будет установлено 24 миллиона беспроводных датчиков и приводных устройств, или мест установки датчиков по всему миру. В том числе 39 % из них будут использоваться в рамках новых возможностей, которые стали доступны только при появлении беспроводной сенсорной сети. К 2014 году количество WSN-устройств будет составлять 15% от всех мест установки датчиков для контрольно-измерительного оборудования промышленности, а к 2016 году - 33%.

На сегодняшнем рынке три четверти промышленного дохода WSN поступает из обрабатывающей промышленности; причем нефтяная отрасль и электроэнергетика являются самыми быстрорастущими. Например, PetroChina внедряет проекты IoT на своих нефтяных месторождениях с целью реконструкции 200 000 нефтяных скважин. Технология WSN, применяемая в цифровых преобразованиях нефтяных скважин, будет использовать онлайн-мониторинг для измерения объема добычи нефти и обеспечения безопасности производства.

В энергетике, которая в настоящее время переживает модернизацию системы энергоснабжения, технология WSN также играет важную роль при осуществлении контроля безопасности оборудования передачи и трансформации энергии, а также реконструкции миллиардов умных счетчиков.

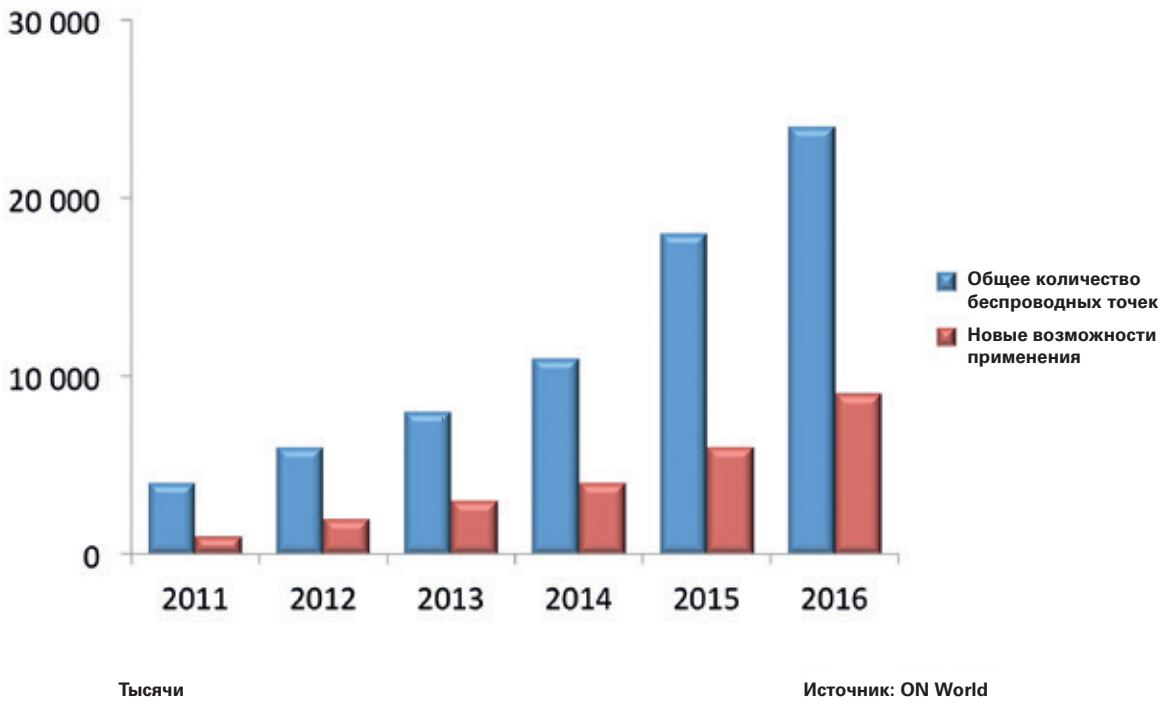
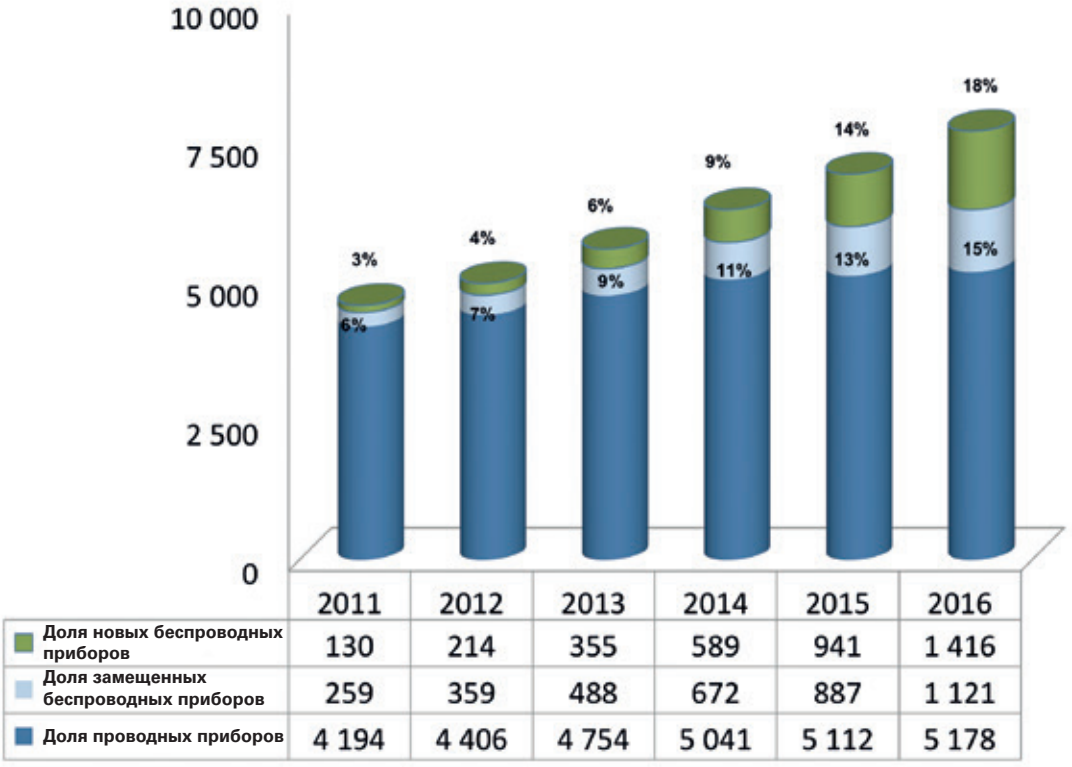


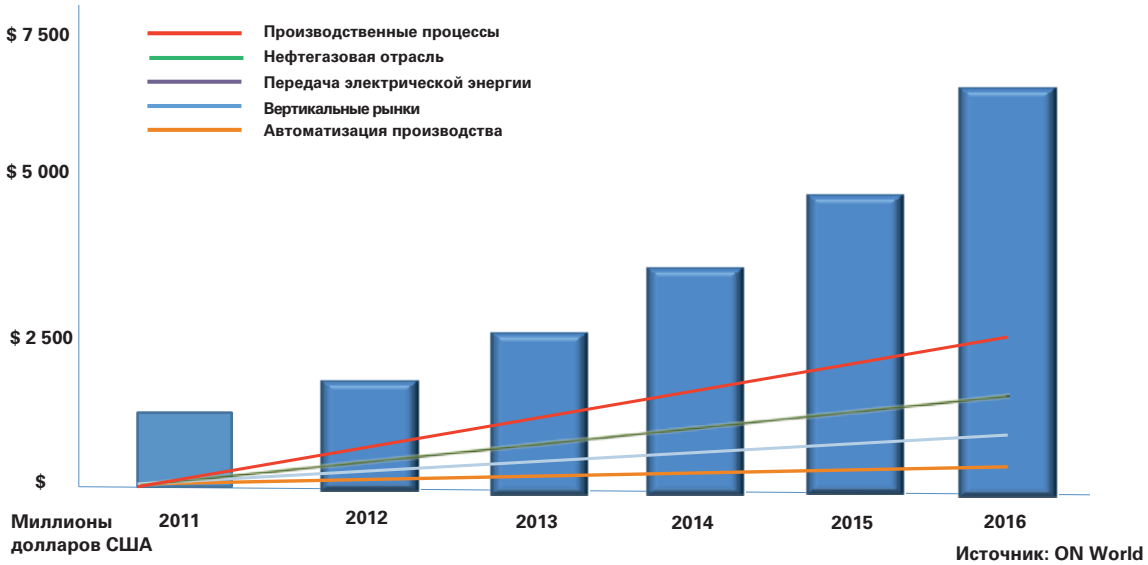
Рисунок 2-1 | Количество беспроводных точек установки датчиков в промышленности во всем мире [8]



	2011	2012	2013	2014	2015	2016
Доля новых беспроводных приборов	130	214	355	589	941	1 416
Доля замещенных беспроводных приборов	259	359	488	672	887	1 121
Доля проводных приборов	4 194	4 406	4 754	5 041	5 112	5 178

Источник: ON World

Рисунок 2-2 | Мировые поставки промышленных портативных контрольно-измерительных приборов (проводных и беспроводных) [8]



Источник: ON World

Рисунок 2-3 | Рост доходов WSN во всех отраслях промышленности [8]

Раздел3

Технология WSN

3.1 Характерные особенности WSN

В целом, WSN можно описать как сеть узлов, которые совместно осуществляют мониторинг окружающей среды и сбор данных, обеспечивают взаимодействие между людьми или компьютерами и окружающей средой [2]. В настоящее время WSN, как правило, включают сенсорные узлы, узлы приводных устройств, шлюзы и клиентов. Большое количество сенсорных узлов, расположенных в случайном порядке внутри или возле контролируемой области (поле обнаружения), формируют сети путем самоорганизации. Сенсорные узлы осуществляют контроль собранных данных для их передачи на другие сенсорные узлы скачкообразным методом. Во время передачи отслеживаемые данные могут обрабатываться несколькими узлами для перехода к узлу шлюза после маршрутизации с несколькими переходами, и, в конечном итоге, достичь узла управления по интернету или при помощи спутника. Пользователь осуществляет конфигурацию и управление WSN при помощи узла управления, публикует задачи по мониторингу и осуществляет сбор контролируемых данных.

По мере развития сопутствующих технологий, стоимость оборудования WSN резко снизилась, а возможности их использования постепенно выходят за пределы оборонной отрасли, распространяясь на промышленный и коммерческий сектора. Следует отметить, что стандарты технологии WSN были хорошо проработаны, а именно Zigbee®[1], WirelessHart, ISA 100.11a,

1 Zigbee® является примером востребованного продукта, имеющегося в продаже. Настоящая информация предоставлена для удобства пользователей настоящего стандарта и не представляет собой одобрение настоящего продукта со стороны МЭК.

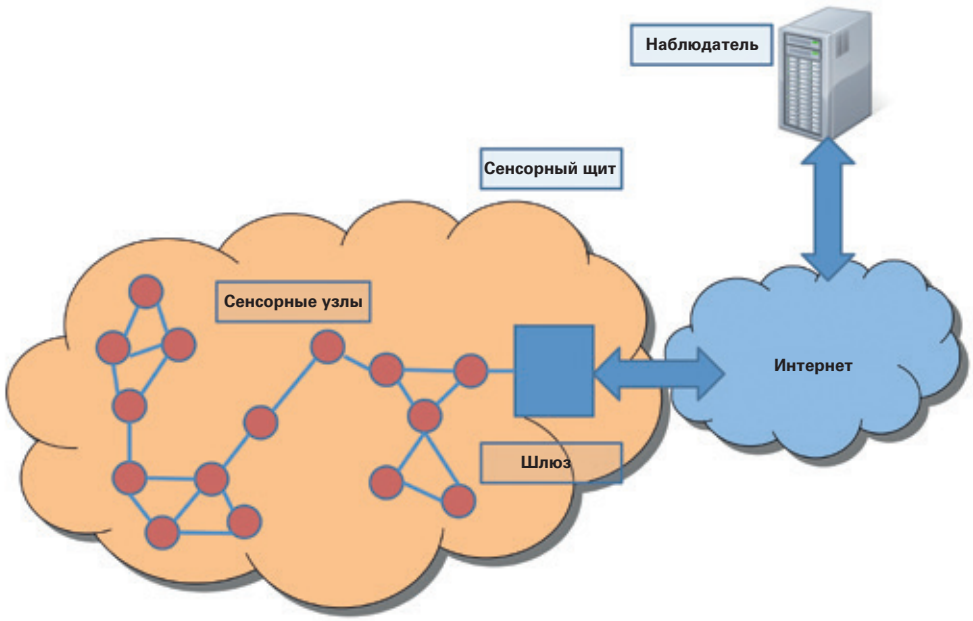


Рисунок 3-1 | Беспроводные сенсорные сети

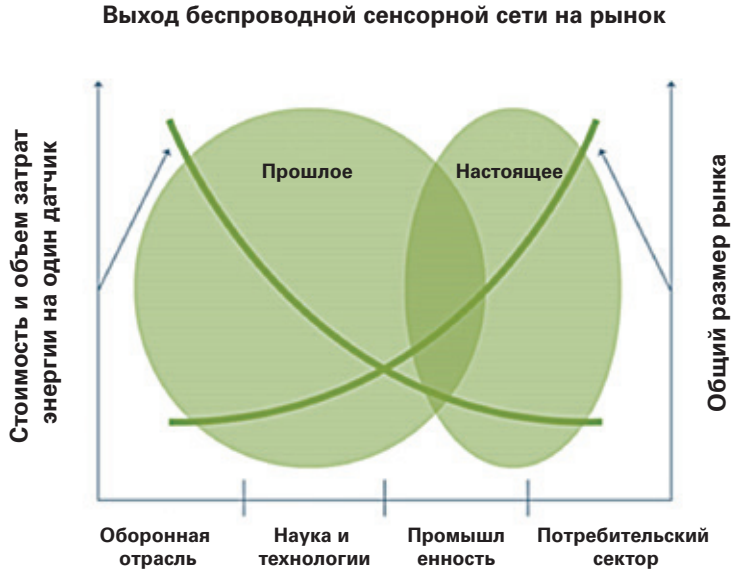


Рисунок 3-2 | Размеры рынка прикладных решений WSN [9]

беспроводные сети для промышленной автоматизации - автоматизация процессов (WIA-PA) и другие. Кроме того, новые возможности применения режимов WSN, которые появляются в промышленной автоматизации и домашних приложениях, общий размер рынка приложений WSN продолжит стремительный рост.

3.2 Узлы датчиков

Сенсорный узел является одной из основных частей WSN.Аппаратное обеспечение сенсорного узла, как правило, состоит из четырех частей: силового модуля, модуля управления энергопотреблением, датчика, микроконтроллера и беспроводного приемопередатчика, см. рисунок 3-3. Силовой модуль обеспечивает электропитание системы. Датчик является центральным элементом узла WSN, который может получить информацию о состоянии окружающей среды и оборудования. Датчик отвечает за сбор и преобразование сигналов, таких как свет, вибрация и химические сигналы в электрические сигналы с последующей их передачей на микроконтроллер. Микроконтроллер принимает данные от датчика и проводит их соответствующую обработку. Затем беспроводный приемопередатчик (RF-модуль) осуществляет передачу данных для физической реализации процесса связи.

Важно, чтобы конструкция всех частей узла WSN учитывала характеристики узла WSN – малый размер и ограниченная мощность.

3.2.1 Технология миниатюризации датчика на основе MEMS

Технология миниатюризации узлов WSN на базе микроэлектромеханических систем (MEMS) была в значительной степени усовершенствована за последние годы. Основой технологии MEMS являются возможности сочетания технологии микроэлектроники, технологии микрообработки и технологии упаковки. Различные уровни микрочувствительных структур 2D и 3D могут быть созданы на основе микроэлектроники и технологии микрообработки, представляющими собой миниатюрные чувствительные элементы. Эти миниатюрные чувствительные элементы, связывающие цепи питания и схемы преобразования сигнала, могут быть собраны воедино в виде миниатюрного MEMS-датчика.

В настоящее время на рынке уже существует множество типов миниатюрных MEMS-датчиков, которые могут использоваться для изме-

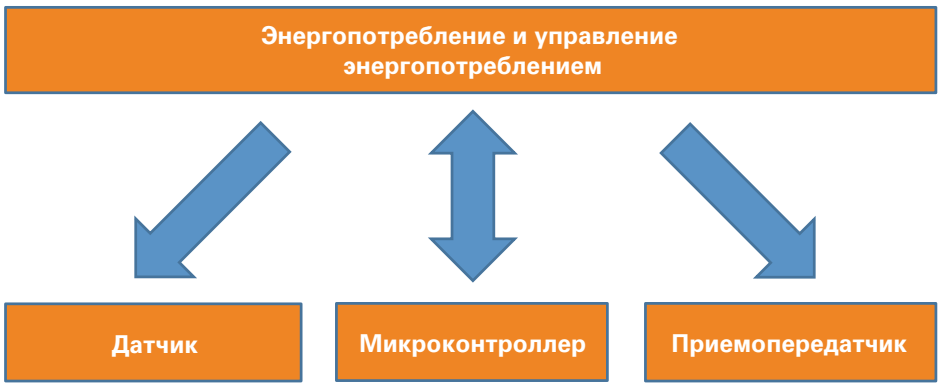


Рисунок 3-3 | Аппаратная структура узла WSN-датчика

рения различных физических, химических и биологических сигналов, в том числе смещение, скорость, ускорение, давление, напряжение, растяжение, звук, свет, электричество, тепло, значение pH и т. д. [10]. В 2003 году исследователи из Калифорнийского университета в Беркли (UCB) разработали узел WSN-датчика (тип «умная пыль») с микро-датчиком. Фактический размер измерительного модуля MEMS составлял всего 2,8 мм × 2,1 мм [11].

3.2.2 Технология сбора энергии окружающей среды

Узлам требуется источник энергии, а сбор энергии из окружающей среды (внешних источников) используется для питания небольших автономных датчиков, например, датчиков на базе технологии MEMS. Эти системы зачастую очень маленькие по размеру и требуют небольшой мощности, однако их применение ограничено зависимостью от мощности аккумулятора.

Сбор энергии окружающей среды может осуществляться не только при помощи обычных оптических ячеек, но и с помощью миниатюрных пьезоэлектрических кристаллов, микроосциляторов, элементов термоэлектрической генерации или устройств, принимающих электромагнитные волны [12] [13].

Некоторые компании стали извлекать коммерческую выгоду из сетевых возможностей применения датчиков с использованием устройств поглощения энергии. Например, немецкая компания EnOcean предоставила устройства для сбора световой энергии, устройства для сбора энергии вибрации и устройства для сбора тепловой энергии в целях умного освещения зданий и контроля загрязненности воздуха. Для контроля гигиены труда в строительстве и исправности оборудования на рынок вышло множество продуктов, собирающих энергию пьезоэлектрической вибрации. Британская компания Perpetuum предлагает ряд продуктов, которые преобразуют энергию механических вибраций в электрическую энергию, используемую для непрерывного питания автономных, не требующих технического обслуживания промышленных беспроводных узлов датчиков. Для этих узлов датчиков энергия вибрации от ударов ваших пальцев, стучащих по столу, может быть достаточной для питания датчика, отправляющего 2 кБ данных на удаление 100 м каждые 60 секунд.

Для мониторинга систем трубопроводов было разработано большое количество продуктов, собирающих энергию на базе разности температур. Продукция компании Nextreme может производить 0,25 Вт электроэнергии за счет разницы температур на уровне 60 ° C в области присутствия поглощающих энергию материалов площадью 3,2 мм × 1,6 мм. На рисунках 3-4 и 3-5 показаны некоторые узлы датчиков, настроенных при помощи устройств поглощения энергии окружающей среды.

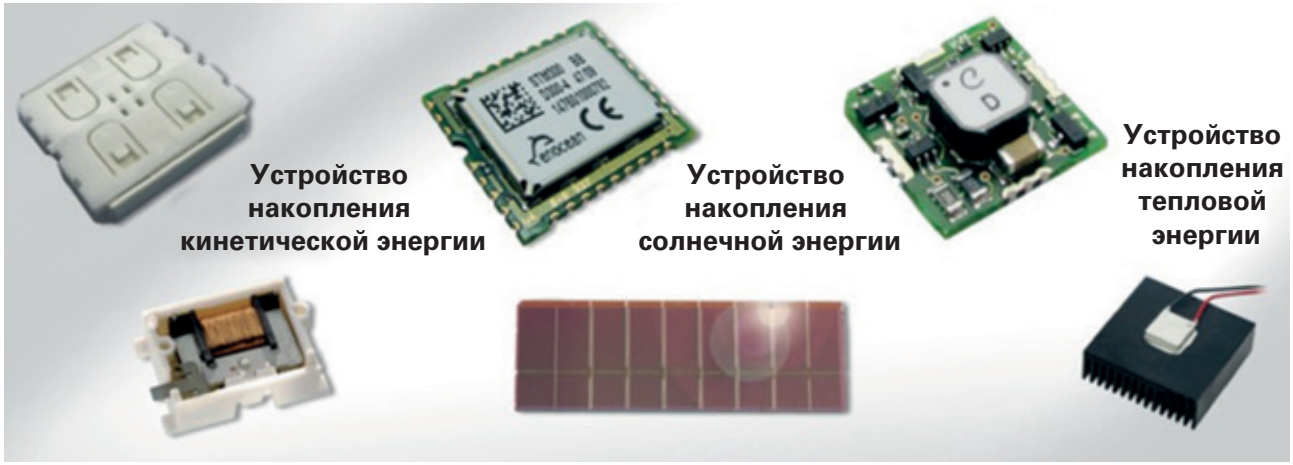


Рисунок 3-4 | Узлы датчиков, сконфигурированные с помощью устройств накопления энергии из окружающей среды [14]

Рисунок 3-5 | Система контроля двигателя на базе накопления энергии вибрации [14]

3.3 Технология сетевого доступа

Сеть доступа, длина которой колеблется от нескольких сотен метров до нескольких миль, охватывает все устройства между магистральной (базовой) сетью и пользовательскими терминалами. Ее называют «последней милей».

Поскольку магистральная сеть, как правило, использует оптическое волокно с высокой скоростью передачи, сеть доступа стала слабым местом всей сетевой системы.

Как показано на рисунке 3-6, по причине открытости беспроводных каналов возникают конфликты во временном, пространственном или частотном измерении, когда канал используется несколькими пользователями. Функция технологий сетевого доступа заключается в управлении и координации использования ресурсов каналов для обеспечения взаимосвязи и коммуникации нескольких пользователей на общем канале.

В зависимости от расстояния и скорости доступа, существующие технологии сетевого доступа можно разделить на четыре категории: беспроводная локальная сеть (WLAN), беспроводная городская сеть (WMAN), беспроводная персональная сеть (WPAN) и беспроводная глобальная сеть (WWAN). Тем не менее, общая тенденция развития высокой скорости передачи данных не совсем соответствует требованиям применения WSN по следующим основным причинам:

- С точки зрения надежности рабочая среда WSN, как правило, достаточно жесткая. Плохие условия среды с узкополосным многочастотным шумом, помехами и многоканальными эффектами не позволяют создать надежную связь по причине скудных ресурсов каналов. Эту проблему еще предстоит решить.

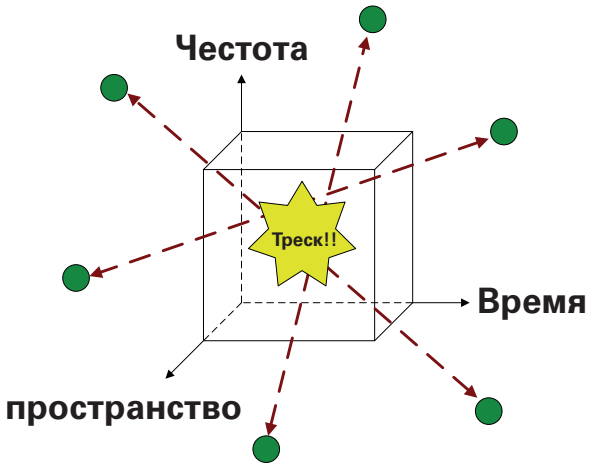


Рисунок 3-6 | Технологии доступа [14]

- С точки зрения возможностей в режиме реального времени, использование WSN и IoT и предполагает более строгие требования в режиме реального времени, чем другие. Небольшая латентность может привести к серьезной поломке. Поэтому в большинстве случаев применения WSN и IoT необходимо обеспечить надежную связь в режиме реального времени.
- С точки зрения энергоэффективности низкое энергопотребление является залогом поддержания длительной эксплуатации автономных устройств на аккумуляторах и снижения затрат на техническое обслуживание. Это также является еще одним требованием при использовании WSN и IoT, особенно для устройств с аккумуляторами, которые трудно заменить.

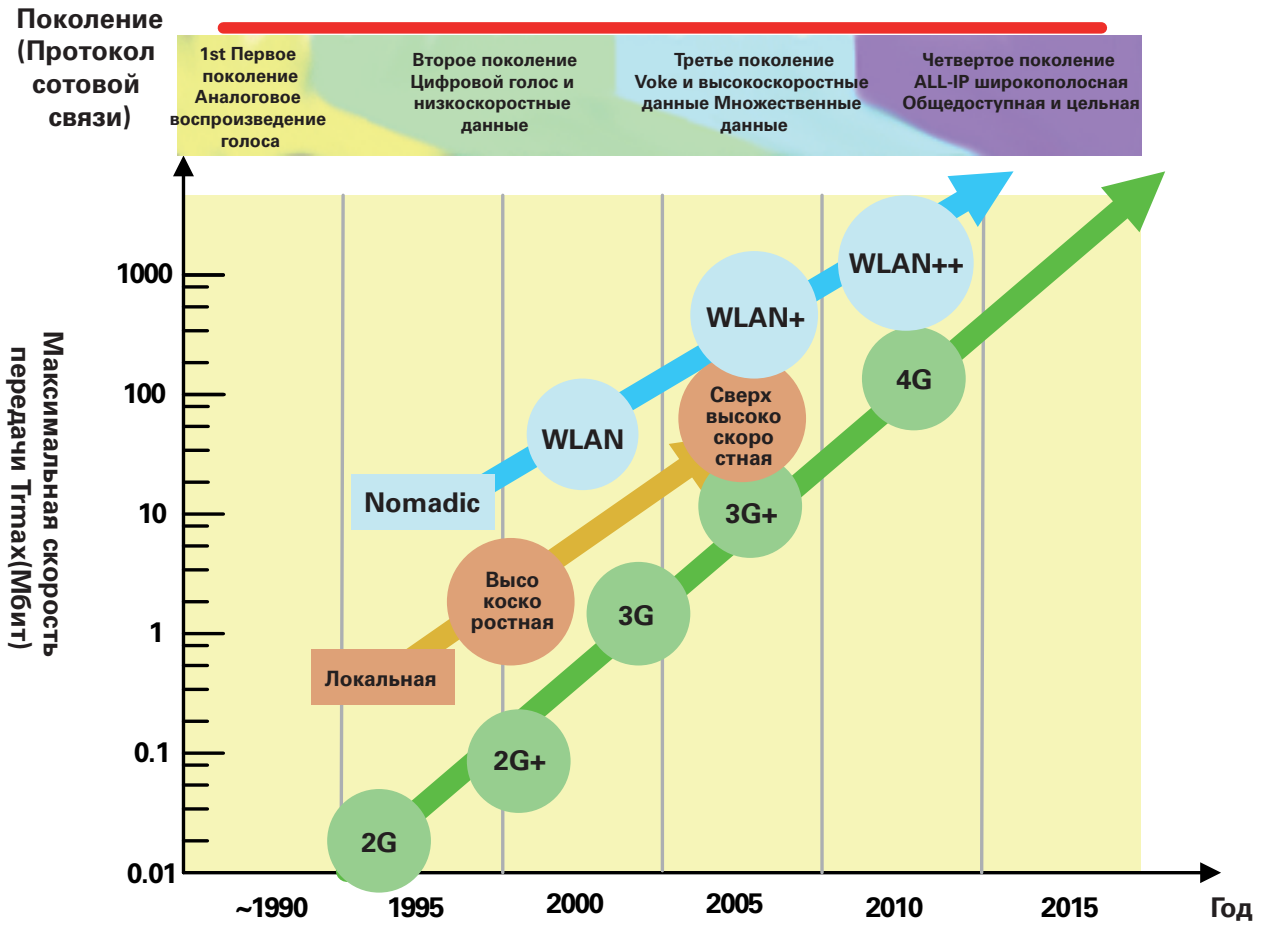


Рисунок 3-7 | Развитие тенденций технологий доступа [15]

В зависимости от конкретных требований применения WSN разработки в области технологий сетевого доступа уже достигли значительного успеха.

Примерами системных и заслуживающих внимания технологий доступа являются Bluetooth 4.0 с ориентацией на медицинскую WSN; IEEE 802.15.4e [16] с ориентацией на промышленную WSN; и WLAN IEEE 802.11™ [17] в контексте IoT. Описание этих технологий представлено в Приложении A.

3.4 Топология

Как правило, WSN состоит из нескольких узлов сетевых датчиков и шлюза для подключения к Интернету. Общий алгоритм развертывания WSN выглядит следующим образом (см. Рис. 3-8): во-первых, узлы сети датчиков передают свой статус окружающим элементам и получают статус от других узлов для обнаружения друг друга. Во-вторых, узлы сенсорной сети организованы в подключенную сеть в соответствии с определенной топологией (линейная, звезда, дерева, ячеистая и т.д.).

Наконец, подходящие пути вычисляются в построенной сети для передачи полученных датчиком данных. Мощность узлов сенсорной сети, как правило, обеспечивается аккумуляторами, поэтому дальность передачи узлов WSN невелика. Дальность передачи может составлять от 800 до 1 000 метров в открытой среде за пределами помещения с прямой видимостью. Она существенно уменьшается в случае закрытой окружающей среды в помещении примерно до нескольких метров. Сеть датчиков для расширения охвата сети использует режим многоскачковой передачи. То есть узлы сенсорной сети являются одновременно передатчиком и приемником. Первый сетевой узел датчика, узел источника, отправляет данные в соседний узел для передачи данных на шлюз. Ближайший узел пересылает данные одному из своих ближайших узлов, которые находятся на пути к шлюзу.

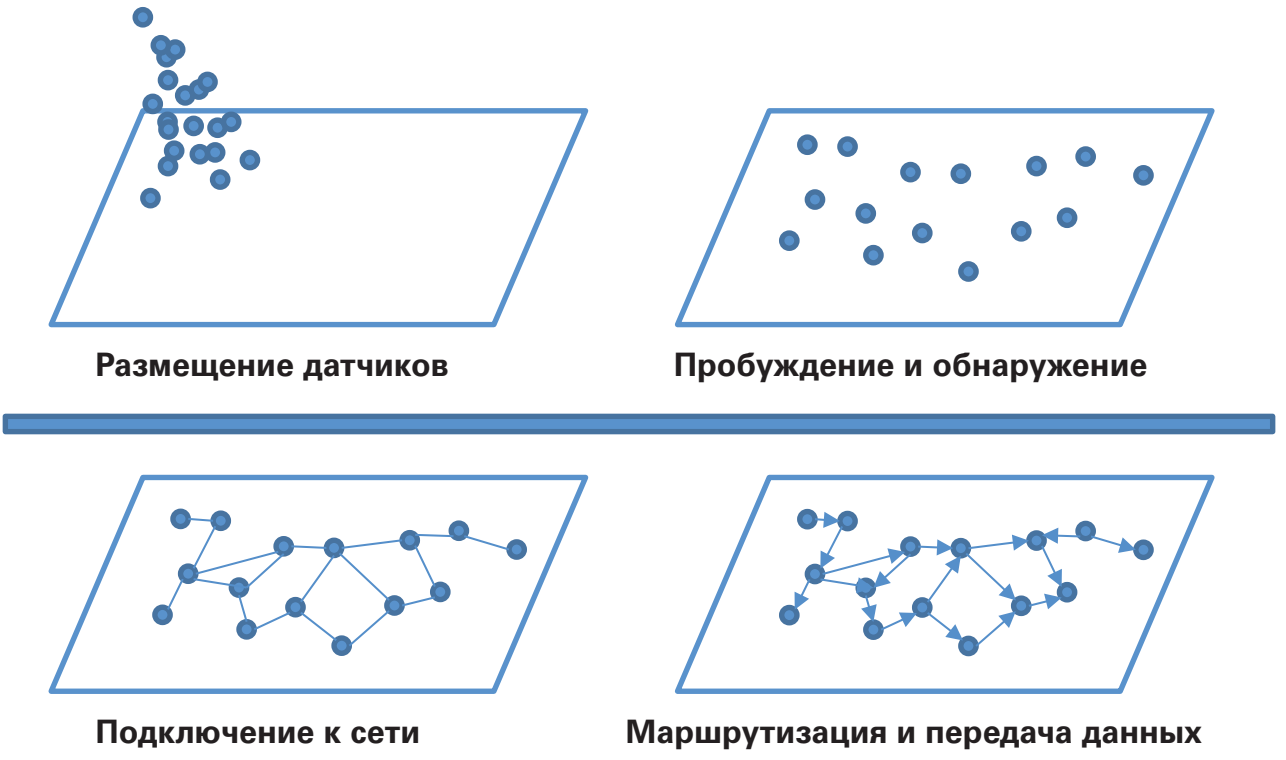


Рисунок 3-8 | Процесс организации и передачи данных WSN [18]

Переадресация повторяется до тех пор, пока данные не поступят на шлюз - пункт назначения. Протоколы и некоторые технологии внедрения WSN могут быть адаптированы к устоявшейся архитектуре и технологиям беспроводных и проводных компьютерных сетей. Тем не менее, особенностями WSN являются самоорганизация, самоадаптация, ограниченная энергия узлов и нестабильные линии передачи.

3.4.1 Самоорганизующиеся надежные сетевые технологии

Узлы WSN располагаются в случайном порядке, а сами узлы можно перемещать, скрывать и интерферировать. Топология ячеистых сетей имеет значительные преимущества по гибкости и надежности по сравнению с другими сетевыми технологиями. Метод управления сетевыми узлами в виде самоорганизации может значительно улучшить надежность сети, в результате чего появилась умная технология ячеистой сети, как показано на рисунке 3-9. В умных специализированных ячеистых сетях узел первым делом осуществляет мониторинг соседних узлов и измеряет уровень сигнала, а затем выбирает соответствующий соседний узел для временной синхронизации и отправляет запрос соединения. Затем соседний узел отправляет запрос на шлюз. Шлюз принимает запрос и выделяет узлу сетевые ресурсы. Благодаря ячеистой сети узлам сети датчиков могут быть выделены два или более пути передачи сигналов (данных) с целью повышения надежности сети. Сеть с синхронизированным по времени ячеистым протоколом (TSMP) [19] пылевой сети может оказывать поддержку самоорганизующейся сети и поддерживать сеть, состоящую из ста узлов.

3.4.2 Технологии недорогих IP-соединений

В структуре ранних сенсорных сетей, как правило, использовались внутренние адреса для управления узлами сенсорной сети. Длина адреса была относительно короткой и подходит для внедрения встроенных датчиков с малой мощностью в узлы сети. Однако, метод управления внутренними адресами несовместим с IP-технологией Интернета, что увеличило сложность взаимодействия между узлами сенсорной сети и обычными узлами IP-сети. Следовательно, необходимо решить проблему подключения WSN и IP-сети.

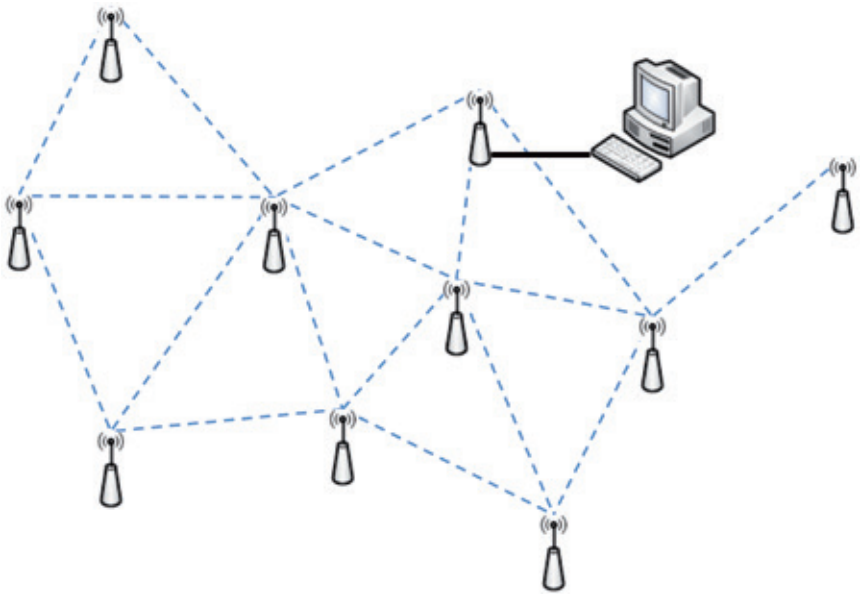


Рисунок 3-9 | Ячеистая самоорганизующаяся сеть [14]

Традиционные адреса IPv4 постепенно исчерпывают свой ресурс, а новая технология IPv6 обладает огромным ресурсом адресов, который подходит для развертывания широкого спектра сетей датчиков. В результате появилась беспроводная технология 6LoWPAN с низким энергопотреблением на основе IPv6 [20]. 6LoWPAN, как правило, использовала упрощенный протокол IPv6 над канальным уровнем протокола IEEE 802.15.4. Сжатие заголовка и

перезагрузка фрагментации пакетов реализованы путем добавления адаптационного уровня между IP-уровнем и канальным уровнем, который является надежным методом обеспечения адаптивности протокола между сетью IPv6 и сетью датчиков, как показано на рисунке 3-10. Продукты сенсорной сети компании Sensinode на базе NanoStack [21] и компании TI на базе CC-6LoWPAN [22] используют технологию 6LoPAN для обеспечения возможностей масштабируемости, непрерывной и надежной связи между сетью датчиков и IP-сетью.

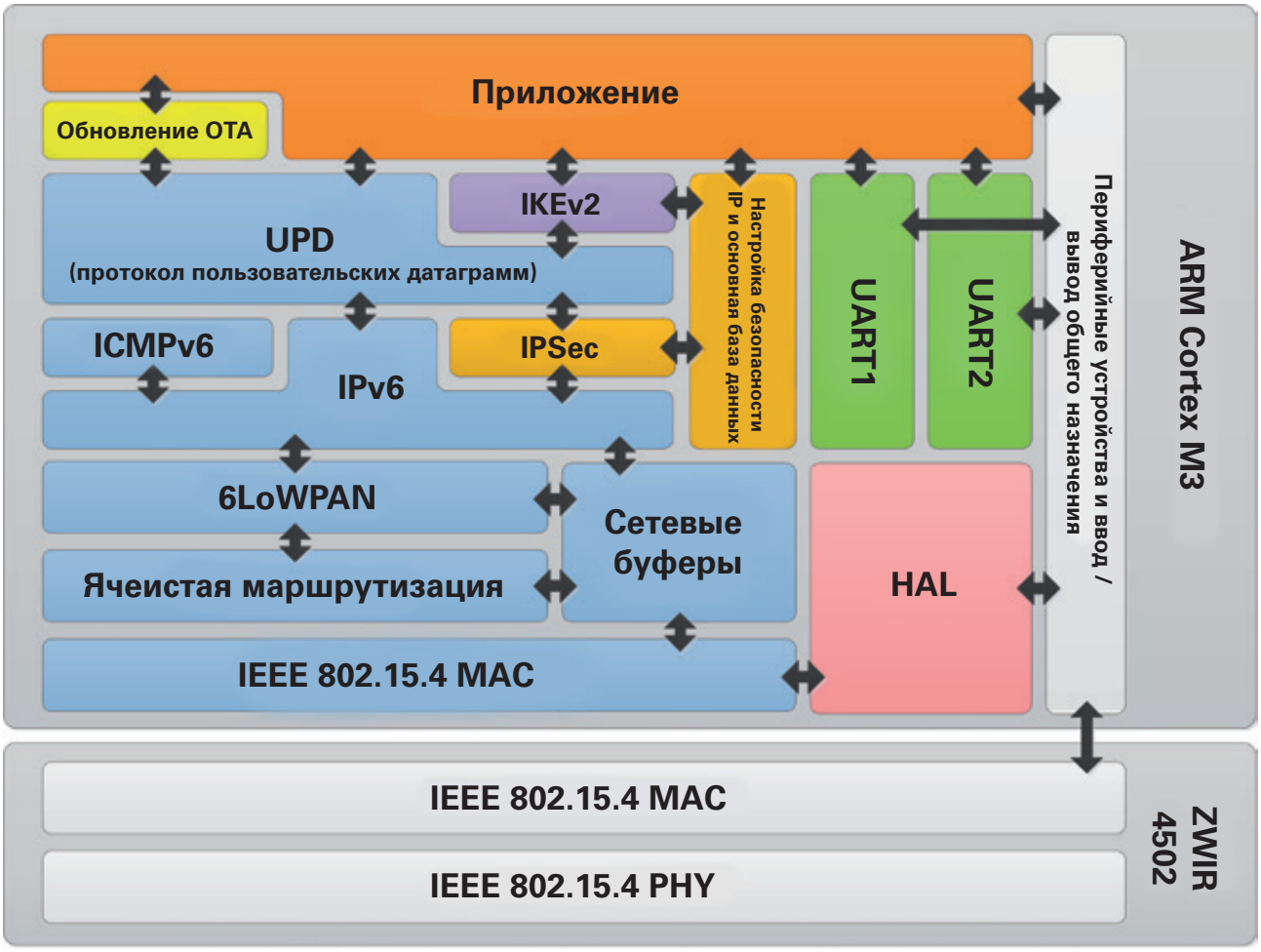


Рисунок 3-10 | Пакет протоколов 6LoWPAN [14]

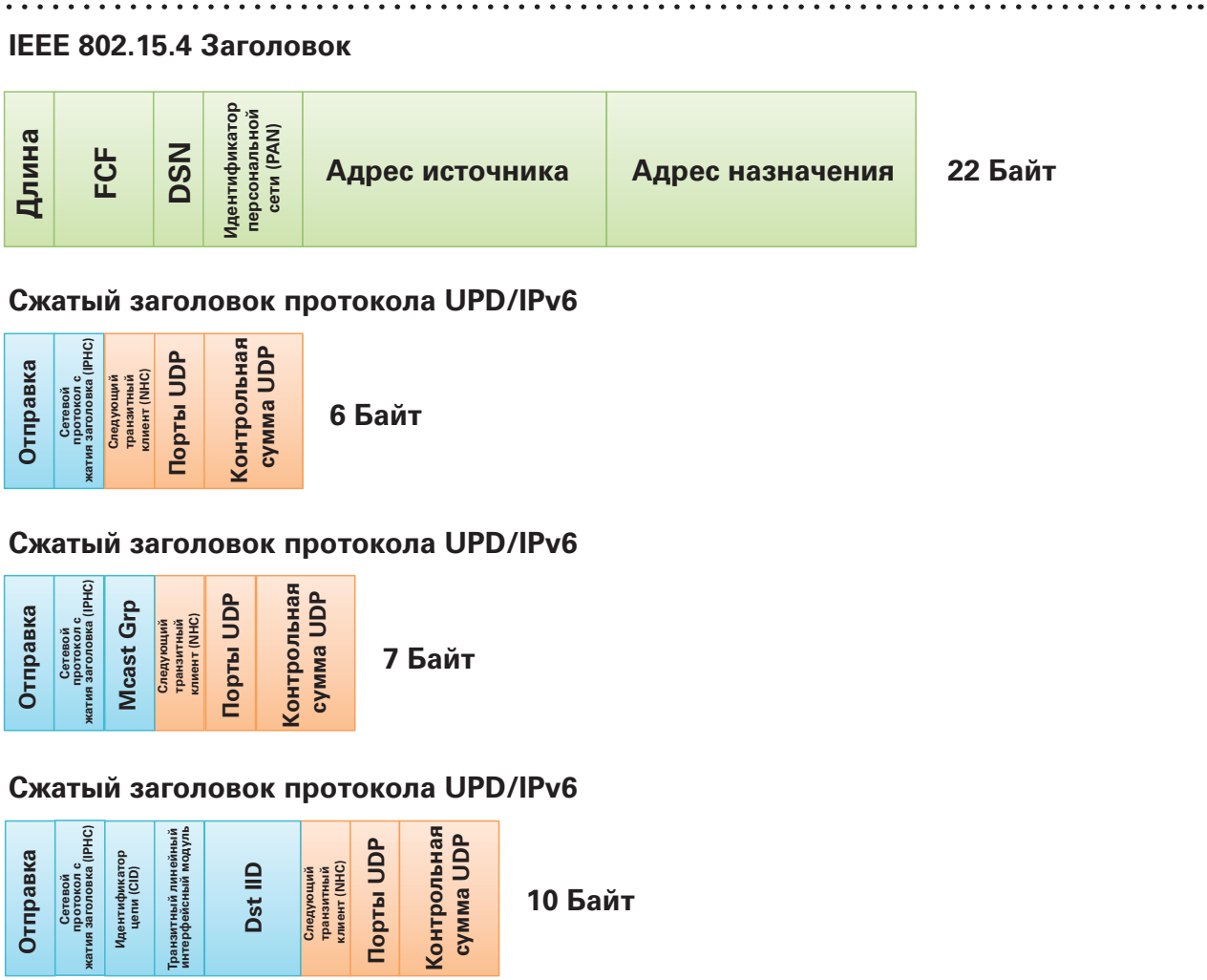


Рисунок 3-11 | Пример улучшенного сжатого заголовка 6LoWPAN [23]

3.4.3 Саморегулируемая технология управления потоками

Одним из отличий между WSN и традиционными проводными сетями является нестабильность беспроводной связи. В WSN связь между узлами восприимчива к помехам и окклюзии, что приводит к сбою передачи сигнала. Традиционная сеть - это стабильная проводная сеть, данные которой могут быть потеряны исключительно по причине перегруженности. Принцип управления потоком заключается в том, что отправитель данных настраивает отправляемый трафик в соответствии с ситуацией потери передачи данных. Когда происходит потеря данных, отправитель уменьшает скорость передачи.

А когда данные не теряются, отправитель увеличивает скорость передачи. Такие механизмы управления потоком не подходят для WSN [23], поскольку потеря данных в сетях датчиков в основном обусловлена перегруженностью, помехами и окклюзией. Только снижение скорости передачи данных не может решить эту проблему, а только снижает производительность сети. Для решения проблемы деградации производительности сети в условиях нестабильной передачи данных предлагается использовать адаптивное управление потоком. Адаптивное управление потоком проверяет причину потери пакетов данных и осуществляет адаптацию передаваемого потока данных.

В то время как в соответствии с качеством канала и количеством ошибок передачи лучшая скорость передачи данных между узлами имеет приоритет для получения хорошей стабильности сети с учетом расстояния передачи и пропускной способности.

3.5 Группирование данных

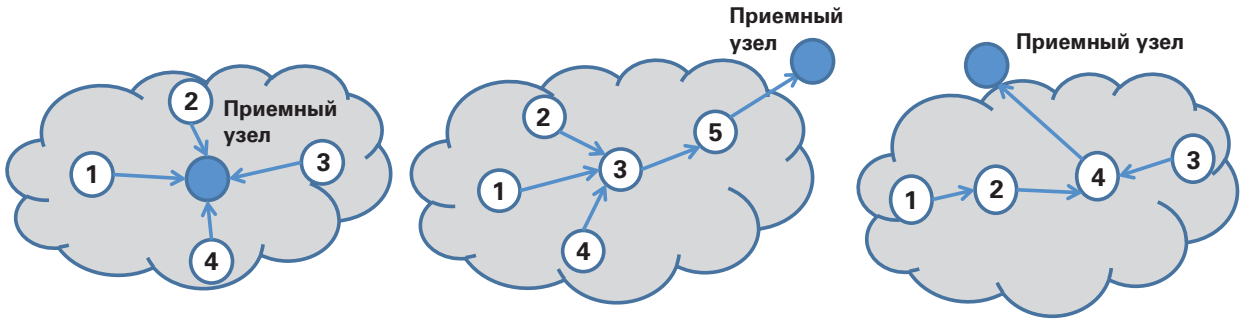
В среде сенсорной сети с ограниченными энергетическими характеристиками неприемлемо осуществлять передачу данных с каждого узла на узел приемника по многим причинам, а именно: заряда аккумулятора, возможности обработки, емкости хранилища и пропускной способности канала связи. Это связано с тем, что в сенсорных сетях с большим покрытием информация, сообщаемая соседними узлами, имеет некоторую степень избыточности, следовательно, при передаче данных по отдельности в каждом узле осуществляется чрезмерная перегрузка каналов связи и избыточное потребление энергии всей сенсорной сети, тем самым сокращая срок службы такой сети.

Во избежание вышеупомянутых проблем стали использоваться методы группирования данных. Группирование данных - это процесс интеграции нескольких копий информации в один экземпляр, что является эффективным и способным удовлетворить потребности пользователей в рамках срединных узлов датчиков.

Использование группирования данных способствует как экономии энергии, так и получению точной информации. При передаче данных потребляется намного больше энергии, чем при обработке данных в сенсорных сетях. Следовательно, с учетом проведения локальных вычислений в рамках узлов и узловых объемом памяти операции по группированию данных призваны удалять большое количество избыточной информации для сведения к минимуму количества передач данных и экономии энергии. В сложной сетевой среде очень трудно обеспечить точность информации, полученной исключительно путем сбора нескольких выборок данных из распределенных сенсорных узлов. В результате для контроля данных одного и того же объекта требуется совместная работа нескольких датчиков, которая в значительной степени повышает точность и достоверность полученной информации.

Производительность протокола группирования данных тесно связана с топологией сети. Затем можно провести анализ некоторых протоколов группирования данных в соответствии с топологиями сети звезда, дерево и цепь, как показано на рисунке 3-12.

Технология группирования данных позволит сэкономить энергию и повысить точность информации при этом придется пожертвовать производительностью в других областях. С одной стороны, в процессе передачи данных и поиска группирующих узлов, операции по группированию данных и ожидание поступления других данных, вероятно, будут увеличиваться при средней латентности сети. С другой стороны, по сравнению с обычными сетями, сенсорные сети имеют более высокий процент потери данных. Группирование данных позволит значительно сократить их избыточность, однако, привести к непреднамеренной потере большего количества информации, снижая устойчивость функционирования сенсорной сети.



a) Топология WSN–звезда **b) Топология WSN–дерево** **c) Топология WSN–цепь**

Рисунок 3-12 | Три вида топологий WSN: звезда, дерево, цепь [14]

3.6 Безопасность

В Голливуде было снято множество фильмов о том, как будет выглядеть будущее, и появление IoT идет в одной канве с версией будущего, озвученного Голливудом. Обе версии видения будущего имеют много общего: машины приобретают огромную силу и влияние в высоко автоматизированном обществе. Вопрос конфиденциальности и безопасности внутри этого общества для каждого индивидуума становится весьма сложно реализуемым на практике, поскольку сложная цепь, в рамках которой были созданы условия безопасности, является по сути бесконечной, а самое слабое звено определяет уровень безопасности всей системы. IPv6 имеет достаточное количество IP-адресов для охвата прогнозируемых десятков миллиардов точек данных, которые создадут наш новый мир. Вопрос в том, могут ли все они быть защищены до того уровня, который может обеспечить права индивида на конфиденциальность и защитить системы от вредоносных атак.

В обычных сетях TCP / IP система безопасности создается для защиты конфиденциальности, целостности и доступности сетевых данных, обеспечивая надежность системы и ее защиту от вредоносных атак, которые могут привести к сбоям в работе систем и раскрытию информации.

Безопасность WSN в качестве характеристики среды узлов и среды приложений требует не только традиционной защиты безопасности, но также и наличие особых требований в отношении защиты, безопасности и конфиденциальности (*TSP*) WSN-сетей.

3.6.1 Защита, безопасность и конфиденциальность

В зависимости от сценария приложения TSP WSN могут требовать защиты целостности, доступности, конфиденциальности, невозможности аннулирования и конфиденциальности пользователей. Она поддерживает целостность и надежность системы, защищая ее от вредоносных атак. TSP WSN может потребоваться осуществлять защиту узлов от несанкционированного доступа, защиту каналов связи и маршрутизации на сетевом уровне [24]. Для обнаружения атак TSP могут потребоваться функции регистрации / проверки.

Технология TSP WSN состоит из аутентификации сообщений, шифрования, контроля доступа, идентификации подлинности и т.д. Потребности WSN в системе TSP должны быть классифицированы следующим образом: безопасность узлов, криптоалгоритмы, управление ключами, безопасная маршрутизация, группирование данных [25] [26].

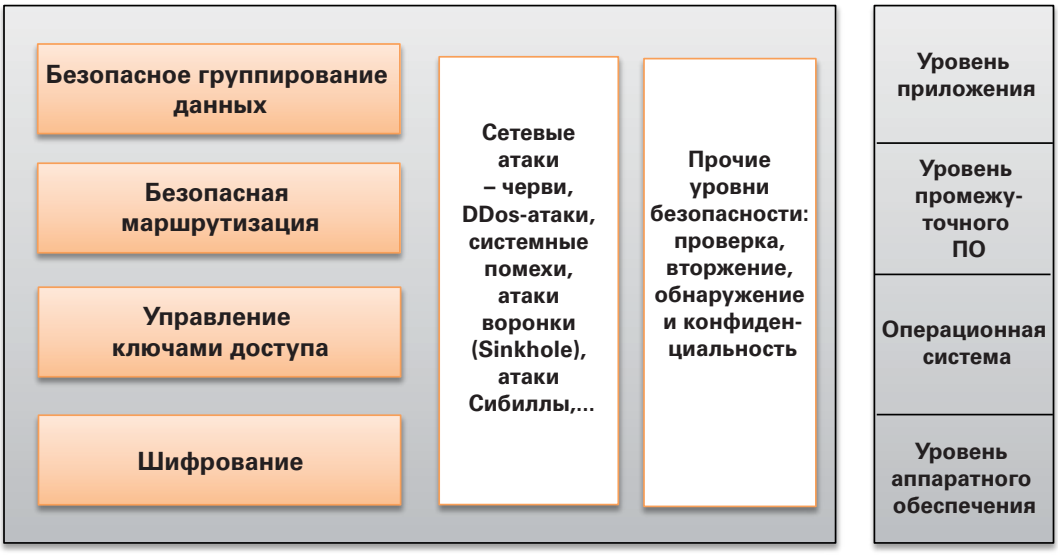


Рисунок 3-13 | TSP-архитектура WSN-сетей [27]

Безопасность узла и «лишение сна»

Узел WSN может быть взломан через его логические интерфейсы или путем прямых физических атак; он может быть перемещен без разрешения или украден.

Безопасность узла может включать функции безопасного пробуждения и безопасной загрузки. Легкий рабочий цикл имеет решающее значение для обеспечения длительного срока службы узлов датчиков с питанием от аккумуляторов. Существуют особые сервисные атаки, так называемые «атаки лишения сна» [28], которые препятствуют переходу узла датчика в энергосберегающий спящий режим, что, в свою очередь, значительно сокращает срок службы атакуемого узла датчика. Стандартные механизмы безопасности, такие как коды аутентификации сообщений или шифрование групп данных, не могут предотвратить «атаки лишения сна»: узел активируется, и энергия тратится на обработку полученного сообщения. Атака может быть замечена только тогда, когда заряд аккумулятора уже был израсходован. На рисунке 3-14 показан узел датчика с радиоприемником пробуждения с низким энергопотреблением. Радиоприемник пробуждения прослушивает канал, когда узел датчика находится в спящем режиме. Он вызывает срабатывание датчика при получении сигнала пробуждения. Для повышения уровня безопасности системы радио пробуждения, сигнал пробуждения является закодированным [29].

Поскольку код пробуждения используется только один раз и, является индивидуальным для каждого узла, его можно отправлять в незашифрованном виде при пробуждении узла.

3.6.2 Криптографические алгоритмы

Шифрование - это специальный алгоритм для изменения исходной информации узла датчика данных, который не позволяет неавторизованному пользователю распознать исходную информацию при получении доступа к зашифрованной информации. Сети WSN государственной инфраструктуры неизбежно подвергаются множеству операций. Традиционные коды проверки подлинности сообщений, симметричное шифрование и шифрование с открытым ключом показали множество недостатков [30] [31]. Поэтому возникла необходимость в новой системе шифрования для WSN. Испанская компания Libelium разработала библиотеки шифрования waspmote для обеспечения безопасности данных WSN умного города в 2010 году. В основном их беспроводные сенсорные устройства поддерживали эти библиотеки. Библиотеки предназначены для разных механизмов шифрования и механизмов консультаций на уровне канала передачи данных, уровне сети и уровне приложения. При этом, они расширяют протокол Zigbee®, обеспечивая его большую безопасность, см. Рисунок 3-15.

Рисунок 3-14 | Радиоприемник безопасного пробуждения [29]

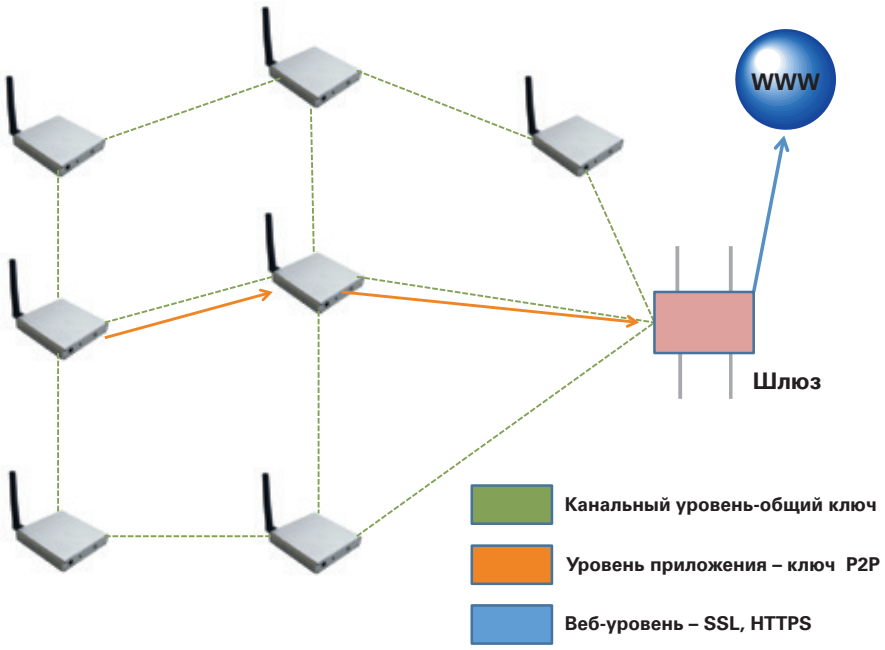


Рисунок 3-15 | Примеры типичного использования библиотек шифрования waspmote [32]

3.6.3 Управление ключами WSN

В целом, система управления ключами призвана обеспечить безопасность WSN. Управление ключами включает в себя генерацию, распределение, верификацию, обновление, хранение, резервное копирование, обеспечение действительности и уничтожение ключей. Эффективная система управления ключами также является основой других механизмов безопасности, таких как безопасная маршрутизация, безопасное позиционирование, группирование данных. Типичные схемы управления ключами в WSN охватывают управление ключами общего применения, управление случайными ключами, управление ключами местоположений, управление ключами кластеризации и управление ключами общего пользования [33].

В ходе процедуры безопасной начальной загрузки создается безопасная конфигурация узла датчика, например, устанавливается ключ соединения. Поскольку существует множество процедур изначальной загрузки, и выбор соответствующей процедуры в значительной степени обусловлен конкретной средой, нормальное функционирование сети датчиков в некой степени отделено от начальной загрузки, следовательно, имеется возможность изменить процедуру начальной загрузки без каких-либо изменений в архитектуре безопасности для нормальной эксплуатации. Соответствующая процедура начальной загрузки в значительной степени зависит от приложения и его среды. Таким образом, было предложено несколько различных процедур начальной загрузки [34]: аппаратный ключ (токен), предварительная конфигурация ключей при изготовлении узлов, физическая защита сообщений, внутриполосная связь в течение фазы настройки с низким уровнем безопасности, внеполосная коммуникация.

3.6.4 Безопасная маршрутизация WSN

Поскольку WSN используют при передаче данных несколько транзитных шлюзов и самоорганизацию в сети, каждому узлу также требуется обнаружение маршрутизации, установление маршрутизации, обслуживание маршрутизации. Безопасный протокол маршрутизации представляет собой полное эффективное решение маршрутизации и может быть необходимым условием для группирования данных и безопасного удаления избыточности от исходного узла до принимающего узла. Мно-

гие защищенные маршрутизированные сети были специально разработаны для WSN, их можно разделить на три группы в зависимости от структуры сети: линейная маршрутизация, иерархическая маршрутизация и географическая маршрутизация [35].

Типичные методы протоколов безопасной маршрутизации включают в себя методы на основе информации обратной связи, информации о местоположении, алгоритма шифрования, метода многоканального выбора и иерархических структур. Различные протоколы безопасной маршрутизации могут решать проблемы различных видов атак [36], например, протокол безопасной маршрутизации на основании информации обратной связи, которая включает в себя информацию о задержке, защите, местоположении, избыточной мощности в кадре подтверждения управления уровнем доступа к среде (MAC). Хотя в рамках этого метода не используется шифрование, он может обеспечить защиту от типичных атак, например, ложной информации о маршрутизации, атаки cesspool и червей. Большинство современных протоколов безопасной маршрутизации предполагают, что сеть датчиков является стационарной, поэтому имеется необходимость разработать новые протоколы безопасной маршрутизации для обеспечения мобильности узлов датчиков [37].

3.6.5 Безопасное группирование данных WSN

Безопасное группирование данных призвано обеспечить безопасность каждого узла. Таким образом, общий алгоритм безопасного группирования данных состоит в следующем: первые узлы предоставляют надежные и достоверные данные и передают их на большие агрегирующие узлы. Большие агрегирующие узлы оценивают достоверность данных и проводят расчеты по группированию на основе избыточности. Каждый агрегирующий узел выбирает следующий безопасный и надежный транзитный шлюз и передает данные на центральный узел. Центральные узлы оценивают достоверность данных и осуществляют окончательный расчет по группированию [38].

Изначально группирование данных использовалось для экономии энергии, а при его осуществлении почти не учитывались вопросы безопасности. В настоящее время безопасное группирование данных в основном осуществляется посредством аутентификации и шифрования на основе теории кластера, кольца и иерархии. Университет Мюнхена разработал прототип группирования данных, который основан на протоколе DTLS с целью практического осуществления защищенных схем передачи. Красный круг на рисунке 3-16 представляет собой их безопасный прототип группирования данных.

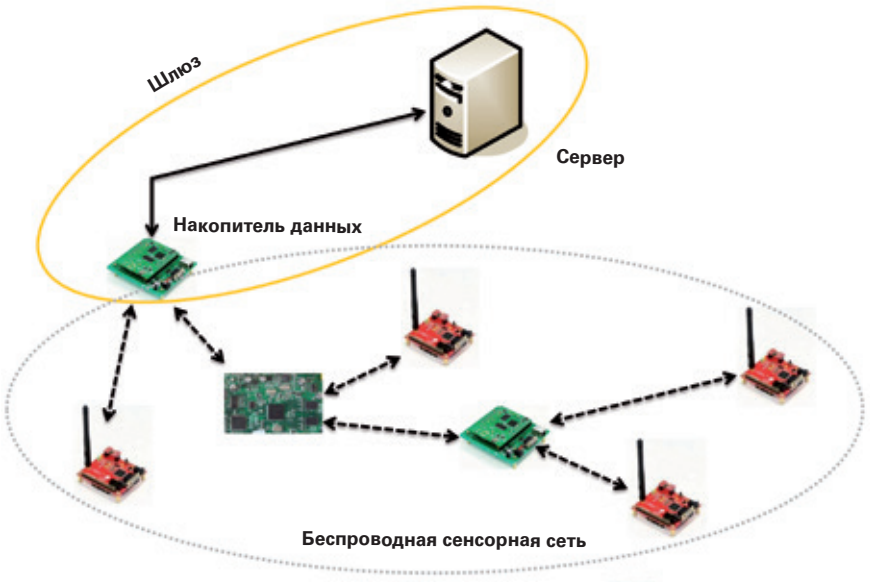


Рисунок 3-16 | Продукты безопасного группирования данных [39]

Раздел 4

Проблемные аспекты WSN

4.1 Системные характеристики, архитектурные отклонения и требуемая структура архитектуры

IoT имеет широкий спектр проблемных аспектов, отличительной чертой которых является их масштаб. Каждая проблема, которую имеет современный интернет, также относится к IoT, но ее масштаб, как правило, намного больше, а последствия - более значительны. Примерами таких проблем являются:

- Перечень доменов сценариев использования: на данный момент интернет уже глубоко проник в жизнь людей, а также деятельность предприятий и организаций, тем не менее, масштаб и глубина такого проникновения в контексте IoT будет только увеличиваться. Появятся не только новые области применения (удаленный контроль срока хранения запасов в режиме реального времени; мониторинг групп конечных пользователей; мониторинг совместного траффика; и др.), а также увеличится степень проникновения процессов и действий с использованием информационно-коммуникационных технологий (ИКТ). Это обеспечивается внедрением радиочастотных идентификаторов (RFID) в цепочки создания стоимости. Информационные технологии уже позволяют компаниям отслеживать объемы поставок продукции внутри компании, а RFID уже проникли в каждый элемент цепи создания стоимости вплоть до отдельных позиций и в рамках каждой организационной единицы (производство; внешняя логистика; розничная торговля, и др.).
- Разница в моделях бизнеса: Web 2.0 уже привел к появлению новых бизнес-моделей и быстрому распространению новых, революционных бизнес-моделей, эта тенденция только будет усиливаться после того, как IoT станет значительной частью будущего Интернета.
- Собственность и аренда: на данный момент в интернете исключительное право собственности и эксклюзивное использование является урегулированным правилом, тем не менее, социология IoT будет совершенно иной. Сложные системы, например, городские сенсорные сети, не обязательно будут принадлежать одной организации, при этом влияние групп, не являющихся владельцами, будет только увеличиваться (объединения адвокатов, государственные органы, законодательные органы и т.д.). Кроме того, чаще всего в рамках одной системы свою деятельность будет осуществлять более чем одна организация. Например, производитель оригинального оборудования (OEM) может нанять нескольких сторонних поставщиков из другого региона для проведения технического обслуживания своего производственного оборудования, что, в свою очередь, потребует наличие удаленного доступа к производственной системе IoT.
- Спектр охватываемых объектов: спектр «вещей», о котором будет собираться информация, который будет отслеживаться и обрабатываться через IoT, будет слишком большим. По размеру он будет охватывать великое множество объектов от микроскопических и даже субмикроскопических (бактерии, наноботы и т.д.) объектов до макроскопических объектов в масштабе планет или даже больше. В цифровом исчислении эти объекты будут весьма разными, а их составляющие будут также зависеть от контекста. Например, для судоходной компании целые контейнеры обычно составляют максимальную шкалу детализации и, следовательно, являются «вещами», а для

розничного оператора-получателя, а также для конечного потребителя «вещами» будут являться отдельные элементы такой продукции в таком контейнере.

- Временные рамки и надежность: IoT будет использоваться в тех сферах, где управление в режиме реального времени с высоким уровнем надежности будет обязательным (автоматизированное производство, управление воздушным судном и т.д.), в то время как другие практические возможности (мониторинг ледников, контроль стада и т.д.) могут осуществляться практически в режиме офлайн в рамках временных рамок, измеряемых минутами или даже годами.

Базовые рамки указанной выше задачи приведут к возникновению весьма разнообразных проблем, которые системы IoT должны будут решить. Такое положение вещей, естественно, будет преобразовываться в различные системные проблемы и задачи, многие, если не большинство, из которых будут сформулированы на межсистемном уровне. В частности, проблемы и задачи будут касаться производительности всех систем IoT и меньшего количества отдельных членов или даже частей. Таким образом, архитекторы IoT будут сталкиваться с разнообразными качественными требованиями, и для соответствия тем же качественным требованиям у них будет целый спектр возможных выборов. Эта проблема наглядно представлена в таблице 1. Для каждого качества системы имеется более чем одно архитектурное представление, благодаря которому это качество может быть изменено. Например, системная масштабируемость. Одним из представлений оказания влияния на масштабируемость является функциональное представление. Например, чтобы установить приоритет распределенных функций над централизованными функциями. Та же стратегия может быть реализована с точки зрения информации, обработка которой осуществляется в рамках системы.

Другими словами, системные качества пересекаются в более чем одном архитектурном представлении. Кроме того, достижение одного качества при помощи одного представления (например, масштабируемость) может оказать неблагоприятное воздействие на другие системные качества (например, безопасность).

В архитектуре появляются различные расхождения, поскольку пространство решений для архитектур является многомерным и запутанным, качественные требования пересекаются более чем с одним системным аспектом, а определенное качество может быть получено более чем одним способом. В частности, различные группы разработчиков создадут совершенно разные архитектуры и реализуют несовместимые способы внедрения системы для одного и того же набора требований, если не будут использоваться какие-либо смягчающие механизмы. Обратите внимание, что данная проблема не является новой, однако, в IoT она еще более усугубляется из-за огромного количества областей сценариев использования, а также различных культур и лучших практик, которые получили свое развитие в каждой области сценариев использования.

Таблица 4-1 | Использование архитектурных представлений о качествах системы (отбор) [40]

		Системные качества			
		Защита, безопасность и конфиденциальность	Производительность и масштабируемость	Доступность и устойчивость	Масштабируемость
Архитектурное представление	Функциональное	Средняя	Средняя	Низкая	**Высокая**
	Информационное	Средняя	Средняя	Низкая	**Высокая**
	Согласованность	Средняя	**Высокая**	Средняя	Средняя
	Внедрение	**Высокая**	**Высокая**	**Высокая**	Низкая
	Эксплуатационное	Высокая	Низкая	Средняя	Низкая

Помимо угрозы функциональной совместимости имеется еще одно отрицательное последствие расхождения архитектуры: сниженная «горизонтальная рециркуляция» функций, модулей и концепций в зависимости от области (домена). То есть, поток лучших практических решений, функциональных модулей и др. через границы области использования будет затруднен разнообразной, неконтролируемой экосистемой расходящихся архитектур. Это оказывает влияние как на капитальные затраты (например, затраты на инновации и развитие), так и операционные расходы (например, системы с высоким уровнем сложности, и новому персоналу требуется некоторое время для получения базового понимания). Поэтому расхождение в архитектуре также отрицательно влияет на коммерческую привлекательность IoT.

Перечисленные выше проблемы не решаются сами собой, наоборот, в данной ситуации необходимы корректирующие действия. Требуется структура архитектуры (эталонная модель, эталонная архитектура, а также руководство по ее применению), которая способствует повторному использованию архитектурных принципов и повторному использованию системных модулей и концепций. Эталонная модель обеспечивает согласованную онтологию и семантику для описания и анализа вариантов использования IoT и систем IoT. Эталонная архитектура представляет собой профессиональные рекомендации по созданию систем IoT, которые отвечают требованиям и ожиданиям заинтересованных сторон IoT. Руководство по применению обоих эталонов также отвечает на вопросы о решении качественных системных требований, избегая архитектурных и системных расхождений.

4.2 Доступ к сверхбольшим измерительным датчикам

Установка измерительных устройств WSN в будущем будет возрастать по экспоненте из-за наличия потребности в комплексном мониторинге в сфере транспорта, электроэнергетики, промышленности и другой важной инфраструктуре. Например, в процессе контроля производственного оборудования на заводах на каждом устройстве необходимо установить различные датчики для измерения таких состояний устройства, как температура и вибрация. По оценкам ABI Research в ближайшие 10 лет появится 50 миллиардов новых устройств межмашинной коммуникации (M2M), а количество устройств WSN невозможно будет сосчитать [41]. Следовательно, возникает проблема о том, как справиться со столь интенсивным доступом к устройствам WSN.

4.2.1 Обработка массивов неоднородных данных

Благодаря широкому применению технологии WSN в информационно-аналитическом процессе различных инфраструктур объем данных, создаваемый WSN-датчиками, вырастет с сегодняшнего уровня EB (1 018 байт) до уровня ZB (1 021 байт). Согласно статистике и прогнозам IDC, в 2009 году общий объем данных составил 0,8 ZB (1 021 байт) и к 2020 году составит 35 ZB [42]. В качестве большей части данных, количество данных, полученных датчиками из физического мира в 30 раз больше, чем от людей. В этом смысле хранение и передача, а также своевременное использование по назначению массовых данных будет беспрецедентно масштабной задачей.

Данные датчиков WSN, в том числе показатели температуры, давления, расхода, скорости и других физических величин, имеют многомерные неоднородные характеристики. Для применения информационной и интеллектуальной инфраструктуры требуется единый механизм обработки этих многомерных неоднородных данных. Однако существующая технология обработки информации затрудняет удовлетворение растущего спроса на WSN.

4.2.2 Интеллектуально управление и услуги динамических изменений

В будущем эксплуатация и управление городской инфраструктурой должно соответствовать требованиям безопасности, энергосбережения, эффективности, удобства и т.д. В настоящее время сбор информации осуществляется автоматически, затем она обрабатывается посредством ручного анализа, по результатам которого принимаются

соответствующие решения и выполняются действия. Тем не менее, такой алгоритм действий уже устарел. Современные условия требуют внедрения интеллектуального контроля, который сможет реагировать на динамические изменения. Во-первых, порядок использования WSN должен пройти преобразования из простого восприятия информации в систему замкнутого цикличного управления. Например, в рамках интеллектуальной транспортной системы для обеспечения нормального функционирования системы городского транспорта необходимо провести динамический анализ дорожного движения и регулировать работу светофоров в режиме реального времени. Тем не менее, управление инфраструктурой имеет большое значение, поэтому обеспечение безопасности и надежности интеллектуального контроля является весьма серьезной проблемой. Во-вторых, сервисный режим WSN необходимо преобразовать из единого и предварительно установленного в динамический и персонифицированный. Например, при умном использовании энергии с целью обеспечения потребительского спроса на электроэнергию и повышения эффективности работы сети, настройка температуры кондиционирования воздуха и уровней освещенности должна быть динамически регулируемой в соответствии с текущей нагрузкой на сеть, условиями окружающей среды, а также индивидуальных особенностей. Следует понимать, что оказание услуг динамической генерации в зависимости от изменений окружающей среды является весьма сложной проблемой.

4.3 Архитектура сети датчиков

Технология сенсорной сети широко используется в строительстве городской инфраструктуры и имеет значительные достижения. Однако, в рамках различных прикладных решений по использованию сенсорных сетей встроенные сетевые датчики и управляющие устройства, как правило, имеют различные аппаратные платформы, операционные системы, базы данных и межплатформенное программное обеспечение. Они не могут быть развернуты в различных неоднородных сетевых средах с бесплатным обменом информацией, кроме случаев, когда они поддерживаются выделенными коммерческими системами и платформами по управлению приложениями. В контексте дизайна архитектуры, большинство сред приложений сенсорной сети разработаны в тесно связанных замкнутых архитектурах. В этом смысле система имеет характеристики хранилища информации и подходит исключительно для среды приложения в небольших отраслях. Более того, разделение и повторное использование архитектуры инфраструктурной системы и услуг в данной области является весьма проблематичным. Кроме того, ресурсы третьих лиц сложно интегрировать в систему с экономической точки зрения. Следовательно, широкомасштабное использование и продвижение сенсорных сетевых технологий является ограниченным.

Таким образом, имеется насущная потребность создать более открытую и гибкую систему, позволяющую устранить эти проблемные места IoT. Полная информатизация является неизбежным этапом развития сенсорных сетей для обеспечения комфортного обмена (совместного пользования) информацией, полученной от датчиков, контроля спроса и внедрения изолированных данных в сенсорную сеть.

Интернет технологии представляют собой естественный технологический выбор для достижения полной информатизации и обмена неоднородными ресурсами, являясь основой для межплатформенного совместного использования ресурсов и услуг.

В настоящее время в мире существуют две тенденции в контексте сетевых датчиков: первая позволяет людям в разных местах по всему миру совместно использовать датчики, а вторая позволяет датчикам взаимодействовать с другими датчиками.

4.4 Параллельный доступ с множеством подключений

Технология беспроводного доступа все больше используется в умных сетях и других промышленных целях, в то же время к данной технологии выставляются все более строгие требования к производительности (крупномасштабность, низкое значение задержки). При использовании умной сети в целях управления

трансформаторными подстанциями задержка, как правило, должна быть в пределах от 0,677 - 2 мс для сетей с десятками узлов; задержка второго уровня - для сетей с тысячами узлов в пределах подстанции; задержка второго или минутного уровня - для будущей инфраструктуры интеллектуальных счетчиков (AMI) с тысячами узлов. Хотя существующие технологии WSN-доступа могут поддерживать задержку второго уровня для сквозной передачи в сотнях сетей, что является достаточным для мониторинга приложений, на данный момент спрос на высокоскоростной параллельный доступ для будущего использования не может быть удовлетворен. Недостатки существующей технологии доступа при работе с приложениями WSN с такими характеристиками, как небольшая интенсивность трафика и высокая степень многопоточности, приведены ниже:

- Существующие технологии планового доступа для обеспечения надежности передачи, как правило, используют такие стратегии, как резервирование временных интервалов повторной передачи, разделение частот между несколькими пользователями, нерегулярное распределение ресурсов и т.д. Потенциал этих защищенных ресурсов не используется в полной мере.
- Технология состязательного доступа должна справляться с конфликтами по использованию ресурсов. По мере увеличения трафика данных параллельно работающих приложений производительность сети резко падает.
- Приложения с высокоскоростными параллельными характеристиками, в частности, приложения управления, чья полезная нагрузка, как правило, является небольшой, будут сильно перегружены по причине большой нагрузки пакетов при использовании существующих технологий доступа, а эффективность доступа к спектру является очень низкой.

На данный момент для решения вышеуказанных проблем было предложено два решения. Первое решение – беспроводной интерфейс на базе Bluetooth для датчиков и приводных механизмов (WISA), предложенный компанией ABB; второе решение - беспроводные сети на базе IEEE 802.11™ для промышленной автоматизации – заводская автоматизация (WIAFA), предложенная группой китайских организаций (более десяти членов) во главе с Институтом автоматизации Шэньяна, Китайской академией наук.

4.4.1 Параллельный доступ с множеством подключений с мультиплексированием с частотным разделением каналов

Технология Bluetooth работает в диапазоне 2 400 - 2 483,5 МГц, имеет 79 выделенных каналов Bluetooth и позволяет обмениваться данными на небольших расстояниях. Технологию Bluetooth можно использовать на физическом уровне при необходимости удовлетворения требований к световому потоку и параллельному доступу с множеством подключений. Кроме того, MAC-уровень можно отрегулировать для поддержки многостанционного доступа с временным разделением каналов (TDMA), мультиплексирования с частотным разделением каналов (FDM) и скачкообразного переключения частоты (FH). Долгосрочное радиочастотное питание является передовой технологией для источников питания.

4.4.2 Параллельный доступ с множеством подключений с распределенными антенными системами

IEEE 802.11™ [17] представляет собой набор спецификаций MAC-уровня и физического уровня (PHY) для внедрения связи WLAN в полосах частот 2,4 ГГц, 3,6 ГГц, 5 ГГц и 60 ГГц. Следуя сетевой архитектуре распределенных антенных систем, PHY на базе IEEE 802.11™, FDM и MAC-уровень на базе TDMA подходят для междугородной связи. Кроме того, комплексное использование выделения ресурсов, поддерживающих состояние каналов, группирование данных, агрегирование пакетов данных и другие методы оптимизации производительности, задержка данных может быть уменьшена до 10 мс. Технологии параллельного доступа с множеством подключений на базе IEEE 802.11™ могут широко использоваться в

таких отраслях, как наполнение пивных бутылок и роботизированные производственные линии, см. Рисунок 4-2.

Рисунок 4-2 | Параллельный доступ с множеством подключений с распределенными антенными системами [14]

4.5 Высокоскоростная передача данных в режиме реального времени

Традиционные WSN-сети осуществляют сбор, обобщение и обработку информации об объектах на территории покрытия и пересылают их наблюдателям для анализа в режиме онлайн или офлайн с низкими требованиями в режиме реального времени, такими как считывание показаний счетчиков, мониторинг окружающей среды и других. Покрытие сети является ограниченным (например, жилой комплекс или открытое пространство площадью в несколько квадратных километров), а требования к задержке - низкие (на уровне минут или часов). Следовательно, при проведении исследований традиционных WSN-сетей основное внимание уделяется возможностям по повышению надежности сети и снижению энергопотребления. Тем не менее, при непрерывном развитии инфраструктуры в умных городах зона покрытия сети увеличивается, и вместе с ними увеличиваются требования к передаче в режиме реального времени. Например, возьмем систему регулирования дорожного движения города.

Такая информация как дорожные условия, количество транспортных средств, скорость движения и т.д., собирается на территории всего города, а затем передается в реальном времени в центр управления, где рассчитывается наиболее приемлемая схема регулирования дорожного движения, которая впоследствии передается обратно в режиме реального времени на соответственные перекрестки. Этот процесс должен осуществляться в течение одной секунды, что является еще одним требованием на передачу данных в рамках системы сенсорной сети в режиме реального времени в различных областях.

Другие сетевые технологии могут использоваться для создания сенсорной сети с обширным покрытием (например, Ethernet, WLAN, сети мобильной связи и т.д.), а также создания неоднородных сетей с различными физическими средами и механизмами управления. Проводные сети, такие как Ethernet, используют медные витые пары или оптические волокна в качестве физического носителя со скоростью от 100 Мбит / с до 1 000 Мбит / с и более и имеют задержку передачи в несколько миллисекунд; скорость передачи беспроводных сетей на базе IEEE 802.11™ и IEEE 802.15.4 может составлять 250 кбит / с - 72,2 Мбит / сек, а задержка передачи составляет от нескольких сотен миллисекунд до нескольких минут. Разработка этих сетевых технологий, в частности, технологий Многоканального входа – многоканального выхода (MIMO) и мультиплексирования с ортогональным частотным разделением (OFDM) в рамках беспроводной связи, значительно увеличивает спектральную эффективность беспроводной сети, повышает производительность сети и, таким образом, закладывает основу для создания сенсорной сети с обширным покрытием. Однако эти сети функционируют лучшим из возможного образом и не учитывают взаимосвязь с другими сетями о том, как обеспечить передачу в режиме реального времени, что является задачей будущих исследований сенсорных сетей.

Исследование сенсорных сетей с передачей информации в режиме реального времени с обширным покрытием вызывает большую озабоченность во всем мире, а имеющиеся решения можно условно разделить на распределенные и централизованные.

4.5.1 Распределенное решение

При входе в сеть распределенное решение разбивает задачи по передаче данных на несколько уровней в соответствии с требованием задачи.

Каждая часть сети определяет различные уровни задач в соответствии с условиями работы в локальной сети в целях обеспечения обширной и постоянной защиты. Распределенное решение отличается относительно высокой надежностью, поэтому повреждение частей сети не влияет на функциональность всей сети. Кроме того, распределенное решение внедряется таким же образом, как и Интернет, и, таким образом, совместимо с существующей сетью и может постепенно увеличивать производительность. Тем не менее, стратегия локального планирования распределенного решения не имеет общего видения, следовательно, в такой ситуации сложно выработать одно лучшее общее решение.

Предложенная архитектура представлена на рисунке 4-3 и сама по себе является архитектурой обширной сети передачи с межрегиональным механизмом интеграции и обмена данными в режиме реального времени в рамках умной сети. Эта архитектура основана на проверенном IP, а его сервисная модель обслуживания является лучшей из возможного, простой и неизменной, подходящей для работы с распределенными алгоритмами.

4.5.2 Централизованное решение

Централизованное решение, по общему мнению, осуществляет управление неоднородными сетями, состоящими из сетей с широким покрытием, единообразно. Для удовлетворения таких потребностей, как задержка передачи, пропускная способность, надежность и т.д., централизованное решение оставляет за собой коммуникационные ресурсы и осуществляет единое планирование в рамках различных неоднородных сетей, что позволяет выполнить общие требования конечной производительности. Централизованное решение является лучшим практическим вариантом при необходимости оптимизировать общесистемное планирование с лучшей производительностью передачи. Тем не менее, сложность - это его слабое место, поэтому его можно устанавливать только в определенных частных сетях в конкретных районах.

Сеть передачи данных в режиме реального времени с широким охватом территории основана на восприятии и координации по следующей схеме. Централизованное планирование в неоднородных сетях осуществляется при помощи многоуровневого снятия информации о состоянии рабочей сети в соответствии с требованиями о передаче задач в режиме реального времени. Решение осуществляет общее управление сетью, что представляет собой сложную задачу и требует максимальной согласованности.

4.6 Систематическое представление и обработка

Семантическая технология является одним из важнейших исследовательских направлений в области информационных технологий за последние годы, в основном по причине больших ожиданий и требований по совместному использованию и обмену знаниями по сети. Семантическое исследование информации WSN становится горячей темой, особенно с развитием WSN и уходом от традиционной концепции интернета до устройств, собирающих информацию на разных уровнях. Семантическое исследование WSN фокусируется на семантическом представлении физического мира, воспринимаемого узлами датчиками. Вкратце семантика WSN относится к значению или смыслу информации, воспринимаемой узлами датчиков [44], с которой базовые данные могут быть использованы лучшим образом.

Семантическое исследование WSN возникло в семантической сети. Существующий веб-контент отдает приоритет неструктурированному и полу-структурированному тексту. Несмотря на то, что семантическая сеть может предоставлять информацию в Интернете в соответ-

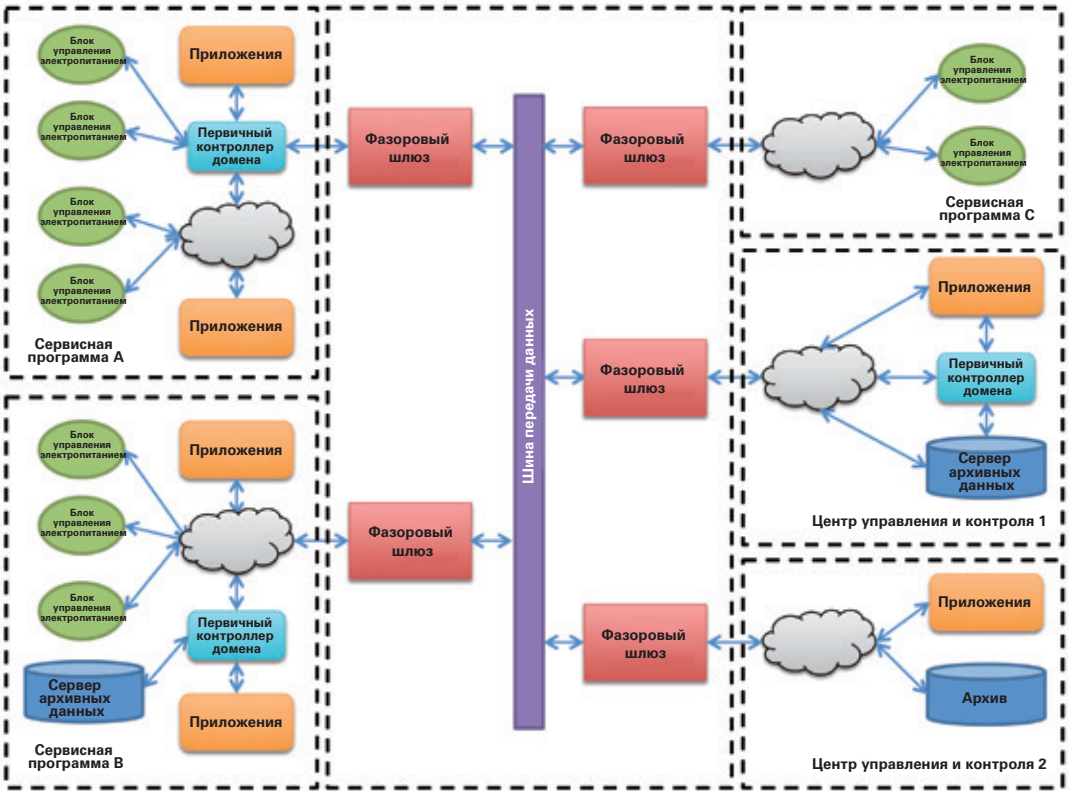


Рисунок 4-3 | Архитектура сети передачи данных с широким покрытием [43]

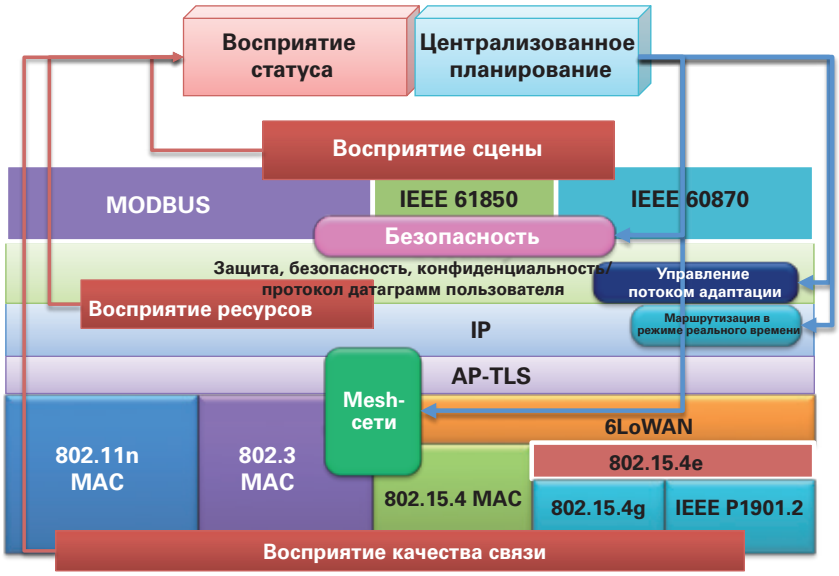


Рисунок 4-4 | Архитектура централизованной сети с передачей данных в режиме реального времени с широким охватом территории [14]

ствии с правильно определенным значением, она направлена на обеспечение лучшего взаимодействия между компьютерами и людьми. Тем не менее, среда WSN представляет собой узел датчика, информационное наполнение которого полностью отличается от информационного наполнения сети. Поэтому, чтобы поместить семантическую информацию узлов WSN в WSN-приложение, научно-исследовательские институты и организации по стандартизации внесли соответствующие решения в поле.

Для решения проблем сенсорной семантики были выделены три ключевые темы исследований:

1) технология семантического представления для терминальных устройств - непосредственно добавляет семантические теги к данным датчиков на уровнях терминальных устройств с целью получения семантического представления;

2) семантическая платформа на базе запросов обрабатывает запрос датчиков по данным при помощи семантической интерпретации данных датчиков и,

3) семантический анализ и управление информацией датчиков на базе технологии облачных вычислений. Ожидается, что это позволит оказывать поддержку крупным узлам датчиков, семантическому выражению и обработке на основе облачных вычислительных платформ.

4.7 WSN повышенной безопасности

В настоящее время WSN тесно связывают инфраструктуру организаций и предприятий с информационной сетью. Ущерб, наносимый инфраструктуре (такой как система энергоснабжения, транспортная система, химическое предприятие и национальная безопасность) вирусными угрозами может привести к невообразимым последствиям. Сети WSN, как правило, являются более подверженными различным угрозам безопасности, поскольку неуправляемая среда передачи более подвержена атакам на систему безопасности, чем сети управляемой среды передачи. С самого начала необходимо учитывать проблемы TSP (защиты, безопасности и конфиденциальности). Угрозы, которым подвергается WSN, могут быть частично нивелированы при помощи технологий сетевой безопасности. Уровень защиты от сложных атак, таких как Sybil, Dos и аномальные узлы, является неудовлетворительным [45].

Задачей TSP в отношении WSN-сетей является защита информации и ресурсов от атак и неправомерных действий. Следовательно, критерии для реализации этой цели весьма обширны и охватывают следующие области: доступность, авторизация, аутентификация, анонимность, конфиденциальность, актуальность, целостность, защита узлов, отказоустойчивость, конфиденциальность и т.д. В будущем масштаб WSN может стать более значительным, а взаимопроникновение WSN с интернетом станет более тесным. Несмотря на значительные исследовательские усилия в сфере безопасности узлов, шифрования, управления ключами, безопасной маршрутизации, безопасного группирования данных, необходимо предпринимать более серьезные меры для обеспечения безопасности WSN в будущем.

4.7.1 Структура протокола безопасности

Принимая во внимание вычислительную способность, потребление энергии и пропускную способность канала связи с узлами датчиков, защиту конфиденциальности и управление идентификацией, необходимо провести исследования в области структуры безопасности протокола, которая будет подходящей и общей моделью для каждого уровня WSN. Поскольку единое решение в области безопасности одного уровня не может быть наиболее эффективным решением, целостный подход к обеспечению безопасности будет включать все уровни общей безопасности в сети [46]. Его цели направлены на повышение эффективности WSN в контексте безопасности, долговечности и возможностей подключения. Основной принцип заключается в том, что затраты на обеспечение безопасности не должны превышать определенный уровень риска для безопасности в определенное время.

В настоящее время имеется множество методов обеспечения специальной безопасности

уровней в WSN, таких как безопасное пробуждение узлов, защита от постороннего воздействия, аутентификация и шифрование для сетевых уровней, регистрация для уровней приложений.

Тем не менее, порядок структурирования протокола других уровней и создания общей инфраструктуры протокола безопасности является серьезной проблемой для исследований в будущем.

В будущем будет создана общая модель, которая может объединить все механизмы уровни безопасности вместе. Другие механизмы позволят защитить WSN от атак, даже если на одном каком-то уровне защита будет преодолена. Тем не менее, экономическая эффективность и энергоэффективность могут по-прежнему являться большими проблемами для решения в рамках исследований в ближайшие годы.

4.7.2 Защита, безопасность и конфиденциальность

Обеспечение конфиденциальности, прав человека на неприкосновенность частной жизни, безопасность данных и целостность обходится весьма дорого. Вопрос заключается в следующем: каков коэффициент затрат и выгод при рассмотрении преимуществ, предоставляемых решением? Хочет ли человек утратить свои права для получения выгоды?

Компании Google и Apple смогли получить больше свободы при работе с личными данными в обмен на выгоды, которые перевешивают риски - по крайней мере, для многих потребителей.

Инфраструктура персональных ключей и полномочия сертифицирующей компании в рамках неограниченного количества источников данных будут облагать налогом систему, и многие игроки будут стремиться свести к минимуму активные меры безопасности и противодействовать исключительно фактически имеющим

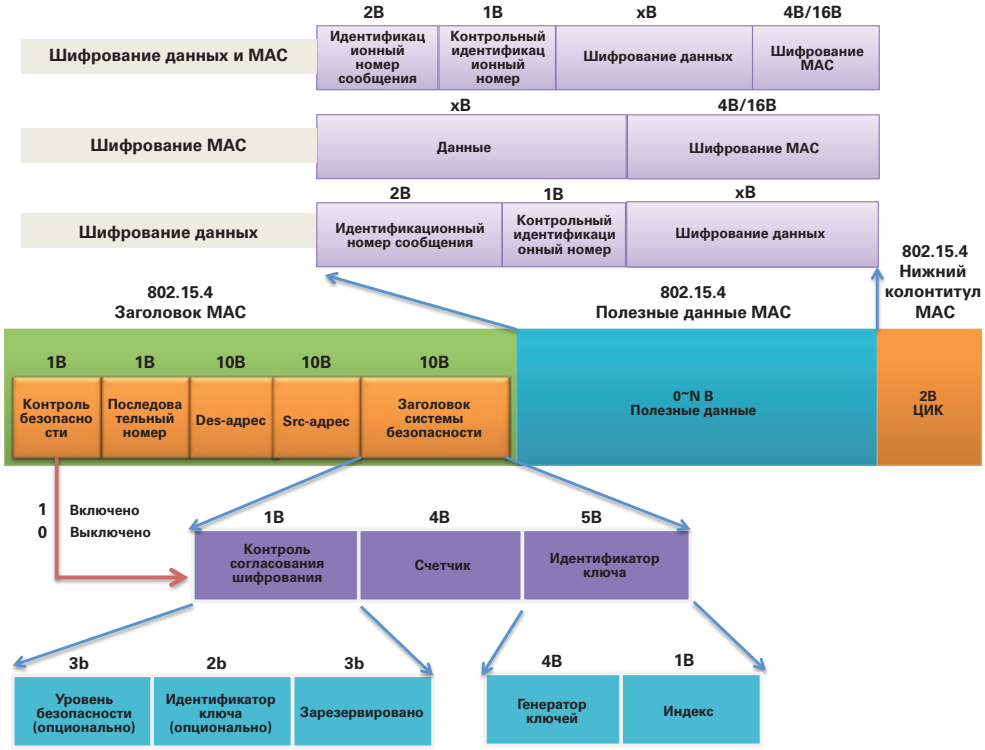


Рисунок 4-5 | Канальный уровень структуры протокола безопасности [14]

место кибератакам - таким образом, подвергая риску всю систему. Сети IoT, отправляющие вредоносные пакеты данных всем подключенным системам, являются худшим кошмаром любого голливудского фильма жанра научной фантастики. Следовательно, важно, чтобы максимальное количество систем функционировали независимо друг от друга во избежание поражения всех остальных вследствие уязвимости одной системы. Такой потенциальный эффект домино является наихудшим сценарием, поскольку плохая целостность данных может привести к ошибкам, величина которых не была предусмотрена какой-либо одной системой. Эффективность активных систем безопасности будет зависеть от понимания того, что такое «нормальный» киберфизический поток данных, однако, это может быть чрезмерно дорогостоящим мероприятием, снизив выгоды или увеличив затраты на обязательные решения IoT.

В целях безопасности структуры WSN имеют четыре качества. Во-первых, безопасность WSN уязвима для сетевых атак из-за широковещательной природы среды передачи данных и ограниченности вычислительных ресурсов узлов датчиков, таких как маленькая мощность и маленькая пропускная способность. Во-вторых, управление идентификацией и защитой является более сложным и комплексным по своей сути по причине глубокой интеграции информационного пространства с физическим миром и повсеместного доступа к информационным технологиям. Таким образом, управление идентификацией и системы защиты сталкиваются с большими проблемами. В-третьих, динамические, неоднородные и массовые характеристики модели восприятия и вычисления WSN также являются серьезными проблемами для эффективной защиты целостности системы, целостности данных, конфиденциальности данных, конфиденциальности пользователей, таких как идентификация, поведение и окружающая среда. Наконец, поскольку WSN имеет большое количество терминалов, различные типы терминалов и динамические адаптивные сетевые структуры, размер и сложность данных среды являются серьезными проблемами для существующей системы контроля безопасности.

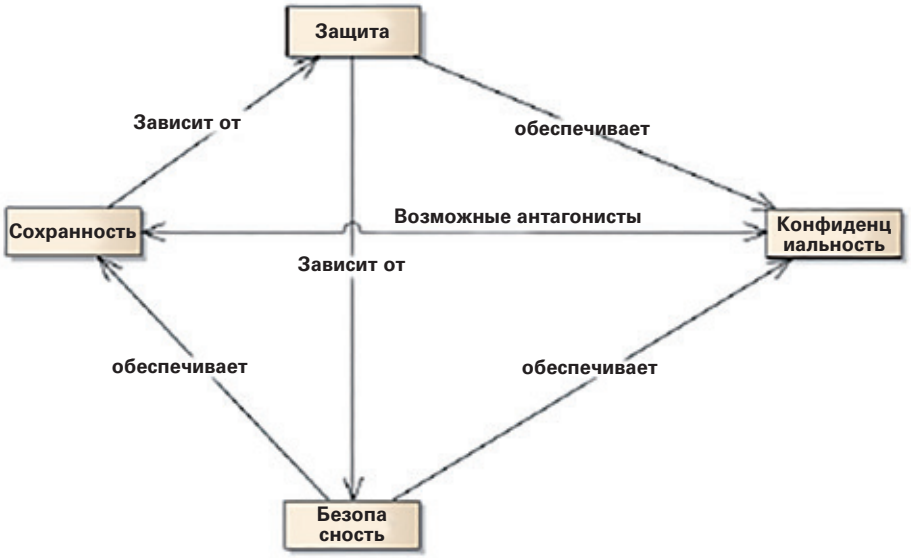


Рисунок 4-6 | Защите безопасности и конфиденциальности [14]

Раздел 5

Использование WSN в инфраструктурных системах

5.1 Использование WSN в умных электросетях

Электрическая сеть является неотъемлемой частью электроэнергетики, а также залогом устойчивости и безопасности любого государства. По мере постепенного увеличения зависимости от электроэнергии во всем мире также увеличивается потребность в обеспечении надежности и качества энергосистемы. Коммунальные предприятия, научно-исследовательские институты и ученые проводят исследования возможностей модернизации энергосистемы с целью обеспечения ее эффективности, экологической безопасности, надежности и интерактивности.

Умная электрическая сеть является источником для возникновения новых возможностей с далеко идущими последствиями. Следовательно, она обеспечивает безопасное внедрение в систему электроснабжения возобновляемых источников энергии (ВИЭ), электрических транспортных средств и распределенных генераторов; позволяет осуществлять более эффективное и надежное снабжение электроэнергией на базе имеющегося спроса и предложения; предоставляет системы комплексного контроля и мониторинга; использование автоматической настройки сети для предотвращения отключений или восстановления электроснабжения (возможности самовосстановления); предоставляет потребителям возможность иметь более эффективный контроль потребления электроэнергии и принимать активное участие на рынке электроэнергии.

Датчики являются краеугольным камнем, позволяющим извлечь из умной электрической сети максимум ее потенциала. Сеть идеи «умной» электросети заключается в том, что такая сеть будет реагировать на спрос в режиме реального времени; для этого потребуются датчики, которые будут предоставлять такую информацию «в режиме реального времени». Сети WSN в качестве «умной вводной периферийной информации» могут быть важным средством продвижения технологии умных электросетей. Технология WSN в умной электросети также будет способствовать дальнейшему промышленному развитию WSN.

5.1.1 Система онлайн-мониторинга линий электропередач

На состояние линий электропередач непосредственно влияют ветер, дождь, снег, туман, лед, молния и другие природные силы; в то же время промышленное и сельскохозяйственное загрязнение также является прямой угрозой безопасной эксплуатации линий электропередач. Рабочая среда и рабочее состояние линий электропередач являются весьма сложными системами. Поэтому возникает необходимость автоматического контроля, большего количества средств управления и защиты для автоматической подачи аварийных сигналов при возникновении аварийных ситуаций, а также требуется корректировка стратегии работы диспетчеров в соответствии с режимом работы с тем, чтобы неисправности обрабатывались на раннем этапе или были изолированными в зародыше.

Традиционные проводные средства связи не соответствуют коммуникационным потребностям онлайн-мониторинга линий электропередачи. Сети WSN обладают отличительной способностью адаптироваться к суровым условиям, большим охватом территорий, самоорганизацией, самостоятельной конфигурацией, большой долей независимости при практическом использовании и идеально подходят для систем мониторинга передачи данных линий электропередачи.

Обладая техническими преимуществами WSN в рамках полного диапазона, система онлайн-мониторинга нескольких элементов может своевременно отправлять предупреждения о стихийных бедствиях, быстро находить места неисправностей, получать данные о сбоях в линиях электропередач, сократить время восстановления после поломки, следовательно, повысить надежность электроснабжения. Использование WSN позволит не только эффективно предотвращать и снизить количество поломок оборудования электроснабжения при их сочетании с системами мониторинга температуры проводника, состояния окружающей среды и погоды в режиме реального времени. Сети WSN также могут предоставлять данные для поддержки эффективного электроснабжения, увеличивая и улучшая динамическую емкость линий электропередачи.

Общая архитектура системы онлайн-мониторинга линий электропередачи показана на рисунке 5-1.

В настоящее время некоторые провинциальные энергетические компании государственной сетевой корпорации Китая (SGCC) продвигают использование технологии WSN в рамках онлайн-мониторинга линий электропередач. Например, с 2013 года энергетические компании Liaoning и Ningxia разрабатывают демонстрационные проекты на базе WSN для онлайн-мониторинга линий электропередач.

5.1.2 Интеллектуальный мониторинг и система раннего предупреждения для подстанций

После десятилетий развития технология автоматизации внутренних подстанций достигла уровня международных стандартов.

Большинство новых подстанций, независимо от разности уровней напряжения, внедряют интегрированные системы автоматизации. Предполагается, что с 2005 года введено в

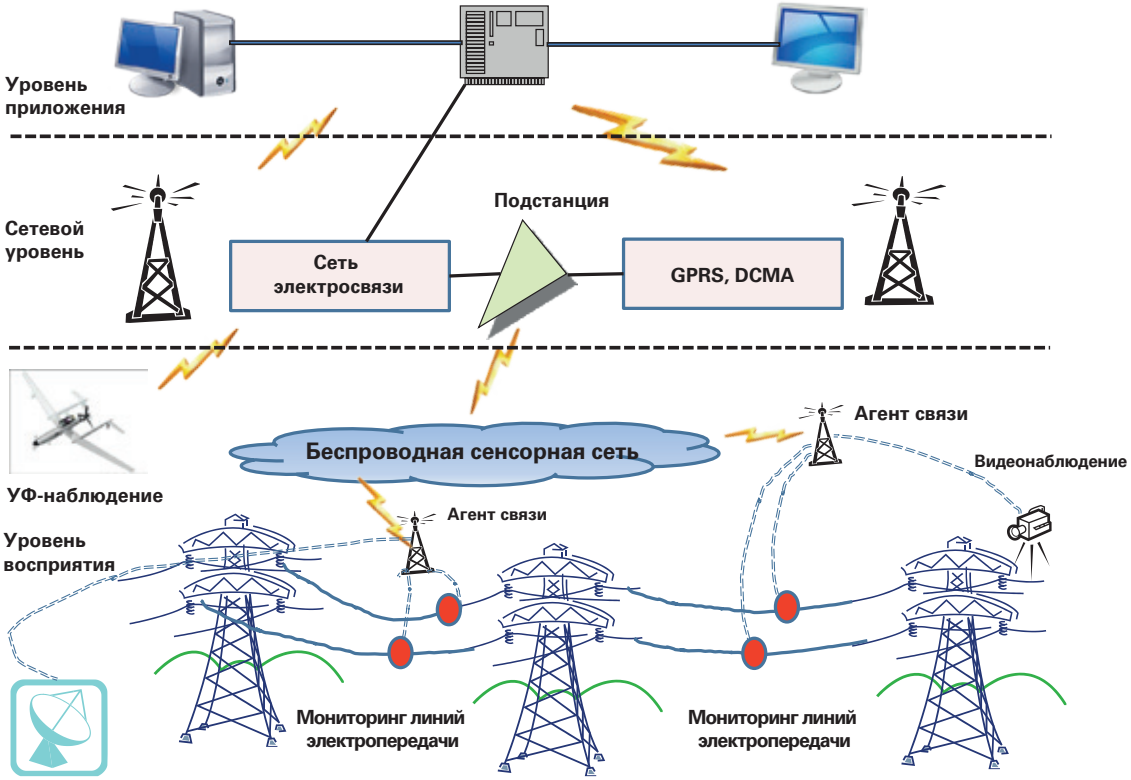


Рисунок 5-1 | Общая архитектура системы онлайн-мониторинга линий электропередач на базе WSN [47]

эксплуатацию более 200 цифровых подстанций с разной степенью автоматизации, степенями напряжения и режимами..

Отличительными чертами цифровых подстанций от обычных подстанций является оцифровка сетевой информации, стандартизация информации подстанции и передача данных по сети. Для подстанций в умных сетях больше внимания уделяется умному оборудованию электроснабжения, обмену информацией, функциональной совместимости и функциям интеллектуального использования внутренней станции. В настоящее время внедрено множество умных контролирующих систем, которые могут улучшить управление умной подстанцией. Сюда относятся мониторинг трансформатора / выключателя / температуры, контроль утечки тока в молниеотводе, оборудование для контроля утечки электричества, контроль утечки SF6 для комбинированного электрооборудования, экологический контроль мониторинг вторичного оборудования, антикражевое оборудование и т. д.

Прикладные решения WSN могут предоставить надежную, точную, оперативную, безопасную и достаточную информацию для управления подстанцией. Такая информация не связана с обычными данными о телеметрии электроснабжения, удаленной связью, дистанционным управлением, дистанционным регулированием. Такие решения также предоставляют информацию об оборудовании, например, состояние системы охлаждения, время срабатывания выключателя, состояние источников энергии механизма передачи, величину тока размыкания и информацию об окружающей среде, данные видеонаблюдения и т.д. В конечном итоге решения осуществляют оцифровку информационного описания, объединение собранных данных, передачу данных по сети, интеллектуальную обработку данных, визуализацию отображаемых данных и принятие производственных решений.

Например, SGCC объединила усилия с Институтом автоматизации Шэньяна (SIA) Китайской академии наук для создания системы государ-

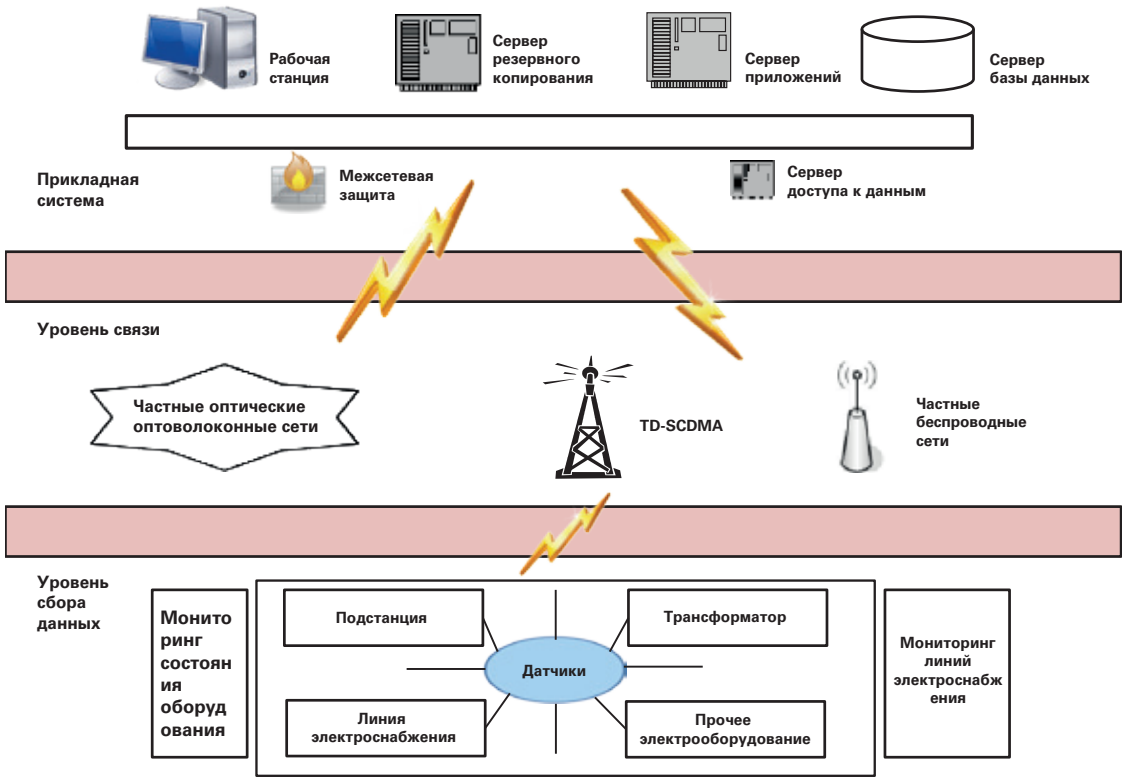


Рисунок 5-2 | Архитектура системы мониторинга рабочего состояния оборудования [47]

ственного технического обслуживания на базе технологий WSN. В провинции Ляонин и в южном округе Паньцзинь, Китай, умные подстанции с рабочим напряжением 220 кВ успешно использовались для создания вспомогательных систем управления. После введения двух систем в эксплуатацию, энергосистема работала стабильно, передача данных проходила хорошо. Связь была установлена на должном уровне, и была создана и принята для практического внедрения хорошая демонстрационная модель.

Следует отметить, что сервисные решения на базе WSN должны быть согласованы с международными мероприятиями по стандартизации, осуществляемыми в рамках умного измерения (например, серии международных стандартов МЭК 62056 (DLMS / COSEM), управляемых группой пользователей DLMS).

5.1.3 Оналйн-мониторинг и система раннего предупреждения распределительных сетей

Распределительные сети напрямую объединяют энергосистему и потребителей электроэнергии. Надежность и качество распределительной сети являются критически важными качествами надежного электроснабжения. Распределительная сеть состоит из основного оборудования, такого как фидеры, распределительные трансформаторы, автоматические выключатели, переключатели и вторичного оборудования, такого как релейная защита, автоматические устройства, измерители и счетчики, оборудование связи и управления и т.д.

Распределительные сети отличаются большим количеством точек подключения, большим территориальным покрытием и линиями электропередач на большие расстояния. Использование WSN в распределительных сетях позволит улучшить систему управления, сэкономить трудовые ресурсы, повысить надежность источника питания и ускорить восстановление работоспособности сети после поломок.

SGCC поддержала пилотный проект применения IoT в Нинся Иньчуань, Хэнань Хеби, Китай, и подтвердила, что использование технологии WSN в распределительных сетях может обеспечить защиту и поддержку строительства распределительных сетей в следующих аспектах:

1) При установке комплексного измерительного оборудования можно отслеживать изменения качества электроэнергии и перепады и пиковые нагрузки в потреблении электроэнергии, кроме того, улучшается точность и своевременность напряжения, тока, гармонических волн и других показателей.
2) При комплексном использовании RFID, систем навигации, видеонаблюдения, умных носимых технологий улучшаются возможности мониторинга в режиме реального времени состояния распределительного оборудования и параметров окружающей среды. Это позволит улучшить возможности по определению местоположения повреждений распределительных линий.
3) Контроль состояния распределительной линии, сети подземных распределительных трубопроводов позволит достичь более высокого уровня автоматического управления эксплуатацией и антикражевыми средствами.

5.1.4 Услуги умного потребления электроэнергии

Основанием услуг умного потребления электроэнергии является надежная энергосистема и концепция современного управления на базе передовых технологий измерения, высокоэффективного контроля, высокоскоростной связи и быстрого накопления энергии для осуществления взаимодействия в режиме реального времени между сетями электроснабжения, снабжением конкретных потребителей, информационного потока и коммерческого потока.

Сети WSN могут объединять терминальное оборудование поставщика с датчиками потребителей для создания полноценной интерактивной сети для получения информации о потреблении электроэнергии, а также сбора информации о параметрах электроэнергии в сложной среде. Анализ интегрированной информации на базе WSN может служить пользо-

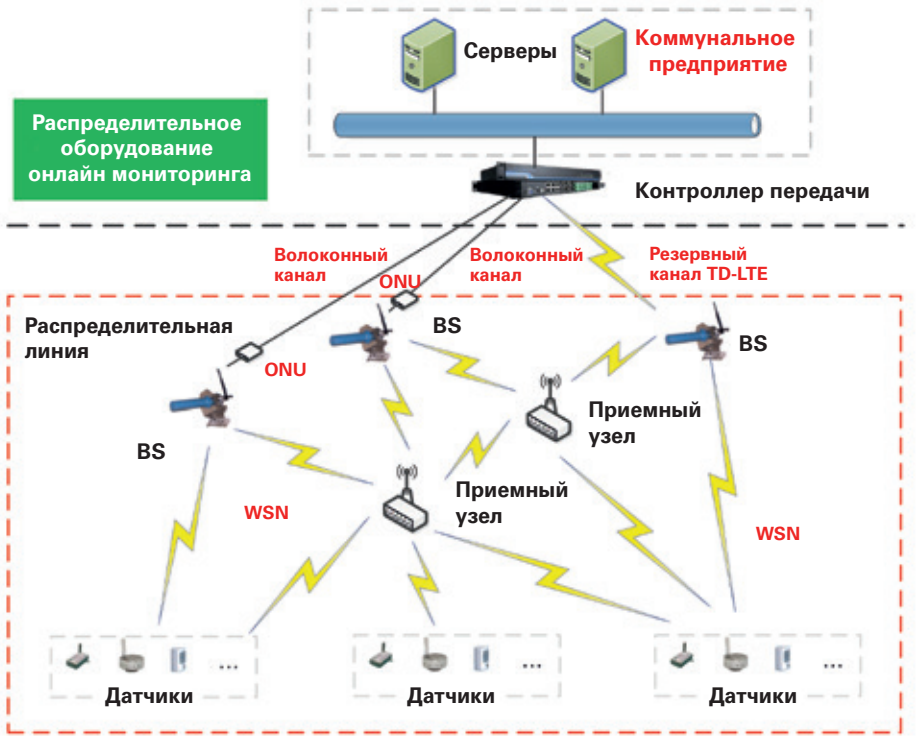


Рисунок 5-3 | Технология WSN, используемая в приложениях мониторинга распределительной сети [47]

вателю в качестве руководства или напрямую корректировать схему потребления электроэнергии, позволит обеспечить наилучшую структуру энергоресурсов, снизить стоимость электроснабжения, повысить надежность и эффективность. Сети WSN имеют большие перспективы применения в сферах умного потребления электроэнергии, таких как умные общины, умные промышленные парки и т.д.

Система сбора данных об электроэнергии является основой для умных услуг по потреблению электроэнергии. Система может осуществлять сбор нескольких видов данных массовых потребителей. Сюда относятся данные для специальных трансформаторов, средних и малых пользователей специальных трансформаторов, трехфазных коммерческих пользователей, однофазных промышленных и коммерческих пользователей, а также данные населения и распределительных трансформаторов для проверки точек измерения. Эти данные можно объединять для построения интегрированных информационных платформ. Архитектура системы сбора данных о потреблении электроэнергии на базе WSN представлена на рисунке 5-4. В настоящее время некоторые провинциальные энергетические компании SGCC начали использовать автоматическую систему считывания данных счетчиков на базе технологии WSN. Например, компания Liaoning Province Electric Power Limited внедрила систему сбора данных о потреблении электроэнергии на основе WSN в более чем 20 000 домашних хозяйств. Система связи основана на стандарте промышленной беспроводной сети - WIA и показала хорошие результаты во время проведения эксплуатационных испытаний. Головная станция имеет точные часы, поэтому часы концентратора линий связи могут быть синхронизированы по восходящей линии связи.

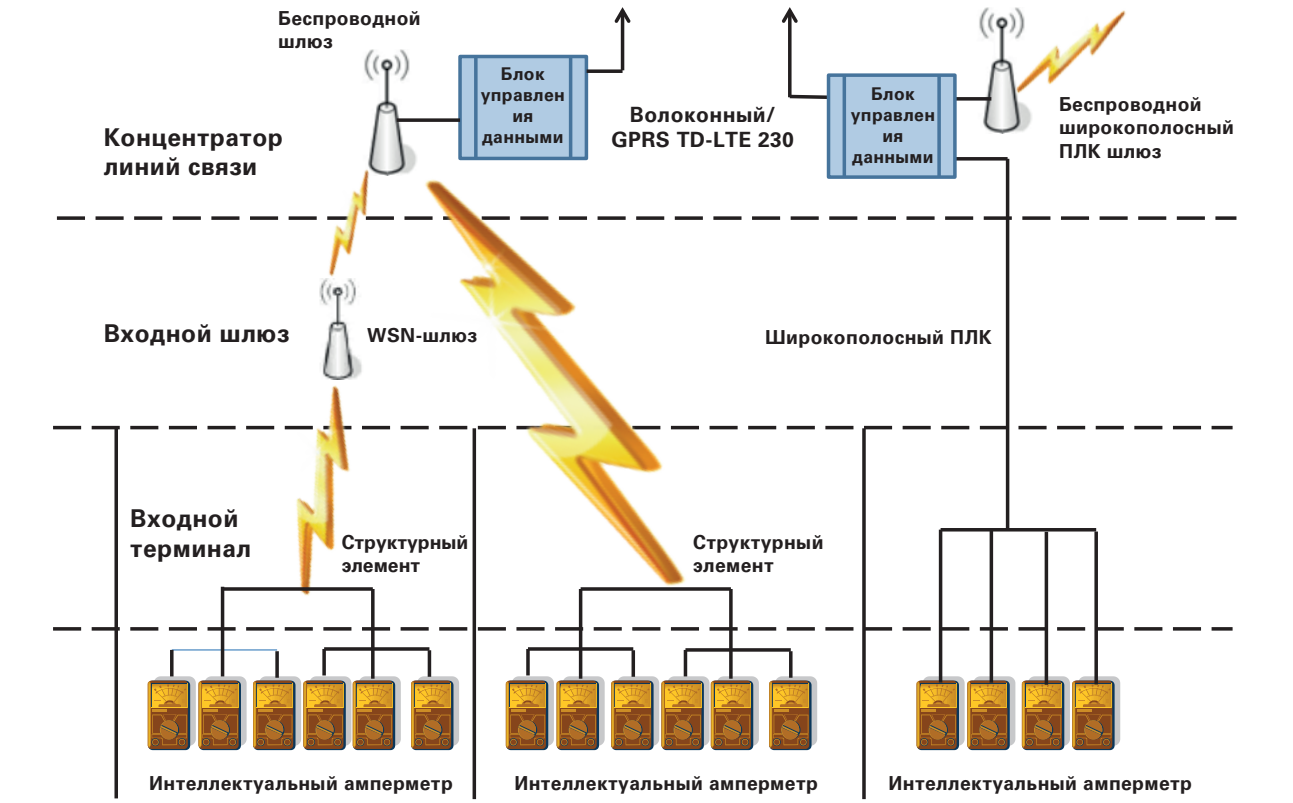


Рисунок 5-4 | Архитектура системы сбора данных о потреблении электроэнергии на базе WSN [47]

5.2 Использование WSN в системах умного водоснабжения

На сегодняшний день потребление воды в мире составляет 300% объема потребления в 1950 году. Быстрые темпы роста населения мира в сочетании с быстрыми темпами роста того, что называют средним классом, обуславливают повышенный спрос на ограниченные ресурсы планеты. В этом контексте ярким примером основного ресурса является наличие питьевой воды. Помимо традиционного государственного регулирования и политики эксплуатации природных ресурсов многие корпорации осознают оказываемое отрицательное воздействие на окружающую среду. Они также осознают социальные и коммерческие преимущества принятия мер по сведению к минимуму отрицательного влияния их деятельности на природные ресурсы. Фиксация такого отрицательного влияния осуществляется путем мониторинга окружающей среды в рамки системы комплексной оценки. Пример такой системы показан на рисунке 5-6, где мониторинг деятельности на степень загрязнение воды является одним из показателей.

5.2.1 Рациональное использование ресурсов (фокус на водных ресурсах)

Внедрение таких «зеленых» мероприятий обуславливается нормативно-правовыми требованиями, а также их влиянием на стоимость акций. Общепринятым в современном обществе является насущная необходимость в более эффективном управлении отрицательным воздействием, которое корпорации оказывают на ограниченные ресурсы, при этом количество выбросов CO2 становится все более важным определяющим показателем суммы платежей за загрязнение окружающей среды по сравне-

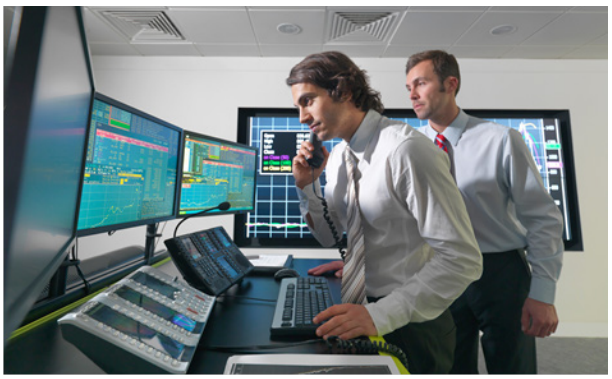


Рисунок 5-5 | мониторинг водоснабжения

нию с полученной прибылью. Таким образом, очевидной является тенденция по инвестированию корпорациями в эту область наряду с правительствами, создающими регламенты и требующими соблюдения новых экологических правил и оплаты новых издержек вхождения на национальный рынок.

В контексте чистой воды необходимо создать систему мониторинга для определения качества базисной линии, а также контроля различных потенциальных источников загрязнений чистой воды. Традиционные рабочие системы и технологии, как правило, не создаются для мониторинга потенциальных загрязнителей, поэтому новые датчики и приводные устройства должны также использоваться для мониторинга веществ, загрязняющих воздух, которые, как правило, являются загрязнителями, которые наиболее сложно контролировать и ликвидировать. Собранная информация может использоваться не только как таблица ключевых показателей эффективности (KPI), но и использоваться для прогнозирования качества воды, основанного на мониторинге соответствующих событий в режиме реального времени, таких как события, вызванные антропогенным воздействием (загрязнение) или природными явлениями (погода). Это может быть полезно для корпораций, которые ведут свою деятельность исключительно в рамках международных нормативных документов и могут стать основанием создания дополнительных ценностей в форме сертификатов выбросов / загрязнений.

Это изменение мировоззрения означает, что корпорациям необходимо перейти от менталитета традиционной рабочей эффективности к устойчивости в качестве конкурентного преимущества на рынке «экологической сознательности». Это означает, оценку и придание наибольшей ценности продуктам и услугам, которые оказывают наименьшее отрицательное влияние на окружающую среду.

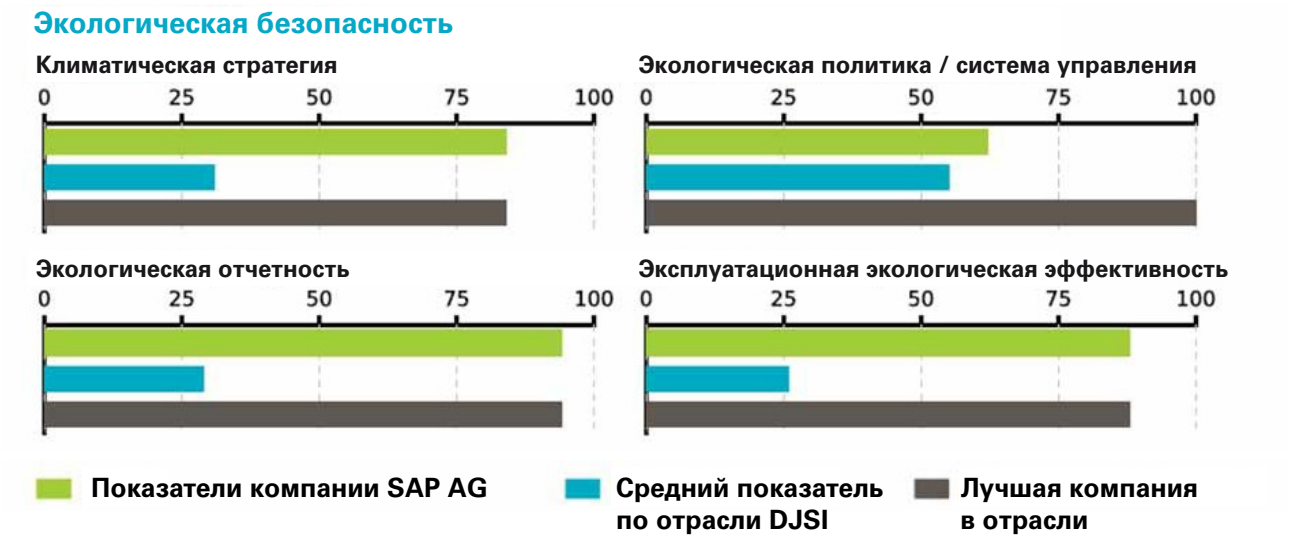


Рисунок 5-6 | Example of score card [49]

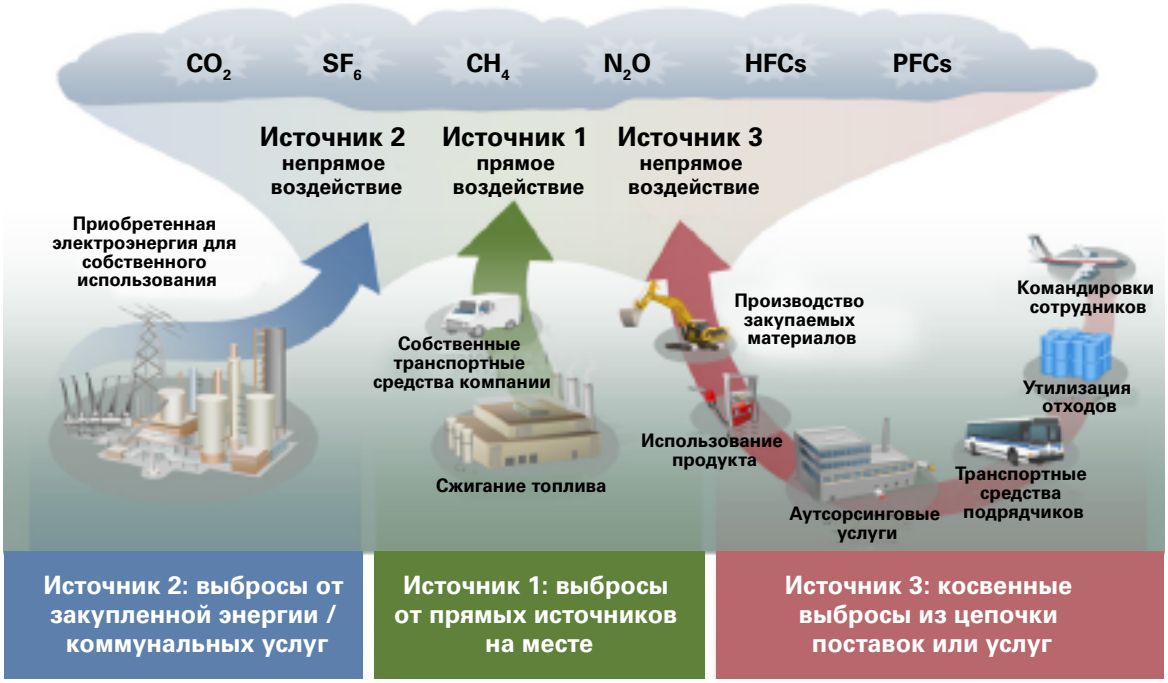


Рисунок 5-7 | Загрязнители воздуха, парниковые газы и угрозы водным ресурсам [48]

5.3 Использование WSN в умных транспортных системах

Снятие данных в беспроводных сетях умных транспортных систем несколько отличается от традиционных концепций и требований к архитектуре WSN. В большинстве случаев работа датчиков основывается на какой-либо инфраструктуре электроснабжения. Например, энергоэффективность, как правило, имеет второстепенное значение в этих системах.

Приложения WSN в умных транспортных системах можно разделить на две категории:

1) Стационарные сенсорные сети на борту транспортного средства или в виде составляющей части транспортной инфраструктуры.
2) Динамические сенсорные сети, в рамках которых отдельные транспортные средства или другие мобильные устройства выполняют функции датчиков.

Последняя категория охватывает приложения, связанные с отслеживанием и оптимизацией потока товаров, транспортных средств и людей, тогда как первая категория включает в основном приложения, которые раньше были покрыты проводными датчиками.

5.3.1 Учет транспортных потоков

Умные решения управления транспортным потоком основаны на точном измерении и надежном прогнозировании транспортных потоков в пределах города. Сюда относится не только оценка плотности автомобилей на данной улице или количество пассажиров внутри конкретного автобуса или поезда, но также и анализ отправных точек и мест назначения транспортных средств и пассажиров.

Мониторинг транспортного движения на улице или перекрестке может осуществляться при помощи традиционных проводных датчиков, таких как камеры, индуктивные петлевые датчики и т.д. Хотя беспроводные технологии могут быть полезными для снижения затрат на развертывание системы таких датчиков, это не

оказывает непосредственное влияние на точность или полезность результатов измерений.

Тем не менее, расширение понятия «датчик» и использование беспроводной технологии во многих автомобилях и смартфонах, позволит транспортным средствам и пассажирам, использующим общественный транспорт, стать «датчиками» для точного измерения транспортных потоков в пределах города.

Методы сбора данных о транспортных потоках, получаемых от транспортных средств, в совокупности называются данными о перемещении транспорта (FCD). Сюда относятся методы, использующие данные относительно небольшого количества транспортных средств, передающих данные о своем местоположении на центральный сервер (например, такси или автобусы отправляют свое местоположение, полученное по GPS), а также методы на базе информации о местоположении мобильных телефонов, полученных из баз данных местоположения в режиме реального времени операторов сотовой сети. Последняя категория подходов фактически не предполагает какого-либо снятия данных самим транспортным средством, тем не менее, использует беспроводную сеть (то есть существующую сотовую сеть) для снятия данных или, скорее, определения текущих характеристик транспортных потоков. Технические проблемы связаны, главным образом, с обработкой потенциально больших объемов данных, различием между полезными и лишними данными и экстраполяцией фактических данных о транспортных потоках на основании наблюдения исключительно подмножества всех транспортных средств.

Расширения понятия FCD, связанного с информацией, полученной от бортовой электроники транспортных средств, получили названия расширенных данных о перемещении транспорта (XFCD). Сбор и оценка данных датчиков температуры, датчиков дождя, антиблокировочной тормозной системы, электронной системы безопасности и системы регулирования тяги колес даже относительно небольшого количества автомобилей могут использоваться для получения информации в режиме реального времени о дорожных условиях. Такие данные могут быть доступны для общественности и / или использованы для улучшения прогнозирования транспортных потоков на основании ожидаемого поведения водителей в ответ на дорожные условия.

Вопросы конфиденциальности должны учитываться при получении данных о местоположении или данных датчиков частных транспортных средств. Тем не менее, это является типичным требующим решения вопросом, который связан с мониторингом дорожного движения, более того, системы, которые не используют беспроводную технологию (например, осуществляющие распознавание номерных знаков), также должны соблюдать требования конфиденциальности в отношении владельцев автомобилей.

Поведение пассажиров общественного транспорта может быть проанализировано при помощи беспроводных технологий аналогично анализу движения транспортных средств на основании FCD.

Например, электронные билеты, которые, как правило, используют технологию RFID для регистрации доступа к станции метро, автобусу или трамваю, фактически превращают пассажира в элемент сети датчиков.

Возможности сбора информации о движении и поведении пассажиров могут быть значительно увеличены, если смартфоны используются для хранения электронных билетов. Полезными для сбора информации о комбинированном

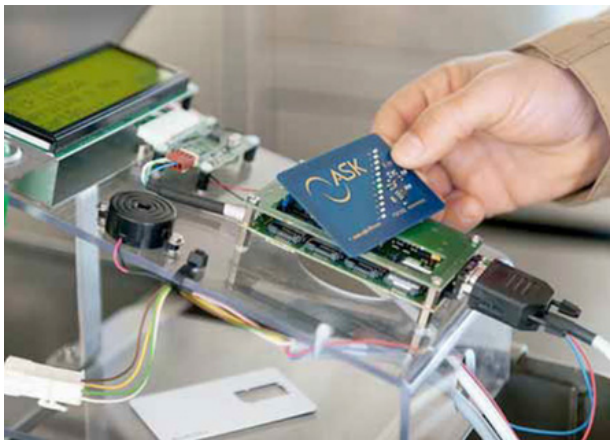


Рисунок 5-9 | Электронные билеты для умных поездок [50]

использовании пассажирами различных видов транспорта могут оказаться приложения об электронных билетах для смартфонов, содержащие возможности, которые обычные электронные билеты не могут предоставить. Однако еще предстоит выяснить, в какой степени пользователи будут готовы делиться данными о местоположении в обмен на удобство использования своего мобильного телефона в качестве билета на автобус или метро.

5.3.2 городская логистика

Урбанизация создает много проблем, особенно в быстро развивающихся странах, где большие города продолжают разрастаться, а увеличение благосостояния населения влечет за собой постоянное увеличение потока товаров в центр города и из него.

На транспортные средства, осуществляющие поставку продукции, припадает значительная доля загрязнения воздуха в городах, а упорядочение потока товаров между городом и его окрестностями является ключом к решению многих транспортных проблем и улучшению качества воздуха.

Многообещающим методом сокращения транспортной нагрузки, вызванной грузовиками, является внедрение городских оптовых складов (UCC), то есть складов недалеко от городской черты, где все товары, предназначенные для городских операторов розничной торговли, группируются, а затем отправляются получателям на базе оптимизированной маршрутизации. В данном случае будут максимально использоваться возможности грузовых автомобилей, уменьшится общее количество необходимых транспортных средств, а также общее расстояние, пройденное для доставки всех товаров в пункты назначения.

Для достижения такой оптимизации необходим тщательный анализ и планирование транспортных потоков в городе, а также мониторинг фактического потока товаров. В данной ситуации проблемы и решения аналогичны изложенным в пункте 5.3.1, однако, имеют большую детализацию. Вместо простого отслеживания подмножества движения транспортных средств по городу, требуется отслеживание движения товаров, как минимум, на уровне грузовых поддонов. Таким образом, грузовой поддон (или другой упаковочный блок) становится «датчиком» для измерения потока товаров. Сочетание нескольких беспроводных технологий (GPS, RFID, WLAN, сотовой связи) совместно со сложными методами анализа данных применяются для получения требуемых данных для оптимизации планирования и маршрутов поставок, а также обеспечения своевременного прибытия и минимизации воздействия транспорта на окружающую среду.

5.3.3 Бортовые WSN

Для обеспечения безопасной и бесперебойной эксплуатации любых транспортных средств используется все большее количество датчиков. Сюда относятся датчики, которые, в своей основе, предоставляют информацию водителю, а также датчики, которые являются частью тяговой системы или обеспечивают движение транспортного средства. По причине критической важности этих подсистем беспроводная технология, как правило, не является приемлемым решением для данного оборудования.

Тем не менее, особенно в больших транспортных средствах, таких как автобусы, поезда и самолеты, многие датчики и приводные механизмы используются в целях, не связанных с безопасностью, например, контроль температуры салона, сбор данных, используемых для профилактического обслуживания транспортного средства или мониторинга состояния перевозимых грузов.

На железной дороге WSN могут играть важную роль в процессе ремонта старых вагонов с использованием современных электрических систем.

В авиации важным является снижение массы за счет экономии медных или алюминиевых кабелей за счет беспроводных датчиков для некритически важных функций. Возможности использования беспроводных датчиков, использующих методы аккумулирования энергии, также обсуждались для контроля механического напряжения композитных материалов, входящих в состав конструкции самолета. Проводка датчиков в таких «умных материа-

лах» увеличивала бы вес конструкции и, следовательно, значительно снижала преимущества композитного материала по сравнению с обычными металлическими конструкциями.

5.3.4 WSN в элементах дорожной инфраструктуры

Управление светофорами на перекрестках, как правило, осуществляется расположенными близко к перекрестку оборудованием, которое получает данные от ряда датчиков (например, индуктивных петлевых датчиков), а также команды центрального блока управления. Такое оборудование переключает сигналы светофора (также называемые сигнальными головками) в соответствии с правила дорожного движения и ситуацией на дороге.

С увеличением количества и сложности датчиков и отображаемых элементов задача регулировщика сводится к выполнению функций связного, а не к простому переключению подключенных компонентов. Светофоры могут быть оснащены индикаторами таймера обратного отсчета, знаки переменных сообщений отображают обновляемые пределы скорости, а оптические или радиолокационные датчики предоставляют информацию о заполнении отдельных полос движения или скорости движения транспортных средств, проезжающих перекресток.

Модернизация инфраструктуры существующего перекрестка с использованием современных технологий требует также обеспечения необходимых линий связи между датчиками, сигнальными головками, знаками переменных сообщений, контроллерами дорожного движения и другими компонентами. Беспроводные технологии могут помочь снизить затраты, устраняя необходимость прокладки коммуникационных кабелей (например, Ethernet) ко всем устройствам на перекрестке. Такая установка в большинстве случаев не будет чистой сетью датчиков, так как она, как правило, также включает устройства отображения или приводные механизмы. Кроме того, сочетание проводных и беспроводных линий связи, а также сочетание различных стандартов проводной / беспроводной связи в рамках одной и той же системы по причине установки компонентов от разных поставщиков представляется практически неосуществимым.

Взаимодействие транспортной инфраструктуры с транспортными средствами посредством беспроводной связи (например, предоставление приоритета автобусам или транспортным средствам экстренной помощи на перекрестках) является еще одним перспективным направлением использования беспроводных технологий в транспортной инфраструктуре. Несмотря на то, что не все практические решения де-факто связаны с обменом данными датчиков по каналам беспроводной связи, в некоторых ситуациях транспортные средства будут предоставлять свои данные датчиков элементам инфраструктуры (например, показатель скорости движения при приближении к перекрестку). Также существуют ситуации, когда элементы инфраструктуры будут предоставлять данные датчиков транспортным средствам (например, дорожная пробка на другой стороне перекрестка).

5.4 Использование WSN в умных городах

5.4.1 Проблемы энергосбережения

С учетом роста потребления и высокой стоимости энергии, а также дефицита ископаемых видов топлива все программы, разработанные государственными учреждениями и специалистами для сокращения спроса на энергию и выбросов CO_2, сводятся к энергоэффективности в качестве абсолютного приоритета.

В Европе энергопотребление зданий (жилых и третичных) составляет 40% от общего потребления энергии, а промышленность и транспорт потребляют еще по 30%.

Государственные органы относятся к этому очень серьезно. В Европе, например, в качестве практического шага в этом направлении в октябре 2012 года была принята Директива об энергоэффективности. Она предусматривает комплекс мер по реконструкции зданий; долгосрочные планы реконструкции коммерческих и жилых зданий и 3%-ный объем реконструкции центральных общественных зданий. Каждое

государство-член Европейского союза должно было внедрить эти цели в рамках национального законодательства к июню 2014 года.

5.4.2 Энергоэффективность зданий– практический пример

Компания Schneider Electric запустила совместную программу «ДОМА» во Франции в 2008 году [51]. Эта программа предусматривала комплекс мероприятий по оснащению зданий соответствующими решениями для достижения лучшей энергетической эффективности в течение четырех лет. Программа «ДОМА» позволила изучать, совершенствовать и тестировать простые, эффективные, экономически устойчивые решения по эффективному использованию энергии, внедряя систему активного контроля с возможностью оптимизации потребления энергии при помощи автоматизированных систем контроля и мониторинга.

Одним из достижений этой программы стало понимание того, что энергетическая система состоит из трех (квази) независимых подсистем, каждая из которых предотвращает бесполезное энергопотребление:

1) Подсистема распределения (мир машин): производство энергии, трансформация; хранение.
2) Подсистема использования (мир людей): услуги по энергоснабжению жильцов.
3) Конструктивная подсистема (мир материалов): передача энергии между помещениями и внешней средой.

Эта программа представила новое видение энергетических характеристик здания, построенного на решениях, которые охватывают качество внешней конструкции, производительность оборудования и активный контроль. Эти элементы представляют собой три практических направления, которые дополняют друг друга и не имеют практического порядка применения.

5.4.3 Активный контроль в зданиях

На основании описанного выше подхода программа «ДОМА» представила протокол активного контроля на базе трех шагов для максимального увеличения производительности здания, одновременно обеспечивая его

Рисунок 5-10 | Системный подход по обеспечению энергоэффективности зданий

совместимость с умной системой электроснабжения.

1) Выполнение комплекса мероприятий в каждой комнате по очереди: для достижения максимальной энергетической эффективности здания необходимо оптимизировать услуги, оказываемые жильцу на уровне комнаты или отдельного участка третичного здания. Контроль отдельных участков позволяет жильцу адаптировать окружающую среду к своей деятельности и необходимому уровню комфорта.
2) Оптимизация энергоснабжения: для удовлетворения потребностей жильцов необходимо оптимизировать энергоснабжение на основе экономических издержек и затрат на углеводороды. Затем управление энергоснабжением и распределением энергии осуществляется на основании суммы потребностей каждого участка. Это позволяет контролировать источники энергии и отношения с экосистемой более высокого уровня, т.е. района, города и т.д. Эта стратегия облегчает прогнозирование развития умных сетей. Она позволяет создать систему, в рамках которой каждый уровень способствует оптимизации на более высоком уровне. Он также позволяет раскрыть потенциал управления спросом на электроэнергию в зданиях. Следовательно, необходимо перейти от независимого вертикального управления к управлению несколькими решениями по зонам.
3) Привлечение заинтересованных сторон: для повышения энергоэффективности здания необходимо разработать поэтапный план действий с целью тщательного поиска и анализа возможных источников экономии. Тем не менее, перечень потребностей у заинтересованных сторон является разным. Следовательно, необходимо внедрить ряд информационных стратегий, учитывающих специфические потребности каждого заинтересованного лица и определить их сферы ответственности за принятие энергоэффективных решений.

Пространственная и временная фрагментация здания и его технических систем оказывают сильное влияние на эффективность мониторинга и экономии энергии за счет активного контроля. Таким образом, реализация стратегий активного контроля меняет архитектуру команд управления и сбора данных решений активного контроля на основании экосистемы управления зонами, как показано на рисунках 5-11 и 5-12, где датчик комфорта выполняет функцию одного из ключевых элементов.

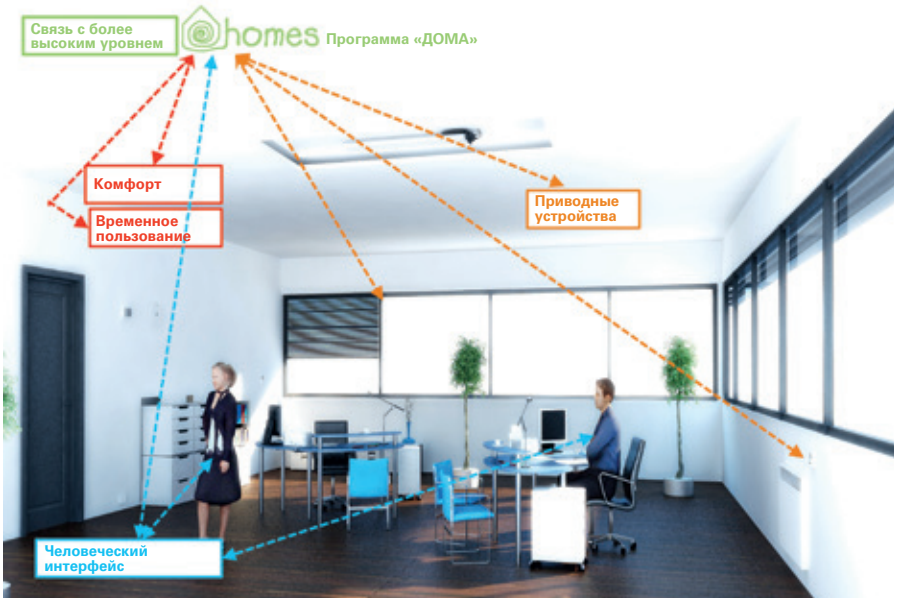


Рисунок 5-11 | Зональный контроль [50]

Рисунок 5-12 | Охват временной фрагментации в контексте экономии [50]

Рисунок 5-13 | Примеры экономии денежных средств [50]

Кроме того, была проведена оценка на пяти экспериментальных площадках, представляющих различные климатические зоны, сектора, возраст конструкции зданий, количество тепловой энергии, энергии горячей воды и вида владельца. Размер экономии составил от 25% для жилых зданий и до 56% для школ, что доказывает обоснованность вышеуказанных выводов, см. Рисунок 5-13.

5.4.4 WSN– ключ к улучшению энергоэффективности построенных зданий

Комплексное управление на зональном уровне возможно исключительно при условии тщательного мониторинга за окружающей средой (свет, температура, относительная влажность, CO_2), а также активности жильцов (обнаружение присутствия, аварийные сигналы). С учетом того, что всего несколько процентов новых зданий строятся каждый год, перед нами стоит масштабная задача по внедрению активного зонального контроля в миллионах

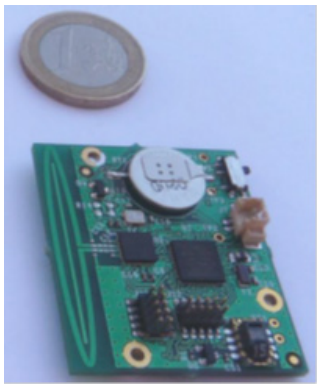


Рисунок 5-14 | Автономные электронные элементы датчика [50]

Рисунок 5-15 | Прототипы датчиков Schneider Electric [50]

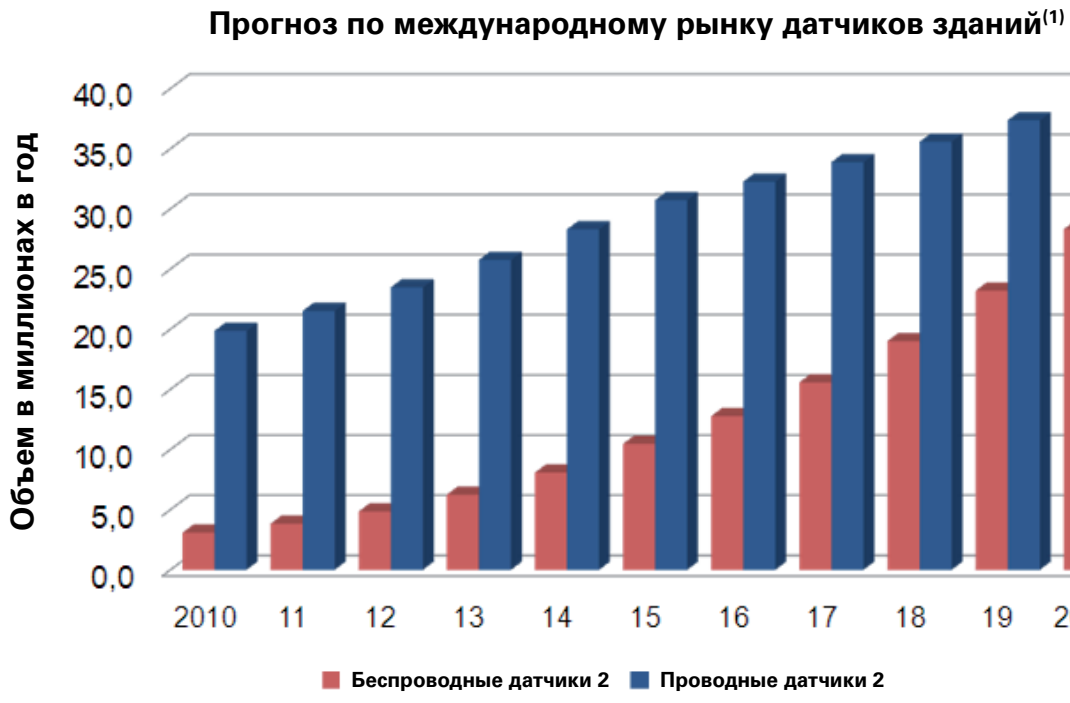


Рисунок 5-16 | Прогноз по международному рынку датчиков зданий [52]

существующих зданий. Единственным способом достижения поставленной цели является использование беспроводных датчиков или датчиков без источника питания во избежание использования сотен миллионов аккумуляторов, которые необходимо будет установить и проводить техническое обслуживание.

Практическая осуществимость внедрения автономного мультифизического беспроводного датчика была наглядно продемонстрирована. Результаты были представлены в Мюнхене на конференции по сбору и хранению энергии в июне 2011 года.

Прототип на базе фотоэлектрического (PV) элемента проводил измерения температуры, относительной влажности и интенсивности света и осуществлял передачу этих данных каждые 10 минут по радио 802.15.4 с использованием протокола ZigBee® Green Power. Средняя потребляемая мощность составляла 5 μВт, что было достаточно для функционирования датчика в течение 8 часов в сутки при менее, чем 100 люксах.

Исследование IMS Research, проведенное в октябре 2011 года [52] показало, что объем продаж датчиков на рынке строительства будет непрерывно расти, тем не менее, объем продаж беспроводных датчиков будет расти намного быстрее.

Для целей протокола обмена данных ZigBee® Alliance утвердил внедрение набора функций Green Power в стандарт ZigBee в 2012 году [53]. Он позволяет интегрировать в ZigBee® ячеистые беспроводные датчики с очень ограниченным зарядом, который, к примеру, пополняется за счет аккумулирования энергии. Такой механизм обуславливает его привлекательность в качестве решения, осуществляющего функцию контроля внутри здания.

Сеть WSN - это ключевой элемент многоцелевого контроля в зданиях на зональном уровне, позволяющий повысить энергоэффективность с учетом окружающей среды, в которой находится здание, обеспечивая комфорт и жизнедеятельность жильцов.

5.5 Дополнительные преимущества использования WSN

5.5.1 Методы повышения энергоэффективности

Согласно «Аналитическому докладу» МЭК от 2010 года «Решение энергетической проблемы – роль МЭК в период с 2010 по 2030 год»: «На сегодняшний день, из всего теоретического объема энергии в топливе две трети теряются в процессе генерации, еще 9% – в процессе передачи / распределении. Следовательно, только 30% первичной энергии потребляется в виде электричества в месте использования». Тем не менее, IoT может оказаться подспорьем в решении этой проблемы. В качестве эффективного средства получения информации он может осуществлять мониторинг в режиме реального времени в отношении преобразования энергии и своевременно проводить анализ и обрабатывать большой объем данных. Кроме того, он может также быстро реагировать на отклоняющиеся от нормы состояния и гарантировать безопасность системы, поскольку сможет обеспечить правильное управление всем процессом (от генерации до транспортировки и использования) энергосистемы на самом низко структурированном уровне и в динамическом режиме.

5.5.2 Вклад в мониторинг окружающей среды

Загрязнение окружающей среды, непредвиденные природные и экологические катастрофы и ущерб, нанесенный в результате человеческой деятельности, являются основными экологическими проблемами, которые необходимо решать в настоящее время. Раннее выявление, оповещение и проведение чрезвычайных мер являются ключевыми шагами по предотвращению крупных экологических катастроф. Интернет вещей, обладающий огромными возможностями по сбору данных и огромным охватом территории, позволит осуществлять всесторонний мониторинг в режиме реального времени окружающей среды. В данном случае технология совместной обработки данных и умного распознавания может повысить эффективность раннего предупреждения. Следова-

тельно, несложно предположить, что IoT будет играть ключевую роль в предупреждении и прогнозировании наводнений, загрязнения лесов, вод и т.д.

5.5.3 Улучшение качества социально-бытовых услуг

IoT предлагает возможности увязывания и подбора различных элементов социально-бытовых услуг через интернет: людей, оборудования и ресурсов социального обслуживания. С одной стороны, IoT позволяет поставщикам услуг получать информацию о потребностях людей и предоставлять им индивидуальные и высококачественные услуги; а с другой стороны, люди могут лучше осознать свои потребности, а также ответственность за окружающую среду вокруг них. Несложно предположить, что IoT изменит образ жизни людей во многих аспектах. Например, умная система здравоохранения на основе IoT и умные домашние системы принесут больше удобств и комфорта в жизни людей.

Раздел 6

Стандарты WSNs и системы

6.1 Общие положения

Стандартизация является важной предпосылкой для обеспечения функциональной совместимости не только между продуктами разных поставщиков, но и между различными решениями, приложениями и доменами (рабочими областями). Последние представляют особый интерес для IoT и WSN, поскольку общий доступ к устройствам, датчикам и действующим субъектам (узлам) из разных областей приложений, ведущих к новым междоменным (многопрофильным) приложениям, является основной целью IoT.

Фактор функциональной совместимости должен приниматься в расчет на разных уровнях от отдельных компонентов до коммуникационного, информационного, функционального и коммерческого уровня. На уровне компонентов в основном отражаются устройства, такие как датчики и приводные устройства, а также шлюзы и серверы, которые запускают приложения. Уровень связи отвечает за обмен данными между компонентами, в то время как информационный уровень представляет фактические данные. Функциональный уровень связан с функциональностью, которая может быть представлена программными приложениями, а также аппаратными решениями. На коммерческом уровне представлены описания бизнес взаимодействий. В рамках обеспечения WSN и IoT обмена информацией между «вещами» и приложениями, охватывающими различные области приложений, основной интерес представляют общие стандарты информационного и коммуникационного уровня. Кроме того, общие функции могут использоваться в рамках различных областей применения. На уровне компонентов находятся различные типы устройств. Тем не менее, стандарты, определяющие, к примеру, форм-факторы и разъемы для модулей (например, беспроводные модули, платы управляющего процессора (CPU)) являются актуальными.

Предпосылкой для успешной стандартизации являются отобранные сценарии использования и требования. Архитектурные стандарты необходимы для структурирования всей системы и определения соответствующих функций, информационных потоков и интерфейсов.

Поскольку WSN будет использоваться в более широком контексте IoT, необходимо также учитывать стандарты IoT и процедуру стандартизации. В частности, это касается высокоскоростного протокола обмена данными, информационного и функционального уровня.

Обратите внимание, что приведенный ниже перечень стандартов и процедур по стандартизации не является исчерпывающим.

6.2 Текущее состояние

IEEE 802.5.14 является наиболее важным стандартом связи для WSN. Он определяет физический и канальный уровень беспроводной передачи ближней связи с низким энергопотреблением, малой сложностью и низкой стоимостью. Он использует полосы частот ISM на уровне 800/900 МГц и 2,4 ГГц. IEEE 802.15.4 является основой для других стандартов, таких как ZigBee®, WirelessHart, WIA-PA и ISA.100.11a, которые определяют региональные и национальные спецификации. Этот базовый стандарт был опубликован в 2003 году, а его последующие редакции в 2006 и 2011 году. В стандарт был внесен ряд изменений для регулирования дополнительных протоколов физического уровня, региональных полос частот и конкретных областей применения. На данный момент положения стандарта охватывают дополнительные полосы частот (например, телевизионный неиспользуемый частотный спектр, региональные

диапазоны), функциональность при сверхнизком энергопотреблении и конкретные решения, такие как контроль движения поездов.

Технология Bluetooth также является беспроводным протоколом ближней связи, определенным специальной группой по интересам Bluetooth. В Bluetooth 4.0 был включен протокол низкого энергопотребления, который отличается от приложений с низким энергопотреблением.

Технология RFID используется не только в контексте WSN, но и представляет общий интерес для IoT.

Основной движущей силой стандартизации являются ISO / IEC JTC 1 / SC 31 стандартизации с их серией стандартов ISO / IEC 18000, содержащими определения различных RFID технологий. Другие организации, такие как ISO, EPCglobal и DASH7 внесли свой вклад в создание этих стандартов или их использовали.

Хотя нижние коммуникационные уровни, как правило, предназначены для определенных прикладных подходов, таких как WSN, сетевой и более высокий коммуникационный уровень должны предпочтительно использовать общие протоколы в целях обеспечения взаимодействия между сетями. Кроме того, необходимо учитывать конкретные требования определенных технологий, например, низкое энергопотребление и небольшие вычислительные возможности WSN. На сегодняшний день набор IP-протоколов де-факто является стандартом для этих уровней. Хотя ранее определенными стандартами рабочей области был определен свой собственный стек протоколов, на сегодняшний день все они переходят на IP. В случае с WSN и IoT IPv6 является предпочтительным решением. Доступным и стабильным является комплект стандартов IPv6 (сеть уровня приложений), составленный Инженерная рабочая группа Интернета (IETF) (RFC 2460 и другие). IETF работает над конкретными расширениями и протоколами для поддержки устройств и сетей с малой потребляемой мощностью, в частности, в контексте IEEE 802.15.4. Рабочая группа 6LoWPAN определяет преобразование данных IPv6 на IEEE 802.15.4 (например, RFC 6282). Рабочая группа по вопросам восстановления рассматривает возможности маршрутизации по сетям с малой мощностью и потерями данных (например, RFC 6550). Рабочая группа по протоколу ограниченного приложения (CoAP) определяет протокол приложения для устройств и сетей с ограничениями. Такой протокол является альтернативой протоколу HTTP, используемому для веб-сервисов RESTful, с учетом особых требований устройств и сетей с ограничениями.

Спецификации ZigBee® являются расширением стандарта IEEE 802.15.4, добавляя к нему сетевые уровни, уровни безопасности и инфраструктуру приложений. Они охватывают различные области применения, такие как автоматизация домов и зданий, здравоохранение, управление энергопотреблением и светом, а также услуги связи. Оригинальные спецификации Zigbee® определяют свои собственные протоколы сетевого и прикладного уровня, в то время как последние IP-спецификации Zigbee® строятся на IPv6 и CoAP.

Для фактического обмена данными между приложениями существуют различные подходы, которые часто используют сервис-ориентированную архитектуру (SOA). Примером является OPC-UA, который является стандартом МЭК, а SOAP, WSDL определены Консорциумом всемирной паутины (W3C). Стандарт XML, определенный W3C, является широко распространенным форматом кодирования. В контексте WSN следует учитывать возможности практического использования этих протоколов при задействовании ограниченных устройств и сетей. Открытый геопространственный консорциум (OGC) определил набор открытых стандартов по интеграции, функциональной совместимости и эксплуатации подключенных к сети датчиков и сенсорных систем (возможность подключения датчиков к сети).

Для управления устройствами и сетями широко используется протокол SNMP, определенный IETF. NETCONF представляет собой новый подход к управлению сетью IETF. На сегодняшний день IETF стала охватывать управление ограниченными устройствами и сетями. Другими рассматриваемыми протоколами управления устройствами для IoT являются TR-69, составленный Broadband Forum (BBF), и Управление устройствами Открытого мобильного альянса (OMA).

Семантическое представление информации является важной проблемой в WSN и IoT, позволяющей облегчить обмен знаниями и проведения автоматической конфигурации систем и приложений. В своей семантической сетевой деятельности W3C определяет базовые протоколы, такие как RDF, RDFS и OWL. В данном случае необходимо принимать в расчет специфические требования ограниченных сетей и устройств. Кроме того, свое определение получила онтология сети семантических датчиков. Для реализации запросов географически распределенной информации OGC определил GeoSPARQL.

Европейский институт телекоммуникационных стандартов (ETSI) TC SmartM2M приступил к работе над приложениями и требованиями для нескольких областей применения с целью разработки коммуникационной архитектуры M2M и соответствующих интерфейсов между устройствами, шлюзами, сетевыми узлами и приложениями с акцентом на предоставлении услуг M2M. Результаты такой деятельности были внедрены в OneM2M.

ISO / IEC JTC 1 / SWG 7 (сети датчиков) разработала услуги ISO / IEC 29182 для эталонной архитектуры сенсорных сетей и сервисов, а также интерфейсы для совместной обработки информации. На данный момент ведется работ над сенсорными сетевыми интерфейсами для общего применения и умных сетевых систем. ISO / IEC JTC 1 / SWG 7 (IoT) начали анализ требований рынка и пробелов в стандартизации IoT.

ITU собрал целевую группу M2M для изучения ландшафта стандартизации IoT и определения общих требований. Основное внимание этой группы уделяется сектору здравоохранения. Совместная координационная группа (JCA-IoT) осуществляет координацию деятельности МСЭ-Т по IoT, в том числе сетевые аспекты идентификации функциональности и общедоступные сенсорные сети (USN). Кроме того, МСЭ вносит изменения в более или менее связанные направления деятельности, например, в сети следующего поколения, включая USN, безопасность и идентификацию (присвоение имен и нумерация).

IEEE помимо 802.15.4 также осуществляет исследования умных преобразователей (серия 1451) и системы общедоступного контроля зеленого сообщества (серия 1888).

Информационные модели, обладающие, как правило, семантическим представлением или онтологией, доступны для различных областей применения, таких как «умная электросеть» согласно IEC TC 57, отраслевая автоматизация согласно IEC TC 65 и ISO TC 184, а также автоматизация зданий согласно ISO TC 205 и ISO / IEC JTC 1 / SC 25.

В контексте IoT важными также являются стандарты данных об изделии, определенные, например, стандартом IEC SC 3D, стандартами идентификации ISO и ITU и стандартами местоположениями, определенными, например, ISO / IEC JTC 1 / SC 31 и OGC.

Кроме того, для WSN и IoT очень важны стандарты безопасности и конфиденциальности.

Таблица 6-1 | Мероприятия по стандартизации WSN/IoT (не являются исчерпывающими)

Организация	Группа	Связь с WSN/IoT	Стандарты	Текущая деятельность
IEEE	802	Протокол физического и канального уровня беспроводной сети малого радиуса действия	802.15.4-2011 (в том числе поправки a, c и d), 802.15.4e-2012, 802.15.4f.2012, 802.15.4g-2012, 802.15.4k-2013, 802.15.4j-2013	Неиспользуемые телевизионные частоты, ж/д связь
IETF		Набор IP-протоколов (сеть на уровне приложений)	Например, RFC 2460 (IPv6), RFC 2616 (HTTP), RFC 768 (UDP), 1180 (TCP),RFC 5246 (TLS), RFC 4301 (IPsec)	
IETF	Ротационная	Маршрутизация для сетей С низким энерго- потреблением и потерей данных	RFC 5548, RFC 5673, RFC 5826, RFC 5867, RFC 6206, RFC 6550, RFC 6551, RFC 6552, RFC 6719, RFC 6997, RFC 6998	Многоадресная маршрутизация, Угрозы безопасности Положения о применимости Различных приложений
IETF	Основная	Протокол приложения Ограниченных устройств/сетей	RFC 6690, draft-ietf-core-coap-18 (ожидает публикации в виде RFC)	Групповая связь, HTTP- преобразование ресурсы, управление устройствами
IETF	6LoWPAN	IPv6 преобразование Ограниченных беспроводных сетей (например, IEEE 802.15.4)	RFC 4919, RFC 4944, RFC 6282, RFC 6568, RFC 6606, RFC 6775	Сжатие IPsec заголовка, DECT преобразование малой мощности

Организация	Группа	Связь с WSN/IoT	Стандарты	Текущая деятельность
Zigbee® Alliance			Спецификация 2007, IP-спецификация, Спецификация RF4CE, Автоматизация зданий, Дистанционное управление, Умное энергоснабжение, Профиль умного энергоснабжения 2, Здравоохранение, Домашняя автоматизация, Light Link, Телеком. услуги, Шлюзы	Розничные услуги
ISO/IEC JTC 1	SC 31	RFID, NFC	ISO/IEC 14443, ISO/IEC 15693, ISO/IEC 15961, ISO/IEC 15962, ISO/IEC 18000, ISO/IEC 18092, ISO/IEC 21481, ISO/IEC 24791, ISO/IEC 29160	
EPCglobal		RFID (электронный код продукта)	EPCglobal данные тега, Передача данных тегов, EPCglobal протокол высокочастотного интерфейса, Протокол воздушного интерфейса EPCglobal UHF “Gen2”, Информационные услуги EPC (EPCIS)	
ISO	TC 104	RFID (отслеживание контейнеров)	ISO18185	
DASH7		RFID	ISO/IEC 18000-7	Протокол DASH7 Alliance
W3C		Приложения связи, Web-службы	XML, SOAP, WSDL, REST	
МЭК	TC 65	Приложения связи	IEC 62541 (OPC-UA)	

Организация	Группа	Связь с WSN/IoT	Стандарты	Текущая деятельность
IETF	opsawg	Управление Устройствами и сетями	RFC 1155, RFC 1157, RFC1213, RFC3411-3418 (SNMPv3)	Управление Ограниченными устройствами
IETF	netconf	Управление Устройствами и сетями	RFC 4741-4744	Безопасность
BBF	BroadbandHome	Управление устройствами	TR-69	
OMA	DM WG	Управление устройствами	DM 1.3	Версия 2.0, Ограниченные устройства (Lightweight DM)
W3C		Семантическое представление	RDF, RDFS, RIF, OWL, SPARQL, EXI, SSN онтология	Бинарные RDF, Моделирование Памяти объектов (OMM), Обработка RDF-потока
OGC	Поддержка Сетевых датчиков DWG	Приложения связи Web-сервисы	Обзор и архитектура Высокого уровня, Приложения связи, Web-сервисы, Язык-модель датчиков, Язык-модель преобразователей, сервис Контроля датчиков, Сервис планирования датчиков, служба Оповещения о датчиках, Web Службы веб-уведомлений	
OGC	GeoSPARQL SWG	Семантическое представление	GeoSPARQL	

Организация	Группа	Связь с WSN/IoT	Стандарты	Текущая деятельность
ETSI (OneM2M)	TC SmartM2M	Связь M2M, архитектура, Сценарии использ, требования, интерфейсы	TS 102689, TS 102690, TS 102921, TS 103092, TS 103093, TS 103104, TR 101584, TR 102691, TR 102725, TR 102732, TR 102857, TR 102898, TR 102935, TR 103167	Взаимодействие, Безопасность, Умные города, Умные приборы, семантика
ISO/IEC JTC 1	SWG 7	Сенсорная сеть, архитектура, интерфейсы приложений	ISO/IEC 29182, ISO/IEC 20005	Интерфейсы Умных электросетей (ISO/IEC 30101),Общие Интерфейсы приложений (ISO/IEC 30128)
МСЭ-Т	Фокус-группа M2M	Архитектура M2M, требования, интерфейсы приложений, электронное здравоохранение		Требования, архитектура, API, протоколы, электронное здравоохранение (ЭЗ), стандартизация и анализ пробелов, Система ЭЗ M2M, Сценарии использования ЭЗ
ISA		Протокол физического и канального уровня для беспроводной сети малого радиуса действия	ISA100.11.a	
IEEE	P1451	Умные преобразователи	IEEE 1451 (ISO/IEC/ IEEE 21451)	

Организация	Группа	Связь с WSN/IoT	Стандарты	Текущая деятельность
IEEE	P1888	Контроль в рамках общины	IEEE 1888	
МСЭ-Т	SG16	Межплатформенное ПО сенсорной сети общего доступа, приложения, идентификация	F.771, F.744, H.621, H.642	Приложения IoT, теговая идентификация
МЭК	TC 57	Информационные модели, «умная электросеть»	IEC 61850, IEC 61968, IEC 61970	Отображение Web- услуг, Заменяемая интеграция, Пользовательский интерфейс, Рыночный интерфейс
МЭК	TC 65	Информационные модели, автоматизация производства	IEC 6242, IEC 62714, IEC 62794,	
ISO	TC 184	Информационные модели, автоматизация производства	ISO 13584, ISO 15926	
ISO/IEC JTC 1	SC 25	Информационные модели, Автоматизация зданий	ISO/IEC 14543	
ISO	TC 205	Информационные модели, Автоматизация зданий	ISO 16484	
МЭК	SC 3D	Данные об изделии	IEC 61360	
ISO	TC 184	Данные об изделии	ISO 13584	
ecl@ss		Данные об изделии	ecl@ss 7.0	
МЭК	TC 65	Беспроводная сенсорная сеть	IEC 62591, IEC 62601, IEC 62734	
ISO	TC 46	Идентификаторы	ISO 27729, ISO 26324, ISO 3297, ISO 2108, ISO 10957	

Организация	Группа	Связь с WSN/IoT	Стандарты	Текущая деятельность
ISO/IEC JTC 1	SC 31	Местонахождение	ISO/IEC 24730, ISO/IEC 24769	
ISO/IEC JTC 1	SC 31	Идентификаторы	ISO/IEC 15459	
МСЭ-Т	SG2	Идентификаторы	E.101, Y.2213	
МСЭ-Т	SG13	Сенсорная сеть общего доступа	Y. 2221	
МСЭ-Т	SG17	Безопасность	X.1171, X.1311, X.1312, X.1313	
OGC	SWE	Местонахождение	Услуги по определению местонахождения OpenGIS	
3GPP	SA1, SA2, SA3	Сервисы и система		Оптимизация МТС, связь МТС
3GPP	G2, R1, R2, R3	Сеть радиодоступа		Технология расширения беспроводного доступа к МТС
3GPP	CT1, CT3I, CT4	Сети передачи данных		Оценка влияния протоколов 3GPP
3GPP2	TSG-SX	Связь M2M для сетей CDMA2000		Исследование связи M2M
CCSA	TC10/WG3	Связь M2M следующего поколения		Связь M2M, сети
CCSA	TC5/WG7	типичное приложение M2M		
МСЭ-Т	JCA-NID	Система идентификации		Сетевой характер системы идентификации (в том числе RFID)

6.3 Потребности и перспективы в области стандартизации

Сети WSN и IoT не являются цельной технологией, а представляют собой сложные системы, использующие различные технологии от уровней физической связи до прикладных программ. Кроме того, они используются во многих областях и в разных средах. Последствием этих факторов является сложная среда стандартизации. Как указано выше, на сегодняшний день уже существует большой набор действующих стандартов и проводится ряд мероприятий по стандартизации. Однако, они охватывают только определенные аспекты и области применения системы в общем или основное внимание уделяют конкретным сценариям использования.

Интернет вещей и WSN являются базовыми технологиями для существующих и будущих областей стандартизации МЭК, таких как умная электросеть, промышленность 4.0 и умные города. Следовательно, важно, чтобы МЭК имела глубокое понимание их сути, среды стандартизации и специфические потребности практических областей МЭК с целью обеспечения стандартизации в нужном направлении, а также выявления и заполнения пробелов стандартизации. Это необходимо делать в тесном сотрудничестве с другими органами по стандартизации.

Начиная со сценариев использования конкретных областей применения (т.е. умной электросети, промышленности 4.0, умных городов) необходимо определить требования и структуру архитектуры, соответствующую потребностям МЭК. Это позволит определить перечень существующих стандартов, которые могут быть использованы в дальнейшем, а также ряд пробелов, которые необходимо устранить.

6.4 Проблемы и потребности в дальнейшей стандартизации

Сети WSN – это новая технология, которая охватывает различные уровни и аспекты информационных технологий. Поэтому стандартизация этого типа сетей имеет свою уникальную сложность:

- Разобщенность: связь, координация и единое планирование отсутствуют в разных организациях по стандартизации и между ними.
- Несовместимость: WSN использует различные аспекты информационных технологий, следовательно, ее стандарты имеют сложную структуру и разнообразны по своей природе. Тем не менее, разные стандарты, разработанные различными организациями по стандартизации, являются несовместимыми.
- Отсутствие гармонизации: на сегодняшний день некоторые прикладные области WSN были уже реализованы. Несмотря на то, что различные организации по стандартизации проводили работы по стандартизации с разных точек зрения и с разной глубиной, большая часть такой работы находится на начальном этапе и не готова к применению на рынке.
- Противоречивость: поскольку приложения не прошли синхронизацию, а стандарты еще не были разработаны, конструкции приложений не соответствуют разработкам в рамках стандартов, что влияет на повторное использование и взаимодействие между приложениями, препятствуя дальнейшей индустриализации.

Для решения вышеуказанных проблем необходимо, чтобы стандартизация WSN улучшала связь и координацию действий между различными организациями по стандартизации, позволяла осуществлять единое планирование, оптимизацию распределения ресурсов и сокращение повторения однотипной работы.

Раздел 7

Выводы и рекомендации

Сети WSN и IoT не являются цельной технологией, а представляют собой сложные системы, использующие различные технологии от уровней физической связи до прикладных программ. Кроме того, они используются во многих прикладных областях и в разных средах. Последствием этих факторов является сложная среда стандартизации. Как уже излагалось в настоящем аналитическом докладе, на сегодняшний день в области WSN существует множество прикладных решений, присутствует много сложностей, и ведутся работы по стандартизации. Эти факторы позволяют создать множество возможностей для промышленных предприятий, исследовательских организаций и органов по стандартизации благодаря уникальным характеристикам WSN. Указанные выше факторы обуславливают их привлекательность в современных и будущих инфраструктурных решениях.

IoT и WSN основаны на технологических областях, регулируемых МЭК, например, умная электросеть, промышленность 4.0 и умные города, следовательно, важно, чтобы МЭК имела глубокое понимание их сути, среды стандартизации и специфические потребности заинтересованных сторон МЭК в области WSN. Для проведения стандартизации в правильном направлении, выявления и заполнения пробелов в стандартах требуется тесное сотрудничество как внутри, так и вне МЭК (т.е. с другими действующими органами по стандартизации).

7.1 Общие рекомендации

7.1.1 Крупномасштабные WSN

По мере увеличения количества узлов в крупномасштабных WSN, увеличивается плотность сети, следовательно, вероятность отказа канала связи становится более высокой. МЭК рекомендует учитывать в дальнейших исследованиях другие критерии эффективности сети, например, проблемы качества обслуживания (QoS) для приложений, работающих в режиме реального времени, и мобильность узлов в некоторых специальных средах.

7.1.2 Исследования системной архитектуры и технологий интеграции, подходящих для крупного сбора данных и динамических изменений

МЭК рекомендует промышленным предприятиям и исследовательским институтам разработать для WSN системную архитектуру и технологию интеграции. Системная архитектура, основанная на протоколе SOAP в сочетании с технологией интеграции, например, OPC-UA, семантическом представлении и обработке, необходима для реализации свободного обмена информации в различных неоднородных сетевых средах.

7.1.3 Разработка общей модели для обеспечения безопасности

По мере установки все большего количества узлов на производительность, как правило, оказывает влияние внедрение дополнительных сервисов обеспечения безопасности в WSN, в частности, в рамках инфраструктуры. Поэтому МЭК рекомендует соответствующим исследовательским организациям объединить свои усилия для разработки общей модели в целях обеспечения безопасности каждого уровня, а также налаживания взаимодействия между этими уровнями.

7.1.4 Технология параллельного доступа с множеством подключений к WSN

МЭК рекомендует приложить значительные усилия для разработки и использования технологии высокоскоростного доступа в допол-

нение к современным технологиям доступа, несмотря на их относительную новизну. Технология высокоскоростного доступа может еще Выводы и рекомендации больше улучшить эффективность ограниченного беспроводного спектра и оказать поддержку более крупным сетям.

7.2 Рекомендации, адресованные МЭК и ее комитетам

7.2.1 Требуемые базовые стандарты для архитектуры WSN

MSB рекомендует SMB разработать соответствующие стандарты унифицированной архитектуры WSN. Необходимо определить требования и архитектурную структуру, начиная со сценариев использования прикладных областей, удовлетворяющих потребностям МЭК (т.е. умных электросетей, промышленности 4.0, умных городов). Исключительно по результатам проведенного анализа можно будет определить перечень существующих стандартов, которые можно использовать в дальнейшем, а также перечень пробелов, которые необходимо заполнить.

7.2.2 Технический вклад WSN в автоматизацию производства

MSB рекомендует SMB принимать активное участие в разработке WSN для автоматизации производства с требованиями к параллельному доступ с множеством подключений. IEC TC 65 ведет деятельность в этой области.

7.2.3 Быстрое развитие стандартов WSN для автоматизации производства

MSB рекомендует SMB внедрить стандарты WSN для автоматизации производства, обращая особое внимание на гармонизацию уже существующих национальных или региональных стандартов.

7.2.4 Преимущества совместной деятельности промышленных ассоциаций по вопросам WSN в целях автоматизации производства

MSB рекомендует SMB поощрять технические комитеты использовать разработки WSN на глобальном промышленном уровне. Многие промышленные ассоциации активно работают в этой области, проводят исследования и составляют аналитические записки, отражающие определенные взгляды на проблемные вопросы. При проведении стандартизации необходимо учитывать данные наработки.

7.2.5 Стандарты по сертификации систем

MSB рекомендует CAB проанализировать будущие потребности в области стандартизации для продвижения и поддержки модульной сертификации WSN. Поскольку сложные системы, как правило, имеют очень алгоритмы действий, сертификация крупномасштабных систем – это не может быть набором прямолинейных положений. Тем не менее, в ближайшем будущем может появиться модульная сертификация. Большая часть сертификации модульной системы проводится в отношении отдельных системных модулей, и только небольшая часть сертификационных требований применяется в отношении интегрированной системы. Другими словами, система «наследует» сертификацию своих модулей.

Приложение A

Технологии сетевого доступа

A.1 Тенденции развития технологий сетевого доступа

В соответствии с текущими требованиями в отношении приложений WSN развитие технологий сетевого доступа достигло значительного прогресса. Наиболее распространенной и используемой технологией представительского доступа является Bluetooth 4.0 с уклоном на использование WSN в медицинских целях, а также IEEE 802.15.4e с уклоном на использование WSN в промышленных целях, а также WLAN IEEE 802.11™ с точки зрения IoT.

A.1.1 Bluetooth 4.0

Учитывая характеристики и требования медицинских и некоторых других прикладных областей IoT, в частности, требование низкого потребления мощности, Bluetooth SIG опубликовал последнюю редакцию стандарта Bluetooth 4.0 в 2012 году.

Ориентированный на компактные устройства с высокой степенью интеграции, Bluetooth 4.0 использует технологию легкого доступа для работы в режиме ожидания с низким энергопотреблением, что обеспечивает чрезвычайно низкое энергопотребление, как в рабочем режиме, так и в режиме ожидания. Даже аккумулятор кнопочного типа может поддерживать бесперебойную работу устройства Bluetooth®4.0 в течение нескольких лет. В следующей таблице представлены параметры Bluetooth 4.0 и традиционной технологии Bluetooth.

Таблица A-1 | Сравнительная характеристика Bluetooth 4.0 с традиционной технологией Bluetooth [54]

Техническая характеристика	Традиционная технология Bluetooth	Bluetooth с низким энергопотреблением
Расстояние/диапазон	100 м (330 футов)	50 м (160 футов)
Скорость передачи данных по воздуху	1 Мбит/с - 3 Мбит/с	1 Мбит/с
Пропускная способность приложения	0.7 Мбит/с - 2.1 Мбит/с	0,27 Мбит/с
Количество активных подчиненных	7	Не определено, зависит от модели
Безопасность	56/128-бит и уровень приложения, определенный пользователем	128-битная AES со счетчиком CBC-MAC и уровень приложения, определенный пользователем
Надежность	Адаптивность к резким скачкам частоты, FEC, быстрый ACK	Пассивное подтверждение приема, 24-битный ЦИК, проверка целостности 32-битных сообщений

Задержка (при отсутствии подключения)	Обычно 100 мс	6 мс
Общее время отправки данных (определение срока службы батареи)	100 мс	3 мс, <3 мс
Голосовое управление	Да	Нет
Сетевая топология	Scatternet	Звезда-шина
Потребляемая мощность	1 в качестве эталона	от 0,01 до 0,5 (в зависимости от способа использования)
Пиковое потребление тока	<30 мА	<15 мА

A.1.2 IEEE 802.15.4e

Характеристики WSN очень похожи на низкоскоростную WPAN, следовательно, большинство WSN принимают IEEE 802.15.4 в качестве основного стандарта связи. Более того, ZigBee® [55], WirelessHART [56], ISA100.11a [57] и WIA-PA [58] созданы на базе стандарта IEEE 802.15.4. Поэтому, для достижения высокой надежности, жестких требований функционирования в режиме реального времени использования IoT в промышленности, Рабочая группа IEEE 802.15.4 предложила использовать IEEE 802.15.4e в 2012 году.

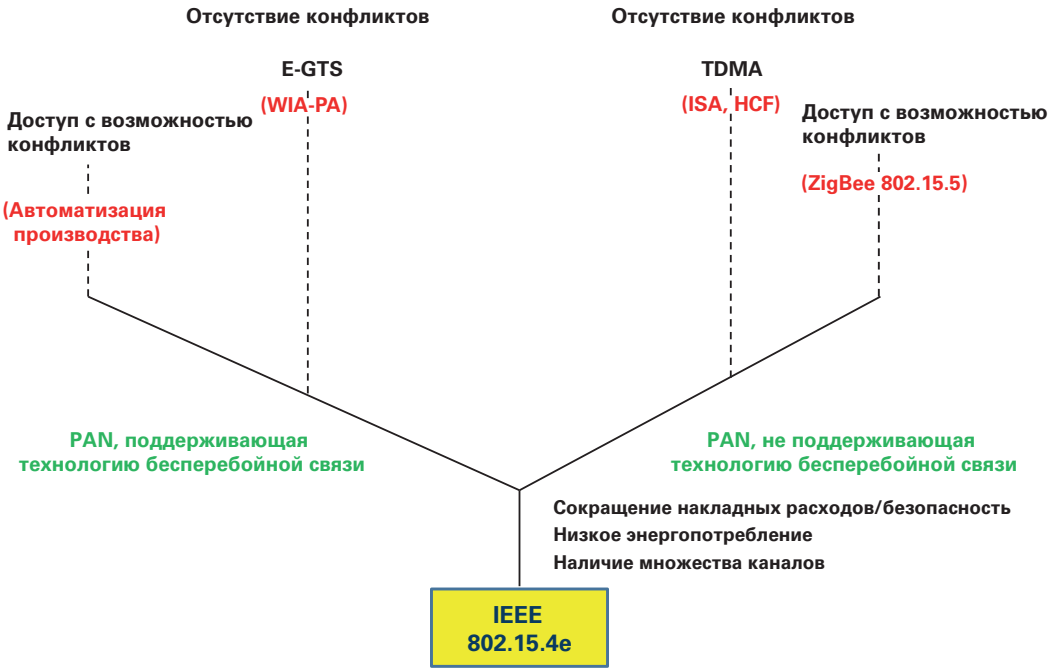


Рисунок A1-1 | Архитектура технологии сетевого доступа IEEE 802.15.4e [59]

Технология IEEE 802.15.4e в основном используется в промышленных целях и расширяет IEEE 802.15.4 при помощи четырех методов доступа, включая неконкурентный метод расширения GTS на базе Beacon (технологии бесперебойной связи). Этот метод поддерживает WIA-PA, ориентированный на автоматизацию производства, неконкурентный метод TDMA, не поддерживающий технологию бесперебойной связи, поддерживающий ориентированный на автоматизацию WirelessHART и ISA100.11a, являющейся сопоставимой технологией доступа на базе Beacon, поддерживающий приложения для автоматизации производства, и метод конкурентного доступа, не поддерживающий технологию бесперебойной связи, с поддержкой Zigbee® и IEEE 802.15.5 [60].

A.1.3 WLAN IEEE 802.11™

Основными преимуществами WLAN IEEE 802.11™ в контексте IoT являются:

- простая интеграция WLAN-клиентов и устройств с Интернетом,
- его широкое использование в качестве технологии беспроводной связи в домашних хозяйствах, офисах и промышленности,
- ее поддержка мобильными устройствами,
- низкое энергопотребление, приемлемое для промышленных целей и сенсорных сетей.

Беспроводные локальные сети, основанные на стандарте IEEE 802.11™ [17], как правило, используются для беспроводной передачи данных в офисах, на конференциях и встречах, домашних хозяйствах, а также в промышленности. Сети WLAN IEEE 802.11 обеспечивают легкую интеграцию в Интернет при помощи спецификаций с сетевым ориентированием и подобно Ethernet-сетям, а также при помощи их стабильной, коммерчески успешной и широко распространенной экологически безопасной системы.

Преобладающими сетевыми топологиями сетей IEEE 802.11™ WLAN являются WLAN-клиенты, подключенные к точкам доступа сети WLAN.

Рисунок A1-2 | Маломощный Wi-Fi модуль GainSpan GS1011M [61]

Также возможно использование и других сетевых топологий, в частности, беспроводных многосвязных сетей (IEEE 802.11s [62]). WLAN IEEE 802.11™, обеспечивающая скорость передачи данных 56 Мбит / с при использовании IEEE 802.11a / g, 150 Мбит / с и более при использовании IEEE 802.11n, и до 1 Гбит / с при использовании IEEE 802.11ac.

Кроме того, WLAN также внедряются в беспроводную связь промышленного сектора и сенсорные сети. Такие компании, как GainSpan, предлагают так называемые маломощные Wi-Fi-клиенты (см. Рис. A1-2). Низкое энергопотребление достигается при помощи энергоэффективного оборудования и последующего использования возможностей энергосбережения спецификации IEEE 802.11™. Wi-Fi Alliance планирует осуществить сертификацию этой технологии. Ожидается внесение следующих изменений к IEEE 802.11™, которые имеют отношение к IoT и WSN. Например, дополнительные уровни PHY для субдиапазона ГГц в IEEE 802.11ah и для диапазона 60 ГГц в IEEE 802.11ad / aj.

Список литературы

[1] ASHTON, K. *That 'Internet of Things' Thing. In the real world, things matter more than ideas*. RFID Journal, 22 June 2009. Available from: http://www.rfidjournal.com/articles/view?4986

[2] BRÖRING, A. et al. *New generation sensor web enablement.* Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652

[3] SENSEI. *Integrating the physical with the digital world of the network of the future.* Available from: http://www.sensei-project.eu/

[4] CHONG, C.-Y. and KUMAR, S. P. *Sensor networks: Evolution, opportunities, and challenges.* Proceedings of the IEEE 91(8), 2003, pp. 1247-1256.

[5] KUMAR, S. and SHEPHERD, D. *Sensit: Sensor information technology for the warfighter*. Proceedings of the 4th International Conference on Information Fusion (FUSION'01), 2001, pp. 3-9.

[6] COY, P. and GROSS, N. et al. *21 Ideas for the 21st Century*. Business Week Online, 1999, pp. 78-167. Available from: http://www.businessweek.com/1999/99_35/2121_content.htm

[7] NI, L.M. *China's national research project on wireless sensor networks*. Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'08), 2008, p. 19.

[8] HATLER, M., GURGANIOUS, D. and CHI, C. *Industrial wireless sensor networks. A market dynamics report*. ON World, 2012.

[9] Figure courtesy of Silicon Labs and RTC Magazine: http://rtcmagazine.com/files/images/4151/RTC1212_SilLabs_fig1_medium.jpg

[10] Yole Development SA. *MEMS technology: World's smallest barometric pressure sensor*. Micro News, 2009, 78:1.

[11] K AHN, J. M., K ATZ, R. H. and PISTER, K. S. J. *Mobile Networking for Smart Dust*. ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 99), Seattle, WA, August 17-19, 1999.

[12] ANG, R.J., TAN, Y.K. and PANDA, S.K. *Energy harvesting for autonomous wind sensor in remote area*. 33rd Annual IEEE Conference of Industrial Electronics Society (IECON'07), Taipei, Taiwan, 2007.

[13] TANG, L. and GUY C. *Radio frequency energy harvesting in wireless sensor networks*. International conference on communications and mobile computing, 2009, pp. 644648.

[14] Courtesy of Shenyang Institute of Automation, Shenyang, China, 2014.

[15] FP7 EXALTED consortium, *D3.3 – Final report on LTE-M algorithms and procedures*, project report, July 2012. Available from: http://www.ict-exalted.eu/fileadmin/documents/EXALTED_WP3_D3.3_ v1.0.pdf

[16] IEEE 802.15.4e-2012, *IEEE Standard for local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer.*

[17] IEEE Std 802.11™-2012, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,* IEEE Computer Society, March 2012.

[18] UIMER, C. *Wireless Sensor Networks*. Georgia Institute of Technology, 2000. Available from: www.craigulmer.com/portfolio/unlocked/000919_sensorsimii/wireless_sensor_networks.ppt

[19] PISTER, K. and DOHERTY, L. *TSMP: Time synchronized mesh protocol*. [C]. Proceedings of the IASTED International Symposium, Distributed Sensor Networks (DSN 2008), 2008, pp. 391398. Available from: http://robotics.eecs.berkeley.edu/~pister/publications/2008/TSMP%20DSN08.pdf

[20] SHELBY, Z. and BORMANN C. *6LoWPAN: The wireless embedded Internet*. New York, NY, USA: John Wiley & Sons Ltd, 2009. Available from: http://elektro.upi.edu/pustaka.elektro/Wireless%20Sensor%20Network/6LoWPAN.pdf

[21] Sensinode. Available from: www.sensinode.com\\EN\\products\\software.html

[22] *6LoWPAN Sub1GHz Evaluation kit.* Texas Instruments. Available from: www.ti.com/tool/CC-6IOWPAN-DK-868

[23] HUI, J., CULLER, D. and CHAKRABARTI, S. *6LoWPAN: Incorporating IEEE 802.15.4 into IP architecture*. IPSO, Industrial Ethernet Book Issue 59, 1997. Available from: http:// w w w.i e b me dia.com / inde x .php?id=7176& pa r e n t id= 6 3&t h e m e i d=25 5 & h f t= 5 9 & s ho w d e t ail= true&bb=1&PHPSESSID=a3tc6d9vhs5ab6svu8ahcb4c10

[24] BLILAT, A., BOUAYAD, A., CHAOUI, N. and EL GHAZI, *M. Wireless sensor network: Security challenges.* Network Security and Systems (JNS2), 2012 National Days of. IEEE, 2012, pp. 6872. Available from: http://novintarjome.com/wp-content/uploads/2014/05/Wireless-Sensor-Network.pdf

[25] JAIN, A., K ANT, K. and TRIPATHY, M. R. *Security solutions for wireless sensor networks*[C]. Proceedings of the 2012 Second International Conference on Advanced Computing and Communication Technologies (ACCT '12). IEEE Computer Society, 2012, pp. 430433.

[26] WANG, Y., ATTEBURY, G. and RAMAMURTHY, B. *A survey of security issues in wireless sensor networks* IEEE Communications Surveys and Tutorials 8, 2006, pp. 223.

[27] ALZAID, H. *Security map for WSN*. 2009. Available from:http://www.wsn-security.info/Security_ Map.htm

[28] MARTIN, T., HSIAO, M., HA, D. and KRISHNASWAMI, J. *Denial-of-service attacks on battery- powered mobile computers*. Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04), IEEE, 2004, pp. 309318. Available from: http://www.ece.vt.edu/ tlmartin/power-secure/percom_martin_camera-final.pdf

[29] FALK, R. and HOF, H.-J. *Fighting insomnia, a secure wake-up scheme for wireless sensor networks*. Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'09), Athens/Glyfada, Greece, 18-23 June 2009, pp. 191196.

[30] LE X. H., SANK AR, R., KHALID, M., and SUNGYOUNG, L. *Public key cryptography-based security scheme for wireless sensor networks in healthcare*. Proceedings of the 4th International Conference on Ubiquitous Information Management and Communication (ICUIMC '10). ACM, 2010.

[31] SZCZECHOWIAK, P., K ARGL, A., COLLIER, M. and SCOTT, M. *On the application of pairing based cryptography to wireless sensor networks*. Proceedings of the second ACM conference on Wireless network security. ACM, 2009: 1-12.

[32] Libelium, *Encryption libraries for waspmote sensor networks*. Available from: http://www.libelium.com/products/waspmote/encryption/

[33] KALITA, H. K. and K AR, A. *Key management in secure self-organized wireless sensor network: a new approach*. Proceedings of the International Conference and Workshop on Emerging Trends in Technology (ICWET '11). ACM, 2011, pp. 865870.

[34] FALK, R. and HOF, H.-J. *Security design for industrial sensor networks*. Information Technology, Vol. 52, No. 6, Oldenbourg, 2010, pp. 331-339.

[35] AL-K ARAKI, J. N. and K AMAL, A. E. *Routing techniques in wireless sensor networks: a survey*. Wireless communications, IEEE, Vol. 11, No. 6, 2004, pp. 628.

[36] WOOD, A. D., FANG, L. and STANKOVIC, J. A. *SIGF: a family of configurable, secure routing protocols for wireless sensor networks*. Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. ACM, 2006: 35-48.

[37] SEN, J. *A survey on wireless sensor network security*. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, 2009, pp. 5578. Available from: http:// arxiv.org/ftp/arxiv/papers/1011/1011.1529.pdf

[38] JHA, M. K. and SHARMA, T. P. *Secure data aggregation in wireless sensor network: a survey*. International Journal of Engineering Science and Technology (IJEST), Vol. 5, No. 3, 2011.

[39] SCHMITT, C. *Cooperation between all components in the established wireless sensor network*. Technische Universität München, 2009. Available from: https://corinna-schmitt.de/doku.php?id=wsn_research

[40] ROZANSKI, N. and WOODS, E. *Software systems architecture: Working with stakeholders using viewpoints and perspectives*. Addison-Wesley Professional, 2nd edition, 2011.

[41] DUNLAP, J. *From billing & technology convergence to ecosystem convergence: Why M2M matters to your business*. Pipeline: Technology for Service Providers, Vol. 8, No. 7, 2011, pp. 13. Available from: http://pipelinepub.com/1211/OSS_BSS/pdf/7230_PipelineDecember2011_ A5.pdf

[42] FELDMAN, S. *Unified information access: Creating information synergy*. IDC, 2012. Available from: http://www.infonortics.com/sdv-12-post/feldman.pdf

[43] MYRDA, P. T. and KOELLNER, K. *NASPInet-The internet for synchrophasors*. 43rd Hawaii International Conference on System Sciences (HICSS), IEEE, 2010, pp. 16.

[44] HEBELER, J. et al. *Semantic Web Programming*. John Wiley & Sons, Inc., 2009.

[45] WOOD A. D. and J.A. Stankovic. 2002. "Denial of Service in Sensor Networks." IEEE Computer, 35 (10), 54-62.

[46] PATHAN, A. S. K., LEE, H. W. and HONG, C. S. *Security in wireless sensor networks: issues and challenges*. The 8th International Conference on Advanced Communication Technology (ICACT 2006). IEEE, 2006, Vol. 2, 6 pp.-1048. Available from: http://arxiv.org/ftp/arxiv/papers/0712/0712.4169.pdf

[47] Courtesy of State Grid Corporation of China, 2014.

[48] Courtesy of SAP.

[49] *Industry group leader report,* "Sustainability Scores". RobecoSAM AG, 2013. Available from: http://www.sustainability-indices.com/images/Industry_Group_Leader_DJSI2014_Wipro-Ltd.pdf

[50] Courtesy of Schneider Electric.

[51] http://www2.schneider-electric.com/sites/corporate/en/press/press-kit/homes-project.page

[52] Courtesy of IMS Research.

[53] ZigBee 2012, *ZigBee specification overview*. Available from: http://www.zigbee.org/Specifications/ZigBee/GreenPower.aspx

[54] Bluetooth Low Energy. Wikipedia: The Free Encyclopedia. 31 July 2014 at 05:16. Available from: http://en.wikipedia.org/wiki/Bluetooth_low_energy

[55] ZigBee Alliance. http://zigbee.org/Home.aspx

[56] IEC 62591, *Industrial communication networks Wireless communication network and communication profiles WirelessHART™*.

[57] IEC/PAS 62734, *Industrial communication networks – Fieldbus specifications – Wireless systems for industrial automation: process control and related applications.*

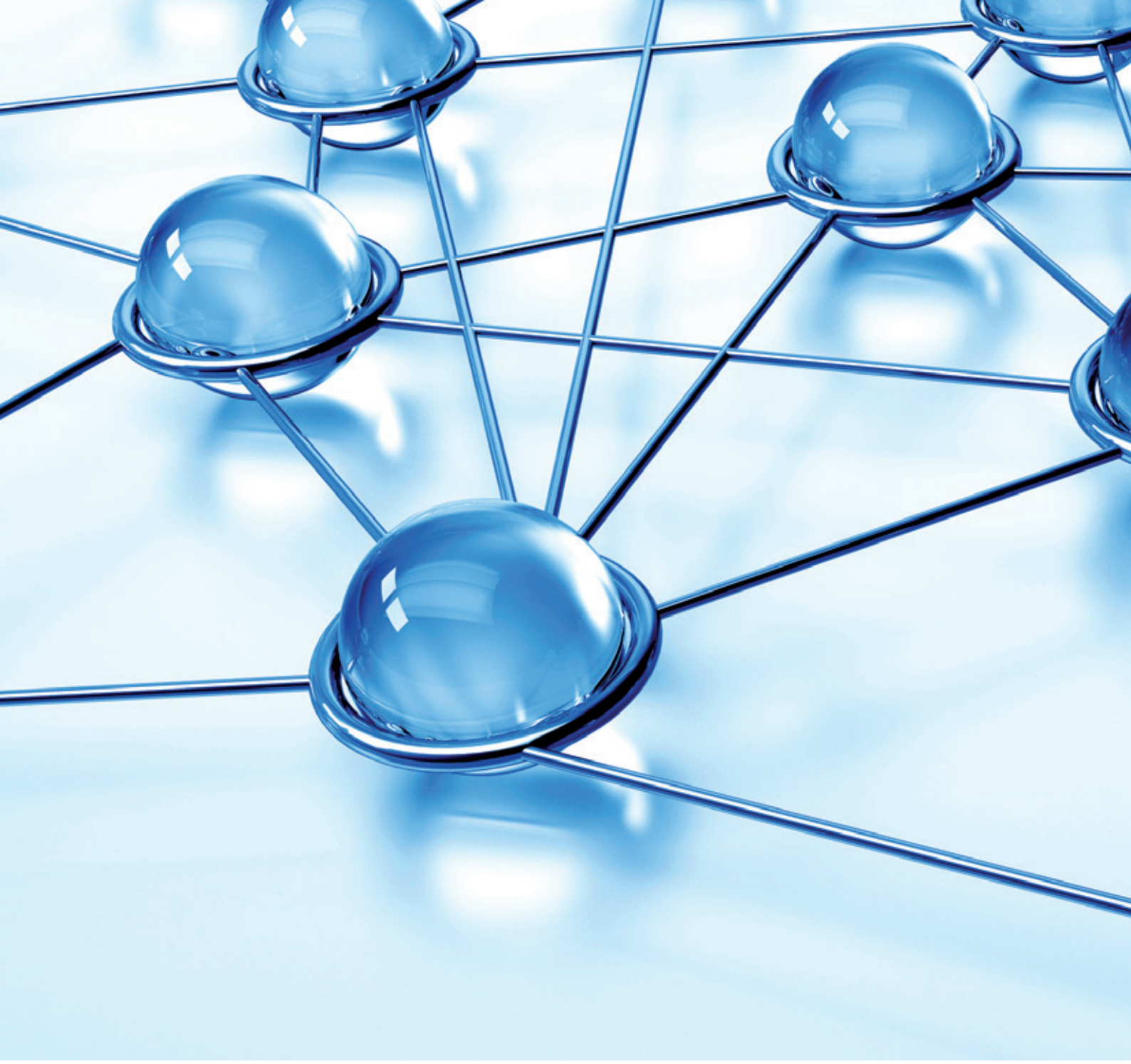
[58] IEC 62601, *Industrial communication networks – Fieldbus specifications – WIA-PA communication network and communication profile.*

[59] IEEE Std 802.15.4e-2012, *Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*. April 2012.

[60] IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs). IEEE 802.15.5 WPAN Mesh Networks. http://grouper.ieee.org/groups/802/15/pub/Meeting_Plan.html. May 2005.

[61] GainSpan, *Low Power Wi-Fi Modules and Embedded Software*, Product Photography, Available from: http://www.gainspan.com/news/media_kit

[62] IEEE Std 802.11s-2011, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 10: Mesh Networking*, IEEE Computer Society, September 2011.



ISBN 978-2-8322-5593-3

Международная электротехническая комиссия®

3 rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

T +41 22 919 02 11
info@iec.ch
www.iec.ch