А.Е.Кучерявый, А.В.Прокопьев, Е.А.Кучерявый

Самоорганизующиеся сети

УДК 681.327.39

Самоорганизующиеся сети.

Авторы: Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А.

Санкт-Петербург

ISBN 978-5-86983-318-1

Рассматриваются концепции развития сетей связи общего пользования, на основе прогнозов развития делается вывод о предстоящем принципиальном изменении их архитектуры и состава клиентской базы. В среднесрочной и долгосрочной перспективе сети связи общего пользования будут в основе своей самоорганизующимися, а клиентская база сетей будет формироваться из машин, механизмов, биомасс и т.п. Дается определение самоорганизующихся сетей, рассматриваются всепроникающие сенсорные сети, сети связи для транспортных средств, медицинские сети, молекулярные наносети. Анализируются стандарты и проекты стандартов семейства IEEE 802.15 как международной нормативной базы для создания самоорганизующихся сетей и протоколы ZigBee и 6LoWPAN.

Для специалистов в области связи, аспирантов и студентов университетов.

ISBN 978-5-86983-318-1

© Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А., 2011

Содержание

1. Современные концепции и сети связи общего пользования..... 12

1.1. Концепция сетей связи следующего поколения. 12

1.2. Сети фиксированной и мобильной связи. 13

1.3. Стандарты IEEE 802.11 и самоорганизующиеся сети. 19

1.4. Определение и примеры самоорганизующихся сетей. 25

1.5. Особенности IPTV как сетевой структуры NGN. 28

1.6. Прогноз развития беспроводных технологий до 2020 года и концепция Умных Всепроникающих Сетей. 33

2. Сенсорные сети. Кластеры и выбор головного узла. 45

2.1. Общие положения. 45

2.2. Отличия USN и MANET. 51

2.3. Кластерная организация сенсорных сетей. 55

2.4. Требования к алгоритмам маршрутизации в USN. 58

2.5. Классификация алгоритмов маршрутизации в USN. 61

2.6. Существующие алгоритмы выбора головного узла. 67

2.6.1. Алгоритм случайного выбора головного узла LEACH. 67

2.6.2. Алгоритм с предопределённым выбором головного узла HEED. 69

2.6.3. Алгоритм случайного выбора головного узла ERA 70

2.6.4. Алгоритмы PEGASIS и иерархический PEGASIS. 71

2.6.5. Алгоритм RRCH. 73

3. Централизованный алгоритм выбора головного узла для гомогенных USN 76

3.1. Диаграммы Вороного. 76

3.1.1. Выпуклая оболочка 76

3.1.2. Диаграммы Вороного 77
3.2. Диаграммы Вороного для USN. 80
3.3. Выбор головного узла в кластере. 84
3.3.1. Алгоритм выбора головного узла 85
3.4. Результаты моделирования 87
4. Алгоритм выбора головного узла для однородной USN. 91
4.1. Покрытие 91
4.2. Покрытие по периметру. 93
4.3. Алгоритм выбора головного узла в кластерной сенсорной сети. 96
4.4. Результаты моделирования 101
5. Алгоритм выбора головного узла для неоднородной USN. 107
5.1. Предположения и периметрическое покрытие. 108
5.1.1. Предположения. 108
5.1.2. Периметрическое покрытие 110
5.2. Новый алгоритм. 112
5.2.1. Алгоритм для нахождения полного периметрического покрытия 112
5.2.2. Алгоритм выбора головного узла для обеспечения покрытия 114
5.3. Результаты моделирования 117
5.3.1. Первый сценарий 119
5.3.2. Второй сценарий 122
6. Алгоритмы выбора головного узла для мобильных сенсорных сетей. 125
6.1. Мобильные сенсорные сети 125
6.2. Комбинированный критерий прогнозирования. 127

6.2.1. Критерий связности 127
6.2.2. Критерий покрытия..... 129
6.2.3. Критерий мобильности. 131
6.2.4. Критерий остаточной энергии..... 131
6.3. Предикторы. 132
6.4. Распределённый алгоритм кластеризации. 133
6.4.1. Фаза 1: информационное обновление. 134
6.4.2. Фаза 2: Формирование кластера. 136
6.5. Результаты моделирования. 137
6.5.1. Первый сценарий. 140
6.5.2. Второй сценарий. 141
7. Семейство стандартов IEEE 802.15..... 144
7.1. Стандарт IEEE 802.15.1 146
7.1.1. Общее описание. 146
7.1.2. Архитектура ядра системы..... 148
7.1.3. Система передачи данных 153
7.1.4. Объекты транспортной структуры..... 157
7.1.5. Общая структура пакета 158
7.1.6. Физические каналы. 159
7.1.7. Физические соединения..... 164
7.1.8. Логические соединения. 165
7.1.9. Каналы L2CAP. 167
7.1.10. Топология сети. 168
7.2. Стандарт IEEE 802.15.3 170
7.2.1. Общее описание 170
7.2.2. Формирование и разрушение пикосети..... 171

7.2.3. Безопасность функционирования сети. 175
7.2.4. Формат сверхцикла 802.15.3. 176
7.2.5. Обмен данными между устройствами. 178
7.2.6. Управление питанием. 180
7.2.7. Характеристики физического уровня 2.4 Ггц.....180
7.2.8. Управление уровнями. 182
7.3. Общие сведения о стандарте IEEE 802.15.6. 183
7.3.1. Спецификации физического уровня для IEEE 802.15.6...189
7.3.2. Спецификация MAC уровня в IEEE 802.15.6. 195
7.3.3. Безопасность передачи данных. 198
8. Стандарты IEEE 802.15.4 201
8.1. Общие сведения о стандарте IEEE 802.15.4. 201
8.2. Компоненты IEEE 802.15.4 WPAN. 202
8.3. Архитектура сети 203
8.4. Архитектура протоколов 204
8.5. Функциональный обзор 206
8.6. Надежность. 213
8.7. Безопасность. 215
8.8. Альтернативный физический уровень на базе UWB. 216
9. Протокол ZigBee. 220
9.1. Архитектура стека протоколов ZigBee. 223
9.2. Архитектура ZigBee сети. 224
9.3. Маршрутизация. 227
9.4. Обслуживание маршрутов. 231
9.5. Взаимодействие с сетью связи общего пользования. 231
10. Протокол 6LoWPAN. 235

10.1. Преимущества 6LoWPAN 235
10.2. Сжатие заголовков IPv6 237
10.3. Концепции «mesh-under» и «route-over». 241
10.4. Neighbor Discovery. 242
10.4.1. Назначение адреса 247
10.4.2. Взаимодействие узел-маршрутизатор. 248
10.4.3. Взаимодействие маршрутизатор-маршрутизатор 250
10.5. Защита данных в 6LoWPAN 252
10.6. Сравнение 6LoWPAN с существующими корпоративными стандартами. 254
11. Введение в наносети. 256
11.1. Классификация наносетей. 256
11.2. Молекулярные наносети 258
11.3. Синтез феромонов 262
11.4. Приложения наносетей. 268
Сокращения 270
Литература. 285

После первых минут изумления дон Мигель постарался подавить слишком интимные переживания, теоретик искусства был потрясен в нем не меньше, чем муж доньи Лусии. Он не мог отрицать: это абсолютно противное всем канонам произведение волновало, нравилось. Оно было прекрасно. Все здесь не по правилам, - сказал он наконец, - но должен признаться – это великолепно.

Лион Фейхтвангер. Гойя, или Тяжкий путь познания.

Уважаемый Читатель!

Эпиграф к книге – из мира искусства. Предмет исследования – самоорганизующиеся сети – действительно так нов и оригинален по своей сути, что его появление можно сравнить с революцией в любом профессиональном деле, в том числе и в живописи.

Концепция самоорганизующихся сетей ломает сложившиеся стереотипы и, в первую очередь, в архитектурном построении и в клиентской базе сетей связи. Самоорганизующаяся сеть не обладает некоей устойчивой архитектурой, число узлов в ней и взаимосвязи между ними случайны в каждый конкретный момент времени. С появлением самоорганизующихся сетей и человек с принадлежащими ему терминалами перестает быть центральным

звеном клиентской базы сетей связи. Механизмы и конструкции, животные и растения, тело человека вот примеры терминалов новых сетей связи. 7 триллионов беспроводных устройств на 7 миллиардов человек к 2017 – 2020 годам – прогноз ведущих экспертов в области телекоммуникаций.

Вместе с тем, самоорганизующимся сетям присущи, естественно, и некоторые стандартные характеристики сетей связи. Анализируя состав самоорганизующихся сетей, мы видим сети доступа (Ad Hoc – целевые сети) и транзитные сети (Mesh – ячеистые). Изучая потоки трафика, мы находим их самоподобные свойства. В кластерной организации самоорганизующихся сенсорных сетей центральную роль играют алгоритмы маршрутизации трафика (выбора головного узла). Есть и общепринятые параметры качества обслуживания, такие как задержки и потери, хотя зачастую они вторичны, а на первый план выходят длительность жизненного цикла сети и доля покрытия пространства.

Все это можно найти в книге. Кроме того, в книге рассмотрены и новейшие направления развития уже для самоорганизующихся сетей, такие как медицинские нательные сети и молекулярные наносети. Последние основаны на передаче информации с помощью перемещения вещества, а не на использовании электромагнитных волн.

Математический аппарат для самоорганизующихся сетей предусматривает широкое использование геометрических

построений, что, в общем-то, естественно для сетей, в которых происходит достаточно частое изменение структуры и взаимосвязей. Впрочем, в свое время геометрические построения также играли существенную роль при анализе и синтезе сетей связи. Можно вспомнить замечательную книгу моего папы Евгения Ивановича Кучерявого “Построение городских телефонных сетей”, изданную в 1972 году в соавторстве с И.М.Ждановым. Так что, все возвращается на круги своя, но в новой, иногда противоречащей классическим принципам построения сетей форме.

Книга содержит 11 глав. В первой главе анализируются концептуальные положения развития сетей связи общего пользования и обосновывается тезис о завершении этапа развития, хорошо известного как сети связи следующего поколения и переходе к концепции Умных Всепроникающих Сетей, базовой составляющей которых является Интернет вещей и входящие в его состав всепроникающие сенсорные сети.

Главы со второй по шестую посвящены всепроникающим сенсорным сетям и алгоритмам выбора головного узла кластера. Кластерная организация для всепроникающих сенсорных сетей является преобладающим способом их построения. Материалы этих глав основаны на диссертации А.Салима, выполненной в СПб ГУТ им. проф. М.А.Бонч-Бруевича под моим руководством.

В седьмой и восьмой главах достаточно подробно рассматриваются стандарты и проекты стандартов семейства IEEE 802.15, в том числе и самый новый из них – IEEE 802.15.6, в

проекте которого представлены предложения по организации медицинских нательных сетей.

Девятая и десятая главы посвящены новым протоколам, используемым для построения всепроникающих сенсорных сетей – ZigBee и 6LoWPAN. Последний непосредственно связан с внедрением протокола IPv6 и позволяет в принципе присвоить IP адреса всем сенсорным узлам.

Одиннадцатая глава открывает путь Читателю в неизведанный еще мир молекулярных наносетей, которые также являются самоорганизующимися. Основанные на перемещении вещества, в рассматриваемом в книге варианте с помощью феромонов, молекулярные наносети требуют пристального внимания и совместных усилий связистов, химиков и биологов. Раздел 11.3 написан кандидатом химических наук Т.Г.Федулиной из Санкт-Петербургской Лесотехнической Академии.

Такая получилась книга. Читайте, обсуждайте, развивайте.

Д.т.н., профессор,

почетный член НТОРЭС им.А.С.Попова

А.Е.Кучерявый

Санкт-Петербург, Август 2011г.

1. Современные концепции и сети связи общего пользования.

1.1. Концепция сетей связи следующего поколения.

Концепция сетей связи следующего поколения (NGN – Next Generation Networks) появилась в конце 20-ого – начале 21-ого века как основа для создания пакетных сетей связи общего пользования [3,5,6,28,50,167,168,169]. Концепция NGN предусматривала эволюционный переход от сетей связи с коммутацией каналов [15] к пакетным и создание пакетной сети связи общего пользования с возможностью предоставления пользователям любых услуг с неким гарантированным уровнем качества обслуживания [25,28,42,164]. Теоретической базой для создания NGN являлась конвергенция сетей связи [12,19,20,21,22,23]. В качестве технологической базы для реализации концепции NGN изначально были приняты программные коммутаторы (Softswitch) [11,25], а впоследствии и мультимедийная подсистема IMS (IP Multimedia Subsystem) [4,59,159,170,172] на базе протокола SIP (Session Initiation Protocol) [25,32,57,88,94]. Коммерческая составляющая концепции NGN включала в себя, в первую очередь, возможность предоставления новых по сравнению с передачей речи услуг пользователям с целью приумножения или хотя бы сохранения клиентской базы для традиционных операторов электросвязи. К этим услугам относились услуги по передаче данных и услуги по передаче видео [21,22,23]. Возник даже такой термин как Triple Play, включивший в себя как раз передачу речи, данных и видео. Передача данных при этом, естественно, обеспечивала доступ к Интернет, а

предоставление видео услуг основывалось на передаче телевидения поверх IP (IPTV) [165,166]. Однако, к этому времени (начало 21-ого века) множество новых провайдеров услуг также предлагали и услуги доступа в Интернет, и предоставление видео услуг. Исходя из предназначения концепции NGN для традиционных операторов электросвязи, нужен был еще один дополнительный стимул для пользователей, который делал бы предпочтительным их нахождение в клиентской базе именно этих операторов. С учетом эволюционно накопленных ресурсов традиционных операторов электросвязи этим стимулом стал гарантированный уровень качества обслуживания при реализации концепции NGN [42,163,164], в том числе и для передачи речи [8,160,161,162].

На рис.1.1 представлены основные сетевые структуры, входящие в концепцию NGN.

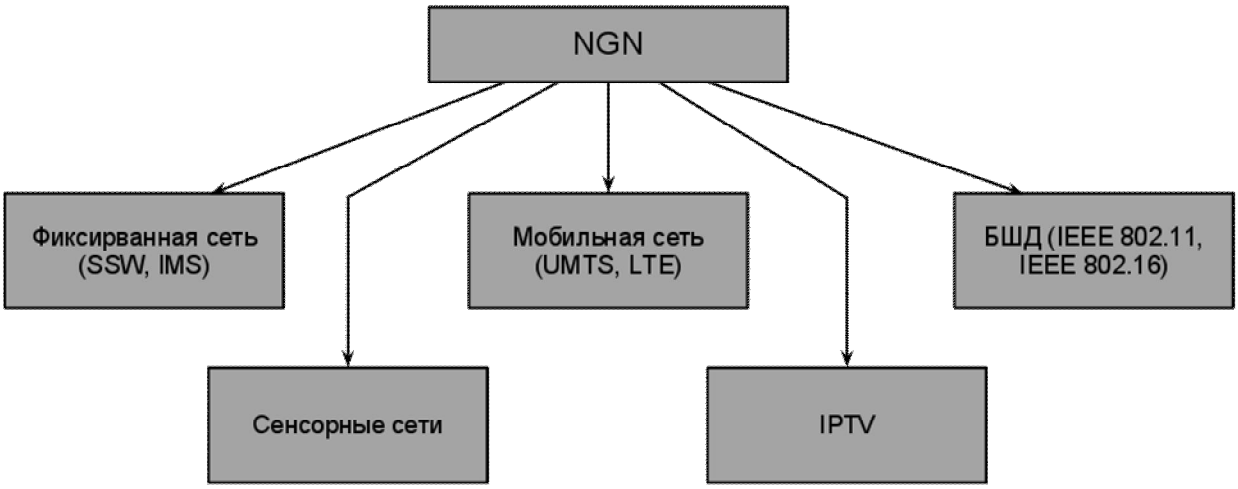


Рис.1.1. Сетевые структуры в концепции NGN.

1.2. Сети фиксированной и мобильной связи.

Как уже отмечалось выше, пакетные сети фиксированной связи строятся в настоящее время на базе технологических

решений SSW и IMS. Подсистема IMS используется также в соответствии со своим предназначением и для построения мобильных сетей связи. Такое технологическое решение по единообразному построению систем сигнализации и управления, а подсистема IMS предназначена, в первую очередь, именно для выполнения указанных функций, позволяет не только оптимизировать затраты для операторов, оказывающих услуги и в фиксированной, и в мобильной сетях, но и предоставлять новый спектр услуг – конвергентные [174].

Существует достаточное количество системных решений и литературных источников по применению SSW и IMS [3,4,6,11,23,25,28,50,52,169,170,171,172]. Стоит, однако, отметить, что в настоящее время осуществляется поиск новых решений для построения ядра сети NGN. В рамках работ Сектора Стандартизации Международного Союза Электросвязи разрабатываются требования к сетям распределенного обслуживания DSN (Distributed Service Network) [175]. В отличие от SSW и IMS решения DSN ориентированы изначально на обслуживание трафика P2P (Peer-to-Peer), что может привести к лидирующей роли этих новых решений уже в ближайшие годы.

Развитие мобильных сетей связи в настоящее время осуществляется на основе технологических решений третьего поколения 3G. Системы третьего поколения были разработаны достаточно давно, например, спецификации на 3G были созданы консорциумом 3GPP (3rd Generation Partnership Project) в 1999 году, а уже в 2001-2002 годах в Японии было развернуто

широкомасштабное внедрение систем 3G [33]. Следует отметить, что передача речи в системах 3G осуществляется с помощью коммутации каналов и это естественно для системы, разработанной в начале века. На рис.1.2 представлен прогноз доли трафика VoIP [34,202] в общем объеме разговорного трафика, из которого видно, что в момент разработки систем 3G эта доля не превышала нескольких процентов, в то время как в настоящее время и в ближайшем будущем эта доля превысит 50% [34]. Передача трафика VoIP в системах с коммутацией каналов существенно дороже, чем в системах с коммутацией пакетов [101].

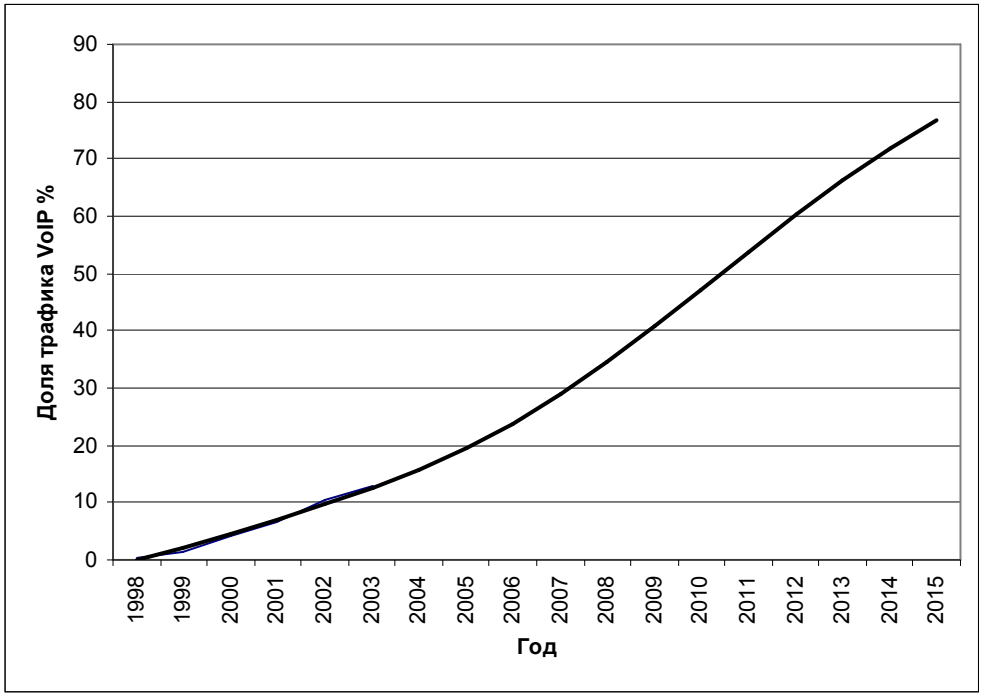


Рис.1.2. Прогноз роста доли трафика VoIP на горизонте планирования до 2015 года.

На рис.1.3 приведены относительные стоимости передачи речи в сетях с коммутацией каналов (3G), сетях с коммутацией пакетов (LTE – Long Term Evolution) и при модернизации систем 3G путем дооснащения их подсистемой HSPA (High Speed Packet

Access). Как видим наименьшие затраты на передачу трафика VoIP наблюдаются в системе пакетной коммутации LTE. Однако не только этот факт стал причиной необходимости разработки комитетом 3GPP2 новой технологической базы, коей для мобильных сетей является система долговременной эволюции LTE [54].

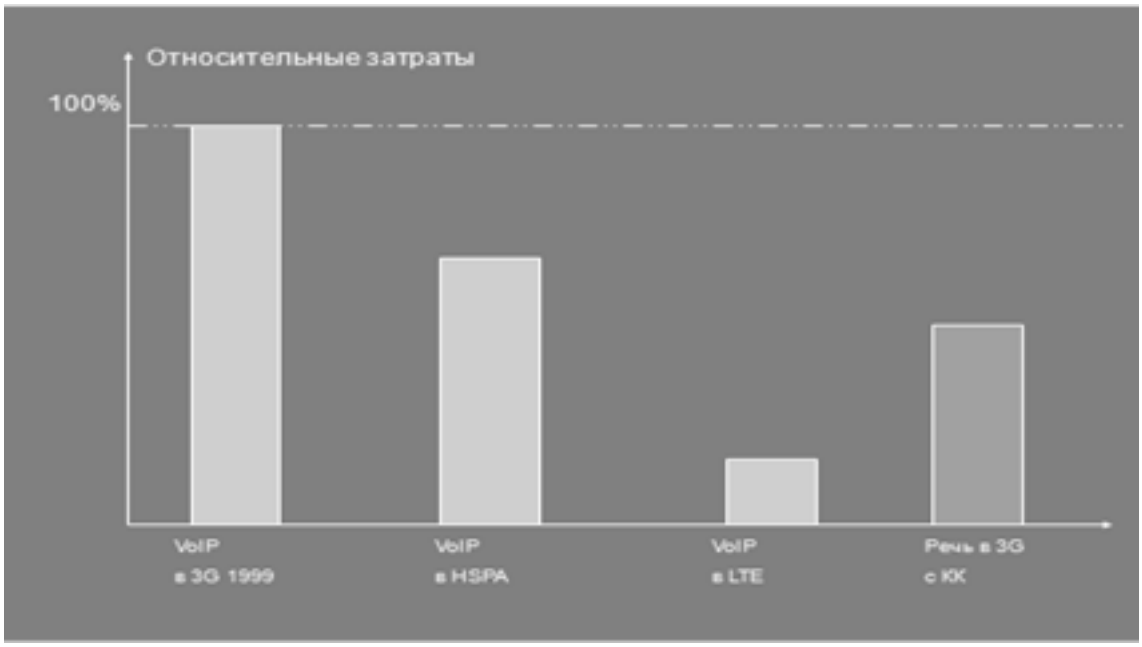


Рис.1.3. Относительные затраты на передачу речи для систем 3G и LTE.

На рис.1.4 приведен прогноз средней скорости доступа для сетей связи Российской Федерации, выполненный на основе закона Нильсена (оптимистический прогноз), преобладании тенденции внедрения на сетях доступа технологий xPON (прагматический прогноз), сохранении развития сети доступа на технологиях xDSL (пессимистический прогноз). С учетом характеристик жилой застройки, плотности населения и его доходов можно считать целесообразным для городов с населением более 1млн. человек

рассматривать на горизонте планирования до 2015 года среднюю скорость широкополосного доступа по оптимистическому прогнозу (127 Мб/с), для областных центров с численностью населения менее 1 млн. человек и районных центров с численностью населения более 100 тысяч человек – по прагматическому прогнозу (70 Мб/с), для райцентров с численностью населения менее 100 тысяч человек по пессимистическому прогнозу (27 Мб/с) или в зависимости в возможной технологии доступа на сети в 2015 году. Последнее целесообразно также отнести и к сельским поселениям, т.е. в зависимости от возможной в 2015 году технологии доступа на конкретной территории [34,52].

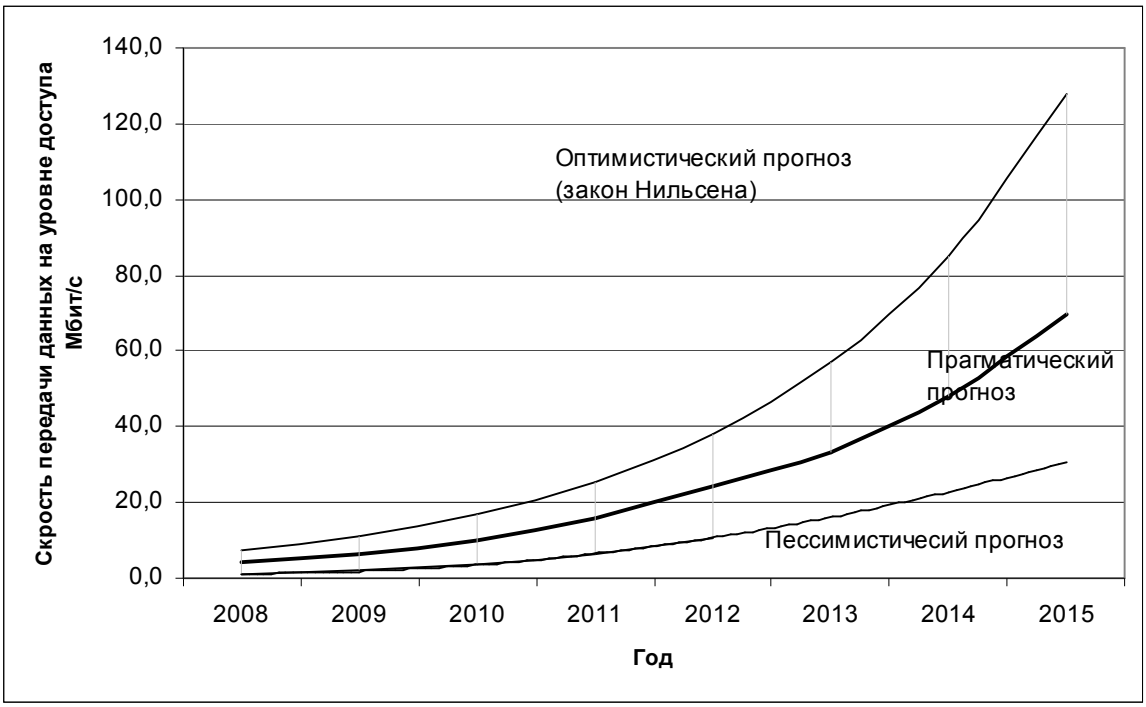


Рис.1.4. Прогноз прироста средней скорости на доступе.

Проведенный анализ требуемых на горизонте планирования удельных скоростей передачи на доступе на горизонте планирования до 2015 года показывает, что указанным требованиям для сетей мобильной связи как раз и отвечает

технология LTE. В таблице 1 приводятся сравнительные характеристики динамики развития HSPA и HSPA+ (High Speed Packet Access) и LTE. Как видим, число планируемых и строящихся сетей LTE превосходит аналогичный показатель для HSPA и HSPA+ вместе взятых [92].

Таблица 1. Темпы роста сетей HSPA, HSPA+ и LTE.

Характеристика сети	HSPA	HSPA+	LTE
Число сетей в эксплуатации	404	135	22
Число стран	153	70	16
Число планируемых и строящихся сетей	103	60	79-линейные испытания, 167-планируется и строится

Одной из наиболее перспективных в техническом плане технологий для мобильной связи представляются также решения WiMax. Действительно, в соответствии со стандартом IEEE 802.16m [123] данная технология может обеспечивать устойчивую передачу речи и данных даже на скоростях до 350 км/час (низколетящие самолеты и иные подобные объекты). Однако,

широкое развитие сетей 2-2.5G, 3G и предстоящее внедрение LTE делают всемирное развитие этой технологии проблематичным. На сегодняшний день число пользователей сотовых сетей связи в мире составляет 5.3 млрд, в том числе пользователей 3G – 600 млн (первый квартал 2011 года). На том же временном интервале число пользователей WiMax составило 25 млн.

1.3. Стандарты IEEE 802.11 и самоорганизующиеся сети.

Следующими сетевыми структурами, входящими в состав концепции NGN, являются сети широкополосного беспроводного доступа, которые формируются на основе стандартов IEEE 802.11 [114-121] и IEEE 802.16 [122,123]. Принципы построения сетей беспроводного широкополосного доступа на указанных стандартах достаточно подробно рассмотрены в [34], поэтому в настоящей книге остановимся только на идеях IEEE 802.11, приведших в конечном итоге к созданию самоорганизующихся сетей.

Работа над стандартами беспроводных сетей, разрабатываемых комитетом IEEE 802.11, до 1985 года шла достаточно медленно, заинтересованность рынка в подобных технологиях практически отсутствовала, а частоты в гигагерцовом спектре подпадали под государственное лицензирование. В 1985 году Федеральная Комиссия по Связи (FCC) США провела выделение новых частот, названных «индустриальные, научные и медицинские» (Industrial, Scientific and Medical, ISM) частоты, а лицензирование оборудования, работающего на этих частотах, было отменено. Это событие послужило мощным толчком к

развитию сетей WLAN – потенциальные операторы больше не нуждались в получении лицензии, значит при неудаче коммерческой эксплуатации устройств, работающих на частотах ISM, они не несли потерь, связанных с лицензиями – именно эти издержки зачастую являются самыми существенными при операторской деятельности. Кроме того, отсутствие лицензирования дает возможность формирования малых альтернативных операторов и ведение ими коммерческой деятельности без необходимости больших начальных инвестиций, которые под силу только крупным операторам. Помимо этого, снятие лицензирования позволило корпоративным клиентам задуматься о возможности развертывания WiFi в офисах и на предприятиях.

В 1989 году Рабочая Группа IEEE 802.11 начала детальную проработку физического и канального уровней для будущего стандарта. Разработка стандарта IEEE 802.11 была эпохальным событием в развитии беспроводных локальных сетей связи. Финальная версия документа была одобрена 26 июня 1997 года.

Стандарт IEEE 802.11 определяет базовый набор услуг, называемый Basic Service Set (BSS), позволяющий сети из двух и более фиксированных или мобильных станций обмениваться данными в некоторой ограниченной области пространства. В стандарте определены два режима функционирования:

– Ad hoc (Ad hoc – латинское выражение, означающее по-английски “for this purpose”, т.е целевой режим, целевая сеть). Этот режим позволяет станциям, оснащенным картами доступа IEEE

802.11, обмениваться данными без инфраструктуры оператора, подразумевающей наличие базовой станции (точки доступа) и т.п. Обмен данными непосредственно между двумя станциями называется независимый базовый набор услуг Independent Basic Service Set (IBSS). Станции, как правило, осуществляют передачу широковещательных и других служебных пакетов в рамках какой-либо ограниченной области без непосредственного доступа в сеть, например, NGN или Интернет. Режим Ad hoc может быть достаточно просто сконфигурирован для различных приложений, например, обмена данными. Именно этот вариант построения сетей по стандартам IEEE и положил начало теории и практике создания самоорганизующихся сетей связи (self – organizing) [38,39,41].

– Инфраструктурный. В этом режиме станции взаимодействуют через точку доступа, принадлежащую оператору. Точка доступа обычно подключается к сети NGN или Интернет путем ее подсоединения к фиксированной сети. Каждая точка доступа покрывает сигналом некоторую ограниченную территорию, размер которой зависит от типа стандарта семейства IEEE 802.11 и, в среднем, ее диаметр составляет от 50 до 100 метров для открытых пространств. В случае если сеть WiFi разворачивается в здании, размер территории уменьшается в зависимости от конфигурации здания, а также типов материалов, из которых оно построено. Каждая станция должна быть ассоциирована с точкой доступа, причем только с одной. Точки доступа размещаются таким образом, чтобы их сигналы перекрывались, позволяя мобильным станциям перемещаться в

рамках пространства покрытого сигналом от различных точек доступа – для перехода обслуживания некоторой станции с одной точки доступа к другой осуществляется процедура хэндовера (handover или handoff), позволяющая осуществить переассоциацию станции при переходе от одной точки доступа к другой.

Архитектуры IBSS и BSS приведены на рис.1.5.

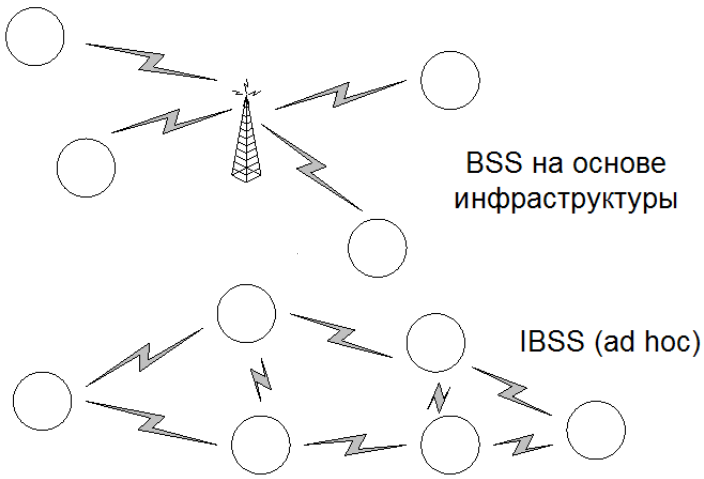


Рис.1.5. Архитектуры стандарта IEEE 802.11.

Самоорганизация в подобных сетях основана на обеспечении одновременного множественного доступа к каналу связи и распределенном доступе к среде передачи. С этой целью в стандартах IEEE 802.11 для подуровня MAC (Media Access Control) канального уровня модели взаимодействия открытых систем было предложено использовать функцию распределенного доступа к среде передачи DCF (Distributed Coordination Function). Для доступа к каналу при этом используется процедура множественного доступа с детектированием несущей и предупреждением коллизий (CSMA/CA – Carrier Sense Multiple Access With Collision

Avoidance). Отметим, что такое же построение MAC используется и во всех современных стандартах IEEE для самоорганизующихся сетей, например, в стандартах семейства IEEE 802.15.

С целью обеспечения функционирования MAC и уменьшения возможных коллизий в стандарте IEEE 802.11 введен ряд интервалов между передачей кадров. Короткий межкадровый интервал SIFS (Short Inter Frame Space) используется для вспомогательных (необходимых) кадров, например кадра подтверждения ACK (ACKnolegment). Распределенный межкадровый интервал для режима DCF - DIFS (Distributed Inter Frame Space) обеспечивает возможность справедливого распределения ресурсов, т.е. конкурентной борьбы за канал. И, наконец, расширенный межкадровый интервал EIFS (Extended Inter Frame Space) используется в случае возникновения ошибки.

Детектирование (контроль) несущей является одной из самых важных функций доступа к каналу связи (MAC IEEE 802.11x) для предупреждения возможных коллизий. Эта функция осуществляется на физическом уровне и является энергоемкой для постоянного использования и в связи с этим выполняется по запросу. Контроль виртуальной несущей осуществляется с использованием «вектора резервирования сети» Network Allocation Vector (NAV). Иллюстрация применения NAV показана на Рис.1.6.

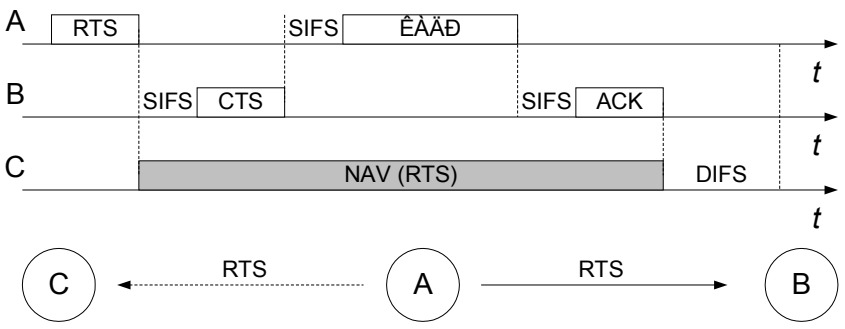


Рис.1.6. Использование «вектора резервирования сети»

Обмен информацией в IEEE 802.11x обеспечивается с помощью механизма RTS/CTS (Request to Send / Clear To Send). Функционирование механизма RTS-CTS происходит по следующему алгоритму (рис.1.7): передатчик передает кадр RTS приемнику, в котором содержится адрес приемника и полное время, необходимое для передачи информационного кадра. В связи с широковещательной процедурой передачи информации для IEEE 802.11x кадр RTS принимается всеми станциями в пределах досягаемости. Необходимый приемник определяется по адресу и отвечает кадром CTS после SIFS, а остальные станции в пределах досягаемости устанавливают «вектор резервирования сети». Кадр CTS также принимается всеми станциями в пределах досягаемости, но уже возможно другими. При этом передатчик передает информационный кадр после SIFS, а новые станции устанавливают «вектор резервирования сети». После выполнения перечисленных шагов все станции в пределах досягаемости и RTS, и CTS проинформированы о резервировании канала. Осуществляется передача информационного кадра DATA и, если передача успешна, приемник передает подтверждение ACK после SIFS, «Вектор резервирования сети» истекает, канал снова свободен.

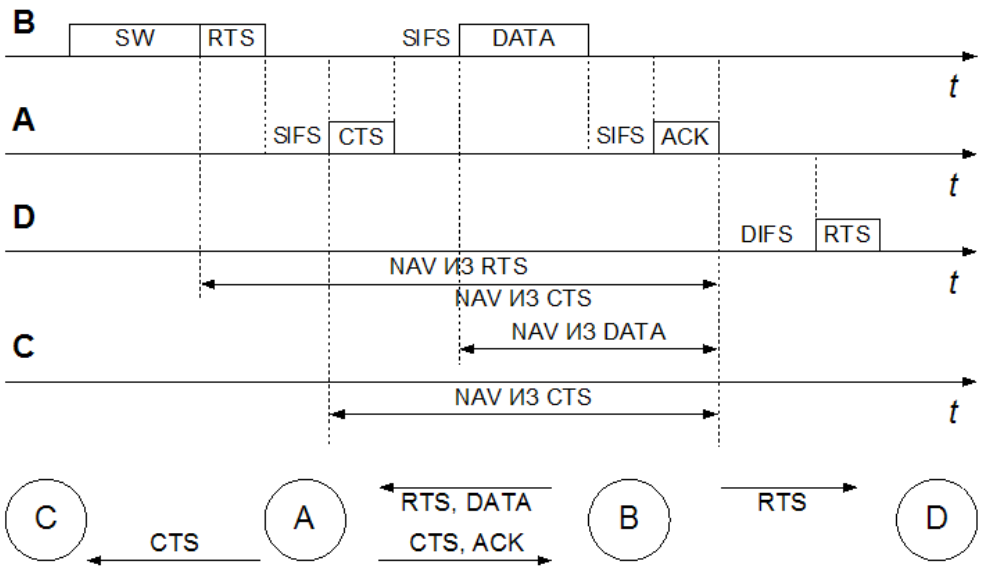


Рис.1.7. Пример алгоритма функционирования RTS-CTS

Как уже отмечалось выше, для предотвращения коллизий используется процедура CSMA/CA.

В настоящее время сети беспроводного широкополосного доступа широко используются не только для передачи данных, но и для передачи речи [49]. Анализ трафика и вопросы планирования сетей беспроводного широкополосного доступа рассмотрены в [96].

1.4. Определение и примеры самоорганизующихся сетей.

В предыдущем разделе было показано на примере анализа построения сетей связи на основе стандартов семейства IEEE 802.11, как появились самоорганизующиеся сети. В настоящее время эти сети находят все большее применение при организации сетей связи и предоставлении новых услуг. Кроме того, принципиальные изменения, происходящие в клиентской базе сетей связи, заключающиеся прежде всего в том, что большую часть клиентской базы со временем составят машины, устройства, конструкции, биомассы [26,98] и т.д., а не человек с

разнообразными терминалами, позволяют сделать вывод о том, что и обслуживание этой новой преобладающей клиентской базы должно осуществляться по-новому построенными сетями [40]. В настоящее время общепризнано, что такими сетями являются самоорганизующиеся [39,47,61,62,66,72,91].

Самоорганизующейся называется сеть, в которой число узлов является случайной величиной во времени и может изменяться от 0 до некоторого значения Nmax. Взаимосвязи между узлами в такой сети также случайны во времени и образуются для достижения сетью какой-либо цели или для передачи информации в сеть связи общего пользования или иные сети [51].

Архитектура самоорганизующейся сети представлена на рис.1.8.

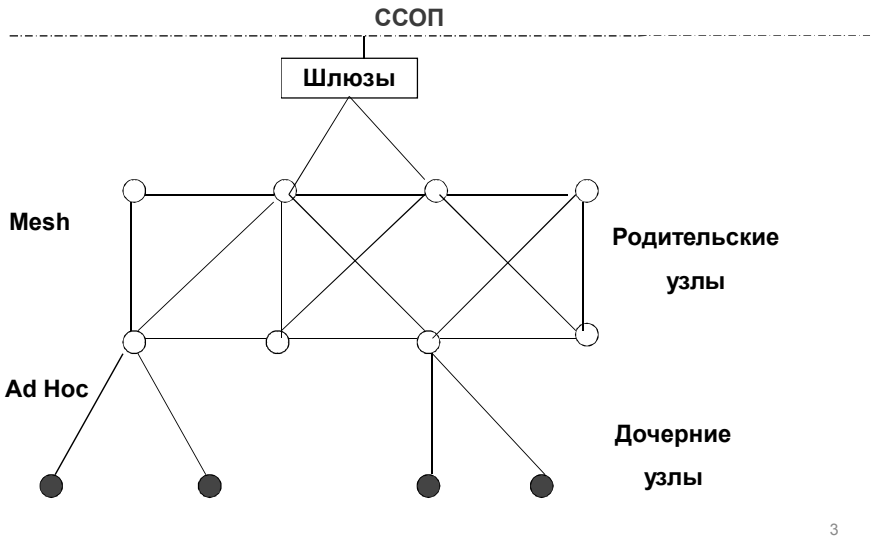


Рис.1.8. Архитектура самоорганизующейся сети.

Самоорганизующаяся сеть, как и все сети связи, состоит из сетей доступа и транзитной сети. Сеть доступа называется Ad Hoc

(целевая сеть) [38,75,185,188], а транзитная сеть – mesh (ячеистая) [67,106]. Как видно, из рис.1.8, узлы сети Ad Hoc не имеют функций маршрутизации и могут осуществлять взаимосвязь лишь с ближайшими узлами. В связи с этим достаточно часто узлы Ad Hoc называют дочерними. Последнее в силу самоорганизации сети вовсе не означает, что дочерний узел строго привязан к какому-либо родительскому узлу. В процессе жизненного цикла сети дочерний узел может быть привязан к любому наиболее близко расположенному родительскому узлу, а при определенных условиях и сам может превратиться на время или навсегда в родительский узел, например, в однородных беспроводных сенсорных сетях, алгоритмы функционирования которых будут рассмотрены в следующих главах.

Узлы mesh имеют встроенные функции маршрутизации и могут поддерживать установление соединения не только к ближайшему узлу, но и ко многим другим. Такой сетевой режим называется multi-hop (многошаговое соединение) в отличие от соединений для дочерних узлов Ad Hoc сети, ограниченных одним шагом в установлении соединения (one-hop). Mesh узлы достаточно часто называют родительскими узлами, что подчеркивает транзитную функцию mesh сети. Очевидно, что узлы самоорганизующейся сети могут совмещать родительские и дочерние функции, например, по аналогии с хорошо известными из истории развития связи в нашей стране комбинированными междугородными/местными автоматическими телефонными станциями.

Среди приложений сенсорных сетей можно выделить функционирующие уже сегодня [39]:

- беспроводные (всепроникающие) сенсорные сети (USN – Ubiquitous Sensor Networks),
- сети для транспортных средств (VANET – Vehicular Ad Hoc Networks),
- муниципальные сети (HANET – Home Ad Hoc Networks),
- медицинские сети (MBAN – Medicine Body Area Network).

Наиболее значимыми по предполагаемому объему внедрения в настоящее время считаются сети USN, которые включены и в состав концепции NGN как одна из составляющих NGN сетевых структур. Сетям USN будет посвящена отдельная глава, поэтому далее перейдем к анализу последней из изображенных на рис.1.1 сетевых структур для NGN – телевидению поверх IP (IPTV).

1.5. Особенности IPTV как сетевой структуры NGN.

Особенности IPTV как сетевой структуры концепции NGN состоят прежде всего в ином характере потоков трафика IPTV по сравнению, в первую очередь, с речевым трафиком [24]. Если речевой трафик в сетях с коммутацией каналов с достаточной для практики степенью точности мог быть аппроксимирован пуассоновским потоком [44,45,58,132], а трафик VoIP может также быть представлен как пуассоновский поток [76,132], то трафик IPTV имеет, как правило, самоподобный характер [151]. При этом, коэффициент Херста, характеризующий степень самоподобия,

может изменяться в достаточно широких пределах, достигая значений H=0.8 [53,97,158]. В таких случаях говорят о ярко выраженном самоподобии, что требует иных методов оценки потоков трафика и расчета сетей связи.

Определение самоподобия дается через автокорреляционную функцию [9,13,16,34,56,86,205]. Пусть процесс задан последовательностью $X = (X_1, X_2, ..X_t..)$, где $t = 1,2,...$

Его автокорреляционная функция

$$r(k) = \frac{\sum_{i=1}^{N-k}(X_i - \overline{X})(X_{i+k} - \overline{X})}{(N-k)\sigma^2} \qquad (1.1)$$

где N - число элементов последовательности,

σ^2 - дисперсия.

Под агрегированным процессом понимается, процесс, заданный последовательностью, элементы которой получены их элементов исходного процесса путем усреднения по блокам из m последовательных элементов.

Агрегированный процесс по блокам длины m

$$X^{(m)} = (X_1^{(m)}, X_2^{(m)}, ..X_t^{(m)}..) \qquad (1.2)$$

где

$$X_t^{(m)} = \frac{1}{m}(X_{tm-m+1} + \ldots + X_{tm}) \qquad (1.3)$$

его автокорреляционная функция

$$r_m(k) \qquad (1.4)$$

Процесс X называется строго самоподобным в широком смысле, если

$$r_m(k) = r(k) \text{ где } m = 2,3,... \qquad (1.5)$$

Иными словами, процесс, строго самоподобен в широком смысле, если при его агрегировании по блокам любой длины, автокорреляционные функции исходного процесса и агрегированных процессов равны, т.е. коэффициент корреляции не изменяется при усреднении по блокам.

Процесс X называется асимптотически самоподобным (second order), если

Если $\lim_{m\to\infty} r_m(k) = g(k)$ (1.6)

Т.е. при усреднении по блокам $m \to \infty$ он сходится к самоподобному.

Процесс X называется строго самоподобным в узком смысле, если

$$m^{1-H} X^{(m)} \overset{\bullet}{=} X \text{ (равенство распределений)}, \qquad (1.7)$$

где H - коэффициент Херста

Самоподобие в узком смысле означает, что функции распределения исходного и агрегированных процессов одинаковы, а степень самоподобия характеризуют коэффициентом Херста.

Из (1.7) следует, что для дисперсий процессов

$$D(X^{(m)}) = m^{2(H-1)} D(X) \tag{1.8}$$

Часто при оценке коэффициента Херста пользуются выражением

$$\ln\left(\frac{D(X^{(m)})}{D(X)}\right) = (2H-2)\ln(m) \tag{1.9}$$

Здесь скобка $2H-2$ имеет геометрический смысл коэффициента наклона прямой, которая аппроксимирует функцию

$$\ln\left(\frac{D(X^{(m)})}{D(X)}\right) = f\left(\ln(m)\right) \tag{1.10}$$

Далее для примера приведем результаты исследований, полученных при изучении трафика IPTV на модельной сети. В качестве теоретической базы для обработки данных о потоках, имеющих ярко выраженную степень самоподобия, использовалось вейвлет-преобразование [10].

На рис.1.9 представлены характеристики пуассоновского трафика, а на рис.1.10 трафика IPTV 60-секундного фрагмента фильма, имеющего высокую степень самоподобия. Последний был измерен на модельной сети [53].

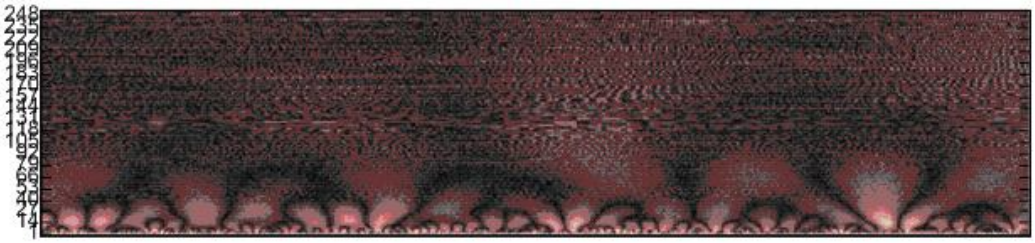


Рис.1.9. Вейвлет преобразование для пуассоновского потока.

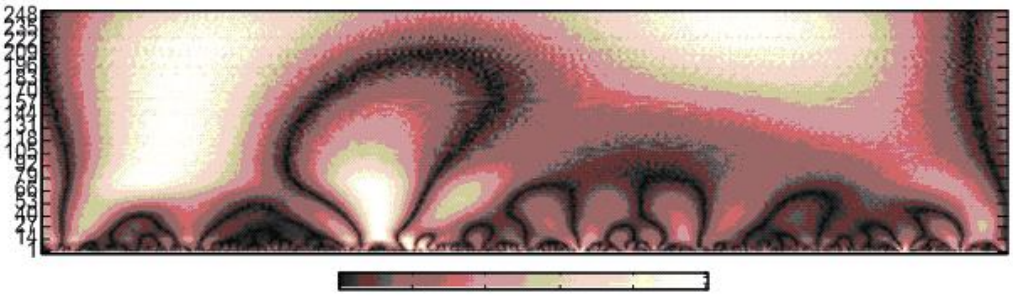


Рис.1.10. Вейвлет преобразование для измеренного трафика при длине фрагмента фильма 60 с.

Как видим, вейвлет анализ (использовались вейвлеты Хаара) показывает принципиально иную природу трафика IPTV по сравнению с пуассоновскими потоками трафика.

Заканчивая рассмотрение концепции NGN, отметим, что эта концепция была создана на рубеже веков и полностью оправдала себя в первом десятилетии 21 века. Однако технологии развиваются настолько быстро, что к настоящему времени назрела необходимость создания новой концепции развития сетей связи общего пользования, чему причиной являются прогнозы развития беспроводных технологий на горизонте планирования до 2020 года.

1.6. Прогноз развития беспроводных технологий до 2020 года и концепция Умных Всепроникающих Сетей.

Беспроводные всепроникающие сенсорные сети (Ubiquitous Sensor Networks, USN) являются одной из самых перспективных технологий 21 века [214]. Дешевые и «умные» сенсоры, в достаточно больших количествах объединенные в беспроводную сеть, подключенную к глобальной телекоммуникационной сети, предоставят в будущем беспрецедентные по широте услуги по контролю и управлению домами, предприятиями, автомобилями, организмами [26,27,29,30,31,61,64,65,77,80,83,84,85,87,135,150,155] и т.п. Более того, USN найдут широкое применение в таких стратегически важных областях как военная стратегия, управление кризисными и чрезвычайными ситуациями, борьба с терроризмом и т.п. Сети USN в зависимости от типа сенсоров могут быть развернуты на земле, в воздухе, под и над водой [63,195], в зданиях и, наконец, на и в живых организмах, например, на и в теле человека [98]. Для поддержки заданных характеристик каждый сенсор должен быть построен в соответствии с определенной архитектурой, в которую как основные элементы входят непосредственно само сенсорное устройство, память, антенна, источник питания.

Планируется и непосредственное использование сенсоров в жизнедеятельности самого человека, а именно: контроль медицинских показателей, в том числе при свободном перемещении человека, контроль местонахождения и личностных характеристик с помощью интегрированных с человеком сенсоров,

контроль местонахождения животных и т.д. Для этих целей существуют проекты, когда сенсоры встраиваются в поводок и/или ошейник собаки, в обувь людей, имплантируются и т.п.

Оставляя вне дискуссии неприятные моральные аспекты такого развития сети, тем не менее, придется признать, что такое технологическое развитие безусловно приведет к несколько иным характеристикам в обществе, которое уже выйдет из стадии электронного. Учитывая всепроникающий характер сенсорных сетей, вполне уместным кажется назвать такое общество ubiquitous [135,152,204], т.е. в нашем случае это название звучит по аналогии с электронной Россией как всепроникающая Россия, или кратко ***u***-Россия. Переход от ***e***-России к ***u***-России является не столь отдаленной перспективой как в связи с быстрым развитием технологий сенсорных сетей, так и в связи с проектами по созданию ***u***-обществ за рубежом.

В период интенсивного развития концепции NGN сетевые структуры USN входили в NGN как составная часть. В то время считалось, что клиентскую база USN составят сотни миллионов сенсорных узлов. Однако, стремительное развитие этой новой технологии, появление концепций Интернета вещей (IoT – Internet of Things) [51,149,176,178,201] и Вэба вещей (WoT – Web of Things) [182,189], привели к пересмотру перспектив развития сенсорных сетей и в соответствии с современными прогнозами число беспроводных устройств составит 7 триллионов на 7 миллиардов человек к 2017 – 2020 годам [207].

На рис.1.11 приведены примеры использования сенсорных узлов, включая радио идентификаторы (RFID), включающие в себя в том числе такие новейшие приложения USN как мониторинг роста животных и растений [149].

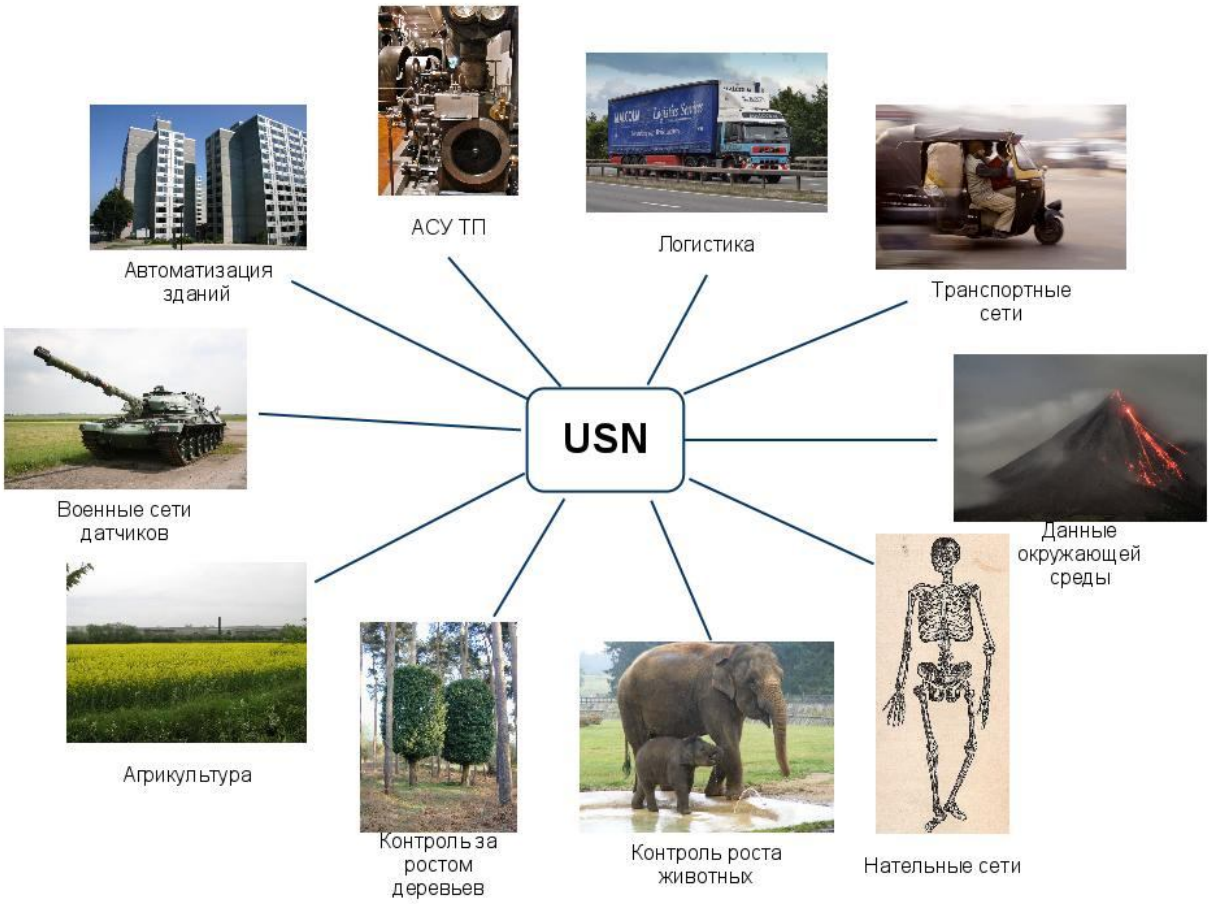


Рис.1.11. Примеры использования USN сетей.

Планируемое принципиальное изменение клиентской базы потребовало от мирового телекоммуникационного сообщества пересмотра концептуальных основ построения сетей связи с учетом существенного преобладания в клиентской базе сетей будущего устройств, биомасс, конструкций и т.п.

Сектор стандартизации Международного Союза Электросвязи в настоящее время рассматривает возможность замены концепции

NGN на концепцию Умных Всепроникающих Сетей (SUN – Smart Ubiquitous Networks) [192], включающую в себя концепцию NGN как одну из составных частей.

Структура концептуальной модели SUN приведена на рис.1.12.

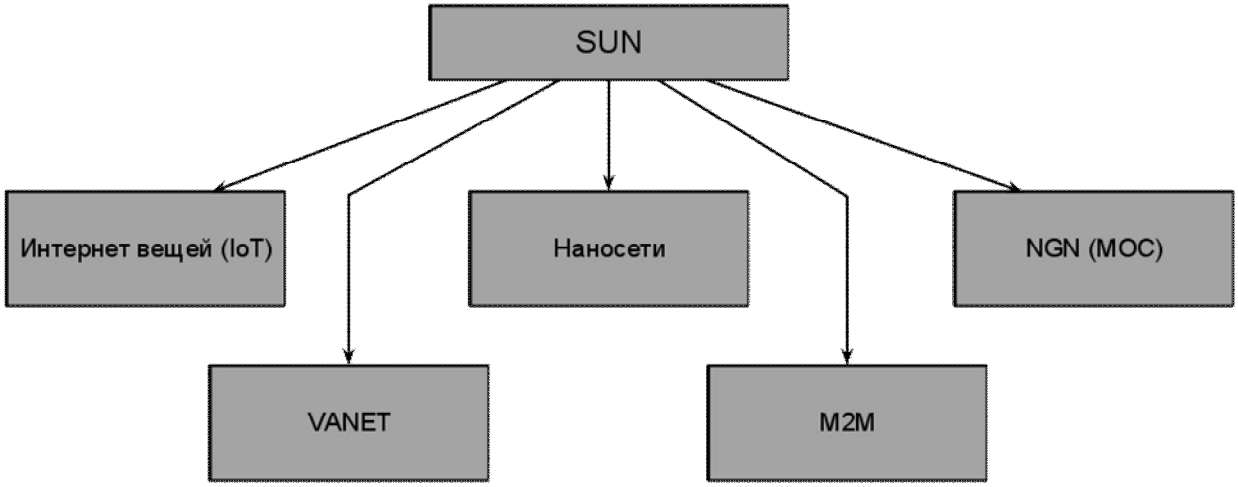


Рис.1.12. Структура концептуальной модели SUN.

В состав концептуальной модели SUN входят Интернет вещей (IoT), сеть NGN, модернизированная до уровня поддержки межмашинных коммуникаций (MOC – Machine Oriented Communications) [179], наносети [70], транспортные сети VANET [121,143,177] и сети устройство – устройство (M2M – Machine-to-Machine) [90].

На рис.1.13 приведена структура Интернета вещей. Интернет вещей включает в себя сетевые структуры USN, построенные на базе протокола 6LoWPAN (Low energy IPv6 based Wireless Personal Area Networks protocol). Протокол 6LoWPAN [183,213] обеспечивает возможность присвоения IP адреса сенсорным узлам

и RFID или их группам. Именно эта возможность делает USN с применением IP адресации основой Интернета вещей.

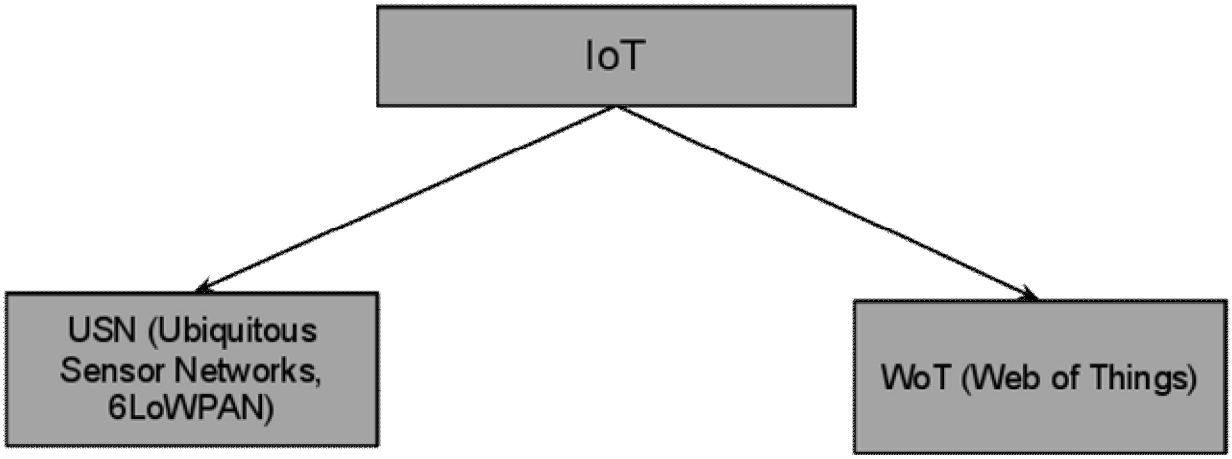


Рис.1.13. Структура Интернета вещей.

Веб вещей является составной частью Интернета вещей и предоставляет возможность мониторинга и управления вещами с помощью страниц WWW. На рис.1.14 приведена структура организации Веба вещей [182], из которой видно, что ключевую роль в этом применении IoT играет брокер Веба вещей, позволяющий использовать веб вещей как для изначально приспособленных для этого вещей (Web enabled things), так и для тех вещей (non-Web enabled things), для которых необходимы соответствующие шлюзы (GW-gateway), например, для вещей, функционирующих по протоколам ZigBee [215] или Bluetooth [126]. На рис.1.14 приложения (application) Веба вещей подразделяются на мониторинг, управление, услуги, в том числе смешанные (mash up).

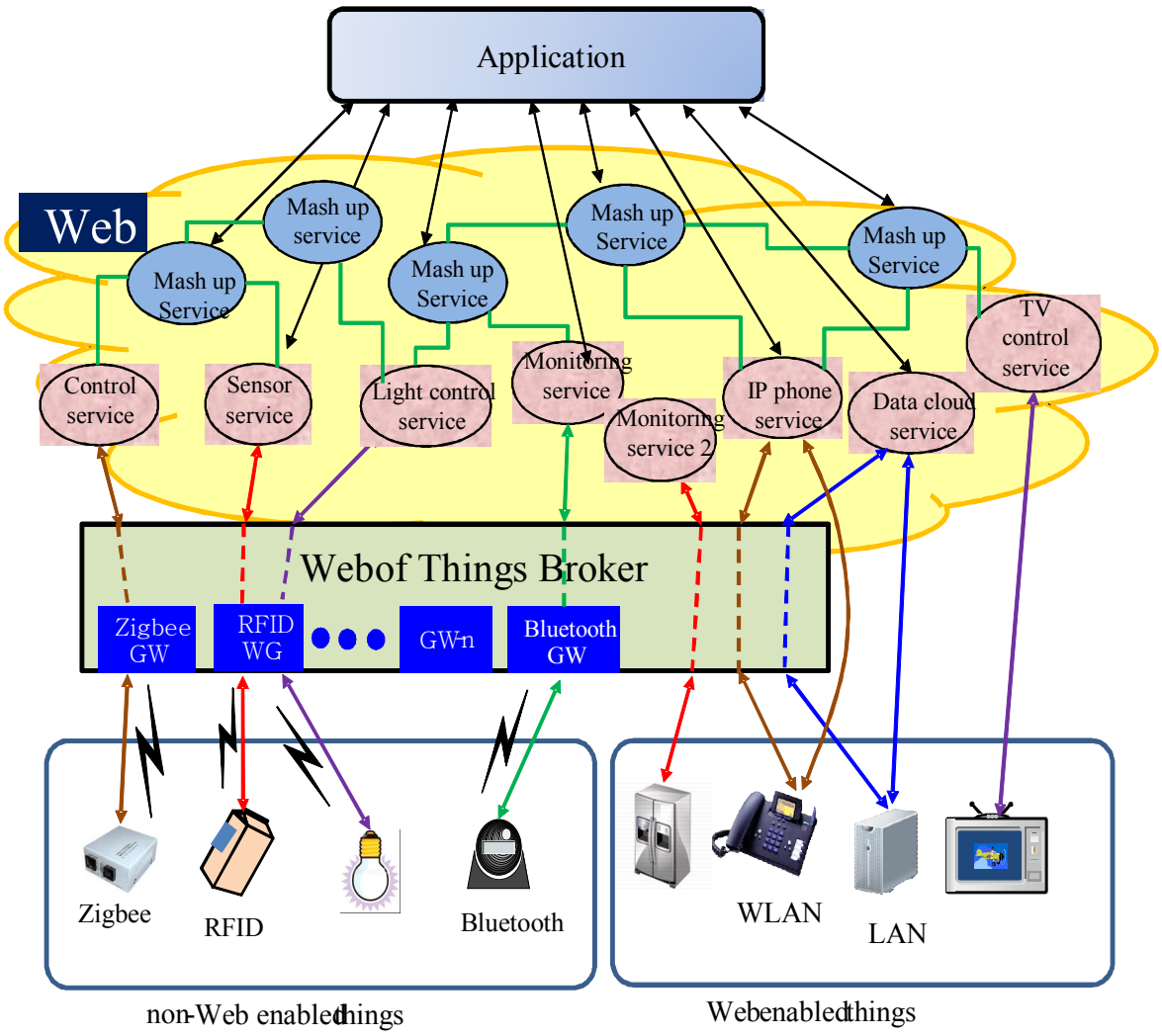


Рис.1.14. Архитектура Веба вещей.

На рис.1.15 приведена структура M2M [90]. Как видим, основное отличие M2M от IoT состоит в том, что M2M поддерживает всевозможные взаимосвязи между устройствами, для которых IP адрес не является необходимым условием установления соединений. Отметим также, что в МСЭ-Т существуют предложения, в соответствии с которыми M2M рассматривается как подсистема IoT.

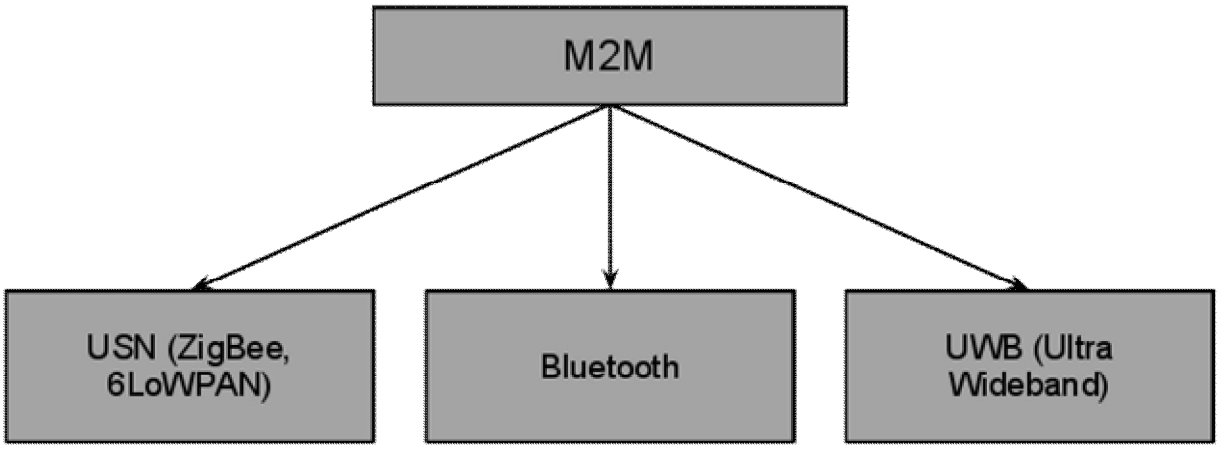


Рис.1.15. Структура M2M.

В качестве устройств, не поддерживающих адресацию IP, рассмотрены сенсорные узлы и RFID, функционирующие по протоколу IEEE 802.15.4, Bluetooth и UWB устройства. Естественно, что при наличии соответствующих шлюзов такие устройства (вещи) могут быть присоединены и к сетям IoT.

Одним из наиболее перспективных направлений в развитии систем беспроводного доступа являются сети транспортных средств VANET (Vehicular Ad hoc Network) [143]. Сети VANET принадлежат к классу мобильных Ad hoc сетей MANET (Mobile Ad hoc Network) [47], хотя им присущ и ряд особенностей, как с точки зрения применения, так и с точки зрения протоколов. Следует заметить, что, несмотря на название VANET, в этих сетях предусматривается не только режим функционирования Ad hoc, но и комбинированный, когда элементы сети VANET могут соединяться с инфраструктурными узлами сети.

В соответствии с рекомендацией МСЭ-Т Y.2281 [177] предусматриваются следующие варианты организации взаимосвязей для сетей VANET:

- V2V (Vehicular to Vehicular), транспортное средство – транспортное средство,
- V2I (Vehicular to Infrastructure), транспортное средство – инфраструктура,
- V2H (Vehicular to Home), транспортное средство – дом,
- V2G (Vehicular to Grid), транспортное средство – вычислительные ресурсы.

Наибольшее продвижение в настоящее время сети VANET получили в проектах для автомобильных сетей, что и неудивительно, поскольку, например, число абонентов телефонной сети в Российской Федерации сегодня немногим более 40 миллионов, а число автомобилей составляет 38 миллионов. Как видим, с точки зрения объема значения числа пользователей телефонной и автомобильной сетей сопоставимы. В настоящем разделе остановимся на автомобильной сети, архитектура которой показана на рис.1.16 [34].

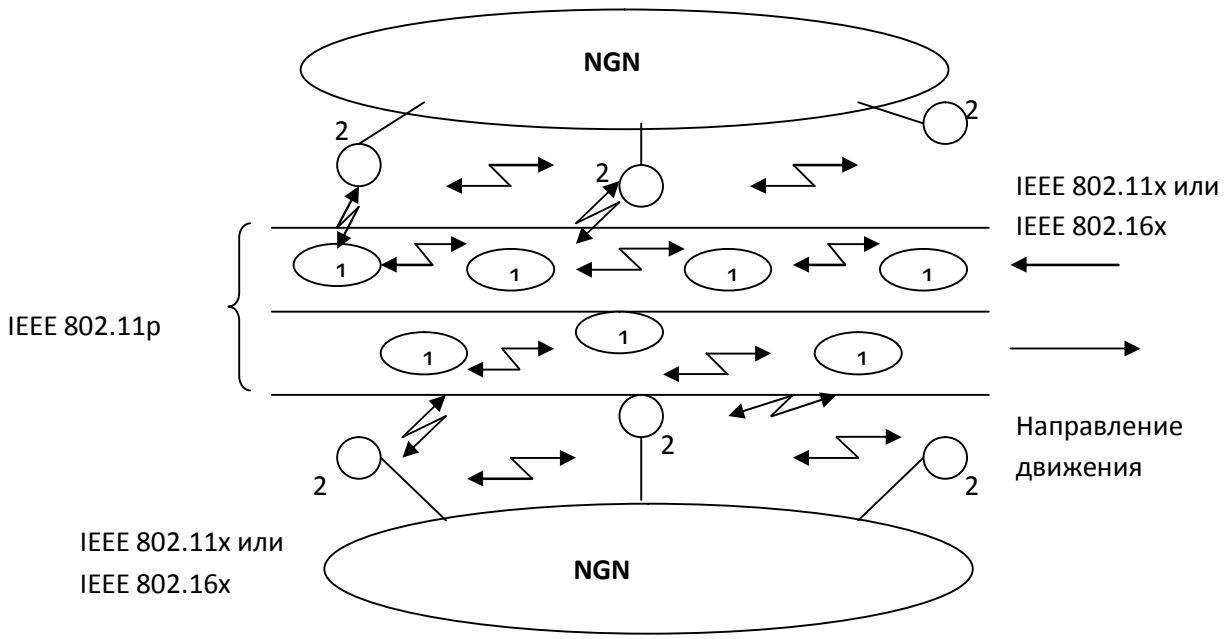


Рис.1.16. Архитектура VANET для автомобильной сети.

На рис.1.16 автомобили обозначены как узлы класса 1, а инфраструктурные узлы придорожной сети как узлы класса 2. Взаимодействие автомобилей осуществляется в режиме Ad hoc, в то же время автомобиль может взаимодействовать и с придорожной инфраструктурной сетью, связанной с сетью связи общего пользования NGN. Естественно, что пассажиры автомобиля могут с использованием мобильных телефонов 2/2.5/3G и непосредственно пользоваться услугами сотовых сетей связи общего пользования.

Какие же варианты применения современных средств телекоммуникаций делают их привлекательными для создания автомобильных сетей, несмотря на наличие у пользователей сотовых телефонов?

Приложения VANET для автомобильных сетей можно разделить на две большие группы:

- обеспечение безопасности,

- обеспечение повышенного комфорта.

В части приложений обеспечения безопасности в первую очередь можно выделить три группы:

- помощь водителю (навигация, объезд массовых столкновений, изменение дорожной разметки),

- информационная поддержка водителя (скоростной режим, информация о проведении дорожных работ),

- предупредительная сигнализация (аварийные ситуации, преграды или происшествия, неблагоприятные дорожные условия).

В качестве примера можно привести отказ подушки безопасности у движущегося автомобиля, информация о нем по сети VANET сразу же будет передана следующим за ним автомобилям. В части навигации сети VANET могут предоставить информацию не только о местоположении своего автомобиля как GPS/ГЛОНАСС/ГАЛИЛЕО, но и любого другого, а также о пробках, в том числе и их численные оценки.

В части приложений по обеспечению повышенного комфорта можно выделить следующие. Создание группы по интересам POI (Points of Interest) в локальных пробках, информация о текущем трафике на дорогах, погода, возможности приема сообщений, игры в режиме on-line и т.д. Интересной представляется также возможность осуществления P2P соединений, в том числе с домом через придорожную сеть и сеть NGN. Полезной может являться

также информация от придорожной сети об отелях, станциях заправки, меню в ресторанах и т.д.

Анализируя приложения VANET для автомобильных сетей, следует отметить, что эти приложения дают качественно новые возможности как с точки зрения безопасности, так и с точки зрения комфорта.

Еще одной составляющей концепции SUN, пожалуй, наименее изученной, являются наносети. На рис.1.17 приведена структура беспроводных сенсорных наносетей WNSN (Wireless Nano Sensor Networks) [69,70].

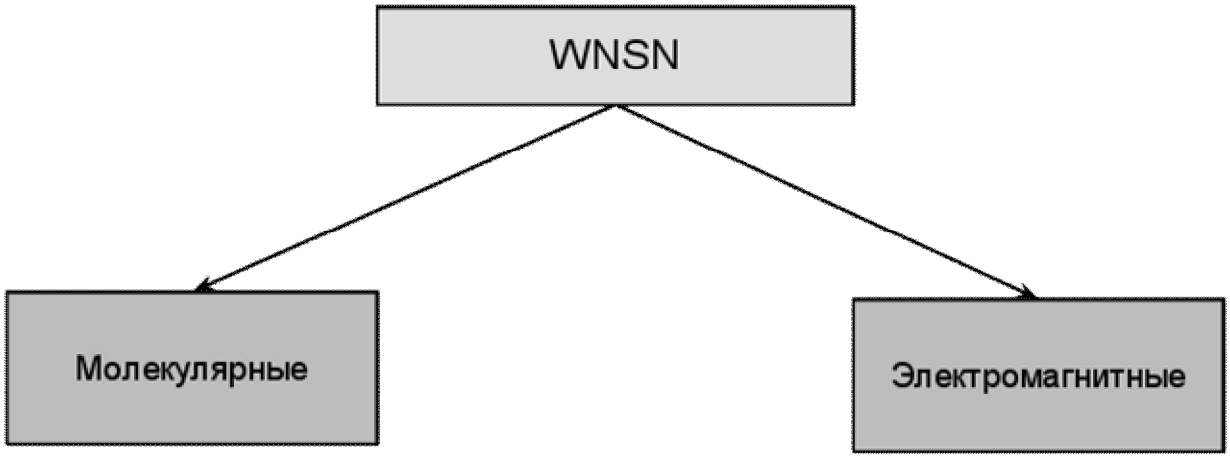


Рис. 1.17. Структура беспроводных наносенсорных сетей.

Как видим, в структуре беспроводных наносенсорных сетей выделяются сети на основе передачи информации с помощью электромагнитных волн и молекулярные сети. В беспроводных наносенсорных молекулярных сетях передача информации осуществляется с помощью перемещения вещества. С учетом изложенного, можно дать следующее определение наносетей. Наносеть является самоорганизующейся сетью, в которой в

качестве узлов сети используются наномашины, а информация и сигнализация могут быть переданы, в том числе и путем перемещения вещества [51].

Завершая анализ новой концепции SUN, отметим, что принципиальные изменения в концепции развития сетей связи стали возможными, в первую очередь, благодаря достижениям в области теории и практики создания самоорганизующихся сетей. Далее в книге будут рассмотрены принципы создания и функционирования, а также протоколы для наиболее распространенных самоорганизующихся сетей – сенсорных, а также подходы к созданию нетривиальных по своей сути молекулярных наносетей.

2. Сенсорные сети. Кластеры и выбор головного узла.

2.1. Общие положения.

Беспроводные всепроникающие сенсорные сети USN представляют собой самоорганизующиеся сети, состоящие из множества беспроводных сенсорных узлов, распределённых в пространстве и предназначенных для мониторинга и/или управления характеристиками окружающей среды или объектами, расположенных в ней. Пространство, которое покрывается сенсорной сетью, называют достаточно часто сенсорным полем. Собственно беспроводные сенсорные узлы представляют собой миниатюрные устройства с ограниченными ресурсами: зарядом батареи, объемом памяти, вычислительными возможностями и т.д. Однако, объединение большого числа этих элементов в сеть обеспечивает возможность получения реальной картины происходящих событий и процессов в рамках этого сенсорного поля[43,46,48,93,102,108,153,157,173,180,181,196,197,199,206,209,212].

Беспроводные сенсорные узлы могут собирать информацию о наблюдаемых явлениях и передавать её далее для обработки и анализа. Примерами собираемой информации могут быть данные о температуре, влажности, условиях освещения, сейсмической активности и т.д. Такие данные могут быть использованы как для выявления каких-либо событий, так и для управления ими [34].

Выбор конкретных решений для сенсорных узлов при распределении беспроводной сенсорной сети в первую очередь

зависит от функциональных возможностей, размера, затрат, энергетических характеристик и в настоящее время при начале достаточно широкого внедрения сенсорных сетей – от обеспечения требуемого качества обслуживания [141,142].

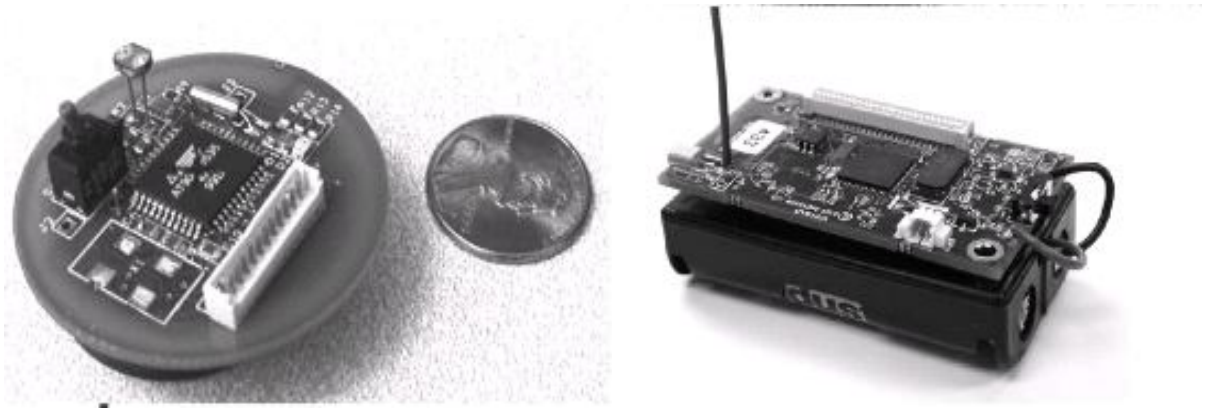


Рис. 2.1. Сенсорные узлы.

Примеры конструкций современных сенсорных узлов приведены на рис. 2.1, а на рис. 2.2 рассматривается типовая архитектура сенсорного узла. Типовая архитектура сенсорного узла включает в себя следующие элементы: один или несколько сенсоров, собирающих информацию об окружающей среде и/или её составляющих, центральный процессор и память, радиопередатчик, устройство электропитания.

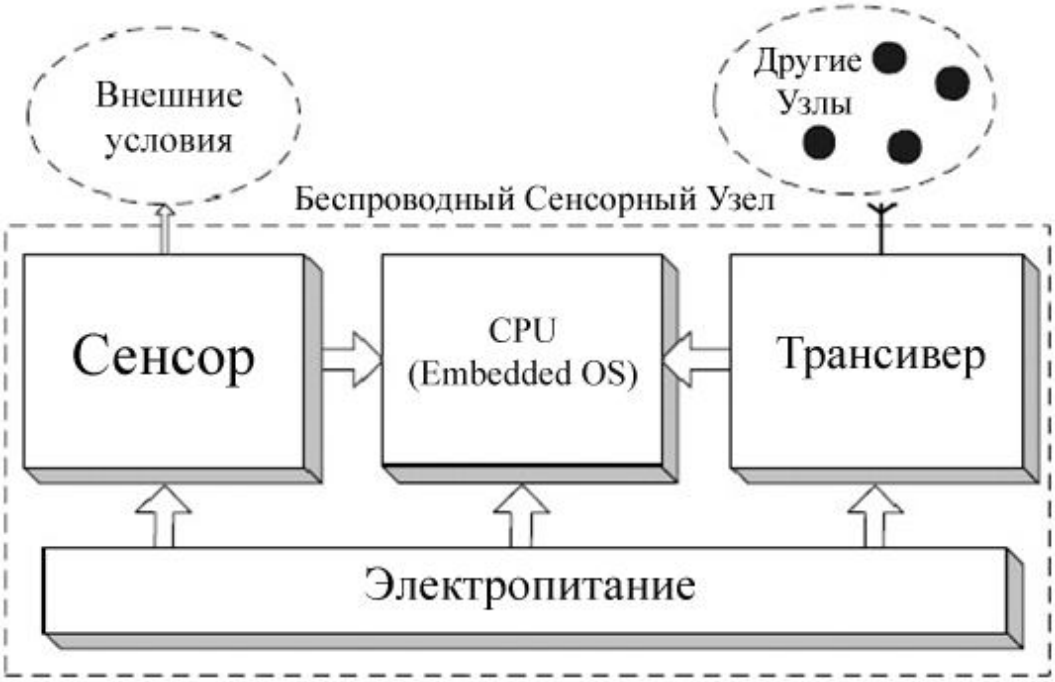


Рис. 2.2. Типовая архитектура сенсорного узла.

Создание сенсорной сети из беспроводных сенсорных узлов, будь-то разнообразные задачи мониторинга окружающей среды, периметрической защиты, контроля перевозок и т.д. [216], требует как выбора архитектуры сети, так и протоколов взаимодействия элементов этой сети между собой и с внешними (например, NGN или IoT) сетями.

В настоящее время можно выделить несколько характеристик архитектуры беспроводных сенсорных сетей.

Гомогенные или гетерогенные USN. Беспроводная сенсорная сеть может быть построена на однотипных или разнотипных сенсорных узлах. Гомогенной сетью, соответственно, является сеть, в которой все сенсорные узлы имеют подобные измерительные и вычислительные возможности. Поскольку сенсорная сеть может содержать тысячи сенсорных узлов,

построение сенсорной сети как гомогенной выглядит экономически обоснованным решением, естественно тогда, когда это возможно. В гетерогенной сети различные сенсорные узлы могут обладать различной энергоёмкостью, измеряемым набором параметров, вычислительными возможностями. Примером гетерогенной сенсорной сети может являться сеть мониторинга, в которой ряд сенсоров реализует функции видеонаблюдения, а остальные – аудиоконтроль.

Случайное или детерминированное размещение сенсорных узлов. Сенсорные узлы могут быть случайным образом разбросаны по некоторой территории (как это показано на рис.2.3) или предварительно размещены в соответствии с планом построения сети. Естественно, что алгоритмы распределения данных между сенсорными узлами в первом и втором случае могут существенно отличаться.

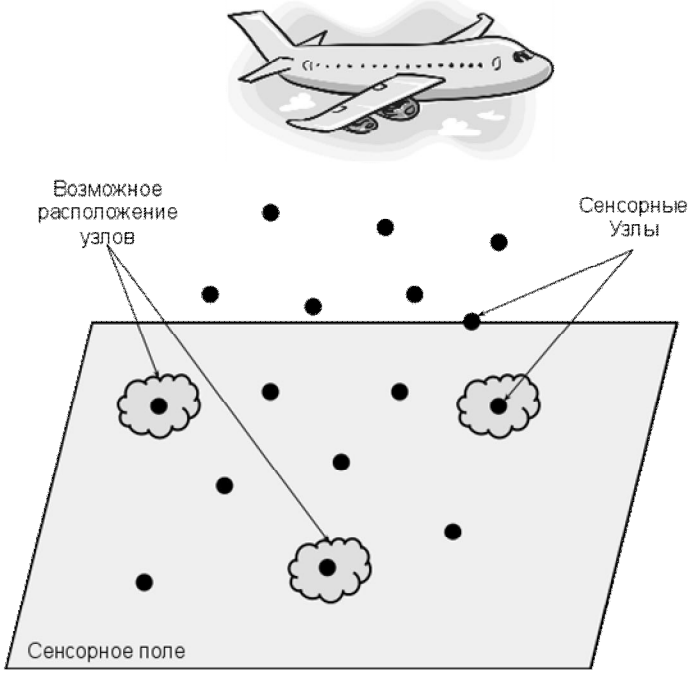


Рис.2.3. Пример сенсорной сети, в которой сенсорные узлы размещаются случайным образом.

Статичность или мобильность. Беспроводные сенсоры могут быть статичными или мобильными. Сенсорная сеть может быть построена как на основе первых, так и вторых, а также любой их комбинации.

Необходимость совместного функционирования автономных узлов, зачастую недоступных для замены, адаптация к динамически изменяемым условиям внешней среды и задачам являются фундаментальными направлениями для исследовательских работ в области беспроводных сенсорных сетей так же, как и решение проблем динамически изменяющейся топологии или требований по низкому энергопотреблению. Конфигурация сенсорной сети должна иметь возможность видоизменяться (самоорганизующаяся сеть) в зависимости от текущего положения в пространстве, возможностей электропотребления, деталей решаемых задач. Поскольку сенсорные узлы взаимодействуют с окружающей средой, они должны иметь возможность динамически приспосабливаться к решению конкретной задачи. Мобильность узлов, их отказы, критичные изменения во внешней среде требуют высокой степени динамичности от сенсорной сети в целом. Поэтому, топология конкретной сенсорной сети или её части может изменяться многократно в течение срока её функционирования. Фрагменты беспроводной сенсорной сети в связи с этим нуждаются в современных алгоритмах, которые должны быть робастными и адекватными к изменяющимся условиям.

Сенсорные узлы конструируются так, чтобы потреблять как можно меньше энергии, поскольку они могут функционировать в

недружественной внешней среде и замена источника питания может быть невозможна как таковая. Поэтому, сенсорный узел может выйти из строя как по причине критичной ситуации во внешней среде, так и вследствие потери возможности энергоснабжения. Отметим, что даже операционная система для сенсорных узлов разработана с учетом требований по минимальному энергопотреблению [198]. Однако, как уже отмечалось выше, сенсорная сеть содержит тысячи сенсорных узлов и наиболее важным свойством сенсорной сети в целом должно быть выполнение сетью своих функций даже при выходе из строя какого-то максимально возможного числа сенсорных узлов. В соответствии с изложенным, необходимо создавать такие алгоритмы управления сенсорными узлами, чтобы минимизировать энергопотребление. Число пакетов информации, передаваемых, принимаемых, обрабатываемых каждым сенсорным узлом должно быть таким, чтобы расход энергии был минимизирован.

Другой проблемой при построении беспроводных сенсорных сетей является то, что расстояние, на которое сенсорный узел передаёт информацию, может быть существенно меньше, чем в традиционных радиосистемах. Мощность передатчика должна быть мала (это способствует и низкому энергопотреблению) и архитектура беспроводной сенсорной сети должна тогда представлять собой сеть с распределёнными интеллектуальными ресурсами. Такие сети, как уже выше отмечалось, относятся к самоорганизующимся. Распространенным примером

самоорганизующихся сетей служат сети MANET (Mobile Ad Hoc Network).

2.2. Отличия USN и MANET.

Рассмотрим основные соответствия и отличия для обоих классов сетей [61,99,100,146].

Сети USN и MANET подобны в следующем:

- обе являются распределёнными не инфраструктурными беспроводными сетями,
- маршрутизация между узлами может быть многоранговой (multi-hop),
- узлы обеих сетей как правило питаются от батарей и, следовательно, необходимы усиленные меры по энергосбережению,
- обе сети используют радиоканалы в не лицензируемом спектре, что может приводить к интерференции с техническими средствами других радио технологий,
- самоуправление необходимо вследствие распределённой природы обоих классов сетей.

Сети USN и MANET отличаются следующими характеристиками следующим:

- узлы MANET всегда существуют во взаимодействии с человеком (например, Лаптоп, PDA, мобильный терминал и т.д.), в то время как сенсорные узлы

ориентированы на взаимодействие не с человеком, а с окружающей средой,

- сенсорные узлы как правило интегрированы в окружающую среду для сбора информации, в то время как узлы MANET - как мобильные станции,
- число узлов в сенсорных сетях так же, как и их плотность во много раз больше, чем в MANET,
- вследствие особенностей применения беспроводных сенсорных узлов, например, для контроля за вулканической деятельностью или за пожарами, частота выхода из строя узлов USN (в зависимости от приложения) может быть существенно выше, чем в MANET, что приводит к необходимости наличия гибких механизмов реконфигурации сети,
- в отдельных случаях сенсорные узлы должны быть мобильными, но в большинстве приложений они статичны, в отличие от MANET,
- для ряда приложений вместо идентификатора индивидуального сенсорного узла (например, адреса) реальное местоположение является более важным атрибутом, что подчеркивает целевую направленность сенсорной сети на решение задач определенного приложения,
- USN зачастую рассчитаны на вполне определённого пользователя сети, возможно, единственного (например, оператор сети по сбору информации о климатических

условиях в теплице), в то время как MANET является многопользовательской сетью,

- узлы MANET как правило находятся непосредственно у человека или близко к нему и, естественно, достаточно просто перевести их в режим сохранения энергии, в то время как для узлов USN это действия должно осуществляться без участия человека. Сравнение соответствий и различий MANET и USN показывает необходимость разработки для USN специальных протоколов и алгоритмов для обеспечения функционирования беспроводной сенсорной сети.

Как уже отмечалось выше, беспроводные сенсорные сети могут использоваться повсеместно. Рассмотрим далее для примера ряд приложений беспроводных сенсорных сетей:

Наблюдения за внешней средой. Сенсорные сети могут быть использованы для мониторинга изменения климата [37], пожароопасности в лесных массивах, контроля температуры, влажности, освещённости в сельском хозяйстве и т.д. Выше для примера был приведен рис.1.11, характеризующий области применения беспроводных сенсорных сетей. Ниже конкретизируем ряд из них.

Военный мониторинг. На рис. 2.4. приведён пример использования сенсорных сетей в военной области.

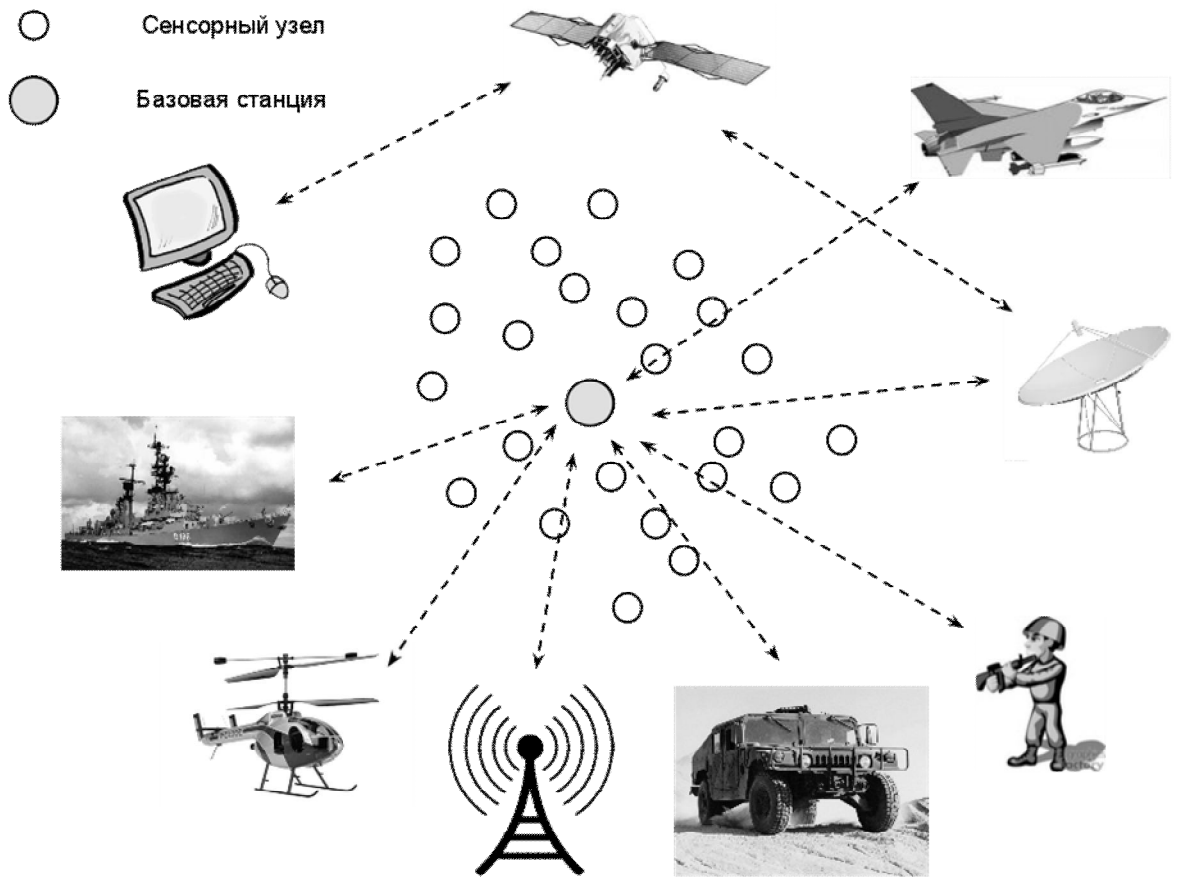


Рис.2.4. Пример использования сенсорной сети в военной области.

Мониторинг зданий. Достаточно важные задачи по мониторингу жилого фонда, систем водоснабжения и т.д. составляют значительную часть приложений сенсорных сетей.

Контроль здоровья. Сенсорные узлы могут размещаться не только в зданиях, в лесах и т.д., но и на и в теле человека и иных биомасс. Одно из новых важнейших приложений сенсорных сетей получило название MBAN (Medicine Body Area Network) и изучается в рабочей группе IEEE 802.15.6 [144,145]. В главе 8 будут достаточно подробно рассмотрены разрабатываемые этой группой стандарты.

Список приложений можно было бы продолжить, но уже рассмотренных вполне достаточно для того, чтобы сформировать архитектуру беспроводной сенсорной сети, изображенную на рис. 2.5. Для связи с сетью связи общего пользования (NGN, Internet) используется шлюз, поскольку в настоящее время в сенсорных сетях для взаимодействия сенсорных узлов в основном применяется специальный энергосберегающий протокол Zig Bee, не относящейся к категории TCP/IP протоколов.

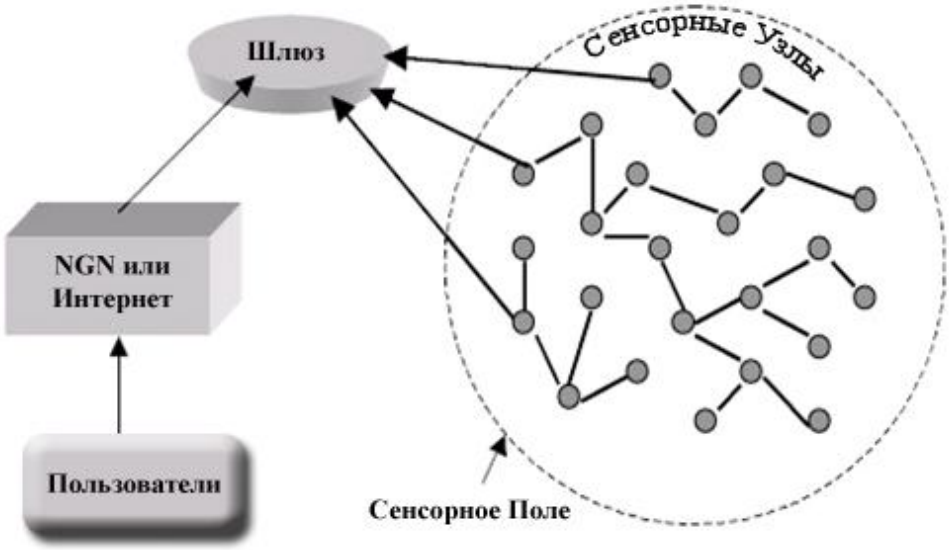


Рис.2.5. Архитектура сенсорной сети.

2.3. Кластерная организация сенсорных сетей.

Кластерная организация считается эффективной и масштабируемой для решения подобных задач, но лишь при условии рационального выбора головного узла в кластерной сети в конкретный момент времени [95,194,211]. Действительно, являющийся головным в момент времени t_1 сенсорный узел не обязательно должен быть им же в момент времени t_2, ибо существующий головной узел уже может затратить достаточно

большое количество энергии на передачу сообщений от всех сенсорных узлов кластера к моменту времени t_2. Поэтому, в момент времени t_2 головным узлом в кластере может быть назначен и иной сенсорный узел, сохранивший к этому времени наибольший энергетический запас.

Одним из самых известных механизмов, обеспечивающих функционирование сенсорных сетей и выбор головных узлов, является алгоритм LEACH (Low Energy Adaptive Cluster Hierarchy) [104]. Алгоритм LEACH предусматривает вероятностный выбор сенсорного узла на роль головного в начале функционирования сенсорной сети, а впоследствии ротацию на основе энергетических характеристик сенсорных узлов. Подобное решение, естественно, продлевает длительность функционирования сенсорных узлов и сети в целом, но, как будет показано далее по результатам моделирования, не решает задачи обеспечения лучшего покрытия в течение достаточно длительного времени. И, это, в общем-то, естественно, поскольку при создании LEACH такая задача и не ставилась.

Существует достаточно много алгоритмов, которые в той или иной степени пытаются улучшить LEACH. Это и алгоритмы, основанные на максимуме остаточной энергии, местоположении узла-кандидата в головной кластерный узел по отношению к другим узлам, информации о топологии сети в текущей момент времени. Алгоритм HEED (Hybrid Energy – Efficient Distribution) [210] использует гибридный критерий для выбора головного узла на основе анализа остаточной энергии и расположения

близлежащих узлов. Все эти алгоритмы направлены, как и LEACH, в первую очередь на максимизацию длительности функционирования сенсорных узлов и сети в целом.

Однако с развитием сенсорных сетей появились и другие задачи, требующие пристального внимания. Например, задача о качестве обслуживания, которое является важнейшей метрикой для любой сети, в том числе и сенсорной. Действительно, очень важна проблема увеличения срока жизни сенсорной сети. Однако, если эта сеть не будет выполнять свои функции в требуемом объеме, то и сама задача увеличения срока жизни сенсорной сети, не удовлетворяющей требованиям по качеству обслуживания, схоластична.

В системах мониторинга одним из важнейших требований является его непрерывность, т.е. обеспечение мониторинга параметров на всем пространстве или процессе. Исходя из сказанного, необходимо разработать такой алгоритм выбора головного узла кластера, который обеспечивал бы лучшее покрытие заданной для мониторинга области двумерного пространства (плоскости) в течение достаточно длительного периода времени. Этот подход означает, в целом, оптимизацию как срока жизни сенсорной сети, так и оптимизацию выполнения сенсорной сетью своих функциональных задач с заданным качеством обслуживания в течение достаточно длительного периода времени.

Далее в книге будут рассмотрены примеры создания новых алгоритмов выбора головного узла в беспроводных сенсорных сетях и требуемая при этом математическая база и инструментарий моделирования.

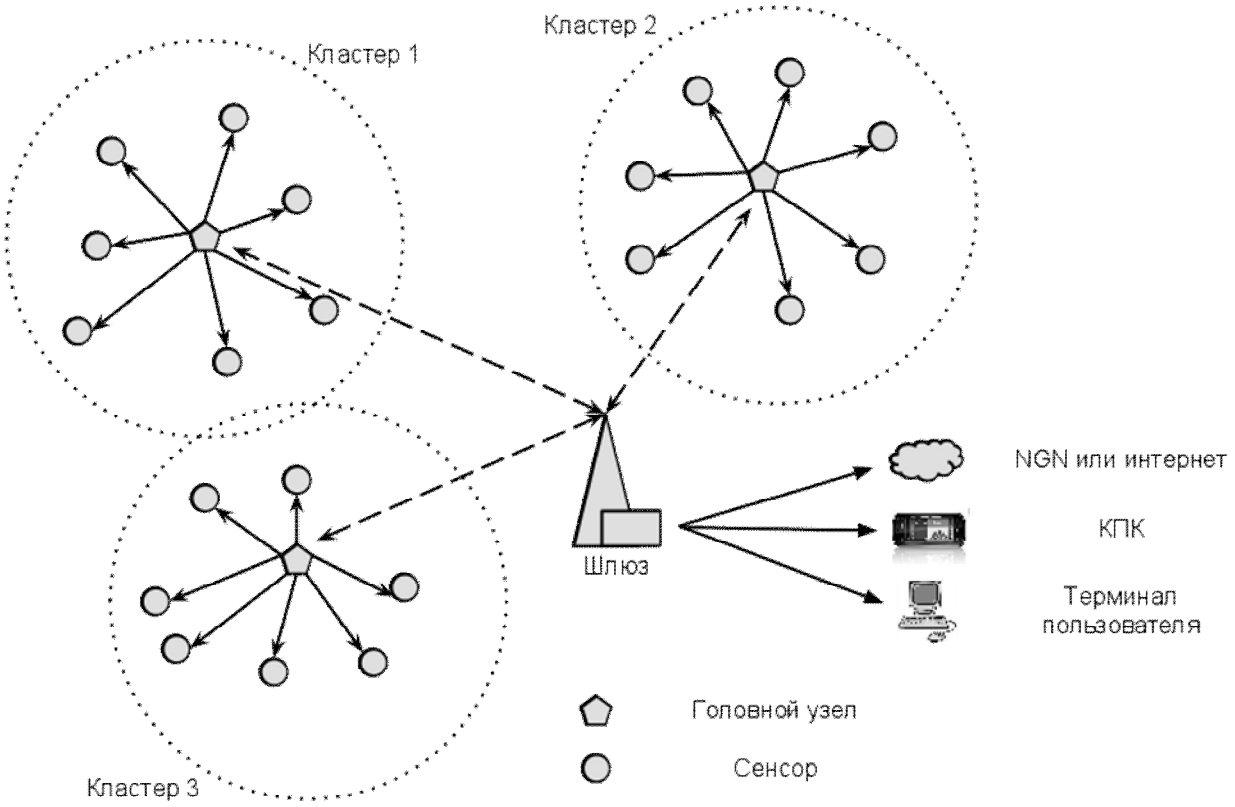


Рис.2.6. Кластерная архитектура USN.

2.4. Требования к алгоритмам маршрутизации в USN.

Поскольку сенсорная сеть может не иметь постоянной инфраструктуры, вряд ли возможно использовать классические алгоритмы маршрутизации для сенсорных сетей. Кроме того, в USN трафик данных может быть сгенерирован так, что одна и та же информация может быть представлена в сети от различных сенсорных узлов, функционирующих в какой-либо зоне. Поскольку размеры сенсоров и затраты на них лимитированы так же, как и их ресурсы: энергия, память, вычислительные возможности –

передавать одну и ту же информацию по сети от многих сенсорных узлов нецелесообразно.

Поэтому при разработке алгоритмов маршрутизации в беспроводных сенсорных сетях должны учитываться следующие факторы:

Самоорганизация. Сенсорные сети должны иметь возможность самоорганизации. Исходя из этого, вычислительные возможности, возможности обеспечения связи, управление возможности должны быть достаточными для обеспечения автономного существования.

Энергетическая эффективность. Сравнивая прогресс в области производства процессоров, памяти и т.п., можно отметить, что в производстве источников питания, к сожалению, этот прогресс не так заметен. Сенсорные узлы проектируются как правило с обеспечением питания от батарей и, соответственно, срок их жизни в первую очередь определяется системой электропитания. Достаточно часто источник энергии не может быть восполнен, поскольку сенсорные узлы могут быть размещены в недоступных для человека местах. Минимизация энергопотребления – одна из важнейших исследовательских задач в области беспроводных сенсорных сетей.

Гибкость. Алгоритмы в сенсорных сетях должны обладать достаточной гибкостью для того, чтобы они могли адаптироваться к различным приложениям USN. Условия функционирования различных приложений, окружающая среда и возможности самого

сенсорного узла изменяются в широких пределах. Хотя некоторые условия и могут быть предварительно спрогнозированы или даже определены перед созданием сети, топология сети может многократно изменяться в процессе функционирования USN вследствие введения новых узлов, отказов существующих, критичных изменений внешней среды. Все эти возможности должны быть учтены при разработке алгоритмов для беспроводных сенсорных сетей.

Масштабируемость. В беспроводных сенсорных сетях число сенсорных узлов в зависимости от решаемой задачи может изменяться от нескольких сотен до тысяч. Не случайно, в спецификациях Zig Bee число сенсорных узлов, расположенных в одной зоне, может достигать 64000. Сети большого масштаба и высокой плотности с лимитированной полосой пропускания должны к тому же предоставлять услуги с определённым уровнем качества обслуживания. Поэтому, много работ посвящено проблемам эффективного управления скоростью передачи и организации расписания для передачи информации.

Толерантность к отказам. В отличие от традиционных сетей беспроводные сенсорные сети случайным образом строятся и взаимосвязи сенсорных узлов в них также случайны во времени. Сенсорные узлы могут выходить из строя вследствие недостаточного уровня электропитания, возникновения критических условий во внешней среде, выхода из строя аппаратной части и т.д. Если вышло из строя несколько сенсорных узлов, это еще не должно означать существенных последствий не

только для сенсорной сети в целом, но и для её фрагментов. Другими словами, USN должна быть нечувствительна к отказу какого-либо сенсорного узла и должна далее поддерживать требуемый уровень качества обслуживания.

Точность и латентность. Обеспечение достаточной точности и информации в реальном времени – одна из важнейших задач для множества приложений USN. Алгоритмы должны гарантировать, что данные будут переданы через беспроводную сенсорную сеть в соответствии с требуемым временем и точностью. Идеальный алгоритм должен обеспечить своевременную передачу информации с заданной точностью и с минимальными энергозатратами.

2.5. Классификация алгоритмов маршрутизации в USN.

Многие исследователи предлагали различные решения по алгоритмам маршрутизации для USN с учётом требуемых особенностей, изложенных выше. Предложенные алгоритмы маршрутизации в USN могут быть объединены в различные группы в соответствии с критериями, разработанными в [60,71]. В таблице 2.1 показана простая классификация алгоритмов маршрутизации в USN с использованием типового подхода. В фокусе интересов нашего исследования далее рассмотрим более подробно схемы одноуровневой и иерархической маршрутизации для сети USN.

В одноуровневой сети все узлы играют одинаковую роль и обладают одинаковой функциональностью. Собранные данные передаются в сеть посредством многоранговой маршрутизации как это показано на рис.2.7. Алгоритмы в одноуровневой сети должны

обеспечить передачу большой транзитной информации через сеть и, естественно, они являются ориентированными на приложения. В основном, алгоритмы для одноуровневой сети являются централизованными, поскольку, как уже выше отмечалось, их основная задача состоит в обеспечении транзита данных через однородную сенсорную сеть. Во многих случаях алгоритмы для одноуровневой сети достаточно сложны, поскольку существуют как масштабность, так и динамическое изменение топологии USN. SPIN (Sensor Protocols for Information via Negotiation) [103] и DD (Direct Diffusion) [131] алгоритмы являются базовыми для одноуровневой беспроводной сенсорной сети, на основе которых разработаны все последующие одноуровневые алгоритмы.

В иерархических сетях сенсорные узлы играют различную роль и появляются две категории сенсорных узлов: головной кластерный узел (CH – Cluster Head) и члены кластера. Более высокий уровень сенсорных узлов собирает информацию от членов кластера и управляет более низким уровнем. После агрегации данных, узлы более высокого уровня направляют её при необходимости на следующий уровень. Для примера на рис.2.7 показана трехуровневая иерархическая беспроводная сенсорная сеть. Головные узлы кластеров взаимодействует с узлами сети связи общего пользования, изображёнными на рис.2.7 в виде базовых станций. Каждый головной узел кластера собирает данные с узлов своего кластера, агрегирует их и передаёт далее. Все иерархические алгоритмы маршрутизации помогают в выборе наилучшего CH и кластеризация узлов осуществляется на основе

принципа минимизации расхода энергии. Поскольку головные узлы кластера ответственны за сбор, агрегацию и передачу данных на достаточно большие расстояния, они должны быть в большей степени энергетически независимыми, чем просто члены кластера. Алгоритмы выбора головного кластерного узла предусматривают ротацию и переназначение головного узла кластера периодически в зависимости от распределения нагрузки в целом по беспроводной сенсорной сети.

Таблица 2.1. Простая классификация алгоритмов маршрутизации.

Критерий	**Категория**	**Примеры**
Сетевая структура	Одноуровневая	SPIN [103]
	Иерархическая	LEACH [104]
Знания о ресурсах	На основе остаточной энергии	HEED [210]
	На основе точности расположения	Directed Diffusion [131]
Управление протоколами	Централизованное	SPIN [103]
	Географическое	GFG [131]

	На основе QoS-	SAR [193]
	На основе теории очередей	COUGAR [208]

Сравнивая одноуровневые и иерархические алгоритмы маршрутизации, можно отметить, что иерархические алгоритмы представляют больше возможностей по продвижению различных приложений USN. Следующие характеристики иерархических алгоритмов были отмечены в исследовательских работах [60,71,210]:

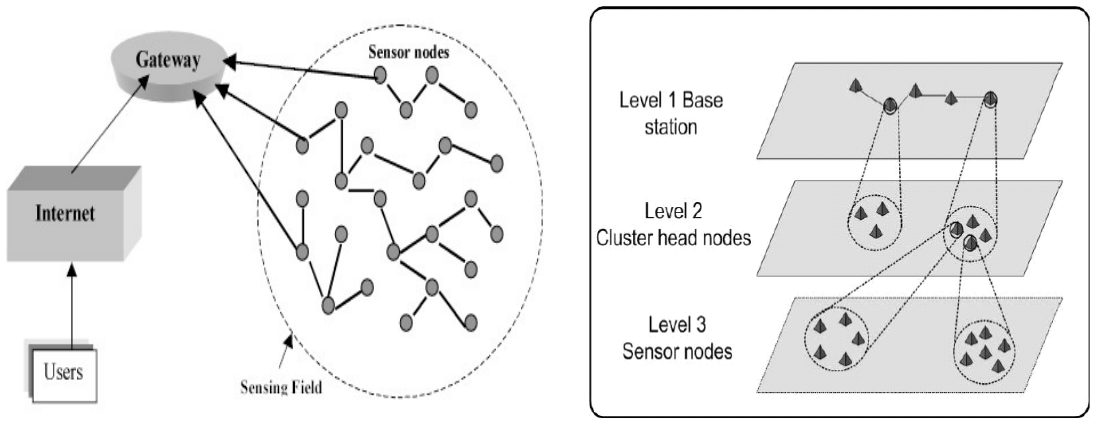


Рис. 2.7. Типовые архитектуры USN.

- **Иерархическая маршрутизация в сети является эффективным путём для снижения энергозатрат.** Действительно, управление со стороны головного узла кластера членами кластера снижает нагрузку на членов кластера (в каждый момент времени энергию затрачивают

только активные узлы, транзит обеспечивается CH). За счёт агрегации данных головной узел кластера уменьшает поток заявок во внешнюю сеть.

- **Иерархическая маршрутизация позволяет гибко решать различные задачи с учётом возможностей сенсорных узлов.** Иерархическая маршрутизация позволяет балансировать нагрузку сети. При этом, узлы с высокой энергоёмкостью (возможно с постоянным энергоснабжением) могут агрегировать данные и передавать их в сеть связи общего пользования, в то время как узлы с низкой энергоёмкостью могут использоваться исключительно для сбора данных.
- **Иерархическая маршрутизация позволяет достаточно просто реализовать расписание и избежать коллизий.** Члены кластера под управлением головного узла могут следовать вполне определённому расписанию для передачи, приёма и чтения информации. Следовательно, сенсорные узлы могут расходовать меньше энергии, находясь в состоянии покоя и активизируясь только в момент их временного интервала для передачи, приёма и чтения информации. В результате, естественно, снижаются коллизии в кластере, и сеть может обслужить более высокую нагрузку. Иерархическая маршрутизация в связи с этим часто используется для масштабных беспроводных сенсорных сетей, состоящих из сотен и тысяч узлов.

- **Иерархическая маршрутизация позволяет использовать достаточно простые схемы маршрутизации.** Хотя одноуровневая маршрутизация может использовать оптимальные маршруты, её реализация достаточно сложна. Небольшие возможности сенсорных узлов при этом могут стать проблемой для реализации сложных алгоритмов и схем. Иерархическая маршрутизация предполагает разделения соединений на внутри кластерные и внешние. Только головной узел кластера отвечает за внешние соединения, в то время как члены кластера взаимодействуют только на внутри кластерном уровне. Такая простая маршрутизация уменьшает число сообщений в кластере.
- **Иерархическая маршрутизация позволяет более просто осуществить рассылку запросов, чем одноуровневая.** Когда, например, из внешней сети или со стороны шлюза, необходимо разослать запрос, этот запрос направляется только к головным узлам кластеров. Головной же узел каждого кластера рассылает далее запрос членам кластера с учётом возможностей и необходимости. Такой подход также позволяет уменьшить число сообщений.

Хотя иерархическая маршрутизация обладает и недостатками, такими как необходимость времени на синхронизацию, бóльший заголовок для кластерного управления, не оптимальная маршрутизация, тем не менее с учетом выше изложенного иерархическая маршрутизация является предпочтительной для построения USN, особенно масштабных.

2.6. Существующие алгоритмы выбора головного узла.

В соответствии с вышеизложенным в книге далее будут проведены исследования по разработке новых алгоритмов для иерархических беспроводных сенсорных сетей. Основной проблемой при создании алгоритмов для иерархических беспроводных сенсорных сетей является выбор головного узла кластера. Существует два подхода к выбору головного узла кластера: случайный выбор головного узла и предопределённый выбор головного узла. Рассмотрим далее алгоритм случайного выбора головного узла, при использовании которого ротация головных узлов может производиться из всех членов кластера с учётом их характеристик в текущий момент времени.

2.6.1. Алгоритм случайного выбора головного узла LEACH.

Иерархический алгоритм адаптивной кластеризации с низким потреблением энергии LEACH (Low-Energy Adaptive Clustering Hierarchy) [104] предполагает обеспечение баланса расхода энергии в беспроводной сенсорной сети. Алгоритм LEACH является базовым и существует много алгоритмов, основанных на нём. Базовая идея LEACH состоит в следующем: сенсорные узлы могут быть случайным образом выбраны как головные на основе предыдущей информации об их функционировании. При этом, в кластере каждый сенсорный узел генерирует случайное число от 0 до 1. Каждый сенсорный узел имеет порог T_h (LEACH), который соответствует предварительно определённому числу головных сенсорных узлов в сети. Если интегрированное случайное число меньше, чем T_h (LEACH), то сенсорный узел может стать

головным; в противном случае этот узел остаётся только членом кластера. Вычисление T_h (LEACH) является ключевой задачей при реализации алгоритма LEACH.

$$Th(LEACH) = \begin{cases} \dfrac{p}{1 - p \times (r \times \mathrm{mod}\dfrac{1}{p})} & if \quad n \in G \\ 0 & otherwise \end{cases} \qquad (2.1)$$

В (2.1) P – предопределенный процент головных узлов среди всех сенсорных узлов. Оптимальное значение P оценивается в 5% от общего числа сенсорных узлов.

Текущий интервал функционирования сенсорной сети определяется как r, G – число сенсорных узлов, которые не были выбраны головными за последние 1/p интервалов. Это уравнение определяет тот факт, что узел, который был головным в последних интервалах функционирования сенсорной сети, не имеет шансов вовсе или имеет минимальные шансы снова стать головным в рассматриваемом интервале. В результате, такой выбор головного узла способствует балансу энергетических возможностей каждого из сенсорных узлов сети. Кроме того, при выборе головного узла другие сенсорные узлы выбирают одного из членов кластера для осуществления контроля за мощностью получаемого сигнала (RSS – Received Signal Strength) от головного узла.

После того, как кластер сформирован, головной узел широкополосным способом рассылает расписание передачи и запрашивает своих членов кластера о передаче данных на основе известного TDMA подхода. В последующих фазах головной узел

является ответственным за агрегирование данных и передачу их на шлюз и в сеть связи общего пользования. Весь сбор данных локализуется в кластере. После определённого времени нахождения в стабильной фазе, сеть снова переходит в стадию формирования. При этом, следует отметить, что стадия формирования существенно короче, чем стабильная. В связи с этим, LEACH имеет достаточно короткий заголовок.

LEACH является очень эффективным алгоритмом. С его помощью достигается снижение энергозатрат в 7 и более раз по сравнению с прямым взаимодействием сенсорных узлов и от 4 до 8 раз по сравнению с другими алгоритмами маршрутизации [104]. В то же время LEACH не даёт гарантий по выбору «хорошего» сенсорного узла в качестве головного узла кластера. Поскольку в алгоритме LEACH нет предположения о текущем энергетическом состоянии сенсорного узла, то в качестве головного может быть выбран давно не избираемый член кластера с неудовлетворительными энергетическими характеристиками.

2.6.2. Алгоритм с предопределённым выбором головного узла HEED.

Гибридный распределённый энергоэффективный алгоритм кластеризации (HEED – Hybrid Energy – Efficient Distributed) [210] является развитием алгоритма LEACH. Для преодоления проблемы выбора «плохого» члена кластера в качестве головного узла в LEACH, алгоритм HEED предлагает использовать предопределённый выбор головного узла. В алгоритме LEACH,

когда предполагается, что каждый член кластера имеет равновероятные шансы стать головным узлом кластера, сеть может выбрать в качестве головного узел, который будет иметь наихудшие показатели по энергосбережению и, соответственно, по возможности выхода из строя. Алгоритм HEED ставит вероятность выбора узла головным в зависимости от его существующей энергоспособности, и решение принимается в зависимости от энергетических затрат. Кроме того, алгоритм HEED учитывает многоранговую природу взаимосвязей в беспроводных сенсорных сетях для дальнейшего энергосбережения.

HEED использует информацию о текущей энергоёмкости сенсорного узла как основной параметр для выбора члена кластера в качестве головного узла. Выбранный в качестве головного узел информирует близлежащие узлы о том, что он стал головным. Эти сообщения от головных узлов используются сенсорными узлами для выбора себе наилучшего головного узла и, соответственно, кластера. В случае, если головной узел кластера находится достаточно далеко от шлюза с сетью связи общего пользования, он может передать агрегированную информацию через головной узел другого кластера.

2.6.3. Алгоритм случайного выбора головного узла ERA.

Алгоритм осведомлённости об остаточной энергии (ERA – Energy Residue Aware) [82] представляет собой ещё один алгоритм иерархической маршрутизации. Алгоритм ERA также является развитием алгоритма LEACH и включает в анализ вопроса выбора

головного узла в кластере затраты на осуществление взаимодействия. Затраты на осуществление взаимодействия включают в себя остаточную энергию головного узла кластера ($E_{CH\text{-}rem}$), затраты энергии на взаимодействие головного узла с базовой станцией (E_{toBS}), затраты энергии на взаимодействие членов кластера с головным узлом (E_{toCH}). В этом состоит принципиальная разница с алгоритмом HEED: алгоритм ERA использует ту же схему выбора головного узла, что и LEACH (случайный выбор), но обеспечивает лучший выбор головного узла за счёт использования дополнительных параметров, определённых выше. Уравнения (2.2) помогают определять затраты кластера при выборе того или иного узла в качестве головного и найти головной узел кластера с максимальной остаточной энергоёмкостью. В (2.2) множество S_c является множеством для головных узлов, множество S_N является множеством для членов кластера.

$$\begin{cases} (E_{CH-res})_i = (E_{CH-rem})_i - (E_{toBS})_i, & i \in S_c \\ (E_{nonCH-res})_j = (E_{nonCH-rem})_j - (E_{toBS})_{ji}, & j \in S_N, \forall i \in S_c \\ \max\{(E_{CH-res})_i + (E_{nonCH-res})_j \mid \forall i \in S_c\} & j \in S_N \end{cases} \qquad (2.2)$$

Алгоритм ERA может использоваться как для внутри кластерных, так и для межкластерных соединений.

2.6.4. Алгоритмы PEGASIS и иерархический PEGASIS.

Алгоритм PEGASIS (Power-Efficient Gathering Sensor Information Systems) – эффективная по мощности система сбора информации от сенсоров – не имеет прямого отношения к кластерной организации беспроводных сенсорных сетей, но будет

рассмотрен далее для полноты анализа основных алгоритмов маршрутизации в USN.

Алгоритм PEGASIS [147,148] nпредусматривает основанный на LEACH алгоритм организации сенсорных узлов в последовательную цепочку и периодическое обновление первого узла в цепочке так же, как это предусмотрено в кластерных USN. В алгоритме PEGASIS цепочка формируется таким образом, чтобы сенсорные узлы взаимодействовали только с ближайшими и только один из узлов являлся бы передающим информацию на базовую станцию в каждом из интервалов функционирования сенсорной сети. Для определения ближайших узлов каждый узел использует значение RSS для оценки расстояния до узла и затем выбирает значение мощности сигнала так, чтобы взаимодействовать только с ближайшими узлами.

Построение цепочки позволяет минимизировать расстояние, на которое передаётся информация, а ротация первого сенсора в цепочке увеличивает длительность функционирования отдельных сенсорных узлов. Такой подход позволяет для беспроводных сенсорных сетей снизить общее энергопотребление и увеличить длительность функционирования USN в целом.

Алгоритм PEGASIS лучше алгоритма LEACH от 100% до 200% в отношении гибели 1%, 25%, 50% и 100% узлов сенсорной сети и топологий [148]. Однако, цепочки алгоритма PEGASIS создают дополнительные задержки при передаче информации. Кроме того, динамическое изменение топологии в алгоритме

PEGASIS требует, чтобы каждый сенсорный узел знал об энергетических возможностях своих ближайших соседних узлов для вычисления маршрута передачи данных. Последнее существенно усложняет заголовок и помимо этого приводит к проблемам при функционировании сенсорной сети в условиях большой нагрузки.

Для снижения задержки был предложен иерархический алгоритм PEGASIS [147]. В этом алгоритме в качестве целевой функции для минимизации используется «энергия х метрика задержки». Алгоритм иерархический PEGASIS использует CDMA для кодирования сигналов и пространственное разделение сенсорных узлов. Алгоритм строится в виде иерархического дерева, причём каждый выбранный узел какого-либо уровня передаёт данные на узел верхнего уровня иерархии. Этот метод позволяет обеспечить параллельную передачу данных и уменьшить задержки сигналов до значений 0 (lgN), где N – число узлов.

2.6.5. Алгоритм RRCH.

Алгоритм циклической очерёдности выбора головного узла в кластере RRCH (Round-Robin Cluster Head) [154] предполагает формирование кластера только единовременно. После фиксации кластера для выбора головного узла в нём на протяжении его функционирования используется известный метод циклической очередности [42]. Так же, как и в LEACH каждый из членов кластера имеет возможность стать головным узлом, головной узел задаёт расписание для членов кластера и т.д.

С учётом простоты процесса формирования кластера, RRCH избегает потерь энергии при рекластеризации. Естественно, что с точки зрения энергетических параметров RRCH имеет при этом лучшие результаты, чем LEACH. Однако, жёсткая фиксация кластера приводит к тому, что в целом один из кластеров может перестать выполнять свои функции с надлежащим качеством обслуживания быстрее, чем в LEACH, в котором как раз рекластеризация и приводит к возможности распределить ресурсы равномерно между всеми кластерами одной сенсорной сети.

Отметим, что в целом проблеме качества обслуживания при использовании тех или иных алгоритмов маршрутизации в беспроводных сенсорных сетях до последнего времени не уделялось должного внимания. И, это естественно, поскольку проблема состояла, в основном, в создании сенсорных сетей. В настоящее же время рынок сенсорных сетей растет настолько интенсивно, что уже в этом году его объём превысит 50 млрд. $ [34]. Повсеместное и масштабное применение сенсорных сетей, в том числе для задач мониторинга климата в целом, параметров окружающей среды и т.д. ставят задачу обеспечения качества обслуживания в сенсорных сетях как одну из важнейших.

Исходя из сказанного, разработка новых алгоритмов для выбора головного узла в беспроводных сенсорных сетях в настоящее время должна проводиться с учётом требований по качеству обслуживания. В последующих главах будет рассмотрен ряд новых алгоритмов выбора головного узла в беспроводных

сенсорных сетях, разработанных в Санкт-Петербургском Университете Телекоммуникаций.

3. Централизованный алгоритм выбора головного узла для гомогенных USN

3.1. Диаграммы Вороного.

В главе представлены результаты разработки алгоритма выбора головного узла CHS (Cluster Head Selection), который имеет лучшие характеристики, чем базовый алгоритм LEACH. Алгоритм основан на методах вычислительной геометрии и, поэтому, глава начинается с анализа возможностей диаграмм Вороного для обеспечения выбора головного узла в кластере.

Диаграммы Вороного [74], также известные как мозаики Дирихле, представляют собой фундаментальную структуру данных в вычислительной геометрии. Рассмотрим сначала особенности диаграмм Вороного как геометрической конструкции.

3.1.1. Выпуклая оболочка

Подмножество A плоскости является выпуклым, если для любых двух точек $p,q \in A$ линейный сегмент p, q содержится в A целиком. Выпуклая оболочка $COH(A)$ множества A является наименьшим выпуклым множеством, содержащим A. Любые две несовпадающие точки $p=(p_x, p_y)$ и $q=(q_x, q_y)$, определяемые двумя оболочками полуплоскостей hh_{pq} и hh_{qp} тогда определяются следующим образом:

$$hh_{pq} = \{r = (r_x, r_y) \in R^2 \mid Det(p,q,r) \geq 0\} \qquad (3.1)$$

Определитель *Det(p,q,r)* задается как:

$$Det(p,q,r) = \begin{vmatrix} 1 & p_x & p_y \\ 1 & q_x & q_y \\ 1 & r_x & r_y \end{vmatrix} \tag{3.2}$$

Пусть S – конечное множество различных точек R^2. Тогда можно определить *COH(S)* как пересечение оболочек полуплоскостей. Более того, *COH(S)* равно пересечению этих полуплоскостей, определённых точками в множестве S таким образом, что оно содержит все точки множества S:

$$COH(S) = \bigcap_{p_i p_j \in S} \left\{ h_{p_i p_j} : S \subset h_{p_i p_j} \right\} \tag{3.3}$$

Как непустое пересечение полуплоскостей, *COH(S)* является выпуклым многоугольником. Тогда можно представить этот многоугольник перечнем его последовательных вершин, расположенных по часовой стрелке. В этом случае *COH(S)* соответствует циклически определенному перечню точек из множества S.

3.1.2. Диаграммы Вороного

Рассмотрим множество $S = \{p_1, \ldots, p_n\}$ из n различных точек на плоскости. Ячейка Вороного или многоугольник Вороного $V(p_i)$ для точки $p_i \in S$ определяется как:

$$V(p_i) := \left\{ q \in R_2 : d(p_i, q) \le d(p_j, q), i \ne j \right\} \tag{3.4}$$

В (3.4) $d(p,q)$ - стандартная Евклидова метрика для точек p и q. Диаграмма Вороного $V(S)$ для множества S есть совокупность подмножеств из R^2, содержащих ячейки Вороного и все их пересечения. Граница ячейки Вороного содержит вершины Вороного и рёбра.

Точка $q \in R^2$ находится на ребре $e(p_i,p_j)$, если $d(q,p_i) = d(q,p_j)$ и $d(q,p_k) \geq d(q,p_i)$, при $k \neq i,j$.

Тогда $q \in R^2$ является вершиной Вороного, если она находится как минимум на двух рёбрах. Окружность C является пустой окружностью по отношению к S, если там нет точек из S внутри окружности.

Для любых трёх точек p_i,p_j, и p_k, которые не расположены на одной линии, существует единственная окружность C_{ijk}, проходящая через p_i,p_j, и p_k. Окружность C_{ijk} является окружностью Вороного, если она представляет собой пустую окружность. Начав с диаграммы Вороного $V(S)$, определим теперь граф Делоне $DG(S)$ на множестве S. Вершины графа $DG(S)$ являются точками множества S. Две вершины p_i и p_j, соединяются рёбрами в $DG(S)$, если существует ребро $e(p_i,p_j)$ положительной длины на диаграмме Вороного $V(S)$.

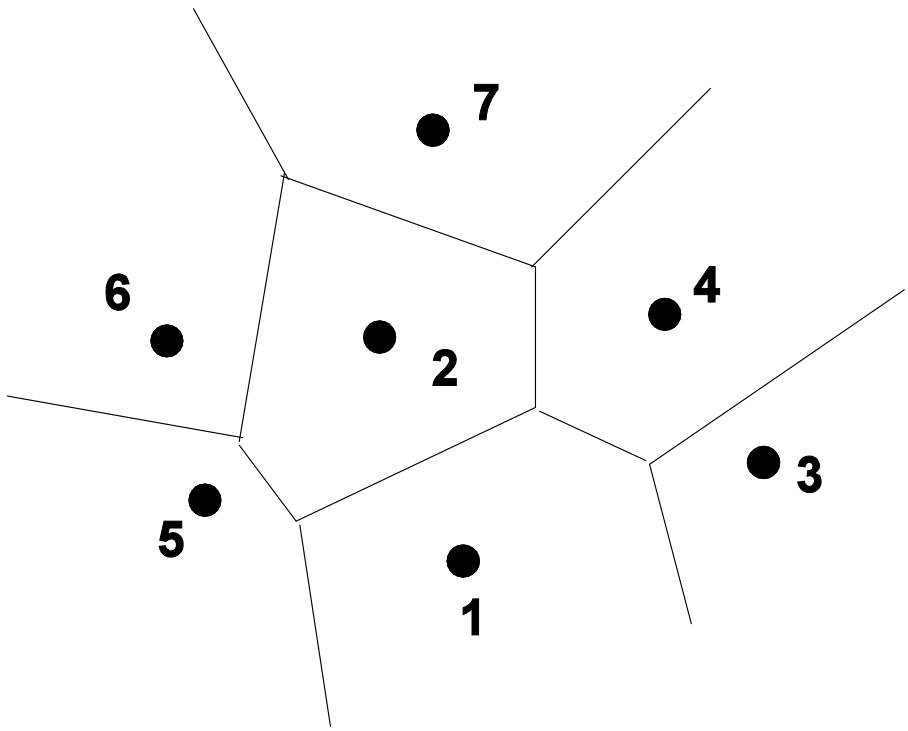


Рис. 3.1. Диаграмма Вороного для 7 точек.

Пусть *D(S)* прямая линия, принадлежащая графу *DG(S)* Делоне. Для точки из *S* множества *D(S)* представляет триангуляцию выпуклой оболочки *CH(S)*. Исходя из этого, прямая линия, принадлежащая графу *D(S)* Делоне, называется триангуляцией Делоне для множества точек *S*.

Пример триангуляции Делоне представлен на рис. 3.2.

Триангуляция Делоне *D(S)* дуальна с диаграммой Вороного *V(S)* в следующем: вершины диаграммы Вороного соответствуют триангуляции Делоне и в то же время ячейки Вороного соответствуют вершинам *D(S)*. В продолжении отметим, что эффект выпуклых оболочек и окружностей в триангуляции Делоне также легко может быть найден. Более того, для любого набора из трёх точек p_i,p_j, и p_k из множества *S* тогда следует, что p_i,p_j, и p_k

создают триангуляцию в $D(S)$, если и только если, окружность C_{ijk} является окружностью Вороного.

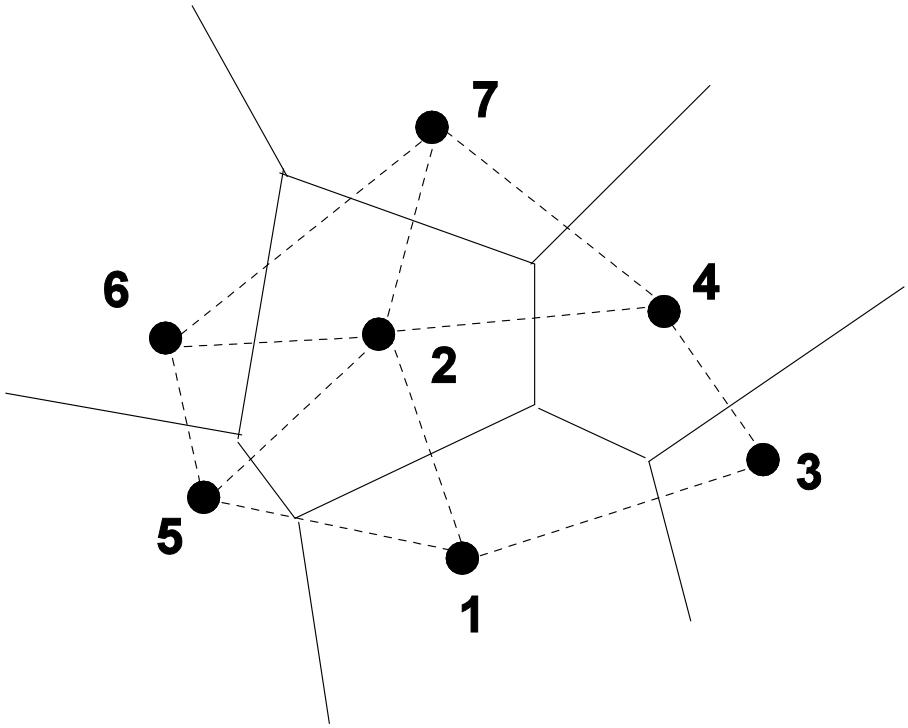


Рис. 3.2. Триангуляция Делоне.

3.2. Диаграммы Вороного для USN.

Беспроводные сенсорные сети являются гомогенными, если все их сенсорные узлы имеют одинаковые память, вычислительные возможности, мощность батареи, измеряемые параметры и телекоммуникационные возможности. В противном случае, сенсорные сети называются гетерогенными.

Областью покрытия (или областью детектирования) сенсора s_i в некотором сенсорном поле называется область, в которой любое событие из этого поля может быть детектировано сенсором s_i. Набор сенсоров $SN(s_i)$ является близлежащим к сенсору s_i, если все сенсоры этого набора размещены в области покрытия s_i. Сетевым

покрытием сенсора s_i в сенсорном поле является такая область, в которой сенсор s_i может обеспечивать взаимосвязь с любым сенсором этой области. Набор сенсоров $SN(s_i)$ является близлежащим к сенсору s_i, если все сенсоры этого набора размещены в области сетевого покрытия s_i.

Пусть $S = \{ s_1 ,..., s_n \}$ - конечное множество из n фрагментов на плоскости. Диаграмма Вороного для S, обозначаемая $Vor(S)$, является фрагментом плоскости, содержащий S в составе n ячеек $VC(s_i), 1 \leq i \leq n$ таких, что каждая ячейка Вороного включает только один фрагмент s_i, причём любая точка, расположенная в $VC(s_i)$ ближе к s_i, чем любой другой фрагмент в S.

На рис. 3.3 триангуляция Делоне (жирные линии) поверх диаграммы Вороного (пунктирные линии) представляет возможную беспроводную сенсорную сеть в виде выпуклого многоугольника. Конечные точки рёбер ячейки Вороного образуют вершины Вороного. Диаграмма Вороного для множества S является объединением ячеек Вороного для всех фрагментов, входящих в S. Триангуляция Делона, обозначенная далее $dt(S)$, дуальна с диаграммой Вороного. Граф $dt(S)$ имеет рёбра между двумя фрагментами, если и только если их ячейки Вороного имеют части ребра.

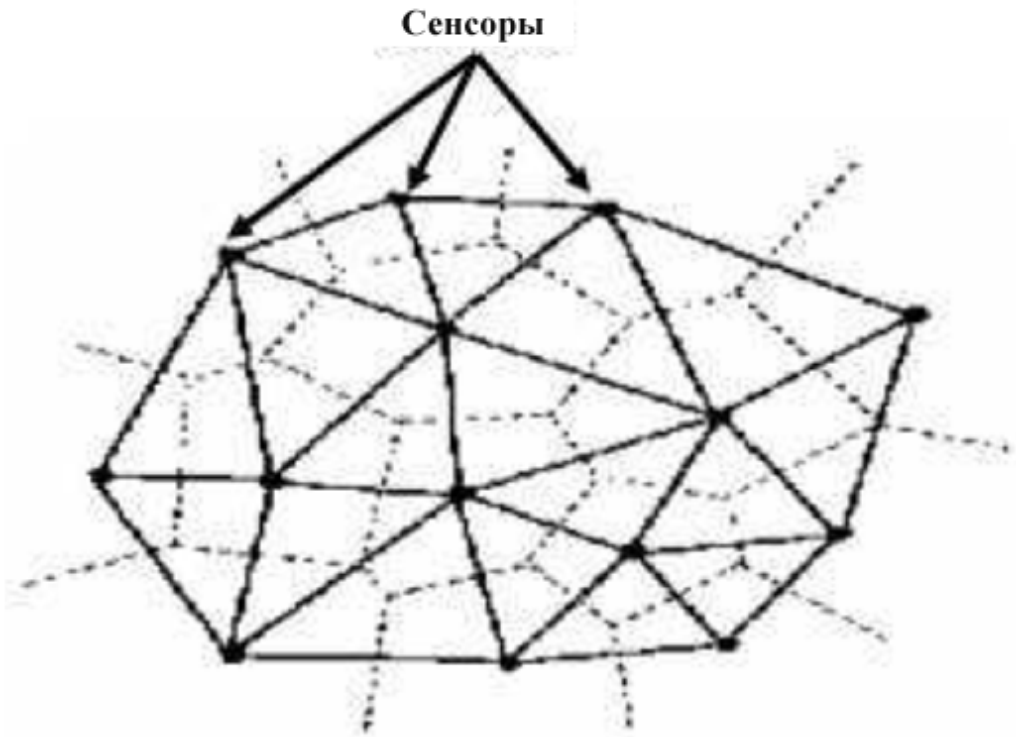


Рис. 3.3. Триангуляция Делоне поверх диаграммы Вороного для беспроводной сенсорной сети.

Некоторые теоремы по связности и покрытию для диаграмм Вороного будут полезны далее при разработке алгоритма выбора головного узла:

- Пусть r есть радиус покрытия сенсорной окружностью и $k \geq 3$. Выпуклая область А гарантирует k-покрытие, если точно k гомогенных сенсоров расположены в ней и если ширина А не превосходит r.
- Пусть $k \geq 3$. Пересечение k-покрытия сенсорными окружностями не пустое, если и только если пересечение любых трёх из этих k окружностей не является пустым. Иллюстрация к этой теореме приведена на рис.3.4.а.

- Пусть r есть радиус покрытия сенсорной окружностью и $k \geq 3$. Сенсорное поле является k-покрытым, если любой релеевский треугольник [104], области шириной r в сенсорном поле включает в себя по крайней мере k активных сенсорных узлов.
- Пусть $k \geq 3$. Поле является гарантировано k-покрытым, если для любого фрагмента поля, в котором существует по крайней мере один смежный фрагмент, такое пересечение (линза) содержит по крайней мере k активных сенсоров (рис. 3.4b)

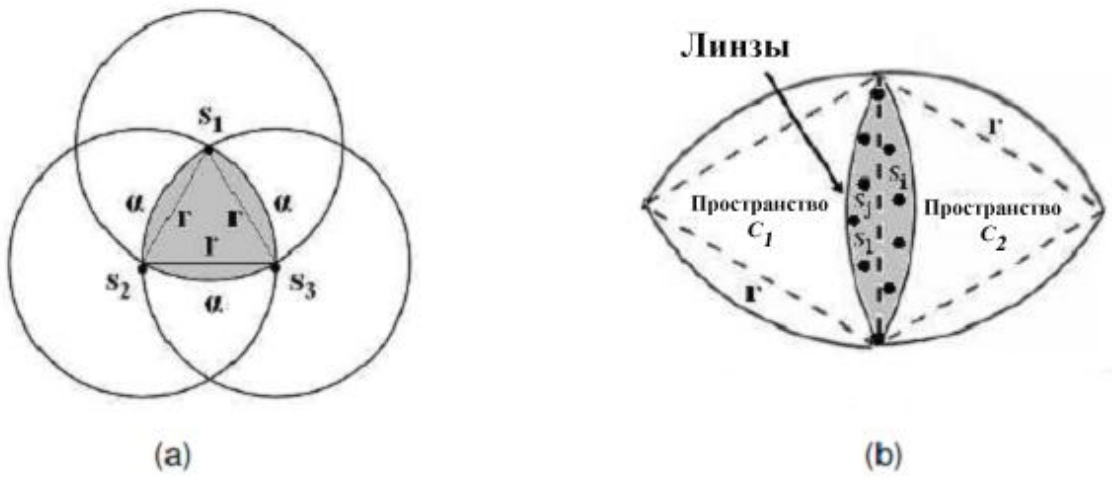


Рис. 3.4. Пересечение трех сенсорных окружностей (3.4.a) и смежные фрагменты поля (рис. 3.4.b).

Пусть все сенсоры имеют одинаковые покрытия и сетевое покрытие радиусов r и R соответственно. Тогда достаточно легко построить сеть, которая покроет заданное поле. Для этой цели предлагается структура сенсорного поля, разделённая на релеевские треугольники со стороной r, такие, что два смежных фрагмента пересекаются, сложенные как линзы. В результате получаем релеевскую решётку, изображённую на рис.3.5.

Централизованный алгоритм управления выбором головного узла кластера со стороны базовой станции имеет определенные преимущества, хотя и применим далеко не всегда. Действительно, базовая станция может обладать знанием о сенсорной сети в целом, в том числе о мощности сенсорных узлов, вычислительных возможностях, памяти и т.д. В данном разделе будем полагать, что возможно осуществление передачи информации на базовую станцию от всех узлов, например, с использованием GPS передатчиков. Кроме того, будем считать, что сенсорные узлы не являются мобильными.

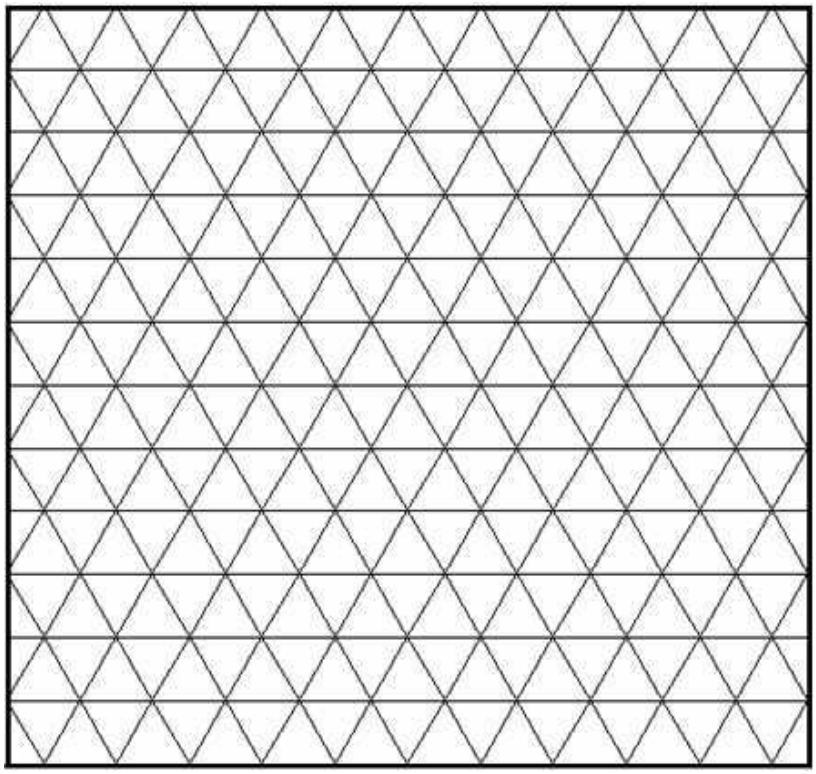


Рис. 3.5. Релеевская решётка для сенсорного поля

3.3. Выбор головного узла в кластере.

Начнём выбор головного узла с узлов, расположенных в трёх пересечениях заданного фрагмента сенсорного поля. При каждой

последующей итерации выбора будем проверять отобранные ранее сенсорные узлы с точки зрения покрытия выбранного фрагмента. Одновременно, будем увеличивать степень покрытия смежных фрагментов сенсорного поля. Будем повторять этот процесс до тех пор, пока не будут опробованы все фрагменты сенсорного поля. Предположим также, что каждый фрагмент сенсорного поля имеет уникальный идентификационный номер.

Выбор различных минимальных подмножеств активных сенсорных узлов будет производиться на основе фрагментов релеевской решётки. Поскольку схема выбора активных сенсоров основывается на пересечениях для всех фрагментов, важно, чтобы эти пересечения были определены во всём сенсорном поле и включали бы отдельные подмножества сенсоров в различных интервалах. Кроме того, необходимо, чтобы базовая станция генерировала фрагменты релеевской решётки случайным образом в каждом интервале времени.

3.3.1. Алгоритм выбора головного узла

Итак, базовая станция в каждом интервале случайным образом генерирует фрагмент решётки, которая содержит смежные повторяющиеся релеевские треугольники. Базовая станция случайным образом назначает для каждого кластера головной узел, который является ответственным за k-покрытие кластера в заданном интервале времени.

Каждый головной узел расположен в кластере и выбирает в качестве членов кластера близлежащие к нему с целью покрытия

фрагмента сенсорного поля. Базовая станция рассылает пакет, называемый «Перечень головных узлов» CHL (Cluster Head List), включающий идентификационные номера всех сенсорных узлов, выбранных головными. Когда сенсорный узел получает CHL, он проверяет номера *id*. Если в перечне есть его номер, то сенсорный узел удаляет его из CHL и передаёт далее уточнённый CHL. В противном случае, сенсорный узел транслирует пакет далее.

В таблице 3.1 приведён алгоритм CHS выбора сенсорного узла на основе диаграмм Вороного и триангуляции Делоне, реализованный с помощью релеевских решёток [36].

Таблица 3.1. Алгоритм выбора головного узла кластера CHS.

1:	**for** each round a slicing grid **do**
2:	$CHL = \{\}$
3:	**for** each cluster **do**
4:	Select s_i where s_i with six slices
5:	$CHL = CHL \cup s_i$
6:	**end for**
7:	Sink translate packet include CHL
8:	**for** each senor s_i **do**
9:	**if** $s_i \in CHL$ **then**
10:	Remove s_i from CHL
11:	Update CHL
12:	Forward CHL
13:	**else**

```
14:         Forward CHL
15:         end if
16:         end for
17:   end for
```

Скорость вычисления алгоритмов LEACH и CHS практически одинакова с точки зрения обеспечения функционирования сенсорной сети. Это положение относится и по всем далее предложенным алгоритмам. Кроме того, в предложенных алгоритмах бóльшая часть вычислений, чем в LEACH, осуществляется непосредственно в сенсорном узле, что уменьшает нагрузку на заголовок пакета.

3.4. Результаты моделирования.

Моделирование осуществляется на языке C#.Net. Сеть из 100 сенсорных узлов размещается в зоне размером 200 × 200 м^2. Размещение сенсорных узлов с координатами *(x, y)* проводится случайным образом в соответствии с равномерным распределением.

Далее для простоты будем называть такой способ построения сенсорной сети случайным. При неравномерном распределении построение сенсорной сети связано с тем, что какие-либо узлы сенсорной сети группируются в определённой её части вместе, что может обеспечить большее покрытие именно в этой части сенсорного поля. Будем называть такое построение сети неравномерным.

На рис. 3.6 представлены обзоры отображений процесса моделирования на C#.Net для предложенного алгоритма CHS, а в таблице 3.2 параметры, используемые при моделировании.

Таблица 3.2. Параметры и их значения для моделирования.

Параметр	**Обозначение**	**Значение**
Первичная энергия на узел	E	*2j*
Tx/Rx	E_{elec}	*50 nj/bit*
Постоянное усиление	ε_{fs}	*10 pj/bit/m*^{2}
Мультисетевая постоянная	ε_{mp}	*0.0013 pj/bit/m*^{2}
Потери на участках (экспоненциальные)	n	*2*
Порог энергии головного узла	E_{th}	10^{-4}
Размер пакета	K	*30 bytes*
Скорость пакета	B	*1 packet/s*
Широкополосная зона вещания	R	*70 m*
Радиус сенсора	r	*15 m*
Радиус кластера	$r_{cluster}$	*2r*

Перечень и значения параметров являются типовыми и применялись для оценки эффективности алгоритма LEACH и других.

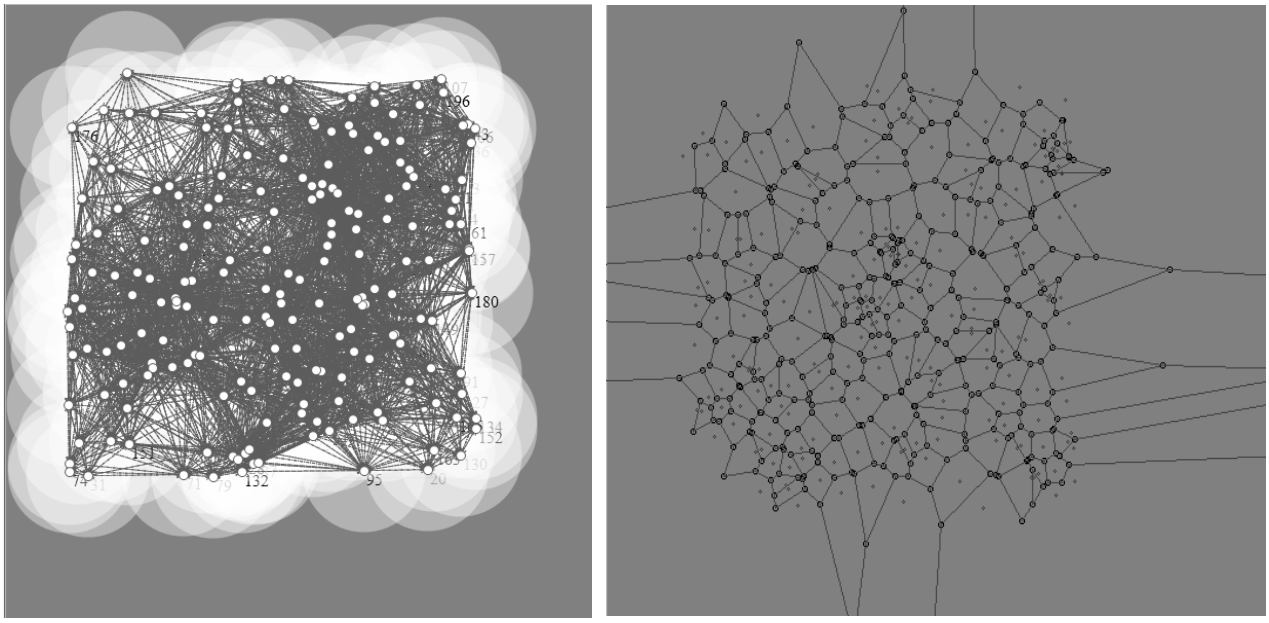


Рис. 3.6. Экранные формы.

Проведём сравнение разработанного алгоритма с базовым алгоритмом LEACH [104] по энергетической эффективности.

Для сравнения будем использовать общий расход энергии в Джоулях за промежуток времени. При этом в общий расход энергии включены как энергия, расходуемая внутри кластера, так и энергия, расходуемая при передаче информации от сенсорной сети к базовой станции. Сравнительные характеристики приведены на рис. 3.7, анализ которого показывает существенное преимущество разработанного алгоритма CHS над базовым алгоритмом LEACH. Действительно, в одной и той же сенсорной сети при использовании базового алгоритма LEACH энергия в 200 Джоулей

расходуется менее, чем за 2×10^4 сек., в то время как в предложенном алгоритме это время составляет около 3×10^4 сек.

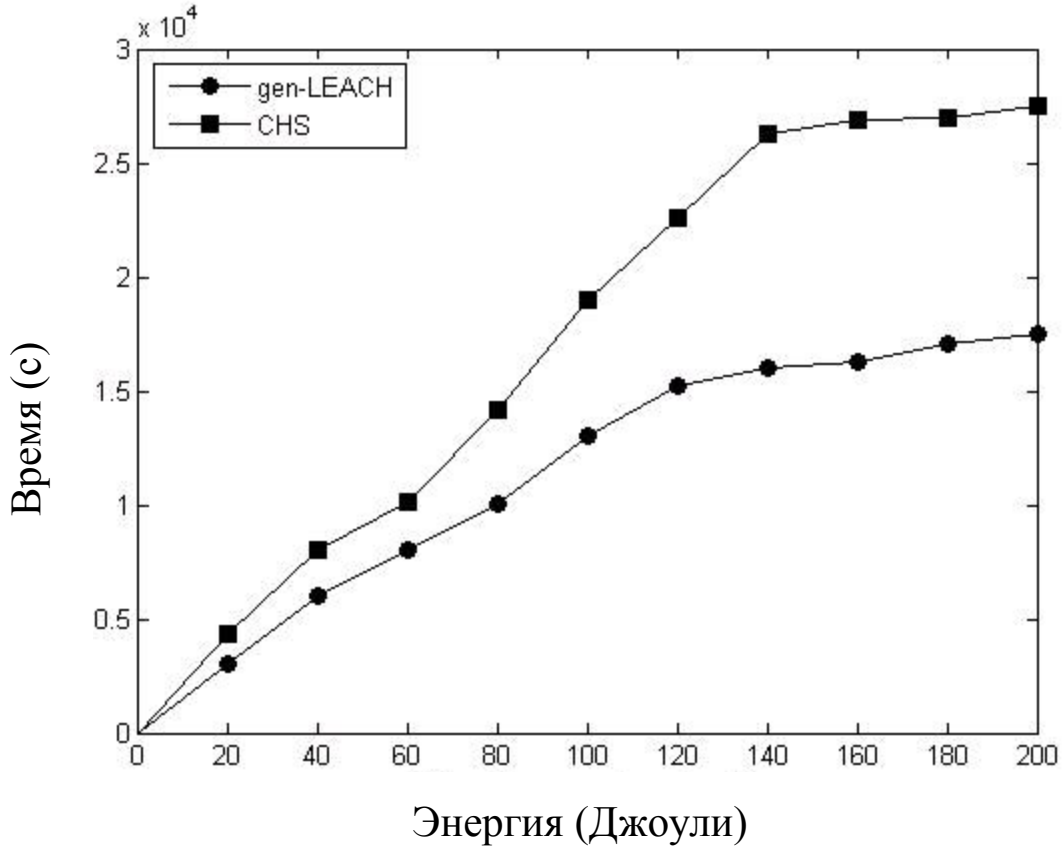


Рис.3.7. Отображение процесса моделирования для CHS.

4. Алгоритм выбора головного узла для однородной USN.

В настоящей главе будет рассмотрен новый алгоритм выбора головного узла кластере для решения проблем покрытия CHSC (Cluster Head Selection for Coverage), который является распределённым кластерным алгоритмом и может быть использован для однородных сенсорных сетей, где наиболее важным параметром является полное покрытие в течение достаточно длительного времени [35,37,137]. Предложенный алгоритм основывается на периметрическом покрытии и выборе наилучшего кандидата на уровень головного узла кластера из всех сенсорных узлов, входящих в рассматриваемую сеть. Примером сетей, где полное покрытие является критичным параметром качества обслуживания, являются сети мониторинга, например, мониторинга климата.

4.1. Покрытие.

Как уже отмечалось выше, с развитием сенсорных сетей появились и другие задачи, требующие пристального внимания. Например, задача о качестве обслуживания, которое является важнейшей метрикой для любой сети, в том числе и сенсорной. Действительно, очень важна проблема увеличения срока жизни сенсорной сети. Однако, если эта сеть не будет выполнять свои функции в требуемом объеме, то и сама задача увеличения срока жизни сенсорной сети, не удовлетворяющей требованиям по качеству обслуживания, схоластична.

В системах мониторинга одним из важнейших требований является его непрерывность, т.е. обеспечение мониторинга параметров на всем пространстве или процессе. Исходя из сказанного, в настоящей работе мы поставили перед собой цель разработать алгоритм выбора головного узла кластера, который обеспечивал бы лучшее покрытие заданной для мониторинга области двумерного пространства (плоскости) в течение достаточно длительного периода времени. Этот подход означает, в целом, оптимизацию как срока жизни сенсорной сети, так и выполнения сенсорной сетью своих функциональных задач с заданным качеством обслуживания в течение достаточно длительного периода времени.

Рассмотрим примеры алгоритмов, направленных на обеспечение покрытия беспроводной сенсорной сетью. Алгоритм конфигурирования покрытия *CCP* (Coverage Configuration Protocol) (Wang, 2003) [203] является децентрализованным алгоритмом, который конфигурирует сеть для достижения покрытия ее специфических областей. В течение цикла жизни сенсорной сети *CCP* изменяет степень покрытия сетью, которая требуется при реализации определённого приложения. Таким образом, достигается некоторое k-покрытие, где k выражается, например, в процентах от общего покрытия некоторого пространства. Алгоритм *CCP* интегрирован с алгоритмом SPAN (Chen, 2001) [81] для обеспечения и покрытия, и связности, однако целью по-прежнему остаётся достижение k-покрытия для обеспечения покрытием некоторых специфических областей пространства.

Алгоритм минимального и максимального путей [200] предполагает оценивать покрытие с помощью определения этих путей следующим образом. Минимальным путем считается путь между двумя заданными сенсорными узлами, при котором общее число сенсоров вдоль прохождения пути минимально, а максимальным путём, соответственно, считается такой путь, для которого число сенсоров максимально.

Для последующего решения поставленной задачи по выбору головного узла однородной кластерной сенсорной сети с обеспечением лучшего покрытия в течение достаточно длительного времени используем далее результаты работ по разработке алгоритма покрытия *CPC* (Check Perimeter Coverage).

4.2. Покрытие по периметру.

Рассмотрим более подробно алгоритм *CPC*.

Предположим, что существует набор сенсоров $S = \{s_1,\ldots,s_n\}$, в плоскости A. Каждый из сенсоров s_i, $i = 1\ldots n$ определяется координатами (x_i,y_i) на плоскости A и имеет радиус действия r_i, т.е. может обеспечивать мониторинг любого требуемого объекта или процесса на расстоянии r_i, от сенсора s_i.

Введем следующие определения.

Определение 1. Рассмотрим любые два сенсора s_i и s_j. Точка периметра s_i является периметрически покрытой посредством s_j, если эта точка находится внутри области покрытия s_j.

Определение 2. Рассмотрим любой сенсор s_i. Будем говорить, что s_i является k-периметрически покрытым, если все точки периметра s_i являются периметрически покрытыми как минимум k сенсорами помимо самого сенсора s_i. Соответственно, сегмент периметра s_i сенсора является k-периметрически покрытым, если все точки сегмента периметрически покрыты как минимум k сенсорами помимо самого сенсора s_i.

На рис. 4.1 изображено покрытие сегмента периметра сенсора s_i сенсором s_j.

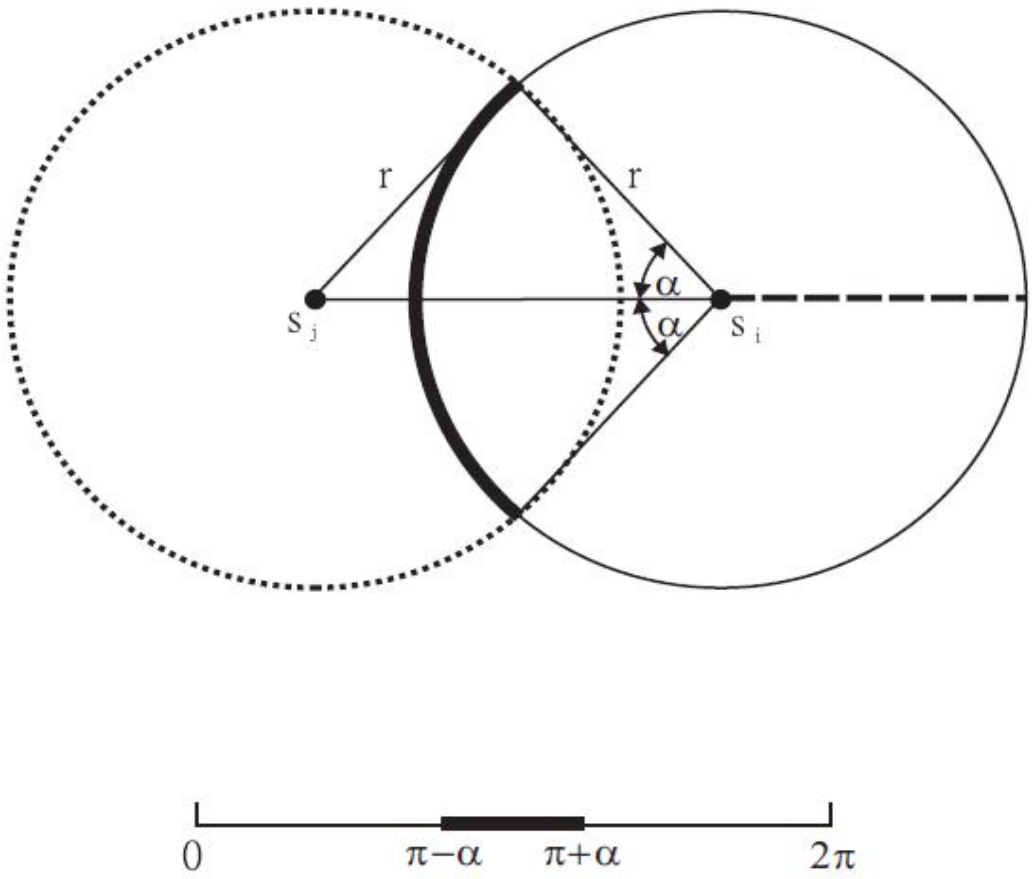


Рис. 4.1. Определение покрытия сегмента периметра сенсора s_i сенсором s_j.

Рассмотрим два сенсора, расположенных на плоскости с координатами (x_i,y_i) и (x_j,y_j), соответственно. Заметим, что

$$d(s_i, s_j) = \sqrt{|x_i - x_j|^2 + |y_i - y_j|^2} \qquad (4.1)$$

есть расстояние между s_i и s_j. Если $d(s_i, s_j) > 2r$, то s_j не может внести никакого вклада в покрытие периметра s_i. В ином случае покрытия периметра сенсора s_i сенсором s_j может быть определено в соответствии с рис.4.1. Без потери общности положим, что s_j покрывает сегмент правой части периметра s_i ($y_i = y_j$, $x_i > x_j$).

При этом угол α находится из уравнения:

$$\alpha = \arccos\left(\frac{d(s_i, s_j)}{2r}\right) \qquad (4.2)$$

Таким образом, дуга s_i, определяемая углом [π - α, π + α], является сегментом периметра сенсора s_i, покрытого сенсором s_j.

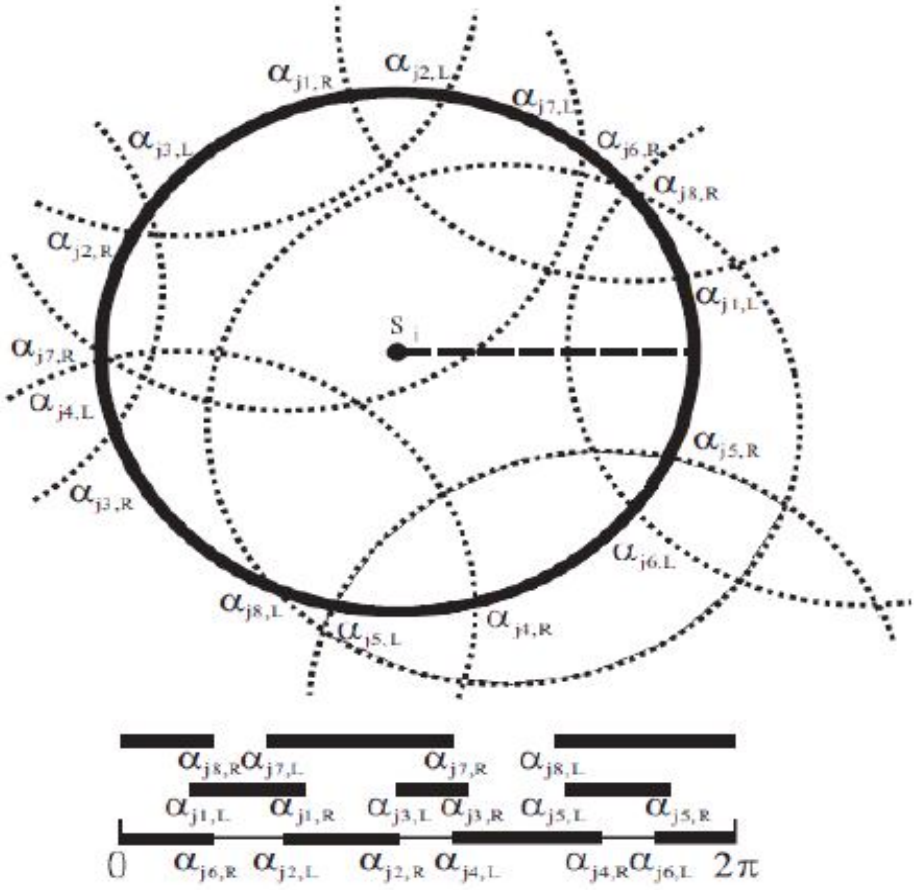


Рис. 4.2. Определение покрытия периметра s_i множеством сенсоров плоскости А.

Данный подход может быть обобщен и на множественное покрытие периметра сенсора s_i различными сенсорами из множества сенсоров, расположенных на плоскости A. Покрытие периметра сенсора s_i множеством сенсоров изображено на рис. 4.2. Проверка покрытия периметра s_i может быть осуществлена с помощью алгоритма *СРС*.

4.3. Алгоритм выбора головного узла в кластерной сенсорной сети.

Рассмотрим новый алгоритм выбора головного узла в кластерной сенсорной сети, обеспечивающий лучшее покрытие в

течение достаточно длительного времени, и объединяющий в себе решение двух задач: лучшего покрытия на основе периметрического подхода предыдущего раздела и выбора головного узла с учетом его энергетических характеристик.

Предлагаемый алгоритм назван *CHSC* (Cluster Head Selection for Coverage) – выбор головного узла в кластере для покрытия. В алгоритме *SHSC* вводится понятие кластерного радиуса r_{cl}.

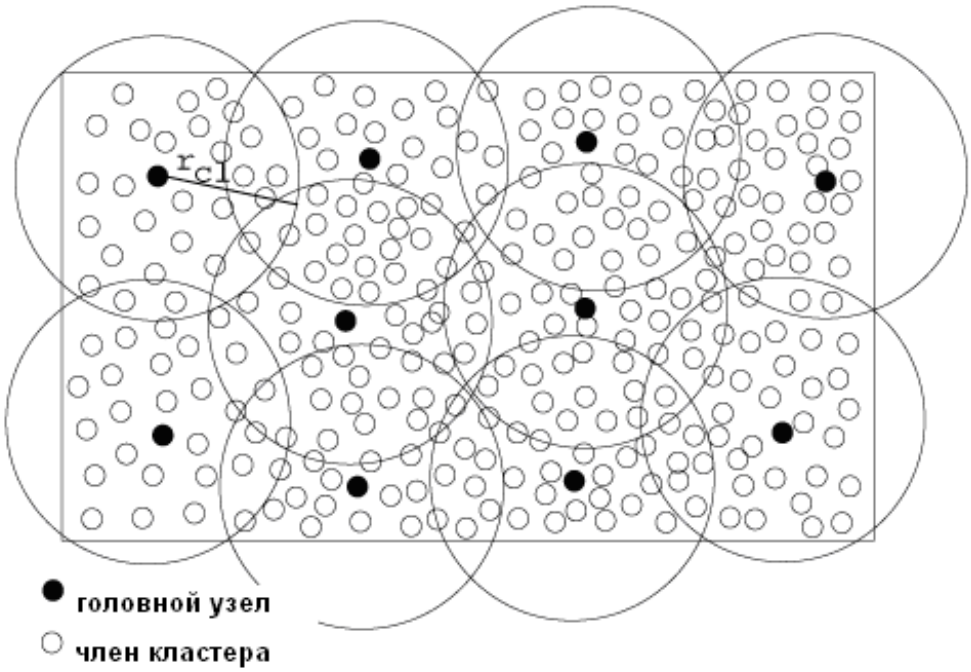


Рис. 4.3. Однородная кластерная сеть и параметр r_{cl} алгоритма *CHSC*.

На рис. 4.3 изображена однородная кластерная сенсорная сеть, покрывающая полностью некую плоскость А. Как уже отмечалось выше, любой из обычных сенсорных узлов (на рис.4.3 изображен как член кластера) может стать головным и наоборот. Параметр r_{cl} в определенной степени вносит упорядоченность в структуру кластерной сенсорной сети на рис.4.3. При этом любой сенсорный узел в пределах своего кластера обращается к головному узлу

напрямую (one-hop), в то время как передача информации от головного узла к шлюзу может быть и многошаговой (multi-hop).

Таблица 4.1: Алгоритм проверки периметрического покрытия *CPC*

1: **Input:** Sensor node s

2: **Output:** "**True**" s full Perimeter Coverage, "**False**" s not full Perimeter Coverage.

3: find $N(s) = \{s_j : d(s_i,s_j) \leq 2r\}$

4: **for** every s_j in $N(s)$ **do**

5: Determine the angle of s's is arch, denoted by $[\alpha_j,L,\alpha_j,R]$, that is perimeter-covered by s_j.

6: Place the points α_j,L and α_j,R on the line segment $[0,2\pi]$.

7: end for

8: sort all these points in an ascending order into a list L.

9: mark each point as a left or right boundary of a coverage range.

10: Traverse the line segment $[0,2\pi]$ by visiting each element in the sorted list L from the left to right and determine the perimeter-coverage of.

11: **if** line without cutting (i.e L without empty element) **then**

12: return "**True**".

13: **else**

14: return "**False**"

15: **end if**

Алгоритм *CHSC* вначале собирает информацию об остаточной энергии для всех сенсорных узлов (если остаточная энергия ($E(s_i)$) i–ого сенсорного узла равна 0, то этот узел, естественно, исключается из дальнейшего функционирования в сенсорной сети).

Информация об остаточной энергии рассылается каждым сенсорным узлом в области $2 \times r_{sensing}$, где $r_{sensing}$ – радиус действия сенсорного узла в сети для выполнения функций мониторинга. После получения информации от всех соседей каждый сенсорный узел выполняет алгоритм *CPC* для проверки периметрического покрытия. Принимая во внимание, что сенсорные узлы находятся в статическом положении, ближайшие узлы должны обменяться информацией о своем местоположении только один раз – в начале жизненного цикла сенсорной сети.

Таблица 4.2: Алгоритм 2. Алгоритм выбора головного узла для покрытия *CHSC*.

1: $S = \{s : E(s) > 0\}$, $E(s)$ -residual energy of sensor node s

2: $S_{CH} = \{\}$

3: $CL(s_i) = \{\}$ // The members of cluster head s_i

4: **while** $S \neq \{\}$ **do**

5: **if** ($CPC(s_i) == True$) and ($E(s_i) > E_{th}$) then

6: $S_{CH} = S_{CH} \cup s_i$

7: $N(i) = \{s : d(s, s_i) < r_{cl}\}$

8: $CL(s_i) = N(i) \cup s_i$

9: $S = S \setminus N(s_i)$

10: **end if**

11: **end while**

12: **for** every s_i in S_{CH} **do**

13: $\forall s \in CL(s_i$ do s_i send **JOIN** message to cluster head

12: **end for**

Каждый из сенсорных узлов ожидает окончания активизации сети и затем может объявить себя новым головным узлом в кластере для исходящих соединений. Это происходит в том случае, если за время активации сенсорный узел не получил никаких информационных сообщений от любых других узлов, объявивших себя головными. При объявлении себя головным узлом сенсорный узел рассылает это информационное сообщение всем сенсорным узлам, находящимся в пределах расстояния r_{cl} Принятие решения об объявлении себя головным узлом осуществляется на основе возможности обеспечения лучшего покрытия и наличия достаточной энергии $(E(s_i) > E_{th})$ где E_{th} – пороговое значение необходимой энергии для головного узла в кластере). Информационное сообщение содержит информацию о местонахождении нового головного узла кластера. После получения сообщения от нового головного узла кластера все сенсорные узлы в пределах r_{cl} исключают себя из дальнейшего рассмотрения на роль головного узла.

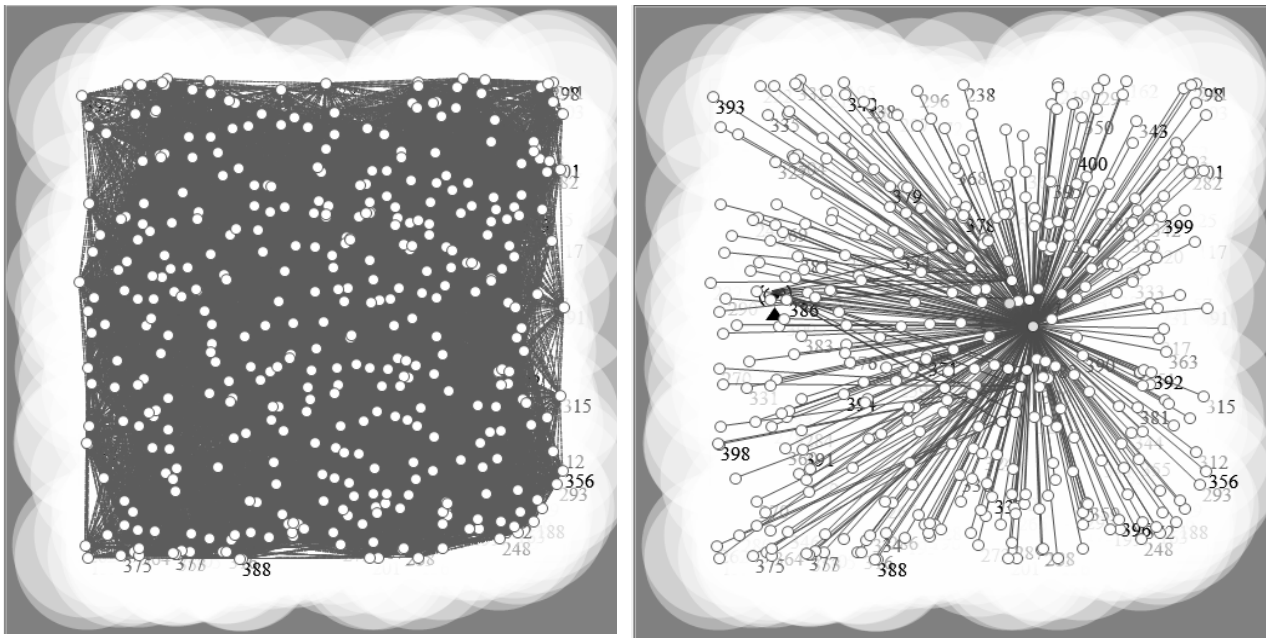
Каждый сенсорный узел содержит таблицу всех головных узлов, от которых он получил информационное сообщение об объявлении себя головным, на доступном для узла расстоянии. Эта информация используется сенсорным узлом для принятия решения о том, членом какого кластерного узла этот узел будет. Иногда может оказаться, что два сенсорных узла с подходящими характеристиками объявляют себя головными в пределах одного и

того же $r_{cl.}$ Тогда головной узел в конечном итоге определяется по наибольшей остаточной энергии.

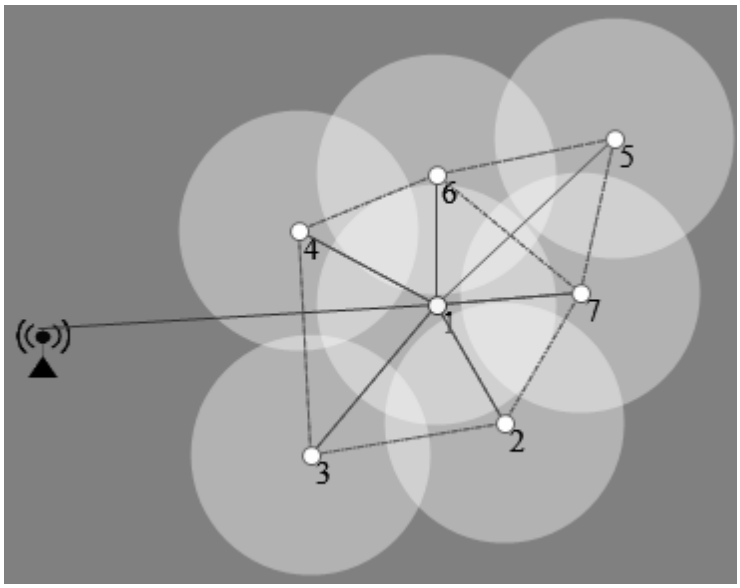
4.4. Результаты моделирования.

Моделирование осуществляется на языке C#NET. Параметры моделирования приведены в таблице 4.1. На рис. 4.4 показаны параметры экранных форм, получаемых в процессе моделирования.

Сенсорные узлы предполагаются однородными по своим свойствам. В процессе моделирования реализуются два сценария: первый посвящен анализу влияния эффекта изменения параметра r_{cl} на число головных кластерных узлов и длительность полного покрытия при использовании алгоритма *CHSC*, а второй сценарий – сравнению предложенного алгоритма *CHSC* с известным базовым алгоритмом LEACH.



(a) Сенсоры (b) Кластеризация



(c) Кластерная сеть

Рис. 4.4. Экранные формы.

В обоих случаях в качестве плоскости А используется квадрат 200 × 200 м, число сенсоров в момент начала жизни сети составляет 400. Шлюз с сетью связи общего пользования расположен в центре сети.

Таблица 4.1. Параметры моделирования.

Параметр	**Обозначение**	**Значение**
Первичная энергия на узел	E	*2j*
Tx/Rx	E_{elec}	*50 nj/bit*
Постоянное усиление	ε_{fs}	*10 pj/bit/m*^{2}
Мультисетевая постоянная	ε_{mp}	*0.0013 pj/bit/m*^{2}
Потери на участках (экспоненциальные)	n	*2*

Порог энергии головного узла	E_{th}	10^{-4}
Размер пакета	K	*30 bytes*
Скорость пакета	B	*1 packet/s*
Широкополосная зона вещания	R	*70 m*
Радиус сенсора	r	*30 m*

На рис. 4.5 представлена зависимость среднего числа головных узлов в сети от параметра r_{cl}. Как видим, при значении r_{cl} в 20м число головных узлов (кластеров) в сети очень велико, а именно: шестьдесят, - но при этом обеспечивается и наилучшее покрытие во времени. На рис. 4.6 длительность полного покрытия при значении r_{cl} в 20м более, чем в 2 раза больше, чем длительность полного покрытия при r_{cl} в 50 метров. Заметим, что при r_{cl} = 20 метров средняя численность узлов в кластере около 7, включая головной.

Для сравнения алгоритмов LEACH и CHSC примем значение r_{cl} = 40м (среднее из рассмотренных выше).

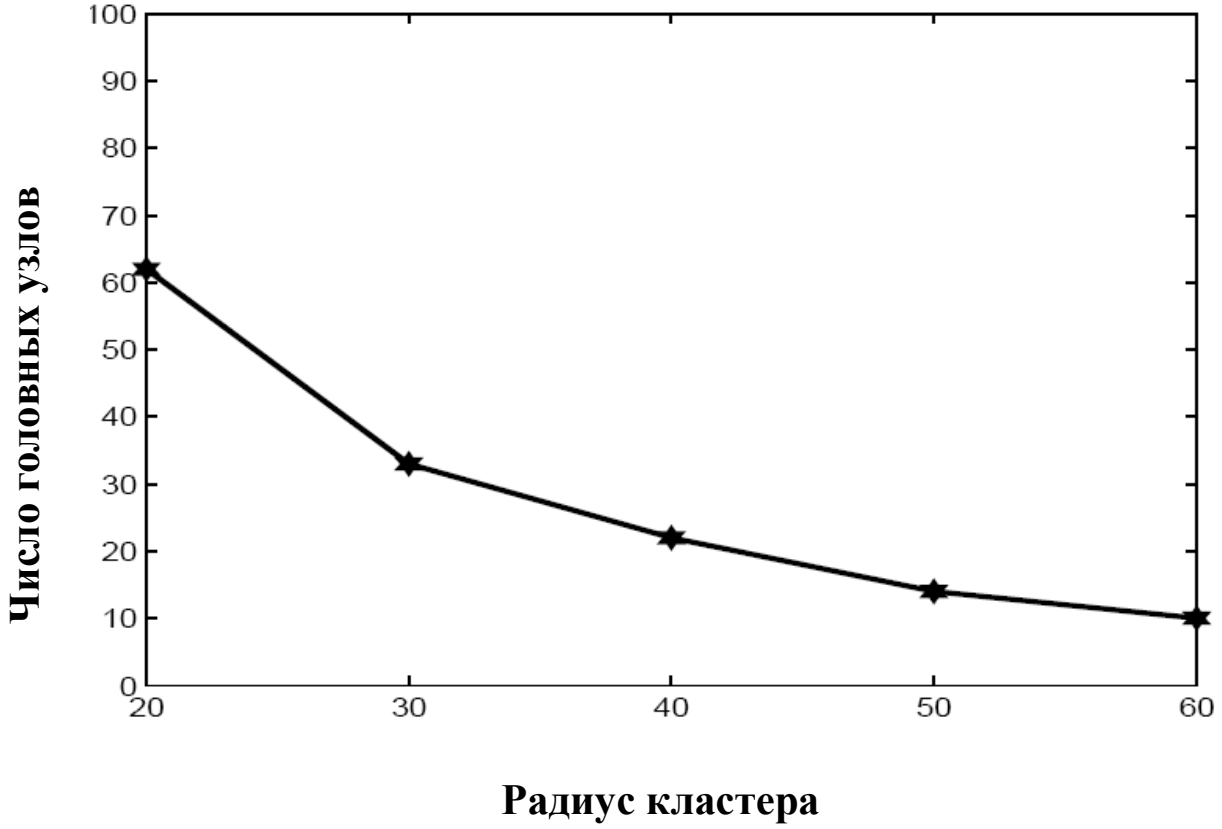


Рис. 4.5. Среднее число головных узлов (кластеров) в зависимости от r_{cl}.

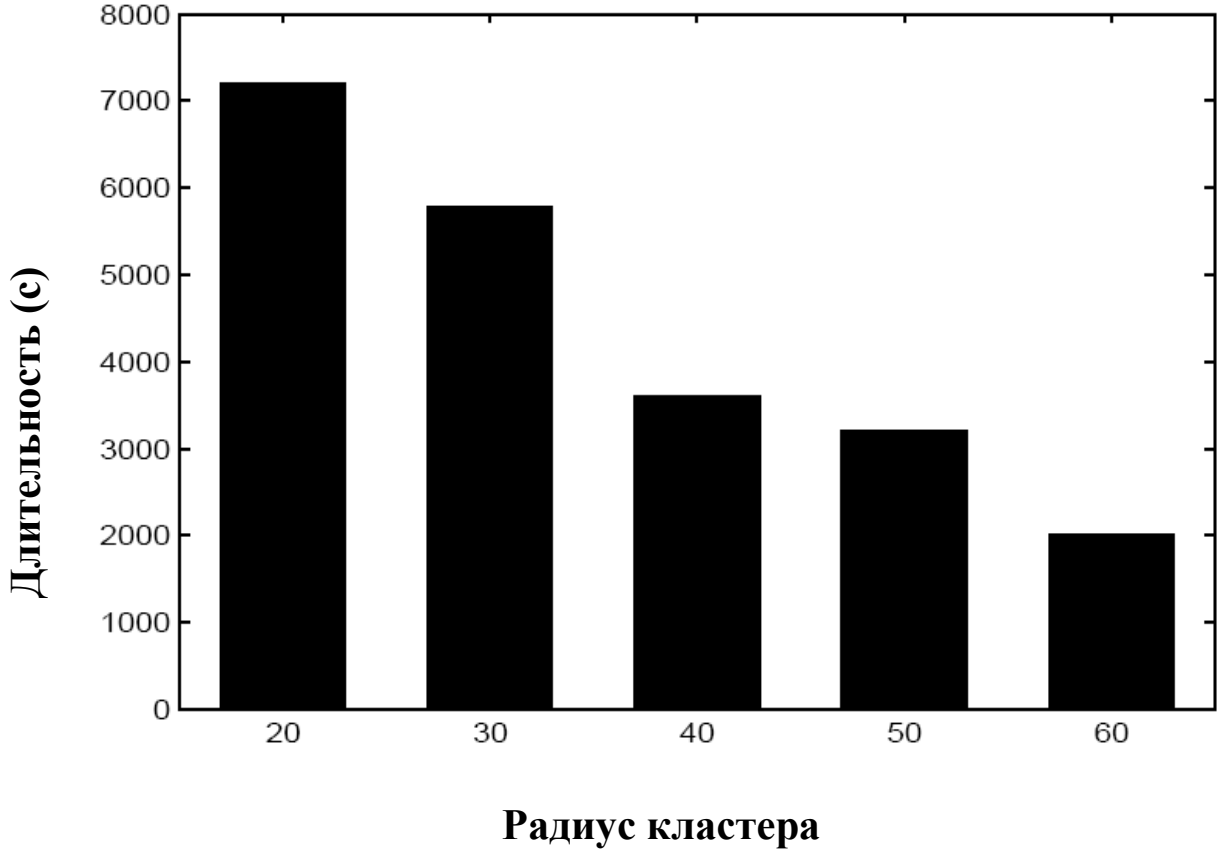


Рис.4.6. Длительность полного покрытия в зависимости от r_{cl}.

На рис. 4.7 приведено сравнение LEACH и CHSC по длительности *k*-покрытия (к = 100%, 90%, 80%) сети. Как видим, предложенный алгоритм значительно увеличивает длительность существенного покрытия сети. Длительность покрытия больше при значении к = 100%, а в случаях к = 90% и к = 80% длительность *k*–покрытия при использовании CHSC превосходит длительность *k*–покрытия при использовании LEACH в несколько раз.

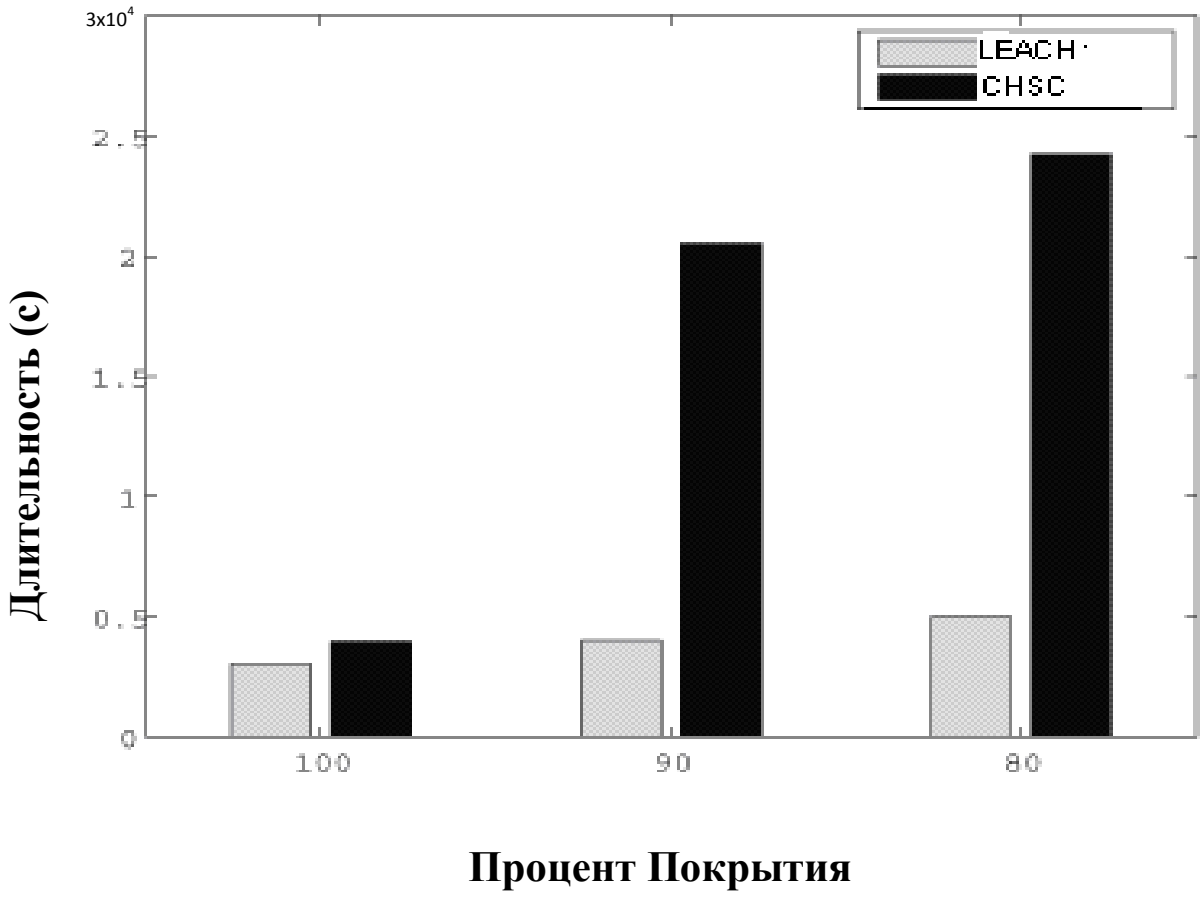


Рис. 4.7. Сравнение *k*–покрытия при использовании LEACH и CHSC.

Одновременно улучшается и такая важная характеристика, как число долговременно живущих сенсорных узлов. На рис. 4.8 приведено сравнение числа живущих узлов при использовании

LEACH и CHSC в зависимости от числа циклов моделирования.

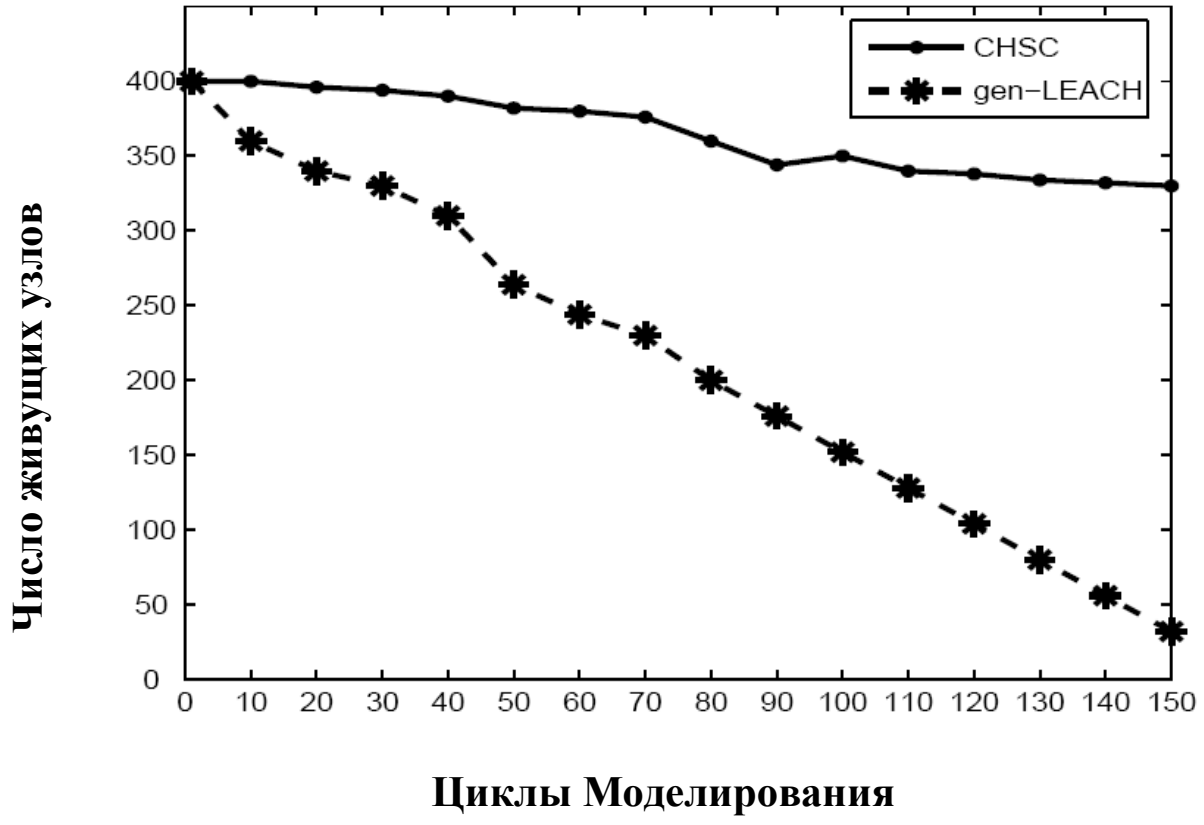


Рис.4.8. Сравнение числа живущих узлов при использовании LEACH и CHSC.

5. Алгоритм выбора головного узла для неоднородной USN.

В предыдущей главе был разработан алгоритм выбора головного узла в кластере для гомогенных (однородных) сенсорных сетей. Однако, сенсорные узлы бывают различными по архитектуре и функциональности. Поэтому, гетерогенные сенсорные сети, состоящие из сенсорных узлов с различными характеристиками, также достаточно часто встречаются на практике. Пример гетерогенной (неоднородной) сенсорной сети приведен на рис. 5.1.

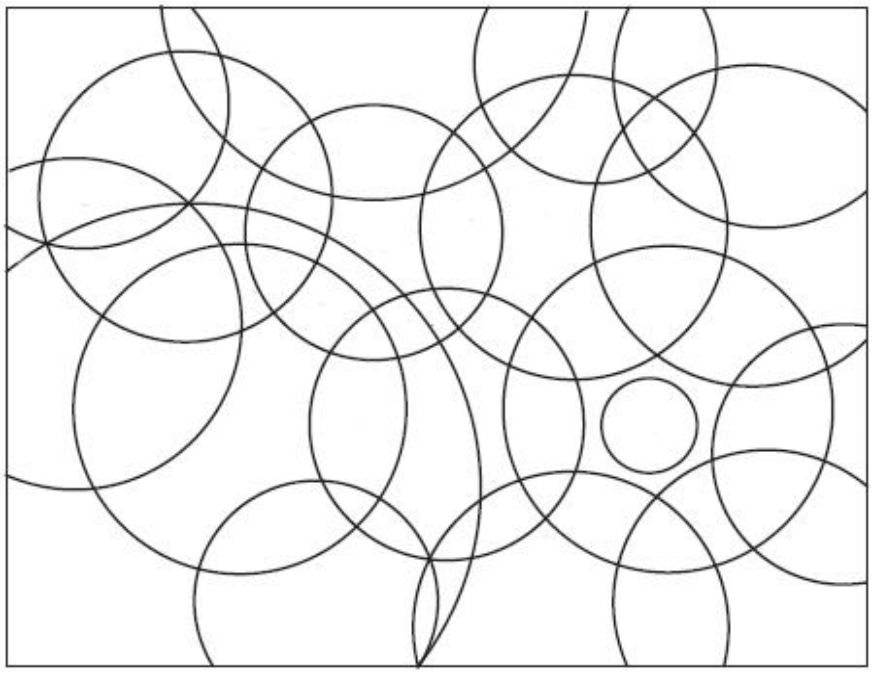


Рис. 5.1. Гетерогенная беспроводная сенсорная сеть.

Одним из классических примеров гетерогенных сенсорных сетей является подводная сенсорная сеть [78], в которой различные сенсоры измеряют характеристики воды, шумы, наличие движения и т.д.

В настоящей главе будет рассмотрен подход с использованием техники периметрического покрытия кластерными сенсорными сетями для создания гетерогенных USN.

При этом, будет разработан алгоритм выбора головного узла для покрытия (CSC – *Cluster Head selection for Coverage*) на основе алгоритма полного периметрического покрытия (FPCN – Full *Perimeter Coverage Nodes*) с использованием туннельного параметра (r_{cl}), который определяет минимальное расстояние между любыми двумя головными узлами кластеров в формируемой сети [138]. Моделирование показывает, что алгоритм CSC обеспечивает лучшее покрытие и жизненный цикл сети, чем базовый алгоритм LEACH.

5.1. Предположения и периметрическое покрытие.

В этом разделе вначале будут рассмотрены предположения, допускаемые при решении задачи и далее принципы периметрического покрытия.

5.1.1. Предположения.

Следующие предположения принимаются при решении задачи:

- **Аппаратная часть.** Предполагается, что каждый сенсорный узел оборудуется сенсорным устройством для измерения параметров, широковещательным телекоммуникационным устройством и процессором.

- **Локализация.** Позиционное расположение каждого сенсорного узла известно в любой глобальной системе координат с возможностью локализации системы [186]. Для упрощения, будем предполагать, что для каждого узла известно его местоположение в пространстве в координатах (x_i, y_i). Близлежащие узлы определяются как доступные друг другу в пределах радиовидимости.
- **Стационарность узлов.** Сенсорные узлы предполагаются статичными. Измеряемые ими явления могут быть динамичными.
- **Телекоммуникационные протоколы.** Полагаем, что телекоммуникационные протоколы могут обеспечить всю необходимую для сети информацию.
- Все сенсорные узлы случайно распределены в области мониторинга. Кроме того, сенсорные узлы распределены с достаточной плотностью, чтобы не было изолированных узлов.
- Сенсорный радиус действия для сенсорных узлов может быть различным (гетерогенные сенсорные радиусы взаимодействия).

Будем также предполагать, что каждый узел знает про свои близлежащие узлы, включая их идентификацию и координаты. Эта информация может быть собрана посредством сообщений типа “beacon” или “hello” и периодически претерпевать изменения, связанные с топологией сенсорной сети.

5.1.2. Периметрическое покрытие.

Когда сенсорные узлы имеют различные сенсорные и коммуникационные радиусы, сенсорный узел может иметь один или несколько переходов (hop) к своему первому покрытому близлежащему узлу.

В этом случае, два покрытых узла могут иметь один или несколько переходов для взаимодействия друг с другом. Таким образом, нет возможности рассматривать только один подход между близлежащими узлами для нахождения первого покрытого близлежащего узла заданным сенсорным узлом.

Для сбора информации о покрытии узлов используется следующий метод [109,110]. Каждый сенсорный узел s_i может определить, покрыт он периметрическим сенсорным узлом s_j или нет. Рассмотрим сенсорные узлы s_i и s_j, расположенные на плоскости с координатами (x_i,y_i) и (x_j,y_j), с сенсорными радиусами r_i и r_j соответственно. Может быть рассмотрено три варианта, как это проиллюстрировано на рис. 5.2.

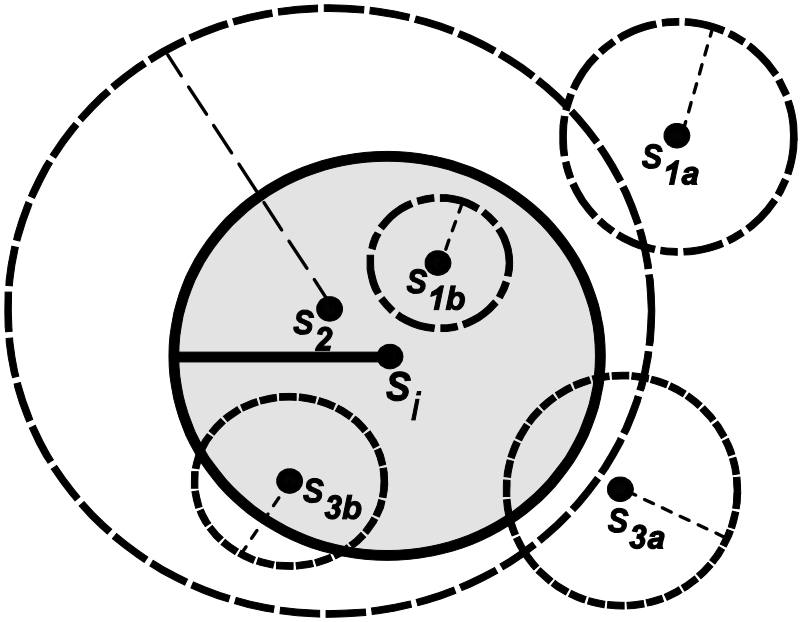


Рис. 5.2. Варианты периметрического покрытия.

- **Вариант 1**: s_i не является периметрически покрытым посредством s_j, если

а) $(r_j < d(s_i,s_j) - r_i)$ *at* $r_j > 0$, как показан узел s_{1a} на рис. 5.2,

б) $(r_j < r_i - d(s_i,s_j))$ *at* $r_j > 0$, как показан узел s_{1b} на рис. 5.2.

- **Вариант 2**: Радиус сектора s_i полностью $[0,2\alpha]$ периметрически покрыт посредством s_j, если

а) $(d(s_i,s_j) < r_i)$ *и* $(r_j > d(s_i,s_j) + r_i)$, как показан узел s_2 на рис. 5.2.

- **Вариант 3**: Сегмент s_i с узлом $[\pi\text{-}\alpha, \pi+\alpha]$ периметрически покрыт посредством s_j, если

а) $(d(s_i,s_j) > r_i)$ *и* $(d(s_i,s_j) - r_i < r_j < d(s_i,s_j) + r_i)$, как показан узел s_{3a} на рис. 5.2,

б) $(d(s_i,s_j) > r_i)$ и $(r_i - d(s_i,s_j) < r_j < r_i + d(s_i,s_j))$, как показан узел s_{3b} на рис. 5.2.

Во всех случаях α определяется из следующей формулы:

$$r_j^2 = r_i^2 + d(s_i, s_j)^2 - 2r_i \times d(s_i, s_j) \times \cos(\alpha) \qquad (5.1)$$

5.2. Новый алгоритм.

В этом разделе будет рассмотрен новый алгоритм для нахождения полного периметрического покрытия, который далее будет использован в алгоритме выбора кластерного узла для покрытия.

5.2.1. Алгоритм для нахождения полного периметрического покрытия.

Алгоритм для нахождения полного периметрического покрытия (*Full Perimeter Coverage Nodes* - FPCN) приводится в таблице 5.1.

Алгоритм FPCN определяет набор узлов, который состоит из полностью периметрически покрытых сенсорных узлов. Алгоритм выбора кластерного узла для покрытия (*Cluster head Selection for Coverage* – CSC) использует этот набор для выбора головного узла.

Таблица 5.1. Алгоритм FPCN.

1: $S = \{s_i : E(s_i) > 0\}$, $E(s_i)$ residual energy of sensor node s_i.

2: *FC:* a set of sensors candidate to be cluster head.

3: $FC = S$

{ Removing the sensors which belong to Case1(b)}

4: **for** every s_i in FC do

5: $NS(s_i) = \{ s_j : Area(s_i) \cap Area(s_j) \neq 0\}$

6: **for** every s_i in $NS(s_i)$ **do**

7: **if** $(Area(s_i) \subset Area(s_j))$ **then**

8: s_i become not sensing node.

9: $FC = FC \setminus s_i$

10: **end if**

11: **end for**

12: **end for**

Removing the sensors which not perimeter coverage

13: **for** every s_i in FC **do**

14: **for** every s_j in $NS(s_i)$ **do**

15: Determine the angle of s_i's is arch, denoted by $[\alpha_{j,L},\alpha_{j,R}]$ that is perimeter- covered by s_j.

16: Place the points $\alpha_{j,L}$ and $\alpha_{j,R}$ on the line segment $[0,2\pi]$

17: **end for**

18: sort all these points in an ascending order into a list L.

19: Mark each point as a left or right boundary of a coverage range.

20: Traverse the line segment $[0,2\pi]$ by visiting each element in the sorted list L from the left to right and determine the perimeter-coverage of s_i.

21: **if** line with cutting (i.e., L with empty element) **then**

22: $FC = FC \setminus s_i$.

23: **end if**

24: **end for**

После получения обновленной информации от всех близлежащих узлов, каждый сенсорный узел s_i останавливается,

если его сенсорное поле покрыто другим сенсорным узлом s_j. Если не всё сенсорное поле покрыто, то каждый сенсор определяет угол сегмента s_i для каждого сенсора из списка $[\alpha_{j,L},\alpha_{j,R}]$ и место точек $\alpha_{j,L}$ и $\alpha_{j,R}$ на линейном сегменте $[0,2\pi]$, как это показано на рис. 5.2, и сортирует все эти точки по порядку в лист L.

После этого, каждая точка маркируется как левая или правая в радиусе покрытия и получается траверс линейного сегмента $[0,2\pi]$ из листа L слева направо как показано на рис.5.2.

Псевдокод FPCN обеспечивается алгоритмом таблицы 5.1.

5.2.2. Алгоритм выбора головного узла для обеспечения покрытия.

В изложенном подходе полностью периметрически покрытые сенсорные узлы являются лучшими кандидатами на функции головного кластерного узла, поскольку такие узлы могут поддерживать наибольшее число членов кластера.

Далее предложим метод, названный CSC. Как уже отмечалось выше, метод и алгоритм CSC основаны на туннельном параметре r_{cl}, который определяется как минимальное расстояние между любыми двумя головными узлами кластера в сети. Используя этот параметр, CSC позволяет достаточно точно распределить кластерные узлы по сети. Параметр r_{cl} может быть мягко настроен при изменении передающей мощности головных узлов кластера. В CSC сенсорные узлы взаимосвязаны непосредственно с выбранными головными кластерными узлами, в то время как

маршрутизация данных от головного узла кластера к шлюзу может быть многошаговой (multi-hop), как это показано на рис. 5.3.

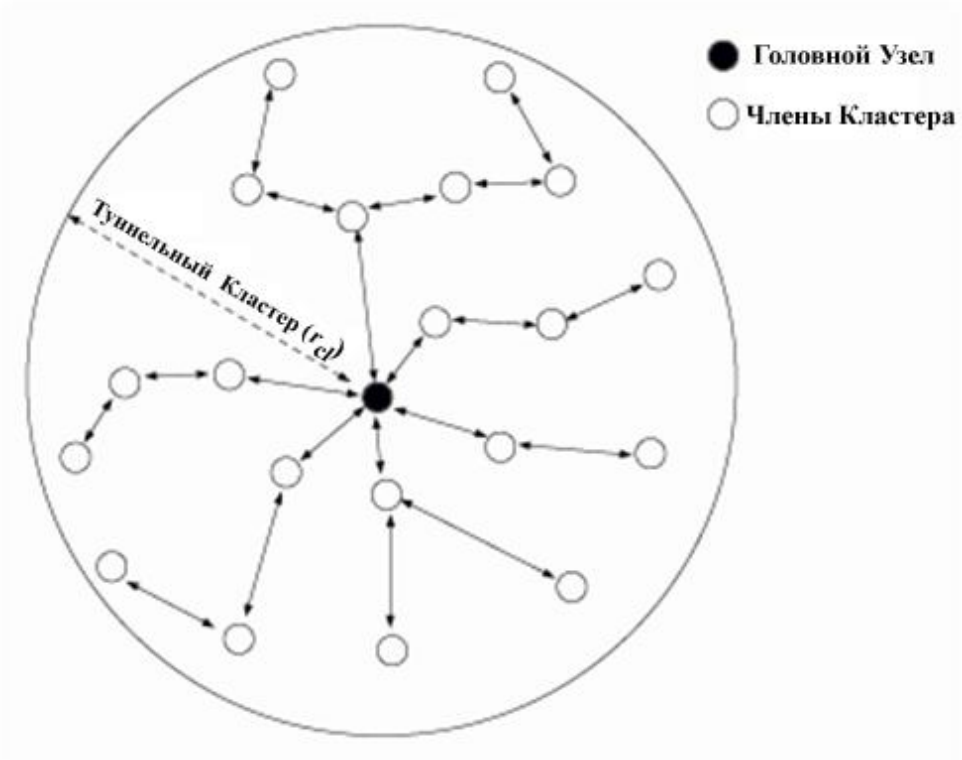


Рис.5.3. Многошаговая маршрутизация.

В начале функционирования CSC каждый сенсор широковещательно распространяет пакет информации о его остаточной энергии для всех близлежащих узлов. Во избежание коллизий этих пакетов, узлы используют информацию о пространстве перед передачей пакета (аналогично вектору резервирования в WiFi). После получения информации от всех близлежащих сенсорных узлов включается алгоритм FPCN. С учетом того, что сенсорные узлы статичны, близлежащие узлы должны подтвердить свое местоположение только однажды в начале жизненного цикла сенсорной сети.

Каждый сенсор ожидает некоторое время (время активации), прежде чем он решит объявить себя новым головным кластерным узлом или нет. Если в течении времени активации сенсорный узел не получает сообщений о том, что какой-либо узел уже объявил себя головным, то данный узел сам объявляет себя головным, рассылая соответствующие сообщения всем узлам в пределах r_{cl}. Сообщение содержит информацию о местоположении нового головного сенсорного узла. После получения сообщения от нового головного узла кластера, все сенсорные узлы в области действия r_{cl} исключают себя из дальнейших претендентов на роль головного узла.

Каждый сенсор создаёт таблицу всех головных узлов кластера от которых он получил сообщение. Эта информация используется далее сенсорным узлом для принятия решения о членстве в том или ином кластере. В случае, если два сенсорных узла с одинаковыми затратами на передачу информации, действующие в одной и той же области r_{cl} определяют себя головными узлами, побеждает тот узел, у которого выше энергетические возможности. Псевдокод для алгоритма CSC приведён в таблице 5.2.

Таблица 5.2. Алгоритм CSC.

1: $S = \{s : E(s) > 0\}$, $E(s)$ residual energy of sensor node s.

2: $S_{CH} = \{\}$, a set of cluster head nodes.

3: $CM(s_i) = \{\}$, a set of cluster members.

4: **while** FC ≠ {} **do**

5: **if** $(s_i \in FC$ *and* $E(s_i) > E_{th})$, E_{th} - threshold energy for node to be

cluster head

then

6: $S_{CH} = S_{CH} \cup s_i$

7: $r_{cl} = 2 \times r_i$

8: $CM(s_i) = \{s:d(s, s_i) \leq r_{cl}\}$

9: $S = S \setminus N(s_i)$

10: **end if**

11: **end while**

12: **for** every s_i in S_{CH} **do**

13: s_i sends Announce message to all $s \in CM(s_i)$

14: All $s \in CM(s_i)$ sends JOIN message to s_i

15: **end for**

5.3. Результаты моделирования.

Программа моделирования была составлена на C#. NET. Сенсорные узлы предполагались неравномерно распределёнными случайным образом на плоскости. Предполагается также, что сенсорные узлы имеют возможность регулирования своей мощности передатчика в зависимости от расстояния до узла-приёмника.

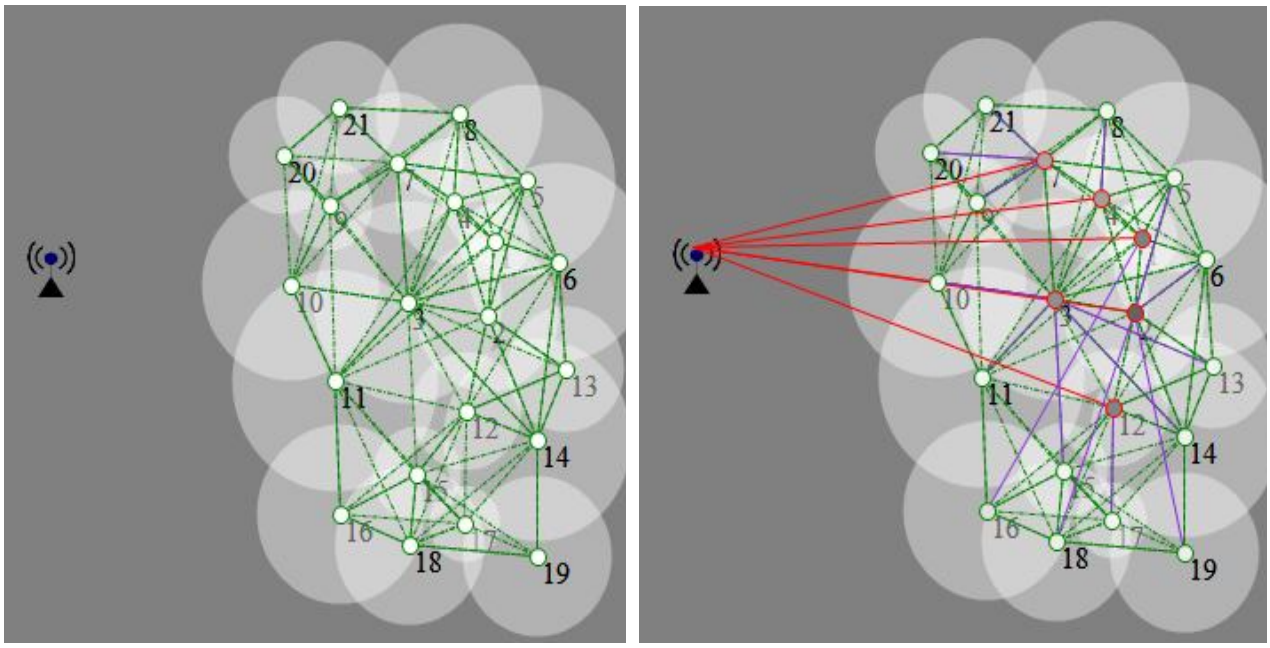


Рис. 5.4. Экранные формы.

Параметры, используемые при моделировании, приведены в таблице 5.3, а экранные формы – на рис. 5.4.

При моделировании изучались два сценария.

Первый сценарий использовался для анализа собственно алгоритм CSC, а второй – для сравнения его характеристик с базовым алгоритмом LEACH [104].

При этом использовались следующие метрики для оценки эффективности алгоритмов:

- число головных узлов в цикле жизни сенсорной сети,
- процент покрытия,
- жизненный цикл.

Таблица 5.3. Параметры моделирования.

Параметр	**Обозначение**	**Значение**
Первичная энергия на узел	E	*2j*
Tx/Rx	E_{elec}	*50 nj/bit*
Постоянное усиление	ε_{fs}	*10 pj/bit/m*^{2}
Мультисетевая постоянная	ε_{mp}	*0.0013 pj/bit/m*^{2}
Потери на участках (экспоненциальные)	n	*2*
Порог энергии головного узла	E_{th}	10^{-4}
Размер пакета	K	*30 bytes*
Скорость пакета	B	*1 packet/s*
Широкополосная зона вещания	R	*70 m*
Радиус сенсора	r	*15 - 30 m*
Радиус кластера	r_{cl}	*2r*

5.3.1. Первый сценарий

В этом сценарии сенсорные узлы случайным образом распределены на площади 200 × 200 м. Число сенсорных узлов 400. Целью моделирования является анализ эффективности CSC в сети.

Головные узлы кластеров агрегируют пакеты данных, полученные от активных сенсоров, и затем передают эти пакеты в шлюз.

Рис. 5.5 показывает среднее число головных узлов за период жизненного цикла сенсорной сети. Число узлов возрастает с ростом значения периода. Это связано с уменьшающейся плотностью сенсорных узлов вследствие их выхода из строя.

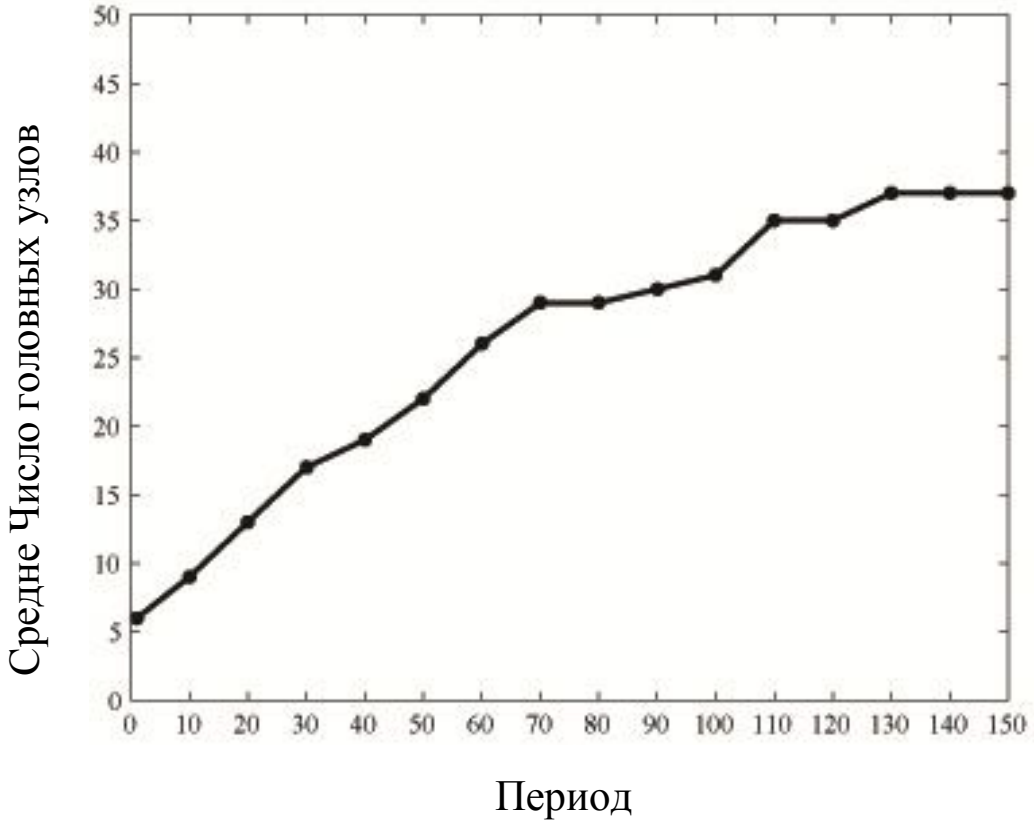


Рис. 5.5. Среднее число головных узлов за период.

Рис. 5.6 показывает зависимость числа погибших узлов с течением времени.

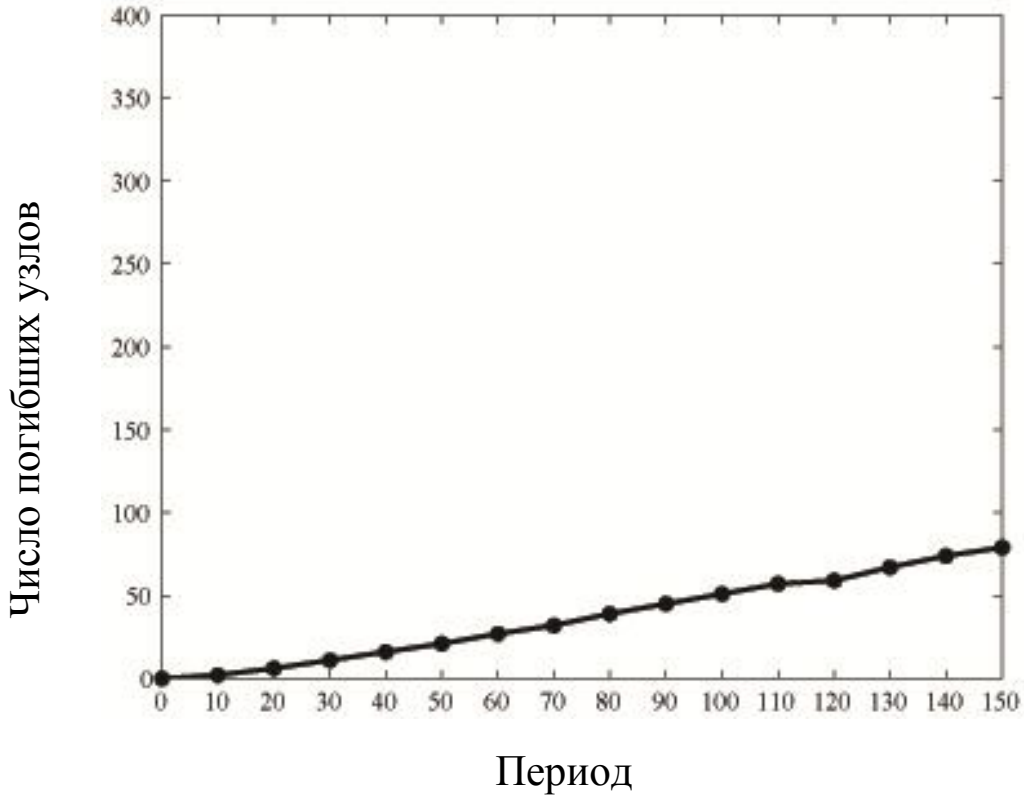


Рис. 5.6. Число погибших узлов.

Рис. 5.7 показывает сетевое покрытие, обеспечиваемое алгоритмом CSC. Как видно из рис. 5.7 CSC обеспечивает 100% покрытие в течение достаточно длительного времени.

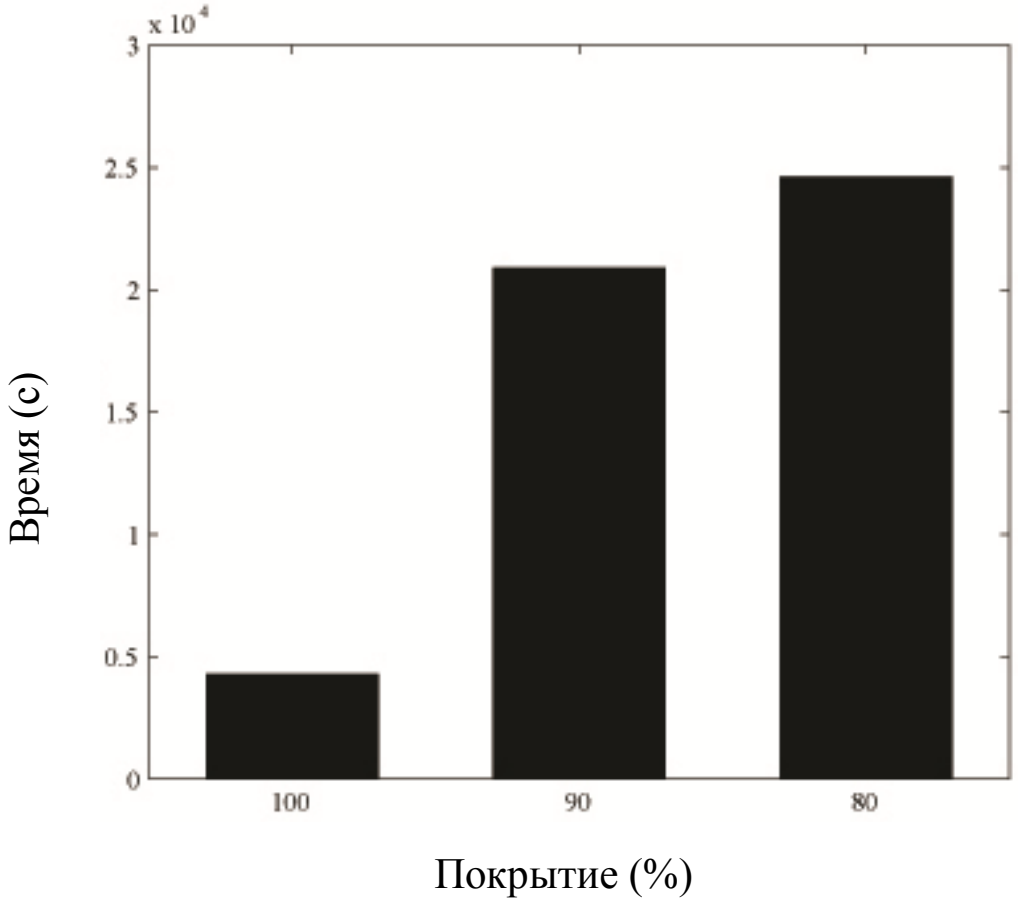


Рис. 5.7. Покрытие во времени.

5.3.2. Второй сценарий.

В этом сценарии сенсорные узлы случайно распределены на плоскости 200м*200м. Число сенсорных узлов 400. Шлюз фиксирован и расположен в центре сети. Сравним алгоритмы CSC и базовый LEACH.

На рис. 5.8 приведено сравнение жизненного цикла CSC и базового LEACH, где под жизненным циклом понимается время до гибели первого узла. Как видим, CSC обеспечивает существенно лучшие характеристики, чем базовый LEACH.

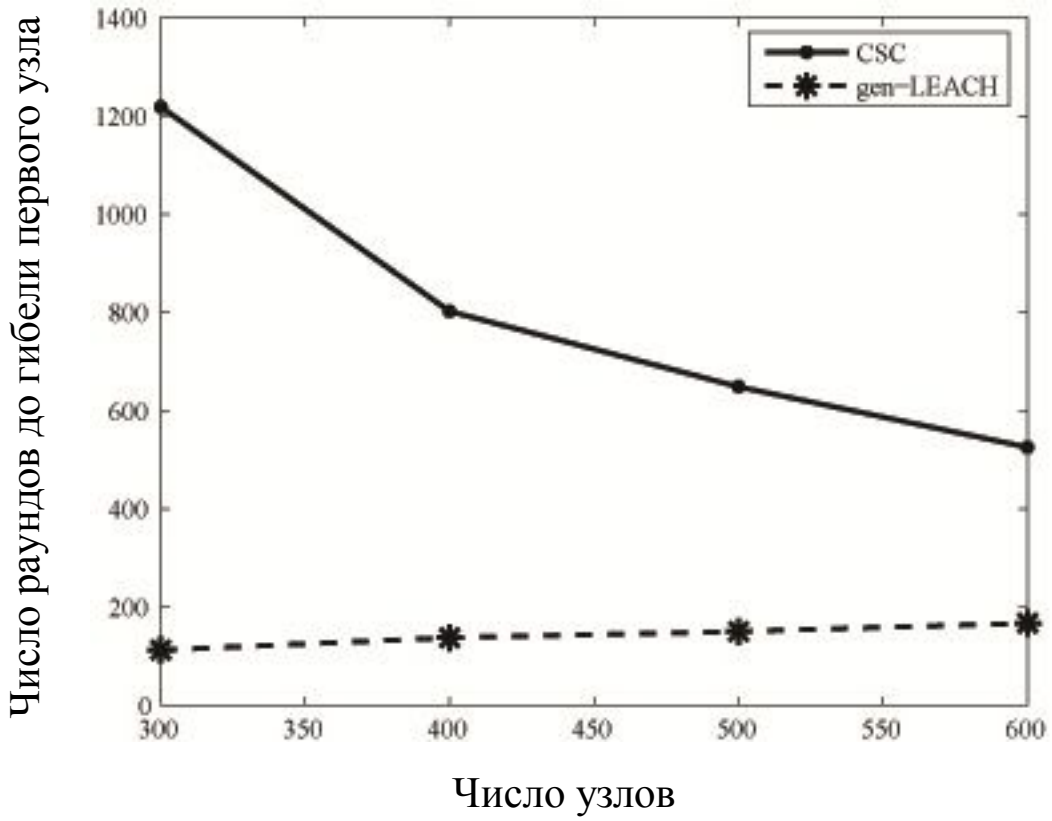


Рис. 5.8. Жизненный цикл CSC и базового LEACH (до гибели первого узла).

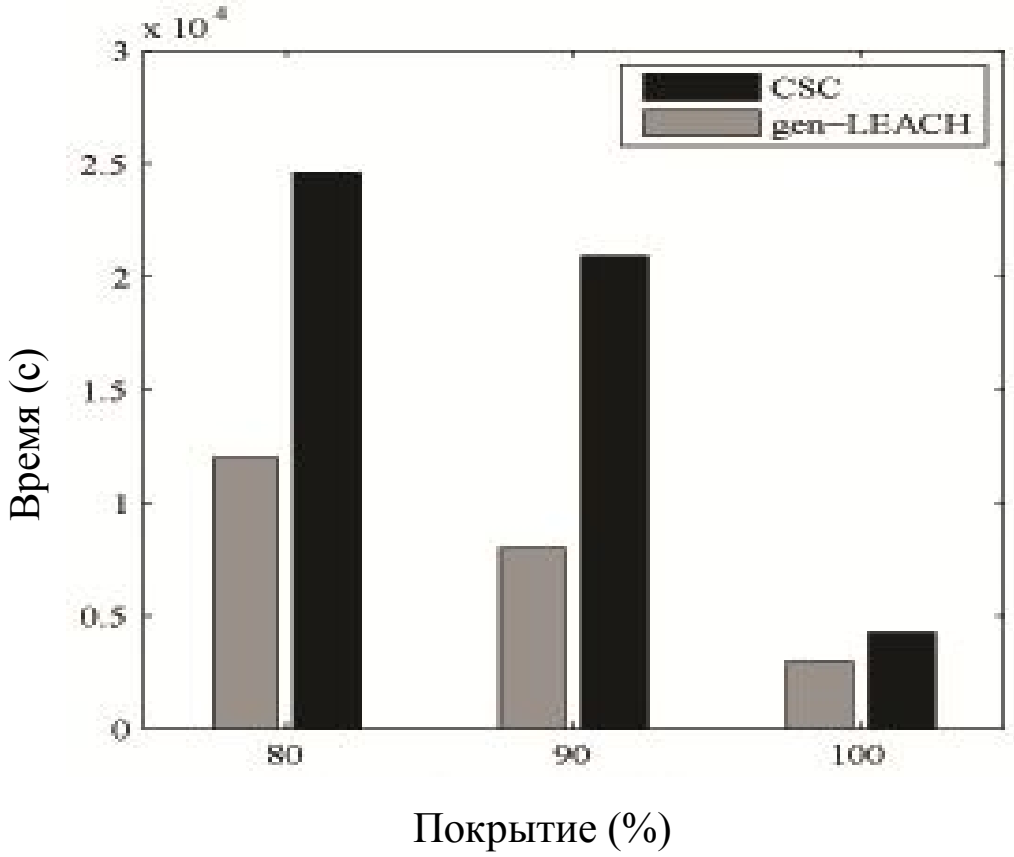


Рис. 5.9. Сравнение CSC и базового алгоритма LEACH по *k*-покрытию.

На рис. 5.9 показано сетевое покрытие в течение времени для CSC и базового LEACH. Как видно из рис.5.9, CSC обеспечивает существенно лучшие характеристики покрытия, чем LEACH.

6. Алгоритмы выбора головного узла для мобильных сенсорных сетей.

6.1. Мобильные сенсорные сети.

В последние годы появился новый вид сенсорных сетей – мобильные сенсорные сети MSN (Mobile Sensor Networks). Эти сети сохранили все особенности беспроводных сенсорных сетей USN и, кроме того, к этим особенностям добавилась ещё мобильность. Кластерная архитектура нашла применение и в USN, поэтому поиск наилучших вариантов организации кластера и выбора головного узла для MSN является сегодня актуальной задачей. В главе рассмотрен алгоритм кластеризации для MSN на основе использования предикторов. Алгоритм представляется адекватным для выбора головного узла кластера и организации кластеров в мобильных беспроводных сенсорных сетях.

Достаточно много исследований появилось в последние годы по проблемам создания беспроводных мобильных сенсорных сетей в области алгоритмов маршрутизации, покрытия, управления ресурсами, безопасности и т.д. Формируется следующий этап в развитии беспроводных сенсорных сетей. Алгоритмы, используемые при кластеризации в стационарных USN [73], не могут адекватно отражать процессы в MSN и, соответственно, требуется разработка новых.

В мобильных сенсорных сетях сенсорные узлы, как правило, устанавливаются на мобильных платформах и способны к географическому перемещению при необходимости. Заметим, что

в отличие от другого типа беспроводных сетей – мобильных Ad Hoc сетей [79,184], именуемых MANET, где мобильность рассматривается как неконтролируемый фактор, в MSN мобильность может рассматриваться как ценная управляемая способность [107,109], посредством которой смогут быть получены более интеллектуальные и более гибкие и адекватные к внешним условиям сенсорные сети, чем стационарные USN. Например, в [133] управляемая мобильность введена в сенсорный узел для обеспечения устойчивости сети. Указанный подход, правда, основывался на использовании предварительно определённых кабельных сетей и не позволял строить сеть для случайных событий. Подобный подход можно увидеть и в [191] для процессов размножения, когда сенсорный узел имеет возможность использовать три различные кабельные сети для оптимизации покрытия.

Естественным в этих условиях выглядит появление алгоритма LEACH – Mobile или LEACH – M [136] как варианта LEACH, который поддерживает мобильность. В алгоритме LEACH – M мобильный сенсорный узел декларирует себя членом кластера, когда он находится в движении, и затем подтверждает свою доступность к осуществлению сеанса связи (на основе TDMA) головному узлу кластера. Это может приводить, к сожалению [104], к динамическому вхождению и выбытию не головных узлов кластера в устойчивой фазе, когда члены кластеры зафиксированы после его формирования. Однако, в LEACH-M кластеры динамически формируются каждый раз, когда сенсор

перемещается, увеличивая накладные расходы в управлении кластером.

Основное различие между LEACH-M и подходом к созданию нового алгоритма состоит в том, что предлагаемый алгоритм обеспечивает существенное увеличение жизненного времени сети и стабильность сформированного кластера за счёт использования комбинированного критерия прогнозирования.

6.2. Комбинированный критерий прогнозирования.

В разделе предлагается комбинированный критерий прогнозирования, основанный на трёх эвристических предикторах.

6.2.1. Критерий связности

Связность является мерой возможностей взаимосвязи любого из сенсорных узлов с любым другим сенсорным узлом в сети.

На рис. 6.1 связность иллюстрируется с помощью зелёных линий между сенсорными узлами.

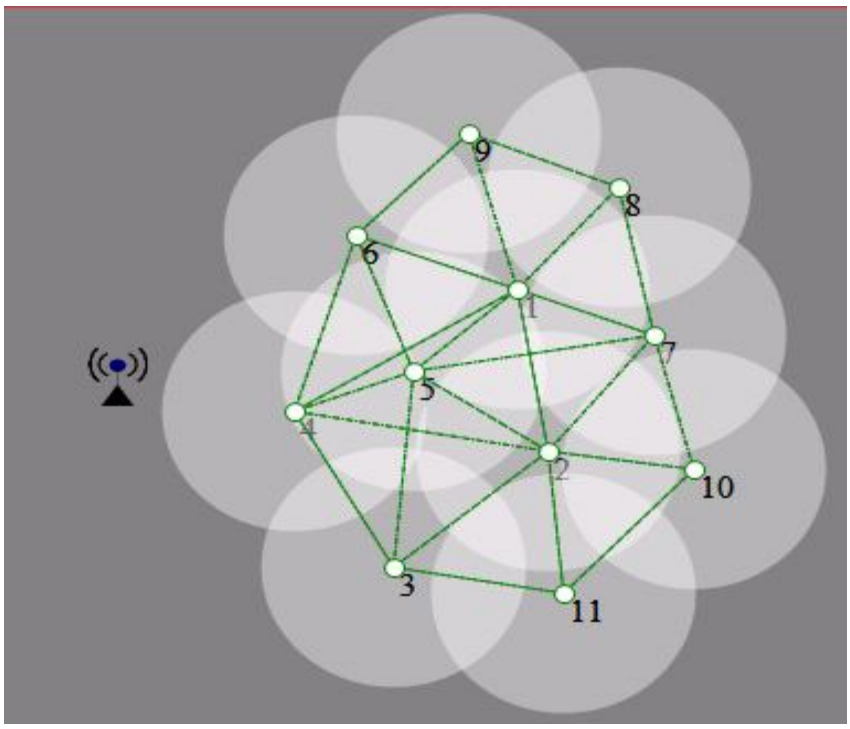


Рис. 6.1. Связность в сенсорной сети.

Рассмотрим мобильную беспроводную сенсорную сеть, состоящую из достаточно большого числа сенсорных узлов, обозначенных как $S = \{s_1,\ldots,s_n\}$. Сенсорные узлы распределены на достаточно большом сенсорном поле и предназначены для детектирования специфических событий. Областью взаимосвязи сенсорного узла s будем называть область, в которой сенсорный узел s может взаимодействовать непосредственно с другими сенсорными узлами. Максимальное расстояние между сенсорным узлом s_i и любым другим сенсорным узлом s_j, где s_j попадает в диапазон взаимосвязи s_i, будем называть пределом взаимосвязи (R_i) сенсорного узла s_i. Множество близлежащих к сенсорному узлу сенсоров представим как $N(s_i)$. Тогда $N(s_i)$ определяется из следующего уравнения:

$$N(s_i) = \{ s_j: d(s_i, s_j) < R_i\} \quad (6.1)$$

В (6.1) d – Евклидово расстояние между сенсорными узлами s_i и s_j. С учётом изложенного, критерий связности $ConC(s_i)$ в момент времени T может быть записан следующим образом:

$$ConC(s_i) = |N(s_i)| \quad (6.2)$$

6.2.2. Критерий покрытия.

Большинство подходов к выбору головного узла в кластере основано на балансе энергетических возможностей сенсорных узлов, но, как уже выше было отмечено, с точки зрения качества обслуживания целесообразно рассматривать проблему полного покрытия в течение достаточно большого периода времени, особенно для систем мониторинга. Предел действия сенсорного узла (r) сенсорного узла s определяется как максимальное расстояние между сенсором s и любой точкой ρ в области действия сенсора s. Точка ρ покрывается сенсорным узлом s, если Евклидово расстояние между ρ и s меньше, чем r сенсорного узла s.

Сегмент Seg_{ij} есть секция периметра покрытия сенсорного узла s_i, который в свою очередь покрывается сенсорным узлом s_j. Сегмент Seg_{ij} представляется в угловых терминах как закрытый интервал $[\Theta^s_{ij}, \Theta^b_{ij}]$, где Θ^s, Θ^b являются соответственно начальным и конечным углами сегмента Seg_{ij} для начальной и конечной точек.

Рассмотрим два сенсорных узла s_i и s_j и расстояние d между ними. Тогда, используя теорему косинусов, длина L_{ij} сегмента Seg_{ij} есть:

$$L_{ij} = \arccos\{\frac{r_i^2 + d^2 - r_j^2}{2d \times r_j}\} \quad (6.3)$$

Начальный и конечный углы могут быть определены как $\theta_{ij}^s = \frac{\theta_{ij} - L_{ij}}{2}$ и $\theta_{ij}^b = \frac{\theta_{ij} + L_{ij}}{2}$, где θ_{ij} является угловой координатой сенсорного узла s_i при определении направлении s_j относительно воображаемой линии полярной оси.

Перечень сегментов сенсорного узла s_i, обозначаемый как SL_i, является множеством таких сегментов, что:

- сегмент A в SL_i не может быть отнесен ни к какому-либо другому сегменту в SL_i, каждый сегмент в SL_i перекрывает точно два сегмента, причём один с другой стороны, за исключением двух сегментов (первый и последний сегменты), каждый из которых перекрывает только простой сегмент в SL_i.

С учётом изложенного можно записать критерий покрытия $CovC(s_i)$ в момент времени t следующим образом:

$$CovC(s_i) = \frac{Cov(s_i)}{2\pi} \quad (6.4)$$

Если $CovC(s_i)$ есть периметрическое покрытие сенсорного узла s_i, то справедливо следующее уравнение:

$$Cov(s_i) = \sum_{\forall Seg_{ij} \in SL_i} | Seg_{ij} | - \sum_{\forall Seg_{ij}, Seg_{ik} \in SL_i : j \neq k} | Seg_{ij} \cap Seg_{ik} | \quad (6.5)$$

6.2.3. Критерий мобильности.

Мобильность, естественно, является важнейшим фактором в принятии решения о выборе головного узла. С учётом частости изменения функций голоного узла целесообразно выбирать в качестве головного узел, который перемещается не очень быстро. Когда головной узел перемещается быстро, сенсорные узлы могут выпадать из кластера и, как результат, наступает реаффиляция. Реаффиляция имеет место, когда один или несколько сенсорных узлов переходят из одного кластера в другой кластер в течение интервала стабильного существования кластеров.

Вычисление мобильной скорости для каждого сенсорного узла s_i осуществляется по формуле:

$$MC(s_i) = \frac{\sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2}}{\Delta t}, \qquad (6.6)$$

В (6.6) $(x_t – y_t)$ и $(x_{t-1} – y_{t-1})$ - координаты сенсорного узла s_i в моменты времени t и $t-1$ и Δt – интервал времени между t и $t-1$.

6.2.4. Критерий остаточной энергии.

Головные узды кластеров отвечают за координацию взаимодействия членов кластера, агрегацию данных и их передачу на базовую станцию непосредственно или через многоранговые соединения. Поскольку головной узел кластера нуждается в приёме большого числа пакетов, то он затрачивает больше энергии, чем все другие узлы. В разработанном алгоритме DCA (Distributed Clustering Algorithm) головные узлы кластера периодически

проходят ротацию, что позволяет увеличить цикл жизни сенсорной сети.

Критерий остаточной энергии REC (s_i) определяется для каждого узла по следующей формуле:

$$REC(s_i) = E(s_i), \tag{6.7}$$

С учетом 6.2, 6.4, 6.6 и 6.7 комбинированный критерий $CC(s_i)$ для сенсорного узла s_i в момент времени t определяется следующей формулой:

$$CC(s_i) = \alpha \times ConC(s_i) + \beta \times CovC(s_i) + \frac{\gamma}{1 + MC(s_i)} + \xi \times REC(s_i), \tag{6.8}$$

В (6.8) $\alpha + \beta + \gamma + \xi = 1$.

6.3. Предикторы.

В этом разделе рассмотрим три эвристических предиктора, которые будут использованы при моделировании.
Комбинированный критерий прогнозирования CC должен быть предсказан в текущее время t_c в соответствии с историей этого критерия $HCC = [(CC_1, t_1), (CC_2, t_2), ..., (CC_n, t_n)]$, где $t_1 < t_2 < \ldots < t_n$. Для этого могут быть использованы:

- Простой точечный предиктор SPP (Single Point Predictor). Этот предиктор всегда предсказывает следующее значение как предыдущую величину HCC:

$$PCC = SPP(t_c) = CC_n \tag{6.9}$$

- Линейный экстраполяционный предиктор LEP (Linear Extrapolation Predictor). Для линейного экстраполяционного предиктора используется следующая формула:

$$PCC = LEP(t_c) = \frac{t_c - t_{c-1}}{t_n - t_{n-1}}(CC_n - CC_{n-1}) + CC_{n-1} \qquad (6.10)$$

Гибридный предиктор HP (Hybrid Predictor). Гибридный предиктор представляет собой смесь точечного и экстраполяционного предикторов.

$$PCC = \begin{cases} CC_n, & n \quad is \quad odd \\ \frac{t_c - t_{c-1}}{t_n - t_{n-1}}(CC_n - CC_{n-1}) + CC_{n-1}, & n \quad is \quad even \end{cases} \qquad (6.11)$$

Гибридный предиктор как правило использует линейное предсказание, но в отдельных случаях может учитывать скачкообразные изменения процесса.

Рассмотренные предикторы широко используются в мобильных сетях для предсказания маршрута перемещения мобильных станций, именно эти предикторы выбраны для построения алгоритмов выбора головного узла в мобильных сенсорных сетях.

6.4. Распределённый алгоритм кластеризации.

Рассмотрим новый алгоритм кластеризации DCA (Distributed Clustering Algorithm) [139].

Прежде, чем перейти к рассмотрению алгоритма, сделаем следующие предположения:

- Все сенсоры гомогенны с одинаковыми характеристиками.
- Топология сети может изменяться и сенсорные узлы могут перемещаться со скоростью от 0 до 2 м/с.
- Сенсорные узлы осуществляют свою активность без централизованного управления.

Введем параметр, называемый кластер-хоп. Кластер-хоп определяется как максимальное число сенсорных узлов между головным узлом кластера и периферийными узлами, включая последние. Этот динамический параметр определяет процедуру формирования кластера и служит как входной параметр для процесса формирования кластера.

DCA содержит две фразы: информационное обновление и формирование кластера.

В фазе информационного обновления каждый сенсорный узел вычисляет свои предикторы комбинированного критерия *PCC*. Далее, базируясь на значении кластер-хопа r_{hop}, осуществляется процесс распространения *PCC*. Во время фазы формирования кластера сенсорные узлы уже имеют взвешенный взгляд на свою близость и информацию о *PCC*.

6.4.1. Фаза 1: информационное обновление.

Прежде всего, каждый сенсорный узел вычисляет свой *PCC* в соответствии с каким-либо эвристическим предиктором. На втором шаге алгоритма вычисленное значение *PCC* передаётся в радиусе r_{hop} близлежащим сенсорным узлом. Полностью алгоритм распространения информации о *PCC* приведён в таблице 6.1.

В результате действия алгоритма каждый сенсорный узел сети имеет информацию об узлах, для которых *PCC* является наибольшим в области r_{hop} для близлежащих узлов. Синхронизация между узлами для реализации алгоритма не требуется вследствие того, что сенсорные узлы верифицируются при распространении информации о *PCC* в предварительно определённый промежуток времени. Алгоритм PCC позволяет формировать большие кластеры, ограниченные только значением радиуса r_{hop}.

Таблица 6.1. Алгоритм распространения информации о *PCC*.

1: Calculate Predicted Combined Criterion PCC(s_i)

2: $Max_i.CC \leftarrow PCC(s_i)$

3: $Max_i.id \leftarrow i$

4: **while** $r_{cl} > 0$ **do**

5: Transmit Max_i to $s_j \forall s_j \in N(s_j)$

6: Wait a period of time to receive the Max_i from all $s_j \in N(s_j)$

7: **if** all messages received **then**

8: Determine maximum $Max_j.CC$.

9: **if** $Max_j.CC > Max_i.CC$ **then**

10: $Max_i.CC = Max_j.CC$

11: $Max_i.id = Max_j.id$

12: **end if**

13: **end if**

14: $r_{cl} = r_{cl} - 1$

15: **end while**

6.4.2. Фаза 2: Формирование кластера.

После определения сенсорных узлов с наибольшим значением *PCC* можно перейти ко второй фазе алгоритма, на которой формируется собственно кластер. Далее не будем адаптировать подход к формированию кластера, в соответствии с которым сенсорный узел с наибольшим значением *PCC* приглашает войти в свой кластер другие близлежащие сенсорные узлы. Будем формировать кластер таким образом, чтобы все кластеры были более или менее одних размеров и более или менее одинаково распределены по сенсорным узлам, причём допуск сенсорных узлов в кластер осуществляется кластером самостоятельно. Для реализации указанного разработан распределённый кластерный алгоритм DCA (Distributed Cluster Algorithm), приведённый в таблице 6.2.

Таблица 6.2. Распределённый кластерный алгоритм (DCA).

1: **if** ($Max_i.id = I$ *or My_Cluster_Head* message received) **do**

2: s_i considered as Cluster head

3: Broadcast a *Cluster_Head*($CC(s_i)$) message for all neighbors

4: **else**

5: select node $s_j = Max_i.id$ as Cluster head

6: Broadcast a *My_Cluster_Head* message to s_j

7: **end if**

8: **if** (s_i received *Cluster_Head_message*) **then**

9: Wait a period of time

10: **if** (time expired) **then**

11: send *Join* message to s_j which has minimum *PCC*

12: **end if**

13: **end if**

14: **if** (s_i received *Join* message from s_j) **then**

15: Update the cluster table by s_j

16: **end if**

Алгоритм DCA функционирует следующим образом. Каждый сенсорный узел s_i, для которого определено наибольшее значение *PCC*, позиционирует себя как головной узел кластера и рассылает всем сенсорным узлам сообщение Cluster-Head, содержащее значение $PCC(s_i)$. Если же s_i не является претендентом на роль головного узла в кластере, то такой сенсорный узел выбирает узел с наименьшим значением *PCC* и направляет ему сообщение *Join* о вхождении в кластер. Головной узел собирает информацию от всех сенсорных узлов своего кластера в маршрутную таблицу и формирует её в зависимости от поступивших сообщений *Join*.

6.5. Результаты моделирования.

Программа моделирования была написана на языке C#.NET. Сенсорные узлы распределялись неравномерно случайным образом на плоскости. Предполагалось также, что сенсорные узлы имеют достаточно мощности, чтобы можно было покрыть расстояния до узла – получателя информации.

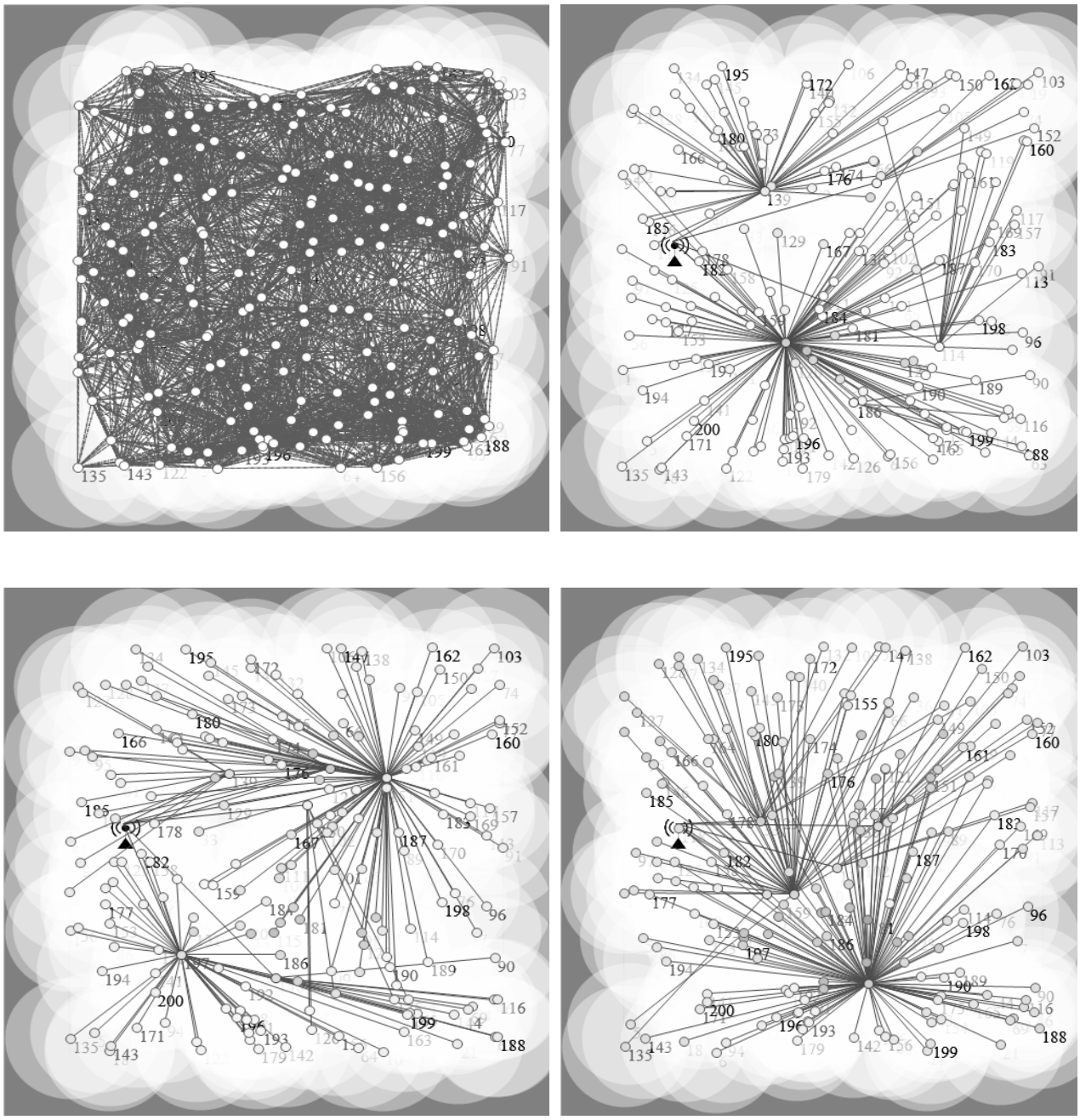


Рис. 6.2. Отображение модели на экране.

При моделировании использовалась стандартная энергетическая модель, когда все энергозатраты разделяются на две части: передача и приём сообщений. Параметры и их значения, используемые при моделировании, сведены в таблицу 6.3 и соответствуют типовым при исследованиях вопросов кластеризации в сенсорных сетях.

Таблица 6.3. Параметры и их значения, используемые при моделировании.

Параметр	**Обозначение**	**Значение**
Первичная энергия на узел	E	*2j*
Tx/Rx	E_{elec}	*50 nj/bit*
Постоянное усиление	ε_{fs}	*10 pj/bit/m*^{2}
Мультисетевая постоянная	ε_{mp}	*0.0013 pj/bit/m*^{2}
Потери на участках (экспоненциальные)	$\frac{\varepsilon_{fs}}{\varepsilon_{mp}}$	*87*
Размер пакета	K	*30 bytes*
Скорость пакета	B	*1 packet/s*
Радиус сенсора	R	*25 m*
Широкополосная зона вещания	R	*2r*
Радиус кластера	r_{hop}	*2r*

Для последующих исследований было выбрано 2 сценария. В первом сценарии исследуются вопросы эффективности DCA при использовании различных предикторов SPP, LEP и HP. Во втором сценарии, предложенный алгоритм сравнивается с известным LEACH-M [136]. Для оценки эффективности алгоритмов используется метрика жизненного цикла сети – интервал времени

между началом функционирования и гибелью последнего из живущих сенсорных узлов.

6.5.1. Первый сценарий.

В первом сценарии сенсорные узлы случайно распределены на плоскости размером 200м*200м. Число узлов в сети составляет 100. Целью моделирования является проверка эффективности критерия связности (α=1, β=0, γ=0 и ξ=0), критерия покрытия (α=0, β=1, γ=0 и ξ=0), энергетического критерия (α=0, β=0, γ=1 и ξ=0) и критерия мобильности (α=0, β=0, γ=0 и ξ=1) в алгоритме DCA при использовании SPP, LEP и HP предикторов.

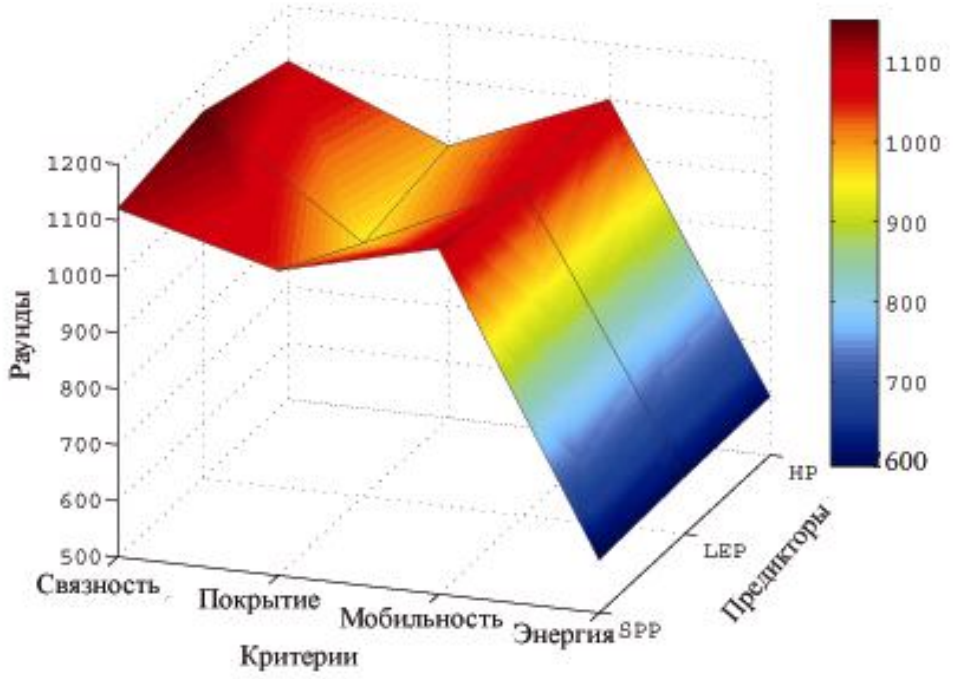


Рис. 6.3. Эффективность критериев в DCA.

На рис. 6.3 изображен жизненный цикл сенсорной сети для различных критериев в условиях использования различных предикторов. Как видим, критерий связности наилучшим образом подходит для обеспечения жизненного цикла сенсорной сети.

6.5.2. Второй сценарий.

В этом сценарии сенсорные узлы случайным образом распределены на плоскости 200м*200м и число сенсоров изменяется от 200 до 400 с шагом 50. Будем считать также, что $\alpha = \beta = \gamma = \xi = 0.25$.

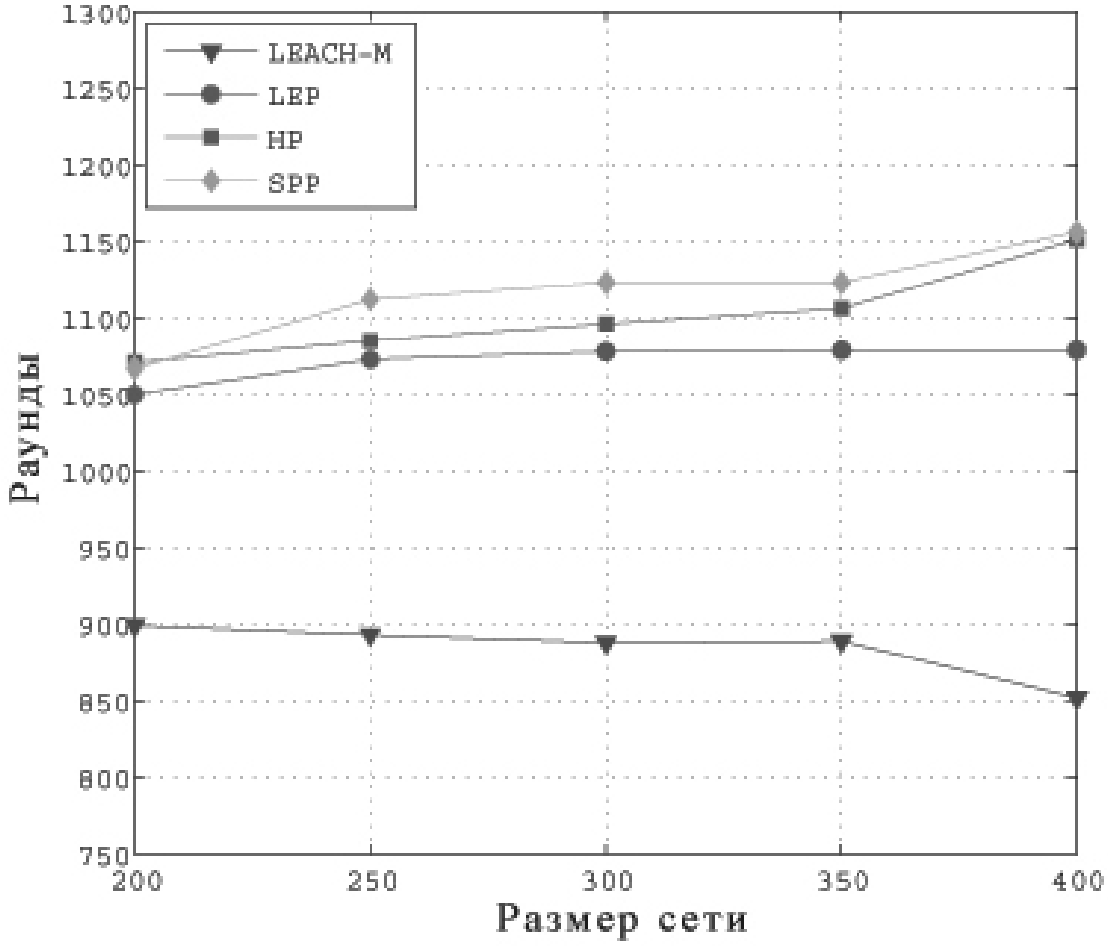


Рис. 6.4. Жизненный цикл сети с использованием различных версий DSA в сравнении с LEACH-M в случае, когда шлюз расположен в центре сети.

На рис. 6.4 шлюз расположен в центре сети. Простые расчёты могут показать, что в этом случае достигается минимальное значение Евклидова расстояния между узлами и шлюзом. На рис. 6.4 сравнивается жизненный цикл DCA с различными

предикторами (LEP, HP, SPP) с жизненным циклом сети при использовании классического алгоритма LEACH-M. Как видим, алгоритм DCA увеличивает жизненный цикл сети при использовании всех предложенных предикторов по сравнению с алгоритмом LEACH-M. Объяснение этому состоит в том, что LEACH-M использует случайный выбор головного узла (и как следствие – размера кластера), что может приводить к более быстрой гибели отдельных сенсорных узлов. Алгоритме же DCA головной узел выбирается с учётом множества критериев, что и обеспечивает хорошее распределение головных функций среди сенсорных узлов.

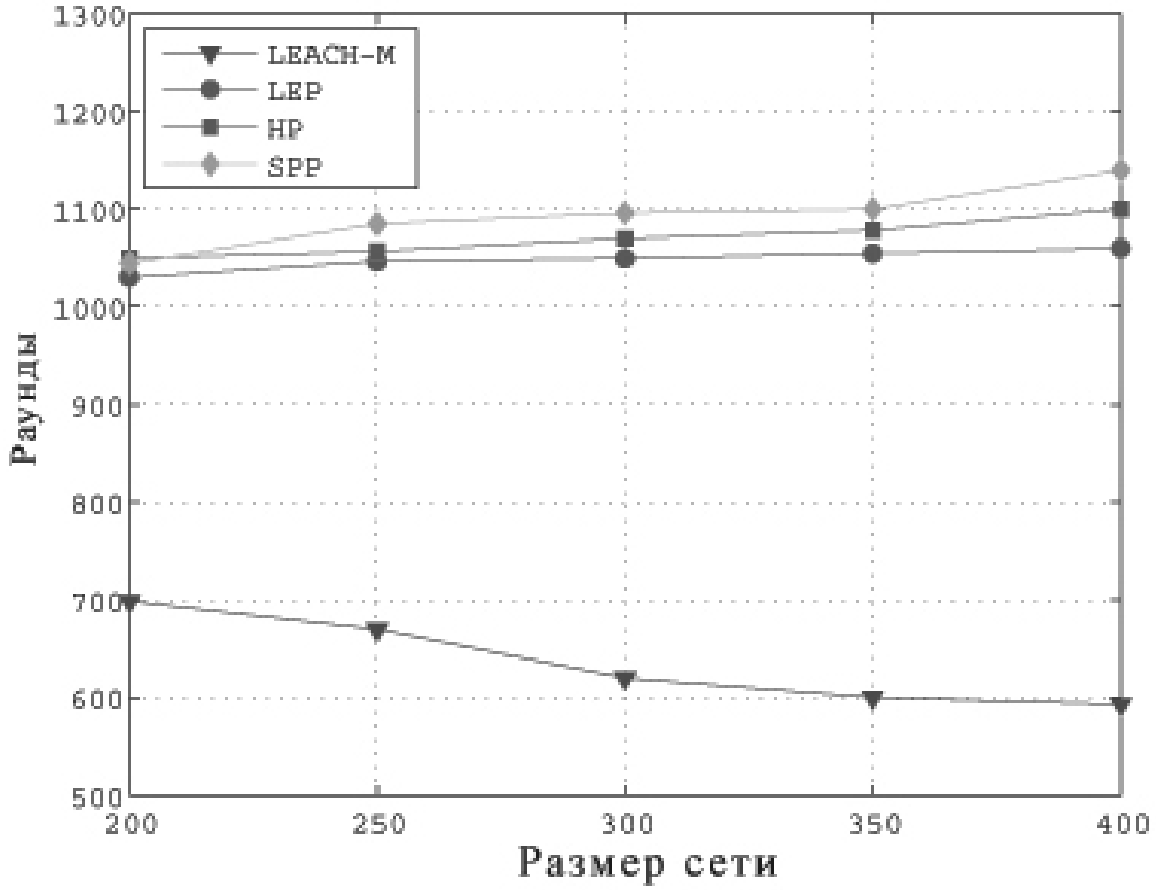


Рис. 6.5. Жизненный цикл сети для различных версий DSA в сравнении с LEACH в случае, когда шлюз расположен вне сети.

И в случае, когда шлюз расположен вне сети, алгоритм DSA обеспечивает более длительный жизненный цикл сети, чем алгоритм LEACH-M. Анализ зависимостей на рис.6.4 и рис. 6.5 показывает также, что простой предикатор SPP обеспечивает наибольший по длительности жизненный цикл сенсорной сети во всех рассмотренных случаях.

7. Семейство стандартов IEEE 802.15.

В настоящей главе будут рассмотрены общие принципы построения стандартов семейства IEEE 802.15, а также более подробно стандарты IEEE 802.15.1 (Bluetooth) [126] и IEEE 802.15.3 (высокоскоростные стандарты WPAN, в том числе UWB) [89,127,128], которые должны найти определенное применение в реализации концепции SUN в части IoT и WoT. В последующих главах будут подробно рассмотрены стандарт IEEE 802.15.4 [129,130] как базовый для USN, и протоколы ZigBee и 6LoWPAN. Отдельный раздел будет посвящен также работам по стандартам IEEE 802.15.6 [144,145], которые являются основой для создания медицинских сетей.

Рабочая группа IEEE 802.15 WPAN направляет свои усилия на разработку стандартов для WPAN сетей. Эти стандарты предназначены для организации в беспроводную сеть переносных и мобильных вычислительных устройств таких, как персональные компьютеры, КПК, периферийные устройства, мобильные телефоны, пейджеры, сенсоры и потребительская электроника, позволяя им общаться и взаимодействовать друг с другом. Одна из основных целей этой рабочей группы состоит в том, чтобы публиковать стандарты, практические рекомендации и нормативные документы, которые имеют широкий рынок применимости и позволяют эффективно решать вопросы сосуществования и взаимодействия с другими проводными и беспроводными сетевыми решениями. Рабочая группа IEEE 802.15 состоит из 6 подразделений.

Исследовательская группа 1: Занимается разработкой и стандартизацией физического и канального уровней стека протоколов Bluetooth. В 2002 году группой был выпущен стандарт IEEE 802.15.1-2002 на базе спецификации Bluetooth 1.1. После выхода обновленной спецификации Bluetooth 1.2 исследовательская группа представила новую версию стандарта IEEE 802.15.1-2005. После опубликования IEEE 802.15.1-2005 исследовательская группа 1 приняла решение, что все более поздние версии спецификации Bluetooth не станут в будущем стандартами IEEE.

Исследовательская группа 2: Рассматривает вопросы совместного функционирования беспроводных персональных сетей (WPAN) и других беспроводных систем, работающих в не лицензируемом частотном диапазоне, таких как WLAN.

Исследовательская группа 3: Занимается разработкой высокоскоростных WPAN, группой разработан стандарт IEEE 802.15.3-2003, регламентирующий функционирование физического и канальных уровней для построения сетей на скорости до 55 Мб/с. Позднее в 2005 году целевой группой IEEE 3b были разработаны поправки к стандарту, устраняющие некоторые ошибки и включавшие в себя некоторые оптимизации. В рамках целевой группы 3a долгое время предпринимались попытки разработать альтернативный физический уровень на базе технологии UWB [156,190].

Исследовательская группа 4: Исследования данной группы сосредоточены вокруг низкоскоростных WPAN. Данные сети отличаются надежностью передачи данных, невысокой пропускной способностью каналов, низким энергопотреблением. Первая редакция стандарта была выпущена в 2003 году. В марте 2004 года была сформирована исследовательская группа 4b, которая выпустила в 2006 году обновленную версию стандарта. Параллельно в исследовательской группе 4a велись работы по созданию альтернативного физического уровня на базе технологии UWB, позволяющей определять местоположение объекта с высокой точностью. Стандарт альтернативного физического уровня был выпущен в 2007 году.

Исследовательская группа 5: Целью исследований данной группы является ячеистая маршрутизация в WPAN сетях.

Исследовательская группа 6: Данная группа была организованна осенью 2007 года, объектом исследований данной группы выступают сети масштаба тела человека или как их еще называют – нательные сети (BAN), характеризующиеся малой мощностью и низкой частотой.

7.1. Стандарт IEEE 802.15.1

7.1.1. Общее описание.

Стандарт IEEE 802.11.1-2005 регламентируют беспроводную технологию Bluetooth, коммуникационную систему малого радиуса действия, призванную заменить кабельные соединения между портативными или фиксированными электронными устройствами.

Основные преимущества этой системы – устойчивость, низкое энергопотребление и стоимость.

Bluetooth сети функционируют в не лицензируемом частотном диапазоне 2,4 ГГц. Система использует передатчик с перескоком частоты для борьбы с интерференцией и затуханием и предоставления множества несущих с расширенным спектром (FHSS - Frequency Hopping Spread Spectrum). При радиочастотной передаче используется импульсная двоичная частотная модуляция, для упрощения конструкции передатчика.

Физический радиоканал разделяется между группой устройств, синхронизирующихся общим таймером. Устройство, передающее синхросигналы называется ведущим (master), все остальные – подчиненные (slave). Группа синхронизированных устройств образуют пикосеть (piconet). Устройства, входящие в такую сеть, используют специфичную модель перескока частоты, алгоритмически определяющуюся на основе полей адреса и таймера ведущего устройства. Простейшая модель смены частот – перебор в псевдослучайном порядке 79 частот. Адаптивная модель переключения может исключать использование некоторых частот, используемых другими устройствами в том же диапазоне (такими, как Wi-Fi устройства).

Для передачи данных физический канал делится на временные отрезки – слоты. Данные передаются в пакетах, размещенных во временных слотах, в некоторых случаях несколько слотов может предоставляться для передачи одного пакета. Над физическим

каналом расположены уровни, образующие физические соединения (physical link) и формирующие логические каналы и соединения с помощью специальных протоколов. Физическое соединение организуется между устройствами, передающими пакеты. В рамках пиконет физическое соединение может быть только между ведущим и ведомым устройствами. Физическое соединение предназначено для организации одного и более логического соединения, поддерживающего передачу синхронной, асинхронной и изохронной нагрузок, а также широковещательной рассылки. Нагрузка в логическом соединении мультиплексируется в физическое соединение занятием временных слотов, на основе функции распределения в менеджере ресурсов.

7.1.2. Архитектура ядра системы

Ядро системы (core system) охватывает четыре нижних сегмента и связанные с ними протоколы, определенные стандартом и общим профилем доступа GAP (generic access profile). Законченное приложение требует определенное количество дополнительных услуг и протоколов верхнего уровня, детализированных в спецификациях Bluetooth, и не входящих в стандарт IEEE 802.15.1. Рис. 7.1 демонстрирует архитектуру ядра системы.

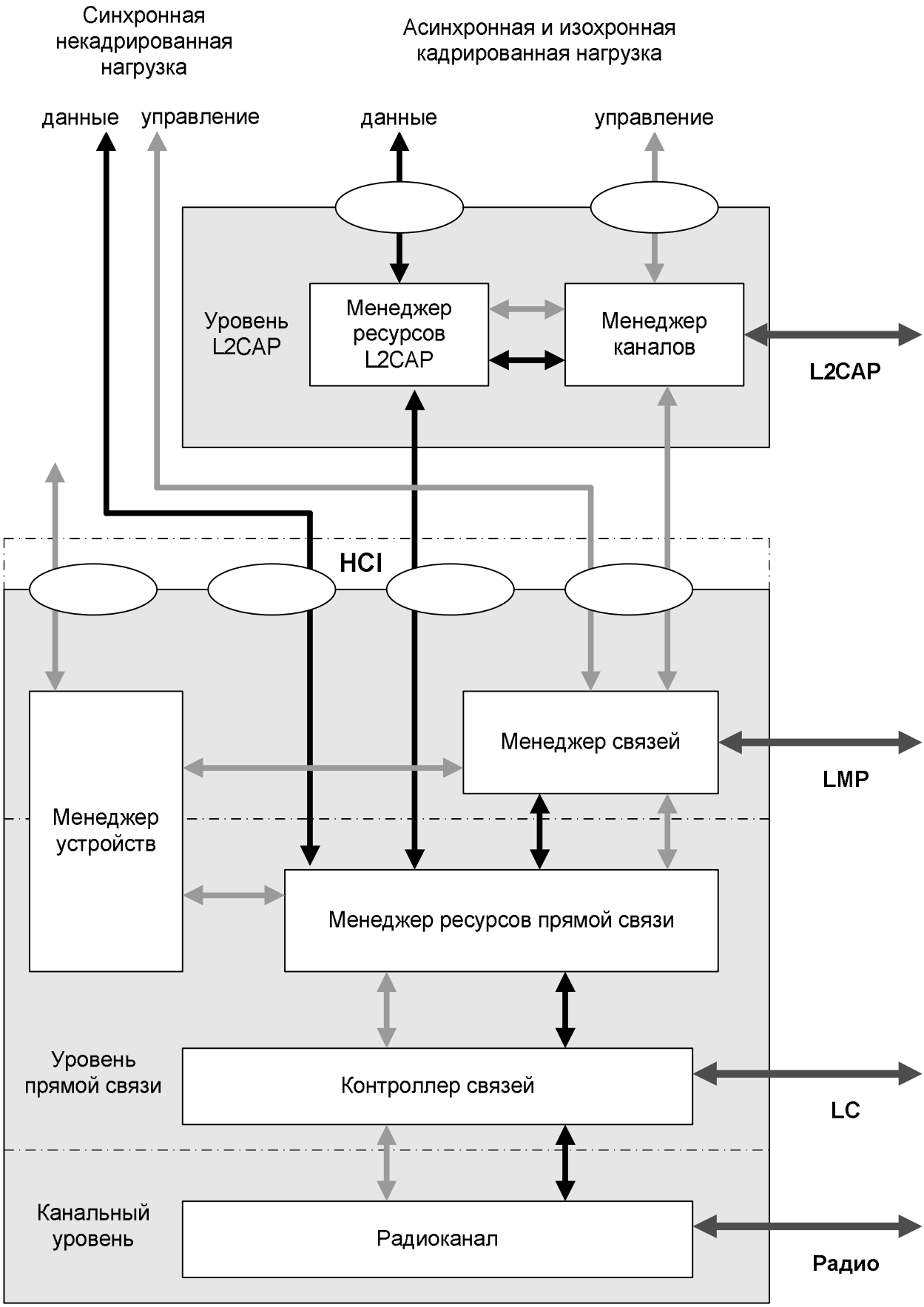


Рис. 7.1. Архитектура ядра системы.

Ядро системы представляет четыре нижних уровня, каждый с ассоциированным коммуникационным протоколом. Нижние три уровня иногда группируют в подсистему (известную как контроллер). Часто при реализации стандарта реализуют физический коммуникационный интерфейс (называемый также хост контроллер интерфейс HCI – host controller interface) и всю остальную систему, включающую в себя протокол управления и адаптации логических соединений L2CAP (Logical Link Control and Adaptation Protocol), услуги и протоколы верхнего уровня (называемые хостом) [111,112]. Этот стандарт обеспечивает взаимодействие между независимыми системами, определяя протокол сообщений, которыми обмениваются эквивалентные слои, а также взаимодействия между отдельными подсистемами путем определения общего интерфейса между контроллером и хостом.

Стандарт взаимодействия определяется для всех операций между устройствами. Протоколы ядра системы включают в себя радиочастотную передачу, протокол управления соединениями (LCP – Link Control Protocol), протокол обслуживания соединений (LMP – Link Management Protocol) и протокол L2CAP, каждый из которых полностью определен в стандарте IEEE 802.15.1.

Ядро системы предоставляет сервисы через точки доступа к сервисам (SAP), показанные на рис.7.1 в виде овалов. Услуги состоят из основных примитивов, контролирующих работу системы. Услуги можно разделить на три части:

– услуги управления устройствами, модифицирующие поведение и состояние устройств;
– услуги управления транспортом, создающие, модифицирующие и удаляющие транспортные потоки (каналы и соединения);
– услуги данных, используемые для передачи данных через транспортные потоки.

Так как архитектура определяется с возможностью разделения коммуникаций между хостом и контроллером через HCI интерфейс, сделан ряд общих допущений. Предполагается, что контролер имеет ограниченные возможности в буферизации данных по сравнению с хостом. Поэтому, L2CAP выполняет некоторое простое управление ресурсами при подаче протокольных блоков данных (PDU) на контроллер для транспортировки на заданное устройство. Управление включает в себя разделение сервисных блоков данных (SDU) на более удобные в обслуживании PDU и, впоследствии, фрагментацию PDU на пакеты, подходящие по размеру буферу контролера. Также проверяется наполнение буфера контролера, чтобы убедится в наличии каналов с требуемыми параметрами качества обслуживания (QoS). L2CAP протокол может опционально предоставлять возможности обнаружения ошибок и повторной передачи пакетов. Эта функция рекомендуется для приложений с высокими требованиями к надежности передачи данных пользователя. Еще одной функцией протокола L2CAP является управление потоком на основе окна, которое может быть использовано для контроля буфера в

принимающем устройстве. Оба эти необязательных параметра позволяют увеличить качество обслуживания в некоторых сценариях.

Для создания, обслуживания и уничтожения L2CAP каналов транспортировки протоколов услуг и потоков данных от приложений применяется менеджер каналов. Менеджер каналов взаимодействует с локальным менеджером соединений (LM) для создания новых логических соединений, а также конфигурации данных соединений на предоставление транспортных потоков с заданным качеством обслуживания. Данные от приложений поступают на менеджер ресурсов L2CAP, который отвечает за передачу фрагментированных PDU на уровень прямой передачи (BB), а также контролирует использование физических каналов. Поведение устройства контролируется с блока управления устройством. Созданием, обслуживанием и уничтожением логических каналов, а также обновлением параметров, связанных с физическими соединениями между устройствами занимается блок администрирования соединений (LM). Для связи с LM другого устройства применяется протокол администрирования соединений (LMP). Доступ к физическим каналам, происходит с помощью блока управления ресурсами BB. В задачи контроллера соединений входит кодирование и декодирование пакетов. Контроллер соединений использует протокол управления соединениями LCP, позволяющий управлять потоком данных, а также передавать сигналы подтверждения и запросов повторной передачи. Блок RF

предназначен для передачи и приема пакетов с данными на физическом канале.

7.1.3. Система передачи данных

Ядро системы предоставляет несколько стандартных типов транспорта для передачи данных протоколов услуг и приложений. Рис. 7.2 демонстрирует их.

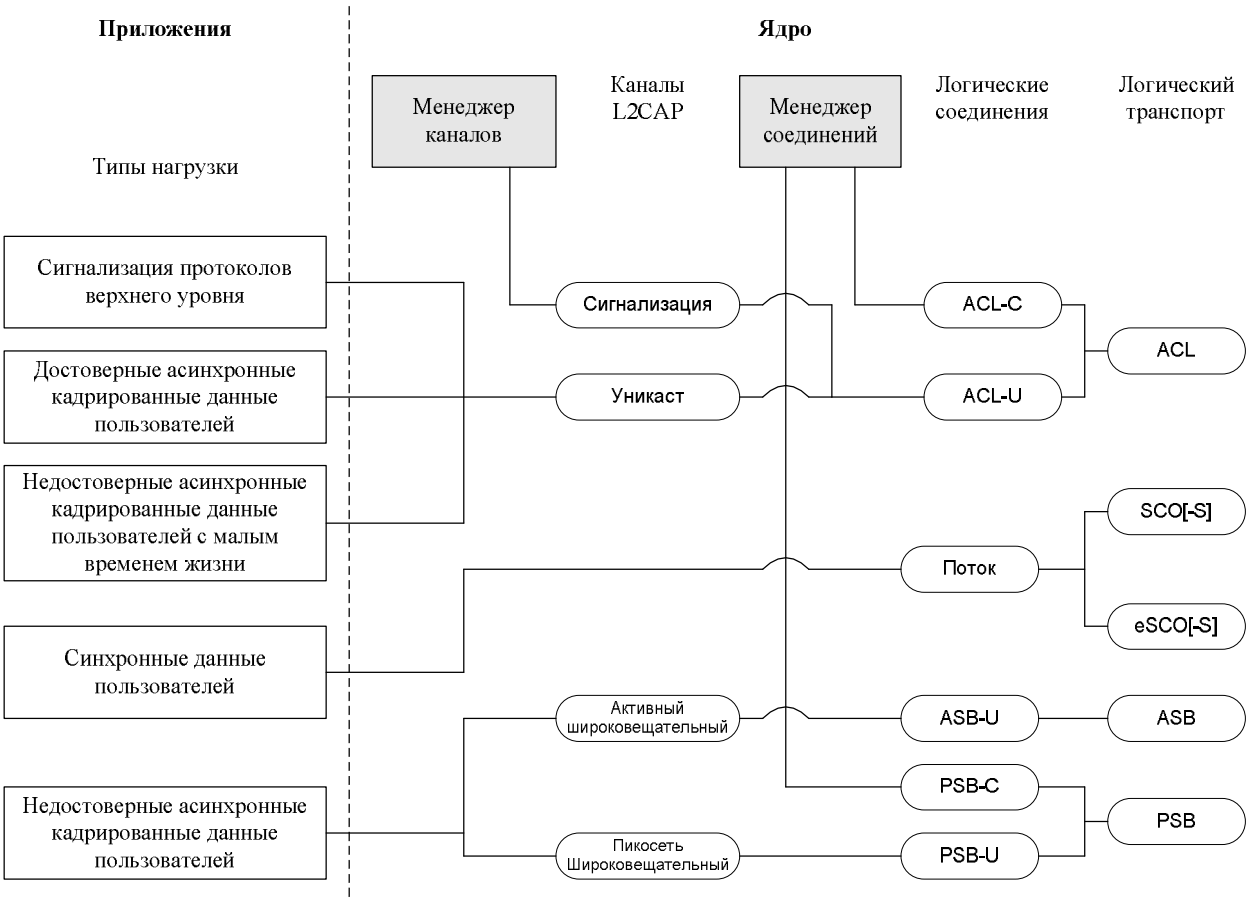


Рис. 7.2 Типы транспорта.

Транспорт, доступный для приложения, показан на рисунке в виде закрашенных прямоугольников. Логические соединения представлены на рисунке с помощью имени связанного с ним логического транспорта и суффикса, определяющего тип передаваемых данных. Буква «C» обозначает соединения управления, использующее протокол LMP, «U» показывает

передачу пользовательских данных (L2CAP PDU), а буква «S» является признаком потоковых соединений, транспортирующим не форматируемые синхронные или изохронные данные. На рисунке также представлены различные типы данных, которые можно передавать в сети.

L2CAP сервис предоставляет основанный на кадрах транспорт для передачи асинхронных и изохронных данных. Приложение передает данные для услуги в кадрах различного размера. вплоть до установленного максимального размера кадра в канале, и эти кадры доставляются в том же самом виде ожидающему приложению на удаленном устройстве. Каналы, ориентированные на соединение, могут быть установлены для передачи уникаст (точка-точка) данных между двумя устройствами. Для передачи широковещательных пакетов используют каналы без установления соединений. Учитывая топологию пикосеть, только ведущее устройство может стать источником широковещательного пакета. Поток данных при широковещательной рассылке однонаправленный, в случае передачи данных точка-точка каналы могут быть как однонаправленными, так и двунаправленными.

Каналы L2CAP имеют связанные с ними параметры качества обслуживания, которые устанавливают ограничение на передачу пакетов. Например, эти параметры позволяют обозначить, что трафик является изохронным, и, следовательно, имеют ограниченный срок жизни, после чего они становятся недействительными, или о том, что данные являются надежными и

должны быть доставлены без ошибок как бы много времени это заняло.

Если приложению не требуется доставка данных в кадрах, возможно потому, что оно передает уже кадрированный поток, тогда можно отказаться от использования каналов L2CAP и использовать BB соединение напрямую. Некадрируемые потоки используют логический транспорт SCO.

Ядро системы поддерживает прямую транспортировку изохронных данных приложения или данных с постоянной скоростью передачи, используя поток SCO или расширенный поток SCO. Эти логические соединения резервируют необходимую полосу пропускания физического канала и предоставляют транспорт с постоянной скоростью. Данные передаются в пакетах фиксированного размера в фиксированные интервалы, которые определяются во время установки канала. Соединения eSCO предоставляют больший выбор скоростей, а также обеспечивают более высокую надежность благодаря использованию повторной передачи в случае ошибки.

Для обеспечения надежности передачи данных в областях с высоким радиочастотным шумом предусматривается несколько степеней защиты на каждом уровне. В заголовках пакетов BB уровня используют прямую коррекцию ошибок (FEC) для обеспечения возможности коррекции ошибок приемником и контроль ошибок в заголовках (HEC) для определения наличия ошибок после коррекции. Некоторые виды BB пакетов включают

FEC для защиты полезной нагрузки. Также некоторые пакеты включают в себя поле контроля с помощью циклического избыточного кода (CRC).

На уровне логического транспорта ACL результаты алгоритма нахождения ошибок используются для организации простого ARQ протокола. Это позволяет повысить надежность с помощью повторной передачи пакетов, не прошедших проверку на наличие ошибок. Соединения eSCO используют модифицированную версию этой схемы для повышения надежности, разрешая ограниченное число повторных передач.

L2CAP предоставляет дополнительный уровень контроля ошибок, разработанный для определения ошибок, неконтролируемых протоколом BB, и организации запроса на повторную передачу поврежденных данных. Это обеспечивает уровень надежности, требуемый типичными приложениями.

Широковещательные пакеты не имеют обратного маршрута, поэтому использование ARQ схемы невозможно, однако приемник все же может определить ошибки в принимаемых пакетах. Для обеспечения надежности каждый пакет при широковещательной рассылке передается по нескольку раз в надежде, что хоть одна копия будет передана без ошибки. Даже с применением данного подхода нет полной гарантии успешной доставки данных всем получателям.

Передатчик может удалить пакеты из очереди, поэтому приемник не получит части пакетов в последовательности. Определение данного типа ошибки ложится на L2CAP.

7.1.4. Объекты транспортной структуры

Взаимодействие объектов транспортной структуры показывает Рис. 7.3.

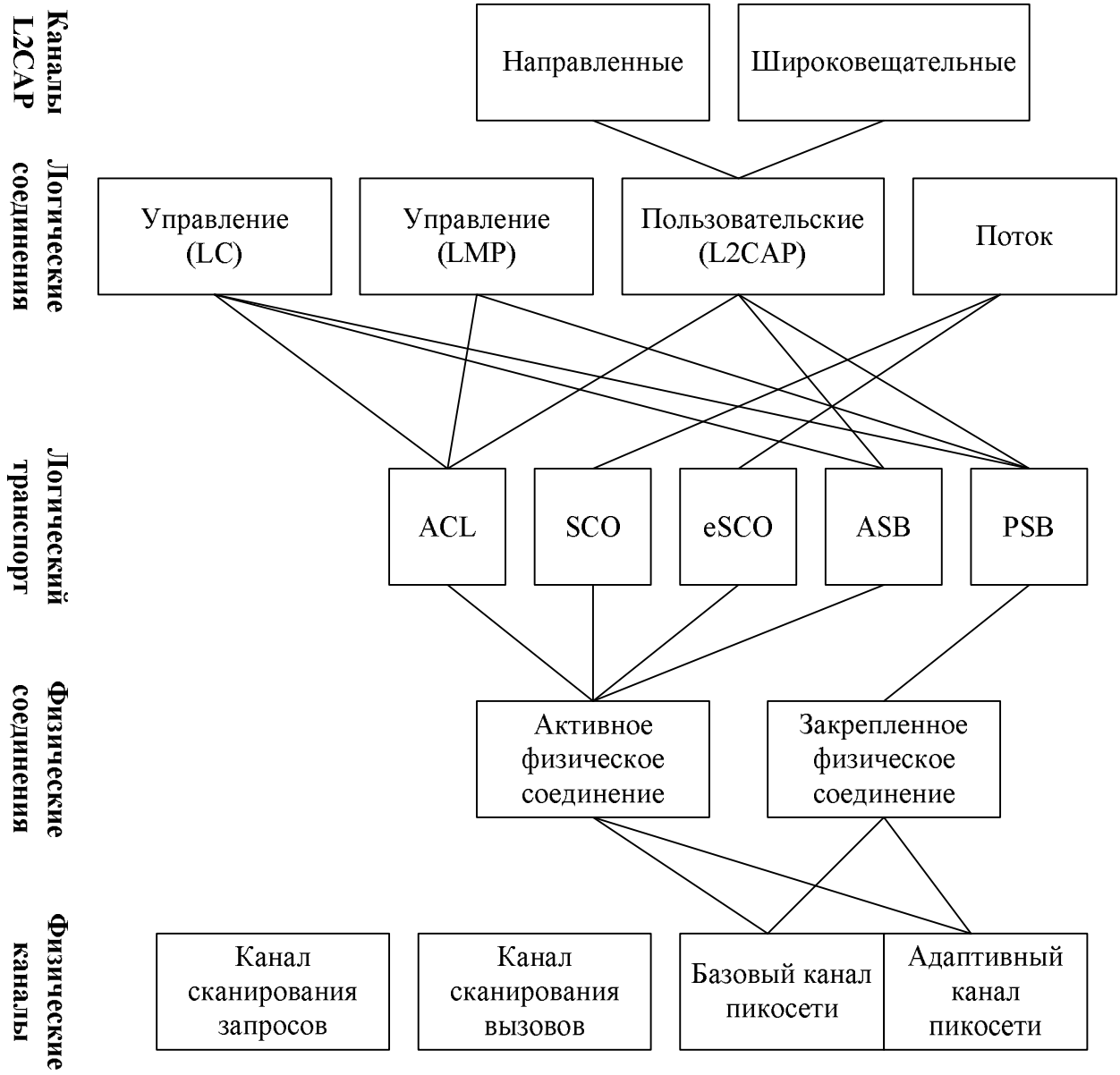


Рис. 7.3. Элементы транспортной архитектуры.

7.1.5. Общая структура пакета

В общей структуре пакета отражены архитектурные слои, встречающиеся в стандарте IEEE 802.15.1. Структура пакета предназначена для оптимального использования в условиях нормальной эксплуатации. Общую структуру показывает Рис.7.4.

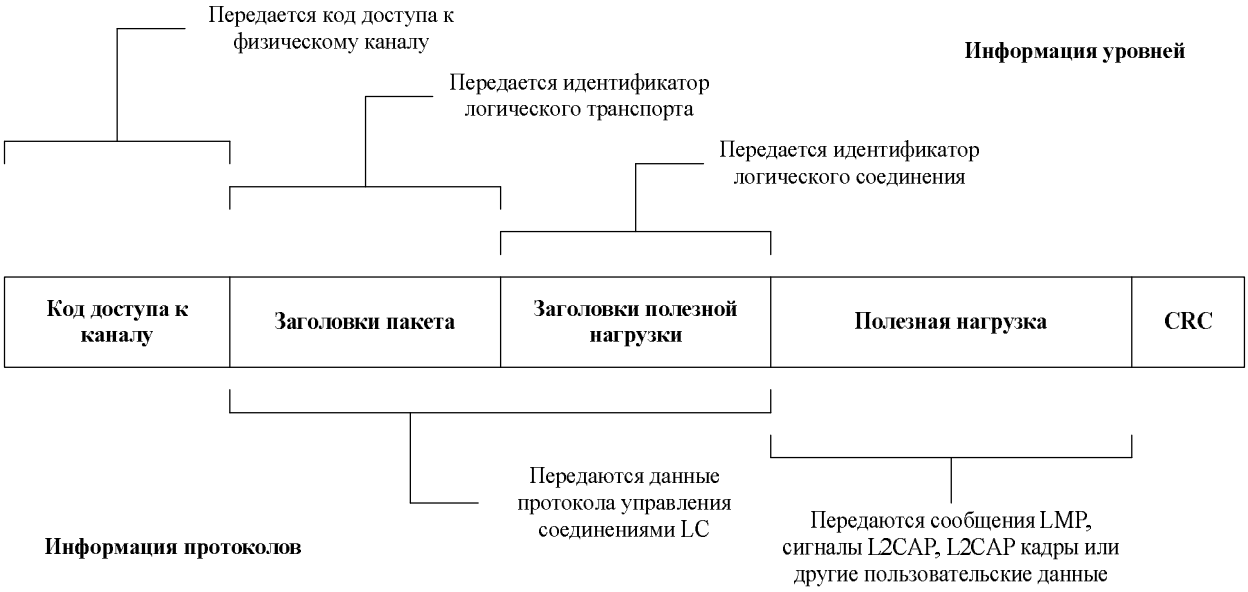


Рис.7.4. Структура пакета.

Пакет обычно включает в себя только те слои, которые необходимы для предоставления слоев, используемых при передачи данных. Например, простейший запрос на физическом канале присоединения не создает каких-либо логических соединений, поэтому содержит в себе лишь код доступа к каналу (CAC), связанный с физическим каналом. При обычной коммутации внутри пикосети используются пакеты со всеми полями, так как данные проходят через все архитектурные уровни.

Все пакеты включают в себя CAC, он используется для идентификации коммуникации на определенном физическом

канале. Для адресации устройств не выделяется специального поля, вместо этого идентификатор LT_ADDR помещается в заголовок пакета. Большинство пакетов содержит в себе заголовок пакета, который помимо адреса устройства включает в себя часть данных LCP протокола.

Заголовок полезной нагрузки содержит в себе идентификатор логического соединения (LLID), используемый для маршрутизации нагрузки, и поле, показывающее длину полезной нагрузки. Некоторые типы пакетов также содержат поле CRC проверки в конце пакета.

Полезная нагрузка используется для транспортировки пользовательских данных. Интерпретация этих данных зависит от типа логического транспорта и LLID, например, для транспорта ACL в полезной нагрузке совместно с данными от приложений передаются сообщения LMP и сигнализация L2CAP. Для потоков SCO и eSCO нагрузка содержит только пользовательские данные.

7.1.6. Физические каналы.

Самым нижним уровнем архитектуры является физический канал. Определено несколько видов физических каналов, каждый из которых характеризуется радиочастотой в комбинации с временными параметрами. Для уменьшения эффекта интерференции на всех видах каналов периодически происходит смена частот.

Два устройства используют общий физический канал для связи. Для достижения этой цели их приемо-передатчики должны

быть одновременно настроены на одну и ту же частоту и они должны быть в номинальном диапазоне друг от друга. Учитывая, что число несущих радиочастот ограничено, и что в одних и тех же пространственных и временных областях может действовать большое количество устройств, существует высокая вероятность появления двух независимых устройств, настроенных на одну несущую, что в результате приведет к коллизии на физическом канале. Чтобы смягчить нежелательные последствия коллизий, каждая передача на физическом канале начинается с кода доступа, использующегося в качестве корреляционного кода устройствами, настроенными на физический канал. Код доступа всегда присутствует в начале каждого передаваемого пакета.

Стандартом определяются четыре физических канала. Каждый из них оптимизирован и предназначен для определенных целей. Два из этих каналов (базовый и адаптивный физические каналы пикосети) используются для связи между подключенными устройствами и связанны с конкретной пикосетью. Оставшиеся физические каналы используются для обнаружения устройств (физический канал сканирования запросов), а также для подключения устройств (физический канал сканирования вызовов).

Устройство может использовать только один из этих физических каналов в определенный момент времени. В целях поддержки конкурентного доступа к среде устройство обеспечивает временное разделение каналов (TDM). Таким образом, устройство может одновременно работать в нескольких пикосетях, а также обнаруживать и подключаться к любой из них.

Всякий раз, когда устройство синхронизируется по времени, частоте и коду доступа к физическому каналу, оно называется подключенным к этому каналу (независимо от того, вовлечено оно или нет в передачу данных в канале). Стандарт предполагает, что устройство может быть подключено только к одному физическому каналу в любой момент времени, однако продвинутые устройства могут быть способны подключаться одновременно к нескольким физическим каналам, но этот процесс не описывается в стандарте.

Базовый физический канал пикосети характеризуется использованием псевдослучайной последовательности смены частот. Последовательность смены частот уникальна для каждой пикосети и зависит от физического адреса ведущего устройства. Стадия последовательности смены частот определяется встроенным таймером (CLKN) ведущего устройства. Все устройства входящие в пикосеть синхронизируются с каналом. Канал делится на временные интервалы, где каждый слот соответствует определенной частоте. Временные слоты пронумерованы в соответствии с CLKN ведущего устройства.

Контроль доступа к базовому физическому каналу осуществляется ведущим устройством. Ведущее устройство может начать передачу только в четные интервалы, его пакеты позволяют синхронизировать сеть. Пакеты, переданные ведущим устройством, могут занимать до пяти временных интервалов в зависимости от типа.

Каждая передача ведущего устройство содержит информацию об одном из логических каналов, в ответ на это ведомые устройства могут передавать свои данные. Характеристики ответа определяются логическим транспортом. Например, если была дана информация о логическом транспорте ACL, ведомое устройство, которому был адресован пакет, может передать с начала следующего временного слота (нечетного) пакет с информацией для того же логического транспорта. Такой пакет может занимать до 5 временных интервалов в зависимости от типа. При широковещательной рассылке ни одно из ведомых устройств не может ответить.

Базовый канал может быть совместно использован любым количеством устройств, ограниченным только количеством ресурсов, доступным ведущему устройству. Только одно устройство в пикосети может быть ведущим и именно с ним происходит весь обмен информацией. Физический канал не поддерживает передачу данных напрямую между ведомыми устройствами.

Однако существует ограничение на количество логических связей, которые могут быть поддержаны в рамках пикосети. Это означает, что существует ограничение на количество устройств, которые могут активно участвовать в обмене данных с ведущим устройством.

Базовый физический канал пикосети поддерживает ряд физических связей, логических транспортов и услуг, а также L2CAP каналов, используемых в целях коммуникации.

Адаптивный физический канал пикосети отличается от базового двумя свойствами. При передаче данных ведомым устройством частота не пересчитывается, а остается той же, на которой осуществлялась передача ведущего устройства. Адаптивный канал может основываться на меньшем наборе, чем 79 частот. Некоторые из частот могут быть помечены как неиспользуемые. Топология и поддерживаемые уровни для адаптивного канала идентичны базовым.

Для того чтобы устройство могло быть обнаружено другим участниками пикосети, используется физический канал сканирования запросов. Обнаруживаемое устройство прослушивает канал в ожидании запроса, а после получения начинает отсылать ответы. Для того чтобы устройство могло обнаружить другие устройства, оно перебирает все доступные физическому каналу частоты в псевдослучайной последовательности, отправляет запрос на каждой частоте и прослушивает канал в ожидании ответа.

Физический канал сканирования запросов использует более медленную модель переключения частот и требует кода доступа для исключения случаев занятия одной и той же частоты совместно двумя устройствами, использующими различные физические каналы. Код доступа берется из зарезервированного набора кодов запроса доступа (IAC), распределенного между всеми

устройствами. Один код доступа используется для общего запроса и ряд дополнительных кодов доступа зарезервированы для ограниченных запросов.

Устройства, которые готовы принять подключения, задействуют физический канал сканирования вызовов. Соединяемые устройства прослушивают канал в ожидании вызова, после чего обмениваются последовательностью сообщений с вызывающим устройством для установления соединения. Для того, чтобы устройство могло соединиться с другим устройством, оно перебирает все доступные каналу частоты в псевдослучайной последовательности, отправляет запрос на каждой частоте и прослушивает в ожидании ответа.

Для доступа к физическому каналу сканирования вызовов применяется код, получаемый из адреса сканирующего устройства. На данном типе каналов используется более медленная скорость смены частот по сравнению с базовым и адаптивным физическими каналами. Алгоритм выбора следующей частоты использует показания встроенного таймера устройства в качестве входных данных.

7.1.7. Физические соединения.

Базовый и адаптивный каналы пикосети поддерживают физические соединения, которые могут быть активными или закрепленными. Физическое соединение представляет собой соединение точка – точка между ведущим и ведомым устройством.

Оно всегда присутствует, когда ведомое устройство синхронизировано в пикосети.

Физическое соединение называется активным, если между устройствами по умолчанию используется логический транспорт ACL. Активное физическое соединение может быть переведено в режимы HOLD или SNIFF, что позволяет модифицировать время, когда соединение активно и может обслуживать нагрузку.

Физическое соединение между ведущим и ведомым устройством называется закрепленным, если ведомое устройство синхронизировано в пикосети, но не имеет активного ACL логического транспорта. Для регулярной синхронизации таких устройств применяются сигнальные последовательности (beacon train) – специальные временные интервалы.

7.1.8. Логические соединения.

Для поддержки требований транспорта данных от различных видов приложений существует набор логических соединений. Каждое логическое соединение связанно с логическим транспортом, который имеет ряд особенностей. Эти характеристики включают в себя контроль потока, передачу подтверждений, механизмы повторной передачи, нумерацию последовательностей и т.д. Логический транспорт может обслуживать различные типы логических соединений. Логический транспорт может быть передан с помощью активного физического соединения поверх базового или адаптивного физических каналов пикосети.

Идентификаторы логического транспорта и сигнальная информация реального времени передаются в заголовках пакета, а для некоторых логических соединений в заголовках полезной нагрузки. Контрольная сигнализация, для которой не требуется выделенного временного слота для ответа, передается с помощью LMP.

Таблица 7.1 демонстрирует все типы логического транспорта, типы логических соединений и физические каналы, которые могут поддерживать их, а также краткое описание назначений логического транспорта.

Таблица **7.1.** Типы логического транспорта.

Логический транспорт	Поддерживаемые соединения	Поддерживаемые каналы	Общее описание
Асинхронный, ориентированный на соединение (ACL)	Управления (LMP) ACL-C; Пользовательский (L2CAP) ACL-U	Активное физическое соединение, базовый или адаптивный физический канал	Надежные, ограниченные по времени, двунаправленные, точка-точка.
Синхронный, ориентированный на соединение (SCO)	Поток (некадрированный) SCO-S	Активное физическое соединение, базовый или адаптивный физический канал	Двунаправленные, симметричные, точка-точка. Предназначены для передачи с фиксированной скоростью 64кб/с
Расширенный, синхронный, ориентированный на соединение	Поток (некадрированный) eSCO-S	Активное физическое соединение, базовый или адаптивный	Двунаправленные, симметричные, точка-точка, ограниченное число повторных

(eSCO)		физический канал	передач. Предназначены для передачи с постоянной скоростью.
Активный широковещательн ый (ASB)	Пользовательский (L2CAP) ASB-U	Активное физическое соединение, базовый или адаптивный физический канал	Ненадежные, однонаправленные широко-вещательные пакеты для всех устройств, синхронизированн ых с физическим каналом. Служат для рассылки L2CAP данных группам устройств.
Закрепленный широковещательн ый (PSB)	Управления (LMP) PSB-C; Пользовательский (L2CAP) PSB-U	Закрепленное физическое соединение, базовый или адаптивный физический канал	Ненадежные, однонаправленные широко-вещательные пакеты для всех устройств в пикосети. Служат для передачи LMP и L2CAP данных закрепленным устройствам.

7.1.9. Каналы L2CAP.

L2CAP обеспечивает мультиплексирование ролей, позволяя различным приложениям совместно использовать ресурсы логического соединения ACL-U между двумя устройствами. Приложения и протоколы услуги взаимодействуют с L2CAP, используя канально-ориентированный интерфейс для создания соединений к эквивалентным точкам доступа на другом устройстве.

Конечная точка канала L2CAP идентифицируется с помощью уникального, в рамках устройства, идентификатора канала (CID). L2CAP поддерживает два типа каналов, ориентированных на соединение точка-точка, и на передачу данных группе устройств.

Помимо создания, настройки и ликвидации каналов важной задачей L2CAP является мультиплексирование SDU из клиентских каналов в логическое соединение ACL-U, а также обеспечение отбора SDU в соответствии с заданной приоритетностью. L2CAP каналы могут быть настроены для предоставления требуемого приложением качества обслуживания.

7.1.10. Топология сети.

Каждый раз, когда формируется соединение IEEE 802.15.1, образуется пикосеть, которая состоит из двух или более устройств, занимающих один и тот же физический канал (иными словами, они синхронизированы с встроенным таймером и имеют общую последовательность смены частот).

В одной и той же точке может существовать несколько независимых пикосетей, каждая из которых имеет независимый физический канал. Устройства могут одновременно участвовать в нескольких пикосетях, это организуется на базе TDM. Но устройство не может быть ведущим в более, чем одной пикосети.

Устройство, которое является членом двух или более пикосетей, является участником так называемой рассеянной сети (scatternet). Участие в рассеянной сети не обязательно связано с какими-либо возможностями сетевой маршрутизации. Стандарт

IEEE 802.15.1 не предлагает такой функциональности, которая обеспечивается верхними уровнями протоколов, и не входит в сферу применения данного стандарта.

На рис. 7.5 продемонстрирован пример топологии пикосетей. Устройство A является ведущим в пикосети A, с ведомыми устройствами B, C, D и E. В то же время устройство F является ведущим для устройств E, G и H, а устройство D ведущим для J.

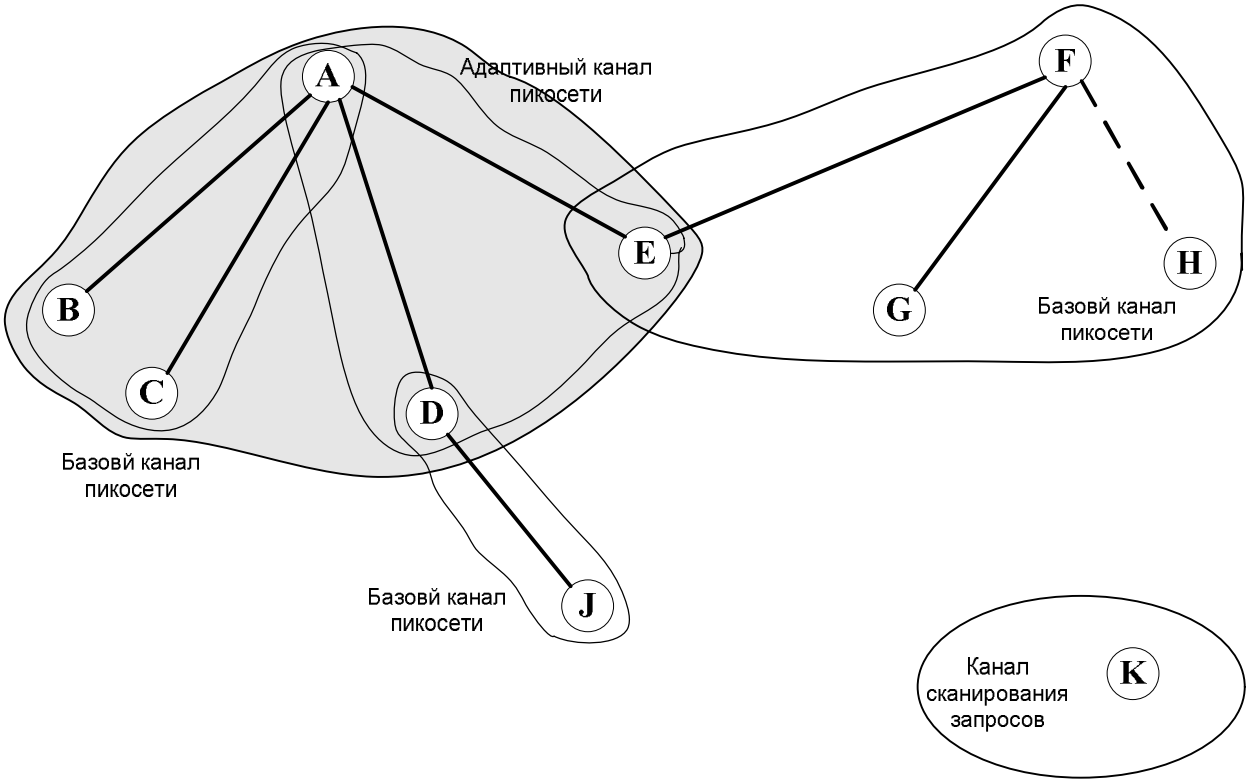


Рис.7.5. Пример топологии IEEE 802.15.1.

В пикосети A используется два физических канала, в пикосети D и F, только один – базовый. Устройство K находится в том же месте, что и остальные, но не входит не в одну из пикосетей, поэтому прослушивает на физическом канале сканирования запросы, в ожидании запроса от другого устройства.

7.2. Стандарт IEEE 802.15.3

7.2.1. Общее описание

Стандарт 802.15.3 регламентирует спецификацию физического и канального уровней высокоскоростных сетей с поддержкой фиксированных и мобильных устройств, работающих на небольшом расстоянии (до 10 м). Для взаимодействия устройств организуется беспроводная персональная сеть, также называемая пикосеть.

Пикосеть 802.15.3 состоит из ряда компонентов, приведенных на рис.7.6. Основными компонентами сети являются устройства (DEV), одно из которых выполняет роль координатора пикосети (PNC). PNC синхронизирует работу сети, регулирует параметры качества обслуживания, энергосбережения, а также контролирует доступ к сети.

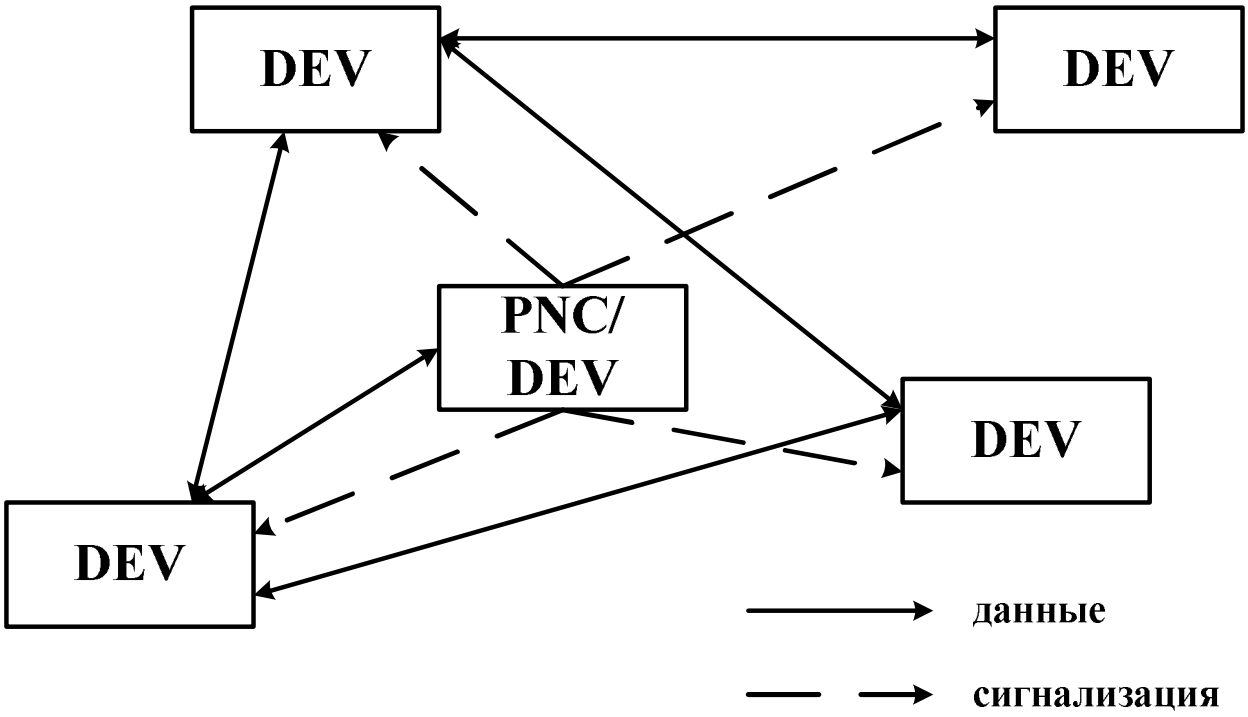


Рис. 7.6. Элементы пикосети 802.15.3.

Так как пикосети 802.15.3 формируются без предварительного планирования и существуют только на то время, пока они необходимы, их относят к специализированным ad hoc сетям.

Стандарт позволяет устройствам создавать вспомогательные пикосети, в этом случае оригинальная сеть именуется родительской пикосетью. Вспомогательные пикосети могут быть дочерними или смежными в зависимости от метода, который используется устройством для связи с родительским координатором. Дочерние и смежные пикосети являются зависимыми сетями, поскольку они обращаются с родительского PNC для занятия канала на время работы устройств.

MAC протокол IEEE 802.15.3 разрабатывался с учетом следующих требований:

- Быстрое время соединения;
- ad hoc сеть;
- поддержка передачи данных с заданным качеством обслуживания (QoS);
- безопасность;
- динамическое членство в сети;
- эффективная передача данных.

7.2.2. Формирование и разрушение пикосети

Пикосеть формируется, когда устройство, которое может выступать в качестве координатора, начинает передавать сигнальные пакеты (beacons). Одна из основных функций PNC

состоит в передачи сигнальных пакетов, содержащих сведения об образованной пикосети. Для того, чтобы начать передачу сигнальных пакетов координатор сканирует доступные радиочастоты в поисках свободной. Если свободная частота не была найдена, устройство имеет возможность начать процесс инициализации зависимой пикосети.

Когда к существующей сети присоединяется новое устройство, координатор проверяет его возможности для того, чтобы посмотреть, не является ли новое устройство более подходящим на роль координатора сети. Если новое устройство подходит больше на роль PNC и текущие настройки безопасности позволяют сменить координатора сети, то управление сетью переходит к новому устройству. Данная передача полномочий учитывает все текущие временные занятия канала, вследствие чего он никак не влияет на доставку данных в пикосети. В случае если координатор хочет покинуть пикосеть, он также инициализирует процесс передачи полномочий.

Дочерняя пикосеть формируется в соответствии с уже созданной сетью, которая становится родительской для нее. Функция создания дочерней пикосети полезна для расширения области охвата сети или переноса некоторых вычислительных задач к другому PNC поддерживаемому устройству. Родительская пикосеть может иметь более, чем одну дочернюю пикосеть. Кроме того, также возможно для дочернего координатора иметь дочернюю пикосеть как часть своей собственной сети. Дочерние пикосети используют различные идентификаторы (PNID) и могут

выступать в качестве автономных за исключением того, что они зависят от частных СТА из родительской пикосети. Включение в сеть и параметры безопасности для дочерней пикосети не связаны с родительским PNC.

PNC дочерней сети является членом родительской пикосети. При этом координатор имеет возможность обмена данными с любыми устройством родительской сети.

Смежная пикосеть формируется в соответствии с существующей сетью. Смежная пикосеть предназначена для совместного использования частотного спектра несколькими сетями, когда нет свободных физических каналов. Одна пикосеть может иметь несколько смежных сетей или оба типа зависимых сетей, дочернюю и смежную, как часть родительской пикосети. Кроме того, PNC смежной сети может связывать дочернюю или смежную сеть со своей собственной. Так же, как и в случае с дочерними сетями, смежные сети автономны и лишь зависят от частных СТА родительской пикосети.

PNC смежной сети не является членом родительской пикосети, поэтому он может обмениваться информацией только с устройствами своей сети.

Если PNC хочет прекратить свою работу и нет другого устройства, способного заменить его, он помещает в информационный элемент (IE) сигнального пакета флаг завершения работы PNC (PNC Shutdown) с целью информирования участников сети. В случае, когда координатор покидает сеть без

предварительной передачи полномочий, пикосеть прекращает свою работу. После истечения ассоциативного временного периода (ATP) устройство с возможностями координатора начинает формирование новой сети стандартным способом. При необходимости завершить работу зависимой сети координатор посылает команду запроса разъединения (Disassociation Request) или использует процедуру уничтожения потока.

В случае прекращения функционирования родительской пикосети и посылки информационного элемента прекращение работы координатора одна из зависимых сетей может продолжить свои действия. Координатор выбранной сети после завершения работы родительской сети убирает информационный элемент родительская сеть (Parent Piconet) из сигнального кадра, тем самым показывая, что пикосеть больше не является зависимой.

Для того, чтобы участвовать в пикосети, устройство должно присоединиться к ней, используя процесс ассоциации. После присоединения к пикосети устройство получает уникальный идентификатор DEVID. Идентификатор DEVID имеет длину в один октет, он используется при коммутации вместо 8 октетного адреса устройства, для уменьшения накладных расходов в системе. В процессе присоединения дополнительно предоставляется информация об услугах, имеющихся в пикосети, а также об услугах, предоставляемых устройствам.

Когда новое устройство присоединяется к пикосети, PNC посылает информацию о всех устройствах в сети, а также помещает в сигнальный кадр информацию о новом устройстве.

Когда устройство хочет покинуть пикосеть или если PNC хочет отключить устройство, запускается процесс разъединения. DEVID отключившегося устройства становится недействительным до тех пор, пока координатор не использует его снова. Однако PNC не позволено повторное использование DEVID до истечения периода ожидания.

7.2.3. Безопасность функционирования сети.

Существует два режима работы пикосети. Первый режим работы сети – открытый. Для функционирования сети не требуется безопасного членства и защита полезной нагрузки (проверка целостности данных или шифрование данных) не осуществляется на MAC уровне. PNC может использовать список разрешенных DEV адресов для ограничения доступа к сети. Во втором режиме работы для того чтобы получить доступ к ресурсам сети, устройству необходимо установить защищенное соединение с координатором. Данные пересылаемые через сеть, могут быть защищены с помощью алгоритмов проверки целостности, а также зашифрованы. Проверка целостности передаваемых данных требуется для большинства команд, передаваемых в пикосети.

Когда включен безопасный режим, устройства, которые хотели бы присоединиться к пикосети, должны создать безопасные соединения с PNC. Устройствам также позволено создавать

безопасные соединения между собой. Процесс создания безопасных соединений не входит в рамки стандарта IEEE 802.15.3. Протокол защиты полезной нагрузки использует симметричный ключ, генерируемый одним из участников обмена информацией.

7.2.4. Формат сверхцикла 802.15.3.

Временные интервалы в пикосети базируются на структуре сверхцикла, проиллюстрированной на рис.7.7. Сверхцикл состоит из трех частей:

- Сигнальный пакет, используется для расстановки занятий временных интервалов и для передачи информации управления для пикосети. Сигнальный пакет состоит из сигнального кадра, а также команд – объявлений, рассылаемых координатором;
- период конкурентного доступа (CAP), используемый для передачи команд и/или асинхронных данных;
- период занятия канального интервала (CTAP), состоящий из занятий канального интервала (CTA), включая CTA управления (MCTA). CTA используются для транспортировки команд, изохронных потоков и асинхронных данных.

Рис.7.7. Формат сверхцикла.

Длина CAP определяется координатором и передается устройствам в сети с помощью сигнального пакета. Для доступа к среде в период конкурентного доступа используется механизм CSMA/CA [113], однако CTAP использует стандартный TDMA протокол, где каждому устройству выделяются специализированные временные окна. MCTA представляют собой CTA, предназначенные для связи между устройствами и координатором.

Все данные пикосети передаются в режиме точка-точка. Существует три способа обмена данными между устройствами. Если CAP включен в сверхцикл, и PNC позволяет передавать данные в нем, то устройства могут использовать CAP для передачи небольшой порции данных без необходимости занимать временные интервалы. Если устройству требуется доступ к каналу на постоянной основе, оно запрашивает у PNC изохронный канал. При наличии свободных ресурсов координатор назначает временной отрезок в CTA для устройства. Асинхронное занятие канала немного отличается, устройство запрашивает доступ к каналу для передачи определенной порции данных. Координатор должен

составить расписание доступа к каналу на основе свободных временных интервалов.

7.2.5. Обмен данными между устройствами.

Для обработки больших кадров данных, поступающих с вышестоящих уровней, стандарт предусматривает фрагментацию и дефрагментацию таких кадров. Возможность фрагментировать данные также полезна для уменьшения частоты появления ошибок в кадрах (FER) путем снижения размера кадра. Фрагменты маркируются порядковым номером, общее их число сообщается принимающему устройству, чтобы для буфера входящих кадров было выделено достаточно памяти.

Если источник передачи хочет проверить доставку кадров, применяется одно из правил подтверждения доставки. Стандарт предоставляет три типа подтверждений. В случае, когда не требуется гарантировать доставку кадров, например, если этим занимаются вышестоящие протоколы, применяется правило no-ACK. В иных случаях используется моментальное подтверждение (Imm-ACK) – каждый кадр индивидуально подтверждается после получения, а также задержанное подтверждение (Dly-ACK), позволяющее принять определенную группу кадров и затем выслать общее подтверждение.

Если передающее устройство не получило подтверждение о доставке, оно может повторно выполнить передачу кадра или отбросить его, выбор осуществляется в зависимости от типа

передаваемых данных и количества уже совершенных попыток передачи.

Устройства, входящие в пикосеть в любой момент времени могут запросить данные об услугах и возможностях других устройств. Стандарт IEEE 802.15.3 поддерживает четыре метода обнаружения информации о других устройствах: команда информационного запроса координатора (PNC Information Request), команда запроса исследования (Probe Request), команду анонса (Announce) и команду услуги пикосети (Piconet Services).

Команда информационного запроса координатора позволяет получить данные об определенном устройстве или обо всех устройствах сразу. Устройства используют команду запроса исследования для получения более подробных данных об устройстве. Одна из целей объединения устройств в пикосеть – это совместное использование разнообразных сервисов. Однако, для осуществления всего этого необходимо знать какие сервисы предоставляются в сети, а также сообщать о своих сервисах другим пользователям пикосети. Для осуществления этого в стандарте предусмотрен информационный элемент сервисов пикосети.

Любое устройство в пикосети может запросить информацию о качестве соединения между собой и другим устройством с помощью команды запроса состояния канала (Channel Status Request).

7.2.6. Управление питанием.

Одной из важных задач при разработке стандарта была задача оптимизации энергопотребления для устройств с аккумуляторным источником питания. Наилучший метод сохранения энергии - это полное выключение устройства на долгий период времени, сравнимый с периодом сверхцикла. В стандарте предусмотрено три технологии для отключения питания устройства сроком на один и более сверхцикл: режим синхронизированного сохранения энергии устройства (DSPS), режим синхронизированного сохранения энергии пикосети (PSPS) и режим асинхронного сохранения энергии (APS). В пикосети устройство может находиться в одном из четырех режимов управления энергией: ACTIVE, DSPS, PSPS или APS.

Режим PSPS позволяет устройству спать в течение интервала определенного PNC. Режим DSPS был разработан для того чтобы позволить группе устройств спать в течение нескольких сверхциклов, но при этом иметь возможность проснутся в течении одного сверхцикла. Режим APS позволяет устройству снижать электропотребление на расширенный период времени.

7.2.7. Характеристики физического уровня 2.4 Ггц.

Для передачи данных на физическом уровне используется полоса частот 2.4 – 2.4835 ГГц. Определено два набора каналов, один состоит из 4 частот и предназначен для приложений с высокой плотностью передачи, а второй содержит 3 частоты и предназначен для сосуществования с сетями 802.11b. Физический

уровень также поддерживает 5 скоростей передачи данных от 11 до 55 Мб/с. Базовая скорость в 22 Мб/с не кодируется, в отличии от других скоростей, использующих модуляцию на основе решетчатого кода.

Для эффективности PHY высчитывает контрольную сумму заголовков для последовательности заголовков физического и канального уровней и добавляет ее к заголовкам MAC уровня. Заголовки для всех кадров передаются на базовой скорости для того, чтобы все устройства в пикосети могли обнаружить передачу данных.

Для формирования преамбулы на физическом уровне используется последовательность с постоянной амплитудой и нулевой автокорреляцией (CAZAC). Последовательность имеет хорошие свойства для получения синхронизации.

Полоса пропускания ограничена 15 МГц, с целью предоставления большего числа каналов, а также для снижения интерференции с другими системами и уменьшения восприимчивости к помехам от других систем. Мощность передатчика ограничивается нормативными актами соответствующих регулирующих органов.

Так как 2.4 PHY работает в не лицензируемом радиочастотном спектре, физическому уровню приходится совместно использовать полосу частот. Для более успешного сосуществования применяются специальные технологии:

– пассивное сканирование;
– динамический выбор канала;
– возможность запроса информации о качестве канала;
– качество соединения и RSSI показатель;
– распределение частот, сводящее к минимуму перекрытие каналов;
– низкая мощность передачи;
– управление мощностью передачи;
– возможность организации смежной сети.

7.2.8. Управление уровнями.

Физический и канальный уровни включают в себя объекты управления, называемые объект управления MAC подуровня и объект управления PHY уровня (MLME и PLME). Эти объекты предоставляют интерфейсы управления уровнем. Для того, чтобы осуществлять MAC операции корректно в каждом устройстве должен присутствовать объект управления устройством (DME). DME является слоенезависимым объектом, ответственным за получение состояний от различных объектов управления и установкой значений специфичных для уровней параметров. Рис. 7.8. демонстрирует взаимоотношение между различными объектами управления.

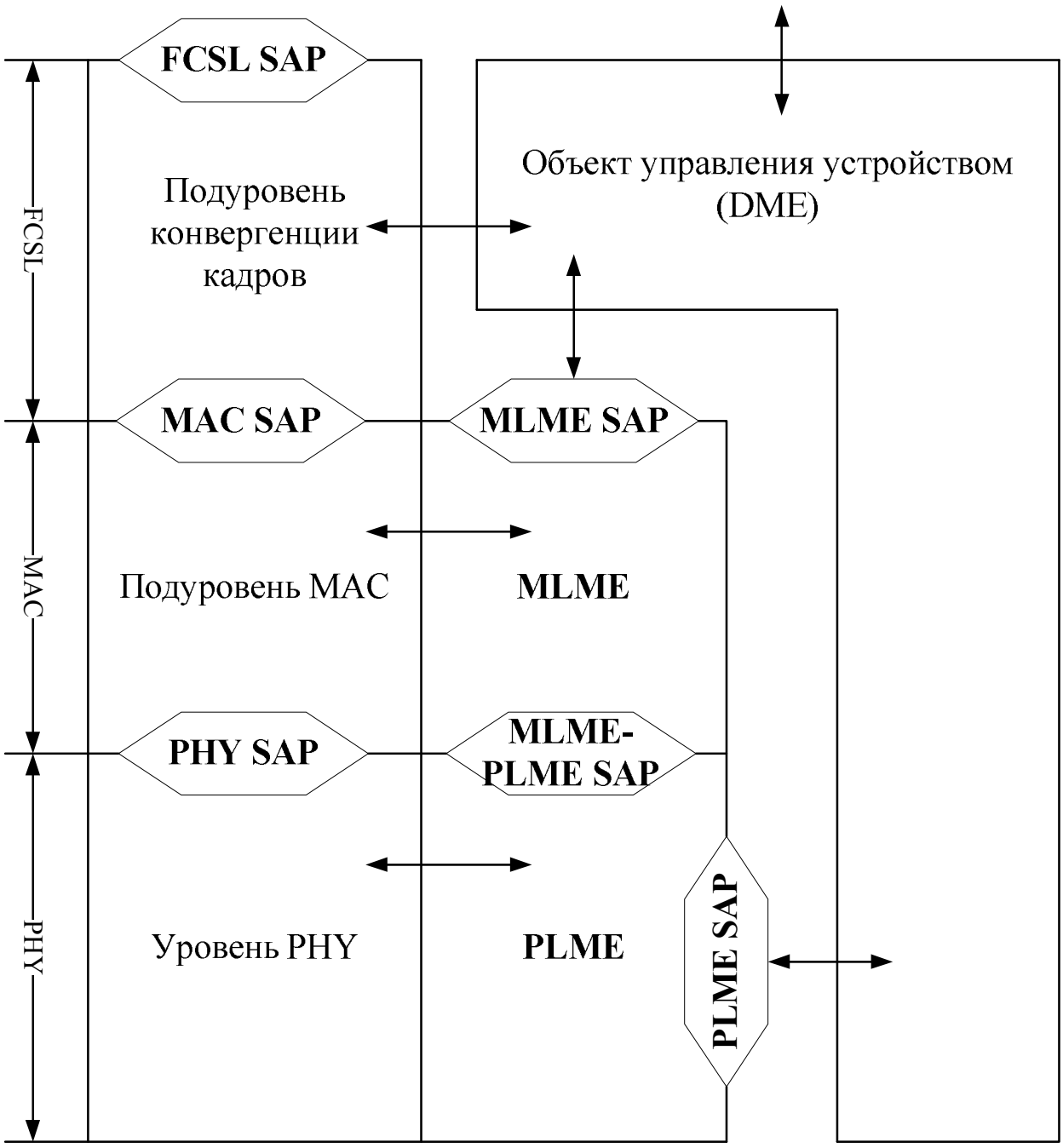


Рис. 7.8. Модель взаимодействия объектов управления.

7.3. Общие сведения о стандарте IEEE 802.15.6.

Основной задачей рабочей группы IEEE 802.15.6 является разработка MAC уровня с поддержкой нескольких физических уровней (PHY) для нательных беспроводных сетей [144]. Целью создания нательных беспроводных сетей (WBAN - Wireless Body

Area Network) является обслуживание различных приложений медицинского направления, например удаленный контроль состояния здоровья человека, а также приложений для бытовой техники и персональных центров развлечения. На рис. 7.9 продемонстрированы возможные сенсорные узлы как на теле человека (или в непосредственной близости от него), так и имплантированные, которые могут быть использованы в WBAN сетях в соответствии с проектом стандарта IEEE 802.15.6 [145]. Такие сети должны обслуживать различные типы нагрузки, передаваемые с различными скоростями и приоритетами. Наличие различных физических уровней позволяет разным устройствам работать на своей частоте.

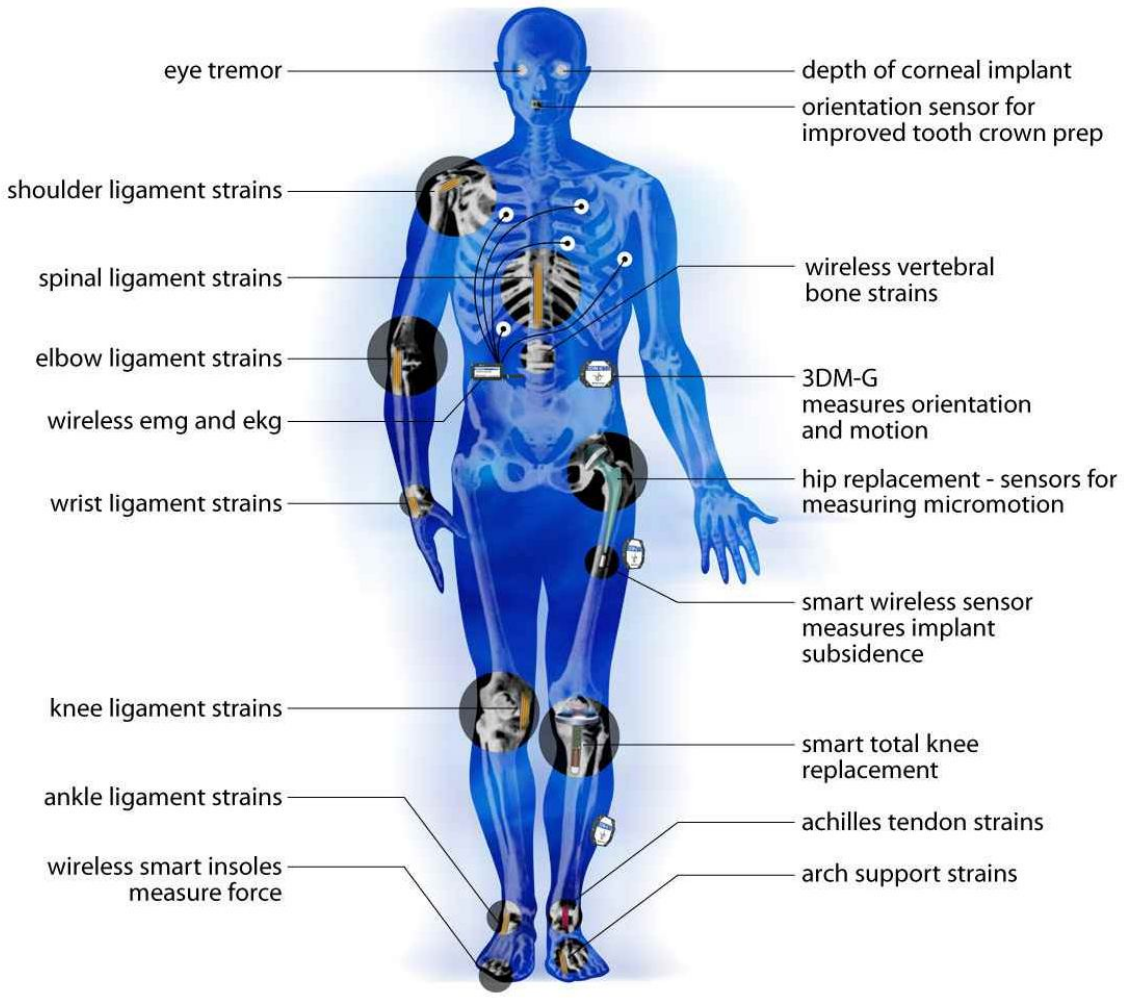


Рис. 7.9. Размещение сенсорных узлов на и в теле человека.

На рис.7.9 приведено размещение возможных сенсорных узлов в соответствии с сегодняшним видением рабочей группы IEEE 802.15.6. Это сенсорные узлы для измерения тремора глаз (колебания глазного яблока относительно направления зрительной оси, eye tremor), нагрузки на связки плеча (shoulder ligament strains), нагрузки на мышцы спины (spinal ligament strains), нагрузки на связки локтевого сустава (elbow ligament strains), электромиографии (регистрация электрической активности мышц) и электрокардиограммы (wireless emg and ekg), нагрузки на связки в запястье (wrist ligament strains), нагрузки на связки в коленном

суставе (knee ligament strains), нагрузки на связки в лодыжке (ankle ligament strains). Кроме того, в состав сенсорных узлов на и в теле человека в том числе и в непосредственной близости от него, включены умные стельки для измерения силы (wireless smart insoles measure force), сенсоры измерения глубины расположения имплантата роговицы (depth of corneal implant), ориентации для пробной коронки зуба (orientation sensor for improved tooth crown prep), гироскопические сенсоры для измерения движения и ориентации в трехмерном пространстве (3DM-G measures orientation and motion), измерения микро перемещений в эндопротезе тазобедренного сустава (hip replacement – sensor for measuring micromotion), измерения имплантатов (smart wireless sensor measures implant subsidence), умный эндопротез коленного сустава (smart total knee replacement), измерения нагрузки на ахиллово сухожилие (ahilles tendon strains) и подъем ступни (arch support strains). Как видим, по сравнению с первыми воззрениями на человека как терминал сети [26,27] и число, и качественный состав сенсоров существенно увеличилось и усложнился соответственно.

Основные приложения технических средств стандарта IEEE 802.15.6 могут быть разделены на два класса:

а) Специализированные медицинские приложения:

носимые,

имплантируемые.

б) Приложения общего характера:

видео и аудио,

передача данных,

управление для интерактивных игр.

При проектировании BAN сетей основной упор делается на энергетическую эффективность, подразумевающую низкое потребление энергии узлами. Сети BAN поддерживают только топологию звезда, правда с высокой степенью масштабируемости. Топология сети представлена на рис.7.10. Для функционирования сети требуется наличие нескольких сенсорных устройств и/или актуаторов, которые связываются с сетевым контроллером WBAN (BNC - BAN Network Controller), реализованном в виде телефона, КПК или ноутбука.

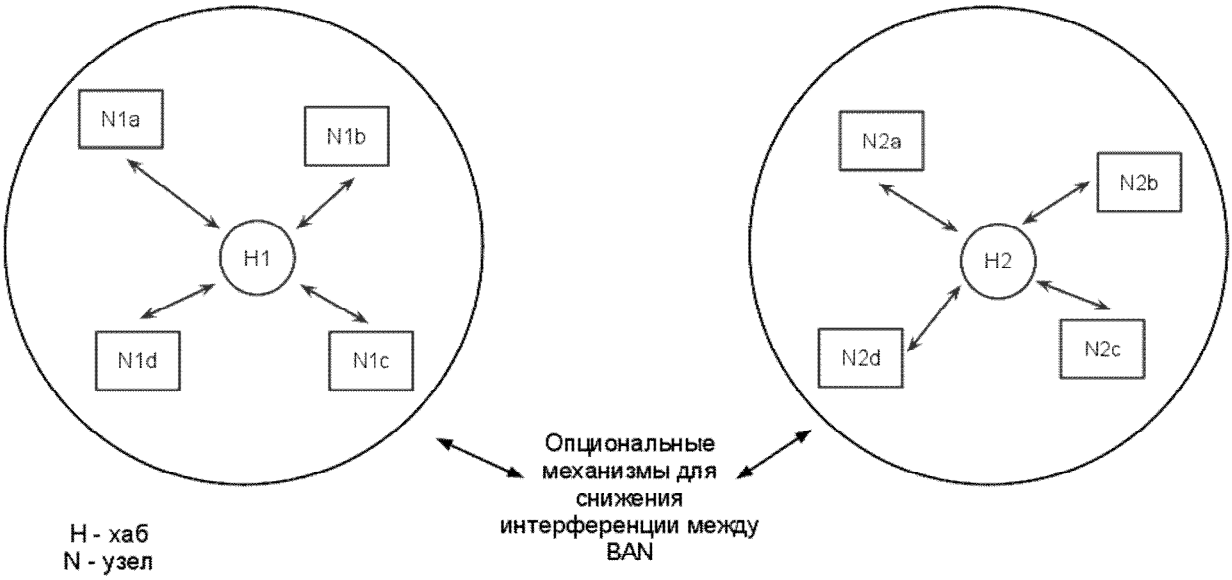


Рис.7.10. Топология сетей BAN.

Для сетей по стандарту IEEE 802.15.6 должны выполняться следующие требования по масштабируемости и жизнеспособности сетей:

- Переменные скорости передачи данных от нескольких Кбит/с

до нескольких Мбит/с.

- Поддержка до 256 устройств.
- Сосуществование с другими сетями BAN.
- Поддержка механизмов обеспечения безопасности передачи данных.
- Гарантированные уровни задержек.
- Гарантированная полоса пропускания.

Выбор физического уровня (рабочих диапазонов частот) стал одной из основных проблем при разработке стандарта. Доступные частоты для WBAN, естественно, контролируются радиочастотными регуляторами. Рис.7.11 показывает некоторые из доступных частот, разрешенных в различных странах. Частотный диапазон услуг связи для медицинских имплантатов (Medical Implant Communications Services - MICS) используется для связи между имплантатами и имеет единый частотный диапазон (402-405 МГц) в различных странах. Еще одним примером разрешенного диапазона является беспроводные услуги для медицинской телеметрии (Wireless Medical Telemetry Services - WMTS). Оба этих диапазона не поддерживают приложения, которые требуют высокую скорость передачи данных. Частотный диапазон для индустриальных, научных и медицинских приложений ISM позволяет реализовать высокоскоростную передачу данных и доступен во всем мире. Однако присутствует высокая вероятность интерференции, т.к. множество устройств стандартов IEEE 802.11 и IEEE 802.15.4 работают в том же диапазоне.

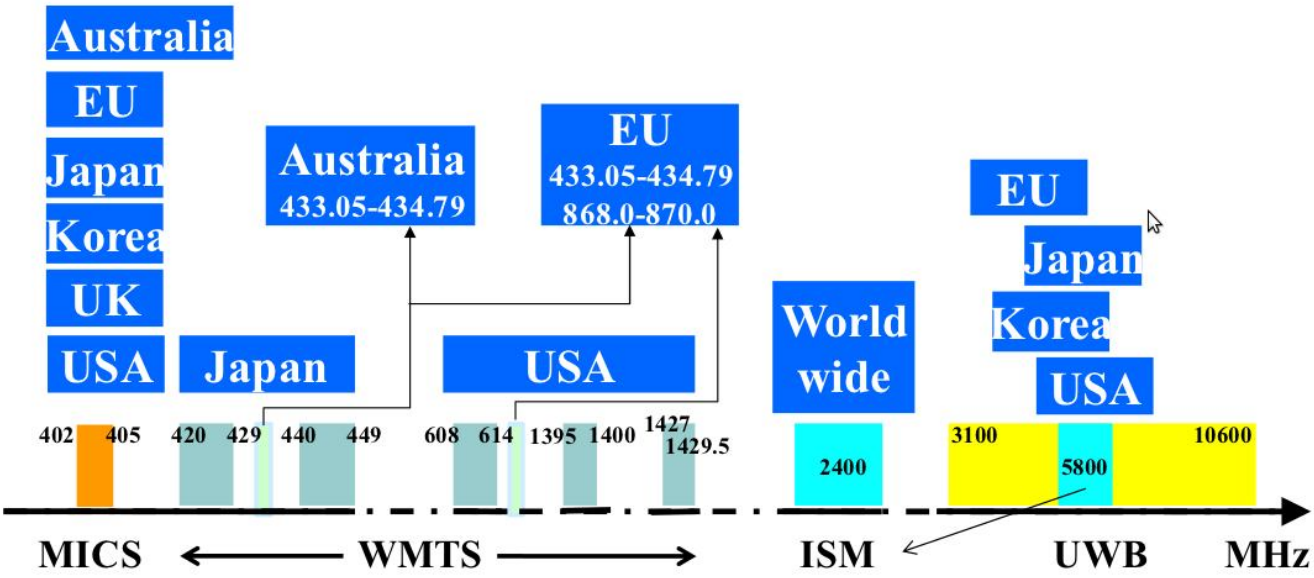


Рис.7.11. Доступные частоты для WBAN в различных странах.

Текущий проект стандарта IEEE 802.15.6 определяет три возможных реализации физического уровня – узкополосный (NB – Narrowband), сверхширокополосный (UWB – Ultra WideBand) и уровень связи человеческого тела (HBC – Human Body Communication). Уровнем выше стандарт определяет обобщенный MAC протокол, обеспечивающий контроль доступа к каналу. Выбор определенного PHY уровня зависит от приложения.

7.3.1. Спецификации физического уровня для IEEE 802.15.6.

Как уже отмечалось выше, IEEE 802.15.6 поддерживает три различных физических уровня: NB, UWB и HBC.

1. Narrowband PHY (NB). Узкополосный физический уровень отвечает за активацию/деактивацию радиопередатчика, оценку чистоты канала (Clear Channel Assessment - CCA) для данного канала и передачу/прием данных. Протокольный блок данных физического уровня (PPDU) - кадр уровня NB PHY состоит из

преамбулы протокола подуровня конвергенции физического уровня (Physical Layer Convergence Procedure - PLCP), заголовка PLCP и сервисного блока данных физического уровня (PHY Service Data Unit - PSDU), как показано на рис.7.12. Преамбула PLCP используется приемником для синхронизации времени и определении смещения несущей. Это первый передаваемый компонент. Заголовок PLCP содержит информацию необходимую для успешного декодирования переданного пакета. Заголовок PLCP передается сразу же за преамбулой PLCP, используя указанную частоту в рабочем диапазоне частот. Последний компонент – блок PSDU, содержащая заголовок MAC, информацию кадра MAC уровня и проверочную последовательность кадра (Frame Check Sequence - FCS). PSDU передается после заголовка PLCP с использованием любой из доступных скоростей в рабочем диапазоне частот. WBAN устройства должны поддерживать передачу и прием в одном из диапазонов частот, указанных в таблице 7.2. В таблице 7.2. приведено соответствие скоростных характеристик и видов модуляции, используемых при передачи заголовков PLCP и PSDU. В NB PHY применяются следующие виды модуляции: дифференциальная бинарная фазовая манипуляция (Differential Binary Phase-shift Keying - DBPSK), дифференциальная квадратурная фазовая манипуляция (Differential Quadrature Phase-shift Keying - DQPSK) и дифференциальная восьмипозиционная фазовая манипуляция (Differential 8-Phase-shift Keying - D8PSK). В частотном диапазоне 420-450 МГц

используется Гауссовская манипуляции с минимальным частотным сдвигом (Gaussian Minimum Shift Keying – GMSK).

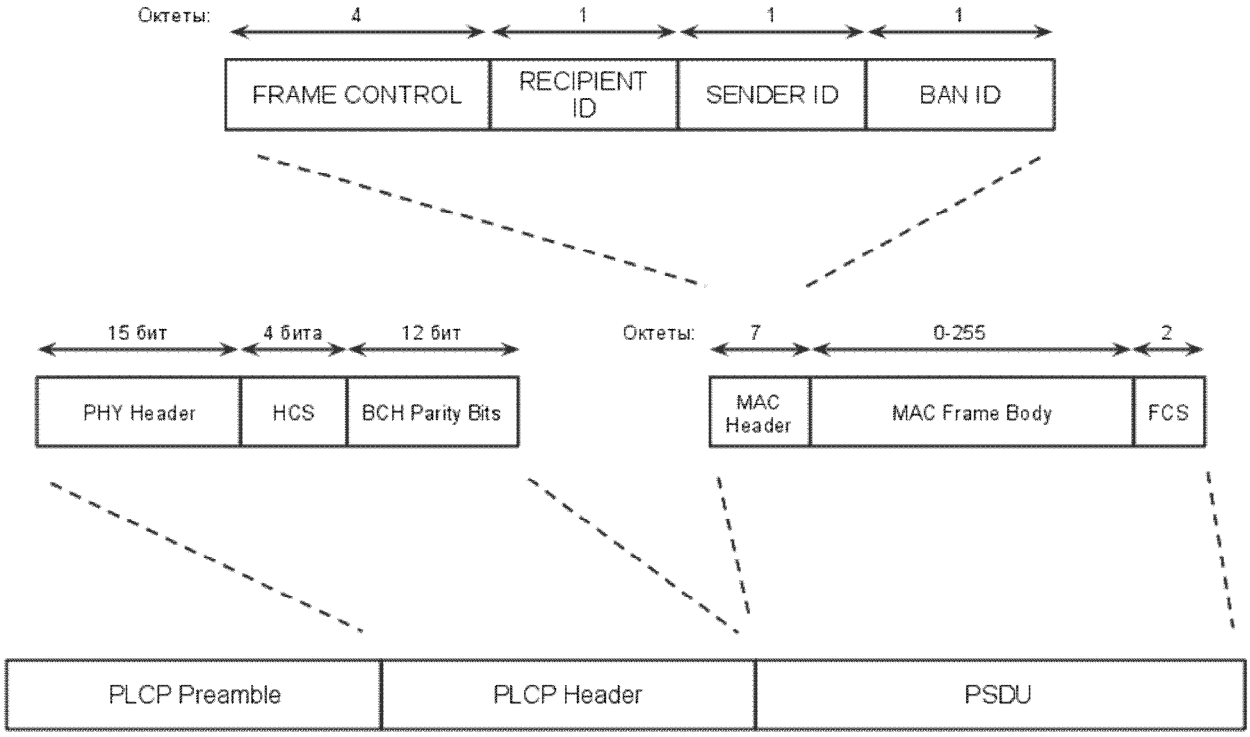


Рис.7.12. Структура PPDU для NB.

Таблица 7.2. Частотные диапазоны, виды модуляции и скорости.

Частота	Компоненты	Модуляция	Символьная скорость (Kbps)	Кодовая скорость BCH (n,k)	Информационная скорость (Kbps)
402-405 МГц	Заг. PLCP	π/2-DBPSK	187.5	(31,19)	57.5
	PSDU	π/2-DBPSK	187.5	(63,51)	75.9
	PSDU	π/4-DQPSK	187.5	(63,51)	303.6
420-450 МГц	Заг. PLCP	GMSK	187.5	(31,19)	57.5
	PSDU	GMSK	187.5	(63,51)	75.9

	PSDU	GMSK	187.5	(63,51)	151.8
863-870 МГц	Заг. PLCP	π/2-DBPSK	250	(31,19)	76.6
	PSDU	π/2-DBPSK	250	(63,51)	101.2
	PSDU	π/4-DQPSK	250	(63,51)	404.8
902-928 МГц	Заг. PLCP	π/2-DBPSK	300	(31,19)	91.9
	PSDU	π/2-DBPSK	300	(63,51)	121.4
	PSDU	π/4-DQPSK	300	(63,51)	485.7
950-956 МГц	Заг. PLCP	π/2-DBPSK	250	(31,19)	76.6
	PSDU	π/2-DBPSK	250	(63,51)	101.2
	PSDU	π/4-DQPSK	250	(63,51)	404.8
2360-2483.5 ГГц	Заг. PLCP	π/2-DBPSK	600	(31,19)	91.9
	PSDU	π/2-DBPSK	600	(63,51)	121.4
	PSDU	π/2-DBPSK	600	(63,51)	485.7

2. Ultra Wideband PHY (UWB). Сверхширокополосный физический уровень использует два частотных диапазона: нижний частотный диапазон и верхний частотный диапазон. Каждый из диапазонов делится на каналы, каждый из которых в свою очередь характеризуется шириной полосы в 499.2 МГц. Нижний частотный диапазон состоит только из трех каналов (1-3). Второй канал имеет центральную частоту 3993.6 МГц и считается обязательным. Верхний частотный диапазон состоит из восьми каналов (4-11), при этом канал 7 с центральной частотой 7987.2 МГц считается обязательным. Все остальные каналы являются опциональными. Типичное UWB устройство должно поддерживать хотя бы один из обязательных каналов. Приемники UWB являются легкими в реализации и позволяют использовать гораздо более низкие уровни

мощности передатчика по сравнению с устройствами, работающими в частотном диапазоне MICS.

На рис.7.13 показана структура протокольного блока данных UWB PPDU, содержащей заголовок синхронизации (Synchronization Header - SHR), заголовок физического уровня (PHY Header - PHR) и PSDU. Заголовок SHR состоит из преамбулы и разделителя начала кадра (Start Frame Delimeter - SFD). В PHY переносится информация о скорости передачи PSDU, длине пользовательских данных и коде шифратора. Информация, содержащаяся в PHR, используется приемником для декодирования PSDU. Скорость передачи данных для этого уровня может изменяться от 0.5 Мбит/с до 10 Мбит/с с обязательной поддержкой скорости 0.4882 Мбит/с.

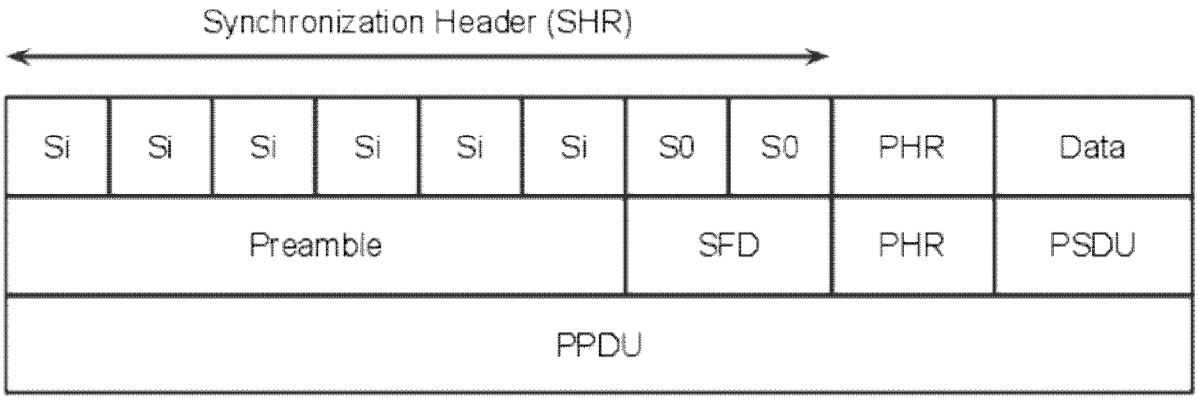


Рис. 7.13. Структура PPDU для UWB.

3. Human Body Communication PHY (HBC): Физический уровень связи для человеческого тела работает в двух частотных диапазонах

с центральными частотами в 16 МГц и 27 МГц с шириной полосы в 4 МГц. Оба частотных диапазона разрешены в США, Японии и Корее, а частотный диапазон 27 МГЦ также разрешен в Европейских странах. HBC представляет собой спецификацию физического уровня связи через электростатическое поле (Electrostatic Field Communication - EFC), которое покрывает весь протокол взаимодействия для WBAN: структуру пакетов, модуляцию, преамбулу/SFD и т.д. Рис. 7.14 показывает структуру PPDU блока EFC, состоящую из преамбулы, SFD, заголовка PHY и PSDU. Преамбула и SFD являются фиксированным шаблоном данных, они генерируются заранее и передаются перед заголовками пакета и пользовательскими данными. Последовательность преамбулы передается четыре разы для точного достижения синхронизации, в то время как последовательность SFD передается только единожды. После приема пакета приемник может определить начало пакета с помощью преамбулы и затем он же находит начало кадра с помощью SFD.

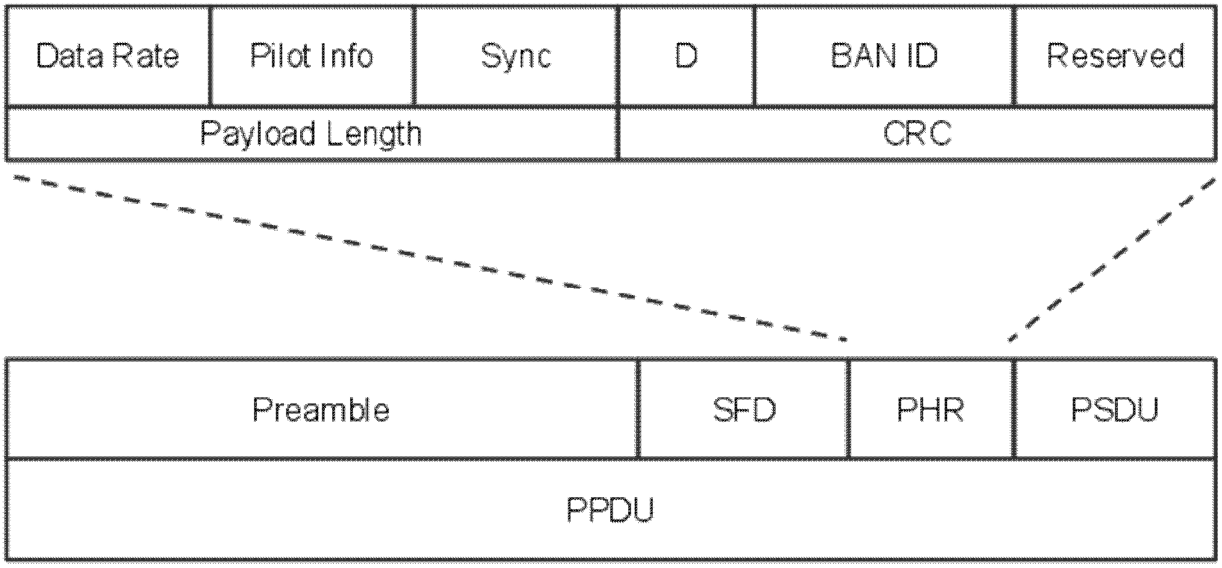


Рис. 7.14. Структура PPDU для HBC.

7.3.2. Спецификация MAC уровня в IEEE 802.15.6.

В IEEE 802.15.6 канал делится с помощью сверхцикловых структур. Каждый сверхцикл ограничивается с помощью сигнальных (beacon) периодов равной длины. Координатор выбирает границы сигнальных периодов и таким образом выбирает распределение слотов. Координатор также может изменить смещение сигнального периода. Обычно сигнальные кадры передаются в каждом периоде за исключением неактивных сверхциклов или, если запрещено регулятором, как, например, в частотном диапазоне MICS. Сеть IEEE 802.15.6 работает в одном из следующих режимов.

1. Сверхцикловой режим с передачей маяков. В данном режиме сигнальные кадры передаются координатором в каждом сигнальном периоде за исключением неактивных сверхциклов или если запрещено регулятором. Рис.7.15 демонстрирует структуру

сверхцикла IEEE 802.15.6, который разделяется на фазу эксклюзивного доступа 1 (Exclusive Access Phase 1 - EAP1), фазу случайного доступа 1 (Random Access Phase 1 - RAP1), фазу типа I/II (Type I/II phase), фазу эксклюзивного доступа 2 (EAP2), фазу случайного доступа 2 (RAP2), фазу Типа I/II и фазу конкурентного доступа (Contention Access Phase - CAP). В периоды EAP, RAP и CAP узлы конкурируют за доступные ресурсы с помощью процедур CSMA/CA или слоттированого протокола доступа Алоха. Фазы EAP1 и EAP2 используются для передачи высокоприоритетных данных, таких как, например, отчет о неотложных происшествиях. Фазы RAP1, RAP2 и CAP используются только для трафика регулярных событий. Фаза Типа I/II используется для занятия исходящих, нисходящих, двунаправленных и отложенных двунаправленных интервалов. В фазах первого и второго типа используется опрос для занятия ресурсов. В зависимости от требований приложения координатор может отменить любой из этих периодов, установив нулевую длину интервала.

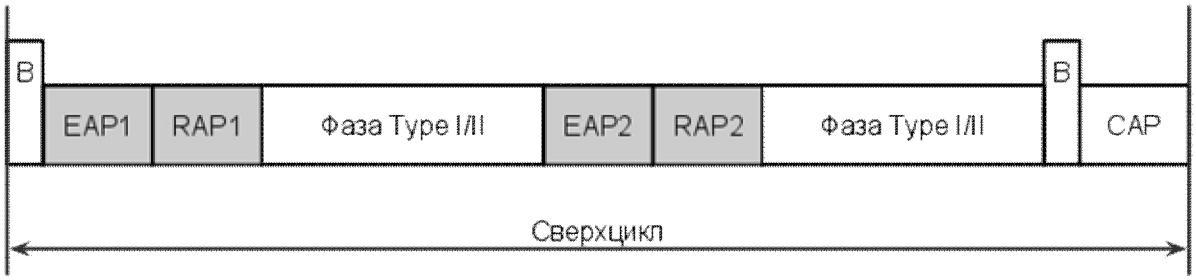


Рис.7.15. Структура сверхцикла IEEE 802.15.6.

2. Сверхцикловой режим без маяков. В этом режиме вся длина сверхцикла покрывается фазой доступа либо первого, либо второго типа, но не обоими сразу.

3. Режим без использования сверхцикла и маяков. В этом режиме координатор предоставляет доступ только с помощью незапланированного запроса доступа типа II.

Механизмы доступа, используемые в каждом периоде сверхцикла, делятся на три категории: механизмы случайного доступа, использующие для занятия ресурсов процедуры CSMA/CA или слоттированого протокола Алоха; импровизированный и незапланированный доступ (без установления соединения), использующий незапланированный опрос/передачу для занятия ресурсов; запланированный доступ (доступ, ориентированный на соединение без привязки к ресурсам), при котором доступ определяется расписанием в одном или нескольких будущих сверхциклах, также называемым 1-периодичное или m-периодичное занятие. Эти механизмы достаточно подробно рассмотрены в проекте стандарта. Далее приведены основные процедуры протокола CSMA/CA.

При использовании CSMA/CA узел устанавливает счетчик отправки в случайную целочисленную величину из равномерного распределения [1, CW], где CW принадлежит интервалу (CWmin, CWmax). Значения CWmin и CWmax зависят от приложения. Узел начинает уменьшать значение счетчика на единицу после каждого пустого слота CSMA, длиной, равной pCSMASlotLength. Данные

передаются, когда счетчик отправки достигает нуля. Значение CW удваивается при каждой ошибочной передаче до тех пор, пока оно не достигнет CWmax. Рис. 7.16 демонстрирует процедуру CSMA/CA. В фазе RAP1 узел ждет в течение периода SIFS = pSIFS и затем разблокирует счетчик до тех пор, пока он не достигнет нуля, когда и начинается передача. В фазе CAP узел блокирует счетчик отправки, так как количество времени до конца слота и CAP фазы меньше суммарного времени для завершения передачи данных и номинального защитного времени (Nominal Guard Time), представленного как GTn. Счетчик отправки будет разблокирован в фазе RAP2.

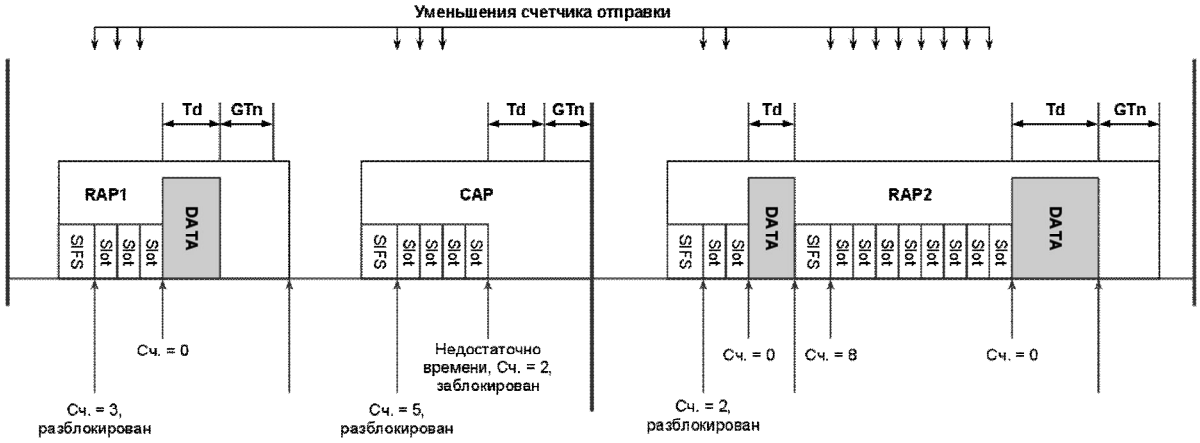


Рис. 7.16. Реализация CSMA/CA в проекте стандарта IEEE 802.15.6.

7.3.3. Безопасность передачи данных.

Проект стандарта определяет три уровня безопасности. Каждый уровень безопасности содержит свои параметры безопасности, уровни защиты и форматы кадров.

1. Уровень 0 - небезопасная связь. Это самый нижний уровень безопасности, на котором данные передаются в незащищенных кадрах. На данном уровне не присутствуют механизмы аутентификации данных, проверки целостности, конфиденциальности и защиты от повторной передачи.

2. Уровень 1 – аутентификация. Это средний уровень безопасности, на котором данные передаются с защищенной аутентификацией, но без шифрования. Конфиденциальность и неприкосновенность частной жизни не гарантируются на данном уровне.

3. Уровень 3 - аутентификация и шифрование. Это наивысший уровень безопасности, на котором данные передаются в безопасных кадрах с использованием механизмов аутентификации и шифрования. Он предоставляет решение для всех проблем безопасности, не покрываемых уровнями 0 и 1.

Требуемый уровень безопасности выбирается во время процесса ассоциации, когда узел присоединяется к сети. Для однонаправленной связи активируется предварительно сформированный мастер-ключ (Master Key - MK) или новый ключ (установленный во время процесса аутентификации). Далее устанавливается парный временный ключ (Pairwise Temporary Key - PTK), используемый один раз за сессию. Для многоадресной связи групповой временный ключ (Group Temporary Key - GTK) используется совместно в мультикастинговой группе. Структура безопасности для проекта стандарта IEEE 802.15.6 приведена на рис. 7.17.

Рис. 7.17. Структура безопасности для проекта стандарта IEEE 802.15.6.

Для гарантированной доставки важных данных в проекте стандарта вводится 8 типов нагрузки, определяемой приоритетами от самого нижнего - нулевого, до самого высокого - седьмого. Перечень типов нагрузки и типов кадров приведен в таблице 7.3.

Таблица 7.3. Перечень типов нагрузки для проекта стандарта IEEE 802.15.6.

Приоритет	**Назначение нагрузки**	**Тип кадра**
0	Фоновый	Данные
1	Негарантированная доставка	Данные
2	Нагрузка с низким приоритетом	Данные
3	Контролируемая нагрузка	Данные
4	Видео	Данные
5	Голос	Данные
6	Медицинские данные или управление сетью	Обслуживание
7	Неотложные или медицинские тревоги	Данные

8. Стандарты IEEE 802.15.4

8.1. Общие сведения о стандарте IEEE 802.15.4.

Беспроводные персональные сети IEEE 802.15.4 нашли свое применение в области сенсорных сетей. Часто такие сети называют LR-WPAN (Low Rate Wireless Personal Area Network – Низкоскоростная беспроводная персональная сеть).

При создании протокола IEEE 802.15.4 были предъявлены определенные требования: сеть должна была быть надежной, легкой в развертывании, с простым протоколом и низким электропотреблением, позволяющим работать долгое время устройствам с аккумуляторным источником питания. При этом требования по дальности действия и скорости передачи достаточно просты.

Некоторые характеристики сетей 802.15.4:

- Скорости передачи 250 kb/s, 40 kb/s и 20 kb/s
- Работа в топологии звезда или каждый-с-каждым
- Использование короткой 16-ти или расширенной 64 битной адресации
- Назначение гарантированных временных интервалов (GTS)
- Использование множественного доступа с контролем несущей и предотвращением коллизий (CSMA-CA)
- Протокол с подтверждениями для гарантированной передачи
- Низкое потребление энергии
- Обнаружение сигнала (ED)
- Индикатор качества соединения (LQI)

- 16 каналов в полосе частот 2450 MHz, 10 каналов в полосе частот 915 MHz и 1 канал в полосе частот 868 MHz.

Различают два типа устройств, применяемых в сетях 802.15.4: полнофункциональное устройство (FFD) и устройство с ограниченными функциями (RFD). FFD может работать в трех режимах: координатор PAN, координатор или просто оконечное устройство. FFD может поддерживать соединение с RFD или другими FFD, в отличие от RFD, который может связываться только лишь с FFD. Применение RFD ограниченно простыми приложениями, такими как детектор света или пассивный инфракрасный сенсор; у них нет необходимости пересылать большое количество данных, и они могут одновременно поддерживать только одно соединение. Следовательно, RFD могут быть реализованы при использовании минимального количества ресурсов и емкостей памяти.

8.2. Компоненты IEEE 802.15.4 WPAN.

Для создания WPAN сети необходима связь не менее двух устройств, одно из которых FFD устройство, функционирующее в качестве PAN координатора. Таким образом, никогда нельзя создать сеть 802.15.4 только из RFD устройств.

Для беспроводной связи не существует четко определенной зоны покрытия, поскольку характеристики распространения непостоянны. Небольшие изменения в положении или направлении движения могут привести к существенному различию в мощности сигнала и качестве связи. Это происходит вне зависимости от того, мобильное или стационарное устройство используется, так как

движущейся объект может повлиять на распространение волн от станции к станции.

8.3. Архитектура сети

Сети 802.15.4 поддерживают два типа архитектур построения: звезда и каждый-с-каждым (одноранговая). Рис. 8. демонстрирует доступные виды архитектур. В архитектуре звезда связь устанавливается между устройствами и единым центральным контроллером, называемым PAN координатором. Устройства, как правило, имеют ряд сопутствующих применений и являются либо узлом начала передачи, либо узлом назначения для сеансов связи в сети. PAN координатор чаще всего используется только для маршрутизации сообщений в сети. Все устройства, присоединенные к сети, независимо от топологии имеют уникальный 64 битный расширенный адрес. Этот адрес может использоваться для прямого установления соединения в пределах сети или он может быть заменен на короткий 16-ти битный адрес, назначенный PAN координатором при присоединении устройства к сети. PAN координатор чаще всего питается от сети в отличие от остальных устройств, которые чаще всего имеют питание от батарей. Применение архитектуры звезда наиболее подходит для автоматизации дома, персонального контроля здоровья.

Одноранговая архитектура также имеет PAN координатор, однако она отличается от архитектуры звезда тем, что любое устройство может общаться с любым другим устройством, если они находились в радиусе действия друг друга. Одноранговая сеть позволяет сформировать более сложную сеть, такую как сеть с

ячеистой архитектурой (архитектура сети, в которой к любому узлу существует два или более маршрута). Одноранговые сети могут быть специальными, самоорганизующимися, самоуправляемыми. Они также позволяют маршрутизировать сообщение от одного узла к любому другому, но эти функции реализуются с помощью протоколов сетевого уровня.

Каждая независимая сеть получает уникальный идентификатор. Этот идентификатор позволяет связываться устройствам внутри сети, используя короткий адрес, и обеспечивает передачу данных между устройствами независимых сетей.

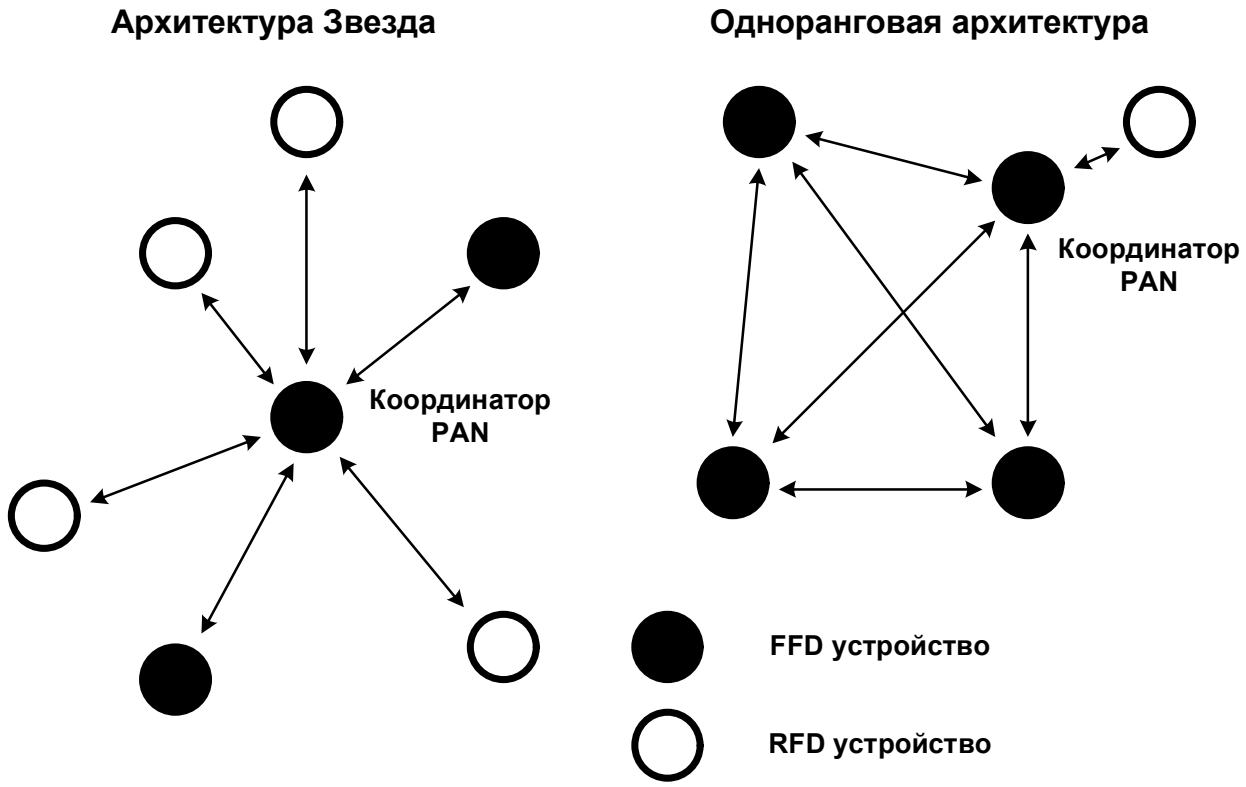


Рис. 8.1. Архитектура сетей 802.15.4.

8.4. Архитектура протоколов

В соответствии с семиуровневой моделью OSI стек протоколов IEEE 802.15.4 включает в себя протоколы физического

и канального уровней.

Протокол PHY предоставляет два сервиса: сервис данных и сервис обслуживания, связанный с компонентом управления физическим уровнем (PLME). Сервис данных PHY позволяет передавать и получать протокольные блоки данных PHY (PPDU) по радио каналу.

Возможности PHY включают в себя активацию и деактивацию радио приемопередатчика, обнаружение сигнала (ED), проверку качества соединения (LQI), выбор канала, освобождение канала, а также передачу и прием пакетов по физической среде. Радиопередача ведется в одной из не лицензируемых полос частот:

- 868–868.6 MHz (Европа)
- 902–928 MHz (Северная Америка)
- 2400–2483.5 MHz (весь мир)

Протокол MAC также предоставляет два сервиса: сервис данных MAC и сервис обслуживания, связанный с компонентом управления уровнем доступа (MLME-SAP). Сервис данных MAC позволяет передавать и принимать протокольные блоки данных MAC (MPDU) через сервис данных PHY.

Возможности подуровня MAC включают в себя управление синхронизацией, доступ к каналу передачи данных, обслуживание гарантированных временных слотов, проверку кадров, доставку кадров подтверждений, установку и разрушение соединений. В качестве дополнительной функции подуровень MAC предоставляет возможность для реализации механизмов безопасности необходимых для приложения.

8.5. Функциональный обзор

Стандарт IEEE 802.15.4 позволяет опционально использовать сверхцикловую структуру. Формат сверхцикла определяется координатором. Сверхцикл ограничивается сигнальным кадром, маяком, посылаемым координатором (Рис. 8.) и делится на 16 равных слотов. Сигнальный кадр посылается в начале каждого сверхцикла. Если координатор не желает использовать сверхцикловую структуру, он может отключить передачу сигнального кадра. Сигнальные кадры служат для синхронизации подключенных устройств, идентификации сети и описания структуры сверхцикла. Любое устройство, желающее передать данные во время периода конкурентного доступа (CAP) между двумя сигнальными кадрами должно получить доступ к каналу, используя слоттированный механизм CSMA-CA. Все транзакции должны быть завершены до следующего сигнального кадра.

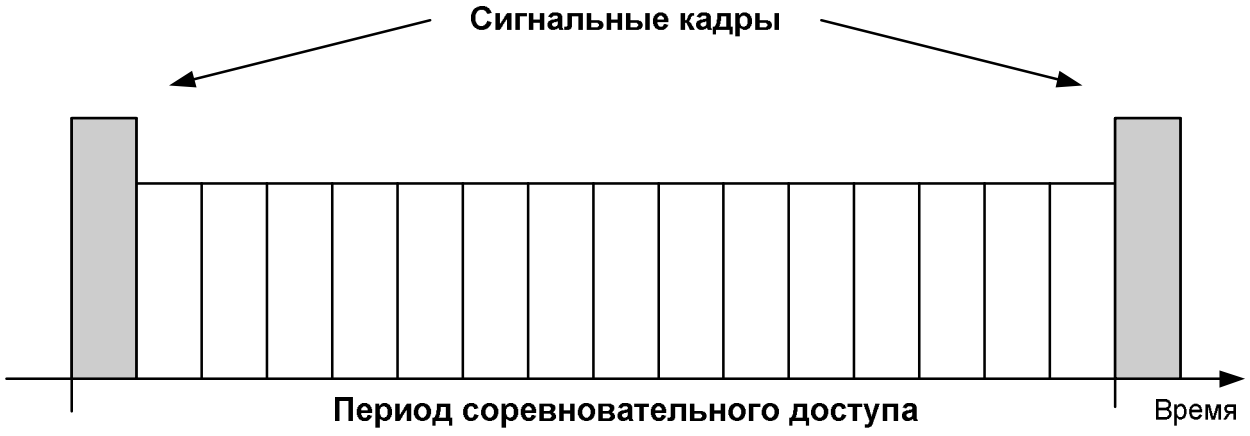


Рис. 8.2. Сверхцикловая структура без использования GTS.

Сверхцикл может быть в активном и пассивном режиме. Во время пассивного режима координатор не связываться с сетью и

может перейти в энергосберегающий режим.

Для приложений, где требуется гарантированная полоса пропускания, координатор PAN может предоставить часть активного периода. Выделенное время будет называться гарантированным временным слотом (GTS), из них формируется период свободный от конкуренции (CFP), расположенный в конце сверхцикла (Рис. 8.). PAN координатор может назначать до 7 периодов GTS и GTS может занимать больше одного временного слота. Однако, определенная часть времени должна остаться для ассоциативного доступа других сетевых узлов или новых устройств, желающих присоединиться к сети. Все ассоциативные транзакции должны быть закончены до наступления CFP периода. Также каждое устройство, передающее в GTS, должно убедиться, что транзакция прекратится до наступления следующего GTS или окончания периода CFP.

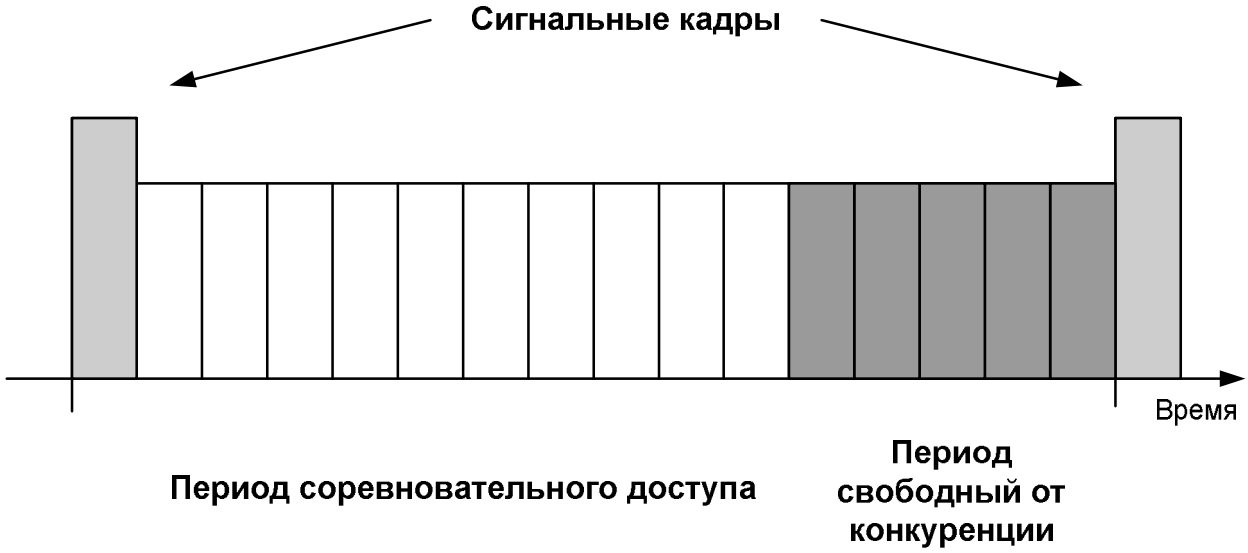


Рис. 8.3. Сверхцикловая структура с использованием GTS.

Существует три типа передачи данных: передача данных координатору, от координатора и между двумя устройствами. В топологии звезда могут применяться только два типа передачи, потому что обмен данными может осуществляться только между координатором и устройством. В одноранговой топологии обмен данными может осуществляться между двумя любыми устройствами, поэтому все три типа транзакций могут применяться в данной топологии.

Когда устройство хочет передать данные в сети с сверхциклами, прежде всего оно прослушивает канал в ожидании сигнального кадра. После его обнаружения устройство синхронизируется со структурой сверхцикла. В подходящей точке устройство передает кадр с данными координатору, используя слоттированный метод CSMA/CA. Координатор подтверждает успешный прием кадра с помощью специального кадра подтверждения. Транзакция на этом заканчивается. Последовательность представлена на рисунке (Рис. 8.).

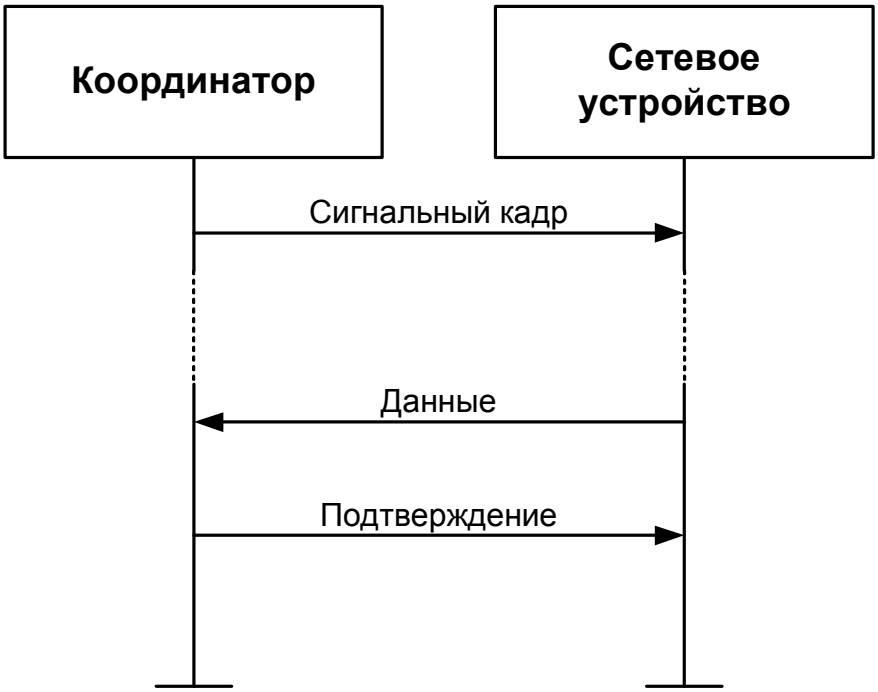


Рис. 8.4. Передача данных координатору в синхронизированной сети.

Когда устройство хочет передать данные в асинхронной сети, оно просто передает кадр данных координатору, используя не слоттированный метод CSMA/CA. Координатор подтверждает успешный прием кадра с помощью специального кадра подтверждения. Транзакция на этом заканчивается. Последовательность представлена на рисунке (Рис. 8.).

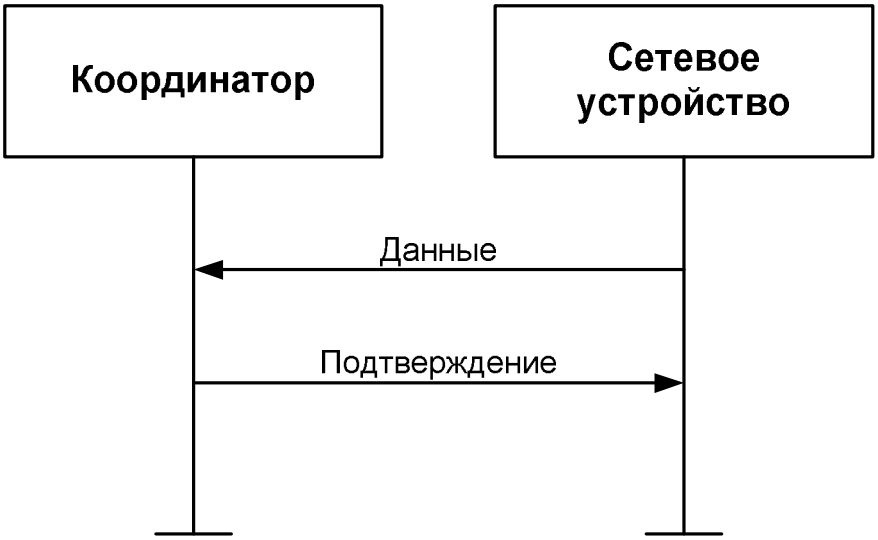


Рис. 8.5. Передача данных координатору в асинхронной сети.

Если координатор хочет передать данные в синхронизируемой сети, он указывает в сигнальном кадре, что устройство ожидает сообщение. Устройство просматривает сигнальный кадр и при обнаружении ожидаемого сообщения передает MAC сообщение запроса данных, используя слоттированный метод CSMA/CA. Координатор подтверждает запрос и передает данные. Устройство подтверждает успешный прием данных с помощью специального кадра подтверждения. Транзакция на этом заканчивается. После получения подтверждения сообщение удаляется из листа ожидающих сообщений в сигнальном кадре. Последовательность представлена на рисунке (Рис. 8.).

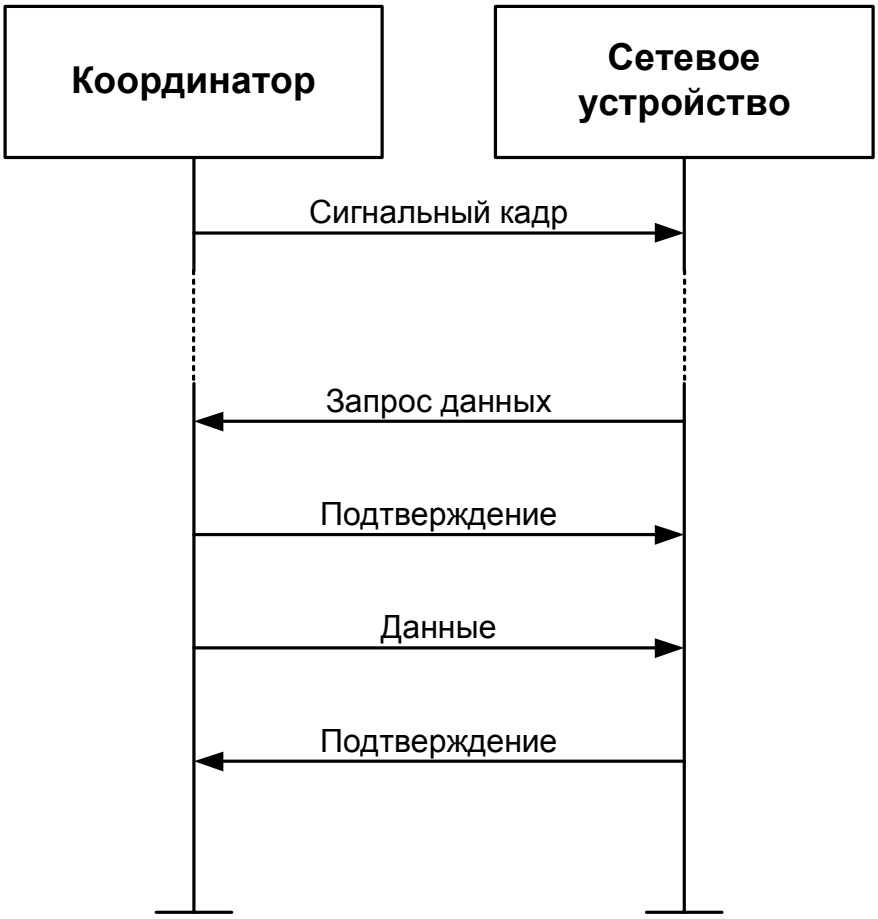


Рис. 8.6. Передача данных от координатора в синхронизированной сети.

Когда координатор хочет передать сообщение в асинхронной сети, он сохраняет данные до тех пор, пока соответствующее устройство не запросит данные. Устройство может контактировать, посылая координатору MAC команду запроса данных с помощью не слоттированного метода CSMA/CA, с определенной приложением частотой. Координатор подтверждает получение запроса с помощью кадра подтверждения. Если для устройства, пославшего запрос, сохранены данные, то они передаются, используя не слоттированный метод CSMA/CA. Если данных для передачи нет, то координатор передает кадр данных с нулевым полем данных, чтобы указать, что никаких данных не сохранено.

Устройство подтверждает успешный прием данных с помощью специального кадра подтверждения. Транзакция на этом заканчивается. Последовательность представлена на рисунке (Рис. 8.).

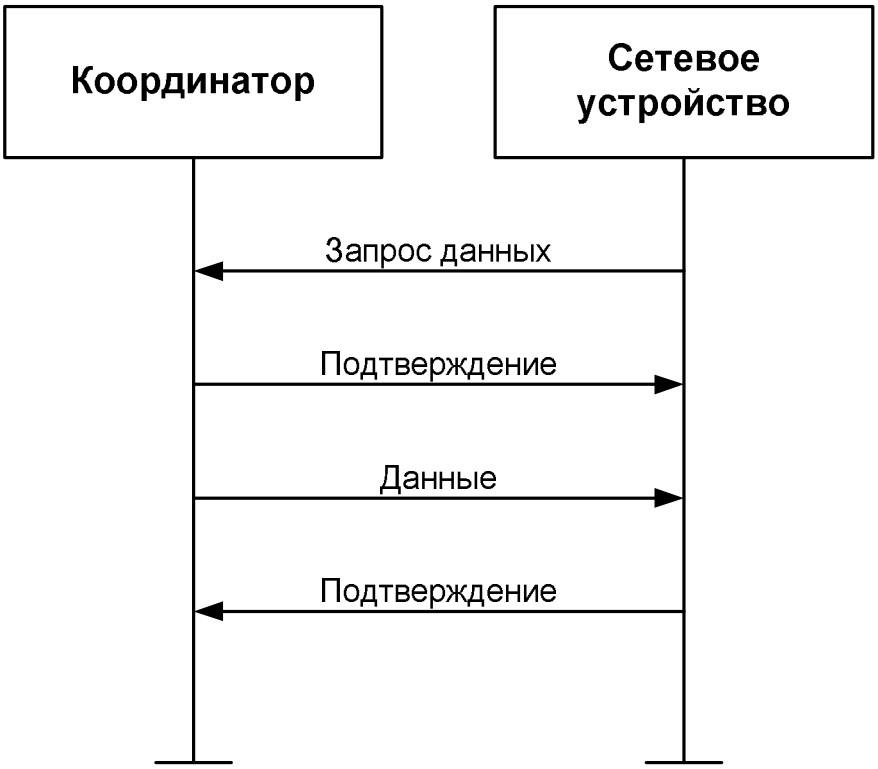


Рис. 8.7. Передача данных от координатора в асинхронной сети.

В одноранговой сети каждое устройство может связываться с любым другим устройством в зоне радио покрытия. Для того, чтобы сделать это эффективно, устройства, которым необходимо соединиться, должны это сделать в определенный промежуток времени либо синхронизироваться друг с другом. В предыдущем примере устройство могло просто передавать данные, используя не слоттированный метод CSMA/CA, но для эффективной работы необходимо провести предварительные мероприятия для достижения синхронизации. Данные действия производятся

протоколами верхних уровней, не относящихся к стандарту IEEE 802.15.4.

Структура кадров была разработана с целью сведения сложности к минимуму, при этом они должны быть достаточно помехоустойчивыми для передачи в канале с сильными шумами. Стандарт IEEE 802.15.4 выделяет четыре типа структур кадров:

- сигнальный кадр используется координатором для передачи маяков;
- кадр данных служит для передачи полезных данных;
- кадр подтверждений служит для подтверждения успешного приема;
- кадр MAC команд служит для управления передачами.

8.6. Надежность.

В стандарте IEEE 802.15.4 предусмотрено несколько механизмов повышения надежности передачи данных, таких как механизм CSMA/CA, подтверждений и проверки данных.

В LR-WPAN применяется два типа доступа к каналу в зависимости от конфигурации сети. В асинхронной сети применяется не слоттированный механизм CSMA/CA. Каждый раз, когда устройство хочет передать кадр данных или MAC команд, оно должно ожидать случайный период времени. Если канал свободен после ожидания, то устройство передает кадр, в противном случае устройство ждет еще один случайный период времени прежде, чем попытается получить доступ к каналу. Кадры подтверждения должны посылаться без использования механизмов CSMA/CA.

В синхронизированной сети используется слоттированный

механизм CSMA/CA, в этом случае период ожидания начинается с момента передачи сигнального кадра. Каждый раз, когда устройство хочет передать кадр во время CAP периода, ему необходимо обнаружить границу (сигнальный кадр), а после этого ожидать случайное число временных слотов, в случае занятости канала устройству необходимо опять ожидать случайное число временных слотов, прежде чем повторить попытку получения доступа. Если канал свободен, то устройство начинает передавать кадр. Кадры подтверждения должны посылаться без использования механизмов CSMA/CA.

Успешный прием и проверка кадров с данными или кадров управления, опционально могут быть подтверждены с помощью специальных кадров. Если принимающее устройство не может обработать полученные кадры данных по какой-либо причине, сообщение не подтверждается. Если источник не получает подтверждения, он предполагает, что передача не удалась и повторяет передачу кадра. Если подтверждение не получено после нескольких попыток, источник может выбирать либо прекращать транзакцию, либо попытаться вновь осуществить ее. Если кадры подтверждений не требуются, источник считает, что передача удалась.

С целью обнаружения битовых ошибок в структуре кадров предусмотрено 16 битное поле для проверки избыточности циклической суммы (CRC).

Протокол был разработан для применения на аккумуляторных устройствах. Однако в некоторых приложениях часть устройств

должна получать питание от сети. Устройствам, питающимся от батареи, потребуется использовать рабочий цикл для снижения энергопотребления. Эти устройства будут проводить большую часть своей жизни в спящем режиме. Каждому устройству необходимо периодически слушать радиоканал с целью обнаружения ожидающего сообщения. Этот механизм позволяет определить баланс между потреблением энергии и временем ожидания доставки сообщений. Устройства, получающие питание от сети, имеют возможность контролировать радиоканал постоянно.

8.7. Безопасность.

Контроль доступа – это сервис безопасности, позволяющий устройству выбрать, с кем оно может устанавливать связь. Если в сети предоставляется сервис контроля доступа, то устройству необходимо составить список контроля доступа (ACL), куда будут занесены устройства, от которых можно получать кадры.

В рамках стандарта IEEE 802.15.4 шифрование данных – это сервис безопасности, использующий симметричный шифр для защиты данных от чтения устройствами без криптографического ключа. Данные могут быть зашифрованы, используя ключ, совместно применяемый в группе устройств (обычно хранится как ключ по умолчанию) или используя ключ известный только двум сторонам (хранится в ACL). Шифрование может осуществляться над полезной нагрузкой сигнального, командного кадров или кадра данных.

Проверка целостности кадра – это сервис безопасности, использующий код целостности сообщения (MIC) для защиты

данных от модификации сторонами без криптографического ключа. Он также обеспечивает уверенность в том, что данные пришли от устройства с криптографическим ключом. В этом стандарте может быть обеспечена целостность кадров данных, сигнальных и командных. Ключ, используемый для обеспечения целостности кадров, может храниться у группы устройств или двух сторон (хранятся в отдельной записи ACL).

Оригинальность последовательности – это сервис безопасности, использующий упорядоченную последовательность входящих кадров для фильтрации повторных пакетов. При получении кадра значение текущего номера в последовательности сравнивается с последним известным номером. Если полученный номер новее сохраненного, то проверка пройдена и номер обновляется, в противном случае кадр отбрасывается. Данный сервис гарантирует, что принимаемые данные новее, чем данные, принятые устройством до этого.

8.8. Альтернативный физический уровень на базе UWB.

Стандарт 802.15.4a создан для поддержки альтернативного физического уровня на базе технологии UWB, а также предоставления расширенных возможностей по отслеживанию мобильных устройств с точностью определения местоположения около 1 м.

Стандарт 802.15.4a расширяет спектр используемых частот, добавляя к поддерживаемому диапазону 14 перекрывающихся каналов с расширенным спектром методом линейной частотной

модуляции (CSS) на частоте 2450 МГц и 16 каналов в трех полосах UWB частот (500 МГц и 3.1 ГГц – 10.6 ГГц). Скорость передачи при использовании физического канала на основе технологии UWB может быть увеличена до 851 кб/с. Для доступа к среде помимо стандартной технологии CSMA/CA можно применять алгоритм ALOHA.

LR-WPAN сети могут работать в нескольких независимых не лицензируемых полосах частот. Устройства LR-WPAN могут быть реализованы в одном диапазоне или нескольких частотных диапазонах, но в каждой реализованной полосе должен поддерживаться обязательный набор каналов этого диапазона для обеспечения совместимости устройств, разделяющих общую полосу.

UWB устройства имеют три независимых частотных диапазона: менее гигагерца (250-750 МГц), низкие частоты (3.1 – 5 ГГц), и высокие частоты (6 – 10.6 ГГц), каждая из UWB частот имеет обязательный канал и устройства предназначенные для этих полос работают независимо от других полос. Для упрощения разработки и внедрения устройства на различных UWB частотах используют одну и ту же полосу пропускания, одни и те же скорости, при этом каждая из полос имеет свою производительность и ограничения на использование в разных регионах.

Спецификация UWB LR-WPAN устройств также включает в себя некоторое количество опциональных улучшений,

позволяющих потенциально улучшить производительность, снизить энергозатраты или улучшить совместную работу разных радиоустройств:

- не подрывает существующие модели LR-WPAN в том, что все приборы, работающие в общей группе, всегда будут иметь возможность взаимодействовать в одном обязательном режиме по умолчанию;
- не поднимает базовую сложность устройств, однако некоторым из существующих LR-WPAN приложений возможно, потребуется увеличение производительности или улучшения возможностей к сосуществованию, при этом сохраняется полная совместимость;
- предоставление возможности UWB LR-WPAN устройствам функционировать в рамках более широкого диапазона радиочастот, в то же время при сохранении высокой производительности и точности.

CSS - это система расширения спектра, похожая как на широкополосную модуляцию с прямым расширением спектра (DSSS), так и на UWB, при этом из-за особых методов модуляции она обладает дополнительными важными свойствами. Применение системы CSS позволяет нескольким сетям одновременно использовать один и тот же частотный канал, а также обеспечивает более высокую производительность. Для еще большего увеличения производительности применяется дифференцированная квадратурная фазовая модуляция. Набор частот в диапазоне 2450 МГц был выбран идентичным сетям IEEE 802.11 High Rate

(HR)/DSSS и IEEE 802.11 extended rate PHY (ERP) для лучшего сосуществования.

LR-WPAN устройства, использующие UWB частоты, работают в спектре отличном от других PHY, использующих нелицензионный спектр. По этой причине важно, чтобы UWB LR-WPAN устройства обеспечивали хорошие показатели сосуществования с другими системами, использующими спектр, перекрывающий UWB диапазон. Исходя из этих соображений, при разработке спецификации UWB PHY в нее были включены дополнительные функции для поддержки сосуществования с другими пользователями спектра, а также с другими UWB систем.

UWB PHY обеспечивает следующие возможности:

– низкую спектральную плотность мощности (PSD), в соответствии с требованиями, предъявляемыми к UWB системам в различных регионах мира;
– несколько частотных диапазонов и рабочие частоты в каждой полосе, чтобы предоставить устройству альтернативный выбор в случае занятости или недоступности рабочей частоты;
– специальные команды, доступные верхним уровням, позволяющие контролировать приемо-передатчик в целях комфортного сосуществования и снижения интерференции;
– опциональное свойство для контроля спектральных характеристик на основе импульсных форм.

9. Протокол ZigBee.

На основе стандарта IEEE 802.15.4 было разработано несколько стеков протоколов для сенсорных сетей. Наибольшее распространение в настоящее время получил индустриальный стандарт ZigBee, разработанный организацией ZigBee Alliance [215], в состав которой входят ведущие разработчики оборудования и программного обеспечения для беспроводных сенсорных сетей. Последняя версия спецификации ZigBee была выпущена в 2007 году. При разработке стека протоколов ZigBee было учтено многое из опыта передовых коллективов разработчиков, работающих в сфере локальных, низкоскоростных, экономичных беспроводных сетей. Спецификация ZigBee обеспечивает стандартизацию организации беспроводной связи между устройствами от разных производителей в различных областях применения. Также спецификация предлагает методы, способствующие быстрому развертыванию и запуску распределенных беспроводных систем управления и наблюдения. Эти методы очень напоминают те, что хорошо известны в проводных промышленных сетях и построены они на концепции профилей устройств. Спецификация интегрировала лучшие модели и практики, принятые при построении локальных распределенных систем управления, их использовании и обслуживании:

- пространственная масштабируемость – количество узлов сети можно увеличивать до 64 тысяч;
- функциональная масштабируемость – одна сеть может использоваться во многих системах управления одновременно,

а их количество и разнообразие можно легко наращивать без изменения программного обеспечения и перенастройки роутеров и координатора сети;

- легкость установки и наладки – оконечные устройства сети сами объявляют о предоставляемых ими сервисах и возможностях и через координатора находят устройства, с которыми они должны взаимодействовать для выполнения целевых задач управления;
- легкость наблюдения за самой сетью и оптимизация ее структуры с помощью специальных методов администрирования;
- решение проблем живучести сети – при потере связи с узлами сети сеть перестраивается, изменяя структуру и маршрутизацию. Можно также легко предусмотреть и дублирование координатора при потере связи с основным координатором;
- решение проблем качества связи – при недостаточном качестве связи можно устанавливать дополнительные роутеры;
- высокая защищенность информации – криптографическая защита на трех уровнях стека. Аутентификация узлов сети;
- открытость для реализации интеграторами собственных протоколов и технологий на базе сервисов предоставляемых ZigBee.

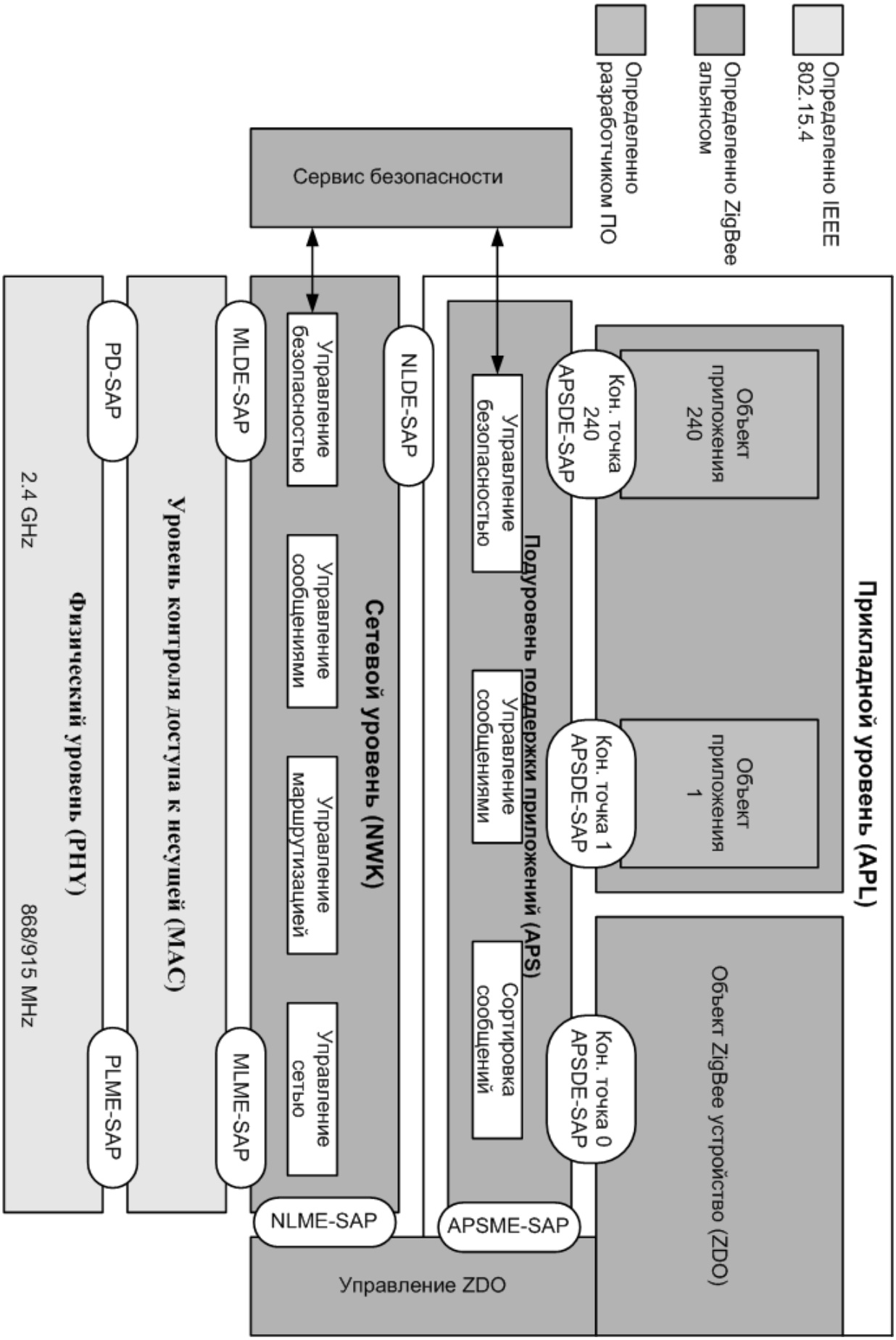


Рис. 9.1. Архитектура стека ZigBee.

9.1. Архитектура стека протоколов ZigBee.

Архитектура стека ZigBee, представленная на рис 9.1, основывается на семиуровневой модели OSI, но регламентирует только часть слоев. Стандарт IEEE 802.15.4-2003 определяет два нижних уровня: физический (PHY) уровень и уровень контроля доступа к среде (MAC). Опираясь на данный стандарт, ZigBee альянс разработал спецификацию, регламентирующую сетевой уровень (NWK), а также структуру прикладного уровня. Прикладной уровень состоит из уровня поддержки приложений (APS), объектов ZigBee устройств (ZDO) и определенных производителем объектов.

Обязанности сетевого слоя NWK включают в себя механизмы, используемые для:

- подключения к сети и отключение от нее;
- применения средств безопасности для кадров;
- маршрутизации кадров до адреса назначения;
- обнаружения и обслуживания маршрутов между устройствами;
- обнаружения ближайших соседей;
- хранения необходимой информации о соседях.

NWK уровень ZigBee координатора также ответственен за инициализацию новой сети и назначение адресов вновь подключившимся устройствам.

Основное назначение подуровня поддержки приложений APS – обеспечить связь сетевого уровня NWK с объектами приложений, его обязанности включают в себя:

- обслуживание таблиц связи (биндинга), определенных как возможность сопоставить два устройства;
- пересылку сообщений между пограничными устройствами;
- определение группового адреса, доставка и фильтрацию групповых сообщений;
- сопоставление 64 битного IEEE адреса и 16 битного NWK адреса;
- фрагментацию, сборку и обеспечение надежной транспортировки данных.

Подуровень ZigBee устройств предоставляет простейший набор функциональных возможностей для обеспечения интерфейса между объектами приложения, профилями устройств и подуровня APS. Обязанности подуровня ZDO включают в себя:

- определение роли устройства в сети (координатор или конечное устройство);
- инициализацию и/или ответ на запрос связи (биндинг);
- управление сервисами безопасности;
- обнаружение устройств в сети и определение, какие сервисы они предоставляют.

9.2. Архитектура ZigBee сети.

Сеть ZigBee включает в себя три типа логических устройств: координатор ZigBee, маршрутизатор ZigBee и оконечное устройство

ZigBee. Соединение не менее двух устройств, одно из которых координатор ZigBee, образует ZigBee сеть.

Координатор ZigBee – полнофункциональное устройство, являющееся координатором PAN. Его функции зависят от топологии сети.

Маршрутизатор ZigBee – полнофункциональное устройство, которое не является координатором ZigBee, однако может быть координатором стандарта IEEE 802.15.4 внутри своей области радиодоступа и маршрутизатором сообщений между устройствами в сети ZigBee.

Конечное устройство ZigBee – любое устройство стандарта IEEE 802.15.4 (RFD и FFD), не являющееся ни координатором, ни маршрутизатором ZigBee.

Сетевой уровень ZigBee поддерживает архитектуры звезда, дерево и ячеистую (Рис.). В архитектуре звезда, сеть контролируется одним устройством, называемым координатор ZigBee. ZigBee координатор отвечает за инициализацию и обслуживание устройств в сети. Все остальные устройства, известные как оконечные устройства, непосредственно общаются с координатором ZigBee. В ячеистой архитектуре и архитектуре дерева ZigBee координатор отвечает за инициализацию сети и выбор некоторых ключевых параметров сети, таких как идентификатор сети и используемый радиоканал, но эта сеть может быть расширена за счет использования ZigBee маршрутизаторов. В сети с архитектурой дерева передача данных и сообщений управления через сеть осуществляется с использованием

иерархической стратегии выбора маршрута и может производится под централизованным управлением, для чего на физическом уровне требуется использовать периодические сигналы маяков от координаторов IEEE 802.15.4. Ячеистые сети используют одноранговые связи, маршрутизация в таких сетях является децентрализованным, распределенным по сети процессом. ZigBee маршрутизаторы в ячеистых сетях не передают маяков IEEE 802.15.4-2003.

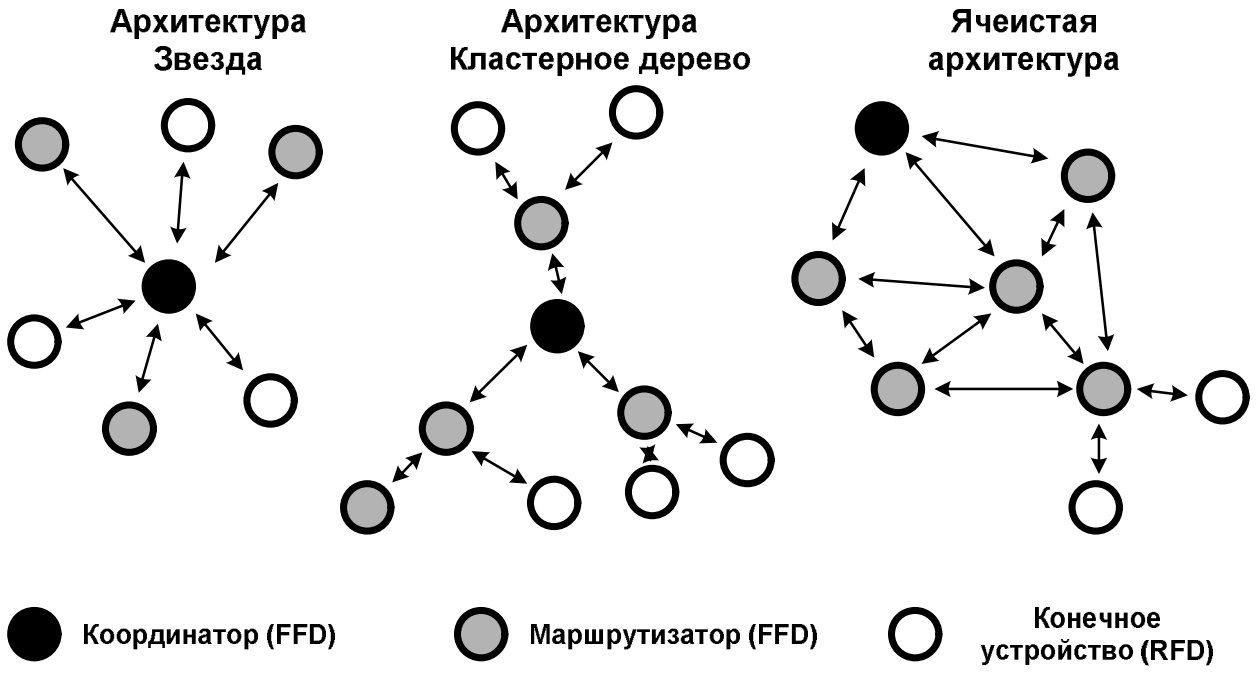


Рис.9.2. Архитектура ZigBee сетей.

ZigBee сети являются самоорганизующимися, после включения координатора сети и выбора первичных настроек все остальные устройства могут подключаться самостоятельно. Координатор начинает с определения уровня энергии на всех доступных частотных каналах. Выбирается канал с наименьшим уровнем энергии. Выбрав канал, координатор определяет наличие в

нем других работающих ZigBee сетей и их идентификаторы через общение с узлами этих сетей. Затем координатор случайным образом выбирает идентификатор для своей сети из диапазона 0x0000-0x3FFE так, чтобы он не совпал с идентификаторами других сетей в том же частотном диапазоне. Сетевой 16-и битный адрес координатора всегда равен 0x0000. Далее координатор разрешает присоединяться к своей сети другим устройствам. Присоединив некоторое количество первых оконечных устройств и маршрутизаторов, координатор отказывается присоединять непосредственно к себе остальных, оставшиеся вынуждены искать уже присоединившиеся к координатору маршрутизаторы (оконечные устройства не могут никого присоединять) и присоединяться к ним. Благодаря этому алгоритму упрощается процесс развертывания сети, сокращается время ввода сети в эксплуатацию. В спецификации также предусмотрен способ заранее запрограммированного подключения устройств к маршрутизатору и координатору.

Во время присоединения к сети устройство получает уникальный в пределах данной сети 16-и разрядный сетевой адрес. С учетом этого сеть может состоять из порядка 64 тысяч узлов. В случае необходимости организации сети с большим количеством узлов следует организовать несколько сетей и связать их шлюзом.

9.3. Маршрутизация.

В зависимости от выбранной топологии сети существует несколько способов маршрутизации в ZigBee сети. Первый способ

маршрутизации в ZigBee сетях – это иерархическая маршрутизация по ветвям древовидной структуры. Иерархической маршрутизацией пользуются по умолчанию все маршрутизаторы и координатор, если у них нет или закончились ресурсы для поддержки других типов маршрутизации.

Другим видом маршрутизации является ячеистая (mesh) маршрутизация. Ячеистая маршрутизация поддерживается только координатором и роутерами, оконечные устройства в ней не участвуют. Оконечные устройства передают пакеты данных только своим родительским узлам, поскольку они не имеют таблиц маршрутизации. Роутеры же, получив пакет данных не предназначенный для его узла-потомка или узла-родителя и не имея соответствующей записи в таблице маршрутизации, инициируют процедуру обнаружения маршрута. Обнаружение маршрута начинается с рассылки соответствующих широковещательных команд всем маршрутизаторам в пределах радиовидимости. Все маршрутизаторы сети принявшие команду создают у себя временные записи о принятом запросе и в разнобой (это специально обеспечивается таймерами со случайно выбранной задержкой) ретранслируют команду дальше, опять же широковещательно. Для того, чтобы широковещательная ретрансляция не превратилась в «радиошторм» у пакетов есть счетчик максимального количества ретрансляций, который уменьшается на 1 при проходе пакета через каждый маршрутизатор.

Возможно существование многих маршрутов прохождения пакетов до узла назначения, но каждый маршрутизатор на пути следования отбрасывает и не ретранслирует пакеты с командами обнаружения маршрута, которые имеют большую стоимость пути, чем уже зафиксированная этим маршрутизатором стоимость у предыдущих пакетов. Если пакет имеет ту же стоимость пути, что уже была зафиксирована маршрутизатором, то он обновляет данные в таблице обнаружения маршрута. Приоритет отдается последнему. Стоимость пути содержится в самом пакете и обновляется в нем всякий раз, когда он ретранслируется маршрутизатором.

Спецификация предлагает несколько вариантов расчета стоимости пути. Самый простой – это просто подсчет количества ретрансляций по маршруту. Более сложный – это вычисление стоимости пути по сумме параметров качества связи между узлами по маршруту LQI. И, наконец, наиболее правильный и самый трудно реализуемый – это суммирование функций от вероятности прохождения пакетов между узлами. Вероятность при этом вычисляется из статистических данных.

Маршрутизатор, являющийся пунктом назначения пакетов команды обнаружения пути, или родительским узлом пункта назначения типа RFD, при получении пакета отвечает пакетом с командой подтверждения. Этот пакет отправляется инициатору маршрута по известному адресу и проходит уже проложенным обратным путем. К этому времени во всех промежуточных маршрутизаторах по пути следования пакета будет создана новая

запись маршрута. Проходящий пакет подтверждения установит статус этой записи маршрута в активное состояние. Дойдя до инициатора обнаружения маршрута, пакет подтверждения завершает процесс формирования маршрута, после которого уничтожаются все временные записи в таблицах обнаружения маршрута во всех промежуточных узлах, а записи таблиц маршрутизации в узлах сохраняются в долговременной памяти.

Рассмотренный выше алгоритм сеточной маршрутизации создает однонаправленный путь. Если в стеке ZigBee константа nwkSymLink установлена в значение TRUE, то этот же путь будет использоваться и для обратной передачи, иначе для обнаружения обратного пути требуется запускать алгоритм маршрутизации заново. Очевидно, что обратный путь может не совпадать с прямым даже при расчете цены по методу простого счетчика переходов, поскольку ветвления по маршруту выбираются на основе генератора случайных задержек.

В спецификации 2006 года введены еще два способа маршрутизации. Это групповая маршрутизация и маршрутизация типа многие к одному. Необходимость в них была вызвана обнаруживающейся при некоторых условиях нестабильностью больших сетей с сеточной маршрутизацией.

Контролируя параметры сети, пытаясь достичь предсказуемого времени доставки сообщений, разработчик сети ограничивает количество узлов, через которые пакет может пройти от источника к получателю. Но спецификация не вносит никаких

ограничений и теоретически можно построить сеть с неограниченным количеством промежуточных узлов.

9.4. Обслуживание маршрутов.

Каждое устройство имеет на уровне NWK счетчик ошибок для всех исходящих соединений, осуществляющих передачу данных. Если значение счетчика превысит определенный параметр, то соединение помечается как сбойное и устройство должно инициировать процедуру восстановления маршрута. Разработчик реализации стека может выбрать либо использование простейшей схемы со счетчиком, либо более точную схему, основанную на временных окнах.

Таким образом, реализуется важное свойство сенсорных сетей – самоустранение неисправностей (self-healing). Динамическая переконфигурация маршрутов в случае выхода из строя или отключения питания некоторых узлов позволяет сенсорной сети самостоятельно поддерживать бесперебойную доставку данных до центра обработки информации в течение длительного периода.

9.5. Взаимодействие с сетью связи общего пользования.

Данные, полученные с сенсоров, необходимо обрабатывать и выводить в необходимом пользователю формате. Производить действия по обработке данных непосредственно на месте сбора нецелесообразно, так как мощность микрокомпьютера (сенсора) ограничена. Установка дополнительного программно-аппаратного комплекса для обработки данных могла бы решить проблему, но, например, при наблюдении за дикой природой невозможна. Для

связи с сетью связи общего пользования устанавливаются шлюзы, передающие поток данных из сенсорных сетей на удаленный центр обработки и хранения информации. В случае наблюдения за окружающей средой это может быть GSM модем или Ethernet интерфейс для подключения к локальной инфраструктуре. Данные после обработки хранятся на определенном сервере и могут быть затребованы пользователем либо клиентской программой через Интернет.

Также часто необходимо обеспечить связанную работу двух и более распределенных в пространстве сенсорных сетей. В этом случае с помощью шлюза организуется интерфейс в транзитную сеть в каждой из сенсорных сетей. В качестве транзитной сети может выступать сеть NGN или глобальная сеть Интернет, защищенные корпоративные сети или специально созданный радиоканал для передачи на большие расстояния. Рис. демонстрирует типичный пример взаимодействия с ССОП.

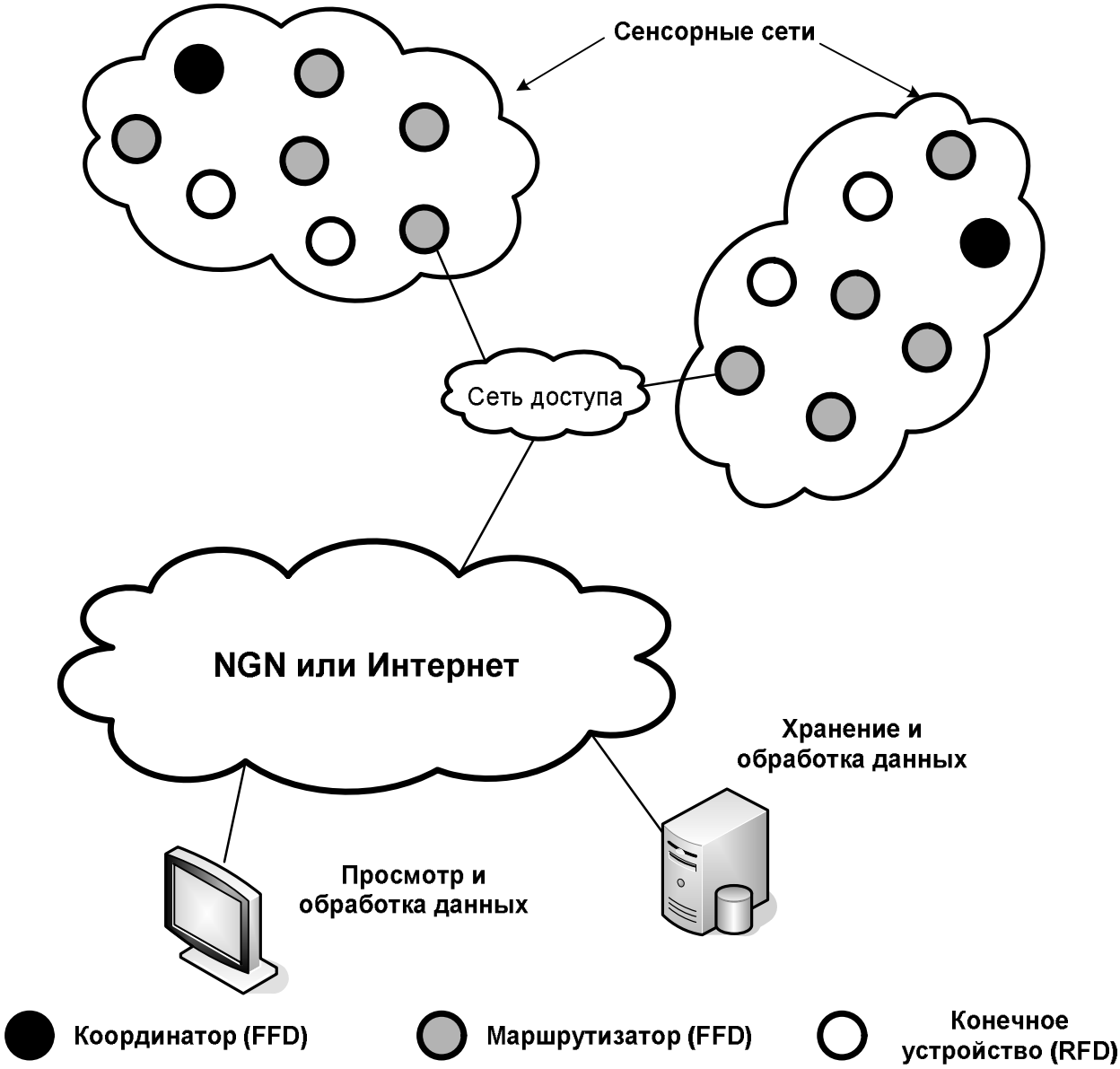


Рис.9.3. Взаимодействие с сетью связи общего пользования.

В настоящее время разработаны и выпущены на рынок шлюзы, позволяющие передавать данные из ZigBee сети в GSM сети мобильных операторов, сети стандарта IEEE 802.11a/b/g, проводные TCP/IP сети. Если не один из готовых вариантов шлюзов не подходит, можно подключить ZigBee модуль к персональному компьютеру посредством интерфейса USB или

RS232 и передавать с помощью любого доступного на компьютере сетевого интерфейса.

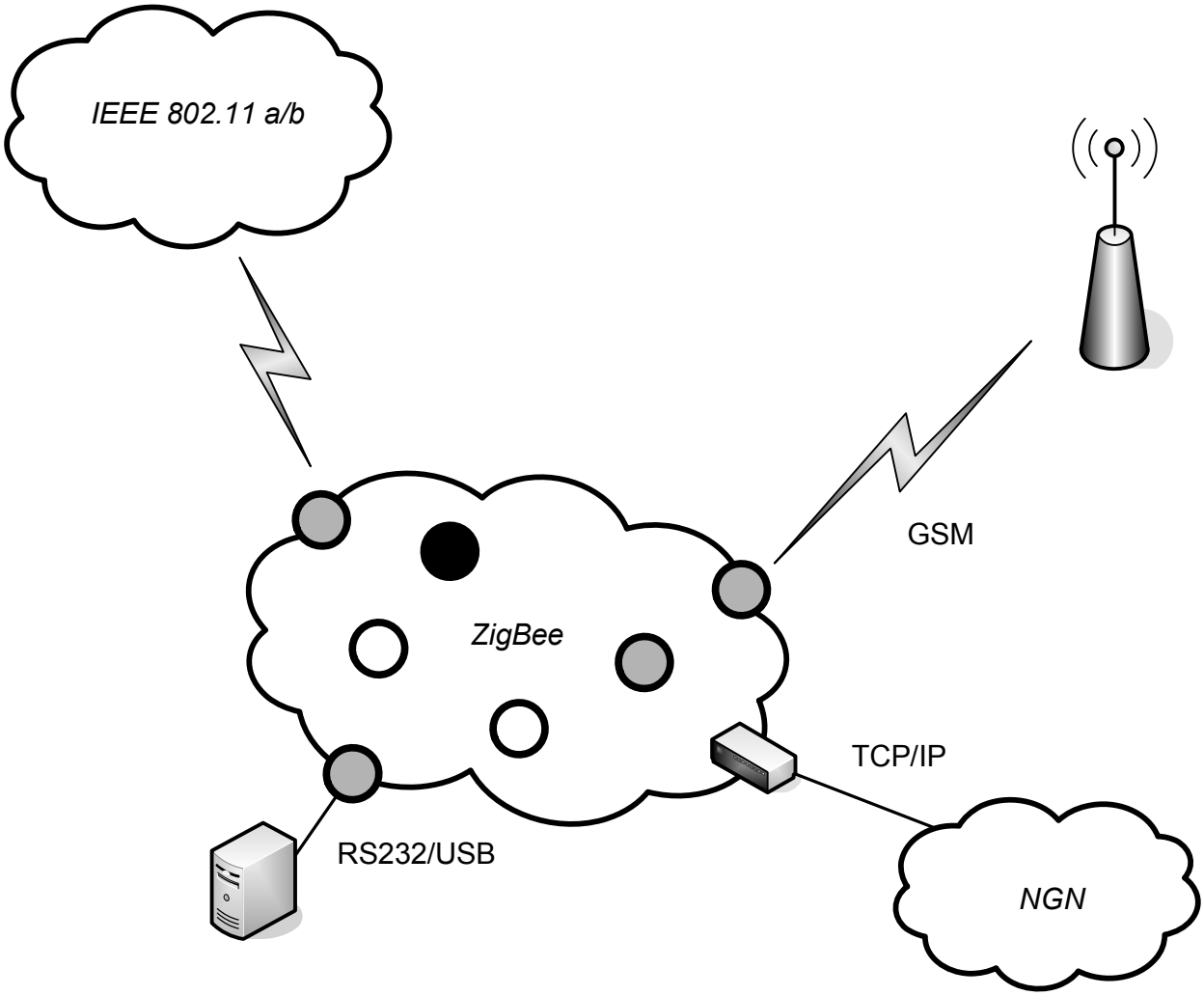


Рис.9.4. Взаимодействие с различными сетями.

10. Протокол 6LoWPAN.

До недавних пор использование IP подхода было невозможно в беспроводных сенсорных сетях, поскольку IP протокол не мог масштабироваться для работы на микроконтроллерах с каналами с ограниченной энергией таких, как радиоканал IEEE 802.15.4. Пакеты, используемые в IEEE 802.15.4, достаточно малы, также весь стек протоколов должен использовать очень малое количество памяти.

Проект стандарта IETF 6LoWPAN, рекомендующий передачу сообщений IPv6 поверх 802.15.4, выпущенный в марте 2007 года, изменил все. Потенциал 6LoWPAN для работы с устройствами с низким потреблением энергии делает его привлекательным для использования не только в портативной технике, но и в широком диапазоне промышленных средств. Встроенная поддержка шифрования AES-128 закладывает основу для надежной аутентификации и безопасности. Для того, чтобы быть конкурентоспособным по отношению к другим протоколам, в 6LoWPAN применяется «плати только за то, что используешь» схема сжатия заголовков. При прямой интеграции с IP маршрутизаторами появляется превосходство в использовании наиболее продвинутых сетевых систем безопасности в отличие от тех, что предлагаются шлюзами в ad hoc сети.

10.1. Преимущества 6LoWPAN

Рабочая группа IETF 6LoWPAN была сформирована для решения проблемы передачи IP пакетов поверх каналов IEEE

802.15.4 способом, удовлетворяющим открытым стандартам и предоставляющим взаимодействие с другими IP каналами и устройствами в той же мере, как и с устройствами 802.15.4.

Такое решение имеет множество преимуществ. Каждый сенсор в 6loWPAN сети имеет персональный IPv6 адрес. Это позволяет многим компаниям производить LR-WPAN устройства, которые могут работать вместе в одной сети, позволяет взаимодействовать данным устройствам, работать с сетевыми компьютерами и оборудованием, которое уже существует. Каждый узел сенсорной сети становится доступен из внешних сетей по IP адресу. Это избавляет от необходимости иметь комплексные шлюзы для каждого локального 802.15.4 протокола, множества адаптеров, используемых существующими приложениями для связи через эти шлюзы, упрощает множество специфичных для шлюзов процедур аутентификации и безопасности. Множество устоявшихся, основанных на IP протоколе программных инструментов, таких как ping, traceroute, SNMP может быть сразу же использовано для объединения в сеть и обслуживания LR-WPAN устройств. Также на базе IP может быть легко реализовано NAT (преобразование сетевых адресов), распределение нагрузки, кэширование. Существующие модели передачи данных на программном уровне и сервисы на базе HTTP/XML/SOAP позволяют упростить процесс разработки приложений для LR-WPAN сетей и унифицировать интеграцию устройств в существующую корпоративную сеть.

10.2. Сжатие заголовков IPv6

Однако использование IP инфраструктуры приносит также и сложности. Адреса и заголовки, используемые в IPv6 большие и поэтому данные, которые необходимо передавать могут оказаться больше, чем размер пакета 802.15.4. В 6loWPAN это решается разбивкой пакета на более маленькие. Применяя сжатие заголовков, можно добиться существенного увеличения размера передаваемой полезной информации. На рисунке представлен 6loWPAN пакет, в котором стандартный 40-байтный IPv6 и 8-байтный UDP заголовки сжаты до 7 байт, что даже меньше обычного ZigBee заголовка (рис.10.1).

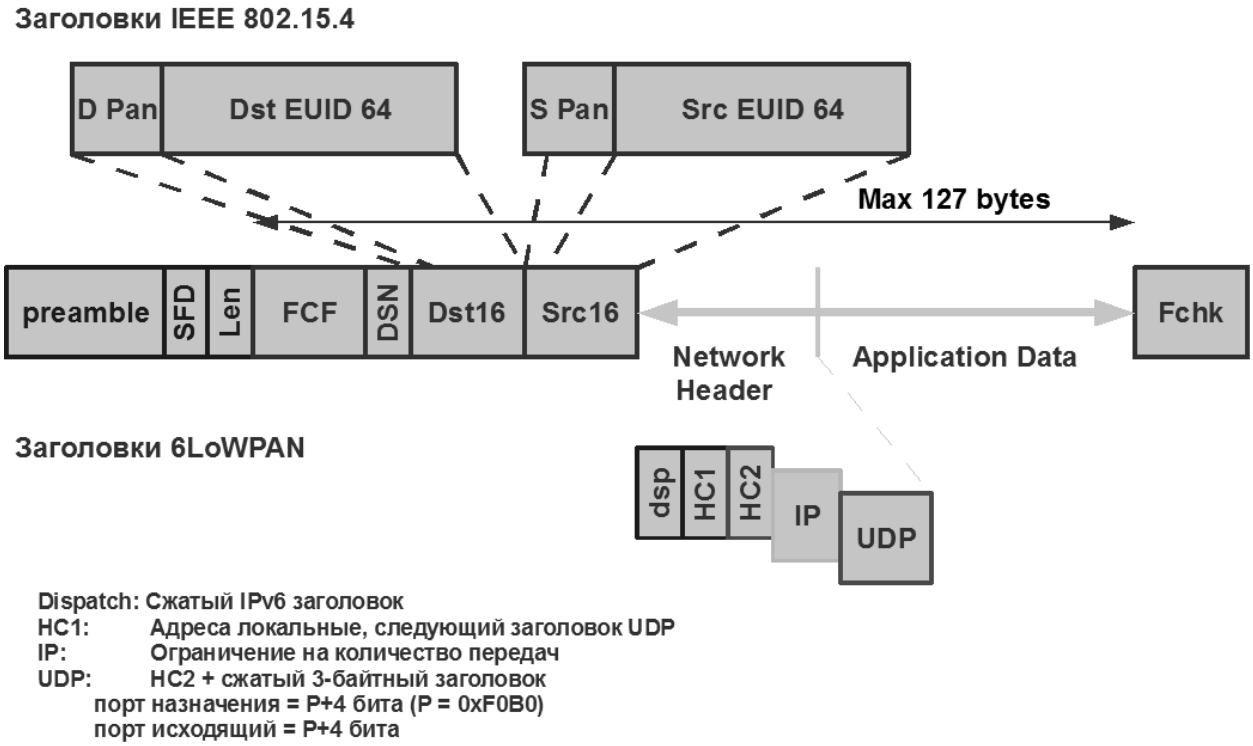


Рис. 10.1. Структура пакета со сжатым IPv6 заголовком.

Когда устройство 802.15.4 связывается с близлежащим устройством IP, адрес может быть сжат до одного байта, указывающего на то, что адрес назначения берется из канального

адреса 802.15.4 пакета. Когда связь устанавливается с устройством вне сенсорной сети, полный IP адрес включается в заголовок. Стандарт IPv6 требует, чтобы все каналы связи поддерживали пакеты размером до 1280 байт. Если передаваемые данные настолько малы, что умещаются в простом пакете 802.15.4, они могут быть добавлены без избыточной информации, в противном случае добавляется заголовок фрагментации для отслеживания того, как сообщение разбито на части. При невозможности устройства самостоятельно доставить сообщение до адресата добавляется заголовок меш (mesh) маршрутизации. При использовании меш маршрутизации адреса источника и назначения могут быть записаны в виде короткого 16-битного или полного 64-битного адресов. В меш заголовок также включается счетчик передач (Hops Left), позволяющий ограничить время жизни пакета максимум четырнадцатью передачами. Выбор меш протокола осуществляется на устройстве при каждой передаче. Рис. 10.2 демонстрирует 6LoWPAN пакет, использующий меш маршрутизацию и сжатие заголовков.

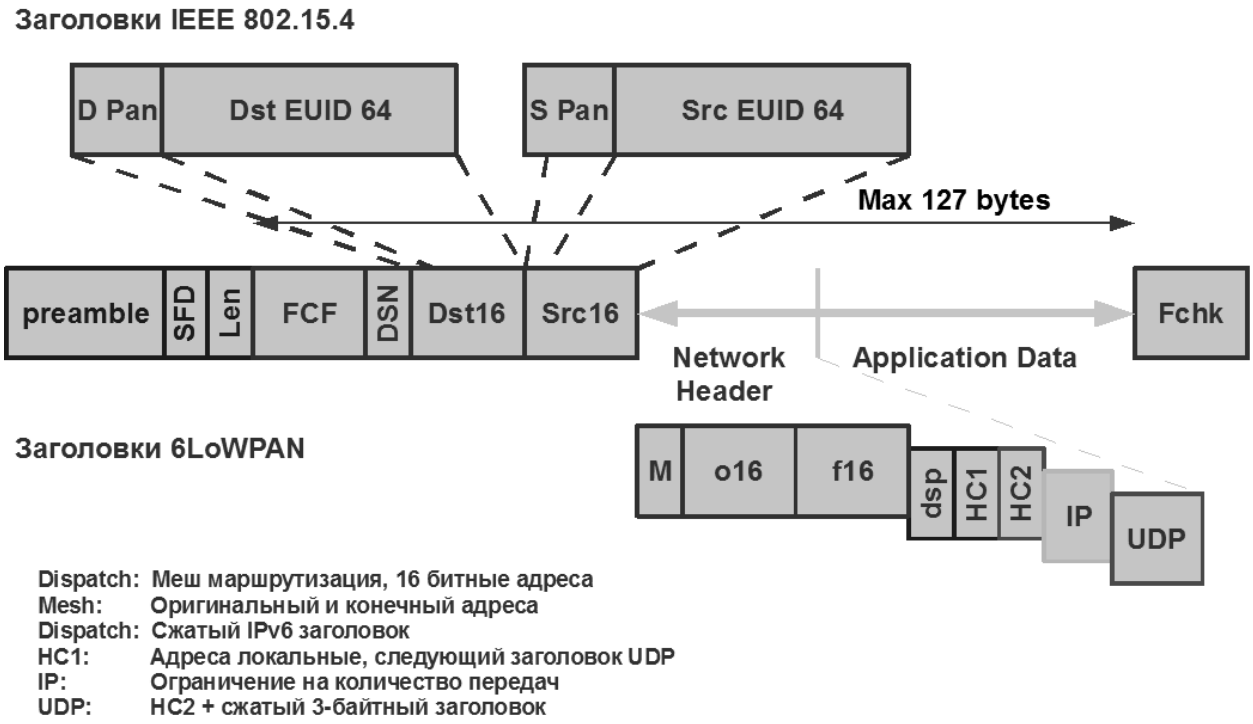


Рис. 10.2. 6LoWPAN пакет с поддержкой меш маршрутизации.

Схемы сжатия заголовков LOWPAN_HC1 и LOWPAN_HC2, как показала практика, не эффективны для большинства практических применений IPv6 в LR-WPAN. Наибольший эффект от использования LOWPAN_HC1 достигается при использовании локальных одноадресных коммуникаций, характерных для протоколов маршрутизации, обнаружения или DHCPv6 и очень редко применяемых в передаче данных уровня приложений.

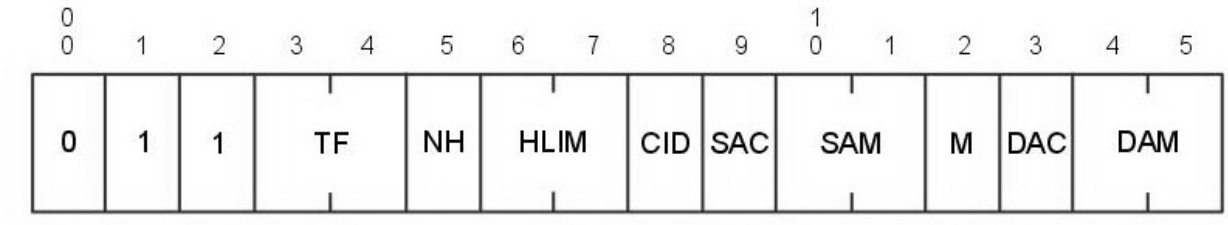
Маршрутизируемый адрес необходимо использовать в случае передачи данных на устройство расположенное вне сети 6LoWPAN или при использовании схемы маршрутизации «route-over». Для маршрутизируемого адреса LOWPAN_HC1 требует передачи префикса IPv6 для обоих адресов — источника и назначения. При использовании мультикаст вещания, требовалось передавать полный 128-битный адрес.

В результате в 2008 году была начата работа над проектом спецификации Compresion Format for IPv6 Datagrams in Low Power and Lossy Networks (draft-ietf-6lowpan-hc), определяющей новый формат кодирования заголовков LOWPAN_IPHC, для эффективного сжатия уникальных локальных, глобальных и мультикаст IPv6 адресов, на основе распространения состояния с помощью контекста. В дополнении в данной спецификации также были предложен ряд улучшений к формату сжатия заголовков, описанному в RFC4944.

Важной особенностью данной спецификации являлось наличие механизма LOWPAN_NHC, формата используемого для сжатия заголовка следующего непосредственно за IPv6 заголовком. В схеме сжатия LOWPAN_HC1 можно было организовать сжатие последующих заголовков используя LOWPAN_HC2, но только для протоколов UDP, TCP и ICMPv6. Однако биты заголовков HC2 размещаются между октетами сжатых заголовков HC1 и несжатыми полями заголовков IPv6. В новой спецификации данные следующего заголовка помещены после всех относящихся к IPv6 битов, что позволяет добиться правильной структуры слоев и обеспечить прямую поддержку заголовков расширений IPv6.

Непосредственно в спецификации описаны форматы для сжатия UDP заголовков, а также инкапсуляции IPv6-в-IPv6 и IPv6 Extension Headers. Но список может быть с легкостью расширен для необходимого набора протоколов.

В общем виде формат LOWPAN_IPHC может быть представлен в следующем виде:



TF	2 бита	Класс нагрузки и метка потока
NH	1 бит	Флаг следующего заголовка
HLIM	2 бита	Флаг ограничения количества передач
CID	1 бит	Идентификатор контекста
SAC	1 бит	Сжатие адреса источника
SAM	2 бита	Режим сжатия адреса источника
M	1 бит	Сжатие мультикаст адреса
DAC	1 бит	Сжатие адреса назначения
DAM	2 бита	Режим сжатия адреса назначения

10.3. Концепции «mesh-under» и «route-over».

Протокол 6LoWPAN включает в себя два типа маршрутизации, механизм меш маршрутизации канального уровня, называемый «mesh-under» и передача пакетов с использованием IP адресации - «route-over». Различия между этими механизмами похожи на различия между мостовыми сетями и IP маршрутизации поверх Ethernet. При «mesh-under» маршрутизации все узлы размещаются на одном канале, обслуживаемом одним или несколькими роутерами, называемыми Пограничными маршрутизаторами 6LoWPAN (6LoWPAN Border Router — 6LBR).

В сетях «route-over» одновременно существует несколько каналов. В отличие от фиксированных IP каналов, участники данных каналов могут меняться в соответствие с свойствами беспроводной сети, такими как низкое энергопотребление и условия окружающей среды. Данные сети состоят из гибкого набора связей между внутренними роутерами, называемыми 6LoWPAN маршрутизаторами (6LoWPAN Routers — 6LR).

В сетях «route-over» имеется два типа маршрутизаторов — 6LBR и 6LR. Пограничные маршрутизаторы расположены на границе сетей 6LoWPAN и остальных сетей, тогда как маршрутизаторы 6LoWPAN размещены внутри сети и выполняют протокол маршрутизации.

В конфигурации «mesh-under» 6LBR выступают как IPv6 маршрутизаторы, тогда как все хосты LR-WPAN находятся на одном канале, на расстоянии одного IP перехода. В такой топологии не существует 6LoWPAN маршрутизаторов, т.к. пересылка обслуживается протоколом маршрутизации канального уровня.

В обоих конфигурациях хосты не принимают участия в маршрутизации и пересылке пакетов, так как они работают в качестве простых IPv6 узлов.

10.4. Neighbor Discovery.

Основных методы, такие как поиск пути, выбор адреса, определение дубликатов адресов, позволяющие функционировать IPv6 сети описываются в RFC4861 - IPv6 Neighbor Discovery. После

того как подается питание и инициализируется проводная IPv6 сеть, узел присоединяется к мультикаст адресу режима запроса, и далее следует операция нахождения дублирующего адреса (Duplicate Adress Detection - DAD) для назначенного локального канального адреса (link-local adress) с помощью посылки многоадресного (мультикаст) сообщения в канал. После этого посылается многоадресное сообщение на общий адрес маршрутизаторов для запроса объявлений маршрутизатора. Если хост получит пакет Router Advertisement (RA) с флагом "A", он автоматически настроит IPv6 адрес с учетом префикса полученного в сообщении RA. Кроме того маршрутизаторы периодически посылают в сеть объявления на мультикаст адрес, включающий все узлы сети.

Узлы посылают сообщения запроса и объявления соседей (Neighbor Solicitation/Neighbor Advertisement - NS/NA) для определения IPv6 адресов узлов назначения на выбранном канале. Использование механизма DAD и рассылка периодических объявлений маршрутизаторов подразумевает, что узлы постоянно получают питание и доступны для соединения большую часть времени.

В механизмах обнаружения соседей маршрутизаторы находят узлы, учитывая, что префикс подсети соответствует домену многоадресной рассылки, и можно послать мультикаст сообщение NS для нахождения узла и его канального адреса. Кроме того DAD подразумевает что все узлы автоматически настроившие свой IPv6

адрес с учетом единого префикса могут быть доступны по локальному канальному многоадресному сообщению.

В сетях LR-WPAN в основном используются два типа топологий - звезда и одноранговая. Топология звезда похожа на обычную IPv6 сеть с маршрутизатором и набором узлов подключенных к единому каналу. Но в одноранговых сетях у узлов есть возможность маршрутизировать и пересылать пакеты. Набор связей между узлами может меняться с течением времени из-за нестабильности беспроводных соединений вследствие влияния внешних физических раздражителей. Также особенностью 6lowpan сетей является наличие двух типов локальных адресов: короткого 16 битного и уникального 64 битного. Учитывая особенности LR-WPAN сетей, потребовалась дополнительная оптимизация и расширения для механизмов IPv6 Neighbor Discovery.

При изменение протокола основные задачи были следующие:

- Оптимизация с помощью механизмов достаточных для работы с обоими вариантами маршрутизации «mesh-under» и «route-over».
- Связь хоста с маршрутизатором должна осуществляться теми же методами, в независимости от используемой маршрутизации «mesh-under» и «route-over».
- Минимизация передачи сигнальной информации, исключением использования мультикаст флудинга и уменьшения количества канальных многоадресных сообщений.

- Оптимизация интерфейса между хостами и основными маршрутизаторами.
- Обеспечение поддержки хостами режима сна.
- Снижение сложности узлов.
- Опциональное распространение контекстной информации и префиксной информации от пограничного маршрутизатора к внутренним.
- Выработка опционального механизма обнаружения дублирующих адресов, подходящего для сетей с маршрутизацией «route-over».

Наиболее важной частью оптимизации является изменение взаимодействия хост-маршрутизатор, которые бы поддерживали спящие узлы и позволили избежать многоадресной рассылки, кроме случаев поиска узлом базового списка роутеров и повторное обнаружение в случае утраты соединения с ним.

Также было разработано расширение для поддержки сжатия заголовков описанного в проекте спецификации [I-D.ietf-6lowpan-hc], с помощью передачи информации о сжатии в новой опции сообщения Router Advertisement.

В дополнении были разработаны опции и отдельные механизмы, которые могут быть использованы в соединениях между 6LR и 6LBR для выполнения многоадресного определения дублирующих адресов (DAD) и распространения информации о префиксе сети и опций сжатия.

Протокол разработан таким образом, что взаимодействие хост-маршрутизатор не подвержено влиянию конфигурации сети 6LOWPAN, оно одинаково при использовании механизмов маршрутизации "mesh-under" и "route-over".

Протокол, описанный в проекте спецификации [ietf-6lowpan-nd] вводит следующие оптимизации и расширения к протоколу IPv6 Neighbor Discovery (RFC4861):

- Инициализируемое хостом обновление информации RA. Это убирает необходимость периодического или не запрашиваемого обновления Router Advertisement от маршрутизаторов к узлам.
- Механизм DAD не выполняются в случае использования IPv6 адресации на базе EUI-64 (так как данные адреса считаются глобально уникальными).
- Механизм DAD не обязателен в случае использования DHCPv6 для назначения адресов.
- Используется новый механизм регистрации адресов с помощью опции Adress Registration передаваемой от узла к маршрутизатору. Это избавляет от необходимости маршрутизаторами использовать мультикаст рассылку Neighbor Solication для нахождения узлов, и обеспечивает поддержку спящих хостов. Это также разрешает использования единых адресных префиксов IPv6 в LR-WPAN с механизмом "route-over".
- Поддержка новой опции сообщения RA, для поддержки контекстной информации используемой в сжатии

заголовков 6LoWPAN.

- Новый необязательный механизм для выполнения DAD поверх сетей LR-WPAN с маршрутизацией "route-over", использующий сообщения запроса и подтверждения дублирующего адреса (Duplicate Adress Request and Confirmation).
- Новый необязательный механизм для распространения информации о префиксах и контекстах в сетях, использующий опцию Надежный пограничный маршрутизатор (Authoritative Border Router - ABRO) для контроля за флудингом изменений конфигураций.
- Представлено несколько новых протокольных констант и изменений некоторых существующих.

10.4.1. Назначение адреса.

Узлы 6LoWPAN конфигурируют свои IPv6 адреса с помощью механизмов, рассмотренных в спецификациях RFC4861 и RFC4862, основываясь на информации, полученной в сообщение Router Advertisement. Однако использование флага M в предложенной оптимизации более ограниченно, по сравнению с рекомендацией RFC4861. Когда флаг M установлен, узел должен использовать DHCPv6 для получения любого не основанного на EUI-64 адреса. В случае же не установленного флага M, сеть должна поддерживать механизмы обнаружения дублирующих адресов, что бы хост мог безопасно использовать механизм регистрации адресов для проверки на уникальность адреса не основанного на EUI-64.

Маршрутизаторы 6LR могут использовать те же механизмы для конфигурации своих IPv6 адресов.

Маршрутизаторы 6LBR отвечают за обслуживание префиксов, назначенных сети LR-WPAN, используя ручную конфигурацию, DHCPv6 Prefix Delegation (RFC3633) или другие механизмы. В изолированных сетях LR-WPAN префикс ULA (RFC4193) должен генерироваться 6LBR.

10.4.2. Взаимодействие узел-маршрутизатор.

Узел посылает сообщение Router Solicitation при включении в сеть, а также в случае потери связи с одним из основных маршрутизаторов (после проверки Neighbor Unreachability Detection по направлению недоступного маршрутизатора).

Узел получает сообщение RA, обычно содержащее опцию надежного маршрутизатора ABRO и дополнительно переносящих одну или несколько опций контекста (6LoWPAN Context Option - 6CO) в дополнении к существующей префиксной информации (Prefix Information Option - PIO) как описано в RFC4861.

В случае, когда хост конфигурирует не канальный (link-local) IPv6 адрес, он регистрирует его на одном или нескольких из своих основных маршрутизаторов, используя опцию регистрации адреса (Adress Registration Option - ARO) в сообщении NS. Узел выбирает время поддержки регистрации (lifetime) и периодически повторяет сообщение ARO (до истечения времени поддержки) для обслуживания регистрации. Время поддержки должно выбираться с учетом периода нахождения узла в состоянии сна. С другой

стороны мобильные узлы, часто меняющие точку взаимодействия с сетью должны выбирать более короткое время поддержки регистрации.

Процесс регистрации может сбиться (опция ARO вернется на узел с не-нулевым статусом), если маршрутизатор определит, что выбранный IPv6 адрес уже используется другим узлом. Это может использоваться для поддержки адресации основанной не на EUI-64, например временной IPv6 адресации описанной в рекомендации RFC4941 или адресации основанной на идентификаторе интерфейса - коротком 16-ти битном адресе 802.15.4 Ошибка также может произойти в случае переполнения кэша Neighbor Cache на маршрутизаторе.

Повторная регистрация может быть совмещена с процессом определением недоступности соседей (Neighbor Unreachability Detection - NUD) по отношению к маршрутизатору, так как оба процесса используют одноадресное сообщение NS. Это возможно в случае когда узел просыпается для того что бы отправить сообщение и ему нужно проверить что маршрутизатор все еще доступен, а также обновить свою регистрацию.

Ответ на регистрацию адреса может быть получен не сразу, т.к. в случае конфигурации "route-over" маршрутизатор 6LR может инициализировать проверку DAD на 6LBR. Узел повторно отправляет сообщение ARO, до получения подтверждения о получении.

В отличие от рекомендации RFC4861 для отправки сообщения Adress Resolution используется не многоадресная рассылка. Вместо этого маршрутизатор поддерживает кэш neighbor Cache всех зарегистрированных адресов IPv6. В случае отсутствия адреса в кэше маршрутизатора считается, что адрес не существует, или закреплен за другим маршрутизатором сети LR-WPAN, или считается внешним для сети. В случае использования конфигурации "route-over" передачи таких пакетов на узел назначения используется протокол маршрутизации.

10.4.3. Взаимодействие маршрутизатор-маршрутизатор.

Необязательные новые механизмы взаимодействия маршрутизатор-маршрутизатор используются только в конфигурации "route-over", где присутствует тип устройств 6LR. Данные расширения опциональны т.к. функции, предоставляемые ими, могут быть реализованы другими протоколами, например DHCPv6, протоколами канального уровня, протоколами маршрутизации или другими механизмами. Подразумевается, что все 6LR настроены на выполнение данных функций однородно. Например, передача контекстной и/или префиксной информации выполняется средствами данного протокола, а DAD выполняется с помощью другого протокола.

6LR могут вести себя как обычные узлы во время инициализации и конфигурации префиксов, посылая сообщения RS и автоматически настраивать свои адреса в отличие от поведения маршрутизаторов в рекомендации RFC4861.

Когда используется многоадресный префикс или распространение контекста, тогда маршрутизаторы 6LR сохраняют полученную (напрямую или нет) ABRO, 6CO и префиксную информацию и повторно распространяют ее в сообщениях RA для других маршрутизаторов или узлов, в ответ на запрос RS. В ABRO предусмотрен флаг версии, позволяющий ограничивать неконтролируемое распространение информации между 6LR.

Дополнительно маршрутизаторы 6LR могут выполнять определение дублирующих адресов на одном или нескольких 6LBR, используя сообщение запроса дублирующего адреса (DAR) и ответа (DAC), содержащего информацию из сообщения Adress Registration. Сообщения DAR и DAC будут передаваться между маршрутизаторами, при этом правило на максимальное количество переходов, равное 255. не распространяется на данные сообщения.

Алгоритм взаимодействие узлов воспроизведен на рис.10.3.

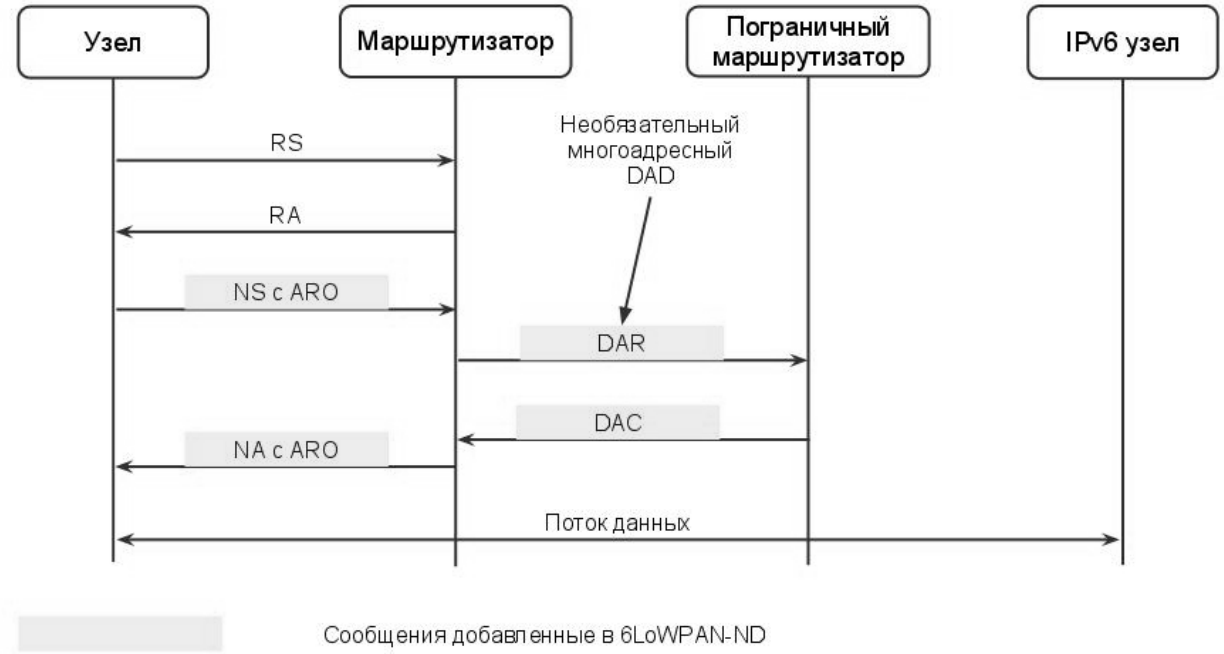


Рис.10.3. Алгоритм взаимодействия узлов.

10.5. Защита данных в 6LoWPAN.

При объединении различных устройств и сетей необходимо подумать о безопасности передачи данных. Передаваемые данные по радио каналу могут быть «подслушаны». Безопасность на физическом уровне является первоначальной основой для защиты информации. IEEE 802.15.4 регламентирует очень мощную систему шифрования AES-128 и все микроконтроллеры интегрируют возможности шифрования в аппаратное обеспечение. Устройство имеет ключ защиты, получаемый при вводе устройства в эксплуатацию, с помощью которого шифруются все передаваемые пакеты и дешифруются принимаемые. С помощью этих ключей устройства также проходят процесс аутентификации.

Сенсорные сети часто подключают к другим сетям, для того чтобы передавать информацию для дальнейшей обработки. Для

немаршрутизируемых протоколов, таких как ZigBee, HART, SCADA и RS-485 подключение может быть выполнено с помощью шлюзов — обычно это компьютеры с IP подключением и интерфейсом в сенсорную сеть. Слабым звеном в обеспечении безопасности обычно становится шлюз. Если шлюз был взломан, то под угрозой окажется вся LoWPAN сеть. Такие шлюзы чаще всего управляются стандартной операционной системой с известными ошибками безопасности, которые могут быть использованы для взлома. Для снижения вероятности взлома шлюзы устанавливают за фаерволом, ограничивающим доступ.

Если сенсорная сеть строится на основе IP протокола, то в качестве шлюза может быть использован простой маршрутизатор между обычной сетью и сенсорной. Это специализированное устройство, на котором нет необходимости запускать стандартную операционную систему и дополнительные приложения. Он может настраиваться и обслуживаться точно так же, как и другие сетевые маршрутизаторы. И может дополнительно предоставлять услуги фильтрации пакетов и ограничения доступа. Маршрутизатор может предоставлять простейшие сервисы трансляции адресов, конфигурируемые правила для фаервола часто используемые в домашних и коммерческих сетях, а также селективно давать доступ к устройствам 802.15.4 из корпоративной сети, подобно DMZ хостов в обычной сети.

10.6. Сравнение 6LoWPAN с существующими корпоративными стандартами.

В настоящее время наиболее популярным протоколом маршрутизации является ZigBee, но он имеет ряд недостатков по сравнению с 6LoWPAN. В ZigBee описывается только лишь взаимодействие с другими узлами 802.15.4, для передачи данных сенсоров для дальнейшей обработки необходимо устанавливать шлюзы, которые не смогут прозрачно обеспечить доступ к определенному сенсорному узлу. Для написания программного обеспечения необходимо реализовывать верхние уровни стека, вместо использования существующих стандартов. Спецификация все еще активно разрабатывается, текущий стандарт ZigBee 2007 не совместим с ZigBee 1.0. Отсутствует транспортный уровень. В настоящее время ZigBee альянс заявил о работе над реализацией поддержки IP в ZigBee стеке.

Стек протоколов SP100.11a находится на ранней стадии развития, но ему придется определить и описать многое из того, что уже сделано в протоколе IP. После реализации стандарта заявлена поддержка разнообразных типов каналов, таких как 802.15.4, 802.11, WiMax. Его отличительной особенностью является использование TDMA технологии.

Стандарт 6LoWPAN описывает, как применить сетевые уровни IP для передачи по каналам 802.15.4. Он позволяет устанавливать передачу между устройствами 802.15.4, а также связывать устройство 802.15.4 с другим IP-оборудованием. Благодаря внедрению IPv6 можно использовать широкий спектр

протоколов верхнего уровня, прикладного программного обеспечения и инструментов. Цель его создания позволить использовать новый класс устройств в обычной манере.

Энергетическая эффективность протокола 6LoWPAN сравнима с корпоративными аналогами. Другие протоколы передают похожую адресную информацию. Протокол 6LoWPAN оптимизирован для обмена информацией в подсети 802.15.4. Больший расход энергии необходим лишь при передаче данных в другие сегменты IPv6 сети, из-за увеличения размера заголовков, но другим протоколам в аналогичной ситуации необходимо передать ту же информацию, только на уровне приложений, для указания шлюзу узла назначения данных.

11. Введение в наносети.

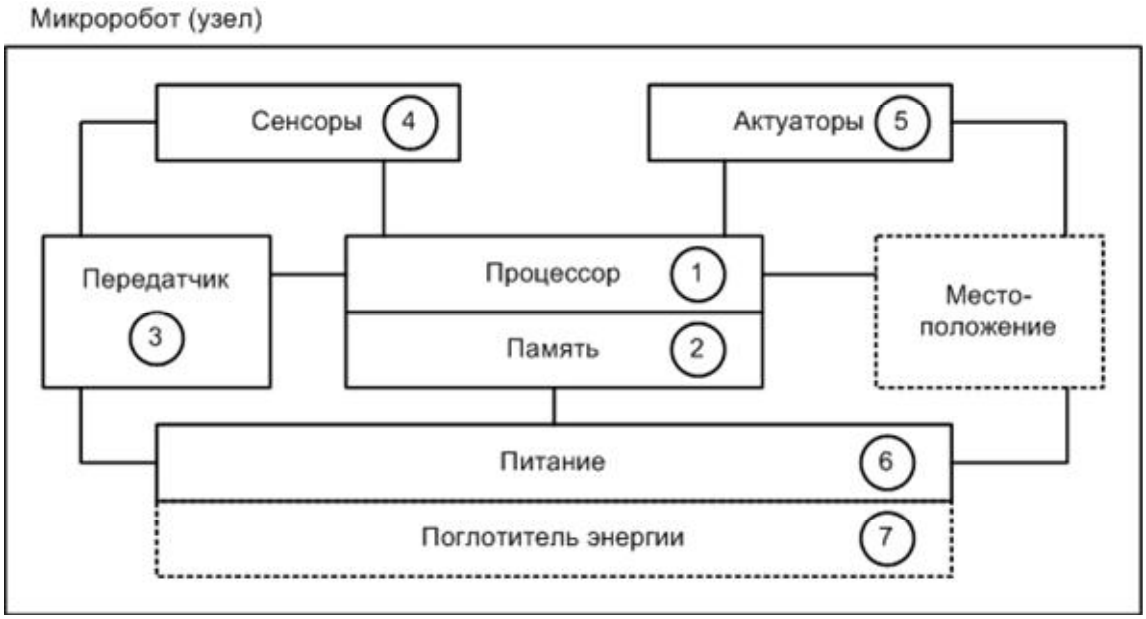
11.1. Классификация наносетей.

Как уже отмечалось выше, в соответствии с прогнозами число беспроводных устройств к 2017 – 2020 годам составит 7 триллионов (на 7 миллиардов человек!) [207]. При этом, каждое из них использует для передачи информации радиочастотный спектр.

Радиочастотный спектр представляет собой ограниченный ресурс, использование которого в настоящее время регламентируется административными процедурами. Поскольку любое административное регулирование ограниченных ресурсов является неэффективным, научное сообщество в последние годы предложило идею так называемых когнитивных сетей [1,68], т.е. сетей с динамическим распределением спектра. Когнитивные сети позволяют более эффективно использовать радиочастотный спектр, но не решают самой проблемы передачи информации с помощью электромагнитных волн. Прошло уже более 100 лет со дня демонстрации А.С. Поповым первого радиоприемника и в условиях принципиального расширения клиентской базы за счет механизмов, конструкций, биомасс и т.д., а также очевидной необходимости разработки в будущем сетей, например, для биороботов [149], возникает задача по созданию сетей, в которых передача информации может осуществляться иными способами, например, с помощью перемещения вещества. Подобные сети получили название наносетей [69]. Определим наносеть в терминах телекоммуникаций следующим образом. Наносеть является

самоорганизующейся сетью, в которой в качестве узлов сети используются наномашины, а информация и сигнализация могут быть переданы, в том числе и путем перемещения вещества.

Наномашина – устройство, состоящее из компонентов наноуровня, способное выполнять специфические задачи на наноуровне, такие как телекоммуникации, вычисление, хранение данных, измерения (сенсоры) и/или воздействия (актуаторы). Определение приведено в соответствии с фундаментальной работой [69]. Примером наномашины может являться клетка, которая в своей структуре повторяет микроробот (или наоборот), что приведено на рис. 11.1 и соответствует рисунку из [69].



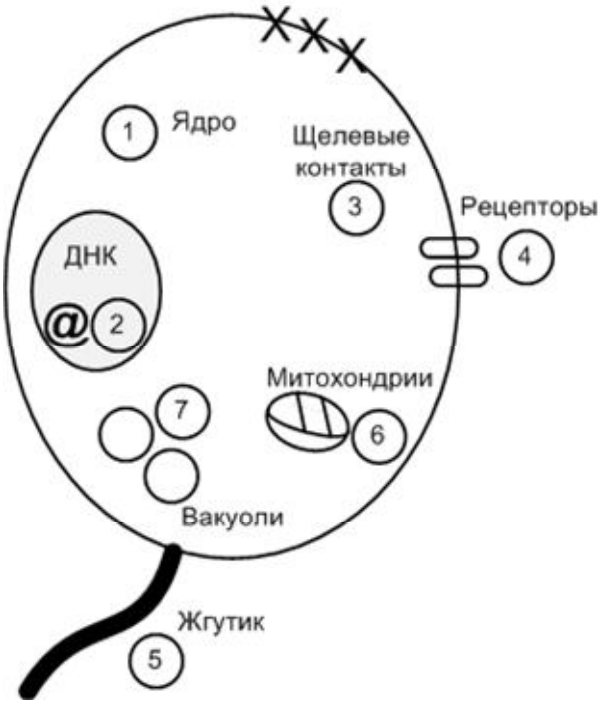


Рис.11.1. Структуры микроробота и клетки.

В классификации наносетей в настоящее время выделяются наносети, в которых информация передается с помощью электромагнитных волн, и наносети, в которых информация передается путем перемещения вещества (молекулярные наносети).

11.2. Молекулярные наносети.

Как уже отмечалось выше, передача информации в таких наносетях может осуществляться путем перемещения вещества.

Молекулярные наносети в настоящее время классифицируются следующим образом [64]:

- наносети, в которых информация передается на расстояния в нано- и микрометры,

- наносети, в которых информация передается на расстояния в микро- и миллиметры,

- наносети, в которых информация передается на метры и более.

В первом случае для передачи информации исследуются возможности положительных ионов кальция. Вторая группа молекулярных наносетей характеризуется использованием для передачи информации, например, жгутиковых бактерий. Для третьей же группы предусматривается проведение исследований по передаче информации с помощью феромонов, пыльцы и спор растений, трансдукции (сенсорного преобразования) света.

Нам представляется, что наиболее реальные возможности имеют молекулярные наносети, построенные на основе передачи информации с помощью феромонов, что предложено в [69]. Использование феромонов потенциально позволяет передавать информацию на сотни метров и километры.

В соответствии с определением [134] феромоны – вещества, вырабатываемые и выделяемые в окружающую среду живыми организмами и вызывающие специфическую ответную реакцию (характерное поведение или процесс развития у воспринимающих их особей того же биологического вида).

Феромоны классифицируются на релизеры и праймеры [17]. Релизерами называются феромоны, которые запускают определенную поведенческую реакцию, а праймерами – те, которые изменяют физиологическое состояние особи. Релизеры в свою очередь подразделяются на аттрактанты (феромоны аггрегации), репелленты (феромоны отпугивания), арестанты (феромоны останавливающие), стимулянты (феромоны

активности), детерренты (феромоны тормозящие реакцию). Такая классификация феромонов позволяет принципиально реализовать на их основе функции по созданию кластеров по аналогии с беспроводными сенсорными сетями. На рис. 11.2 в качестве примера приведены экранные формы по формированию кластеров в беспроводных сенсорных сетях, детально рассмотренные в главах, посвященных алгоритмам выбора головного узла в сенсорных сетях.

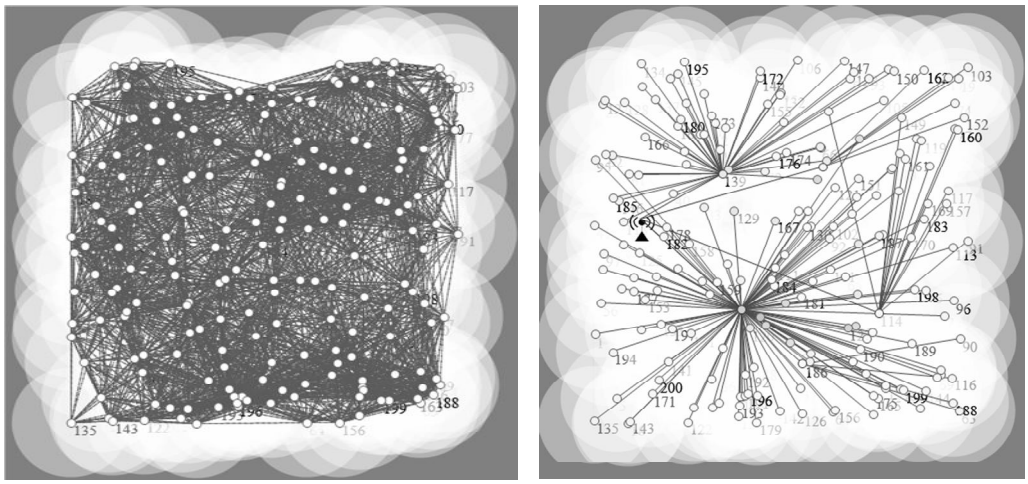


Рис.11.2. Пример формирования кластера в беспроводных сенсорных сетях.

Аттрактанты могут быть использованы для формирования кластера вокруг определенного головного узла, репелленты при ротации головного узла кластера, арестанты при фиксации кластера, стимулянты для передачи информации и детерренты при переходе члена кластера в спящий режим.

Отметим также, что под названием феромоны объединяется достаточно большое число спиртов, углеводородов и иных

химических соединений, обладающих низкой температурой кипения и, соответственно, свойством летучести. Однако, не все летучие спирты, углеводороды и т.п. подпадают под определение феромонов. Действительно, биологические виды используют в качестве феромонов вполне определенные летучие вещества и хотя их количество велико, это не означает, что в качестве феромонов могут быть использованы, например, все спирты. С другой стороны, сказанное не означает, что эти вещества, не отнесенные к феромонам, нельзя использовать для передачи информации. В дальнейшем с целью локализации задачи по передаче информации с помощью перемещения вещества такие химические соединения будем называть псевдоферомонами.

Далее классифицируем возможные виды связи для наносетей с использованием феромонов для передачи информации. Классификация приведена в таблице 11.1.

Таблица 11.1. Классификация видов связи.

Передатчик	**Приемник**
Живой организм	Живой организм
Синтезированный феромон	Живой организм
Живой организм	Искусственный приемник
Синтезированный феромон	Искусственный приемник

Наиболее сложной является задача по созданию искусственного приемника. Задачи синтеза для феромонов во многом решены, чему посвящён следующий раздел главы.

11.3. Синтез феромонов.

К настоящему времени синтезированы уже сотни феромонов. Наиболее успешно развиваются исследования аттрактантов – половых феромонов насекомых. Реакция некоторых насекомых на молекулы феромонов в чрезвычайно низких концентрациях (наноконцентрациях) представляет собой пример одного из наиболее высокочувствительных эффектов, известных науке в настоящее время. Следует подчеркнуть, что действие феромонов могут ощущать особи, находящиеся на расстоянии даже нескольких десятков километров друг от друга. Первый из феромонов, структура которого была установлена – бомбикол (10-транс, 12-цис-гексадиен-1-ол) – половой аттрактант самок тутового шелкопряда Bombix mori [14]. Для запуска специфических реакций в организме насекомого (поведенческих, физиологических, биохимических и т.д.) предельная концентрация бомбикола в воздухе составляет всего 10-12 мкг/мл, а для возбуждения рецепторной клетки на антенне особи достаточно одной молекулы вещества.

Процесс идентификации феромонов повлек за собой разработку ювелирных методов их выделения. Современные методы хроматографии, масс-спектрометрии, ядерномагнитного резонанса позволяют анализировать даже нанограммы вещества, полученные от одной особи. Последнее дает основания полагать, что при соответствующем технологическом прогрессе приемники феромонов могли бы быть реализованы и на упомянутых технологиях. Феромоны могут быть как индивидуальными

соединениями, так и представлять собой смесь основного вещества, преобладающего по массе, с минорными компонентами. Большинство идентифицированных феромонов относятся к относительно простым классам органических соединений: насыщенные и ненасыщенные углеводороды, альдегиды, кетоны, спирты, жирные кислоты, сложные эфиры и некоторые другие. У высших чешуекрылых (Ditrysia) углеродные цепи молекул феромонов не разветвлены и содержат 12-18 атомов углерода (бомбикол). Некоторые виды продуцируют ненасыщенные углеводороды и их эпоксиды (например, 7,8-цис-эпокси-2-метилоктадекан - диспарлюр – половой аттрактант непарного шелкопряда Porthetria dispar). У примитивных чешуекрылых – бабочек березовых молей (Eriocranioidea) феромоны представлены структурами с числом атомов углерода менее 10 [7].

Несмотря на кажущуюся простоту указанных веществ, для варьирования различных запахов насекомые используют также структурные и пространственные (оптические) изомеры веществ. Кроме того, для распознавания сигнала среди других многообразных природных запахов применяются определенные соотношения между количеством как отдельных изомеров, так и между основным и минорными компонентами в смеси. Молекулы феромонов имеют низкие температуры кипения и поэтому обладают высокой летучестью.

С помощью феромонов может осуществляться коммуникация (обмен информацией) насекомых, находящихся даже на

значительном расстоянии друг от друга. Приведем лишь некоторые конкретные примеры такой коммуникации [7,14,17].

Особый тип феромонов – вещества агрегации. При роении и других видах агрегации вместе собираются особи одного пола. Особенно широко агрегационное поведение распространяется у жуков короедов (Ips paraconfusus). Связано это с тем, что для успешной атаки на дерево необходимо массовое заселение, способное ослабить растение хозяина и дать возможность потомству развиваться при пониженном стволовом давлении. В противном случае выделяющаяся смола залепляет ходы и убивает личинок. Короеды обычно используют смесь нескольких веществ, взаимно усиливающих свое действие в присутствии друг друга (синергизм). Эти соединения чаще всего относятся к классу терпенов и их производных (терпеноиды). Иногда в качестве веществ агрегации используются производные жирных кислот. Так, сигналом скопления жуков Trogoderma sp. является смесь этиловых эфиров пальмитиновой, линолевой, олеиновой и стеариновой кислот.

Известны также феромоны, с помощью которых насекомые могут метить свой корм и пути, ведущие к нему. Например, пчелы рода Trigona для этой цели используют смесь, в состав которой входят изомеры цитраля (нераль и гераниаль) и гептан-2-ол. Последний служит также феромоном тревоги у данного вида.

Многие насекомые, образующие семьи или скопления (термиты, тли, клопы, муравьи, пчелы, осы), выделяют химические

вещества, предназначенные для оповещения членов группы об опасности (феромоны тревоги). В результате насекомые либо рассеиваются, либо оказывают сопротивление хищнику. Когда опасность миновала, феромонное вещество улетучивается, прекращая оказывать возбуждающее действие. У муравьев в качестве феромона тревоги может выступать гераниаль и другие терпеноиды.

Некоторые феромоны могут одновременно служить как сигналом тревоги, так и средством защиты. Медоносные пчелы при ужаливании вводят смесь изоамилацетата, изамилбутирата и изоамилпропионата вместе с ядом. Характерный запах привлекает других пчел и побуждает их жалить примерно в то же место, отмеченное феромонным запахом.

У муравьев и термитов для разметки территории и прокладки дорог в качестве «указателя» используются органические кислоты, спирты и терпены. Муравьи могут распознавать свой следовой феромон в концентрации 0.08 пг/см, т.е. 1 мг следового феромона при оптимальном распределении хватило бы на «разметку» тропы длиной 120 тыс. км.

У двукрылых, чешуекрылых и некоторых жуков существуют феромоны метки (маркеры), в частности, детерренты откладки яиц, которыми самка насекомых метит или само яйцо, или субстрат, на который оно отложено. Это позволяет избежать повторной откладки яиц в этом же месте и не допустить перенаселенности данного участка после вылупления личинок.

В ряде случаев феромоны из нескольких компонентов содержат основное вещество, представляющее собой полифункциональное соединение, которое одновременно является и релизером, и праймером. Примером может служить выделяемое пчелиной маткой «царское вещество» (9-кето-2-трансдеценовая кислота).

Существуют феромоны, содержащие олеиновую кислоту, которые способны стимулировать вынос из гнезд разлагающихся остатков, в том числе умерших особей своих сородичей. Муравьи, испачканные этим феромоном, воспринимаются другими рабочими особями, как мертвые, и их «выносят», несмотря на их активное сопротивление.

Применение синтетических половых феромонов находит широкое распространение в развитых странах Европы, в США, Японии в защите лесов, садов, виноградников и хлопчатника. Получили развитие 3 основных направления применения феромонов в защите растений: отлов самцов в ловушки с целью мониторинга, массовый отлов самцов с целью снижения численности популяции и дезориентация самцов с целью прерывания половой коммуникации насекомых. Это позволяет сократить расходы на защиту от насекомых-вредителей в 2-3 раза. Их низкая токсичность, предельно малый расход (1 мг на ловушку), а также широкий перечень (около 2300) различных видов насекомых-вредителей лесного и сельского хозяйства обеспечивает абсолютное преимущество данного подхода, по сравнению с

традиционными способами борьбы с насекомыми-вредителями с использованием пестицидов [2,55].

Как видим, реализация видов связи синтезированный феромон – живой организм имеет достаточно широкое применение. Сам по себе синтез феромонов позволяет получать вещества, идентичные по составу и строению природным феромонам. Однако, производство феромонов требует развитой технологической базы, дорогостоящего оборудования, высокой культуры производства, высококвалифицированных специалистов-химиков. Известные в настоящее время методы тонкого органического синтеза, используемые для получения феромонов, многостадийны (8-9 стадий). Кроме того, дороги исходные соединения и реагенты, что приводит к высокой себестоимости веществ. В настоящее время появились новейшие разработки как российских, так и зарубежных исследователей, которые предлагают прогрессивные методики синтеза феромонов, позволяющие сократить число стадий и таким образом снизить стоимость целевого продукта [2,18,187].

Итак, синтез феромонов продвигается по пути уменьшения стоимости конкретных веществ и расширения их спектра. Что же касается создания пригодного к достаточно широкому использованию приемника феромонов или псевдоферомонов, то здесь имеет место двойственная задача: либо выделить определенные феромоны и/ или псевдоферомоны и разрабатывать искусственный приемних под них, либо разрабатывать некий универсальный приемник, настаиваемый впоследствии на определение тех или иных феромонов или псевдоферомонов. Обе

задачи нетривиальны, но их решение позволит дополнить существующие сети связи дополнительными ресурсами.

11.4. Приложения наносетей.

В соответствии с классификацией видов связей возможны достаточно широкие приложения наносетей. Как показано выше, приложения наносети вида “ синтезированный феромон - живой организм ” уже широко используются, например, в борьбе с сельскохозяйственными вредителями. Представляется, что в обозримом будущем наносети вида «синтезированный феромон - искусственный приемник» после создания такого приемника также могут найти широкое применение для следующих приложений:

- чрезвычайные ситуации, например, с целью локализации пострадавших,
- мониторинг окружающей среды, сельскохозяйственных угодий,
- охранные системы, например, при отсутствии возможностей по стабильному энергоснабжению.

Наносети рассмотрены в разрезе возможного создания на основе перемещения вещества, например, феромонов или псевдоферомонов, сетей связи с дальностью передачи информации на сотни метров и километры. Это направление научных исследований находится на стыке биохимии и информационных технологий и может стать одним из наиболее значимых и в то же время прагматичных уже в ближайшие 5-10 лет. Важнейшей

задачей при этом является создание искусственного приемника феромонов и псевдоферомонов.

Сокращения

ABRO	Authoritative Border	Надежный пограничный маршрутизатор
ACK	Acknowledgement	Подтверждение
ACL	Asynchronous Connection Oriented Link	Логический транспорт, ориентированный на соединение (IEEE 802.15.1)
ACL	Access Control Link	Список контроля доступа (IEE 802.15.4)
AES-128	Advanced Encryption Standard	Улучшенный стандарт алгоритма шифрования
Ad hoc	For this purpose	Целевая сеть
APS	Asynchronous Power Save	Режим асинхронного сохранения энергии (IEEE 802.15.3)
APS	Application support (sublayer)	Подуровень поддержки приложений для протокола ZigBee
ARO	Address Registration Option	Опция регистрации адреса в протоколе 6LoWPAN
ARQ	Automatic Repeat request	Механизм контроля ошибок при передаче данных
ASB	Active Slave Broadcast	Активный управляемый широковещательный логический транспорт
ATP	Association Time Out	Период ассоциативного

	Period	тайм-аута
BAN	Body Area Network	Нательная сеть
BNC	BAN Network Controller	Сетевой контроллер в нательных сетях
BSS	Basic Service Set	Базовый набор услуг
CAC	Channel access Code	Код доступа к каналу
CAP	Contention Access Period	Период конкурентного доступа
CAZAC	Constant-Amplitude Zero Autocorrelation	Последовательность с постоянной амплитудой и нулевой автокорреляцией
CCA	Clear Channel Assessment	Оценка чистоты канала
CCP	Coverage Configuration Protocol	Протокол конфигурирования покрытия
CDMA	Code Division Multiple Access	Множественный доступ с кодовым разделением
CH	Cluster Head	Головной узел кластера
CHS	Cluster Head Selection	Алгоритм выбора головного узла
CHL	Cluster Head List	Перечень головных узлов
CHSC	Cluster Head Selection for Coverage	Алгоритм выбора головного узла кластера для решения задач покрытия
CFP	Contention Free Period	Период без конкуренции
CID	Channel Identifier	Идентификатор канала
CID	Context Identifier	Идентификатор контекста в

		6LoWPAN
CLKN	Clock Native	Встроенный таймер
CP	Contention Period	Период конкуренции
CPC	Check Perimeter Coverage	Алгоритм периметрического покрытия
CRC	Cyclic Redundancy Check	Циклический избыточный код
CSC	Cluster Head Selection for Coverage	Алгоритм покрытия для гетерогенной сенсорной сети
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance	Множественный доступ с детектированием несущей и предупреждением коллизий
CSS	Chirp Spread Spectrum	Линейная частотная модуляция с расширенным спектром
CTA	Channel Time Allocation	Занятость канального интервала
CTAP	Channel Time Allocation Period	Период занятости канального интервала
CW	Contention Window	Окно конкуренции
DAC	Destination Address Compression	Сжатие адреса назначения в 6LoWPAN
DAD	Duplicate Address Detection	Определение дублирующего адреса в 6LoWPAN
DAM	Destination Address Mode	Режим сжатия адреса

		назначения в 6LoWPAN
DBPSK	Differentiated Binary Phase-shift Keying	Дифференциальная бинарная фазовая манипуляция
DCA	Distributed Clustering Algorithm	Распределенный кластерный алгоритм
DCF	Distributed Coordination Function	Функция распределенного доступа к среде передачи
DD	Direct Diffusion	Протокол маршрутизации для одноуровневой сенсорной сети (прямое распространение)
DEV	Device	Устройство сети пиконет в стандарте IEEE 802.15.3
DEVID	DEVice IDentifier	Идентификатор устройства сети пиконет
DIFS	Distributed Inter Frame Space	Распределенный межкадровый интервал
DME	Device Management Entity	Объект управления устройством (IEEE 802.15.3)
DQPSK	Differential Quadrature Phase-shift Keying	Дифференциальная квадратурная фазовая манипуляция
DS	Differentiated Services	Поле «тип услуги» заголовка IP пакета в терминах DiffServ
DSCP	Differentiated Services	Значение поля DS

	Code Points	
DSN	Distributed Service Networks	Сети распределенного обслуживания
DSPS	Device Synchronized Power Save	Режим синхронизированного сохранения энергии
DSSS	Direct Sequence Spread Spectrum	Широкополосная модуляция с прямым расширением спектра
D8PSK	Differential 8-Phase-Shift Keying	Дифференциальная восьмипозиционная фазовая манипуляция
EAP 1	Exclusive Access Phase 1	Фаза эксклюзивного доступа 1
EAP 2	Exclusive Access Phase 2	Фаза эксклюзивного доступа 2
ED	Energy Detection	Обнаружение сигнала
EFC	Electrostatic Field Communication	Связь через электростатическое поле
EIFS	Extended Inter Frame Set	Расширенный межкадровый доступ к каналу
ERA	Energy Residue Aware	Алгоритм осведомленности об остаточной энергии
eSCO	extended Synchronous Connection Oriented	Расширенный синхронный логический транспорт, ориентированный на соединение

EUI-64	Extended Unique Identifier	Расширенный уникальный идентификатор
FCS	Frame Check Sequence	Проверочная последовательность кода
FEC	Forward Error Correction	Прямая коррекция ошибок
FFD	Full Function Device	Полнофункциональное устройство
FHSS	Frequency Hopping Spread Spectrum	Расширение спектра с перескоком частоты
FPCN	Full Perimeter Coverage Nodes	Алгоритм полного периметрического покрытия
GAP	Generic Access Profile	Общий профиль доступа
GMSK	Gaussian Minimum Shift Keying	Гауссовская манипуляция с минимальным частотным сдвигом
GPS	Global Positioning System	Глобальная система позиционирования
GTK	Group Temporary Key	Групповой временный ключ
GTS	Guaranteed Time Slot	Гарантированный временной интервал (IEEE 802.15.4)
HANET	Home Ad Hoc Network	Муниципальная (домашняя) целевая сеть
HBC	Human Body Communication	Уровень связи человеческого тела
HCI	Host Controller Interface	Интерфейс между хостом и

		контроллером
HEC	Header Error Correction	Коррекция ошибок в заголовке
HEED	Hybrid Energy Distribution	Гибридный алгоритм выбора головного узла в кластере
HLIM	Hope Limit	Флаг ограничения количества передач
HP	Hybrid Predictor	Гибридный предиктор
HSPA	High Speed Packet Access	Высокоскоростной пакетный доступ
IAC	Inquiry Access Code	Код запроса доступа
IBSS	Independent Basic Service Set	Независимый базовый набор услуг
IEEE	Institute of Electrical and Electronics Engineers	Институт инженеров в области электротехники и электроники
IETF	Internet Engineering Task Force	Группа специалистов Интернет по инженерным задачам
IMS	Internet Multimedia Subsystem	Мультимедийная IP подсистема
IoT	Internet of Things	Интернет вещей
IPTV	Internet Protocol Television	IP-телевидение
ISM	Industrial, Scientific and Medical	Частоты для промышленных, научных и медицинских целей

LCP	Link Control Protocol	Протокол управления соединением (звеном)
LEACH	Low Energy Adaptation Cluster Hierarchy	Иерархический алгоритм выбора головного узла кластера с низким потреблением энергии
LEACH-M	LEACH for mobile	Алгоритм LEACH для мобильных сенсорных сетей
LEP	Linear Extrapolation Predictor	Линейный экстраполяционный предиктор
LLID	Logical Link Identifier	Идентификатор логического соединения (звена)
LM	Link Manager	Администратор соединения (звена)
LMP	Link Manager Protocol	Протокол администрирования соединения (звена)
LQI	Link Quality Indicator	Индикатор качества соединения
LOWPAN HC1	LOWPAN Header Compression 1	Алгоритм сжатия заголовка 1 для 6LoWPAN
LOWPAN HC2	LOWPAN Header Compression 2	Алгоритм сжатия заголовка 2 для 6LoWPAN
LOWPAN IPHC	LOWPAN IPv6 Header Compression	Алгоритм сжатия заголовка для датаграмм IPv6
LR-WPAN	Low Rate Wireless Personal	Низкоскоростная

	Area Network	беспроводная персональная сеть
LTE	Long Term Evolution	Сети долговременной эволюции
LT_ADDR	Logical Transport Address	Идентификатор адреса логического транспорта
L2CAP	Logical Link Control and Adaptation Protocol	Протокол управления и адаптации логического соединения (звена)
MAC	Media Access Control	Протокол доступа к среде передачи
MANET	Mobile Ad hoc Network	Целевая мобильная сеть
MBAN	Medicine Body Area Network	Нательная сеть для медицинских целей
MCTA	Management Channel Time Allocation	Администрирование занятости канального интервала
MIC	Message Integrity Code	Код целостности сообщения
MICS	Medical Implant Communication Services	Услуги связи для медицинских имплантатов
MK	Master Key	Мастер-ключ
MLME	MAC Sub layer Management Entity	Объект управления подуровнем MAC
MOC	Machine Oriented Communications	Сети связи следующего поколения, модернизированные до уровня поддержки связи

		между устройствами
MSN	Mobile Sensor Network	Мобильная сенсорная сеть
M	Multicast (compression)	Сжатие мультикастингового адреса в 6LoWPAN
M2M	Machine-to-Machine	Сети устройство-устройство
NAV	Network Allocation Vector	Вектор резервирования сети
NAT	Network Address Translation	Преобразование сетевых адресов
NB	Narrowband	Узкополосный
NH	Next Header	Флаг следующего заголовка в 6LoWPAN
NGN	Next Generation Network	Сети связи следующего поколения
NS/NA	Neighbor Solicitation/Neighbor Advertisement	Сообщения запроса и уведомления о ближайших (соседних) узлах в 6LoWPAN
NUD	Neighbor Unreachability Detection	Обнаружение недоступности соседнего узла в 6LoWpan
NWK	Network (layer)	Сетевой уровень для ZigBee
OSI	Open System Interconnection	Модель взаимодействия открытых систем
PAN	Personal Area Network	Персональная сеть
PCC	Predicted combined Criterion	Комбинированный критерий прогнозирования
PCF	Point Coordination	Функция централизованного

	Function	доступа к среде передачи
PEGASIS	Power Efficient Gathering Sensor Information System	Энергоэффективная система (алгоритм) сбора информации о состоянии сенсоров
PDU	Protocol Data Unit	Протокольный блок данных
PHR	PHY Header	Заголовок физического уровня
PIO	Prefix Information Option	Опция префиксной информации в 6LoWPAN
PLCP	Physical Layer Convergence Protocol	Протокол подуровня конвергенции физического уровня
PLME	PHY Layer Management Entity	Объект управления физическим уровнем
PNC	Piconet Coordinator	Координатор пикосети
PNID	Piconet Identifier	Идентификатор пикосети
POI	Points of Interest	Группа по интересам в сети VANET
POS	Personal Operating Space	Персональное рабочее пространство
PSB	Packet Slave Broadcast	Закрепленный управляемый широковещательный логический транспорт
PSD	Power Spectral Density	Плотность спектральной мощности

PSPS	Piconet Synchronized Power Save	Режим синхронизированного сохранения энергии пикосети
PTK	Pairwise Temporary Key	Парный временный ключ
P2P	Peer-to-peer	Соединения «равный с равным»
RA	Router Advertisement	Уведомление от маршрутизатора в 6LoWPAN
RAP1	Random Access Phase 1	Фаза случайного доступа 1
RAP2	Random Access Phase 2	Фаза случайного доступа 2
RFD	Reduced Function Device	Устройство с ограниченными функциями
RFID	Radio Frequency Identification	Радиочастотная идентификация
RRCH	Round-Robin Cluster Head	Алгоритм циклической очередности выбора головного узла
RS	Router Solicitation	Запрос маршрутизатора
RSS	Received Signal Strength	Мощность принимаемого сигнала
RTS/CTS	Request to Send/Clear to Send	Механизм обмена информацией в IEEE 802.11x
QoS	Quality of Service	Качество обслуживания

SAC	Source Address Compression	Сжатие адреса источника
SAM	Source Address Mode	Режим сжатия адреса источника
SAP	Service Access Point	Точка доступа к услугам
SCO	Synchronous Connection Oriented	Логический транспорт, ориентированный на соединение
SDU	Service Data Unit	Сервисный блок данных
SFD	Start Frame Delimiter	Разделитель начала кадра
SHR	Synchronization Header	Заголовок синхронизации
SIFS	Short Inter Frame Space	Короткий межкадровый интервал
SIP	Session Initiation Protocol	Протокол инициирования сеанса связи
SPIN	Sensor Protocol for Information via Negotiation	Протокол маршрутизации в одноуровневой сенсорной сети
SPP	Single Point Predictor	Просто точечный предиктор
SSW	SoftSwitch	Программный коммутатор
SUN	Smart Ubiquitous Network	Умная всепроникающая сеть
TF	Traffic Flow	Класс нагрузки и метка потока в 6LoWPAN
VANET	Vehicular Ad hoc Network	Целевая сеть для транспортных средств
VoIP	Voice over IP	Технология передачи речи в

		сетях IP
V2I	Vehicle to Infrastructure	Сеть между транспортными средствами и инфраструктурной сетью
V2H	Vehicular to Home	Сеть между транспортными средствами и домом
V2G	Vehicular to Grid	Сеть между транспортными средствами и вычислительными ресурсами
V2V	Vehicle to Vehicle	Сеть между транспортными средствами
USN	Ubiquitous Sensor Networks	Всепроникающие сенсорные сети
UWB	Ultra Wide Band	Сверхширокополосная беспроводная технология
WBAN	Wireless Body Area Network	Беспроводная нательная сеть
WiFi	Wireless Fidelity	Высокоточная беспроводная система
WiMax	Worldwide Interoperability for Microwawe Access	Совместимый во всем мире беспроводный доступ
Wi Media	Wireless Media Alliance	Альянс беспроводной среды
WLAN	Wireless Local Area Network	Беспроводная локальная сеть
WMAN	Wireless Metropolitan Area Network	Беспроводная местная сеть

WMTS	Wireless Medical Telemetry Services	Беспроводные услуги для медицинской телеметрии
WNSN	Wireless Nano Sensor Network	Беспроводная наносенсорная сеть
WoT	Web of Things	Вэб вещей
WPAN	Wireless Personal Area Network	Беспроводная персональная сеть
WSN	Wireless Sensors Network	Беспроводная сенсорная сеть
ZDO	ZigBee Device Object	Объект ZigBee устройства
6LoWPAN	Low Energy IPv6 Protocol for WPAN	Протокол, поддерживающий IPv6 с низким потреблением энергии для беспроводных персональных сетей
6LBR	6LoWPAN Border Router	Пограничный маршрутизатор в сети 6LoWPAN
6LR	6LoWPAN Router	Маршрутизатор в сети 6LoWPAN
6CO	6LoWPAN Context Option	Опция контекста в 6LoWPAN

Литература.

1. А.В.Анисимов, С.Д.Андреев, А.М.Тюрликов. Управление энергоэффективной доставкой информации на абонентскую станцию. Электросвязь, №4, 2011.
2. В. Быков, Е. Финкельштейн. Российские феромоны для спасения урожая. The Chemical Journal, N 11, 2009. С. 38-41.
3. Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский, Сети связи. Учебник для ВУЗов. BHV, С. Петербург, 2010.
4. Б.С.Гольдштейн, В.Ю.Гойхман, Ю.В.Столповская. Сети NGN. Оборудование IMS. Учебное пособие. “Теледом”, ГОУВПО СПбГУТ, 2010.
5. А.Б. Васильев, Д.В. Андреев, Д.В. Тарасов, А.Е. Кучерявый. Тестирование технических средств NGN. М., ЦНИИС, 2008.
6. А.Б. Васильев, С.П. Соловьёв, А.Е. Кучерявый. Системно-сетевые решения по внедрению технологии NGN на Российских сетях связи. Электросвязь, № 3, 2005.
7. Введение в биохимическую экологию. Москва: Изд-во Московского университета, 1986.
8. Г.В. Вемян. Передача речи по сетям электросвязи. М. Радио и связь, 1985.
9. Е.С. Вентцель, Л.А. Овчаров. Теория случайных процессов и ее инженерные приложения. М., «Высшая школа», 2000 г.
10. В.И.Воробьев, В.Г.Грибунин. Теория и практика вейвлет-преобразования. Военный Университет Связи, 1999.

11. А.И. Витченко, Ф. Доленц, А.Е. Кучерявый, Л.З. Гильченок. Опытная зона сети с пакетной коммутацией на ОАО «Ленсвязь». Всероссийская конференция «Сети связи следующего поколения». Сборник трудов, Санкт-Петербург, 25-27 февраля, 2003 г.
12. А.Н. Голубев, А.Е. Кучерявый, А.С. Миков. Системы коммутации в конце XX – начале XXI века. Проблемы разработки, внедрения и эксплуатации цифровых систем коммутации. Семинар РНТОРЭС, Пермь, 21-23 апреля, 1997.
13. А.Я. Городецкий, В.С. Заборовский. Информатика. Фрактальные процессы в компьютерных сетях. Учебное пособие. Издательство СПбГТУ, Санкт-Петербург, 2000 г.
14. М. Гудман, Ф. Морхауз. Органические молекулы в действии. Москва: Мир, 1977.
15. И.М. Жданов, Е.И. Кучерявый. Построение городских телефонных сетей. Связь, М., 1972.
16. И.А. Зюльков. Самоподобные свойства трафика систем с повторными вызовами. Воронежский государственный университет, Вестник ВГУ, Серия физика, математика, 2002, №1.
17. В.Д.Иванов. Феромоны насекомых. Соросовский образовательный журнал, №6, 1998.
18. Г.Ю. Ишмуратов, М.П. Яковлева, А.Х. Шаяхметова и др. Асимметрическое эпоксидирование и дигидроксилирование олефинов в синтезе феромонов насекомых. Химия растительного сырья. N 3, 2008. С. 5-32.

19. Р. Кох, Г.Г. Яновский. Эволюция и конвергенция в электросвязи. М., Радио и связь, 2001.
20. А.Е. Кучерявый. Конвергенция сетей связи как основа функциональной архитектуры систем коммутации. Forum International Telecommunication Academy'98. Proceedings, Moscow, April 14-16, 1998.
21. А.Е. Кучерявый. Конвергенция сетей связи и внедрение современных услуг телекоммуникаций. Научно-практический семинар «Проблемы разработки, внедрения и эксплуатации цифровых систем коммутации». НТОРЭС им. А.С. Попова, Воронеж, 1999.
22. А.Е. Кучерявый. Конвергенция сети Интернет и сетей связи общего пользования. Конференция АДЭ «Развитие российского сегмента сети Интернет». Москва, 6-8 октября, 1999.
23. А.Е. Кучерявый, А.Л. Цуприков, Ф. Доленц, И.Г. Мазин. Некоторые аспекты конвергенции сетей ТфОП/ЦСИС и IP. Вестник связи, №4, 2000
24. А.Е. Кучерявый, З.Б. Ревелова, А.И. Парамонов. Реструктуризация трафика сетей связи и новые подходы к прогнозированию их развития. «Электросвязь», №2, 2003.
25. А.Е. Кучерявый, Л.З. Гильченок, А.Ю. Иванов. Пакетная сеть связи общего пользования. «Наука и техника», С.-Петербург, 2004.

26. А.Е. Кучерявый, Е.А.. Кучерявый. От е-России к u-России: тенденции развития электросвязи. «Электросвязь», №5, 2005.
27. А.Е. Кучерявый, Е.А. Кучерявый, А.И. Парамонов. От е-России к u-России. Сенсорные сети. 5-я Международная конференция по NGN (NGN – 2005), материалы, 23-25 августа, 2005, Н.Новгород.
28. А.Е. Кучерявый, А.Л. Цуприков. Сети связи следующего поколения. Центральный научно-исследовательский институт связи (ЦНИИС), Москва, 2006.
29. А.Е. Кучерявый, Е.А. Кучерявый. На пути к u-России и u-сетям. Международный телекоммуникационный симпозиум «Мультисервисные услуги в высокоскоростных системах мобильной связи». СПб, 27-30 июня, 2006. СПб ГУТ, сборник трудов.
30. А.Е. Кучерявый, А.И. Парамонов. Модели трафика для сенсорных сетей в u-России. «Электросвязь», №6, 2006.
31. А.Е.Кучерявый. Сенсорные сети как перспективное направление развития телекоммуникаций. 59-я Научно-техническая конференция профессорского профессорско-преподавательского состава СПбГУТ им. Бонч-Бруевича, Материалы, 22-26 января, 2007.
32. А.Е. Кучерявый, А.А. Станкевич, А.Ю. Иванов. Протоколы SIP и SIP-T. ГУТ, СПб, учебное пособие, 2005.
33. А.Е. Кучерявый, А.И. Парамонов. Прогнозирование развития сетей 3G в Российской Федерации. 62-я НТК,

посвященная Дню Радио. Труды конференции. Апрель 2007. С.-Петербург, издательство СПб ГЭТУ «ЛЭТИ».

34. А.Е. Кучерявый, А.И. Парамонов, Е.А.Кучерявый, Сети связи общего пользования. Тенденции развития и методы расчёта. ФГУП ЦНИИС, 2008.

35. А.Е. Кучерявый, А. Салим. “Выбор головных узлов в однородной беспроводной сенсорной сети для обеспечения полного покрытия”, 64-я Научно-Техническая Конференция. Апрель 2009 г. стр.106.

36. А.Е. Кучерявый, А. Салим. “ Диаграммы Вороного для Беспроводных Сетей”, 64-я Научно-Техническая Конференция. Апрель 2009 г. стр. 108.

37. А.Е. Кучерявый, А. Салим. “Выбор головного узла кластера в однородной беспроводной сенсорной сети”, Электросвязь, № 8, 2009.

38. А.Е. Кучерявый. Целевые сети. 63-я Научно-техническая конференция, посвященная Дню Радио. Труды конференции. Апрель 2008. С.-Петербург, издательство СПб ГЭТУ «ЛЭТИ».

39. А.Е. Кучерявый. Самоорганизующиеся сети и новые услуги. Электросвязь, №1, 2009.

40. А.Е.Кучерявый. Перспективы реструктуризации клиентской базы операторов электросвязи. 10-й форум Международной Академии Связи. Сборник тезисов, Москва, Экспоцентр, 14 мая 2009г.

41. А.Е.Кучерявый. Самоорганизующиеся сети и новые услуги. 62-я Научно-техническая конференция СПбГУТ, Материалы, 8-12 февраля, 2010г.
42. Е.А. Кучерявый. Управление трафиком и качество обслуживания в сети Интернет. Наука и техника, С.-Петербург, 2004.
43. Е.А. Кучерявый, С.А. Молчан, В.В. Кондратьев. Принципы построения сенсоров и сенсорных сетей. Электросвязь, №6, 2006
44. Б.С. Лившиц, Я.В. Фидлин, А.Д. Харкевич. Теория телефонных и телеграфных сообщений. М., Связь, 1971.
45. Б.С. Лившиц, А.П. Пшеничников, А.Д. Харкевич. Теория телетрафика. М., Связь, 1979 г.
46. Д.А. Молчанов, Е.А. Кучерявый. Приложения беспроводных сенсорных сетей. Электросвязь, №6, 2006.
47. Д.А. Молчанов. Самоорганизующиеся сети и проблемы их построения. Электросвязь, №6, 2006.
48. В.И.Мочалов. Разработка и исследование алгоритмов построения отказоустойчивых сенсорных сетей. Автореферат диссертации на соискание ученой степени кандидата технических наук. МТУСИ, М., 2011.
49. А.И. Парамонов, А.Е. Кучерявый. Миграция речевого трафика в современных сетях связи. Электросвязь, №12, 2007.
50. Ю.В. Семенов. Проектирование сетей связи следующего поколения. Наука и техника, С – Петербург, 2005.

51. Ю.В.Семенов, А.Е.Кучерявый, В.О.Пяттаев. Умные всепроникающие сети. 14 Всероссийский Форум “Развитие телекоммуникаций в России”. Сочи, 26-27 апреля 2011г. Материалы Форума, М., ЗАО “Экспо – Телеком”.
52. Ю.В.Семенов, А.Е.Кучерявый, В.О.Пяттаев. Перспективы развития проводного широкополосного доступа в России. Электросвязь №9, 2011.
53. Д.В. Тарасов, А. И. Парамонов, А.Е.Кучерявый. Особенности видеотрафика для сетей связи следующего поколения. Электросвязь, №2, 2010.
54. В.О.Тихвинский, С.В.Терентьев, А.Б.Юрчук. Сети мобильной связи LTE. Технологии и архитектура. Эко-трендз, 2010.
55. Феромоны насекомых для вредителей российского урожая. Материалы Международного форума по нанотехнологиям, Rusnanotech 2010. Москва, 1-3 ноября 2010.
56. Б.С. Цыбаков. Модель телетрафика на основе самоподобного случайного процесса. М: «Радиотехника», 1999 г., №5.
57. М.А. Шнепс – Шнеппе. Интернет-телефония: протокол SIP и его применение. М., Макс-Пресс, 2002.
58. М.А. Шнепс – Шнеппе. Системы распределения информации. Методы расчета. М., Связь, 1979.
59. Г.Г. Яновский. IP Multimedia subsystem: принципы, стандарты и архитектура. Вестник связи №3, 2006.

60. K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, vol. 3, no. 3, 2005.
61. I. F. Akyildiz, W.Su, Y.Sankarasubramaniam, E. Cayirci. A survey on sensor networks. Communications Magazine, IEEE, vol.40, 2002.
62. I.F. Akyildiz. Key Wireless Networking Technologies in the Next Decade. NEW2AN 2006, St. Petersburg, Russia, June 2006. Keynote Speech.
63. F. Akyildiz, D. Pompili, T. Melodia. Underwater acoustic sensor networks: research challenges. Ad Hoc Networks Journal, Elsevier, Volume 3, Issue 3, May 2005.
64. I.F. Akyildiz. Nano-communications: An Overview. www.n3cat.upc.edu/nanoday/nanoday09-ifa.pdf.
65. I.F. Akyildiz, M.C. Vuran, O.B. Akan, W. Su. Wireless Sensor Networks: A Survey revisited. Computer Networks Journal, 2005.
66. I.F. Akyildiz. Key Wireless Networks Technologies in the Next Decade. WWIC 2005 Keynote Speech, Xanthi, Greece, May 2005.
67. I.F. Akyildiz, X. Wang, W. Wang. Wireless mesh networks: a survey. Computer Networks and ISDN Systems, v.47, №4, March 2005.
68. I.F.Akyldiz. Spectrum management in Cognitive Radio Networks. IEEE WiMob 2008 Conference. Proceedings. Avignon, France, 12-14 October, 2008.

69. I.F. Akyildiz at all. Nanonetworks: A new communication paradigm. Computer Networks, Elsevier, 2008.

70. I.F.Akyildiz, J.M.Jornet. The Internet of Nano-Things. IEEE Wireless Communications. December 2010, V.17, № 6.

71. J. N. Al-Karaki and A. E. Kamal. Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications Magazine, vol. 11, no. 6, 2004.

72. A. Ananda, Mun Choon Chan, Wei Tsang Ooi. Mobile Wireless and Sensor Networks Technology Applications and Future Directions. John Wiley & Sons; 2006.

73. L. M. Arboleda, N. Nasser. Comparison of Clustering Algorithms and Protocols for Wireless Sensor Networks. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Ottawa, May 2006.

74. F. Aurenhammer. Voronoi diagrams . A survey of a fundamental data structure. ACM Computing Surveys, 23 (3), September, 1991.

75. P. Bose, P. Morin, I. Stojmenovic, J. Urrutia. Routing with guaranteed delivery in ad hoc wireless networks. Wireless Networks, vol. 7, no. 6, 2001.

76. R.Birke, M.Mellia, M.Petracca, D.Rossi. Experience of VoIP. Traffic Monitoring in a Commercial ISP. International Journal of Network Management, vol.20, Issue 5, 2010.

77. E. H. Callaway. Wireless Sensor Networks: Architectures and Protocols. CRC Press, 2004.

78. B. Carbunar, A. Grama, J. Vitek. Redundancy and Coverage Detection in Sensor Networks. ACM Transactions on Sensor Networks, vol. 2, no. 1, 2006.

79. M. Chatterjee et al. WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks. Journal of Cluster Computing, V. 5/2, April, 2002.

80. S. Cheekiralla. Wireless Sensor Network-Based Tunnel Monitoring. REALWSN 2005, June 20 – 21, SICS, Sweden.

81. B. Chen, K. Jamieson, H. Balakrishnan, R. Morris. Span: an energy efficient coordination algorithm for topology maintenance in ad hoc wireless networks. Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, 2001.

82. H. Chen, C. S. Wu, Y. S. Chu, C. C. Cheng, and L. K. Tsai. Energy residue aware (ERA) clustering algorithm for leach-based wireless sensor networks. 2nd Int. Conf. Systems and Networks Communications (ICSNC), Proceedings, Cap Esterel, French Riviera, France, Aug. 2007.

83. C.-Y. Chong, S.P. Kumar. Sensor Networks: Evolution, Opportunities and Challenges. Proceedings of the IEEE, vol. 91, issue 8, August 2003.

84. C.Y. Chong, S. Mori, K. C. Chang. Distributed tracking in distributed sensor networks. American Control Conference, Seattle, WA, 1996.

85. C. D. Cordeiro, and D.P.Agrawal. Ad Hoc and Sensor Networks: Theory and Applications. World Scientific Publishing, MA, May 2006.
86. M.E.Crovella, A.Bestavros. Self-Similarity in Wide Web Traffic: Evidence and Possible Causes. IEEE/ACM Transaction on Networking, Vol 5, Number 6, December, 1997.
87. T. von Deak. The role of remote sensing in disaster management. ITU News, №10, December, 2007.
88. J. Delaney. The Use of SIP in Communication Network. Journal of Communication Network, v.1, p.1, April-June 2002.
89. ECMA-368. Standard High Rate Ultra Wideband PHY and MAC. Standard, December 2005.
90. ETSI TS 102 689. V.1.1.1. Machine – to - Machine Communications (M2M); M2M Service Requirements. August, 2010.
91. V.Garg. Wireless Communications and Networking. Morgan Kaufmann, 2006.
92. Global 3G and 4G Deployment Status HSPA/HSPA+/LTE/. May, 5 2011. Informa Telecom&Media, 4G Americas, Public Announcement. www.4gamericas.org.
93. L.Goleniewski, K. W. Jarrett. Telecommunications Essentials, Second Edition. Addison Wesley, 2006.
94. V.K. Gurbani, R. Jain. Transport Protocol Consideration for Session Initiation Protocol Networks. Bell Labs Technical Journal, №9 (1), 2004.
95. G. Gupta, M. Younis. Load-balanced clustering of wireless sensor networks. IEEE ICC 2003, vol.3, May 2003.

96. T.Janevski. Traffic Analysis and Design of Wireless IP Networks. Artech House.2003.

97. T.Janevski, Z.Vanevski. Statistical Analysis of Multicast versus Instant Channel Changing Unicast IPTV Provisioning. 16th Telecommunications Forum TELFOR 2008, Serbia, Belgrade, November 25-27, 2008.

98. FET: Future and Emerging Technology in Europe. Bio-ITC Convergence. January, 2008. European Commission Information Society and Media/DG-INFSO.

99. L. Frank. Smart Environments: Technologies, Protocols and Applications. John Wiley&Sons, New York, 2005.

100. M. Frodigh, P.Johansson, P. Larsson. Wireless ad hoc networking: the art of networking without a network. Ericsson Review, 2000.

101. M.Heath, A.Brydon, R.Pow. Prospects for the Evolution of 3G and 4G. Analysis, 2006.

102. Hecker M. et al. Smart Sensor Networks: Communication, Collaboration and Business Decision Making in Distributed Complex Enviroment. International Conference in Mobile Business (IC MB'05). Proceedings. Sydney, Australia, 11-13 July, 2005.

103. W. Heinzelman, J. Kulik, H. Balakrishnan. Adaptive protocols for information dissemination in wireless sensor networks. Proceedings, ACM/IEEE 5th International Conference

Mobile Computing and Networking MobiCom. Seattle, Washington, USA, Aug. 1999.

104. W. Heinzelman, A. Chandrakasan, H. Balakrishnan. An application specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications 1 (4), 2002.

105. W. Heinzelman, A. Chandrakasan, H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. Proceedings 33rd Hawaii International Conference on System Sciences (HICSS), Wailea Maui, Hawaii, USA, Jan. 2000.

106. E.Hossain, K.Leung. Wireless Mesh Networks Architectures and Protocols. Springer; 2007

107. Y. T. Hou, Y. Shi, J. Pan. Lifetime-optimal data routing in wireless sensor networks without flow splitting," in Workshop on Broadband Advanced Sensor Networks, San Jose, CA, 2004.

108. T. T. Hsieh. Using sensor networks for highway and traffic applications. IEEE Potentials Volume 23, Issue 2, April-May 2004.

109. H. Huang, A. W. Richa, M. Segal. Dynamic coverage in ad-hoc sensor networks. Mobile Networks and Applications. Springer Science + Business Media, 10, 2005.

110. C. Huang, Y. Tseng. The Coverage Problem in a Wireless Sensor Network. Mobile Networks and Applications, vol. 10, no. 4, Aug. 2005.

111. IEEE 802.1x. Port-Based Network Access Control, 2004

112. IEEE 802.2. LAN/MAN Logic Link Control. 1998.

113. IEEE 802.3. LAN/MAN CSMA/CD Access Method. 2005.

114. IEEE 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 1999.

115. IEEE 802.11a. Higher-Speed Physical Layer in the 5 GHz band. 1999.

116. IEEE 802.11в. Higher-Speed Physical Layer (PHY) Extension in the 2.4 GHz band.1999.

117. IEEE 802.11e. Medium Access Control (MAC) Quality of Service Enhancements. 2005.

118. IEEE 802.11g. Further Higher-Speed Physical Layer Extension in the 2.4 GHz band. 2003.

119. IEEE 802.11n. Enhancements for Higher Throughput. September, 2009.

120. IEEE 802.11s (draft). Extended Service Set Mesh Networking. 2009.

121. IEEE 802.11p. Wireless Access for the Vehicular Environment. July, 2010.

122. IEEE 802.16-2009. Air interface for Fixed and Mobile Broadband Wireless Access Systems. 2009.

123. IEEE 802.16m. Amendement to IEEE 802.16-2009. Advanced Air Interface with Data Rates of 100Mbit/s mobile and 1Gbit/s fixed. 2011.

124. IEEE 802.1q. Virtual LANs. 2006.

125. IEEE 802.1p. Traffic Class Expediting and Dynamic Multicast Filtering. 2006.

126. IEEE 802.15.1-2005 Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs).

127. IEEE 802.15.3-2003 Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs).

128. IEEE 802.15.3b-2005 Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs) Amendment 1: MAC Sub layer.

129. IEEE 802.15.4-2003 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).

130. IEEE 802.15.4a-2007 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 1: Add Alternate PHYs.

131. C. Intanagonwiwat, R. Govindan, D. Estrin. Directed diffusion: A scalable and robust communication paradigm for sensor networks. Proceedings ACM/IEEE 6th International

Conference Mobile Computing and Networking MobiCom. Boston, USA, Aug. 2000.

132. V.B.Iversen. Teletraffic Engineering and Network Planning. Technical University of Denmark. 20, 2010.

133. A. Kansal et al. Sensing uncertainty reduction using low complexity actuation. ACM Information Processing in Sensor Networks (ISPN), April 2004.

134. P.Karlson, M.Luscher. Pheromones: A new term for a class of biologically active substances. Nature, 183. 1959.

135. B.-T. Kim. Broadband convergence Network (BcN) for Ubiquitous Korea Vision. The 7th International Conference on Advanced Communication Technology ICACT'2005. Phoenix Park, Korea, February 21-23, 2005, Proceedings.

136. D. Kim and Y. Chung. Self-Organization Routing Protocol Supporting Mobile Nodes for Wireless Sensor Network. Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences, Volume 2, 2006.

137. A. Koucheryavy, A. Salim. Cluster head selection for homogeneous Wireless Sensor Networks. Proceedings, International Conference on Advanced Communication Technology, 2009. ICACT 2009. Phoenix Park, Korea.

138. A. Koucheryavy, A. Salim. Cluster-based Perimeter-coverage Technique for Heterogeneous Wireless Sensor Networks. Proceedings, ICUMT 2009 International Conference IEEE on

Ultra Modern Telecommunications, Saint-Petersburg, Russian. 2009.

139. A. Koucheryavy, A. Salim. Prediction-based Clustering Algorithm for Mobile Wireless Sensor Networks. Proceedings, International Conference on Advanced Communication Technology, 2010. ICACT 2010. Phoenix Park, Korea.

140. A. Koucheryavy. Networks Interoperability. ICACT'2009, Proceedings, 15-18 February, Phoenix Park, Korea

141. A. Koucheryavy, A. Prokopiev. Quality of Service (QoS) classes for Ubiquitous Sensor Networks. ICACT'2009, Proceedings, 15-18 February, Phoenix Park, Korea.

142. A.Koucheryavy, A.Prokopiev. Ubiquitous Sensor Networks Traffic Models for Telemetry Applications. Smart Spaces and Next Generation Wired/Wireless Networking.11th International Conference, NEW2AN 2011, and 4th Conference on Smart Spaces, ruSMART 2011. St.Petersburg, Russia, August 2011, Proceedings. LNCS 6869. Springer, 2011.

143. Y.Koucheryavy, J. Jakubiak. Research Challenges in Vehicular Ad hoc Networks. Proceedings, IEEE CCNC 2008, January 10-12, 2008. Las Vegas, USA.

144. K.S.Kwak, S.Ullah, N.Ullah. An Overview of IEEE 802.15.6 Standard. 3rd International Symposium, Applied Science in Biomedical and Communication Technologies (ISABEL), 7-10 November, Rome, Italy, 2010. Proceedings.

145. K.S.Kwak, M.A.Ameen. Current Status of the Proposed IEEE 802.15.6 WBAN MAC Standardization.

146. X. Li. Wireless Ad Hoc and Sensor Networks: Theory and Applications. Cambridge University Press, New York, NY, USA, 2008.

147. S. Lindsey and C. S. Raghavendra. PEGASIS: Power-efficient gathering in sensor information systems. Proceedings IEEE Aerospace Conference, vol. 3, Big Sky, Montana, USA, 2002.

148. S. Lindsey, C. Raghavendra, K. Sivalingam. Data gathering in sensor networks using the energy delay metric. Proceedings, 15th International Parallel and Distributed Processing Symposium (IPDPS), San Francisco, USA, Apr. 2001.

149. G.Marrocco. Pervasive Electromagnetics: Sensing Paradigms by Passive RFID Technology. IEEE Wireless Communications. December 2010, V.17, № 6.

150. Megerian. S., Koushanfar. F., Potkonjak. M., Srivastava. M.B. Worst and best-case coverage in sensor networks. IEEE Transactions on Mobile Computing, Volume 4, Issue 1, Jan.-Feb.2005.

151. M.Mellia, M.Meo. Measurement of IPTV Traffi from an Operative Network. European Transactions on Telecommunications, 2009.

152. T. Murakami. Toward the Realization of a Ubiquitous Network Society. WSIS'05, Tunis, 16-18 November, 2005. Japan's Workshop for WSIS.

153. D.J. Nagel. Wireless Sensor Systems and Networks: Technologies, Applications, Implications and Impacts. Seminar materials, The George Washington University, 2005.

154. D.-H. Nam, H.-K. Min. An efficient ad-hoc routing using a hybrid clustering method in a wireless sensor network. Proceedings IEEE 3rd International Conference "Wireless and Mobile Computing, Networking and Communications (WiMOB)", White Plains, New York, USA, Oct. 2007.

155. D.Niculescu. Communication paradigms for sensor networks. IEEE Communications Magazine, Volume 43, Issue3, March 2005.

156. I.Oppermann, M.Hamalainen, J.Iinatti. UWB Theory and Applications. John Wiley & Sons, 2004.

157. B.Otis, J.Rabaey. Ultra-Low Power Wireless Technologies for Sensor Networks. Springer, 2006.

158. A.Paramonov, D. Tarasov, A.E.Koucheryavy. The Video Streaming Monitoring in the Next Generation Network. LNCS, Springer. 9 th NEW2AN, LNS 5764, 15-18, September, 2009.

159. M.Poikselka, G.Mayer. The IMS: IP Multimedia Concepts and Services. 3rd Edition. J.Wiley&Sons, 2009.

160. Recommendation G.107. The E-model, a computational model for use in transmission planning. ITU, 2005.

161. Recommendation P.800. Methods for subjective determination transmission quality. ITU, 1996.
162. Recommendation P.800.1 Mean Opinion Score (MOS) terminology. ITU, 2006.
163. Recommendation Q.543. Digital exchange performance design objectives. ITU.1993.
164. Recommendation Y. 1541. Network Performance Objectives for IP-based Services. 2006.
165. Recommendation Y. 1901. Requirements for the Support of IPTV Services. 2009.
166. Recommendation Y. 1910. IPTV Functional Architecture. 2008.
167. Recommendation Y. 2006. Description of Capability Set 1 of NGN Release 1. 2008.
168. Recommendation Y. 2007. NGN Capability Set 2. 2010.
169. Recommendation Y. 2012. Functional requirements and architecture of the NGN. ITU, 2010.
170. Recommendation Y. 2021. IMS for Next Generation Network. ITU, 2006.
171. Recommendation Y. 2111. Resource and Admission Control Functions in Next Generation Networks. 2008.
172. Recommendation Y. 2211. IMS-based Real-Time Conversational Multimedia Services over NGN. 2007.
173. Recommendation Y. 2221. Requirements for Support of Ubiquitous Sensor Network (USN) Applications and Services in the NGN Environment. 2010.

174. Recommendations Y.2000 series. Y. Suppl.14. Service Scenarios over FMC. 2011.

175. Recommendation (draft) Y.dsnarch. Architecture of DSN. TD GEN680, NGN-GSI, May 9-20, 2011.

176. Recommendation (draft) Y.NGN-IoT-arch. Architecture of NGN for support of the Internet of Things. TD GEN697, NGN-GSI, May 9-20, 2011.

177. Recommendation (draft) ITU-T Y.2281 (Y.NGN-vehicle). Framework of networked vehicle services and applications using NGN. TD PLEN184, SG13 ITU-T meeting, January 17-28, 2011.

178. Recommendation (draft) Y.Terms-IoT (Internet of Things Related terminology). TD GEN749, NGN-GSI, May 9-20, 2011.

179. Recommendation (draft) Y.MOC-Reqts. Requirements for support of machine oriented communication applications in the NGN environment. TD GEN752, NGN-GSI, May 9-20, 2011.

180. Recommendation (draft) Y.USN-arch. Functional Architecture for USN. TD GEN723, NGN-GSI, May 9-20, 2011.

181. Recommendation (draft) Y.UbiNet-hn. Framework of object-to-object communication using ubiquitous networking. TD GEN732, NGN-GSI, May 9-20, 2011.

182. Recommendation (draft) Y.WoT. Framework of Web of Things. TD GEN735, NGN-GSI, May 9-20, 2011.

183. RFC4919. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. 2007

184. L. Reynau, D. Meddour. An Open Architecture that Manages Quality of Service within Ad Hoc Networks. Proceedings, IEEE IWWAN, 2004.

185. S. K. Sarkar, T. G. Basavaraju, C. Puttamadappa. Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications. Auerbach Publications, Boston, MA, USA, 2007.

186. A. C. C. Sawides, M. Srivastava. Dynamic fine-grained localization in ad hoc networks of sensors. Proceedings of the ACM/IEEE International conference on Mobile computing and networking. Rome, July 2001.

187. P.W. Schaefer, G. Gries, R. Gries, D. Holden. Pheromone components and diel periodicity of pheromonal communication in Lymantria Fumida. Journal of Chemical Ecology. Vol. 25, N 10, 1999.

188. C.Siva, R.Murthy, B.S. Manoj. Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall, 2004.

189. Z.Shelby. Embedded Web Services. IEEE Wireless Communications. December 2010, V.17, № 6.

190. X.Shen, M.Guizani, R.Qiu. T.Le-Ngoc. Ultra-Wideband Wireless Communications and Networks. John Wiley & Sons, 2006.

191. T. Small, Z. J. Haas. The shared wireless infostation model: a new ad-hoc networking paradigm. Proceedings ACM Mobihoc, ACM Press, 2003.

192. Smart Ubiquitous Networks (SUN). TD PLEN193, SG13 ITU-T meeting, January 17-28, 2011.

193. K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie. Protocols for self-organization of a wireless sensor network. IEEE Personal Communication Magazine, vol. 7, no.5.

194. S. Soro and W. B. Heinzelman. Cluster head election techniques for coverage preservation in wireless sensor networks. Ad Hoc Networks, Elsevier, Volume 7, 2009.

195. SOSUS. http://www.pmel.noaa.gov/vents/acoustics/sosus.html.

196. I.Stojmenovic. Handbook of sensor networks. Algorithms and architectures. John Wiley & Sons; 2005.

197. A.Swami, Q.Zhao, Y-W.Hong, L.Tong. Wireless Sensor Networks. Signal Processing and Communications Perspectives. John Wiley & Sons, 2007.

198. Tiny OS webpages, http://www.tinyos.org.

199. V. Tsetsos, G. Alyfantis, T. Hasiotis, O. Sekkas, S. Hadjiethymiades. Commercial Wireless Sensor Networks: Technical and Business Issues. The second Annual Conference on Wireless On-demand Network Systems and Services. WONS'05. Proceedings, 2005.

200. G. Veltri, Q. Huang, G. Qu, M. Potkonjak. Minimal and maximal exposure path algorithms for wireless embedded sensor networks. Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA, 2003.

201. Vision and Challenges for realizing the Internet of Things. European Commission. 2010.

202. VoIP: Developments In The Market. Organisation for Economic Co-operation and Development, 2006.

203. X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, C. Gill. Integrated coverage and connectivity configuration in wireless sensor networks. Proceedings of the First International Conference on Embedded Networked Sensor Systems (Sensys), Los Angeles, CA, 2003.

204. M. Weiser. Hot Topic: Ubiquitous computing. IEEE Computing. October 1993.

205. W.Willinger, M.Taqqu, R.Sherman, D.Wilson. Self similarity through high-variability. IEEE/ACM Transactions on Networking, Vol. 5, No. 1, 1997.

206. J. S. Wilson. Sensor Technology Handbook. Newnes, 2005.

207. Wireless World Research Forum, July, 2009, №4.

208. Y. Yao, J. Gehrke. The cougar approach to in-network query processing in sensor networks. ACM SIGMOD Record, vol. 31, no. 3, 2002.

209. Y. Li, M. T. Thai, W. Wu. Wireless Sensor Networks and Applications. Springer, 2008.

210. O. Younis, S. Fahmy. Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach. Proceedings, IEEE INFOCOM, Hong Kong, China, 2004.

211. O. Younis, M. Krunz, S. Ramasubramanian. Node clustering in wireless sensor networks: Recent developments and deployment challenges. IEEE Network, vol. 20, no. 3, 2006.

212. F. Zhao, L. J. Guibas. Wireless Sensor Networks: An Information Processing Approach. Morgan Kaufmann, 2006

213. D. E. Culler, J. Hui. 6loWPAN Tutorial. IP on IEEE 802.15.4 Low-Power Wireless Networks. Arch-Rock, 2007

214. 21ideas for the 21st century. Business Week, August 1999.

215. www.zigbee.com.

216. www.ubitel.ru.