Б.С. Гольдштейн, А.Е. Кучерявый

СЕТИ СВЯЗИ пост-NGN

Б. С. Гольдштейн, А. Е. Кучерявый

Сети связи пост-NGN

Санкт-Петербург
«БХВ-Петербург»
2014

УДК 621.372.88 (075)
ББК 32.883
Г63

Гольдштейн, Б. С.

Г63 Сети связи пост-NGN / Б. С. Гольдштейн, А. Е. Кучерявый. — СПб.: БХВ-Петербург, 2014. — 160 с.: ил.

ISBN 978-5-9775-0900-8

Книга описывает инфокоммуникационные сети пост-NGN второго десятилетия текущего века. Предназначается студентам, бакалаврам и магистрам, а также аспирантам, исследования которых прямо или косвенно затрагивают разные аспекты построения, технической эксплуатации и развития перспективных телекоммуникационных сетей. Инженеры и менеджеры, работающие в области инфокоммуникаций, тоже найдут для себя новое. Авторы излагают самые последние идеи и подходы к инфокоммуникациям, основные ре(э)волюционные технологии и архитектуры, включая такие разные векторы развития инфокоммуникаций, как Интернет вещей (IoT – Internet of Things) и сети мобильной связи 4G поколения SAE/LTE-Advance, всепроникающие сенсорные сети (USN – Ubiquitous Sensor Networks) и мультимедийная IP-подсистема (IMS – IP Multimedia Subsystem), сети для транспортных средств (VANET – Vehicular Ad-Hoc Networks) и молекулярные наносети.

Книга будет полезна топ-менеджерам, инженерам, студентам, аспирантам и всем специалистам, работающим в инфокоммуникационной отрасли.

Рецензенты:
Доктор технических наук Н.С. Мардер
Кандидат технических наук А.Е. Крупнов

Книга выходит при поддержке
Научно-технических центров Аргус и Протей (Санкт-Петербург).

Содержание

Светлой памяти своего директора, учителя и друга Анатолия Николаевича Голубева посвящают авторы эту книгу

Предисловие

Став ректором Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, я получил в свои сотрудники многих замечательных и заслуженных профессоров университета и авторов этой книги, общение с которыми с первых дней оказалось и приятным, и полезным.

В наших вечерних дискуссиях о перспективах IT-образования, о том, чему и зачем надо учить сегодняшних студентов в направлении инфокоммуникационных сетей и систем, отчасти и родилась идея этой книги.

Заведующие двумя ведущими кафедрами университета Борис Гольдштейн и Андрей Кучерявый – не только признанные в отрасли специалисты, авторы многочисленных статей и монографий, профессора, доктора наук, но и весьма харизматические личности в современных инфокоммуникациях. Именно поэтому, скорее всего, они и пошли на такой смелый и рискованный шаг, взявшись за описание инфокоммуникационных сетей 2020 года.

При всей неблагодарности такого занятия шаг этот мне представляется вынужденным. Ведь в нашем общем с авторами университетском труде мы, принимая абитуриентов на 1 курс в 2012 – 2014 годах, выпустим их в жизнь бакалаврами

и магистрами только в 2018 – 2020. И выпустить должны не с набором устаревших знаний о телекоммуникациях эпохи их поступления в ВУЗ, а подготовленными к работе именно в тех сетях пост-NGN конца второго десятилетия XXI века, о которых повествует эта книга.

Помимо общих проблем преподавания современных инфокоммуникаций нас с авторами объединяет и многолетний опыт работы в НИИ отрасли связи. В этом смысле замечательно то, что книга посвящена памяти легендарного генерального директора Ленинградского отраслевого НИИ связи (ЛОНИИС) А.Н. Голубева, более 17 лет руководившего этим головным институтом отрасли.

По общему признанию это были годы наивысшего расцвета института, много давшего российским телекоммуникациям того времени. Все эти годы авторы были ближайшими помощниками и заместителями генерального директора ЛОНИИС, там приобрели опыт, имена, ученые степени и звания, причем в те годы, когда все это доставалось несколько труднее, чем сегодня.

И хотя книга эта – о телекоммуникациях второго десятилетия XXI века, а работа авторов с А.Н. Голубевым относилась к телекоммуникациям второй половины восьмидесятых и девяностых годов XX века и начала нулевых века текущего, общий подход, смелость научного прогноза, сам дух и творческая атмосфера ЛОНИИС эпохи его расцвета сохранились в этой книге, которую я смело могу рекомендовать нашим студентам и аспирантам, да и далеко не только им.

С.В. Бачевский,

ректор СПбГУТ им. проф. М.А. Бонч-Бруевича,
доктор технических наук, профессор

Глава 1
Ре(Э)волюция NGN

Не говори: «отчего это прежние времена были лучше нынешних?», потому что не от мудрости ты спрашиваешь об этом.

Ветхий завет 7:1-10

1.1. Времена не выбирают...

Приведенная в эпиграфе мысль многократно цитируется на протяжении последних тысячелетий и, тем не менее, полностью сохраняет актуальность.

Одной из причин такого феномена является некоторая неопределенность понятий *прежних* и *нынешних* времен, которые в разных контекстах легко относятся к совершенно разным историческим периодам в Древнем Вавилоне или Древней Греции, в Древнем Риме или в Европе эпохи Возрождения, к разным этапам промышленной и научно-технической революций, равно как и к каждому десятилетию нашего бурно меняющегося прямо на глазах мира. По тем же причинам весьма удачным следует признать введенное уже довольно давно понятие *сетей связи следующего поколения NGN* (*Next Generation Networks*), широкое и длительное использование которого обусловлено отчасти тем, что оно однозначно не указывает на те или иные сетевые технологии. Поэтому к NGN в разные годы относили и сети IP-телефонии H.323, и сменившие их сети, построенные на про-

токоле SIP [5, 8], и поколение 3G мобильной связи с технологией *UMTS* (*Universal Mobile Telecommunications System*) [6], и сетевые архитектуры с Softswitch [1] и медиашлюзами, и *WiMAX (Worldwide Interoperability for Microwave Access*), а в самые последние годы – мультимедийную IP-подсистему *IMS* (*IP Multimedia Subsystem*) и новую сетевую архитектуру *LTE/SAE* (*Long Term Evolution/Service Architecture Evolution*).

В этой книге авторы решили сосредоточиться на сетях *пост-NGN* или *FGN* (*Future Generation Networks*), но не углубляться в детализацию этих несколько расплывчатых понятий, а просто ограничить рассматриваемую область инфокоммуникационными сетями текущего десятилетия. Т.е. в книге речь идет о сетях связи 2010-х годов и только о них.

Некоторые причины такого решения наш уважаемый ректор уже отметил в своем предисловии. Действительно, значительную часть своего сегодняшнего рабочего времени авторы посвящают обучению студентов, магистрантов, аспирантов на своих кафедрах и, следовательно, не могут не задумываться о том, какими именно инфокоммуникациями придется заниматься их ученикам после окончания обучения. Притом, по нашему мнению, недавно принятые федеральные образовательные программы третьего поколения (ФГОС III) устарели не совсем безнадежно. Много возможностей они оставляют университетам, и при желании можно преподавать то, что действительно нужно в современных условиях. Поэтому основную часть изложенного в книге материала авторы уже «обкатали» в учебных курсах.

Другая, также упомянутая в предисловии причина – более личная. Действительно, основную часть жизни авторы работали в Ленинградском отраслевом научно-исследовательском институте связи (ЛОНИИС), попав туда по распределению после окончания ЛЭИС им. проф. М.А. Бонч-Бруевича и пройдя бок о бок параллельные пути от инженеров, младших и старших научных сотрудников до руководителей крупных подразделений и заместителей генерального директора по науке. Все это время под руководством Анатолия Николаевича Голубева они дружно и самоотверженно (к сожалению, не все годы одинаково дружно, но, к счастью, всегда самоотверженно и с полной отдачей) трудились над проблемами телекоммуникаций сначала восьмидесятых, девяностых, а затем и нулевых годов.

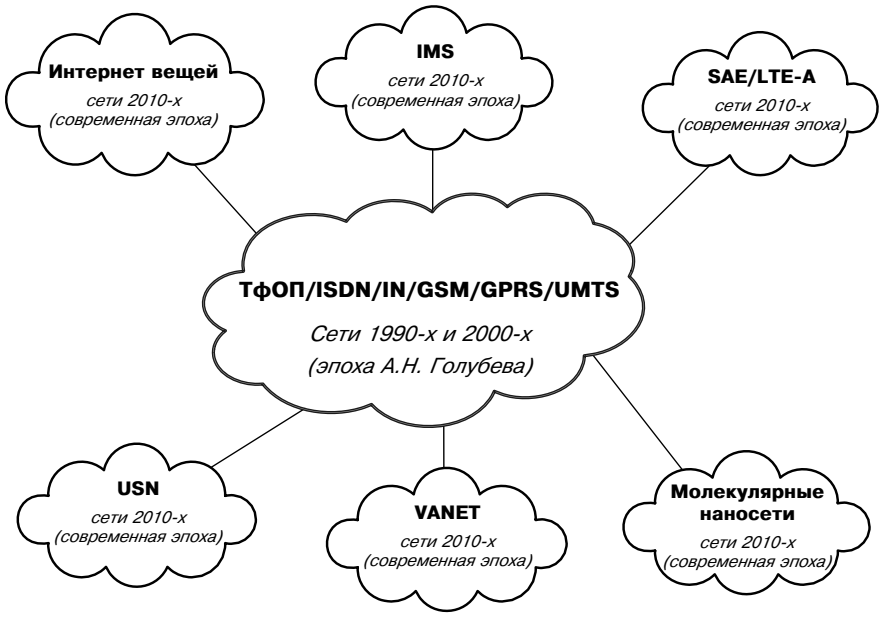

Рис. 1.1. Инфокоммуникационные сети второго десятилетия XXI века

Об этих телекоммуникациях авторами уже написано несколько десятков книг, начиная с [2] в период высшего расцвета TDM-сетей с коммутацией каналов и включая [1] и [11], посвященные сетям NGN нулевых годов текущего столетия. Поэтому, чтобы не терять время читателей и свое собственное, и не переписывать свои тексты из одной книги в другую, авторы решили выстроить эту книгу в соответствии с рис. 1.1. Как показано на этом рисунке, содержимое всех следующих глав соответствует перспективным сетям 2010-х годов, и лишь в этой первой главе мы кратко остановимся на текущем состоянии мобильных и фиксированных телекоммуникационных сетей.

1.2. Эволюция фиксированных сетей связи общего пользования

1.2.1. Три тройки ТфОП

Действительно, обойти полным молчанием ядро сетей на рис. 1.1 не представляется возможным. Начнем его краткое описание с сетей фиксированной телефонной связи ТфОП.

Такая последовательность вполне обоснована, т.к. новые тенденции и разработки, отмеченные в фиксированных сетях предыдущих десятилетий, в сетях мобильной связи также появлялись со средней задержкой приблизительно в 3 – 6 лет.

В сетях фиксированной связи число абонентов, использующих ТфОП не только и не столько для традиционной речевой телефонии, а для широкополосного доступа в Интернет, увеличивается так же быстро и неуклонно, как скорости передачи. А ведь первоначально вся ТфОП была спроектирована просто и исключительно по принципу трех троек: 3 телефонных вызова в час наибольшей нагрузки (ЧНН) плюс 3 минуты разговора (его средняя длительность) плюс полоса 3 кГц (0.3 – 3.4 кГц, вполне достаточная для хорошего качества телефонного разговора). И именно в таком виде ТфОП существовала, мало изменяясь, от самого начала почти до самого конца XX века, когда в начале 1990-х годов Интернет «взорвала» эти три тройки установлением коммутируемых соединений *dial up* с помощью Интернет-модемов. В середине 90-х первые модемы характеризовались скоростями приблизительно 14.4 кбит/с, но весьма быстро более поздние модели достигли скорости 56 кбит/с.

1.2.2. Модемы xDSL и технологии FTTx в сетях доступа

Важной вехой стало появление на массовом рынке в 2003 году модемов по технологии *асимметричной цифровой абонентской линии ADSL* (*Asymmetric Digital Subscriber Line*), с помощью которых легко достигались скорости передачи в несколько мегабитов в секунду.

Дальнейшая эволюция привела к высокоскоростным фиксированным абонентским линиям, основанным на оптоволокне, которое по технологии *FTTx* (*Fiber To The x*) подводится непосредственно в жилые дома (волокно к зданию), к наружным шкафам с распределительным оборудованием (волокно к шкафу) и т.п.

Технология волокна к шкафу предусматривала, что последний участок линии в зданиях или квартирах реализуется на медных проводах с Ethernet. Даже этот способ, когда для последнего участка соединения используется короткий медный кабель, уже позволял достичь скоростей 50 и 100 Мбит/с на линию. Разумеется, технологиями xDSL и FTTx не ограничиваются сегодняшние достижения сетей абонентского дос-

тупа, которые также пережили революционные изменения на рубеже XX и XXI веков.

В исторической аналогии можно даже назвать три источника и три составные части этого революционного движения. Тремя источниками стали речевой трафик, трафик данных и видеотрафик, а тремя составными частями – металлический кабель, оптоволокно и радиоканал. Эти аспекты революции сети доступа подробно рассмотрены в [3]. Здесь же подчеркнем, что сегодня понятие доступа получает совершенно новое значение. В главе 3 будет показано, что в мире IMS разделение между проводной линией и беспроводным каналом как составными частями сети доступа фактически исчезает. И если в мире традиционной телефонии доступ означает доступ к сети, в мире IMS это означает доступ к заказанной услуге.

1.2.3. Интеллектуальная сеть

Не менее радикальные изменения происходили и в Core Network. Это – широкое распространение и развитие сети общеканальной сигнализации ОКС7 и возникшая на основе ОКС7 концепция Интеллектуальной сети *IN* (*Intelligent Network*).

В новых инфокоммуникационных сетях 2010-х, когда все услуги могут быть представлены клиенту в виде облачных сервисов средствами программного обеспечения *SaaS* (*Software as a Service*), инфраструктуры *IaaS* (*Infrastructure as a Service*), платформы *PaaS* (*Platform as a Service*), бизнес-процессов *BPaaS* (*Business Processes as a Service*) или *WaaS* (*Web as a Service*), Интеллектуальные сети 90-х годов могут показаться анахронизмом. И все же той концепции, как и архитектуре компьютера фон Неймана, например, были свойственны черты великого творения. И как сегодняшние компьютеры слабо напоминают прежнюю архитектуру компьютера с арифметико-логическим устройством, памятью команд и данных, но базируются на тех давних идеях, так и концепция Интеллектуальной сети с INAP совсем не похожа на сегодняшние серверы приложений с развитыми на идеях IN интерфейсами *API* (*Application Program Interfaces)*, *OSA* (*Open Service Access*) и др. В посвященной IMS главе 3 мы вернемся к этой преемственности.

1.2.4. ISDN

Определение *ISDN* (*Integrated Services Digital Network*) впервые появилось в списке терминов Оранжевой книги сектора стандартизации телекоммуникаций Международного союза электросвязи *ITU-T* (*International Telecommunication Union – Telecommunication Standardization Sector*), именовавшегося тогда Международным консультативным комитетом по телеграфии и телефонии (МККТТ). В следующих цветных книгах ITU-T были опубликованы рекомендации серии I, описывавшие концепцию, сетевые и пользовательские аспекты, эталонные точки и услуги ISDN.

На русском языке эквивалентами термина ISDN являлись аббревиатуры ЦСИО (цифровая сеть интегрального обслуживания) и ЦСИС (цифровая сеть с интеграцией служб). Но наиболее точной оказалась шутливая англоязычная расшифровка I Still Don't Need it (мне все еще это не нужно).

Идея ISDN-сети базируется на двух специфических типах интерфейсов: интерфейс базового доступа *BRI* (*Basic Rate Interface*), регламентирующий соединение узла коммутации с абонентом, и интерфейс первичного доступа *PRI* (*Primary Rate Interface*), обеспечивающий включение учрежденческих АТС и корпоративных сетей в ТфОП.

Логически BRI представляет собой особым образом структурированный цифровой поток, разделенный на три логических канала: два информационных канала типа B со скоростью передачи 64 кбит/с каждый и один служебный канал типа D со скоростью передачи 16 кбит/с. При этом через один BRI можно передавать два независимых потока сообщений – по числу B-каналов. Разумеется, сегодня сама идея базового доступа 2B+D, предполагавшая один B-канал использовать для речи, а второй B-канал (или оба B-канала) – для передачи данных, выглядит анахронизмом.

Такой принцип разделения каналов можно охарактеризовать высказыванием из «Трех мушкетеров» Александра Дюма: «Для Атоса это слишком много, а для графа де Ла Фер это слишком мало». Действительно, 2B+D для передачи речи чрезмерно много, а для передачи данных безобразно мало. И все же не стоит рассматривать ISDN как ошибочную стратегию развития цифровых телефонных сетей.

ISDN оказала существенное влияние на развитие инфокоммуникаций, позволила Операторам связи накопить полезный опыт, способствовала созданию важнейшего протокола стека ОКС7 – протокола *ISUP* (*ISDN User Part*). Ряд инновационных разработок, выполненных для ISDN, оказался востребован другими телекоммуникационными технологиями.

Функциональная модель цифровой абонентской линии ISDN содержала 4 эталонные опорные точки, обозначаемые латинскими буквами R, S, T, U. Успех подхода с эталонными точками к описанию сетевой архитектуры в ISDN способствовал его использованию в самых разных новейших технологиях, что будет показано в следующих главах этой книги.

1.3. Эволюция сетей мобильной связи

1.3.1. Поколения сетей мобильной связи

Изображенные в ядре на рис. 1.1 первые три поколения сетей мобильной связи параллельно существовали и постепенно сменяли друг друга в 1990-х и 2000-х годах. Всего насчитывается четыре поколения сетей мобильной связи.

Первое поколение 1G почему-то часто называют аналоговым, хотя это уже были цифровые сети связи по аналогии с фиксированными сетями: аналоговый радиодоступ и цифровые узлы коммутации.

Это и система северной мобильной телефонии NMT (Nordic Mobile Telephony) на частоте 450 МГц, и усовершенствованная подвижная телефонная служба AMPS (Advanced Mobile Phone Service), с которой начинал один из Операторов нынешней Большой тройки.

Система NMT-450 была признана первым российским федеральным стандартом мобильной связи, на котором в начале 1990-х начал работать петербургский Оператор связи «Дельта Телеком».

Первые мобильные телефоны сети «Дельта» стоили порядка $2000 – $3000 и весили несколько килограммов. Но для них же в середине 1990-х был организован первый автоматический роуминг региональных Операторов NMT-450 в рамках национальной сети.

Вспомним, что технология NMT-450 была наиболее экономичной для организации связи на больших территориях с малой плотностью населения, хотя и обладала существенными недостатками, обусловленными селективными замираниями из-за многолучевого распространения радиоволн в условиях городской застройки, возможностью прослушивания переговоров с помощью обычных УКВ приемников, легкостью организации клонов телефонов и т.п. Первый звонок через наиболее успешную систему второго поколения – Глобальную систему мобильной связи *GSM* (*Global System for Mobile Communications*) – состоялся 1 июля 1991 года в одном из парков города Хельсинки, а уже в 1994 году сеть GSM заработала в Москве.

1.3.2. Релиз 99. Основы UMTS

Разумеется, в полном соответствии с законом Мура, число транзисторов в интегральных схемах не прекратило свой экспоненциальный рост и после появления технологий 2G, что в свою очередь привело к появлению намного более интенсивных в вычислительном отношении методов мобильной связи, чем сравнительно простой радиоинтерфейс GSM. Это в полной мере проявилось в технологии третьего поколения UMTS, которая может быть в равной степени отнесена как к эволюции, так и к революции в сетях подвижной связи (СПС).

Для поколения 3G ставилась задача: в зависимости от степени мобильности абонента (скорости его передвижения в зоне обслуживания) обеспечить доступ 2.048 Мбит/с для обслуживания стационарных и передвигающихся внутри зданий абонентов (скорость менее 3 км/ч), 384 кбит/с при низкой мобильности (скорость от 3 до 12 км/ч) и локальной зоне покрытия, 144 кбит/с при высокой мобильности (скорость от 12 до 120 км/час). Для достижения этих и больших скоростей при ограниченном частотном ресурсе, для организации постоянно расширяющегося набора услуг разработаны релизы 3GPP, которые и отражают эволюцию мобильной связи в мире.

Первоначально эти релизы (выпуски спецификаций) 3GPP [128] именовались по году ратификации, а позже использовался номер версии. Напомним, что партнерство 3GPP было создано 4 декабря 1998 г. с целью проведения практических работ по стандартизации систем подвижной связи 3G.

Первый комплект выпуска 3GPP для GSM/UMTS был завершен в конце 1999 г., поэтому его назвали релизом 99, но все последующие версии стали называть релизами 4, 5, 6 и т.д. Сегодня, когда пишется эта книга, 3GPP завершает работы над релизом 11. Согласно релизу 99, в технологию UMTS (сеть радиодоступа UTRAN) из GSM были перенесены понятия базовых станций и контроллеров с соответствующим переименованием – эти элементы в сети GSM назывались BTS и BSC, а в UTRAN их называют узлом-B (Node B) и контроллером радиосети RNC. Мобильный терминал MS также получил новое имя и теперь называется пользовательским оборудованием UE.

Кроме того, в релиз 99 для UMTS вошли улучшения программного обеспечения, чтобы поддерживать новый интерфейс Iu (cs) между MSC и UTRAN, причем на верхних уровнях интерфейс Iu (cs) пока остался подобен A-интерфейсу GSM, а вот нижние уровни были полностью переработаны на технологию ATM.

Новые функции UMTS, кроме того, потребовали развития программного обеспечения HLR и центра аутентификации и контроля доступа абонентов *AuC* (*Authentification Center*). Не подвергалась изменениям базовая сеть передачи пакетов GPRS, которая была относительно новой технологией во время спецификации релиза 99 и вполне подходила для высокоскоростного доступа, кроме интерфейса Iu(ps) между SGSN и сетью радиодоступа. Основным отличием от GSM/GPRS является использование ATM вместо Frame relay на нижних уровнях стека протоколов интерфейса Gb. Кроме того, программное обеспечение SGSN было изменено, чтобы прозрачно туннелировать пользовательские пакеты данных GTP (GPRS Tunneling Protocol) к и от RNC, вместо того, чтобы анализировать содержание пакетов и перестраивать их на новый стек протоколов, как было ранее сделано в GSM/GPRS.

1.3.3. Релиз 4. Усовершенствование домена коммутации каналов CS

В релизе 99, как и до него, все речевые вызовы с коммутацией каналов направлялись через базовую сеть GSM или UMTS посредством каналов с временным разделением со скоростью 64 кбит/с внутри трактов E1.

Важным усовершенствованием в релизе 4 явилось новое понятие независимой от носителя базовой сети BICN. Вместо того, чтобы использовать временные интервалы 64 кбит/с с коммутацией каналов, трафик можно было передавать в пакетах IP. С этой целью MSC разделялся на MSC-сервер (MSC-S), который отвечал за управление вызовами (CC) и управление мобильностью (MM), и медиашлюз (MG), который отвечал за медиатрафик, а также за перекодировку пользовательских данных для различных методов передачи.

Таким способом можно, например, получить речевые вызовы через A-интерфейс GSM во временном интервале E1, и преобразовать в медиашлюзе этот поток цифровой речевой информации в пакеты IP.

1.3.4. Релиз 5. IMS и высокоскоростной нисходящий пакетный доступ

Следующим шагом к беспроводной сети полностью на IP является *мультимедийная IP-подсистема* (*IMS*) [18]. Основа для IMS была заложена 3GPP в релизе 5. Последующие релизы расширили ее новыми функциональными возможностями. Вместо того, чтобы использовать домен CS, подсистема IMS обеспечивает установление мультимедийной сессии, в том числе и телефонного соединения, используя в качестве доступа RNS и оборудование домена PS (GPRS).

Ядро IMS состоит из ряда узлов, которые формируют *функцию управления сеансами связи CSCF* (*Call Session Control Function*), базирующуюся на протоколе инициирования сеансов SIP, который был первоначально разработан для фиксированных сетей NGN. CSCF продвигает эту концепцию на шаг дальше и расширяет стандарт SIP рядом функциональных возможностей, необходимых для мобильных сетей. IMS может транспортировать речевые вызовы по IP не только в базовой сети, но также и из конца в конец, то есть, от мобильного устройства до мобильного устройства.

CSCF отвечает за установление соединений и управление сеансами связи, а обмен пользовательскими пакетами данных, которые, например, переносят речь или видео, происходит непосредственно между устройствами конечных пользователей.

Важным нововведением стало объединение функций HLR и АиС в единый *сервер абонентов домашней сети HSS* (*Home Subscriber Server*), содержащий информацию о каждом абоненте домашней сети. Более подробно об этом в главе 3.

С помощью сети радиодоступа UMTS стало возможным реализовать основанную на IP архитектуру мобильной передачи речи и видео. Это произошло не только потому, что UMTS предложила достаточную пропускную способность радиоинтерфейса для таких приложений, но также в силу способа обеспечения мобильности для активных пакетных сессий.

В случае с GPRS мобильностью для соединений с коммутацией пакетов управляет само устройство пользователя, что приводит к прерыванию пакетного трафика на 1-3 секунды. Для речевых вызовов или видеовызовов такое прерывание является неприемлемым. В случае с UMTS управлением мобильностью для активных соединений с коммутацией пакетов осуществляется средствами сети, что гарантирует непрерывный пакетный трафик даже в процессе перемещений пользователя. Поскольку IMS – система, основанная на IP, она не может непосредственно обмениваться информацией с системами телефонии с коммутацией каналов, которые пока еще доминируют в существующих сетях связи. Однако, каждый пользователь должен иметь возможность говорить с любым другим пользователем независимо от вида коммутации (каналов или пакетов), который используется на каждом участке сети между ними.

Это достигается за счет применения медиашлюзов MG, которые осуществляют преобразование между IP и классической передачей во временных каналах тракта E1 сетей с коммутацией каналов, а также MGC, которые осуществляют преобразование SIP (SIP-T) в ISUP.

К сожалению, IMS страдала от ряда ограничений, которые тормозили полную замену ею релиза 99 или релиза 4 с архитектурой MSC. Вот некоторые из них:

- IMS разработана не только и не столько для речевых вызовов, а как платформа интегрального обслуживания всеми видами новых мультимедийных услуг, включая видеоконференции, обмен изображениями, мгновенный обмен сообщениями и другие сервисы. Как следствие, система оказалась относительно сложна;

- чтобы быть принятой пользователями, система IMS должна обеспечивать непрерывность установленного сеанса связи в медиасреде с коммутацией каналов, когда пользователь покидает зону охвата UMTS;
- IMS была разработана для того, чтобы быть платформой, которую сторонние разработчики услуг могли бы использовать для интегрирования своих сервис-платформ на базе IP в среду мобильной сети. Однако Интернет-компании традиционно предоставляют услуги на пользовательских терминалах, соединенных с Интернет не важно каким способом, и, следовательно, не всегда интересуются использованием специальных платформ типа IMS, которые либо есть, либо отсутствуют в сетях разных телекоммуникационных Операторов.

Проблематике IMS целиком посвящена глава 3 этой книги. Более подробную информацию об IMS, ее архитектуре и возможном применении можно также найти в [77,127]. Относительно подробное описание есть в [96]. Рекомендации ITU-T по IMS изложены в [98, 99].

Еще одной важной функцией, введенной 3GPP в релизе 5, была новая схема передачи данных с названием *высокоскоростной нисходящий пакетный доступ HSDPA* (*High-Speed Downlink Packet Access*).

Схема предназначена для увеличения скорости передачи данных от сети к пользователю. В то время как максимальная скорость в релизе 99 была 384 кбит/с, HSDPA увеличила скорость доступа при обычных условиях до нескольких мегабитов в секунду. Многие специалисты телекоммуникационной отрасли видят HSDPA в сочетании со смартфонами и аппаратными модемами 3G для ноутбуков как комбинацию, которая помогла UMTS получить признание массового рынка и широкое использование.

1.3.5. Релиз 6. Высокоскоростной восходящий пакетный доступ HSUPA

Увеличение скорости передачи данных при пакетном доступе продолжалось и в релизе 6. Эта версия спецификации принесла внедрение методов увеличения восходящих скоростей, которые оставались теми же самыми, начиная с релиза 99.

Этот набор функций, называемый *высокоскоростной восходящий пакетный доступ HSUPA* (*High Speed Uplink Packet Access)*, допускает восходящие скорости передачи данных в несколько мегабитов в секунду для единственного пользователя при идеальных условиях. Даже принимая во внимание реалистические условия распространения сигнала, количество пользователей в соте и возможности мобильного устройства, HSUPA все равно позволяет устройствам достичь значительно более высоких восходящих скоростей, чем это было возможно с релизом 99. Кроме того, HSUPA также увеличивает максимальное количество пользователей, которые могут одновременно передавать данные в одной и той же соте. Комбинацию HSDPA и HSUPA часто называют также *высокоскоростным пакетным доступом HSPA*.

В релизе 6 также были введены адаптивные многоскоростные широкополосные кодеки AMR-WB+ (Adaptive Multi-Rate-Wideband-i-codec), позволяющие передавать и принимать речь и музыку с высоким качеством, введена поддержка мультимедийного вещания *MBMS* (*Multimedia Broadcast/Multicast Service*) и расширены диапазоны частот 2100/1900/1800/900/800 МГц для мобильных терминалов и сети радиодоступа UTRAN. С точки зрения IMS релиз 6 был призван ликвидировать некоторые недоработки релиза 5 и добавить несколько новых функций.

Было обеспечено взаимодействие с сетью коммутации каналов, с другими IP-сетями и с разными технологиями доступа (в частности, WLAN), добавлены некоторые объекты и эталонные точки, функции групповой маршрутизации, установления сеансов связи с экстренными службами и множественная регистрация. К возможностям защиты данных были добавлены конфиденциальность сообщений SIP и использование ключей. Были определены сервисные возможности для мультимедийных услуг многоадресной рассылки информации.

1.3.6. Релиз 7. Быстродействующая HSPA и непрерывная пакетная связь

Одним из недостатков систем радиодоступа UMTS и HSPA по сравнению с GSM является высокое потребление мощности во время перерывов передачи, например, между загрузками двух веб-страниц. Даже при том, что никакие пользо-

вательские данные не передаются и не принимаются в это время, требуется существенное количество энергии, чтобы отправлять управляющую информацию, сохранить установленное соединение и произвести сканирование для новых входящих данных.

Только спустя некоторое время, обычно порядка 15-30 с, система переводит состояние соединения в более эффективный по потреблению питания режим. Но даже это состояние все еще требует существенного количества энергии, и батарея продолжает расходоваться до момента, когда сеть, наконец, переводит соединение радиоинтерфейса в состояние сна.

В типичном случае это происходит еще через 30-60 с. Требуется приблизительно 2-3 с, чтобы «проснуться» в этом состоянии, когда пользователь, например, щелкает по ссылке на веб-странице после того, как соединение радиоинтерфейса уже вошло в режим сна.

Сокращение расхода энергии и быстрый возврат к полностью активному состоянию были задачами, решаемыми в релизе 7 и названными *непрерывной пакетной связью CPC*.

Кроме того, релиз 7 3GPP еще раз увеличил максимально возможные скорости передачи данных в нисходящем направлении благодаря использованию нескольких антенн и схем *передачи с многократным вводом/многократным выводом MIMO* и *квадратурной амплитудной модуляции 64* (*64-QAM*).

Максимальные скорости, достигнутые благодаря этим улучшениям при идеальных условиях для сигнала, составляют 21 Мбит/с с модуляцией 64 QAM и 28 Мбит/с с MIMO.

В восходящем направлении функции HSUPA в этом релизе тоже были расширены. В дополнение к схеме модуляции с *квадратурной фазовой манипуляцией QPSK* для восходящего направления в этом релизе специфицирована также 16-QAM, что дополнительно увеличивает пиковые скорости передачи данных до 11.5 Мбит/с при очень хороших условиях для сигнала.

В части IMS релиз 7 был направлен на гармонизацию стандартов 3GPP со стандартами ETSI TISPAN (см. главу 3) и работу IMS в фиксированных сетях связи. В частности, был описан доступ к услугам IMS из проводной сети, эмуляция услуг

ТфОП и взаимодействие с сетями не-IMS, что в совокупности составило содержание усовершенствованной подсистемы *E-IMS* (*Enhanced IMS*). Подробнее об этом в главе 3.

1.3.7. Релиз 8. LTE и Femtocells

В релизе 8 был введен ряд функциональных возможностей, которые окажут значительное влияние на дальнейшее развитие беспроводных сетей.

Во-первых, релиз 8 вводит преемника радиосети UMTS – так называемую *eUTRAN*, а также новую архитектуру базовой сети – *EPC* (*Evolved Packet Core*).

Вместе они известны под названием долговременная эволюция мобильной связи *LTE/SAE* [19]. Поскольку LTE/SAE является во многих отношениях революционным преобразованием сетей 2010-х, она обсуждается отдельно в главе 4.

Для радиодоступа UMTS этот выпуск стандарта тоже содержит некоторые заметные улучшения, чтобы идти в ногу с возрастающими потребностями в скоростях передачи данных. Чтобы достигнуть еще более высоких скоростей, теперь можно агрегировать два смежных носителя UMTS и получить общую полосу пропускания 10 МГц. Тому же способствовало одновременное использование 64-QAM и MIMO. При идеальных условиях радиосвязи может быть достигнута пиковая скорость 42 Мбит/с в нисходящем направлении.

Для приложений VoIP было определено улучшение, которое позволяет сети готовить канал с коммутацией каналов в GSM, для обеспечения хэндовера сеансов связи с коммутацией пакетов из зоны обслуживания UMTS или LTE в зону обслуживания GSM.

В предыдущих выпусках требовалось, чтобы мобильное устройство связывалось одновременно с сетью UMTS и сетью GSM. Поскольку такие абонентские терминалы фактически отсутствуют, была введена функция *непрерывности речевого радиовызова VCC SR*. Этот аспект более подробно обсуждается в главе 4 при рассмотрении опций VoIP в LTE.

Одной маленькой, но важной возможностью, определенной в релизе 8, является функция «В случае крайней необходимости» – *ICE* (*In Case of Emergency*).

Устройства, которые реализуют эту функцию, позволяют пользователю хранить информацию на SIM-карте, к которой можно получить доступ стандартизованным способом в чрезвычайных ситуациях, когда пользователь телефона не способен идентифицировать себя или связаться со своими родственниками. И наконец, релиз 8 заложил основу для управления *Femtocells* (*фемтосотами*), называемыми в стандарте *домашними Node-B*, и группу функций *самоорганизующейся сети SON (Self-Organizing Network*), чтобы облегчить развертывание и обслуживание сетей.

В области IMS в релизе 8 были проработаны централизация предоставления услуг и организация вызовов к экстренным службам. Начиная с этого релиза, архитектурных изменений в IMS практически не производится – ведутся доработки отдельных функций, интерфейсов и процедур. Поэтому содержание главы 3 этой книги преимущественно базируется именно на релизе 8.

Релизы 7 и 8, в которых впервые упомянута и описана архитектура LTE/SAE и соответствующие ей ключевые новшества на радиоучастке, в домене коммутации пакетов и в ядре сети, а также и все предыдущие релизы 3GPP сведены в табл. 1.1.

Таблица 1.1. Релизы 3GPP (Release 99- Release 8)

	R99	R4	R5	R6	R7	R8
Новые термины	UMTS		HSDPA; IMS	HSUPA	HSPA+ и LTE	LTE/ SAE и common IMS
Базовая сеть		Отделение управления от транспорта: MSC Server+Media Gateway; All-IP сеть	Управление сетью в соответствии с концепцией IMS	VoIMS (SIP, RTP, RTCP)	Развитие IMS	SAE – плоская all-IP архитектура сети для сети LTE
Домен коммутации пакетов PS	EDGE			Созданы механизмы взаимодействия между сетью UMTS и WLAN	EDGE Evolution	EPC
Радиоучасток	UTRAN (W-CDMA)		HSDPA; IP-транспорт в UTRAN	HSUPA	MIMO	

1.3.8. Релиз 9. Цифровой дивиденд

С точки зрения LTE релиз 9 [20,42,50] является, главным образом, релизом, который включает в себя функции и исправления, не считавшиеся важными для первых спецификаций LTE в релизе 8. Кроме того, спецификации архитектуры SON и Femtocell (домашний Node-B и домашний eNode-B), введенные в релизе 8, были продолжены и в этом релизе.

Там же, в релизе 9, появилась возможность совершать экстренные вызовы через GPRS и EPS, была введена система предупреждения о массовой опасности PWS (Public Warning System) при стихийных бедствиях, а также были доработаны механизмы информационной защиты GSM и GPRS, которые не менялись в течение некоторого времени, и в которых был обнаружен ряд уязвимостей. Этим релизом 3GPP добавил алгоритм шифрования A5/4 вместе с удвоением длины *ключа шифрования CK* до 128 битов. Были также развиты инфокоммуникационные услуги с определением местонахождения абонентов *LBS* (*Location Base Services*) и услуги *M2M* на основе сетей «машина-машина», чему посвящена глава 2.

1.3.9. Релиз 10. LTE-Advanced

Здесь наиболее важным элементом является развитие LTE до LTE-Advanced и дальнейшее увеличение скорости передачи данных различными средствами: максимальная скорость нисходящей передачи данных – до 1 Гбит/с, восходящей передачи данных – до 500 Мбит/с, т.е. средняя пропускная способность для одного мобильного устройства втрое превышает скорость LTE.

Кроме того, втрое улучшена максимальная эффективность использования спектра для нисходящей передачи – 30 бит/с/Гц, а для восходящей – 15 бит/с/Гц.

В этом релизе продолжились также работы с экстренными вызовами, добавилась возможность перевода вызовов между терминалами. Последняя версия спецификации на момент написания этой книги – релиз 11. В нем добавляются услуга эмуляции USSD, информация о местонахождении терминала и передача SMS без *MSISDN* (*Mobile Station International ISDN Number*). Подробнее обо всем этом в главе 4.

1.4. Конвергенция FMC

Как следует из вышеизложенного, в новых инфокоммуникационных сетях с архитектурой IMS не будет «вертикального» разделения Операторов по типу базовой услуги. Понятия «Оператор фиксированной сети», «Оператор мобильной сети» постепенно отойдут в прошлое. Собственно говоря, эти термины уже далее в книге не встречаются. Разумеется, понятие конвергенция имеет гораздо более широкий смысл, чем отсутствие «вертикального» разделения, о чем будет не раз говориться в следующих шести главах книги, посвященных самым разным, но всегда конвергентным инфокоммуникационным сетям 2010-х.

1.5. Эволюция IP-сетей

Короткой, но чрезвычайно насыщенной истории Интернет посвящены многие сотни книг. Хотя само слово «Интернет» появилось в первых работах Уинтона Серфа и Роберта Канна, а три ключевых протокола – TCP, UDP и IP – появились уже в конце 1970-х годов, непосредственно Интернет-революцию следует отнести к началу 1990-х.

Главным событием 1990-х годов, вероятно, следует считать появление Web (всемирной паутины). Придумал всемирную паутину Тим Бернерс-Ли, базируясь на идеях гипертекста, предложенных еще в 40-х и 60-х годах прошлого века Бушем и Нельсоном [9]. Кстати, Тим Бернерс-Ли с соавторами изобрел также язык HTML, протокол HTTP, Web-сервер и браузер, что и обеспечило в совокупности WWW-революцию, которая привела IP в миллионы офисов и квартир по всему миру и дала толчок разработке и внедрению тысяч новых IP-приложений.

Важнейшим из этих тысяч IP-приложений, по мнению авторов, является IP-телефония. Открытие *VoIP* (*Voice over IP*) как промышленной технологии совершила израильская компания VocalTec, сумевшая к 1995 году собрать воедино достижения в областях цифровых сигнальных процессоров, кодеков, компьютеров и протоколов маршрутизации, чтобы сделать реальными разговоры между фактически любыми точками на планете через Интернет без оглядки на расстояние между абонентами и длительность разговора. О дальнейшем развитии, основных сценариях и алгоритмах IP-телефонии говорится в [6].

1.6. Далее в книге

О чем эта книга, показано на первом рисунке (рис. 1.1). Находящиеся в облаке в центре рисунка традиционные телекоммуникационные сети 1990-х и 2000-х годов кратко рассмотрены в главе 1.

Остальные 6 глав посвящены новым инфокоммуникационным сетям, контуры которых только начинают формироваться к началу десятых годов нашего века, что и определяет ответ на вопрос, когда следует читать эту книгу. Последнее отнюдь не означает, что после 2021 года в нее не будет нужды заглядывать. Более того, есть все основания считать, что именно тогда все или почти все эти новые инфокоммуникационные сети эпохи пост-NGN начнут оказывать решающее воздействие на новое постиндустриальное инфокоммуникационное U-общество [10].

Этапы общественного развития, как они видятся авторам, представлены в табл. 1.2.

Строго говоря, минувшая индустриальная эра зарождалась еще на рубеже века XIX, когда на английских, а затем других технологически передовых европейских фабриках и заводах вместе с паровыми машинами и механическими ткацкими станками начала создаваться новая система организации труда людей в условиях крупномасштабного индустриального производства. И развитие этой индустриальной эры продолжалось без малого два века.

Таблица 1.2. Этапы общественного развития

Этапы развития общества	Доля ИКТ в ВВП	Инфокоммуникационные сети и услуги
Индустриальное (~ 1800 – 1980)	1-2%	ТфОП, ТгОП
Постиндустриальное (~ 1980 – 2005)	2-3%	ТфОП/ISDN/IN +СПС +VoIP
Электронное (2005 – 2015)	10%	+е-бизнес, +е-обучение, +е-правительство, etc
Информационное всепроникающее (~2005 – 2025)	>20%	+сети u-общества в главах 2-7 этой книги

Для постиндустриальной же эры все радикально убыстрилось, роль эффективности использования машин и механизмов – наиболее ценного в индустриальную эру производственного ресурса – упала, инфокоммуникационные технологии стали отвоевывать все более значимую долю всепланетного валового продукта (табл. 1.2).

Начало нового постиндустриального мира – весьма условное, как и все подобные хронологии – авторы относят к 1975 г., когда встретились «два Стива» – Стефан Возняк и Стив Джобс. Это пересечение жизненных путей двух будущих основателей новой компьютерной отрасли произошло в одном из городков Кремниевой долины, как обычно называют густонаселенный компьютерными и другими наукоемкими фирмами район штата Калифорния вдоль дороги 101 от Сан-Франциско до Сан-Хосе.

Впрочем, к моменту встречи Возняк работал там же в крупнейшей компьютерной фирме – Hewlett Packard, а Джобс – в не менее знаменитой тогда компьютерной фирме Atari, так что начало постиндустриальной эры можно датировать и началом 1970-х. А можно и началом 1980-х, основываясь на истории создания Интернет, о чем говорилось в предыдущем параграфе.

Так или иначе, но именно с этого перехода к постиндустриальному обществу началось развитие инфокоммуникационных технологий (ИКТ), что иллюстрирует табл. 1.2. И темпы развития никак не замедляются в 2010-х, что отражает содержание последующих 6 глав нашей книги.

И еще одно замечание к этим 6 главам. С учетом того, что авторы посвящают часть своего времени чтению лекций в СПбГУТ им. проф. М.А. Бонч-Бруевича, настоящая книга ориентирована также и на использование в качестве учебника по новым аспектам курсов основ построения телекоммуникационных сетей и систем, сетей связи и некоторым другим.

Преподавательский уклон книги и новаторский характер излагаемых в ней вопросов требуют от авторов поддержать каждого читателя, который собирается продолжить знакомство с ее следующими главами, первой строкой знаменитого бестселлера «Ребенок и уход за ним» Бенджамина Спока: «*Доверяй себе. Ты знаешь больше, чем тебе кажется*».

Глава 2
Интернет вещей

Жизнь – большая связка мелких вещиц.
Оливер Холмс (1809 – 1894)

2.1. Прогнозы и новые концепции развития сетей связи

В период интенсивного развития концепции NGN в 2000-х годах сетевые структуры всепроникающих сенсорных сетей *USN (Ubiquitous Sensor Networks)* входили в NGN как составная часть. В то время считалось, что клиентскую базу USN составят сотни миллионов сенсорных узлов. Однако стремительное развитие этой новой технологии, появление концепций Интернет вещей *IoT (Internet of Things)* [14,91,101,103,121] и Веб вещей *WoT (Web of Things)* [107,112] привели к пересмотру перспектив развития сенсорных сетей, а согласно сегодняшним прогнозам число беспроводных устройств составит 7 триллионов на 7 миллиардов человек к 2017 – 2020 годам [123].

На рис. 2.1 приведены примеры использования сенсорных узлов, включая радиоидентификаторы *RFID* (*Radio Frequency IDentification*), в том числе и такие новейшие приложения USN, как мониторинг роста животных и растений [91].

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 разнообразных устройств, биомасс, конструкций и т.п.

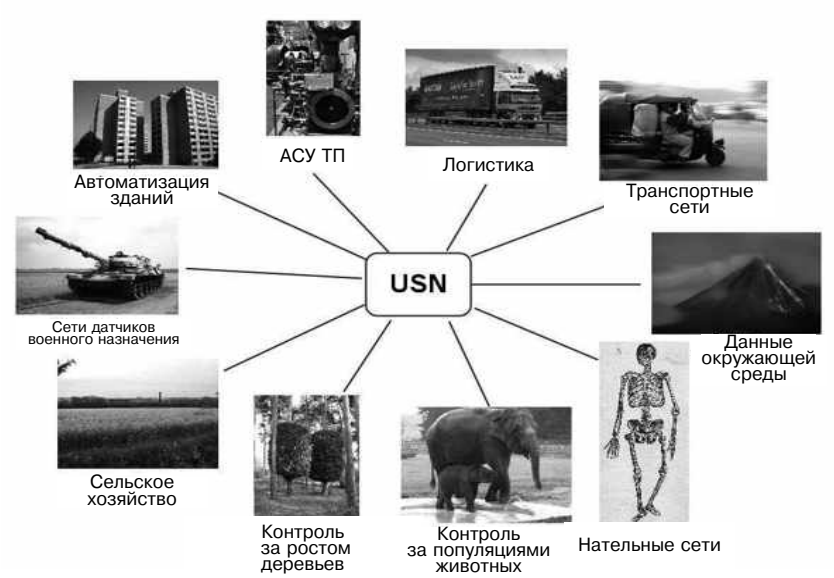

Рис. 2.1. Примеры использования USN сетей

Сектор стандартизации Международного союза электросвязи в начале 2011 года рассматривал возможность замены концепции NGN концепцией умных всепроникающих сетей *SUN* (*Smart Ubiquitous Networks*) [114], включающей в себя концепцию NGN, как одну из составных частей.

Структура концептуальной модели SUN приведена на рис. 2.2.

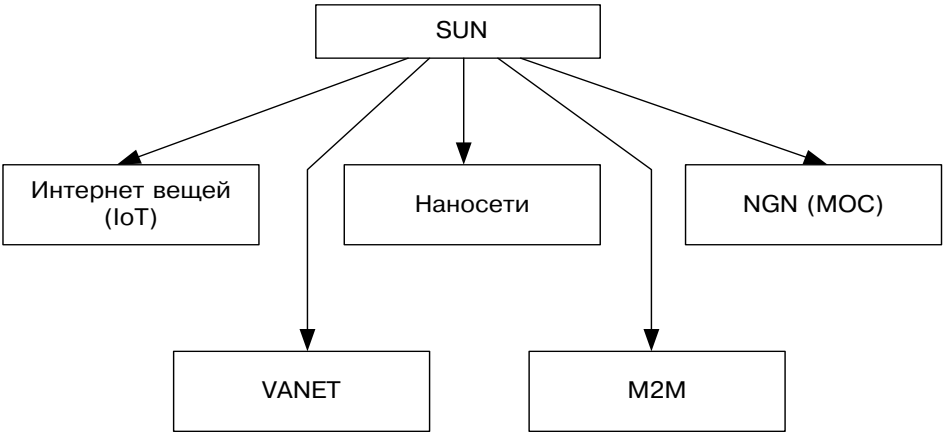

Рис. 2.2. Структура концептуальной модели SUN

В состав концептуальной модели SUN входят Интернет вещей IoT, сеть NGN, модернизированная до уровня поддержки межмашинных коммуникаций MOC (Machine Oriented Communications) [104], наносети [29], транспортные сети VANET [69, 85, 102] и сети машина-машина *M2M* (*Machine-to-Machine*) [44].

На рис. 2.3 приведена структура Интернет вещей, включающая в себя сетевые структуры USN, построенные на базе протокола IPv6 – *6LoWPAN* (*Low energy IPv6 based Wireless Personal Area Networks protocol*). Протокол 6LoWPAN [41, 108] обеспечивает возможность присвоения IP-адреса сенсорным узлам и RFID или их группам. Именно эта возможность делает USN с применением IP-адресации основой Интернет вещей.

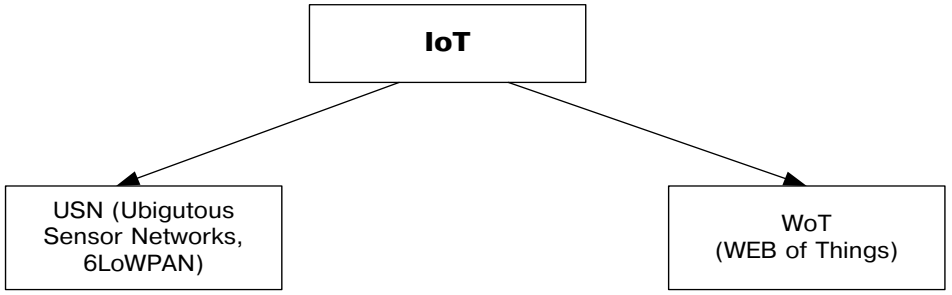

Рис. 2.3. Структура Интернет вещей

Веб вещей является составной частью Интернет вещей и предоставляет возможность мониторинга и управления вещами с помощью страниц WWW. На рис. 2.4 приведена структура организации Веб вещей [107], из которой видно, что ключевую роль в этом применении IoT играет брокер Веб вещей, позволяющий использовать Веб как для изначально приспособленных к этому 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 [129] или Bluetooth [73]. На рис. 2.4 приложения Веб вещей подразделяются на мониторинг, управление, услуги, в том числе смешанные (mash up).

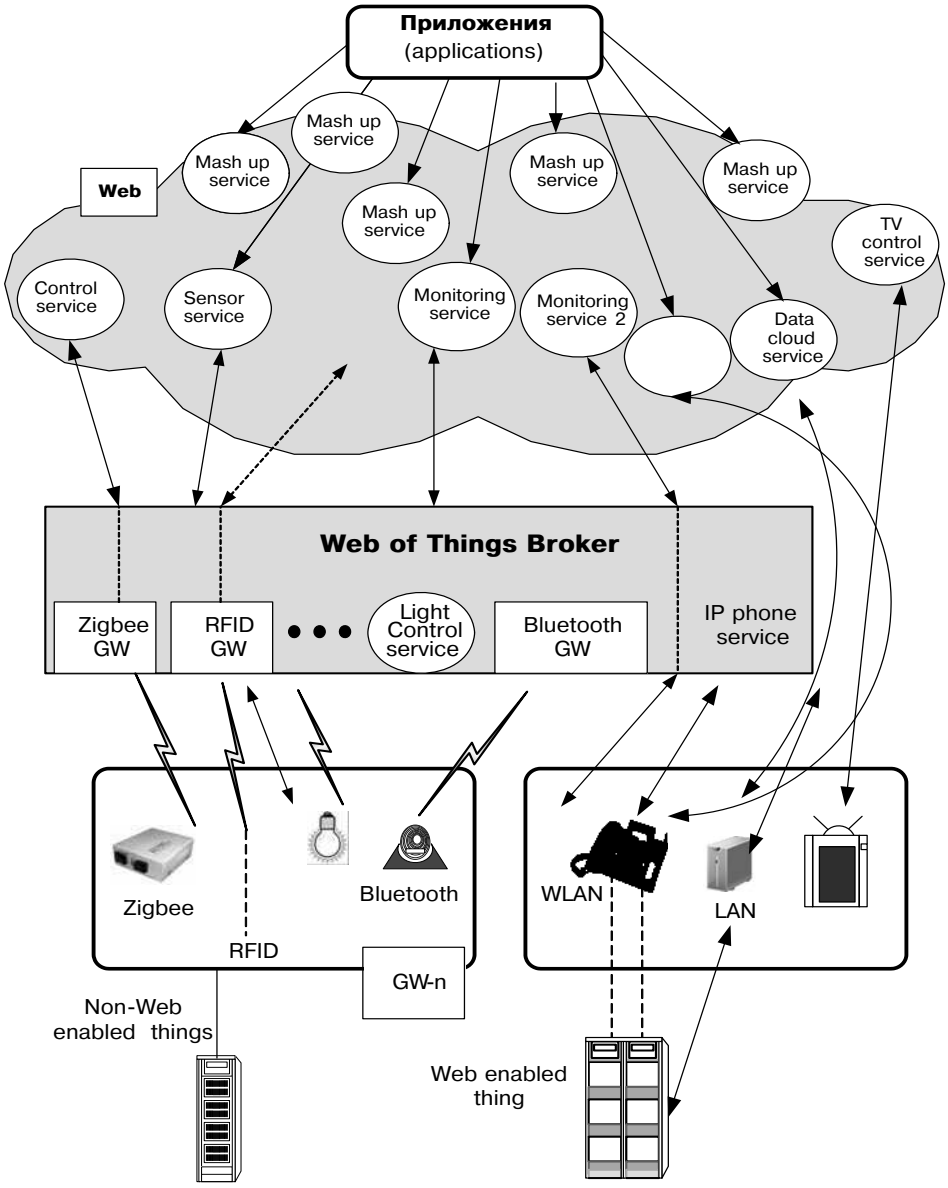

Рис. 2.4. Архитектура Веб вещей

На рис. 2.5 приведена структура M2M [44]. 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 ITU-T существуют предложения, в соответствии с которыми M2M рассматривается как подсистема IoT.

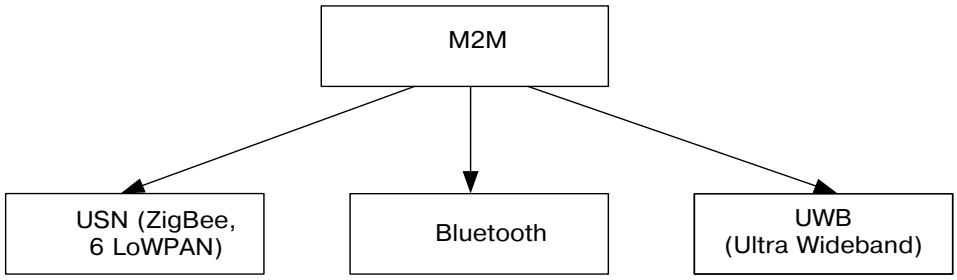

Рис. 2.5. Структура M2M

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. Заметим, что не совсем удачная аббревиатура M2M зачастую заменяется аббревиатурой *D2D (Device-to-Device)*.

В последнее время наибольшую поддержку мирового сообщества получила концепция Интернет вещей [76]. Масштабное внедрение протокола IPv6 с практически безграничным адресным пространством вкупе с применением протокола 6LoWPAN снимает проблему адресации даже для 7 триллионов беспроводных устройств. Сети автомобильного транспорта VANET с учетом прогнозируемого числа автомобилей в Российской Федерации на уровне 60 миллионов на горизонте планирования до 2015 года также органично вписываются в концепцию IoT.

И стандартизация в области медицинских сетей [86, 87] тоже ориентирована на использование принципов IoT. Даже такое уникальное применение, как сеть для книг в библиотечных шкафах [36], рассматривается как часть IoT. Исходя из сказанного, далее в книге мы будем рассматривать концепцию IoT как основу дальнейшего развития инфокоммуникационных сетей.

2.2. Самоорганизация сетей в концепции IoT

Прогноз развития беспроводных технологий показывает, что число разнообразных сенсорных узлов достигнет к 2017 (по некоторым оценкам к 2020) году 7 триллионов. Существующие сегодня сети были построены для обслуживания нескольких миллиардов человек, но никак не нескольких триллионов устройств. Уже несколько лет в мире ведутся исследования, нацеленные на создание принципиально иных, по сравнению с существующими, сетей. Речь идет о самоорганизующихся сетях [12], которые, в отличие от традиционных сетей связи, не имеют конкретной инфраструктуры на протяжении какого-либо (относительно длительного) периода времени.

Самоорганизующейся называется сеть, в которой число узлов является случайной во времени величиной и может изменяться от 0 до некоторого значения N_{max}. 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 в иные сети [14, 16].

Архитектура самоорганизующейся сети представлена на рис. 2.6.

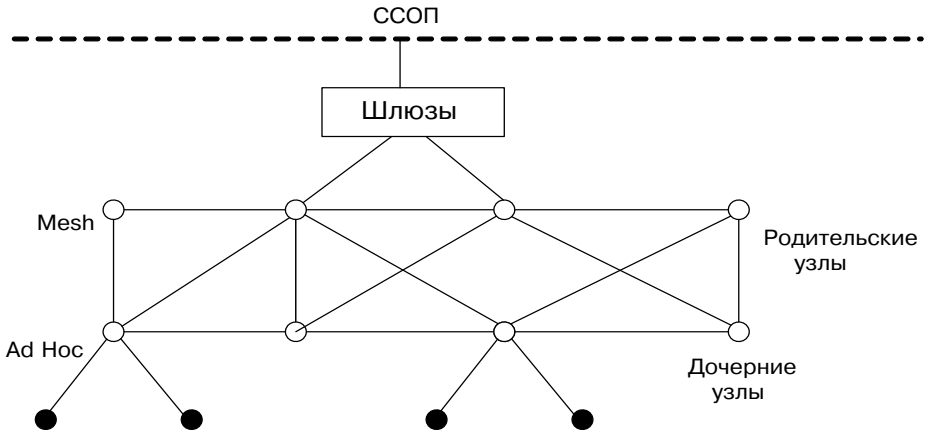

Рис. 2.6. Архитектура самоорганизующейся сети

Самоорганизующаяся сеть, как и все сети связи, состоит из сетей доступа и транзитной сети.

Сеть доступа называется *Ad Hoc* (целевая сеть) [14,33,110,118], а транзитная сеть – *mesh* (ячеистая) [26]. Как видно, из рис. 2.6, 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 сети Ad Hoc, ограниченных в установлении соединения одним шагом (one-hop).

Mesh-узлы достаточно часто называют родительскими узлами, что подчеркивает транзитную функцию такой 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.

Основа концепции IoT – самоорганизующиеся сети. Среди приложений самоорганизующихся сетей можно выделить функционирующие уже сегодня [14]:

- беспроводные (всепроникающие) сенсорные сети (USN);
- сети транспортных средств (VANET – Vehicular Ad Hoc Networks);
- муниципальные сети (HANET – Home Ad Hoc Networks в совокупности с mesh-сетью микрорайона);
- медицинские сети (MBAN – Medicine Body Area Network).

Кроме того, в перспективе прогнозируется и использование самоорганизующихся наносетей, построенных на принципах перемещения вещества.

Далее в книге будут подробно рассмотрены USN, включая примеры приложений военных систем, VANET и молекулярные наносети. В настоящей главе в качестве приложений IoT рассмотрим муниципальные и медицинские сети.

2.3. Муниципальные сети

С точки зрения среднесрочных перспектив развития сети прагматически важными представляются возможности создания домашних Ad Hoc сетей *HANET (Home Ad Hoc Network)* и Mesh-сетей для микрорайонов.

В основе построения домашней сети лежат два дополняющих друг друга процесса: предстоящее широкое распространение беспроводных сенсорных сетей [22] и возможности стандартов IEEE 802.11, IEEE 802.16, IEEE 1900 [62-72], предоставляющих как традиционные NGN-услуги, так и новые, базирующиеся на технологиях Ad hoc и Mesh . Рассмотрим последнее более подробно.

В настоящее время достаточно широко распространены системные и технические решения по предоставлению пакета услуг Triple Play (речь + данные + видео) либо на основе ADSL и её модификаций ADSL2 и ADSL2+, либо на основе доведения оптического кабеля до жилища, в основном, по технологии пассивных оптических сетей *PON (Passive Optic Network).* Обо всем этом говорилось в главе 1.

Последнее из этих двух решений в настоящее время является приоритетным, поскольку, помимо хороших характеристик предоставления услуг для пользователей, дает также заметные преимущества в эксплуатации. Однако появление технических средств WiFi, реализующих стандарт IEEE 802.11n, и планируемое принятие стандарта IEEE 802.11 ac вкупе с решениями альянса WiGig, может существенно дополнить эти системные решения.

Действительно, в проекте стандарта IEEE 802.11ac D5.01 регламентируется скорость передачи свыше 1 Гбит/с на уровне приложений, а в решениях альянса WiGig эта скорость составляет до 7 Гбит/с.

При этом следует отметить, что стандарт WiGig функционирует на частотах свыше 60 ГГц. Не случайно в связи с этим WiFi в рекомендации IEEE 802.11n уже несколько лет назад рассматривался как перспективный способ реализации IPTV. Кроме того, к настоящему времени решен, причем в практической плоскости, вопрос обеспечения гарантированного качества обслуживания при предоставлении услуг передачи речи и видео с использованием технических средств WiFi.

Стандарт IEEE 802.11e предоставляет категории обслуживания *AC (Access Category)*, полностью отвечающие концепции дифференцированных услуг и имеющие соответствие с классами обслуживания рекомендации ITU-T Y.1541 [97].

Введение в стандарте IEEE 802.11e интервала «Возможность передачи без конкуренции» *TXOP (Transmission Opportunity)*» позволяет обеспечить гарантированное качество обслуживания и для речи, и для видео. Период длительности TXOP определяет интервал времени, в течение которого терминал WiFi имеет право инициировать передачу данных через беспроводный канал [12]. Помимо всего вышеуказанного следует отметить, что стоимость точки доступа WiFi в настоящее время колеблется в диапазоне от 50$ до 120 € в зависимости от реализуемых возможностей. Это позволяет предвидеть широкое внедрение точек доступа WiFi в жилищах абонентов и офисах, причем в данном случае точка доступа WiFi является собственностью пользователя.

Перспективы развития беспроводного доступа настолько широки, что в [120] положительно оценивается даже возможность передачи речи поверх протокола Zig Bee.

На рис. 2.7 приведена архитектура домашней Ad Hoc сети, mesh-сети микрорайона и показано их взаимодействие с иными элементами сети связи общего пользования.

В состав домашней сети Ad Hoc входят телефон, компьютер, телевизор – естественно, – все устройства с возможностью взаимодействия с точкой доступа WiFi и являющиеся некими постоянными элементами этой сети, а также разнообразные беспроводные сенсорные узлы, обеспечивающие контроль жизнедеятельности и эксплуатационных характеристик жилища.

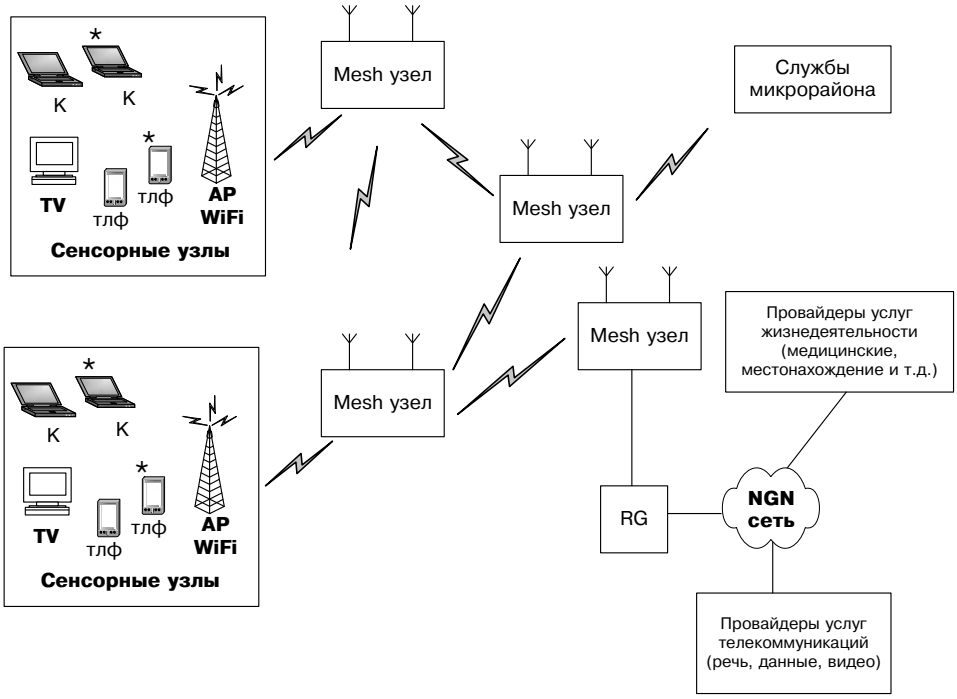

Рис. 2.7. Архитектура домашней сети Ad Hoc

Кроме того, поскольку сеть – Ad Hoc, к ней могут быть временно подсоединены мобильные телефоны и компьютеры гостей, а также мобильные телефоны и компьютеры работников различных служб микрорайона и/или города (на рис. 2.7 отмечены *).

Как видим, такая сеть представляет собой интеграцию решений IoT и существующих инфраструктурных сетей.

Домашние сети Ad Hoc объединены с помощью mesh-маршрутизаторов WiFi (или mesh-маршрутизаторов, выполненных по иной беспроводной технологии) в сеть микрорайона, которая имеет выход на жилищные и эксплуатационные службы микрорайона, а также через абонентские шлюзы *RG (Residental Gateway)* к сети связи общего пользования и далее к провайдерам услуг телекоммуникаций и услуг жизнедеятельности. В такой сети помимо традиционных услуг NGN могут быть предоставлены новые услуги, более точно – даже группы новых услуг, среди которых можно выделить:

- услуги взаимодействия современной бытовой техники и человека;

- услуги обеспечения безопасности жилища, офисов и т.д.;
- услуги мониторинга состояния жилых и рабочих помещений, включая мониторинг освещения, климатических условий, водоснабжения, загазованности и т.д.;
- услуги мониторинга здоровья;
- услуги мониторинга здоровья, местонахождения и адекватности поведения пожилых людей;
- услуги контроля местонахождения детей;
- другие услуги – локального позиционирования в реальном времени RTLS, включая мониторинг дорогостоящих предметов в жилище и оборудования в офисах;
- услуги взаимодействия сотрудников служб микрорайона, района, города при выполнении ими ремонтных и профилактических работ;
- услуги взаимодействия медицинского персонала, находящегося по вызову на дому или в офисе с районной поликлиникой, больницей, медицинскими базами данных;
- услуги вида «Push to Buy» в крупных торговых центрах при создании сетей *SHANET (Shopping Ad Hoc Network);*
- услуги роуминга для пользователей сетей 3G при нахождении этих пользователей в качестве гостей в сети HANET;
- услуги роуминга и доступа в Интернет для пользователей персональными компьютерами и многофункциональными терминалами при нахождении этих пользователей в качестве гостей в сети HANET.

Приведенный список новых услуг неполон, но достаточно многообразен, чтобы уяснить широту охвата жизнедеятельности человека при внедрении муниципальных сетей.

2.4. Медицинские сети

Разработкой стандартов для медицинских сетей занимается рабочая группа IEEE 802.15.6. Основной задачей этой группы является разработка MAC-уровня с поддержкой нескольких физических уровней (PHY) для нательных беспроводных сетей [86]. Целью создания нательных беспроводных сетей *WBAN (Wireless Body Area Network)* является обслуживание разных приложений медицинского направления, например, удаленный контроль состояния здоровья человека. Сенсорные узлы могут располагаться как на теле человека или в не-

посредственной близости от него, так и имплантироваться. Такие сети могут обслуживаться и передаваться с разными скоростями и приоритетами. Наличие различных физических уровней позволяет разным устройствам работать на своей частоте.

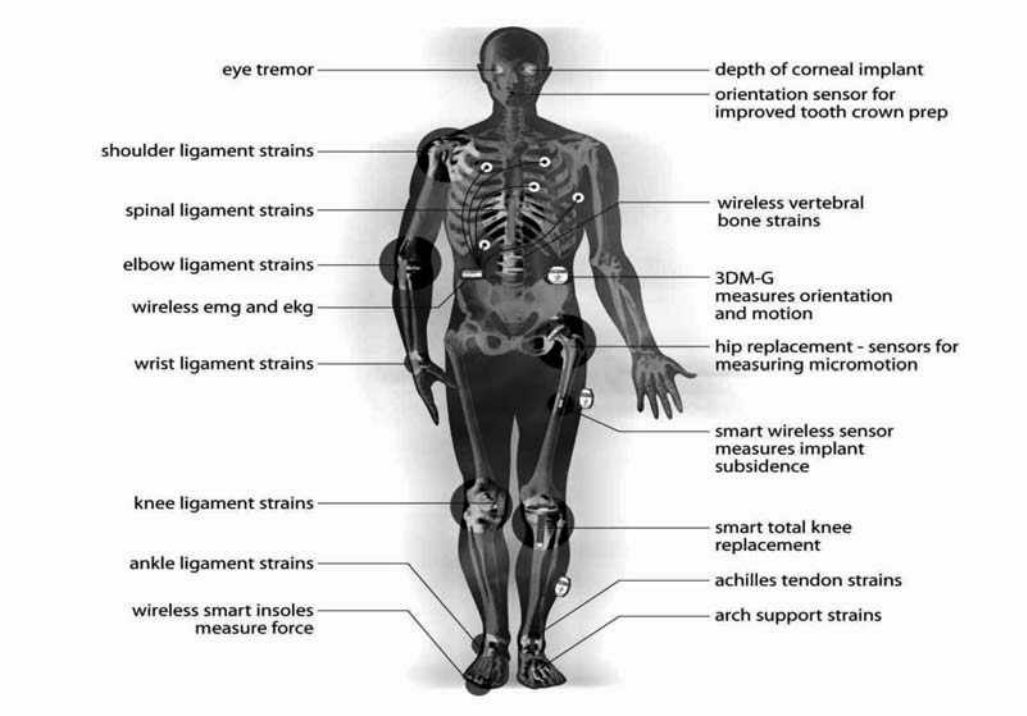

Рис. 2.8. Размещение сенсорных узлов на и в теле человека

На рис. 2.8 [87] приведено размещение возможных сенсорных узлов в соответствии с сегодняшним видением рабочей группы IEEE 802.15.6.

Это сенсорные узлы для измерения тремора глаз, т.е. 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, т.е. регистрация электрической активности мышц, 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, а также 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 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 [10] число сенсоров увеличилось, а качественный состав сенсоров существенно усложнился.

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

Класс 1. Специализированные медицинские приложения:

- носимые,
- имплантируемые.

Класс 2. 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. 2.9.

Для функционирования сети требуется наличие нескольких сенсорных устройств и/или актуаторов, которые связываются с сетевым контроллером *(BAN Network Controller, BNC)*, реализованном, например, в виде телефона, КПК или ноутбука.

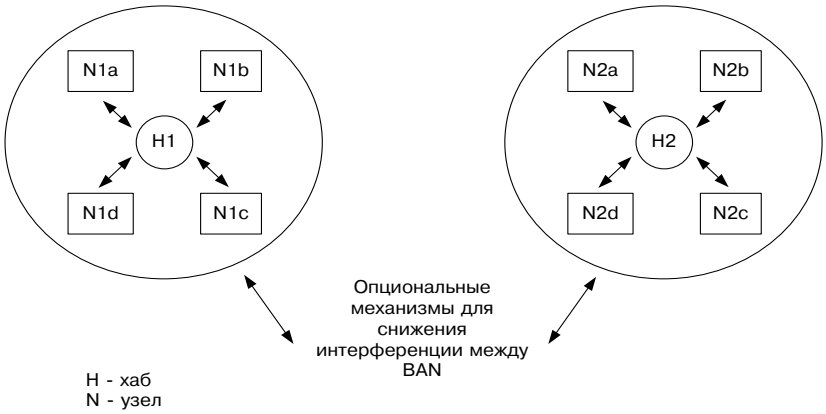

Рис. 2.9. Топология сетей BAN

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

- переменные скорости передачи данных от нескольких кбит/с до нескольких Мбит/с;
- поддержка до 256 устройств;
- сосуществование с другими сетями BAN;
- поддержка механизмов обеспечения защиты передаваемых данных;
- гарантированные пределы задержек;
- гарантированная полоса пропускания.

Текущий проект стандарта IEEE 802.15.6 определяет три возможные реализации физического уровня – узкополосный *NB (Narrowband)*, сверхширокополосный UWB *(Ultra WideBand)* и уровень человеческого тела *HBC (Human Body Communication)*.

Уровнем выше стандарт определяет обобщенный MAC-протокол, обеспечивающий контроль доступа к каналу. Выбор определенного уровня PHY зависит от приложения.

Глава 3
IP Multimedia Subsystem

Лучший способ предсказать будущее состоит в том, чтобы изобрести его.
Алан Кей

3.1. Идея IMS

Э(ре)волюционным переносом в 2010-е идеологии Интеллектуальной сети, упомянутой в главе 1, стала концепция *IMS* (*IP Multimedia Subsystem*) предоставления любой услуги в любом месте пакетной сети NGN. К сожалению, появившись в начале 2000-х, эта концепция несколько опередила время. Как раз тогда чрезмерно надутый инфокоммуникационный пузырь лопнул под грузом несбывшихся надежд, и интерес к IMS был потерян. Теперь же, когда слияния и поглощения Операторов фиксированной связи мобильными Операторами стали способом существования сегодняшнего телекоммуникационного мира, конвергенция сетей и услуг связи вернулась и является образом жизни Операторов, а не желающие поступать таким образом игроки телекоммуникационного рынка весьма скоро перестанут существовать, теперь концепция IMS реальна и своевременна. Именно эта концепция позволяет предоставить любому пользователю любую услугу в любом месте и в любое время.

По сути, это сегодняшняя реализация принципа *ABC* (*Alway Best Connection*) наилучшего соединения с нужной услугой, по наилучшей инфраструктуре доступа, в любое нужное пользователю время и за адекватную стоимость.

При этом вместо пользователя, вынужденного корректировать свое поведение, чтобы соответствовать возможностям инфокоммуникационной сети, сама сеть корректирует свое поведение, чтобы соответствовать развивающимся потребностям мобильного пользователя. Т.е., если в сегодняшних телекоммуникациях пользователь должен постоянно знать об особенностях и ограничениях сети, соответственно адаптировать свое поведение, иметь отдельные номера домашнего и офисного телефонов, факсимильного аппарата в офисе, мобильного телефона и т.п., то с внедрением IMS приходит новая модель, в которой сеть адаптируется к пользователю. Единственный его номер работает для всех типов его терминальных устройств, а сеть «ощущает» ситуацию у пользователя в каждый момент времени и соответствующим образом изменяет свой подход к предоставлению услуг.

По сравнению с традиционной NGN эта концепция развернула границы начавшегося с GSM беспроводного мира, чтобы включить в него проводные сети связи, мир беспроводных LAN и широкополосный беспроводной доступ, мир мобильной телефонии с ее фокусом на мобильность и мир IP с его всепроникающими возможностями. Действительно, современные телекоммуникационные Операторы получают доходы от продажи услуг, а не от предоставления в аренду пользователям ресурсов. Это значит, что более успешным на рынке будет не богатый ресурсами гигант, а эффективный сервис-провайдер с грамотной политикой продвижения своих услуг. С учетом вышеизложенного IMS, возможно, – самое мощное новшество эпохи постNGN среди множества появившихся в отрасли за последние 20 лет, пожалуй, за исключением Интернет вещей. Поэтому авторы и решили посвятить IoT главу 2, а следующую за ней главу – IMS.

3.2. Функциональные преимущества IMS

Как следует из предыдущих параграфов, архитектура IMS отличается от всего, что было до нее. В упомянутых в главе 1 традиционных сетях предоставление услуг и устройства, которые позволяют это делать, рассматриваются как некий монолитный процесс, а в IMS эти устройства видятся больше как набор функций (как и в концепции Интеллектуальной сети, здесь снова отделяется функция от устройства).

И все же из определения IMS следует, что она предназначена для того, чтобы предоставлять Интернет-услуги повсюду и в любое время с использованием технологий сотовых сетей. Но дело в том, что современные сети мобильной связи 3G уже и так могут предоставлять достаточно широкий спектр Интернет-услуг.

В сетях UMTS существуют два домена обслуживания трафика: домен коммутации каналов и домен коммутации пакетов. Домен коммутации каналов в UMTS является эволюционным развитием технологий, уже использующихся в 2.5G, и ориентирован на передачу речи и видео.

Домен коммутации пакетов предоставляет IP-доступ в Интернет. С использованием этих двух доменов пользователь уже может получить различные мультимедийные услуги, в том числе и Интернет-ориентированные. Зачем же тогда разрабатывать IMS? Ответ можно дать такой: чтобы обеспечить *QoS*, *начисление платы, интеграцию и персонализацию различных услуг*. Поясним это. Предоставление разнообразных услуг на базе единой пакетной сети требует гибкой поддержки качества этих услуг. IMS, устанавливая каждое соединение, следит, чтобы пользователям было обеспечено соответствующее качество обслуживания. Другой предпосылкой IMS является усложнение системы начисления платы за мультимедийные сеансы связи.

Если Оператор не принимает во внимание характер трафика мультимедийного сеанса, он может начислить плату за него только очень поверхностным способом – на основании объема переданных данных. При этом пользователю невыгодно пользоваться одними услугами, создающими большой объем трафика, например видео, а Оператору невыгодно предоставлять другие, создающие незначительный объем трафика, например *Instant Messaging* (*IM*). Если Оператор осведомлен о характере передаваемого трафика, то он может использовать в системе начисления платы более эффективные бизнес-модели, несущие выгоду и ему и пользователям.

В IMS применен новый подход к предоставлению услуг, позволяющий Оператору внедрять услуги, созданные сторонними разработчиками или даже самим Оператором, а не производителями телекоммуникационного оборудования. Это позволяет интегрировать различные услуги и предоставляет широкие возможности персонализации и увеличения количества услуг. В 1990-х и 2000-х годах, до внедрения

IMS, в сетях использовались так называемые «вертикальные сервисные платформы», показанные на рис. 3.1, которые успешно справляются с предоставлением небольшого числа ключевых услуг.

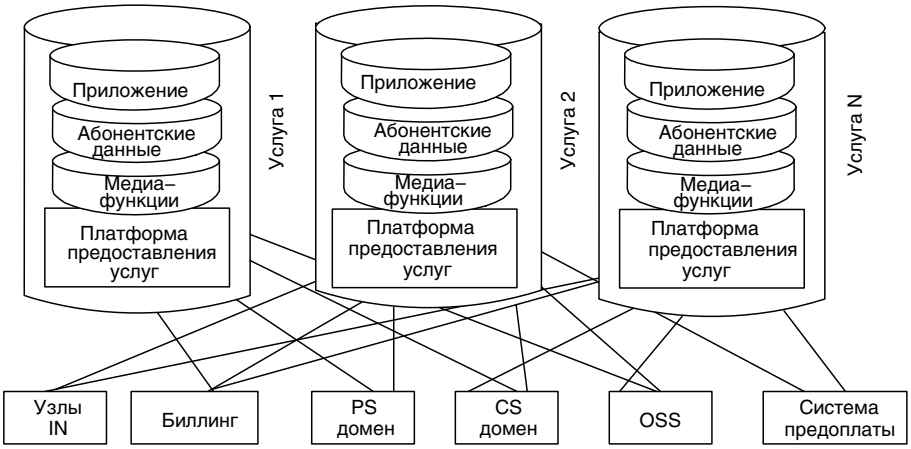

Рис. 3.1. Вертикальные сервисные платформы 2000-х

Подход IMS предполагает горизонтальную архитектуру (рис. 3.2), позволяющую Оператору просто и экономично внедрять новые персонализированные услуги, причем пользователи могут в рамках одного сеанса связи получить доступ к разным услугам. Перечислим некоторые функциональные возможности IMS.

3.2.1. Мультимедийные IP-сеансы

IMS может предоставлять широкий спектр услуг, но одна из них безусловно сохраняет ведущую роль – двусторонняя аудио/видео связь. Для этого архитектура IMS должна поддерживать сеансы мультимедийной связи в IP-сетях, причем такая связь должна быть доступна пользователям как в домашней, так и в гостевой сети. Мультимедийная связь была стандартизована уже в ранних документах 3GPP, еще до появления IMS, но предоставлялась только доменом коммутации каналов.

3.2.2. Качество обслуживания

Поддержка QoS является фундаментальным требованием к IMS. При организации сеанса пользовательское оборудова-

ние извещает IMS о своих возможностях и о своих требованиях к QoS.

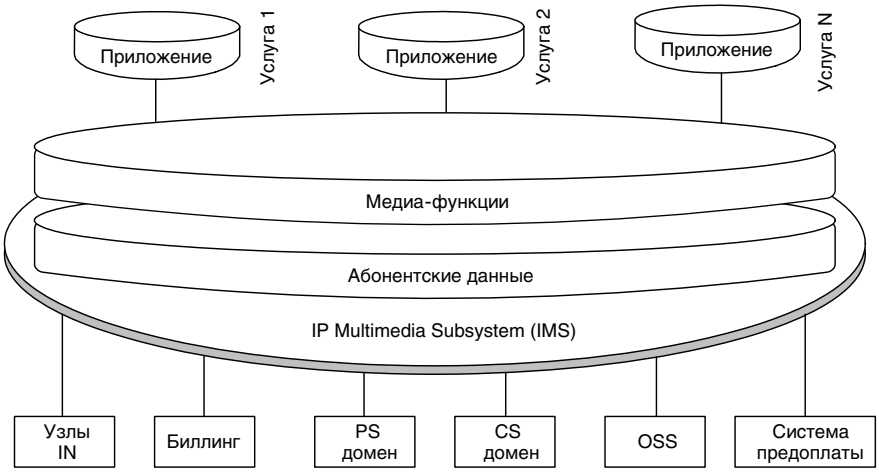

Рис. 3.2. Горизонтальная сервисная IMS-архитектура 2010-х

Как показано в [5], при помощи протокола SIP возможно учесть такие параметры, как тип и направление передачи данных, битовая скорость, размер пакетов, использование RTP, требуемая ширина полосы пропускания. IMS позволяет управлять качеством связи, которое получит тот или иной пользователь, и таким образом дифференцировать пользователей и услуги.

3.2.3. Взаимодействие с другими сетями

Функция поддержки взаимодействия с сетью Интернет очевидна, т.к. благодаря общим протоколам пользователи IMS могут устанавливать мультимедийные сеансы связи с разными службами глобальной сети. Так как переход к тотальному использованию IMS будет постепенным и более или менее длительным, IMS должна также иметь возможность взаимодействия с сетями предыдущих поколений – стационарными и мобильными сетями 1990-х и 2000-х годов с коммутацией каналов и коммутацией пакетов. Функции взаимодействия с сетями коммутации каналов не имеют, разумеется, долгосрочной перспективы, но они абсолютно необходимы в течение долгого периода существования конвергентных сетей.

3.2.4. Инвариантность доступа

Поскольку IP является базовым протоколом доступа в IMS, пользователь может соединиться с сетью множеством способов. Устройства с возможностями IMS могут непосредственно зарегистрироваться в сети IMS независимо от той сети, с которой они соединяются.

Технологии фиксированного доступа, такие как Ethernet LAN, xDSL, HFC (Hybrid Fiber Coax), модемы xDSL, а также беспроводный доступ GSM, GPRS, CDMA, UMTS, WiFi, WiMAX поддерживаются IMS. Точно так же традиционные телефоны ТфОП и некоторые системы VoIP соединяются с сетью IMS посредством соответствующих шлюзов. Таким образом, как и любая IP-сеть, IMS инвариантна относительно протоколов нижних уровней и технологий доступа. Но поскольку 3GPP вначале сконцентрировала свои усилия на эволюции GSM сетей, спецификация первой версии IMS (релиз 5) содержала некоторые GPRS-ориентированные опции. В следующих версиях, уже с шестого релиза, функции доступа были отделены от ядра сети, и началась разработка инвариантности доступа к IMS, получившая название *IP connectivity access* и предполагающая применение любой технологии доступа, которая может обеспечить транспортировку IP-трафика между пользовательским оборудованием и объектами IMS.

3.2.5. Создание услуг и управление услугами

Необходимость быстро внедрять разнообразные услуги, поскольку именно они должны стать основным источником доходов Оператора в XXI веке, потребовала пересмотреть процесс создания услуг в IMS. Чтобы уменьшить время внедрения услуги и обеспечить ее предоставление в гостевой сети, когда пользователь находится в роуминге, в IMS ведется стандартизация не услуг, а возможностей предоставления услуг (*service capability*). Таким образом, Оператор может внедрить любую услугу, соответствующую service capability, причем эта услуга будет поддерживаться и при перемещении пользователя в гостевую сеть, если эта сеть обладает аналогичными стандартизованными service capability. Это достигается благодаря тому, что в IMS принято управление услугой из домашней сети, то есть устройство, имеющее доступ к базе данных пользователей и непосредственно взаи-

модействующее с сервисной платформой, всегда находится в домашней сети.

Для управления услугами Оператор может применять разную *общую политику сети*, распространяющуюся на всех ее пользователей (например, ограничение использования в сети широкополосных кодеков типа G.711), и разную *индивидуальную политику,* распространяющуюся на того или иного пользователя (например, запрет пользования видеосвязью).

3.2.6. Роуминг

Функции роуминга существовали уже в мобильных сетях 2G, и IMS, естественно, эти функции унаследовала. Однако само понятие «роуминг» теперь существенно расширилось и включило в себя:

- GPRS-роуминг – гостевая сеть предоставляет RAN и SGSN, а в домашней находятся GGSN и IMS;
- IMS-роуминг – гостевая сеть предоставляет IP-соединение и точку входа (например P-CSCF), а домашняя сеть обеспечивает все остальные функции;
- CS-роуминг – роуминг между сетью IMS и сетью коммутации каналов.

3.2.7. Защита информации

Функции обеспечения защиты информации необходимы каждой телекоммуникационной системе, и IMS предоставляет уровень защиты, по крайней мере, не меньший, чем GPRS-сети и сети коммутации каналов. IMS производит аутентификацию пользователей перед началом предоставления услуги, предоставляет пользователю возможность запросить конфиденциальность информации, передаваемой во время сеанса, и др.

3.2.8. Начисление платы

Как было отмечено выше, IMS позволяет Оператору или провайдеру услуг гибко назначать тарифы для мультимедийных сеансов. IMS сохраняет возможность начислять плату за сеанс наиболее простым способом – в зависимости от длительности сеанса или от объема трафика, но может также использовать более сложные схемы, учитывающие разную пользовательскую политику, компоненты медиа-данных,

предоставляемые услуги и т.п. Требуется также, чтобы две IMS-сети при необходимости могли обмениваться информацией, нужной для начисления платы за сеанс связи. IMS поддерживает начисление платы в режиме как online, так и offline.

3.3. Архитектура IMS

Для IMS разработана многоуровневая архитектура с разделением транспорта для переноса трафика и сигнальной сети IMS для управления сеансами (рис. 3.3). Таким образом, 3GPP при разработке IMS фактически перенес на мобильные сети основную идеологию Softswitch. Хотя некоторые функции не всегда легко отнести к тому или иному уровню, но такой подход обеспечивает минимальную зависимость между уровнями. В IMS можно выделить:

- User Plane – пользовательский уровень или уровень передачи данных;
- Control Plane – уровень управления;
- Application Plane – уровень приложений.

Прежде чем переходить к детальному рассмотрению элементов IMS-архитектуры, отметим, что 3GPP, по примеру Интеллектуальной сети, а затем Softswitch в IPCC (International Packet Communication Consortium), специфицирует не узлы сети, а функции. Это означает, что IMS-архитектура, как и Интеллектуальная сеть или Softswitch, тоже представляет собой набор функций, соединенных стандартными интерфейсами.

Разработчики вправе комбинировать несколько функций в одном физическом объекте или, наоборот, реализовать одну функцию распределенно, однако чаще всего физическую архитектуру ставят в соответствие функциональной и реализуют каждую функцию в отдельном узле.

Разные функции IMS связываются друг с другом через набор контрольных точек, подобно способу, который был разработан еще в одной упомянутой в главе 1 концепции конца прошлого века – концепции ISDN. Как и в архитектуре ISDN, эталонные точки в IMS используются для идентификации и описания интерфейсов между разными функциональными сетевыми элементами. Функции Call Session Control Function (CSCF), которые находятся в центре рис. 3.3, помещены туда не случайно.

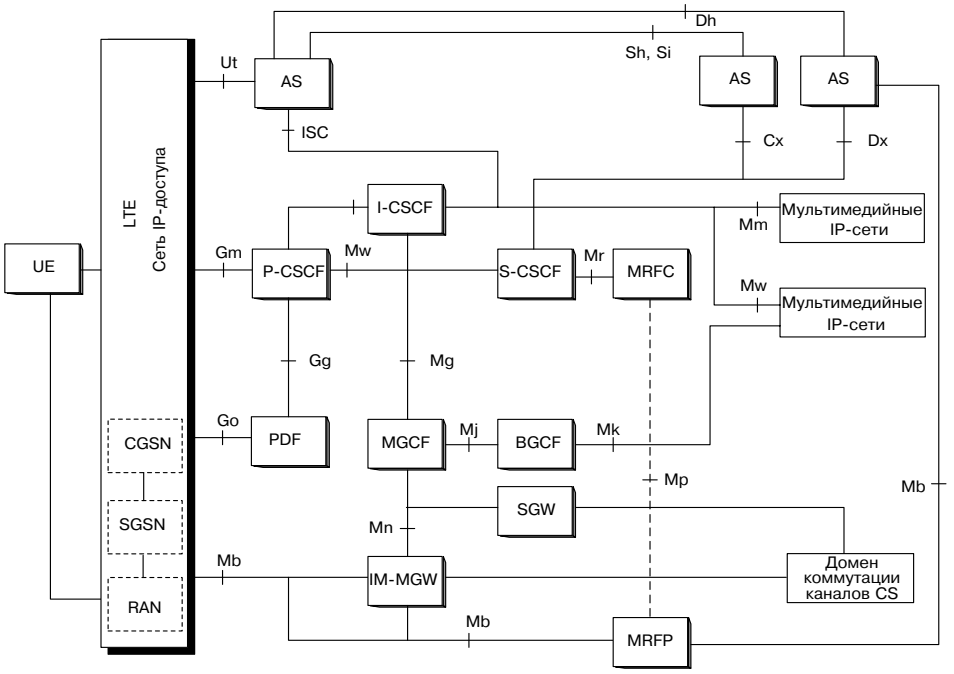

Рис. 3.3. Архитектура IMS

CSCF – сердце и душа IMS – подразделяется на три области ответственности: взаимодействие, обслуживание и управление сеансом прокси. В соответствии с концепцией IMS, каждое сигнальное событие, которое генерирует пользователь, сперва отправляется к прокси-CSCF (P-CSCF) независимо от самого сигнального события, которое может предусматривать такие вещи как запрос сеанса связи, активизацию требуемой функции, выделение сетевого ресурса, запрос обслуживания другим приложением. Таким образом, функция P-CSCF является первым контактом для устройства пользователя в IMS-ядре.

Получив сообщения SIP от пользовательского устройства, P-CSCF пересылает их функции Interrogating Call Session Control Function (I-CSCF) или функции Serving Call Session Control Function (S-CSCF). Функция I-CSCF служит единой точкой регистрации в сети для доступа к услугам IMS как для местных, так и роуминговых пользователей. Как только I-CSCF регистрирует пользователя, S-CSCF вступает во владение и управляет сеансом связи, обеспечивая доступ ко всем требуемым или абонируемым службам.

Важно отметить, что в большинстве случаев I-CSCF ведет себя как SIP-прокси несмотря на то, что ее основная роль в IMS заключается в определении места предоставления услуг. Подчеркнем, что может быть много I-CSCF в пределах сети поставщика услуг, которые ответственны за такие функции, как:

- регистрация, являющаяся процессом назначения S-CSCF;
- управление потоком сеанса, использующееся для того, чтобы направить запрос SIP, который был получен от другой сети, к S-CSCF, или направить запросы SIP от пользователей на разные S-CSCF;
- создание данных в форме Call Detail Records (CDR) для биллинга, генерирующих доход от использования ресурса.

Добавим, что I-CSCF также скрывает топологию, конфигурацию, возможности и емкость сети от посторонних любопытных глаз, т.е. выполняет задачи *межсетевого шлюза, скрывающего топологию* (*Topology Hiding Internetwork Gateway, THIG*).

В действительности, S-CSCF является прокси-сервером SIP, который сеанс за сеансом выполняет управление вхождением в связь абонентов сетевой службы. Он управляет взаимодействием с базами данных сети, такими как *домашний абонентский сервер HSS* для поддержки мобильных пользователей и серверов *аутентификации, авторизации и учета AAA*. В этом качестве S-CSCF также передает сигнальный трафик, генерируемый пользователями роуминга (то есть, пользователями, которые подсоединены к сети в качестве гостей) в их домашние сети, где сохраняется профиль абонентов и откуда присылаются подтверждения их платежеспособности (billability). Как только S-CSCF выполнил свои обязанности проверки пользователя, запрашивающего обслуживание, запрос может быть передан соответствующим серверам приложений и шлюзам, которые требуются для организации запрашиваемого сеанса. Если запрос предназначается для другой сети, то вполне вероятно, что придется применить другую сигнализацию, осуществить преобразование протокола, организовать взаимодействие с другими типами медиа в других сетях.

Центральным для работы IMS является P-CSCF, причем по мере развития архитектуры IMS его обязанности трансформировались. Первоначально P-CSCF нес ответственность за

функцию выбора политики обслуживания PDF (*Policy Decision Function*), которая накапливает, хранит, управляет и обращается к архивированным политикам, чтобы принять решения, связанные с запросами распределения ресурсов IP. По мере развития архитектуры IMS, после ряда дискуссий PDF была выведена из области P-CSCF, чтобы сделать ее более доступной для беспроводных LAN и других сетей доступа. Что же касается элементов P-CSCF, то в силу их роли «привратника» и того факта, что они идеально подходят для сбора данных о сессиях, P-CSCF генерируют записи биллинга, которые могут быть накоплены и переданы *централизованной функции Charging Gateway Function* (*CGF*) перед генерацией пользовательских счетов.

По существу, функции IMS и эталонные точки, описанные здесь, разрабатываются, чтобы обеспечить сигнализацию между устройствами и контролировать доступность и расположение функций и услуг на базе сети. Эти функции и услуги не создаются или поставляются IMS; а просто IMS служит архитектурой, позволяющей сети предоставить их с заданным качеством. Фактически, цель IMS состоит в том, чтобы предоставить ряд услуг, комбинирующих лучшее из того, что есть в унаследованной IMS телефонной сети (согласно главе 1) и лучшее из того, что должна предложить Интернет (включая и инновации главы 2). Кроме того, IMS облегчает предоставление услуг пользователям независимо от их местонахождения, используемого пользовательского устройства или способа доступа. Так как IMS базируется на открытых стандартных протоколах IP и создавалась для мира услуг мобильной и фиксированной связи, она легко сочетает лучшее из Интернет с лучшим из сетей NGN, чтобы объединить эти две территории.

3.4. Пользовательские базы HSS и SLF

Две основные сетевые базы данных обеспечивают поддержку IMS: *сервер абонентов домашней сети HSS* (*Home Subscriber Server*) и *функция местонахождения абонента SLF* (*Subscriber Location Function*). Каждая IMS-сеть содержит один или более серверов пользовательских баз данных HSS. По сути, HSS представляет собой централизованное хранилище информации об абонентах и услугах и является эволюционным развитием *HLR* (*Home Location Register*) из архитектуры сетей GSM. В HSS хранится вся информация, ко-

торая может понадобиться при установлении мультимедийного сеанса: информация о местонахождении пользователя, информация для обеспечения защиты (аутентификация и авторизация), информация о пользовательских профилях, об обслуживающей пользователя S-CSCF, о триггерных точках обращения к услугам. Функции, выполняемые HSS, показаны в общем виде на рис. 3.4.

В HSS размещается информация о пользователе, необходимая сети для поддержки всех функций IMS, связанных с обработкой вызова и установлением сеанса. В числе прочего он содержит информацию об абонировании услуг (часто называемую профилями пользователей) и обеспечивает данные, требующиеся для аутентификации и авторизации пользовательского доступа к услугам.

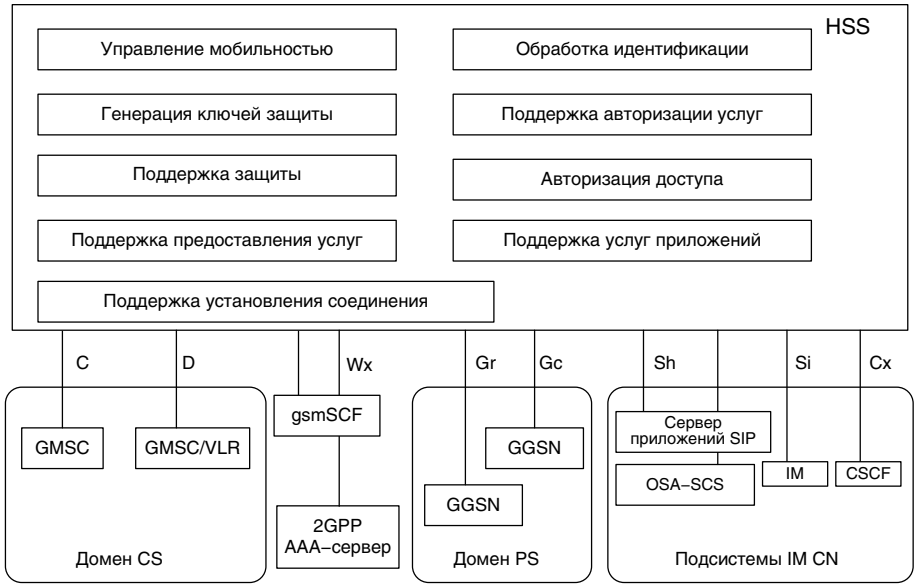

Рис. 3.4. Логические функции HSS

На основе записей в базе данных идентифицируется, к каким услугам пользователь имеет доступ, с какой сетью он в настоящий момент соединен. HSS поддерживает также локализацию пользователя подобно *домашнему регистру местонахождения HLR* и *визитному регистру местонахождения VLR* в мобильных системах предыдущих поколений.

Сеть может содержать более одного HSS в том случае, если количество абонентов слишком велико, чтобы поддер-

живаться одним HSS. Такая сеть, наряду с несколькими HSS, должна будет иметь в своем составе функцию SLF, представляющую собой простую базу данных, которая хранит данные о соответствии информации HSS адресам пользователей. Узел, передавший к SLF запрос с адресом пользователя, получает от нее сведения о том HSS, который содержит информацию об этом пользователе. Как HSS, так и SLF используют для взаимодействия с прочими элементами IMS *протокол Diameter* [4].

3.5. Функция SIP-сервера

Первым сервером CSCF, который упоминался в параграфе 3.2 при обсуждении архитектуры IMS, является прокси-CSCF, который представляет собой начальную точку взаимодействия (на сигнальном уровне) пользовательского IMS-терминала и IMS-сети. Она может быть расположена в разных местах, в пределах домашней сети или в пределах сети, с которой временно соединено визитное устройство. В большинстве случаев P-CSCF находится в гостевой сети, если эта гостевая сеть абсолютно совместима с IMS; в противном случае она «обнаруживается», обычно с помощью DHCP, и используется в домашней сети, совместимой с IMS.

С точки зрения SIP, она является входящим/исходящим прокси-сервером, через который проходят все запросы, исходящие от IMS-терминала или направляемые к нему. Однако P-CSCF может вести себя и как агент пользователя UA, что необходимо для прерывания сеансов в нестандартных ситуациях, и для создания независимых SIP-транзакций, связанных с процессом регистрации.

P-CSCF прикрепляется к терминалу пользователя при регистрации в сети и не заменяется в течение всего срока регистрации. Основным назначением P-CSCF является маршрутизация запросов и ответов SIP между пользовательским терминалом и узлами IMS-сети (I-CSCF, S-CSCF и др.).

P-CSCF выполняет также ряд требований, относящихся к обеспечению защиты. Она устанавливает несколько ассоциаций IPsec, обеспечивающих целостность информации, передаваемой к IMS-терминалу. Создание этих ассоциаций предусматривает аутентификацию пользователя, и выполнив ее, P-CSCF извещает об этом пользователе остальные узлы

сети, чтобы им не нужно было повторно выполнять ту же процедуру.

В задачи P-CSCF входит и проверка правильности построения сообщений SIP, передаваемых IMS-терминалом. Кроме того, P-CSCF производит компрессию и декомпрессию сообщений SIP для того, чтобы ускорить время их передачи по узкополосным каналам (например, на радиоучастке) и, тем самым, уменьшить время установления соединения или предоставления услуги. К тому же, P-CSCF обнаруживает запросы соединений с аварийными службами и либо сообщает об ошибке (релиз 5), либо выбирает S-CSCF, необходимую для организации такой связи. Еще одной задачей P-CSCF является создание учетной информации и отправка ее к узлу, отвечающему за начисление платы. Чтобы обеспечивались масштабируемость и надежность, IMS-сеть обычно содержит несколько P-CSCF, каждая из которых обслуживает некоторое количество IMS-терминалов, зависящее от емкости узла. IMS-архитектура предусматривает, что P-CSCF может находиться как в домашней, так и в гостевой сети. Если сеть базируется на технологии GPRS, то P-CSCF должна находиться там же, где и *GGSN* (*Gateway GPRS Support Node*), т.е. в домашней сети, но по мере распространения IMS это условие не будет обязательным для обоих узлов.

Выбор QoS и управление QoS являются еще одной функцией, которую P-CSCF может выполнять как составную часть своего процесса реализации политики. В пределах этой области ответственности у него есть возможность выбирать нужные варианты политики использования приложения и ресурсов сети, авторизовать доступ к сетевым ресурсам, управлять QoS, организовывать COPM. Наконец, у P-CSCF есть возможность собирать данные, которые требуются для функций биллинга.

Теперь перейдем к рассмотрению *I-CSCF* – еще одного SIP-прокси, расположенного на границе административного операторского домена. Когда SIP-сервер определяет следующую пересылку некоторого SIP-сообщения, он получает от службы DNS адрес I-CSCF соответствующего домена. Кроме исполнения функций SIP-прокси, I-CSCF взаимодействует по протоколу Diameter с HSS и SLF, получает от них информацию о местонахождении пользователя и об обслуживающей его S-CSCF. Если S-CSCF еще не назначена, I-CSCF производит ее назначение.

Дополнительно I-CSCF может шифровать части SIP-сообщений, содержащие важную информацию о домене, такую как число серверов в домене, их DNS-имена и т.п. Эта группа функций называется *THIG* (*Topology Hiding Inter-network Gateway*) – межсетевой шлюз сокрытия топологии.

Поддержка THIG опциональна и не всегда нужна; в частности она не требуется, если провайдер на границе своей сети устанавливает *пограничный контроллер SBC* (*Session Border Controller*). Обычно, чтобы обеспечивалась масштабируемость и надежность, в сети присутствует несколько I-CSCF. Типичным местонахождением I-CSCF является домашняя сеть, однако в ряде специфических случаев, таких как поддержка THIG, она может быть вынесена и в гостевую сеть. И, наконец, обслуживающая функция *S-CSCF* – центральная интеллектуальная функция на сигнальном уровне, т.е. функция SIP-сервера, который управляет сеансом. Помимо функции SIP-сервера, S-CSCF выполняет функцию *регистрирующего сервера сети SIP* (*SIP-registrar*), то есть поддерживает привязку местонахождения пользователя (например, IP-адресом терминала, с которого пользователь получил доступ в сеть) к его SIP-адресу *PUI* (*Public User Identity*).

Аналогично I-CSCF, S-CSCF взаимодействует по протоколу Diameter с HSS, получает от него данные аутентификации пользователя, пытающегося получить доступ к сети, и данные о профиле пользователя, то есть перечень доступных ему услуг – набор триггерных точек для маршрутизации сообщения SIP к серверам приложений. В свою очередь, S-CSCF информирует HSS о том, что этот пользователь прикреплен к нему на срок своей регистрации, и о срабатывании таймера регистрации.

Вся сигнальная информация SIP, передаваемая и принимаемая пользовательским IMS-терминалом, проходит через S-CSCF, к которой прикреплен пользователь. S-CSCF анализирует каждое сообщение и определяет, должно ли оно, по пути к пункту назначения, пройти через серверы приложений, предоставляющие пользователю услуги.

S-CSCF поддерживает сеанс в течение всего времени его продолжения и, по мере надобности, взаимодействует с сервисными платформами и с функциями начисления платы. Одной из основных функций S-CSCF является маршрутизация SIP-сообщений. Если пользователь набирает телефонный

номер вместо SIP URI, то S-CSCF производит преобразование номера формата E.164 в соответствии с RFC3761. Начиная с Release 6, S-CSCF занимается также выбором центра аварийной службы, когда провайдер поддерживает подобные сеансы. Для обеспечения масштабируемости и надежности в сети могут находиться несколько S-CSCF, причем они всегда располагаются в домашней сети.

Функция *Policy Decision Function* (*PDF*) иногда интегрируется с P-CSCF, но может быть реализована отдельно. Эта функция отвечает за выработку политики на основании информации о характере сеанса и о передаваемом трафике (транспортные адреса, ширина полосы и т.д.), полученной от P-CSCF. На базе этой информации PDF принимает решение об авторизации запросов от GGSN и производит повторную авторизацию при изменении параметров сеанса, а также может запретить передачу определенного трафика или организацию сеансов некоторых типов.

3.6. Серверы приложений

Серверы приложений AS (*Application Server*), по существу, не являются элементами IMS, а работают как бы поверх нее, предоставляя услуги в сетях, построенных согласно IMS-архитектуре.

Серверы приложений взаимодействуют с функцией S-CSCF по протоколу SIP. Основными функциями серверов приложений являются обслуживание и модификация SIP-сеанса, создание SIP-запросов, передача тарификационной информации в центры начисления платы за услуги. Серверы приложений могут быть очень разными, но в IMS принято выделять три типа серверов: SIP AS, OSA-SCS, IM-SSF.

Рассмотрим эти три типа серверов приложений:

- *SIP AS* (*SIP Application Server*) – классический сервер приложений, предоставляющий мультимедийные услуги на базе протокола SIP;
- *OSA-SCS* (*Open Service Access – Service Capability Server*) предоставляет интерфейс к серверу приложений OSA и функционирует как сервер приложений со стороны S-CSCF и как интерфейс между сервером приложений OSA и OSA API – с другой стороны;

- *IM-SSF* (*IP Multimedia Service Switching Function*) позволяет использовать в IMS услуги *CAMEL* (*Customized Applications for Mobile Network Enhanced Logic*), разработанные для GSM сетей, а также позволяет управляющей функции *gsmSCF* (*GSM Service Control Function*) управлять IMS-сеансом. Со стороны S-CSCF сервер IM-SSF функционирует как сервер приложений, а с другой стороны – как функция *SSF* (*Service Switching Function*), взаимодействующая с gsmSCF по протоколу CAP.

Помимо обязательного для серверов приложений всех типов SIP-интерфейса со стороны IMS, они могут также иметь интерфейсы к HSS, причем SIP AS и OSA-SCS взаимодействуют с HSS по протоколу Diameter для получения данных о пользователе или для обновления этих данных в HSS, а информационный обмен между IM SSF и HSS ведется по протоколу MAP (рис. 3.5).

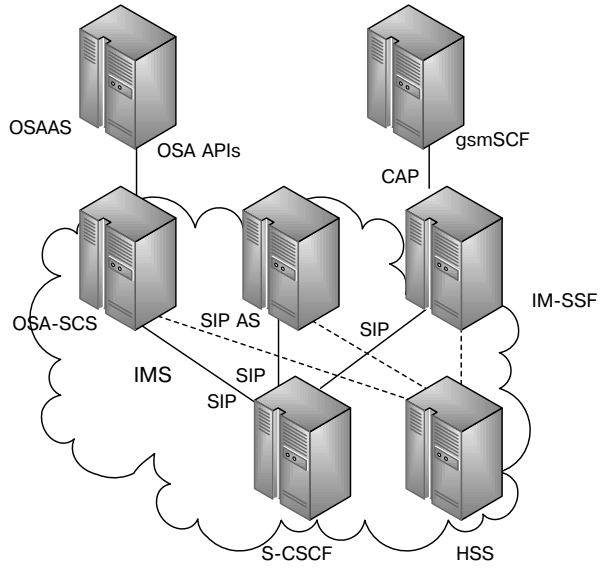

Рис. 3.5. Серверы приложений

Серверы приложений могут находиться либо в домашней, либо в любой другой сети, с которой у провайдера есть сервисное соглашение. Но если сервер приложений находится во внешней сети, он не может иметь интерфейс с HSS.

Следует заметить, что IMS предусматривает также основанный на SIP единый интерфейс, известный как *интерфейс*

IMS Service Control (*ISC*). Этот интерфейс ISC позволяет приложениям, размещенным в Parlay/OSA, SIP и CAMEL, взаимодействовать через интерфейс с ядром IMS.

3.7. Медиасерверы MRF

Функции медиасервера в IMS отданы логическому компоненту, известному как *Media Resource Function* (*MRF*), который служит источником медиа-информации в домашней сети, позволяет воспроизводить мультимедийные объявления, смешивать медиа-потоки, транскодировать битовые потоки кодеков, получать статистические данные и анализировать медиа-информацию. Функции MRF делятся на две части:

- *MRFC – Media Resource Function Controller*
- MRFP – *Media Resource Function Processor*

MRFC находится на сигнальном уровне и взаимодействует с S-CSCF по протоколу SIP. Используя полученные инструкции, MRFC управляет по протоколу MEGACO/H.248 процессором MRFP, находящимся на уровне передачи данных, а тот выполняет все манипуляции с медиа-информацией. Сами MRF всегда находятся в домашней сети.Теперь рассмотрим Media Resource Function, являющуюся *BGCF* (*Breakout Gateway Control Function*). Это SIP-сервер, способный выполнять маршрутизацию вызовов на основе телефонных номеров.

BGCF используется только в тех случаях, когда сеанс инициируется IMS-терминалом, а адресатом является абонент сети с коммутацией каналов (например, ТфОП или мобильной сети 2G). Основными задачами BGCF является выбор той IMS-сети, в которой должно происходить взаимодействие с сетью коммутации каналов, или выбор подходящего PSTN/CS шлюза, если это взаимодействие должно происходить в сети, где находится сам сервер BGCF. В первом случае BGCF переводит сеанс к BGCF выбранной сети, а во втором – к выбранному PSTN/CS шлюзу.

3.8. Шлюз PSTN/CS

Шлюз *PSTN/CS Gateway* (рис. 3.6) поддерживает взаимодействие IMS-сети с ТфОП и доменом CS, реализованных на основе технологии с коммутацией каналов, и позволяет устанавливать соединения между пользователями этих сетей.

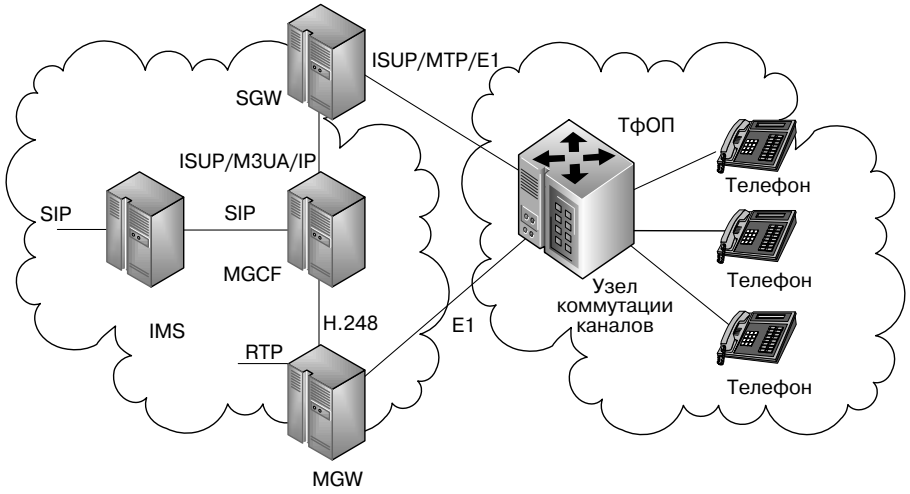

Рис. 3.6. Шлюз PSTN/CS

Шлюз PSTN/CS имеет распределенную структуру, характерную для архитектуры Softswitch:

- SGW – Signaling Gateway;
- MGCF – Media Gateway Control Function;
- MGW – Media Gateway.

Рассмотрим элементы шлюза PSTN/CS несколько подробнее. Шлюз сигнализации *SGW* представляет собой интерфейс для связи с уровнем сигнализации в сети коммутации каналов, производит преобразование нижних протокольных уровней систем сигнализации для двустороннего сигнального обмена между сетью IP и сетью ТфОП. При этом SGW никак не обрабатывает сообщения прикладного уровня.

Функция управления медиа-шлюзом – центральная часть распределенного шлюза PSTN/CS. Она преобразует сообщения ISUP, которые поступают со стороны ТфОП, в сообщения SIP, которые IMS использует для управления сеансом связи через границу между сетями (рис. 3.7). Кроме мэппинга сигнальных протоколов, MGCF управляет по протоколу MEGACO/H.248 ресурсами медиа-шлюза, участвующего в создании соединения.

Транспортный шлюз MGW соединяет сеть IP с сетью коммутации каналов на уровне передачи трафика, выполняя двустороннее преобразование пользовательского трафика, проходящего через границу между сетями.

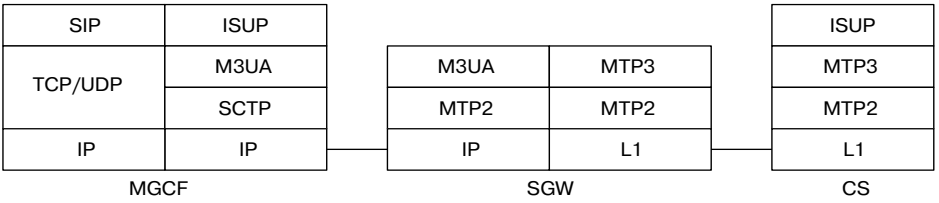

Рис. 3.7. Управление сеансом связи

Со стороны IMS-сети шлюз MGW ведет передачу и прием данных в виде RTP-пакетов, а со стороны сети с коммутацией каналов реализует стандартный TDM-интерфейс. Кроме того, MGW может производить транскодирование информации, если в IMS и в сети коммутации каналов используются разные речевые кодеки (обычно в IMS используется AMR, а в ТфОП используется G.711).

3.9. Шлюз защиты SEG

Для того чтобы защитить уровень управления в *домене защиты* (*security domain*), представляющем собой область сети, которая принадлежит одному провайдеру услуг, и в которой действуют единые административные правила и сетевая политика, трафик на входе в этот домен и на выходе из него будет проходить через шлюз защиты *SEG* (*Security Gateway*). Как правило, границы домена защиты совпадают с границами сети провайдера, а шлюзов SEG в сети провайдера обычно присутствует несколько. В качестве SEG часто выступают пограничные контроллеры SBC.

3.10. Опции оплаты и биллинга в IMS

В области предоставления услуг есть два признанных варианта реализации биллинга:

- *рекуррентный биллинг*, иногда называемый *офлайновым* или *автономным биллингом*, обычно применяющийся к пользователям, которые получают счета каждый месяц за услуги, полученные в предыдущий расчетный период;
- основанный на транзакции биллинг, иногда называемый онлайновым биллингом или биллингом на основе кредитования, применяющийся к клиентам с предоплатой, кото-

рые получают счета за услуги по принципу «транзакция-за-транзакцией».

Можно использовать и тот, и другой принцип в одном сеансе; например, клиент может платить помесячно за передачу речи, но может захотеть начисления платы за те транзакции, когда он загружает фильм или вызывает расширенную услугу.

В существующих сегодня тарификационных ситуациях все компоненты сети IMS – различные CSCFs, BGCF, функция управления медиаресурсами MRCF, MGCF, серверы приложений – собирают информацию по учету их использования, а затем отправляют эту информацию *функции коллектора оплаты* (*CCF*), которая создает *запись данных о начислении платы* и отправляет ее биллинговой системе, а та, в свою очередь, генерирует счет-фактуру для пользователя.

В IMS каждому установленному сеансу присваивается *идентификатор оплаты IMS* (*ICID*), который однозначно определяет сеанс. Дополнительно определяется информация о сетях источника и адресата в целях биллинга и идентификации услуги.

Это также важно для пользователя в роуминге: поскольку разные домены сети имеют свои собственные системы биллинга, важно, чтобы они обменивались данными об использовании, чтобы гарантировать, что деталями роуминга можно обменяться для обеспечения надлежащего биллинга.

В биллинговых ситуациях на базе транзакции обслуживающая CSCF связывается с функцией *начисления платы за сеанс* (*SCF*), которая смотрит на сеть как сервер приложений SIP. Если клиент исчерпывает доступный кредит во время сеанса, SCF имеет возможность приказать S-CSCF завершить сеанс в связи с «недостаточностью фондов».

Как и другие коммуникационные функции в пределах области IMS, протоколы DIAMETER управляют всеми действиями AAA [4]. Функция начисления платы за события (ECF) собирает данные о транзакциях от серверов приложений.

Одну из опций для основанного на транзакциях начисления платы называют *непосредственным начислением платы за события* (*IEC*) или *непосредственным начислением платы за транзакции* (*ITC*).

Когда вызвано IEC, оно вычитает кредит из счета клиента, после чего дает разрешение функции предоставления услуг

(серверу приложений, например) предоставить требуемое обслуживание.

Одну из опций, которая может быть вызвана, называют *начисление платы* за события с резервированием компонента, при ней ECF резервирует определенную сумму в счете клиента, после чего авторизует требуемую услугу. Когда предоставленная услуга заканчивает работу, число использованных кредитов вычитается из счета, и запись о резервированных кредитах удаляется.

3.11. Идентификация в IMS

В любой сети связи необходима идентификация пользователей или пользовательских терминалов, по крайней мере для того, чтобы устанавливать соединения между пользователями, однозначно определенными с помощью идентификаторов. Кроме того, при предоставлении разных услуг зачастую необходимо идентифицировать сами услуги. В этом параграфе мы рассмотрим вопросы идентификации пользователей и услуг в IMS.

Основным идентификатором, присваиваемым пользователю, является *Private User Identity* (*PrUI*). Он имеет формат *NAI* (*Network Access Identifier*), определенный в RFC 2486. Формат выглядит следующим образом: `username@operator.com`.

Заметим, что PrUI используются для идентификации пользователя и для его аутентификации, но в отличие от телефонных номеров в ТфОП, не служат для маршрутизации. Сравнивая сети IMS с 2G, можно провести параллель между PrUI и *IMSI* (*International Mobile Subscriber Identifier*). Пользователю не обязательно знать свой идентификатор PrUI, он может храниться на идентификационной карте, о которой речь пойдет ниже.

Релиз 5 3GPP предписывал каждому пользователю иметь один уникальный PrUI, но в релизе 6 это ограничение убрано, и теперь пользователь может иметь несколько разных PrUI. И хотя на одну идентификационную карту, используемую в UMTS, по-прежнему можно поместить только один PrUI, пользователь может иметь несколько таких карт и несколько терминалов, что в комбинации с использованием другого идентификатора, а именно, *Public User Identity* (*PuUI*), предоставляет пользователю большую гибкость выбора адресов.

Каждому PrUI Оператор ставит в соответствие один или несколько PuUI, имеющих формат SIP URI по RFC 3261 или TEL URL по RFC 2806. В IMS идентификатор PuUI используется для маршрутизации сигнальных SIP-сообщений и в качестве контактной информации для других абонентов. Можно и тут провести параллель с идентификатором *MSISDN* (*Mobile Subscriber ISDN Number*) мобильных сетей 2G.

Когда PuUI представлен в формате SIP URI, он имеет вид `sip:alexander@operator.com`. В SIP URI можно поместить телефонный номер – `sip:+7-812-960-6293@operator.com;user=phone`. Этот формат необходим, поскольку для регистрации протокол SIP требует наличия SIP URI, и, следовательно, нельзя зарегистрировать TEL URL, но можно зарегистрировать SIP URI, содержащий телефонный номер.

С другой стороны, чтобы пользователь мог вызывать терминалы сети связи общего пользования и принимать вызовы от них, он должен иметь TEL URL, имеющий вид `tel:+7-812-960-6293`.

Таким образом, пользователю обычно требуется минимум два разных PuUI. Другая причина иметь несколько PuUI – привлекательная для пользователя возможность иметь разные номера для разных контактов или услуг.

Идентификационная карта IMS-терминала *UICC* (*Universal Integrated Circuit Card*) хранит один PrUI и, как минимум, один PuUI. Полная структура взаимосвязи нескольких PrUI и PuUI хранится в абонентском профиле HSS. Пример такой структуры приведен на рис. 3.8.

Заметим, что UICC – термин, означающий сменную идентификационную карту, имеющую стандартизованный интерфейс с терминалом, а физически карта UICC может содержать несколько логических приложений, таких как хорошо известный *SIM* (*Subscriber Identity Module*), используемый при идентификации пользователей сетей GSM, *USIM* (*Universal Subscriber Identity Module*), который применяется для идентификации в сетях UMTS, и *ISIM* (*IP Multimedia Services Identity Module*) – наиболее важное приложение в контексте этой главы, поскольку служит для идентификации, авторизации и конфигурации терминала при работе в IMS-сети.

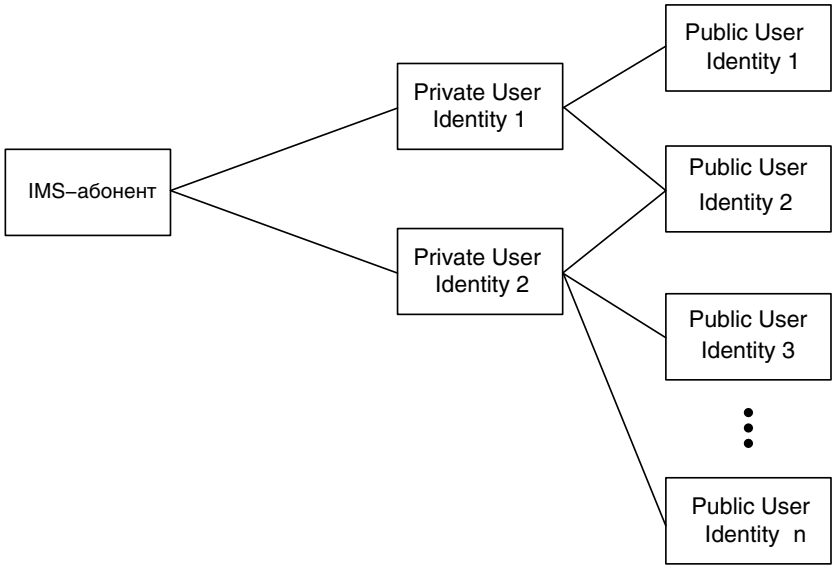

Рис. 3.8. Идентификация IMS-абонентов

Получить доступ к услугам IMS пользователь может только при условии, что в его UICC содержится USIM или ISIM, причем использование последнего предпочтительнее. Структура ISIM приведена на рис. 3.9.

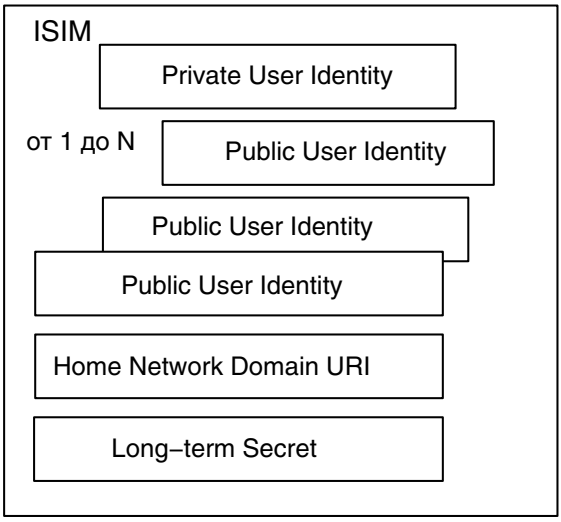

Рис. 3.9. Модуль ISIM

Home Network Domain URI – SIP URI, определяющий имя домашней сети. Он используется для поиска домашней сети при регистрации. В ISIM может храниться только один Home Network Domain URI.

Long-term Secret – поле, используемое в целях аутентификации, проверки целости, расчета ключей шифрования. Поля всех идентификаторов доступны терминалу только для чтения. Чтобы рассказ об идентификации в IMS приобрел некую полноту, упомянем еще об одном идентификаторе – *Public Service Identity* (*PSI*), – появившемся только в 3GPP Release 6. В отличие от описанных выше идентификаторов, PSI присваивается не пользователям, а услугам, размещенным на серверах приложений. Так же, как и PuUI, идентификаторы PSI могут иметь формат SIP URI или TEL URL.

3.12. IMS в стационарных сетях

Хорошо проработанные спецификации IMS, а также успешное внедрение IMS рядом Операторов мобильных сетей, привлекли внимание к этой архитектуре Операторов стационарных сетей.

Основным моментом, выгодно отличающим IMS от других концепций построения сетей NGN, является как раз наличие стандартов, которые дают возможность иметь единообразные и поэтому способные эффективно взаимодействовать сети. До появления архитектуры IMS в 3GPP определенные работы велись и в других упомянутых в книге стандартизующих организациях. В ETSI и в ITU-T разрабатывались элементы архитектуры NGN, в IETF стандартизировались протоколы, в MSF и в IPCC решались вопросы по Softswitch, в DSL Forum создавались спецификации для своей области, но никто не брался за создание целостной системы. И только в 3GPP «почти случайно» создали завершенную систему NGN, концепция которой включает в себя архитектуру, аспекты начисления платы и биллинга, управление, защиту информации и пр., причем все это – с использованием исключительно открытых стандартных интерфейсов. Технический прогресс на этом, разумеется, не останавливается.

В области применения IMS в стационарных сетях можно выделить два направления дальнейших исследований: использование IMS для предоставления новых услуг пользо-

вателям в качестве альтернативы Softswitch и использование IMS как основы для конвергенции стационарных и мобильных сетей *FMC* (*Fixed-Mobile Convergence*). Практической реализацией тех или иных решений в том и другом направлении производители и Операторы занимаются на свой страх и риск, а стандартизация использования IMS в стационарных сетях и построения NGN на базе IMS-архитектуры ведется по упомянутому в начале главы проекту TISPAN комитета ETSI.

Аналогично процессу стандартизации и развития концепции UMTS-сети в 3GPP, в TISPAN стандартизация делится на этапы, результатом каждого из которых в 3GPP и в TISPAN является очередной релиз. Так, релиз 3 TISPAN ориентирован на межсетевую мобильность пользователей и увеличение ширины полосы пропускания в технологиях доступа (VDSL, FTTH, Wi-MAX).

Основной упор в релизе 1 TISPAN делается на использование для доступа к IMS технологий ADSL и WLAN. Он базируется на 3GPP Release 6, наработках по Release 7 и на исследованиях, выполненных в проекте TISPAN. В TISPAN решено сохранить принцип деления функций сети на подсистемы, как это определено в 3GPP, что позволяет добавлять для поддержки изменяющихся требований и наборов услуг новые подсистемы, в частности, подсистемы, специфицированные другими организациями.

Поддержку разнотипного доступа в релизе 1 TISPAN обеспечивают две новые подсистемы:

- *Network Attachment Subsystem* (*NASS*) производит назначение IP-адресов, например, используя протокол *DHCP* (*Dynamic Host Configuration Protocol*), аутентификацию на уровне IP, авторизацию доступа к сети, определение местонахождения на уровне IP и др.
- *Resource and Admission Control Subsystem* (*RACS*) управляет доступом.

Благодаря совместным усилиям TISPAN и 3GPP, архитектура IMS адаптируется к xDSL доступу, для которого поддерживаются мультимедийные услуги, и обеспечивается симуляция услуг PSTN/ISDN, перечень которых приведен в табл. 3.1.

Определены те из этих услуг, симуляция которых обязательна, рекомендована или опциональна.

В таблице показано также соответствие услуг, предоставляемых в IMS, аналогичным услугам в ТфОП/ISDN, причем во избежание путаницы, названия всех услуг даны в оригинальном англоязычном варианте, поскольку устоявшиеся русскоязычные названия есть не у всех услуг ТфОП/ISDN, не говоря уже об услугах IMS.

Таблица 3.1. IMS-услуги TISPAN и 3GPP

Приоритет	Симулируемая услуга в IMS	Эквивалентная услуга ТфОП/ISDN
Обязательно	Originating Identification Presentation (OIP)	Calling Line Identification Presentation (CLIP)
Обязательно	Originating Identification Restriction (OIR)	Calling Line Identification Restriction (CLIR)
Обязательно	Terminating Identification Presentation (TIP)	Connected Line Identification Presentation (COIP)
Обязательно	Terminating Identification Restriction (TIR)	Connected Line Identification Restriction (COIR)
Обязательно	Mallcious Communication Identification (MCID)	Mallcious Call Identification (MCID)
Обязательно	Anonymous Communication Rejection (ACR)	Anonymous Call Rejection (ACR)
Рекомендовано	Communication Diversion (CDiv)	Call Diversion (CDiv)
Рекомендовано	Communication Forwarding Unconditional (CFU)	Call Forwarding Unconditional (CFU)
Рекомендовано	Communication Forwarding on Busy user (CFB)	Call Forwarding Busy (CFB)
Рекомендовано	Communication Forwarding on no Reply (CFNR)	Call Forwarding No Reply (CFNR)
Рекомендовано	Communication Deflection (CD)	Call Deflection (CD)
Рекомендовано	Communication Forwarding on Not-Logged On (CFNL)	Call Forwarding on Mobile Subscriber Not Reachable
Рекомендовано	Communication Waiting (CW)	Call Waiting (CW)
Рекомендовано	Communication Hold (HOLD)	Call Hold (HOLD)
Рекомендовано	Communication Barring (CB) (Outgoing CB, Selective Outgoing CB, Incoming CB)	Outgoing Call Barring (OCB)
Рекомендовано	Follow Me (FM)	Follow Me (FM)
Рекомендовано	Message Waiting Indicator (MWI)	Message Waiting Indicator (MWI)
Опционально	Conferencing (CONF)	Conference Calling (CONF)
Опционально	Advice of Charge (AoC)	Advice of Charge (AoC)
Опционально	Closed User Group (CUG)	Closed User Group (CUG)
Опционально	Fixed Destination Communication	
Опционально	Inhibition of Incoming Forwarded Communications (IIFC)	
Опционально	Direct Dial In (DDI)	Direct Dial In (DDI)
Опционально	Explicit Communication Transfer (ECT)	Explicit Call Transfer (ECT)
Опционально	Trunk Hunting (TH)	

Отдельно TISPAN определяет для IMS подсистему *эмуляции* услуг ТфОП/ISDN, которая позволяет заменить TDM-оборудование коммутации каналов средствами IMS, сохранив в сети традиционные абонентские терминалы. Здесь разница между симуляцией и эмуляцией следующая.

Симуляция заключается в предоставлении ТфОП/ISDN услуг на базе IMS только интеллектуальным терминалам (например, IP-телефонам). При этом не обязательно строго выполнять все требования, предъявляемые к этим услугам, и предоставлять весь спектр услуг – можно ограничиться лишь некоторыми из них, наиболее популярными, возможно, с иными эргономическими характеристиками. *Эмуляция* же заключается в том, что IP-сеть создает для оконечного оборудования видимость того, что она является ТфОП/ISDN сетью. Пользователи не ощущают того, что они подключаются к IP-сети, а не к ТфОП/ISDN, а следовательно, обеспечивается возможность использования и интеллектуальных, и не интеллектуальных терминалов (рис. 3.10).

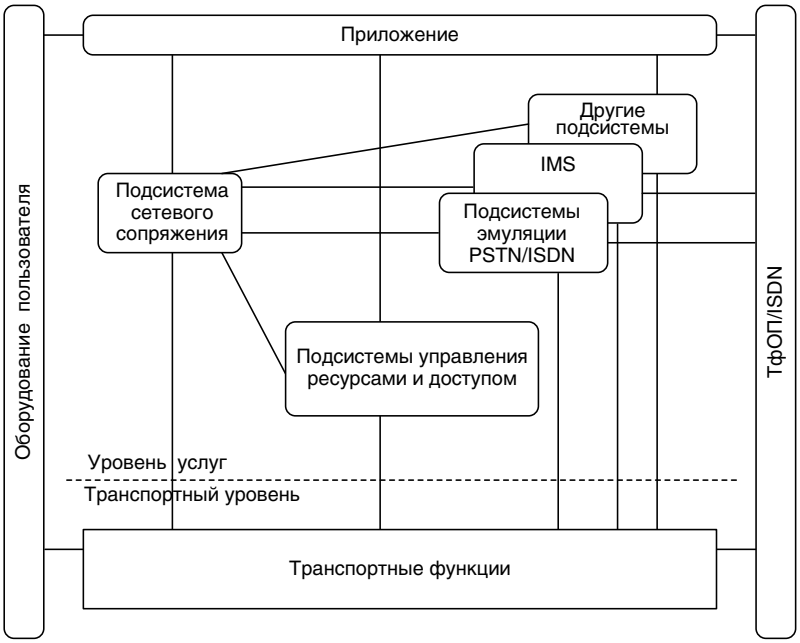

Рис. 3.10. Архитектура NGN-сети в проекте TISPAN

Существует два подхода к созданию подсистемы эмуляции ТфОП/ISDN в современных IP-сетях. Первый из них – применение Softswitch, требующего стандартизации не внутренней

структуры, а лишь внешних интерфейсов. Этот подход и используется в релизе 1 TISPAN NGN. Второй подход – использование (полностью или частично) функциональной архитектуры IMS для определения внутренней структуры подсистемы эмуляции ТфОП/ISDN.

В реальных сетях и, возможно, в будущих стандартах, могут применяться компромиссные варианты, например стандартизация внешних интерфейсов IMS; к тому же функциональная архитектура IMS позволяет создавать реальную физическую архитектуру сети на оборудовании Softswitch (MGC) и медиа-шлюзах (MG). В релизе 2 TISPAN NGN использован второй подход. Но для обоих подходов уже определен сигнальный протокол – SIP-I.

Еще одна новая подсистема – NASS – по сути, замещает, функции домена коммутации пакетов 3GPP и GPRS-процедуры аутентификации, управления и определения местонахождения.

При создании этой подсистемы еще предстоит решить ряд проблем – взаимодействия с механизмами аутентификации на уровне SIP, соблюдения соответствия стандартам Форума DSL, использования одной NASS для каждой из сетей доступа или одной NASS для нескольких сетей доступа (рис. 3.11).

Серым цветом показаны функциональные элементы, которые были определены проектом TISPAN, штриховкой отмечены элементы, подвергшиеся изменению, остальная структура IMS осталась такой, как она описана в стандартах 3GPP.

Функция *IBCF* (*Interconnect Border Control Function*) обеспечивает управляемость на границе между сетями разных провайдеров. Она может содержать в себе THIG, выполняет согласование IPv4 и IPv6, может, в случае необходимости, обращаться к функции IWF, может управлять доступом и назначать полосу пропускания в соответствии с собственной политикой или обращаясь к подсистеме RACS.

Функция *IWF* (*InterWorking Function*) обеспечивает взаимодействие протокола SIP сети IMS с сигнальными протоколами IP-сетей других провайдеров, такими как H.323 или другие реализации SIP.

Функция *I-BGF* (*Interconnect Border Gateway Function*) управляет передачей данных на 3 и 4 уровнях через границу сетей провайдеров. Эта функция играет роль межсетевого экрана и NAT, она защищает ядро сети провайдера, фильтруя

пакеты на основании информации транспортного уровня. Она использует NAPT для сокрытия транспортных адресов элементов ядра сети IMS.

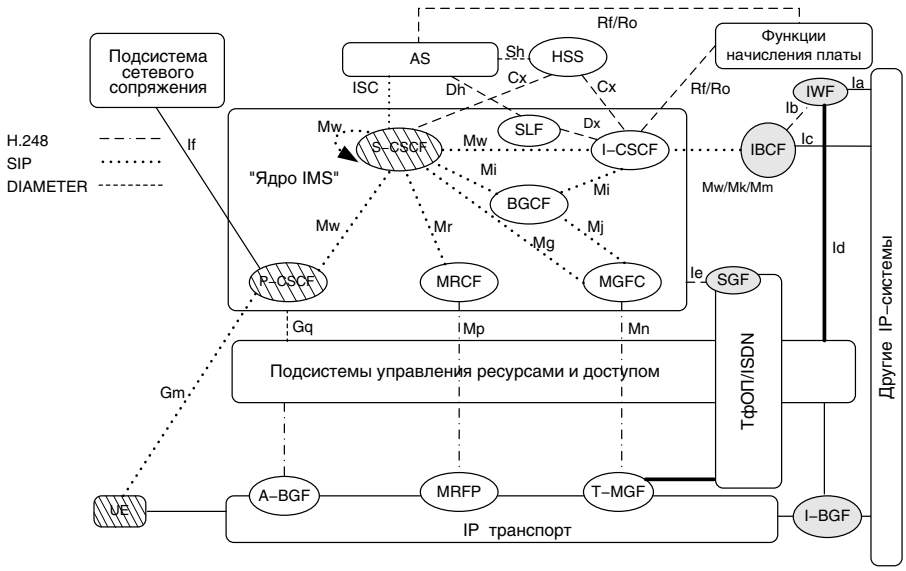

Рис. 3.11. Изменения структуры 3GPP IMS в проекте TISPAN

Опциональными возможностями I-BGF являются: маркировка трафика в целях обеспечения QoS, политика управления шириной полосы пропускания и объемом сигнальной информации, измерение загрузки ресурсов и определение параметров QoS.

Различия между мобильными и стационарными сетями в плане реализации IMS в проекте выглядят следующим образом: существует разница в ширине полосы, в защите, в задержках при передаче; к терминалам стационарной сети предъявляются менее строгие требования (такие как поддержка IPv6, USIM/ISIM, некоторых кодеков); оборудование пользователя не должно хранить информацию о его местонахождении, в терминалах стационарной сети нет явного резервирования сетевых ресурсов; стационарные терминалы жестко не привязаны к пользователям; не реализуется сжатие сигнальной информации; индикация ширины полосы RTCP в SDP обычно не требуется; аутентификация производится без UICC.

3.13. Нововведения и перспективы IMS

После релиза 8 в IMS не появляется каких-либо существенных архитектурных изменений, однако развитие IMS продолжается консорциумом 3GPP по сей день. Рассмотрим ключевые изменения IMS в релизах 9-12.

Релиз 9 добавил в IMS поддержку экстренных вызовов через GPRS и EPC. Описан протокол, основанный на H.248, обеспечивающий взаимодействие IBCF и TrGW (как в домене коммутации каналов, так и в домене пакетной коммутации). Ключевых изменений в архитектуре или процедуре установления сессий нет: сохранен курс на внедрение новых типов услуг (оповещение в случае чрезвычайных ситуаций, M2M коммуникации, VoIP в CS и т.д.). В релизе 10 никаких кардинальных изменений в области IMS не сделано. Продолжен курс на обеспечение непрерывности речевых сеансов или мультимедийных сессий при различных условиях (переключении сеанса связи с одного устройства на другое, изменении технологии доступа в процессе обслуживания). В релизе 11 сохранилось направление создания архитектуры, универсальной для всех технологий доступа, с возможностью развернуть и предоставить любую услугу вне зависимости от типа оборудования пользователей или их возможностей. Среди новых услуг появился сервис симуляции USSD в IMS и *Advanced IP interconnection of services* (*IPXS*), отправка и получение SMS сообщений без MSISDN. В релизе 12 также сохраняется базовая архитектура IMS. Из релиза 11 продолжено развитие технологии симуляции USSD, а также – развитие IPXS. Начиная с релиза 12 в IMS поддерживается услуга IMS-based telepresence. Из вышеизложенного материала этой главы следует, что IMS предлагает существенные преимущества для провайдеров контента, поставщиков услуг и клиентов в равной степени. Преимущества IMS мощны и неоспоримы. Прежде всего, обслуживание может быть развернуто быстрее и более рентабельно, чем когда-либо ранее, благодаря стандартизованной архитектуре IMS. Во-вторых, сеть абсолютно не зависит от технологии доступа – стирается граница между инфраструктурами фиксированных и мобильных сетей, а также разными сферами предоставления услуг (телевидение, информационные услуги, телеком и пр.).

В-третьих, вследствие устранения разделительной линии между проводной и беспроводной связью, возможность перемещать приложения между этими двумя доменами ста-

новится намного более простой, и мобильность может быть включена в существующие приложения, распространяя их за пределы границ традиционной проводной связи.

Приложения становятся более интересными сами по себе благодаря возможностям добавить в комбинации к услуге видеоконференцию, анализ присутствия, мгновенный обмен сообщениями и т.п. Кроме того, IMS намного быстрее реагирует на заказ услуги, т.к. информация о каждом пользователе размещается в единственном хранилище, что делает бизнес-процессы намного более эффективными. По сравнению с так называемой бесплатной речевой связью типа Skype, архитектура IMS имеет преимущества, связанные с тем, что IMS присваивает качеству обслуживания высокий приоритет. Без IMS предсказуемость качества сеанса в Интернет весьма мала, т.к. часто оказывается невозможным узнать, как джиттер, задержка и потеря пакетов будут влиять на тот или иной сеанс.

Другим преимуществом, которое есть у IMS, является сбор данных и служба поддержки биллинга. Бесплатные службы VoIP не делают этого, тогда как IMS не только может собрать данные, но и предложить пользователю множество опций биллинга. Поставщики услуг могут использовать это в своих интересах, предлагая премиальные услуги (лучшее QoS за более высокую цену) или услуги с добавленной стоимостью, такие как загружаемый контент, за который можно начислять плату отдельно. Еще одним плюсом IMS является возможность создать новые услуги из ранее созданных услуг 1990-х и 2000-х годов, объединяя апробированные телекоммуникационные услуги и новые Интернет – или телеком-приложения.

И в заключение отметим еще один аспект. Ясно, что одними плюсами ни одна инновационная технология, упомянутая на страницах этой книги, не ограничивается. При внедрении IMS есть и проблемы. Это, в первую очередь, проблемы CAPEX и OPEX, а также вовлечение Оператора в технологическое перевооружение, в формирование новых, ранее не проверенных деловых отношений с компаниями – поставщиками услуг, которые будут управлять потребительскими ожиданиями в большей степени, чем Оператор, чего не было никогда прежде. Ясно также, что параллельно с внедрением IMS в те же 2010-е годы число компаний типа Google, Skype, Yahoo, предлагающих клиентам бесплатную или дешевую передачу речи, видео, и услуги электронной почты, будет продолжать расти.

Следовательно, многие абоненты будут ожидать бесплатного обслуживания и от Операторов, устанавливающих IMS.

Впрочем, это проблема актуальна более для коммерческого блока Оператора, нежели для инженеров, которым в первую очередь адресована эта книга. Если же кто-то из коммерсантов или топ-менеджеров телекоммуникационных компаний все же дочитал до этих страниц, то для них приведены несколько дилетантских вопросов от авторов.

Сегодня пользователь включает свой ноутбук, начинает работать и делает телефонный звонок приятелю с помощью Skype. Действительно ли это бесплатно? Разве Оператор дает ему каждый месяц бесплатный доступ в Интернет? Разве бесплатно установлены маршрутизатор Cisco или точки доступа DLink? Не лежит ли решение проблемы экономической эффективности IMS на путях перераспределения доходов? Не стоит ли Оператору предоставлять бесплатную телефонию пользователям, приобретающим у него за 3999 руб. в месяц скоростной Интернет + скачивания 30 часов фильмов + видеонаблюдение за ребенком в детском саду + видеонаблюдение за дачей в поселке? Ясно, что это не бесплатно. Стоимость телефонной связи включена в плату 3999 руб. в месяц. Однако, создавая впечатление, что клиент имеет возможность получить нечто ни за что, Оператор привязывает этого клиента и имеет возможность продать ему более полный пакет услуг с помощью IMS.

Рецензентом книги Н.С. Мардером было указано, что эти дилетантские вопросы авторам следовало бы дополнить профессиональными ответами с описанием новой сути взаимоотношений Оператора связи с провайдером услуг, недискриминационным подключением, распределением доходов от услуг, обеспечением качества и разделением ответственности перед пользователем. Авторы полностью согласны с этим и обязуются осмыслить и более развернуто обсудить эти аспекты в отдельной публикации. Здесь же важно подчеркнуть, что IMS – это не только технологическое новшество, а скорее социальное новшество со стороны Операторов и сервис-провайдеров, *фундаментальное* преобразование сети, которая вместе с IMS становится гораздо более мощной и (возможно) более доходной, *адаптируясь к пользователю, а не вынуждая пользователя адаптироваться к сети*. Именно в этом авторам представляется наиболее важное инновационное влияние IMS, по крайней мере, в контексте этой книги.

Глава 4
Долговременная эволюция LTE-A/SAE

А старые обезьяны все еще вспоминают,
как они жили до эволюции.
Феликс Кривин

4.1. Продолжение ре(э)волюции мобильной связи

Поколение 3G существенно изменило ситуацию в инфокоммуникационных сетях: возросла скорость передачи данных за счет принципиально нового подхода к разделению каналов на радиоучастке (W-CDMA), появилась новая концепция IP Multimedia Subsystem, а также некоторые расширения, позволившие улучшать первоначальную технологию W-CDMA (HSDPA, HSUPA, HSDPA+, MIMO).

Существует ряд трендов в области услуг мобильной связи, которые сегодня определяют пользовательский спрос:

- развитие облачных сервисов, для которых важна возможность пользователя получить доступ к сети в любом месте, в любое время;
- приложения Web 2.0, с помощью которых пользователи участвуют во всевозможных Интернет-сообществах, что влечет за собой обмен контентом;

- потоковое видео по запросу и мобильное ТВ;
- интерактивные мобильные игры в реальном времени;
- мобильные приложения, для смартфонов, ноутбуков и планшетов.

С развитием спроса на эти виды услуг, пользователю становятся важны такие показатели качества обслуживания, как:

- средняя и максимальная скорости передачи данных;
- небольшая задержка реакции сети на запросы;
- гарантированное радиопокрытие с приемлемой скоростью доступа даже на границах сот;
- непрерывность обслуживания при переходе от одной сети доступа к другой;
- доступные цены (наиболее привлекательными для пользователя являются безлимитные или псевдобезлимитные тарифы с фиксированной платой).

Из-за преобладания трафика передачи данных над речевым трафиком в мобильных сетях становится очевидной необходимость пересмотра архитектуры сети. Существующие технологии построения мобильных сетей не рассчитаны на экспоненциальный рост трафика данных, поэтому при преобладании фиксированных «плоских» тарифов для Оператора связи такой рост оказывается невыгодным, как показано на рис.4.1.

Как упоминалось в главе 1, в релизе 7 представлены две новые технологии, позволяющие увеличить скорость передачи на радиоучастке: технология *MIMO* (*Multiple In, Multiple Out*) и модуляция 64 QAM. В этом релизе представлена также вторая фаза развития IMS (IMS phase 2), раскрывающая все возможности IP-ядра сети, о чем говорилось в главе 1. Таким образом, в 3G сетях, основанных на технологии W-CDMA и использующих диапазон частот шириной 5 МГц, оказываются практически достигнутыми лимиты скоростей передачи данных. Именно для того, чтобы преодолеть эти ограничения, 3GPP разработал стандарты для сети мобильной связи нового поколения, получившие название *LTE* (*Long Term Evolution*) и *SAE* (*System Architecture Evolution*) [79,95]. Эти стандарты специфицированы 3GPP в релизе 8 в серии спецификаций 36.xxx.

Термин LTE описывает эволюцию сети радиодоступа относительно сетей GSM и UMTS и появление нового стандарта E-UTRAN. Термин SAE описывает эволюцию ядра сети в *Evolved Packet Core* (*EPC*), архитектура которого значительно изменена относительно прежних сетей GSM/3G. Существует собирательный термин *EPS* (*Evolved Packet System*), который объединяет сеть доступа и ядро EPC.

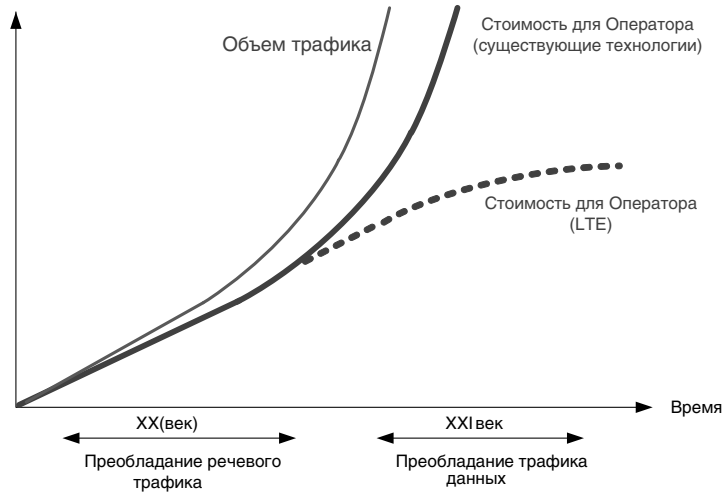

Рис. 4.1. Рост трафика и стоимости его обслуживания

LTE/SAE – это ре(э)волюция мобильных сетей с целью удовлетворить будущие требования к скоростям доступа в таких сетях. Что это означает с точки зрения абонента? Он получает стабильный высокоскоростной доступ к сети, сравнимый с домашним проводным подключением, но в мобильной среде. Для Оператора связи LTE, ко всему прочему, означает внедрение простой и недорогой в обслуживании сети.

4.2. Цели LTE/SAE

При разработке стандарта LTE/SAE преследовались следующие цели:

- максимально эффективное использование ограниченного радиочастотного спектра. LTE можно использовать в парных и непарных спектрах в диапазоне от 1,4 до 20 МГц. LTE почти в 4 раза более эффективно использует спектр частот, нежели HSDPA согласно 3GPP релизу 6;

- высокие скорости доступа, при которых абонент получает максимально скорость до 173 Мбит/с и минимальную задержку 10 мс;
- плоская all-IP архитектура сети, которая существенно снижает стоимость передачи за мегабайт данных;
- новый радиоинтерфейс с новыми технологиями передачи (например, пространственное разнесение антенн MIMO 4x4 может ускорить передачу в направлении к абоненту до 326 Мб/с).

Базовая архитектура EPS состоит из пакетного ядра сети Evolved Packet Core и сети радиодоступа E-UTRAN. Сеть основана полностью на протоколе IP, и больше не включает в себя домен с коммутацией каналов – для передачи речи в LTE используется только технология VoIP. IP-ядро сети снабжено простыми, но эффективными механизмами обеспечения QoS по требованию. Одна из задач концепции LTE/SAE – использование Ethernet (класса carrier-grade) там, где это возможно, в частности, для подключения узлов *eNodeB,* которые являются базовыми станциями LTE.

В сетях мобильной связи 2.5G и 3G домен коммутации пакетов строится на узлах SGSN и GGSN, а сеть доступа состоит из узлов *NodeB* и *RNC*. Ре(Э)волюционный переход к архитектуре LTE/SAE призван оптимизировать производительность сети, максимизировать скорость передачи данных и минимизировать задержку, вносимую сетью. Поэтому вместо четырех типов узлов в плоскости пользователя (NodeB, RNC, SGSN, GGSN) архитектура EPS состоит из узлов *evolved NodeB* (*eNodeB, eNB*) и *SAE Gateway* (*SAE GW*). SAE GW включает в себя два сетевых элемента: Serving Gateway, который отвечает за управление мобильностью между системами доступа GSM и UMTS, и PDN Gateway, осуществляющий взаимодействие с сетью Интернет и локальными сетями и обеспечивающий мобильность абонента между LTE и не-3GPP сетями. Вся сигнальная информация плоскости управления (*IMS Control Plane*) обрабатывается элементом *MME* (*Mobility Management Entity*), как это показано ниже на рис. 4.3. В силу того, что сеть доступа в LTE функционирует без контролера базовых станций (BSC или RNC), большинство функций, ранее выполнявшихся этими сетевыми элементами, теперь оказываются возложенными на саму базовую станцию, eNodeB.

Эти новые базовые станции eNB управляют всеми задачами, связанными с передачей данных по радиоканалу, чтобы обеспечивать быструю повторную передачу и процедуры, связанные с адаптацией к каналу. Ранее эти процедуры должны были управляться RNC, что вызывало дополнительные задержки.

Передача этих функций к eNB обеспечивает более быструю реакцию (например, для реализации повторных передач или для распределения ресурсов), что уменьшает задержки и увеличивает пропускную способность сети в целом. При этом eNB взаимодействует напрямую посредством стандартизованных интерфейсов для обмена пользовательской и сигнальной информацией. Такая архитектура сети с минимальным количеством узлов обеспечивает меньшее количество интерфейсов и упрощает работу сети, исключая необходимость конвертации протоколов сигнализации. Итак, два понятия, о которых пойдет речь далее в этой главе – это LTE и SAE.

4.3. E-UTRAN

4.3.1. Архитектура E-UTRAN

Полное описание *E-UTRAN* можно найти в TS 36.300, а описание его архитектуры – в TS 36.401. Развернутой спецификации E-UTRAN посвящен релиз 9, а дальнейшая эволюция сосредотачивается в IMT-Advance в релизах 10 и 11.

Чтобы соответствовать приведенным в предыдущем параграфе целям, архитектура сети доступа LTE, названная *Evolved UTRAN* (*E-UTRAN*), существенно изменилась по сравнению с 3G/3.5G UTRAN. Иерархический способ построения сети доступа сменился принципом «плоской» архитектуры, в которой элементы равноправно взаимодействуют друг с другом. В соответствии с рекомендацией 3GPP TS 36.300, E-UTRAN имеет архитектуру, представленную на рис. 4.2.

Evolved UTRAN включает в себя eNB, которые представляют собой оконечные пункты для протоколов пользовательского уровня и уровня управления (U-plane и C-plane). Узлы eNB соединены между собой посредством интерфейса X2. Предполагается, что между двумя узлами eNB, которым требуется соединиться друг с другом (например, для хэндовера поль-

зовательского терминала), всегда существует интерфейс X2. Узлы eNB также соединены с EPC посредством интерфейса S1. Интерфейс S1 поддерживает конфигурацию много точек-много точек.

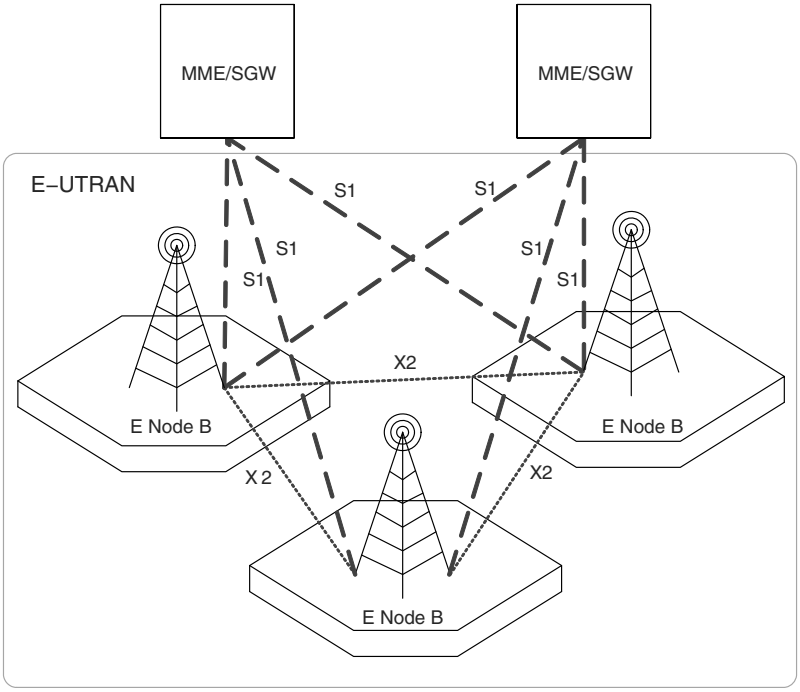

Рис. 4.2. Архитектура E-UTRAN

Как уже отмечалось выше, функции eNB включают в себя не только функции базовой станции 3G (функции NodeB) взаимодействия с мобильными устройствами пользователей через радиоинтерфейс, но и функции *Radio Network Controller* (*RNC*) управления радиоресурсом и маршрутизации пользовательской информации к *шлюзу Serving Gateway*. Согласно TS 36.401, eNB выполняет функции, сведенные в табл. 4.1.

Таблица 4.1. Функции eNodeB

№	Функция	Примечание
1	Перенос пользовательской информации	
2	Шифрование/дешифрование радиоканала	На основании ключа, уникального для каждого соединения
3	Защита целостности информации	
4	Сжатие заголовков	В зависимости от стеков протоколов TCP/IP или RTP/UDP/IP

Окончание табл. 4.1

№	Функция	Примечание
5	Функции управления мобильностью: - переключение (handover) - поиск (paging) - определение местонахождения (positioning)	
6	Защита от межсотовой интерференции	Управление распределением радиочастотного ресурса с целью избежать интерференции
7	Установление и разрушение соединения	
8	Балансировка нагрузки	Перераспределение неравномерной нагрузки между несколькими сотами
9	Распределение сообщений NAS	Требуется определение узла назначения сообщений, т.к. E-UTRAN имеет соединение с несколькими MME/S-GW
10	Синхронизация	
11	Разделение сети радиодоступа	Позволяет пользовательскому терминалу правильно выбрать СПС, к которой следует подключиться (при использовании нескольких сетей в одном частотном диапазоне)
12	Функция MBMS	Трансляция широковещательных и многоадресных сообщений
13	Отслеживание перемещений абонента или оборудования	Реализуется в процессе процедур получения доступа и последующих операций переключения (хэндовер)

4.3.2. Особенности радиоинтерфейса

Ре(Э)волюционные изменения на радиоучастке LTE определяются новой технологией разделения каналов *OFDM* (*Orthogonal Frequency Division Multiplexing*), которая позволяет экономно распределять радиочастотный ресурс, обеспечивая вместе с тем высокую скорость доступа.

Для увеличения эффективности использования радиоресурса применяются также технологии *MIMO* (*Multiple Input Multiple Output*), *HARQ* (*Hybrid Automatic Repeat Request*) и модуляция до 64 QAM, обеспечивающая высокую плотность передаваемой информации.

Радиоинтерфейс LTE поддерживает дуплексные режимы как с *частотным разделением приема и передачи FDD* (*Frequency Division Duplex*), так и с *временным разделением приема и передачи TDD* (*Time Division Duplex*). Используются также дополнительные режимы доступа, например, полудуплексный FDD, при котором прием и передача происходят на

разных частотах не одновременно, а поочередно. Этот подход позволяет экономить радиочастотный спектр, несмотря на то, что он вдвое снижает скорость передачи данных.

Оператору связи для внедрения LTE не требуется новый диапазон частот – радиоинтерфейс LTE создан таким образом, что он может работать на тех же частотах, что и существующие сети поколений 2.5G и 3G, или даже параллельно с ними благодаря заложенному в LTE механизму гибкого назначения спектра, допускающего использование спектров с шириной полосы пропускания 1.4, 3,5, 10, 15 и 20 МГц.

4.3.3. Структура каналов на радиоучастке

E-UTRAN разработан как часть сети All-IP, поэтому сеть доступа LTE больше не имеет элементов, основанных на коммутации каналов. Широковещательные и общие каналы, специфицированные в более ранних версиях 3GPP (HSDPA, HSUPA, MBMS), также используются в LTE. Стек протоколов сигнализации, который используется в LTE, основан на стандартной семиуровневой модели OSI. На третьем уровне представлены логические каналы, которые предоставляют услуги протоколам верхнего уровня, отвечающим за реализацию услуг и работу приложений. Затем логические каналы сопоставляются с транспортными каналами на втором уровне, которые управляют потоками данных (повторными передачами, контролем ошибок, приоритизацией).

На втором уровне функционируют протоколы RLC, PDCP и MAC. На физическом уровне транспортные каналы соотносятся с физическими, использующими радиоинтерфейс.

В этой книге не предполагается подробно останавливаться на рассмотрении физических и транспортных каналов. Основное внимание уделено логическим каналам сетевого уровня. Логические каналы предоставляют свои функции верхним уровням стека протоколов и специфицированы в терминах сервисов верхнего уровня, которые они поддерживают. Каждый логический канал определяется типом информации, которую он переносит. В общем случае, логические каналы LTE разбиты на две группы:

- логические каналы управления (для переноса информации уровня управления);
- пользовательские логические каналы (для переноса пользовательской информации).

Пользовательские каналы (**traffic channels**):

- DTCH – Dedicated Traffic Channel – индивидуальный пользовательский канал с конфигурацией точка-точка, присвоенный пользовательскому терминалу.
- MTCH – Multicast Traffic Channel – однонаправленный канал от eNB к терминалу пользователя. Используется теми терминалами, которые получают MBMS (Multimedia Broadcast Multicast Service) – широковещательные и многоадресные услуги.

Каналы управления (**control channels**):

- BCCH – Broadcast Control Channel – однонаправленный канал для передачи широковещательной информации управления;
- PCCH – Paging Control Channel – однонаправленный канал, который переносит информацию для поиска абонента. Этот канал используется, если сеть не знает соты, в которой в данный момент находится абонент;
- CCCH – Common Control Channel – этот канал предназначен для запроса доступа пользовательского терминала к сети и используется при установлении соединения или реализации иных процедур, требующих выделения индивидуального сигнального канала;
- MCCH – Multicast Control Channel – однонаправленный канал с конфигурацией точка-много точек, передает информацию управления для MBMS от сети к терминалам пользователей;
- DCCH – Dedicated Control Channel – двунаправленный канал с конфигурацией точка-точка, используется для передачи индивидуальной сигнальной информации, если между пользовательским терминалом и сетью существует RRC соединение.

Любая передача данных в LTE производится по заранее определенному «графику передач» в особых пакетных структурах; в LTE не существует непрерывных «канальных» соединений, как в предыдущих сотовых технологиях. Составление графика передач для обоих направлений – задача MAC-диспетчера в eNodeB, который определяет ресурс, необходимый каждому пользователю в каждый момент времени. Решение о выделении того или иного ресурса основывается на полученных *отчетах CGI* (*Channel Quality Indicators*) и на других факторах.

4.4. Эволюция сетевой архитектуры SAE

SAE (*System Architecture Evolution*) – это сетевая архитектура, разработанная с целью бесшовной интеграции мобильной сети с другими сетями, работающими по протоколу IP (рис. 4.3).

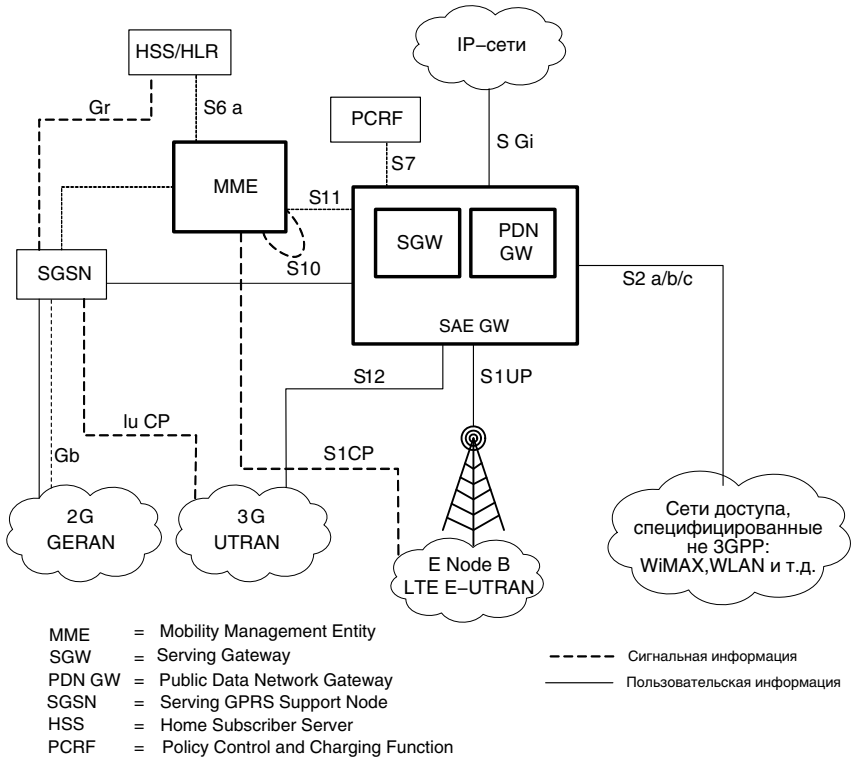

Рис. 4.3. Эволюция сетевой архитектуры SAE

В SAE исчезают такие элементы, как *RNC* (*Radio Network Controller*) и *SGSN* (*Serving GPRS Support Node*), а появляются новые элементы: *evolved Node B* (*eNB*), *MME* (*Mobility Management Entity*) и *SAE Gateway*. Это позволяет сети получить «плоскую» архитектуру сети All-IP. SAE осуществляет также взаимодействие с другими беспроводными не-3GPP сетями (UMTS, WCDMA, WiMAX, WLAN и т.д.), позволяя сетям с не-3GPP технологиями иметь прямой интерфейс с сетью LTE и управлять ими в пределах одной сети LTE/SAE.

SAE включает в себя новое эволюционное пакетное ядро EPC, в которое встроены функции взаимодействия с другими беспроводными сетями. Интерфейс S2 позволяет Операто-

рам связи расширять свои сети другими основанными на IP технологиями доступа, управляя такими функциями, как мобильность, хэндовер, биллинг, аутентификация и защита информации в пределах мобильной сети. В EPC используется также интерфейс S1 для соединения с сетью радиодоступа и интерфейс S3 для взаимодействия с SGSN в целях поддержки хэндовера с сетями GPRS. Интерфейс SGi предназначен для взаимодействия EPC и внешней IP-сети.

4.5. Узел управления мобильностью MME

MME – это центральный элемент опорной сети LTE, взаимодействующий с пользовательскими устройствами UE по протоколу NAS. Его функции охватывают управление и хранение данных пользователя, создание временных идентификаторов и их передачу пользовательским устройствам, аутентификацию пользователей, управление мобильностью и логическими каналами (bearers), а также является оконечной точкой NAS-сигнализации. Процедуры управления мобильностью в MME охватывают поиск и отслеживание состояния пользовательского устройства в зоне обслуживания MME, управление установкой и освобождением ресурсов в зависимости от изменения состоянии пользовательского терминала, а также участие в хэндовере.

Аутентификация и процедуры обеспечения защиты подразумевают взаимодействие с HSS, при котором MME осуществляет проверку идентификации пользователя для защиты от несанкционированного доступа. Для этого пользовательскому терминалу временно присваивается специальный идентификатор, который называется глобальным уникальным временным идентификатором *GUTI* (*Globally Unique Temporary ID*), что позволяет уменьшить количество передач IMSI через радиоинтерфейс. Кроме того, MME выполняет обмен сигнальной информацией с SGSN для предоставления мобильности между 2G/3G и LTE сетями доступа и обеспечивает функции плоскости управления. Для управления абонентскими профилями и подключения к услугам MME получает абонентский профиль из HSS домашней сети и определяет на базе этого профиля пакетную сеть передачи данных, к которой необходимо подключить устройство этого абонента.

4.6. Обслуживающий шлюз S-GW

S-GW является шлюзом пользовательского трафика, а также трафика от 3GPP-сетей доступа 2G, 3G и LTE. Подчеркнем, что весь пользовательский трафик проходит через S-GW, который является *опорной точкой* (*anchor point*) при маршрутизации данных, как в случае передвижения пользователя в зоне обслуживания LTE, т.е. при хэндовере между eNodeB, так и в случае обеспечения мобильности между LTE и другими 3GPP-технологиями доступа, т.е. при выполнении хэндовера от и к 2G/3G-сетей. Следовательно, пользовательский трафик маршрутизируется через S-GW вне зависимости от технологии радиодоступа, в том числе измененной в процессе хэндовера. Возникает опорная точка (anchor point), общая для всех 3GPP-технологий доступа: 2G/3G/LTE. При этом, если в процессе хэндовера изменяется MME, то S-GW также изменяется, но P-GW во всех случаях остается неизменным.

Кроме того, S-GW отвечает за передачу, маршрутизацию и буферизацию нисходящего трафика данных для UEs, который находится в неактивном состоянии в LTE-сети, терминирует передачу нисходящего трафика для пользовательского устройства в состоянии *ECM-IDLE* (*Idle State Mobility Handling*), т.е. становится представителем пользователя, находящегося в неактивном состоянии, а также инициирует запрос на обслуживание входящего сеанса связи, когда трафик требуется доставить к неактивному пользовательскому устройству. Для задач COPM (и не только) подчеркнем, что именно S-GW дублирует пользовательский трафик в случае его законного перехвата.

4.7. Шлюз пакетной сети передачи P-GW

P-GW (*Packet Data Networks Gateway*) является пограничным маршрутизатором пользовательского трафика между EPS и внешними пакетными сетями передачи данных.

В функции P-GW входят распределение и назначения IP-адресов между пользовательскими устройствами, обеспечивает выполнение правил политики и тарификации *PCEF* (*Policy and Charging Enforcement Function*), а именно – *управление скоростью* (*throttling*), *управление доступом* (*gating*) и фильтрацию пользовательских данных, а также подсчет использо-

вания транспортных ресурсов сети (трафика пользователя или длительности сессии). При этом пользовательское устройство может иметь несколько одновременных соединений через P-GW со многими внешними сетями.

4.8. Другие сетевые элементы LTE-A

В состав LTE/SAE включаются сетевые элементы, используемые предыдущими 3GPP-технологиями. В их число входят следующие элементы, упомянутые в главе 1.

SGSN (*Serving GPRS Support Node*) – обслуживающий узел поддержки GPRS, предназначенный для передачи пакетных данных между S-GW и сетью радиодоступа предыдущих поколений 2G и 3G. Для EPS узел SGSN в перспективе необходим только для управления мобильностью между этими системами.

HSS – сервер абонентов домашней сети, предназначенный для хранения пользовательских профилей этих абонентов. Также интегрированная в HSS функция AuC обеспечивает генерацию данных авторизации и аутентификации пользователя, которые хранятся в HSS. Пользовательские профили HSS состоят из подписки, информации безопасности и информации о местонахождении пользователя, постоянных и временных идентификаторов пользователя. HSS хранит дату подключения к услугам, сами услуги, которые может получать пользователь, информацию о том, к какой внешней сети пакетной передачи данных подключен пользователь. Сервер хранит также адрес обслуживающего MME или последнего MME, где был зарегистрирован пользователь.

PCRF (*Policy and Charging Rules Function*) хранит правила политики по обслуживанию потока данных и тарификации. PCRF обеспечивает со стороны сети управление потоками данных в зависимости от оказываемых услуг и от QoS, а также управление тарификацией.

AAA (*Authentication, Authorisation and Accounting*) – центр авторизации, аутентификации и учета – предназначен для обмена информацией авторизации и аутентификации с сетями доступа технологий не-3GPP (Wi-Fi, WiMAX), подключенными к EPC.

4.9. Самоорганизующиеся сети SON

Стандарты самоорганизующихся сетей консорциум 3GPP начал разрабатывать еще в релизах 8 и 9, затем продолжил в релизе 10, который был закончен в июне 2011 года. Релиз 11, посвященный LTE-A, также охватывает дополнительные функции и расширения *SON* (*Self-Organizing Network*) [54], о чем уже упоминалось в другом контексте в главе 2.

Основными мотивами введения архитектуры SON были естественные желания Операторов сокращать (хотя бы не увеличивать) операционные расходы за счет уменьшения степени человеческого вмешательства на этапе планирования, внедрения и эксплуатации своих сетей, снижать капитальные затраты за счет оптимизации использования своих сетевых ресурсов, сохранять и наращивать прибыль, сокращая ошибки из-за человеческого фактора.

Существенную роль в достижении этих трех целей играет эксплуатационное управление OAM&P, объединяющее *управление ресурсами* (*Operations*), *административное управление* (*Administration*), *техническое обслуживание* (*Maintenance*) и *ввод новых ресурсов* (*Provisioning*). Если эти задачи непосредственно контролируются персоналом, даже со средствами автоматизации, этот ручной труд требует большого количества времени, значительных финансовых средств, высококлассных специалистов, и при этом человеческие ошибки все равно возможны. Разработка стандартов SON начата консорциумом 3GPP в релизе 8, затем продолжалась в релизах 9 и 10, а релиз 11 охватывает дополнительные функции и расширения SON (рис. 4.4).

Функция минимизация частоты использования *мобильных тестирующих бригад MDT* (*Minimization of Drive Tests*) на рис. 4.5 была описана в релизе 10 3GPP и относится к проблеме мобильных тестов. Такие тесты в сетях 1990-х и 2000-х реализовались с привлечением ручного труда персонала и потому являлись весьма дорогостоящими. Идея MDT базируется на результатах измерений, получаемых непосредственно от пользовательских устройств и содержащих информацию о местности, что позволяет иметь намного более глубокие знания о характеристиках пропускной способности соты, а также использовать эти знания для автоматизированных SON-функций.

Рис. 4.4. График работы 3GPP над стандартизацией SON

Развитие SON ориентируется на оптимизацию сети радиодоступа LTE, на минимизацию общих издержек на сетевую инфраструктуру SAE/LTE и ее эксплуатацию, на организацию хэндовера и на создание новых сценариев использования существующих и новых технологий. Использование SON для сокращения операционных расходов за счет уменьшения ручной работы и минимизации ошибок из-за человеческого фактора в эксплуатационном управлении OAM&P сети SAE/LTE иллюстрирует рис. 4.5.

Внедрение SON-функций позволяет минимизировать участие человека в эксплуатационных процедурах путем увеличения автоматизации сетевых элементов NE (Network Element), элементов управления доменом DM (Domain Management) и/или элементов управления сетью NM (Network Management).

На рис. 4.5 показано смещение от ручного планирования и конфигурации к мониторингу и управлению сетью средствами встроенной SON. Здесь человеческий фактор переводится на более высокий уровень управления, персонал сети освобождается от рутинных операций и вместо них занимается разработкой политик управления на уровнях сетевых элементов NE, управления элементами DM и управления сетью NM.

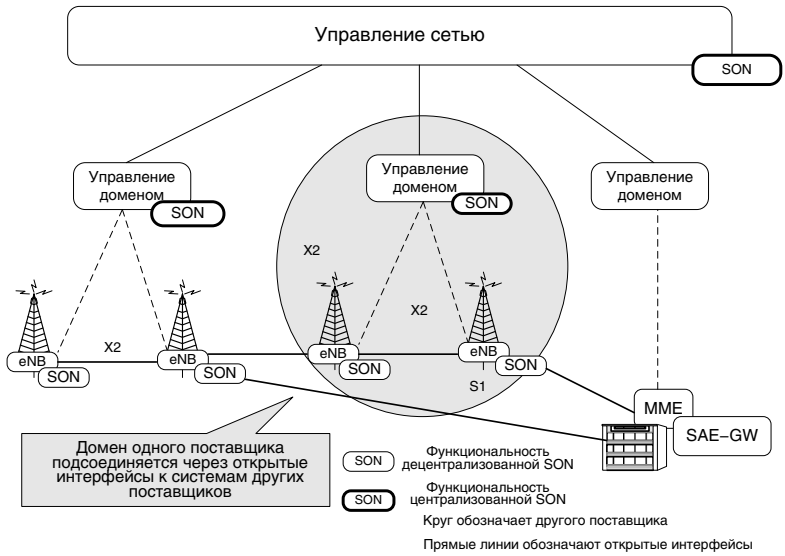

Рис. 4.5. Функции SON в архитектуре OAM&P консорциума 3GPP

На рис. 4.5 видно, что SON-функции располагаются на уровне управления сети NM (централизованная SON с использованием стандартных интерфейсов или интерфейсов от конкретного производителя), на уровне управления доменами DM (централизованная SON с использованием интерфейсов от конкретного производителя) и на уровне сетевых элементов NE (распределенная SON с использованием стандартных интерфейсов или интерфейсов от конкретного производителя, или местная SON, независимая от других и, следовательно, не требующая никаких интерфейсов). На всех этих уровнях в сети LTE выполняются основные группы функций SON:

- самоконфигурация – автоматическое переконфигурирование при реализации плана развертывания сети или при внедрении нового оборудования;
- самовосстановление – автоматическое обнаружение неисправности и ее устранение;
- самооптимизация – автоматическое перераспределение задач между элементами сети с целью эффективного использования сетевых ресурсов, отказоустойчивости, балансировки нагрузки, энергоэффективности, оптимизация емкости и покрытия сети, оптимизация контроля интерференции между смежными сотами и др.

Например, пул узлов управления мобильностью MME может быть общим для всех eNodeB, находящихся под управлением в этой области пула (MME pool area), согласно в 3GPP TS23.401.

Для соседних базовых станций eNodeB средства SON могут перераспределять пользовательский трафик из более нагруженной соты к менее загруженной соседней соте за счет тех пользовательских устройств, которые находятся в области радиопокрытия обоих eNodeB. Т.е. SON может улучшить производительность сети, может разгрузить MME от части сигнальной нагрузки, может управлять перераспределением пользовательского трафика между сотами.

Это особенно эффективно в тех местах, где распределение пользователей по сотам изменяется во времени: спортивные соревнования, массовые мероприятия, автомобильные пробки. Но решение о балансировке сигнальной нагрузки между MME, входящими в один пул, или о хэндовере пользовательского устройства на смежную eNodeB для разгрузки обслуживающей eNodeB должно рассматриваться и относительно пользователя согласно принципу «не навреди». Т.е. SON не осуществляет вынужденный хэндовер пользовательского терминала к смежной соте, если это ухудшит качество обслуживания QoS или сократит пропускную способность новой соты для пользователя по сравнению с сотой, обслужившей его до хэндовера.

Для планирования сети LTE на самой начальной стадии требуются весьма профессиональные проектировщики, значительная трудоемкость и соответствующие финансовые затраты. При этом потребности пользователей в скорости передачи данных и условия окружающей среды обычно быстро изменяются, и, следовательно, возникает необходимость анализа новой ситуации в сети и в переконфигурировании базовых станций как LTE, так и эксплуатируемых совместно с LTE сетей 2.5G и 3G. Более того, стратегия поэтапного внедрения LTE предусматривает целесообразность использования не только макро-eNodeB, но и узких решений микро-eNB, пико-eNB и фемто-eNB, а также Wi-Fi точек доступа. То есть ситуация с переконфигурированием сот еще более усложнится за счет такого разнообразия и количества базовых станций.

Сложнее станут и мобильные тесты, которые даже сейчас являются достаточно дорогими. Целесообразно при этом

расширять списки смежных сот за счет базовых станций, которые не являются смежными в данный момент, но находятся поблизости и могут быть потенциальными кандидатами на соседство. Но, во-первых, это ударит по энергопотреблению и без того слабых аккумуляторов современных пользовательских терминалов, т.к. абонентскому терминалу придется измерять уровень сигнала от канала BCCH большего числа базовых станций.

Во-вторых, это повысит количество неуспешных хэндоверов, увеличит вероятность прерывания речевых сеансов связи, снизит QoS. Поэтому для решения проблемы необходима оптимизация списков смежных сот. Оптимизированный, актуальный список соседств не только увеличит производительность каждой eNodeB и всего пула, но также улучшит пользовательское восприятие качества услуг и коэффициента готовности сети. Этого поможет достигнуть автоматическое установление соседских отношений средствами SON, позволяющее автоматизировать конфигурацию списка соседей каждой базовой станции.

Производительность сети тоже выигрывает от такой оптимизации и актуального списка соседств: например, соответствующая установка соседских отношений увеличит число успешных хэндоверов и уменьшит число обрывов связи из-за недостаточно актуального списка соседств. Именно для сети LTE/SAE с ее плоской архитектурой, без центральных узлов радиосети (например, без контроллеров базовых станций), необходимо конфигурировать большое число параметров соседств в каждой eNodeB всей сети. Притом делать это придется вручную, если не будет использоваться функция SON. Именно поэтому средства SON энергично разрабатываются и активно внедряются во всех разворачиваемых сегодня сетях 4G.

В заключение этого раздела заметим, что строго говоря, технология LTE/SAE в том виде, в каком она появилась в релизах 8 и 9, не является технологией поколения 4G.

В литературе ее принято относить к поколению 3.9G, а к полноценному четвертому поколению относить только LTE-Advance начиная с версии релиза 10. Впрочем, это не более чем вопрос маркировки. Важно то, что LTE-Advance является все той же технологией LTE, равно как и то, что история эволюции на LTE-Advance отнюдь не заканчивается, про что авторы предполагают еще написать в будущем.

Глава 5
Всепроникающие сенсорные сети

Наше тело все время говорит с нами.
Если бы мы только нашли время послушать.
Луиза Хей. «Душа и тело»

5.1. Основы появления сенсорных сетей как составляющей ССОП

Всепроникающие сенсорные сети *USN* (*Ubiquitous Sensor Networks*) являются одной из самых перспективных технологий XXI века. Дешевые и «умные» сенсоры, в довольно больших количествах объединенные в беспроводную сеть, подключенную к сети связи общего пользования, уже сегодня предоставляют беспрецедентно широкий набор услуг контроля и управления телами, домами, предприятиями, автомобилями и т.д. [17,24,39]. Сети USN, в зависимости от типа сенсоров, могут быть развернуты на земле, в воздухе, под и над водой [23,117], в зданиях и, наконец, на коже и внутри живых организмов, в частности человека. Они также находят широкое применение в таких важных областях, как военное дело, управление кризисными и чрезвычайными ситуациями, борьба с терроризмом и т.п. 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. Основные требования к USN могут быть сформулированы следующим образом.

- Объединение большого числа сенсоров в сеть. В большинстве сценариев развертывания сенсорных сетей, на момент написания книги, подразумевается стационарное местоположение сенсоров, причем их количество в сети может достигать нескольких десятков тысяч. В связи с этим важным аспектом эффективного функционирования сети является ее масштабируемость. Однако уже сегодня нельзя обойти вниманием и мобильные всепроникающие сенсорные сети, использование которых также охватывает все стороны деятельности человека и общества.
- Низкое потребление энергии. В связи с тем, что весьма существенная часть сценариев развертывания USN подразумевает нахождение сенсоров в труднодоступных местах, их обслуживание, в частности смена источников питания, может быть невыполнимой задачей. Именно поэтому время жизни сенсора зачастую ограничено временем жизни источника питания – задача снижения потребления энергии как никогда важна, и эффективность ее решения прямо влияет на эффективность и стоимость оборудования. Отметим, что существует ряд подходов, обеспечивающих достаточно продолжительное автономное функционирование сенсоров, например, когда в качестве источника питания используется солнечная батарея, но такое решение, к сожалению, накладывает существенные ограничения на область применения подобных сенсоров.
- Самоорганизация сети. Развертывание сенсорной сети существенно отличается от развертывания традиционных сетей. Зачастую сенсоры распределяются случайным образом по некоторой заданной территории (например, разбрасываются с самолета в тылу врага) и далее такой «набор» сенсоров должен самоорганизоваться в сеть – участие извне, например, администратора, невозможно. Самоорганизация должна быть динамической – выход из строя участников сети по причине, например, их физического уничтожения или разряда источников питания, должен быть определен оперативно, иначе эффективное функционирование сенсорной сети будет под угрозой.

Реализуется и непосредственное использование сенсоров в жизнедеятельности самого человека, а именно: контроль медицинских показателей, в частности, при его свободном перемещении, контроль местонахождения и физиологичес-

ких 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. Стандартизацией подобных сетей занимается рабочая группа IEEE 802.15.6. Оставляя вне дискуссии неприятные моральные аспекты такого развития сети, нам, тем не менее, придется признать, что подобное технологическое развитие безусловно приведет к несколько иным характеристикам общества, которое уже выйдет из стадии электронного.

Учитывая всепроникающий характер сенсорных сетей, вполне уместным кажется назвать такое общество *ubiquitous* [122,10,82]. 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 намечающимися проектами создания **u**-обществ за рубежом. Заметим, что до появления концепции u-общества сенсорные сети именовались *WSN* (*Wireless Sensor Networks*), однако сегодня общепринятой стала аббревиатура USN [100,105,106], во многом благодаря стандартам и проектам стандартов Международного союза электросвязи.

5.2. История создания сенсорных сетей

История создания сенсорных сетей насчитывает более четырех десятков лет [12]. Первые работы над сенсорами и сенсорными сетями были инициированы в оборонном секторе США. Как и в случае с другими технологиями, в том числе и телекоммуникационными (сеть Интернет). Естественно, подобные работы проводились и в СССР, однако до сих пор открытая информация об этом отсутствует.

В начале 50-х годов во время холодной войны с целью обнаружения и наблюдения за советскими малошумными подводными лодками была разработана и развернута система наблюдения *SOSUS* (*Sound Surveillance System*), состоящая из набора акустических сенсоров (гидрофонов), размещенных на дне океана [117]. Позже система SOSUS была переориентирована на гражданский сектор и до сих пор используется национальной океанографической и атмосферной ад-

министрацией *NOAA* (*National Oceanographic and Atmospheric Administration*) для мониторинга, например, сейсмической активности. Во время холодной войны в оборонном комплексе был также разработан противовоздушный комплекс защиты континентальной части территорий США и Канады.

Особенностью этого комплекса, позволяющей говорить о нем как о прототипе сенсорной сети, являлось использование аэростатов в качестве точек осуществления контроля и сбора информации. Позже эта система была дополнена самолетами воздушного предупреждения и управления *AWACS* (*Airborne Warning and Control System*). Эти две военные системы служат хорошим примером построения сенсорных сетей на очень ранней стадии их развития, когда речь о повышении эффективности, оптимизации, автономии и снижении стоимости еще не шла, а человек играл одну из основных ролей в процессе работы этих систем – именно на человека возлагалась ответственность за функционирование, надежность, анализ данных и т.п.

Работы над сенсорными сетями в современном понятии начались в 1980 г. [40] исследованиями в программе «Распределенные сенсорные сети» *DSN* (*Distributed Sensor Networks*), инициированной оборонным агентством по современным исследовательским проектам *DARPA* (*Defense Advanced Research Projects Agency*). Сеть Интернет, разработанная также в рамках агентства DARPA, к этому моменту уже успешно функционировала в течение нескольких лет и объединяла более 200 компьютеров в университетах и научно-исследовательских центрах и институтах США. Разработчиками сети Интернет в рамках проекта DSN были применены усилия по реализации принципов пакетной коммутации и стека протоколов TCP/IP в распределенных сетях, состоящих из простых устройств, позже названных сенсорами.

Аппаратная база для реализации сенсорных сетей в то время была достаточно слабой, и число уже разработанных технологий, которые могли бы быть применены, было сильно ограничено – модемы функционировали на скорости 9600 бод, а технология Ethernet только что вышла на рынок. В связи с этим участники проекта DSN были вынуждены как определять концепцию сенсоров и сенсорных сетей, так и непосредственно осуществлять техническую разработку.

Для поддержки проекта DSN агентство DARPA со своей стороны осуществляло руководство проектом, в связи с чем к этому проекту были также привлечены эксперты по искусственному интеллекту. Среди приоритетных областей исследований, с точки зрения проекта DSN, были определены распределенные вычисления, обработка сигналов и передача данных через беспроводный интерфейс. В первой половине 80-х был создан ряд тестовых сенсорных сетей, среди которых можно отметить следующие:

- тестовая сенсорная сеть под управлением операционной системы Accent, Carnegie Mellon University (США), 1981 г.,
- тестовая акустическая сенсорная сеть для наблюдения за маршрутами вертолетов, Massachusetts Institute of Technology (MIT) (США), 1984 г. [92],
- тестовая сенсорная сеть, усложненная алгоритмами распределенных вычислений, Advanced Decision Systems (США), 1986 г. [40].

Любая технология приносит успех и, соответственно, оправдывает капиталовложения и приносит прибыль лишь при выходе на общедоступный рынок. Как показывает опыт сети Интернет, технология, изначально разработанная для военных целей, может быть успешно применена в гражданском секторе. Выход сенсорных сетей на рынок в той концепции, в которой они были определены в 80-х годах, еще 7 – 8 лет назад был невозможен. Последние несколько лет стали решающими для сенсорных сетей – появились технологии, позволяющие производить сенсоры достаточно малого размера, оснащенные достаточным количеством процессорной мощности и памяти.

Оптимизация как различных алгоритмов и протоколов, так и архитектурных решений аппаратной части сенсора позволили существенно снизить объем потребляемой энергии и добиться беспрерывного функционирования сенсора без смены источника питания на срок более чем 1 – 2 года [16, 17]. Немаловажным фактором успеха сенсорных сетей на широком рынке является их стоимость. Уже сегодня, при очень низком объеме производства по сравнению с целевыми объемами, можно наблюдать приемлемые цены, когда один сенсорный узел стоит около 50 долларов США. Как уже отмечалось выше, прогнозы развития беспроводных устройств рассматривают число в 7 триллионов на горизонте планирования

до 2017 – 2020 годов. При этом стоимостные требования к сенсорным узлам должны быть в пределах десятков центов и единиц долларов в зависимости от приложений.

5.3. Архитектура сенсорных сетей

В главе 2 было введено понятие Ad Hoc сетей. Отмечалось, что Ad Hoc сети – самоорганизующиеся, в которых число элементов сети не является постоянным и, в общем случае, может изменяться в пределах от 0 до некоторого N_{max}.

Беспроводные сенсорные сети являются как раз таким примером самоорганизующихся Ad Hoc сетей, в которых нет общей инфраструктуры за исключением шлюзов связи с другими сетями. Каждый из узлов сенсорной сети должен иметь возможность функционировать как оконечный и как транзитный узел. Действительно, передача данных в сенсорных сетях осуществляется путем их перенаправления к ближайшему узлу шаг за шагом.

Такие сети называются многошаговыми (*multihop*). Следует отметить, что могут существовать и более сложные алгоритмы маршрутизации, когда следующий узел выбирается на основе анализа его характеристик, например, затрат энергии, надежности и т.д. При наличии мобильных сенсорных узлов архитектура самоорганизующейся сенсорной сети становится к тому же и динамической.

В [22, 25] сенсорные сети определяются как «распределенные сети, состоящие из маленьких беспроводных узлов узкой специализации в большом количестве рассредоточенных (случайно) на некоторой поверхности или области» (рис. 5.1). Таким образом, сенсорная сеть представляет собой сравнительно большое множество беспроводных сенсоров, распределенных в некоторой области с достаточно высокой плотностью. В области покрытия радиосигнала каждого из сенсоров должен находиться как минимум еще один сенсор, в этом случае сенсор будет называться соседним. Чем больше «соседей» у каждого из сенсоров, тем более высокой точностью и надежностью обладает сенсорная сеть – очевидно, что отдельный сенсор имеет ограниченную область восприятия, вычислительную мощность, память и питание. Технологии радиодоступа, применяемые в сенсорах и основанные на стандарте IEEE 802.15.4, позволяют передавать данные на расстояние до нескольких десятков метров.

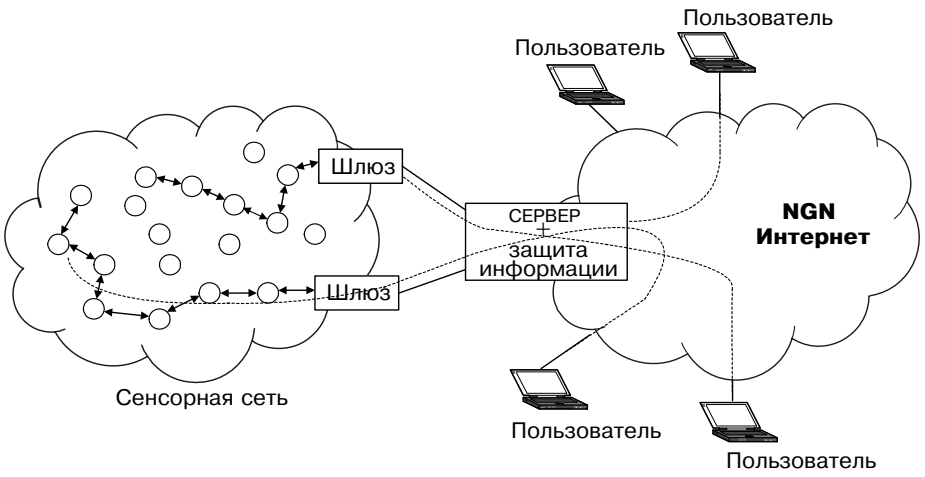

Рис. 5.1. Пример подсоединения сенсорной сети к сети связи общего пользования

Естественно, что чем выше количество соседних сенсоров у каждого из сенсоров, тем более высокой точностью и надежностью обладает сенсорная сеть – в связи с этим предполагается, что в некотором пространстве, где построена сенсорная сеть, сенсоры будут распределены с достаточно высокой плотностью и, соответственно, в большом количестве. Эта сеть, как правило, имеет присоединение к сети связи общего пользования для передачи полученных данных. Присоединение производится посредством некоторого шлюза, который может также реализовывать функции защиты. Отметим, что шлюз обычно не является сенсором, а представляет собой более стабильный сетевой узел (с точки зрения источника питания и ресурсов). Данные могут передаваться как для обработки на серверы, так и прямо заинтересованным пользователям. Очевидно, что сенсорная сеть, состоящая из большого количества сенсоров, должна быть структурирована, т.к. большой объем передаваемой информации может снизить надежность тех узлов, которые находятся в непосредственной близости к шлюзу – постоянная передача транзитных данных может привести к выходу из строя источника питания, а большой объем трафика – переполнить буферы приема.

Кластерная организация является масштабируемой и считается эффективной для решения подобных задач (рис. 5.2), но лишь при условии рационального выбора голов-

ного узла в кластерной сети и в подходящий момент времени [53,116,126].

Действительно, являющийся головным в момент времени t_1 сенсорный узел не обязательно должен быть им же в другой момент времени, так как 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*) [56, 57]. Алгоритм LEACH предусматривает вероятностный выбор сенсорного узла на роль головного в начале функционирования сенсорной сети, а впоследствии ротацию на основе энергетических характеристик других сенсорных узлов. Подобное решение, естественно, увеличивает длительность функционирования сенсорных узлов и сети в целом, но, как будет показано далее, 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 алгоритмы, использующие в качестве критерия количество остаточной энергии, местоположение узла-кандидата на головной кластерный узел по отношению к другим узлам, информацию о топологии сети в текущей момент времени.

Например, алгоритм *HEED* (*Hybrid Energy – Efficient Distribution*) [125] 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 к качеству обслуживания, схоластична.

В системах мониторинга одним из важнейших требований является непрерывность, т.е. обеспечение мониторинга параметров на всем пространстве или на протяжении всего процесса. 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 как оптимизацию 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 более подробно примеры алгоритмов выбора головного узла в беспроводных сенсорных сетях.

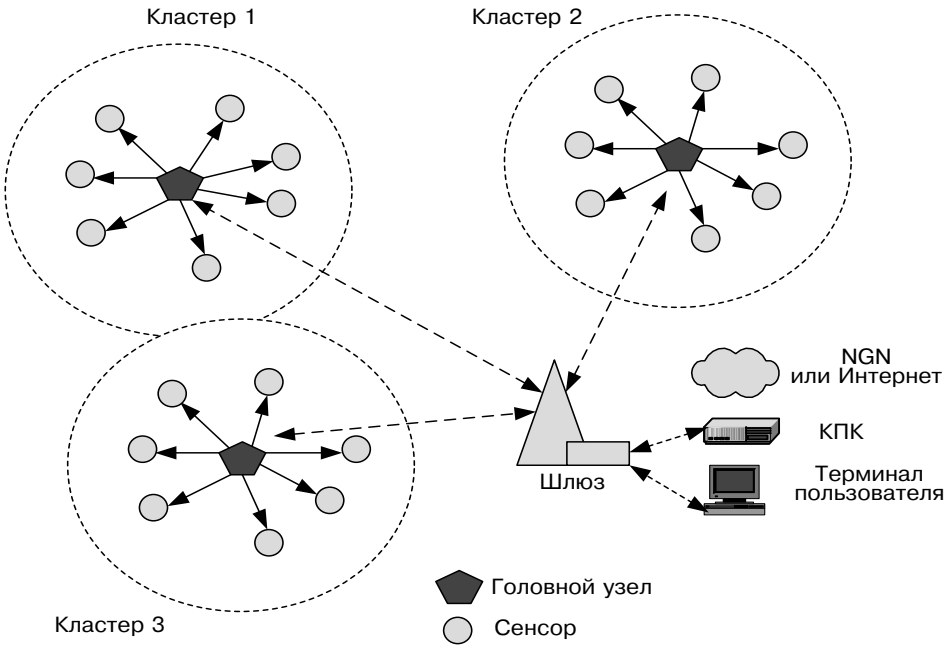

Рис. 5.2. Кластерная архитектура USN

Одним из важнейших параметров при построении сенсорных сетей является потребление энергии. Сенсорный узел в силу своего размера может быть оборудован источником питания со сравнительно небольшим ресурсом. В определенных приложениях сенсорных сетей, например, для решения тактических задач в тылу врага, сенсорный узел является необслуживаемым устройством, и замена источника питания не представляется возможной. Учитывая то, что сенсорный узел может выполнять роль как терминала, так и транзитного узла, увеличение срока действия источника питания является одной из приоритетных задач, которая решается не только путем увеличения времени жизни источника питания, но и путем эффективного его использования.

Учитывая известное классическое соотношение потребления энергии мобильным узлом [111], говорящее о том, что соотношение потребления энергии при «передаче; приеме; ждущем режиме; спящем режиме» представляется соотношением «13: 9: 7: 1», усиленное внимание уделяется снижению времени передачи и приема информации и повышению доли времени, когда сенсор находится в ждущем или спящем режиме. Это необходимо учитывать при разработке алгоритмов маршрутизации.

5.4. Архитектура сенсоров

Сенсор, как и любой телекоммуникационный узел и/или терминал, состоит из аппаратной части и программного обеспечения. Как показано на рис. 5.3, в общем случае сенсор состоит из следующих подсистем: мониторинга и восприятия, обработки данных, а также коммуникационной подсистемы и источника питания.

Подсистема мониторинга и восприятия позволяет сенсору собирать такие данные об окружающей среде как температура, сила света, вибрация, ускорение, магнитное поле, химический состав воздуха, акустика и т.п. Именно эта подсистема определяет ту область или приложение, в котором сенсор может быть использован. Сенсор опционально может быть дополнен и другими подсистемами, такими как, например, позиционирование, генератор электроэнергии и т.п.

Подсистема мониторинга и восприятия содержит аналоговое устройство, непосредственно снимающее определенную

статистику, и аналого-цифровой конвертор, преобразующий аналоговые данные в цифровые для последующей обработки.

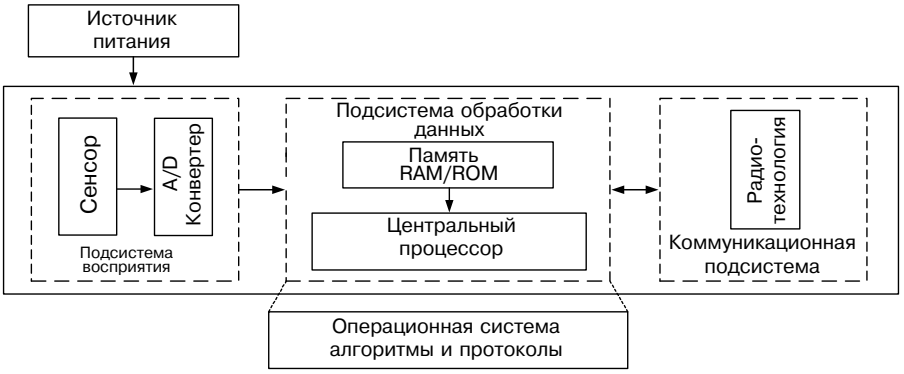

Рис. 5.3. Архитектура сенсорного узла

Подсистема обработки данных включает в себя память и центральный процессор, позволяющие хранить и обрабатывать как генерируемые сенсором данные, так и служебные данные, необходимые для корректного и эффективного функционирования коммуникационной подсистемы.

Важнейшими техническими аспектами реализации сенсора как малого размера телекоммуникационного устройства со сложными функциями, являются следующие.

- **Архитектура**. На сегодня требования к аппаратной части сенсора могут быть такими: частота центрального процессора не менее 20 МГц, объем оперативной памяти не менее 4 КБ, скорость передачи не менее 20 кбит/с. Оптимизация аппаратного обеспечения позволяет снизить размеры сенсора, однако, как правило, это влечет за собой повышение его цены.
- **Операционная система**. Оптимизация операционной системы (ОС) с учетом архитектуры применяемого центрального процессора является необходимой. На сегодня наиболее популярной является ОС с открытым кодом Tiny OS [120], позволяющая достаточно гибко управлять сенсорами разных производителей.
- **Сетевое взаимодействие**. Ограниченный источник питания накладывает существенные ограничения на радиотехнологию, которая может быть эффективно применена

в сенсорных сетях. Более того, ограниченная производительность центрального процессора не позволяет применять стандартные протоколы маршрутизации IP-сетей – высокая сложность расчета алгоритма оптимального пути перегрузит центральный процессор сенсора. Разработано большое количество специальных протоколов маршрутизации для сенсорных сетей.

Помимо рассмотренной классической архитектуры сенсорного узла возможны и другие, что связано, например, с необходимостью не только мониторинга или контроля измеряемых характеристик, но и воздействия на объект измерений. Такой элемент, имеющий возможность воздействия на объект, называется *актором* [94] и его архитектура приведена на рис. 5.4.

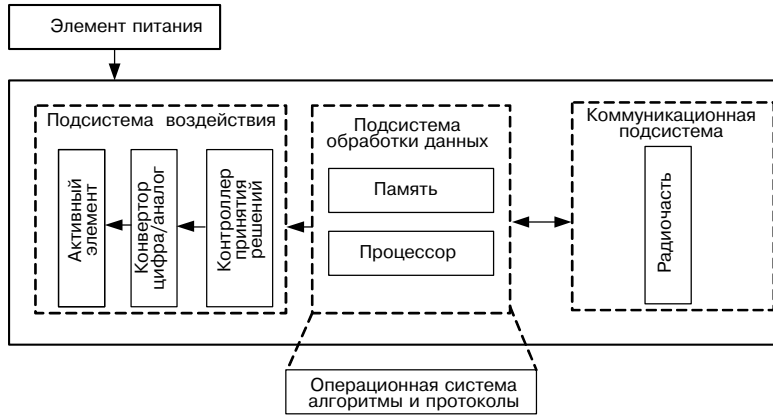

Рис. 5.4. Архитектура акторного узла

Архитектура актора подобна архитектуре сенсорного узла и отличается тем, что с внешней средой взаимодействует активный элемент, например, устройство ввода инсулина больному диабетом. Кроме того, в архитектуре актора отдельно выделяется контроллер принятия решения о воздействии на внешнюю среду. Естественным выглядит возможность объединения актора и сенсора в один узел, архитектура которого представлена на рис. 5.5. Помимо сенсоров и акторов среди беспроводных технических средств мониторинга и контроля целесообразно рассмотреть также радиоидентификаторы *RFID* (*Radio Frequency Identification*), которые не имеют измерительной части, но могут широко использоваться и используются, например, в системах позиционирования.

RFID классифицируются на активные и пассивные. Архитектура активного RFID практически не отличается от архитектуры сенсорного узла.

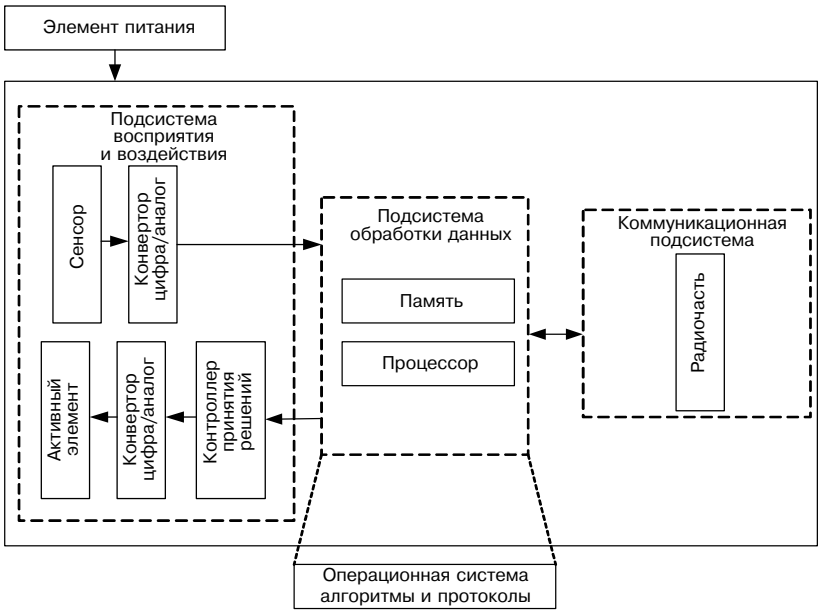

Рис. 5.5. Архитектура комбинированного сенсорно-акторного узла

Существенно более простую архитектуру имеет пассивный RFID, характеризуемый отсутствием элемента питания и необходимостью специального технического устройства – ридера – для считывания информации с него. Архитектура пассивного RFID приведена на рис. 5.6.

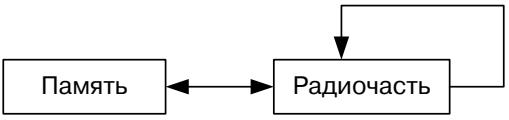

Рис. 5.6. Архитектура пассивного RFID

Как видим, существует достаточно большое разнообразие технических средств, из которых можно конструировать сенсорные сети. Выбор конкретных решений для сенсорных узлов при создании беспроводной сенсорной сети в первую очередь зависит от функциональных возможностей, размера,

затрат, энергетических характеристик, а в настоящее время, с учетом начала довольно широкого внедрения сенсорных сетей – от обеспечения требуемого качества обслуживания [14, 15]. Примеры конструкций современных сенсорных узлов приведены на рис. 5.7.

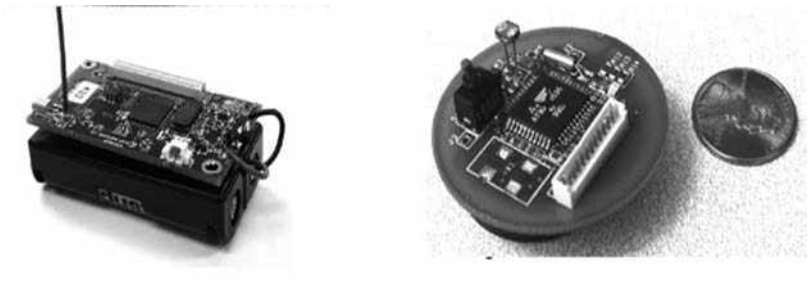

Рис. 5.7. Сенсорные узлы

5.5. Алгоритмы маршрутизации 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 будет получена от разных сенсорных узлов, функционирующих в какой-либо зоне. Кроме того, размеры сенсоров и затраты на них лимитированы так же, как и их ресурсы: энергия, память, вычислительные возможности. Поэтому, передавать одну и ту же информацию по сети от многих сенсорных узлов нецелесообразно. Исходя из сказанного, 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 и управления должны быть достаточными для обеспечения автономного существования.

Энергетическая эффективность. Наблюдая 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, критических 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 [129] 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 определенным уровнем качества обслуживания.

Толерантность к отказам. В отличие от традиционных сетей беспроводные сенсорные сети организуются случайным образом, 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 не должно вызывать существенных последствий как для сенсорной сети в целом, так и для ее фрагментов. Другими словами, USN должна быть нечувствительна к отказу какого-либо сенсорного узла и должна продолжать поддерживать далее требуемый уровень качества обслуживания.

Точность и качество. Обеспечение достаточной точности и актуализация 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 минимальными энергозатратами.

5.5.1. Классификация алгоритмов маршрутизации в USN

Многие исследователи предлагали разные решения по алгоритмам маршрутизации для USN с учетом требуемых особенностей, изложенных выше. Предложенные алгоритмы маршрутизации в USN могут быть объединены в различные группы в соответствии с критериями, разработанными в [21, 30].

В табл. 5.1 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 имеют одинаковые функциональные возможности. Собранные данные передаются в сеть посредством многоранговой маршрутизации. Алгоритмы в одноуровневой сети должны обеспечить передачу большого объема транзитной информации через сеть и, естественно, они ориентированы на приложения.

В основном, алгоритмы для одноуровневой сети являются централизованными, поскольку их основная задача состоит в обеспечении транзита данных через однородную сенсорную сеть. Во многих случаях алгоритмы для одноуровневой сети довольно сложны, поскольку существуют как масштабирование, так и динамическое изменение топологии USN.

Алгоритмы *SPIN* (*Sensor Protocols for Information via Negotiation*) [55] и *DD* (*Direct Diffusion*) [78] являются базовыми для одноуровневой беспроводной сенсорной сети, и на их основе разработаны все последующие одноуровневые алгоритмы. В иерархических сетях сенсорные узлы играют разную 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 при необходимости направляют ее на следующий уровень.

Рассмотрим для примера трехуровневую иерархическую беспроводную сенсорную сеть. Головные узлы кластеров взаимодействует с узлами сети связи общего пользования. Каждый головной узел собирает данные с узлов своего кластера, агрегирует их и передает далее. Все иерархические алгоритмы маршрутизации должны обеспечивать выбор наилучшего СН. 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 и других факторов, таких как энергопотребление, покрытие и т.д.

Таблица 5.1. Простая классификация алгоритмов маршрутизации

Критерий	Категория	Примеры
Сетевая структура	Одноуровневая	SPAN [37]
	Иерархическая	LEACH [56]
Знания о ресурсах	На основе остаточной энергии	HEED [125]
	На основе точности расположения	Directed Diffusion [78]
Управление протоколами	Централизованное	SPAN [37]
	Географическое	GFG [78]
	На основе QoS	SAR [115]
	На основе теории очередей	COUGAR [124]

Сравнивая одноуровневые и иерархические алгоритмы маршрутизации, можно отметить, что иерархические алгоритмы предоставляют больше возможностей продвижения разных приложений USN. Следующие характеристики иерархических алгоритмов были отмечены в исследовательских работах [13,21,30,125]:

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

транзит обеспечивается СН). За счет агрегации данных головной узел кластера уменьшает поток заявок во внешнюю сеть.

- Иерархическая маршрутизация позволяет гибко решать различные задачи с учетом возможностей сенсорных узлов. Иерархическая маршрутизация позволяет балансировать нагрузку сети. При этом узлы с высокой энергоемкостью (возможно с постоянным энергоснабжением) могут агрегировать данные и передавать их в сеть связи общего пользования, в то время как узлы с низкой энергоемкостью 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 определенному расписанию передачи, приема и чтения информации. Следовательно, сенсорные узлы могут расходовать меньше энергии, находясь в состоянии покоя и активизируясь только во временные интервалы передачи, приема и чтения. В результате, естественно, снижаются коллизии в кластере, и сеть может обслужить более высокую нагрузку. Иерархическая маршрутизация в связи с этим часто используется для крупномасштабных беспроводных сенсорных сетей, состоящих из сотен и тысяч узлов.
- Иерархическая маршрутизация проста в реализации. Хотя одноуровневая маршрутизация может использовать оптимальные маршруты, ее реализация, как правило, достаточно сложна. Ограниченные возможности сенсорных узлов при этом могут стать проблемой для реализации сложных алгоритмов и схем. Иерархическая маршрутизация предполагает разделение соединений на внутрикластерные и внешние. Только головной узел кластера отвечает за внешние соединения, в то время как члены кластера взаимодействуют лишь на внутрикластерном уровне. Такая простая маршрутизация уменьшает число сообщений в кластере.
- Иерархическая маршрутизация позволяет упростить рассылку запросов по сравнению с одноуровневой. 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 учетом возможностей и необходимости. Такой подход также позволяет уменьшить число сообщений.

Хотя иерархическая маршрутизация обладает и недостатками, такими, к примеру, как дополнительные затраты времени на синхронизацию и больший заголовок для кластерного управления, тем не менее, с учетом изложенного выше, иерархическая маршрутизация является предпочтительной для построения USN, особенно крупномасштабных.

5.6. Алгоритмы выбора головного узла в кластере

Далее, в соответствии с вышеизложенным, будут рассмотрены алгоритмы для иерархических беспроводных сенсорных сетей. Основной проблемой при создании алгоритмов для таких сетей является выбор головного узла кластера. Существует два подхода к выбору головного узла кластера: случайный выбор и предопределенный выбор. Рассмотрим далее алгоритм случайного выбора головного узла, при использовании которого ротация головных узлов может производиться между всеми членами кластера с учетом их характеристик в текущий момент времени.

5.6.1. Алгоритм случайного выбора головного узла LEACH

Иерархический алгоритм адаптивной кластеризации с низким потреблением энергии *LEACH* (*Low-Energy Adaptive Clustering Hierarchy*) [56] предполагает обеспечение баланса расхода энергии в беспроводной сенсорной сети. Алгоритм LEACH является базовым, существует множество алгоритмов, основанных на нем. Базовая идея LEACH состоит в следующем: сенсорные узлы могут быть случайным образом выбраны как головные на основе информации об их функционировании в предыдущий момент времени. При этом в кластере каждый сенсорный узел генерирует случайное число из интервала [0, 1].

Каждый сенсорный узел имеет порог T_h (LEACH), который соответствует предварительно определенному 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 остается только членом кластера. Вычисление T_h (LEACH) является ключевой задачей при реализации алгоритма LEACH.

$$T_h(LEACH) = \begin{cases} \dfrac{p}{1 - p \cdot (r \cdot \bmod \dfrac{1}{p})}, & \text{если} \quad h \in G \\ 0, & \text{в остальных случаях} \end{cases} \qquad (5.1)$$

В формуле (5.1) величина 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 оптимизации энергетических затрат каждого из сенсорных узлов сети. Кроме того, при выборе головного узла другие сенсорные узлы выбирают одного из членов кластера для контроля мощности получаемого сигнала *RSS* (*Received Signal Strength*) от головного узла.

После того, как кластер сформирован, головной узел рассылает расписание передачи и запрашивает у членов своего кластера передачу 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 определенного 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 довольно 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 [56]. В то же время LEACH не дает гарантии выбора «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 избиравшийся член кластера с неудовлетворительными энергетическими характеристиками.

5.6.2. Алгоритм HEED с предопределенным выбором головного узла

Гибридный распределенный энергоэффективный алгоритм кластеризации *HEED* (*Hybrid Energy – Efficient Distributed*) [125] является развитием алгоритма LEACH. Для преодоления проблемы выбора «плохого» члена кластера в качестве головного узла в LEACH, алгоритм HEED предлагает использовать предопределенный выбор головного узла.

Алгоритм HEED ставит вероятность выбора узла головным в зависимость 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 энергоемкости 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 далеко от шлюза с сетью связи общего пользования, он может передать агрегированную информацию через головной узел другого кластера.

5.6.3. Алгоритм ERA случайного выбора головного узла

Алгоритм осведомленности об остаточной энергии *ERA* (*Energy Residue Aware*) [38] представляет собой еще один алгоритм иерархической маршрутизации. Алгоритм ERA тоже является развитием алгоритма LEACH и включает в анализ вопроса выбора головного узла в кластере затраты на осуществление взаимодействия. Затраты на осуществле-

ние 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 счет использования дополнительных параметров, определенных выше.

Уравнения (5.2) помогают определять затраты кластера при выборе того или иного узла в качестве головного и найти головной узел кластера с максимальной остаточной энергоемкостью. В (5.2) множество S_c является множеством для головных узлов, множество S_N является множеством для членов кластера.

$$\begin{cases} (E_{CH-res})_i = (E_{CH-rem})_i - (E_{toBS})_i, & i \in S_c \\ (E_{nonCH-res})_j = (E_{nonCH-rem})_j - (E_{toBS})_{ji}, & j \in S_N, \forall i \in S_c \\ \max\{(E_{CH-res})_i + (E_{nonCH-res})_j \mid \forall i \in S_c\} & j \in S_N \end{cases} \quad (5.2)$$

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

5.6.4. 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 рассмотрена далее для полноты анализа основных алгоритмов маршрутизации в USN.

Алгоритм PEGASIS [88, 89] предусматривает 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 так, 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 исполь-

зует 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 передается информация, а ротация первого сенсора в цепочке увеличивает длительность функционирования отдельных сенсорных узлов. Такой подход позволяет снизить общее энергопотребление для беспроводных сенсорных сетей и увеличить длительность функционирования USN в целом.

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 [88]. Алгоритм иерархический PEGASIS использует CDMA для кодирования сигналов и пространственное разделение сенсорных узлов. Алгоритм строится в виде иерархического дерева, причем каждый выбранный узел какого-либо уровня передает 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.

5.6.5. Алгоритм RRCH

Алгоритм циклической очередности выбора головного узла в кластере *RRCH* (*Round-Robin Cluster Head*) [93] предполагает формирование кластера только единовременно. После фиксации кластера для выбора головного узла в нем на протяжении его функционирования используется известный метод циклической очередности [15]. Так же, как и в LEACH, каждый из членов кластера может стать головным узлом, головной узел задает расписание для членов кластера и т.д.

С учетом 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 жесткая фиксация кластера приводит к тому, что

один из кластеров может перестать выполнять свои функции с надлежащим качеством обслуживания быстрее, чем в LEACH, в котором рекластеризация приводит к возможности распределить ресурсы равномерно между всеми кластерами одной сенсорной сети.

5.7. Алгоритм распределенной кластеризации

5.7.1. Мобильные сенсорные сети

В последние годы появился новый вид сенсорных сетей – это мобильные сенсорные сети *MSN* (*Mobile Sensor Networks*). Эти сети сохранили все особенности беспроводных сенсорных сетей USN и, кроме того, к этим особенностям добавилась мобильность.

Кластерная архитектура нашла применение и в MSN, 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. Появилось довольно много исследований проблем создания беспроводных мобильных сенсорных сетей в области алгоритмов маршрутизации, покрытия, управления ресурсами, защиты и т.д. Формируется следующий этап в развитии беспроводных сенсорных сетей. Алгоритмы кластеризации в стационарных USN [31] не могут адекватно отражать процессы в MSN, требуется разработка новых алгоритмов.

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

Заметим, что в отличие от беспроводных сетей другого типа – мобильных Ad Hoc сетей [35, 109], именуемых MANET, где мобильность рассматривается как неконтролируемый фактор, в MSN мобильность может рассматриваться как ценная управляемая способность [558, 59], посредством которой смогут быть получены более интеллектуальные и более гибкие и адекватные внешним условиям сенсорные сети, чем стационарные USN.

Например, в [80] управляемая мобильность введена в сенсорный узел для обеспечения устойчивости сети. Указанный подход, правда, основан на использовании предварительно определенных кабельных сетей и не позволял строить сеть для случайных событий. Подобный подход можно увидеть и в [113] для процессов размножения, когда сенсорный узел имеет возможность использовать три разные кабельные сети для оптимизации покрытия.

Естественным в этих условиях выглядит появление алгоритма LEACH – Mobile или LEACH – M [83] 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 [56], к динамическому вхождению и выбытию не головных узлов кластера в устойчивой фазе, когда члены кластера 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 времени жизни сети и стабильность сформированного кластера за счет использования комбинированного критерия прогнозирования.

5.7.2. Комбинированный критерий прогнозирования

В разделе предлагается комбинированный критерий прогнозирования, основанный на трех эвристических предикторах [84].

5.7.2.1. Критерий связности

Связность является мерой возможностей взаимосвязи любого из сенсорных узлов с любым другим сенсорным узлом в сети. На рис. 5.8 связность иллюстрируют зеленые линии между сенсорными узлами. Рассмотрим мобильную беспроводную сенсорную сеть, состоящую из достаточно большого числа сенсорных узлов, обозначенных как $S = \{s_1, ..., s_n\}$. Сенсорные узлы распределены на обширном сенсорном поле и предназначены для детектирования специфических событий.

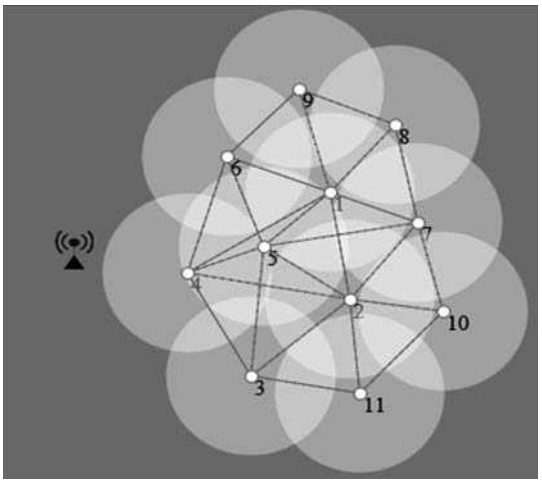

Рис. 5.8. Связность в сенсорной сети

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_1, будем называть пределом взаимосвязи (R_i) сенсорного узла s_j.

Множество близлежащих к сенсорному узлу сенсоров представим как $N(s_i)$. Тогда $N(s_i)$ определяется из следующего уравнения:

$$N(s_i) = \{s_j : \quad d(s_i, s_j) < R_i\} \tag{5.3}$$

В (5.3) параметр *d* – Евклидово расстояние между сенсорными узлами s_i и s_j. С учетом изложенного, критерий связности $ConC(s_i)$ в момент времени *T* может быть записан следующим образом:

$$ConC(s_i) = |N(s_i)|. \tag{5.4}$$

5.7.2.2. Критерий покрытия

Большинство подходов к выбору головного узла в кластере основано на балансе энергетических возможностей сенсорных узлов, но, как уже было отмечено выше, с точки зрения качества обслуживания целесообразно рассматривать про-

блему полного покрытия в течение достаточно большого периода времени [60], особенно для систем мониторинга. Предел действия *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 $\left[\theta_{ij}^s, \theta_{ij}^e\right]$, θ^s и θ^e 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, согласно теореме косинусов, длина L_{ij} сегмента Seg_{ij}:

$$L_{ij} = \arccos\left\{\frac{r_i^2 + d^2 - r_j^2}{2d + r_i}\right\}. \qquad (5.5)$$

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

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

- сегмент А 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, по одному с каждой стороны, за исключением двух сегментов (первый и последний сегменты), каждый из которых перекрывает только один сегмент в SL_i.

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

$$CovC(s_i) = \frac{Cov(s_i)}{2\pi}. \qquad (5.6)$$

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

$$Cov(s_i) = \sum_{\forall Seg_{ij} \in SL_i} \left| Seg_{ij} \right| - \sum_{\forall Seg_{ij}, Seg_{ik} \in SL_i : j \neq k} \left| Seg_{ij} \cap Seg_{ik} \right| . \qquad (5.7)$$

5.7.2.3. Критерий мобильности

Мобильность, естественно, является важнейшим фактором в принятии решения о выборе головного узла. С учетом частого 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:

$$MC(s_i) = \frac{\sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2}}{\Delta t} . \qquad (5.8)$$

В (5.8) $(x_t - y_t)$ и $(x_{t-1} - y_{t-1})$ – координаты сенсорного узла s_i в моменты времени *t* и *t*-1, а Δt – интервал времени между *t* и *t*-1.

5.7.2.4. Критерий остаточной энергии

Головные узлы кластеров отвечают за координацию взаимодействия членов кластера, агрегацию данных и их передачу прямо на базовую станцию или через многоранговые соединения. Поскольку головной узел кластера нуждается в приеме большого числа пакетов, он затрачивает больше энергии, чем все другие узлы. В 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:

$$REC(s_i) = E(s_i) . \qquad (5.9)$$

С учетом 5.4, 5.6, 5.8 и 5.9 комбинированный критерий $CC(s_i)$ для сенсорного узла s_i в момент времени *t* определяется следующей формулой:

$$CC(s_i) = \alpha \cdot ConC(s_i) + \beta \cdot CovC(s_i) + \frac{\gamma}{1 + MC(s_i)} + \xi \cdot REC(s_i). \quad (5.10)$$

В выражении (5.10) сумма $\alpha + \beta + \gamma + \xi = 1$.

5.7.3. 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 $t_1 < t_2 < .... < t_n$. Для этого могут быть использованы:

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

$$PCC = SPP(t_c) = CC_n. \quad (5.11)$$

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

$$PCC = LEP(t_c) = \frac{t_c - t_{c-1}}{t_n - t_{n-1}}(CC_n - CC_{n-1}) + CC_{n-1}. \quad (5.12)$$

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

$$PCC = \begin{cases} CC_n & n\text{-нечетное} \\ \dfrac{t_c - t_{c-1}}{t_n - t_{n-1}}(CC_n - CC_{n-1}) + CC_{n-1}, & n\text{-четное} \end{cases} \quad (5.13)$$

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

Рассмотренные предикторы широко используются в мо-

бильных сетях для предсказания маршрута перемещения мобильных станций. Именно эти предикторы выбраны для построения алгоритмов выбора головного узла в мобильных сенсорных сетях.

5.7.4. Распределенный алгоритм кластеризации

Рассмотрим новый алгоритм кластеризации *DCA* (*Distributed Clustering Algorithm*) [84].

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 самый последний сенсорный узел. Этот динамический параметр определяет процедуру формирования кластера и служит как входной параметр для процесса формирования кластера. DCA содержит две фазы: информационное обновление и формирование кластера. В фазе информационного обновления каждый сенсорный узел вычисляет свои предикторы комбинированного критерия *PCC*. Далее, базируясь на значении кластер-хопа γ_{hop}, осуществляется процесс распространения *PCC*. Во время формирования кластера сенсорные узлы уже обладают информацией о близости других узлов и информацией о *PCC*.

5.7.4.1. 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* передается в радиусе близлежащим сенсорным узлом. Полностью алгоритм распространения информации о *PCC* приведен в табл. 5.2.

В результате действия алгоритма каждый сенсорный узел сети имеет информацию об узлах, для которых PCC является наибольшим в области γ_{hop} для близлежащих узлов.

Таблица 5.2. 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 $\Upsilon_{cl} > 0$ do
5	Transmit Max_i в $s_j \forall s_j \in N(s_i)$
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	$\gamma_{cl} = \gamma_{cl} - 1$
15	end while

Синхронизация между узлами для реализации алгоритма не требуется вследствие того, что сенсорные узлы верифицируются при распространении информации о *PCC* в предварительно определенный промежуток времени. Алгоритм *PCC* позволяет формировать большие кластеры, ограниченные только значением радиуса γ_{hop} .

5.7.4.2. Фаза 2: формирование кластера

После определения сенсорных узлов с наибольшим значением PCC можно перейти ко второй фазе алгоритма, на которой непосредственно формируется 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, причем допуск сенсорных узлов в кластер осуществляется кластером самостоятельно. Для реализации

указанного подхода разработан распределенный кластерный алгоритм *DCA* (*Distributed Cluster Algorithm*), приведенный в табл. 5.3.

Таблица 5.3. Распределенный кластерный алгоритм (DCA)

1	if ($Max_{id} = i \; or \; My\_Cluster\_Head$ 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 $s_j = Maxi.id$ as Cluster head
6	Broadcast a $My\_Cluster\_Head$ message to s_i
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 он 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 со всех сенсорных узлов своего кластера в маршрутную таблицу и формирует ее в зависимости от поступивших сообщений Join.

5.7.5. Результаты моделирования

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

При моделировании использовалась стандартная энергетическая модель, когда все энергозатраты разделяются на две части: передача и прием сообщений. Параметры и их значения, используемые при моделировании, сведены в табл. 5.4 и соответствуют типовым при исследованиях вопросов кластеризации в сенсорных сетях.

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 [83].

Таблица 5.4. Параметры и их значения, используемые при моделировании

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

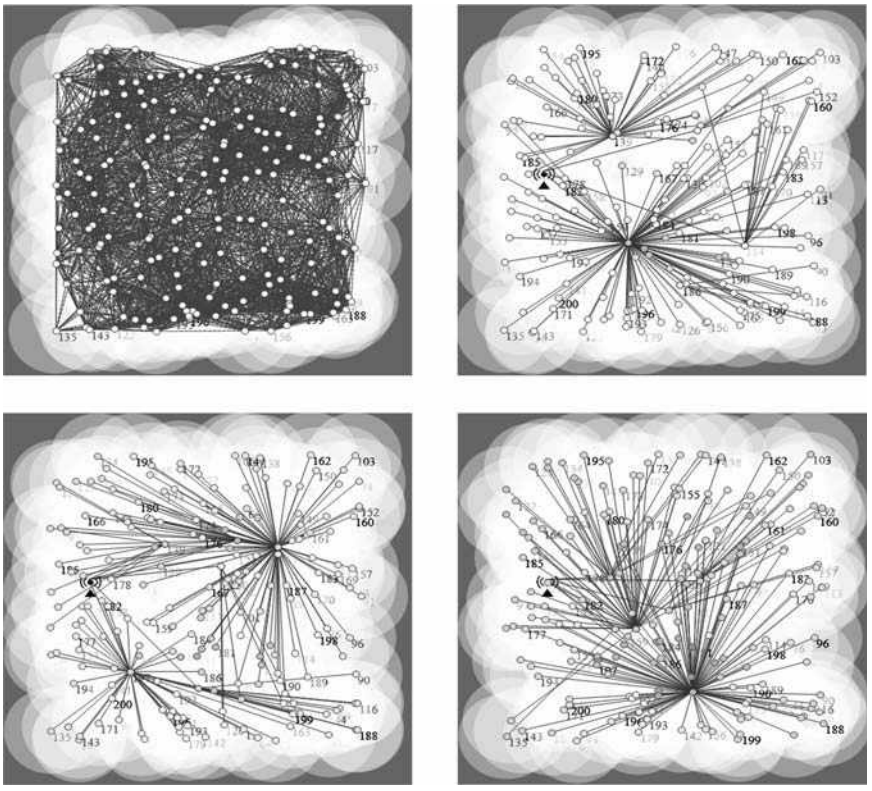

Рис. 5.9. Отображение модели на экране

Для оценки эффективности алгоритмов используется метрика жизненного цикла сети – интервал времени между началом функционирования и гибелью последнего из живущих сенсорных узлов.

5.7.5.1. 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.

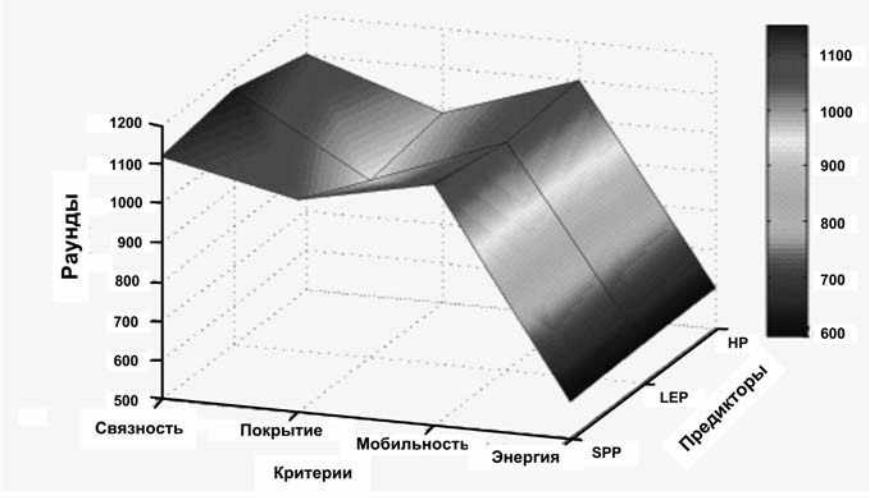

Рис. 5.10. Эффективность критериев в DCA

На рис. 5.10 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.

5.7.5.2. 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 $\alpha = \beta = \gamma = \zeta = 0.25$.

На рис. 5.11 шлюз расположен в центре сети. Простые расчеты могут показать, что в этом случае достигается минимальное значение Евклидова расстояния между узлами и шлюзом. На рис. 5.11 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.

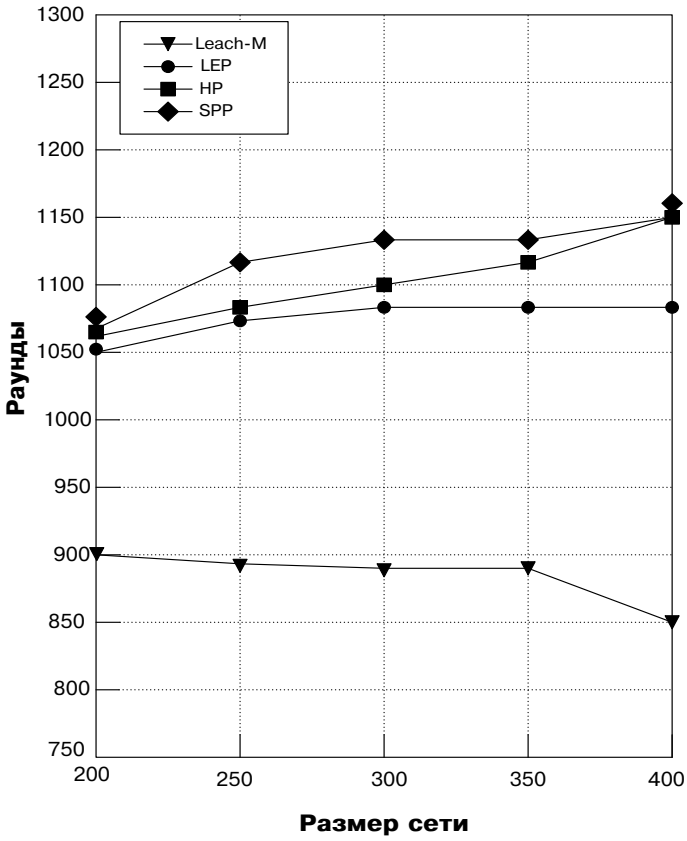

Рис. 5.11. Жизненный цикл сети с использованием различных версий DCA в сравнении с LEACH-M в случае, когда шлюз расположен в центре сети

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.

В алгоритме же DCA головной узел выбирается с учетом множества критериев, что и обеспечивает хорошее распределение головных функций среди сенсорных узлов.

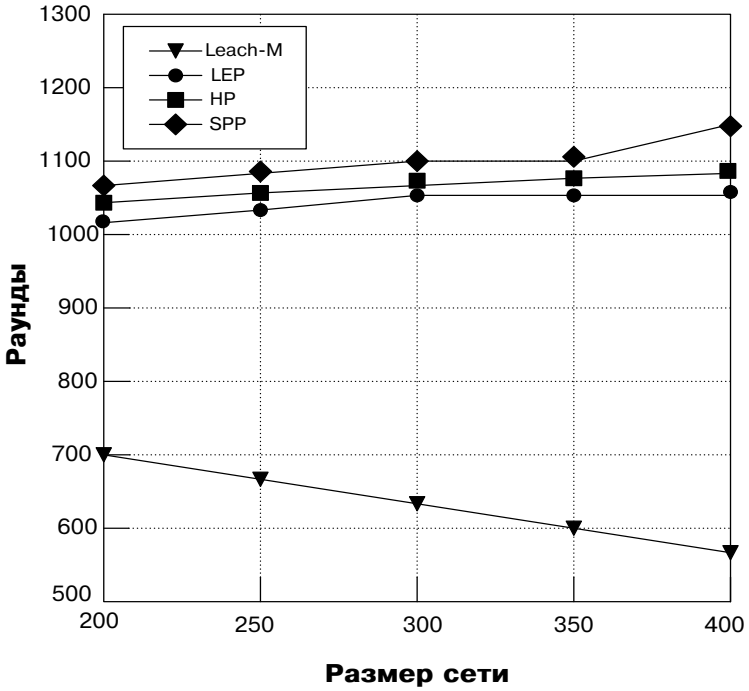

Рис. 5.12. Жизненный цикл сети для различных версий DCA в сравнении с LEACH в случае, когда шлюз расположен вне сети

И в случае, когда шлюз расположен вне сети, алгоритм DSA обеспечивает более длительный жизненный цикл сети, чем алгоритм LEACH-M.

Анализ зависимостей на рис. 5.11 и рис. 5.12 показывает также, что простой предиктор SPP обеспечивает наибольший по длительности жизненный цикл сенсорной сети во всех рассмотренных случаях.

5.7.6. Новые алгоритмы для мобильных сенсорных сетей.

Уже после опубликования материалов по алгоритму распределенной кластеризации появился целый ряд новых алгоритмов для мобильных сенсорных сетей, как ориентированных на конкретные приложения, так и общего характера. Ниже мы рассмотрим наиболее интересные из них, на наш взгляд.

Алгоритм групповой мобильности *GMAC* (*Group Mobility Adaptive Clustering Scheme for Mobile Sensor Networks*) [32] предполагает, что все сенсоры подразделяются на группы, такие, что члены одной группы перемещаются в одном направлении и со скоростью, одинаковой у всех членов группы.

При этом состав группы периодически подвергается ротации как с точки зрения выбора головного узла, так и с точки зрения членства какого-либо из сенсоров в той или иной группе. Определяются две группы: историческая (текущая) и прогнозируемая.

Прогнозируемая группа вычисляется на основе информации о скорости и направлении движения как собственно сенсорного узла, так и близлежащих узлов. Создается прогнозируемый перечень всех близлежащих узлов для каждого сенсорного узла.

Алгоритм, основанный на построении дерева (*Tree-Based Routing Protocol for Wireless Sensor Networks*) [34] из проекта *LAURA* (*LocAlization and Ubiquitous monitoRing of pAtients for health care support*), интересен прежде всего тем, что он разработан для смешанной сети со стационарными и мобильными сенсорными узлами.

При этом стационарные сенсорные узлы образуют некое дерево, в области покрытия которого перемещаются мобильные сенсорные узлы.

Алгоритм позволяет управлять мобильностью перемещающихся узлов. Алгоритм используется в проекте LAURA для отслеживания перемещения пациентов в условиях их нахождения в клинике.

В [119] предлагается алгоритм с предсказанием, основанный на явлении пространственной корреляции между узлами сенсорной сети.

Алгоритм может быть использован как для стационарных, так и для мобильных сенсорных сетей. Естественно, наилучшие результаты при использовании этого алгоритма достигаются для сенсорных сетей с большой плотностью, где больше и пространственная корреляция. Для предсказания используется нормализованный метод наименьших квадратов.

Глава 6
Сети автомобильного транспорта

Автомобиль изменил нашу одежду, манеры, обычаи, способы летнего отдыха, облик городов, потребительское поведение, массовые вкусы и сексуальные позиции.
Джон Китс
.

6.1. Общие сведения о VANET

Одним из наиболее перспективных направлений в развитии систем беспроводного доступа являются *сети транспортных средств VANET* (*Vehicular Ad Hoc Network*) [85]. Сети VANET принадлежат к классу мобильных Ad Hoc сетей MANET (Mobile Ad Hoc Network) [16], хотя им присущ и ряд особенностей, как с точки зрения применения, так и с точки зрения используемых 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. Кроме того, предусматривается широкое использование сенсоров для сбора различной информации в сетях автомобильного транспорта [61].

Создание сетей VANET имеет и вполне ясную коммерческую составляющую. Действительно, на горизонте планирова-

ния до 2015 года в Российской Федерации прогнозируемое число автотранспортных средств составит примерно 60 миллионов единиц. Хорошо известно, что в настоящее время число основных телефонных аппаратов в Российской Федерации немного превышает 40 миллионов. Как видим, эти значения сопоставимы, и создание автомобильных сетей и Оператора (Операторов) этих сетей лишь дело времени.

Сеть VANET является одной из базовых составляющих *Интеллектуальной транспортной системы* (*ИТС*), в состав которой наряду с VANET входят также [45]:

- спутниковые системы позиционирования (ГЛОНАСС/GPS/GALILEO),
- сотовые сети связи разных стандартов,
- придорожная инфраструктура,
- системы взаимодействия и оплаты на основе *протокола DSRC* (*Dedicated Short Range Communications)*,
- системы экстренного вызова в случае аварийных ситуаций e-call и ЭРА-ГЛОНАСС.

Интеллектуальная транспортная система является симбиозом сетей связи и информационных возможностей транспортных средств и систем управления автомобильным движением. Не случайно предлагаемый в настоящее время в качестве протокола канального уровня для ИТС *протокол GeoNetworking* (*Geographic Addressing and Routing*) рассматривается только в совокупности с протоколом IPv6 [46,47,48].

Стандартизация ИТС, включая VANET, теперь согласованно проводится практически всеми ведущими стандартизующими организациями. ITU-T разработал рекомендацию Y.2281 «Структура услуг и приложений с использованием ресурсов NGN для сетевых транспортных средств» [102]; ETSI предлагает стандарты серии 102 636 для архитектуры и протоколов ИТС и серии 102 637 для приложений и услуг; Европейский комитет стандартизации CEN разработал стандарты для протокола DSRC; ISO и IETF являются участниками проекта GeoNET, выполняемого в рамках работ по седьмой программе развития Европейского сообщества.

6.2. Функциональная архитектура, станции и подсистемы ИТС

На рис. 6.1 представлена функциональная архитектура Интеллектуальной транспортной системы с локальной сетью станций ИТС как ядром системы [45]. Локальная сеть ИТС, с целью обеспечить предоставление пользователям полного перечня услуг ИТС, взаимодействует с целевой сетью VANET, выделенными сетями (например, сетью автомобилей конкретного производителя), а также с сетями доступа ИТС, сетями доступа сетей связи общего пользования (ССОП), сетями доступа частных телекоммуникационных сетей для связи с ядром ССОП и/или Интернет.

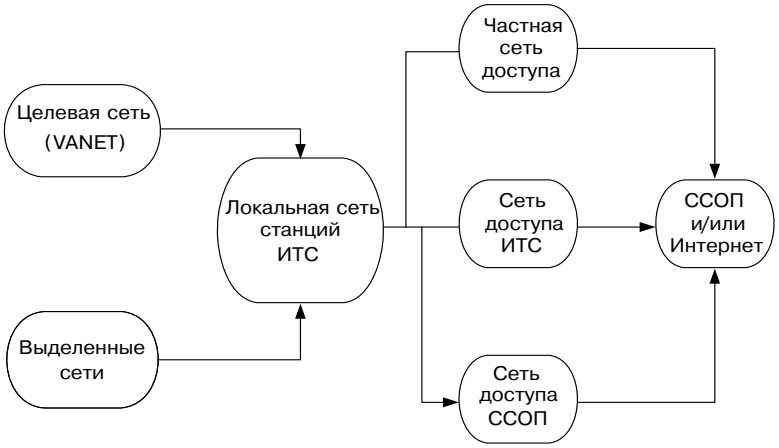

Рис. 6.1. Функциональная архитектура ИТС

Основными функциональными блоками ИТС, используемыми в стандартах ETSI для построения Интеллектуальной транспортной системы, являются станции ИТС. На рис. 6.2 приведена функциональная архитектура станции ИТС. В документе ETSI 302 665 рассматривается четырехуровневая функциональная архитектура станции ИТС, которая включает в себя следующие уровни:

- уровень доступа,
- сетевой и транспортный уровень,
- уровень возможностей,
- уровень приложений.

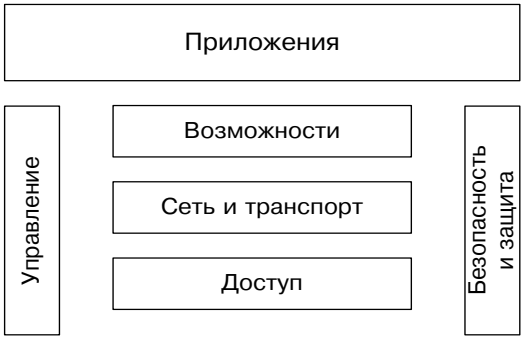

Рис. 6.2. Функциональная архитектура станции ИТС

Уровень доступа включает в себя физический и канальный уровни модели взаимодействия открытых систем OSI (Open System Interconnection), сетевой и транспортный уровни имеют взаимно однозначное соответствие с уровнями 3 и 4 модели OSI, а уровни возможностей и приложений перекрывают остальные уровни модели OSI вплоть до 7 уровня. В дополнение к упомянутым уровням в функциональной архитектуре на рис.6.2 показаны общие для всех уровней функциональные блоки безопасности и администрирования.

Уровень доступа в станциях ИТС включает в себя внутренние и внешние интерфейсы. К внешним интерфейсам относятся, например, интерфейсы с сетями 2G/3G/4G, с навигационной системой GPS и т.д. К внутренним интерфейсам относятся, например, интерфейсы взаимодействия с сетью автомобиля, которая формируется производителем, человеко-машинный интерфейс с водителем и т.д.

Сетевой и транспортный уровни включают в себя как протоколы стека TCP/IP, так и новые протоколы ИТС. В части сетевых протоколов рекомендуется использовать IPv6 с расширенными функциями мобильности и протокол GeoNetworking. Протокол GeoNetworking служит для определения географических координат автомобиля в зоне обслуживания конкретной Интеллектуальной транспортной системы. При появлении автомобиля в конкретной зоне ИТС ему присваивается псевдоадрес, который сохраняется на все время пребывания автомобиля в указанной зоне. Взаимодействие с протоколом IPv6 позволяет при использовании протокола GeoNetworking передать в центральную подсистему ИТС и/или в сеть связи общего пользования необходимую информацию как о месте

расположения автомобиля, так и другую информацию о текущем состоянии автомобиля, запрошенных услугах и т.д. Следует отметить, что не предусматривается непосредственного взаимодействия протоколов GeoNetworking и IPv4. Обеспечение совместимости с сетями IPv4 возложено на сети IPv6.

В ИТС на сетевом уровне предусматривается также использование протокола стандарта IEEE 802.11p для организации сетей VANET [69]. Отметим также, что разработка стандартов ETSI для ИТС проводится в полном соответствии с работами ISO, где подобный проект носит название *CALM* (*Communications Architecture for Land Mobile environment*).

На уровне возможностей предусматривается поддержка взаимодействия с сетями связи, информационная поддержка и поддержка приложений. На следующем уровне определяются три группы приложений: дорожная безопасность, эффективность управления дорожным трафиком и иные приложения. *Безопасность* включает в себя наличие firewall и системы предупреждения вторжений. Используется также идентификационный менеджмент, крипто-ключи, процедуры аутентификации и авторизации, управление профилем пользователя. Заметим, что в качестве пользователя в настоящее время, как правило, рассматривается пара водитель-автомобиль. В архитектуре ИТС присутствует также информационная база, с использованием которой осуществляется управление собственно станцией, приложениями, а также – при необходимости – межуровневое взаимодействие.

ИТС содержит четыре подсистемы:

- персональную,
- центральную,
- собственно автомобильную, функционирующую и в движении, и на парковке,
- придорожную.

Персональная подсистема включает в себя устройства водителя и пассажиров, такие как мобильный телефон, компьютер и т.д. В дальнейшем в состав персональной подсистемы войдет и персональная станция ИТС.

Автомобильная подсистема ИТС изображена на рис. 6.3. Она включает в себя станцию ИТС в составе шлюза ИТС, хоста ИТС и маршрутизатора ИТС. Шлюз ИТС обеспечивает взаимодействие с внутренней сетью автомобиля, формируемой

производителем. На рис. 6.3 показаны также устройства *ECU* (*Electronic Control Unit*), обеспечивающие сбор информации с разных узлов (модулей) автомобиля. Взаимодействие с внешними сетями (придорожной, ССОП и другими) осуществляется с помощью маршрутизатора ИТС.

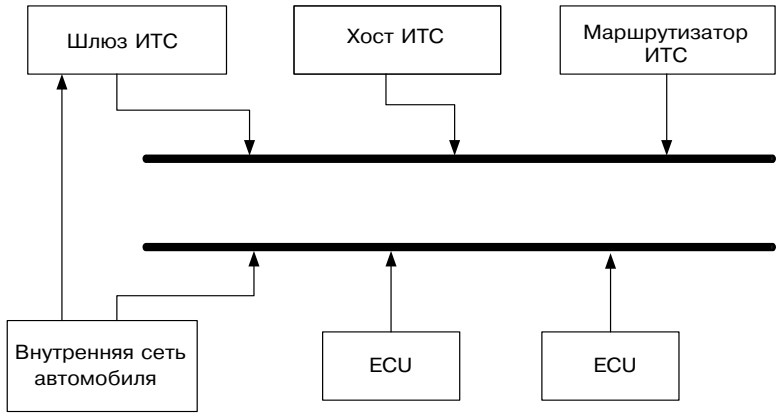

Рис. 6.3. Архитектура ИТС автомобиля

Центральная подсистема включает в себя центральную станцию ИТС и стандартные средства центра для обеспечения безопасности на дорогах и управления трафиком.

Архитектура придорожной подсистемы, показанная на рис. 6.4 ИТС придорожной сети, включает в себя шлюз ИТС, хост ИТС, маршрутизатор ИТС и пограничный маршрутизатор ИТС. Шлюз ИТС обеспечивает взаимодействие ИТС с элементами выделенной придорожной сети, такими как индуктивные шлейфы, табло с изменяющейся информацией (VMS – Variable Message Signs). Пограничный маршрутизатор отделяет домен придорожной подсистемы ИТС от иных доменов сетей, участвующих в формировании Интеллектуальной транспортной системы. Маршрутизатор ИТС совместно с пограничным маршрутизатором обеспечивают взаимодействие станции ИТС с другими сетями (ССОП, 2G/3G/4G и т.д.).

Одной из наиболее сложных структур в Интеллектуальной транспортной системе являются целевые сети VANET (Vehicular Ad Hoc Network), возможные виды взаимодействия которых рассмотрим в следующем разделе.

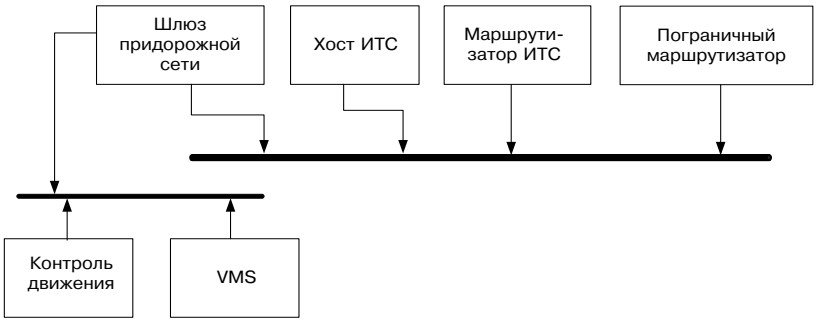

Рис. 6.4. Архитектура придорожной подсистемы ИТС

6.3. Виды взаимодействия в сетях VANET

В соответствии с рекомендацией ITU-T Y.2281 [102] 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.

Европейский институт стандартов в области телекоммуникаций в стандарте ETSI TS 102 636-2 рассматривает сценарии взаимодействия для трех случаев V2V, V2R и R2V. Сценарий V2R практически не отличается от сценария V2I от ITU-T, а сценарий R2V означает взаимодействие автомобиля с придорожной сетью по инициативе придорожной сети.

Для всех упомянутых сценариев в стандарте ETSI 102 636-2 рассматриваются четыре возможных вида связи:

- точка – точка,
- точка – много точек,
- геонаправленный,
- геошироковещательный.

Точка – точка означает связь одной станции ИТС только с одной другой, точка – много точек – одной станции ИТС со многими. Сценарии *геонаправленный* (*GeoAnycast*) и *геошироковещательный* (*GeoBroadcast*) основаны на использовании протокола GeoNetworking. Геонаправленный сценарий подразумевает передачу информации от одной ИТС-станции к произвольной ИТС-станции в пределах географической зоны обслуживания конкретной Интеллектуальной транспортной системы.

Геошироковещательный сценарий предполагает передачу информации от одной ИТС ко всем станциям ИТС в пределах географической зоны обслуживания конкретной Интеллектуальной транспортной системы.

Пример геонаправленного сценария показан на рис. 6.5, а геошироковещательного на рис. 6.6. Передающие и принимающие станции изображены с горизонтальной и наклонной штриховкой, транзитные – вертикальной штриховкой, иные участники дорожного движения – серым цветом без штриховки.

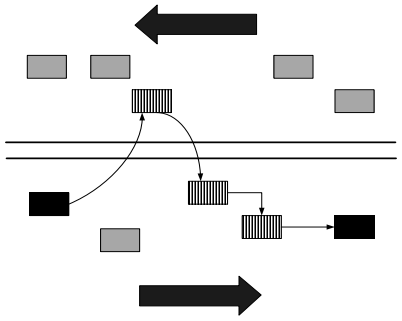

Рис. 6.5. Геонаправленный сценарий

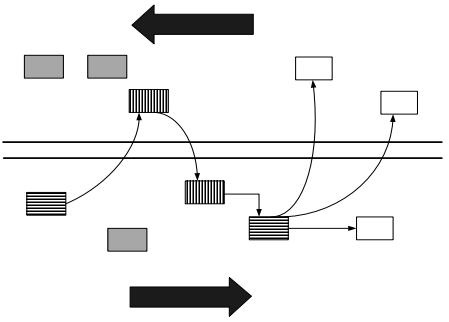

Рис. 6.6. Геошироковещательный сценарий

6.4. Приложения сетей VANET

В соответствии с рекомендацией Y.2281 приложения для сетей VANET подразделяются на 5 групп:

Группа 1. Приложения, ориентированные на техобслуживание автомобиля

- удаленная диагностика,
- перезагрузка данных и программного обеспечения автомобиля.

Группа 2. Приложения, ориентированные на дорожную безопасность

- помощь при авариях,
- поддержка водителя в сложных дорожных ситуациях.

Группа 3. Приложения, ориентированные на пассажиров

- доступ в Интернет,
- аудиовизуальные услуги, в том числе IPTV.

Группа 4. Приложения, ориентированные на оптимизацию дорожного трафика

- помощь в навигации, например, рекомендации по объезду временных препятствий,
- управление скоростью.

Группа 5. Приложения, ориентированные на автомобиль

- логистика,
- парковка.

В Европейском институте стандартов в области телекоммуникаций приводится расширенная по сравнению с ITU-T классификация приложений для сетей VANET. В стандарте ETSI 102 637-1 [49] такая классификация рассматривается как базовый набор приложений VANET. Этот базовый набор приложений VANET на основе стандарта ETSI 102-637-1 приведен в табл. 6.1.

Таблица 6.1. Базовый набор приложений VANET

Класс приложений	Название приложения	Номер приложения	Пользовательский случай
1	2	3	4
Активная поддержка безопасности дорожного движения	Помощь в вождении автомобиля – совместные усилия	UC001	Предупреждение об аварийном состоянии автомобиля
		UC002	Индикация сброса скорости автомобиля
		UC003	Предупреждение о столкновении на перекрестке
		UC004	Предупреждение о приближении мотоцикла

Продолжение табл. 6.1

1	2	3	4
	Помощь в вождении автомобиля – предупреждение о проблемах на дорог	UC005	Включение стоп-сигналов чрезвычайной ситуации
		UC006	Предупреждение о неправильном направлении движения
		UC007	Стоящий автомобиль – авария
		UC008	Стоящий автомобиль – проблемы
		UC009	Предупреждение об условиях трафика на дороге
		UC010	Предупреждение о нарушении требований дорожных знаков
		UC009	Предупреждение об условиях трафика на дороге
		UC010	Предупреждение о нарушении требований дорожных знаков
		UC011	Предупреждение о дорожных работах
		UC012	Предупреждение о риске столкновения
		UC013	Децентрализовано размещенные данные о машине – опасное местоположение
		UC014	Децентрализовано размещенные данные о машине – осадки
		UC015	Децентрализовано размещенные данные о машине – липкая дорога
		UC016	Децентрализовано размещенные данные о машине – плохая видимость
		UC017	Децентрализовано размещенные данные о машине – сильный ветер
Совместное управление трафиком	Управление скоростью	UC018	Регулярное или контекстное предупреждение об ограничении скорости
		UC019	Информирование об оптимальной скорости в зависимости от трафика
	Совместная навигация	UC020	Информация о трафике и рекомендуемые маршруты
		UC021	Расширенный список возможных маршрутов и навигация

Окончание табл. 6.1

1	2	3	4
		UC022	Предупреждение об ограничении доступа и информация об объезде
		UC023	Анимации на экране в автомобиле
Услуги в зоне обслуживания	Услуги местонахождения	UC024	Напоминание о пунктах интереса
		UC025	Автоматическое управление доступом на парковку
		UC026	Электронная коммерция в пределах местной ИТС
		UC027	Загрузка медиа ресурсов
Услуги Глобальной сети Интернет	Коммунальные услуги	UC028	Страховое и финансовое обслуживание
		UC029	Управление автомобилями одного автопарка
		UC030	Управление погрузкой в зоне ИТС
	Управление жизненным циклом ИТС станции	UC031	Резервирование и перезагрузка программного обеспечения и данных автомобиля
		UC032	Калибровка данных автомобиля и придорожных устройств

Действительно, набор приложений в табл. 6.1 достаточно широк и во многих случаях специфичен. Поэтому помимо создания крупного национального Оператора потребуется и создание различных специализированных провайдеров, что необходимо будет увязать с административным устройством Российской Федерации.

Потребуется также и обеспечение совместимости новых геопротоколов с телекоммуникационными протоколами, хотя без широкого внедрения протокола IPv6 не обойтись. Вместе с тем, создание Интеллектуальной транспортной системы является очевидной необходимостью.

При этом важнейшим стратегическим положением представляется построение ИТС в строгом соответствии с международными стандартами и, в первую очередь, со стандартами ETSI, поскольку Российская Федерация является членом Европейской комиссии почтовой и электрической связи (CEPT).

Глава 7
Молекулярные наносети

Будущее уже здесь:
Оно просто распределено неравномерно.
Уильям Гибсон

7.1. Наносети как направление развития сетей связи

Как уже отмечалось выше, в соответствии с прогнозами число беспроводных устройств к 2017 – 2020 годам составит 7 триллионов (на 7 миллиардов человек!) [123]. 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 [27], 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, скажем, для биороботов [91], возникает задача создания сетей, в которых передача инфор-

мации может осуществляться иными способами, например, с помощью перемещения микрочастиц вещества. Подобные сети получили название наносетей [28, 29]. Определим наносеть в терминах телекоммуникаций следующим образом.

Наносеть представляет собой самоорганизующийся сеть, в которой в качестве узлов сети используются наномашины, а информация и сигнализация могут быть переданы, в том числе, и путем перемещения микрочастиц вещества.

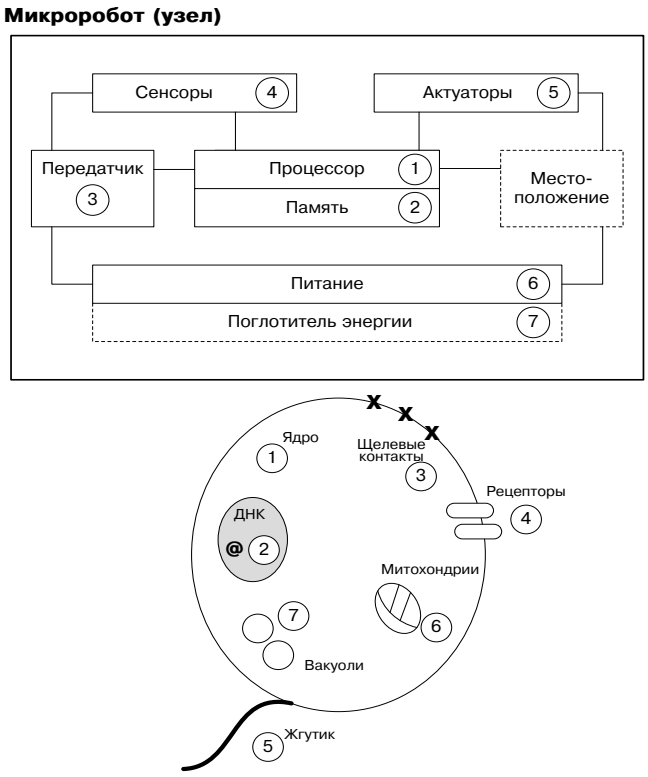

Рис. 7.1. Структуры микроробота и клетки

Наномашина – устройство, состоящее из компонентов наноуровня, способное выполнять на этом уровне специфические задачи, такие как передача данных, вычисление, хранение данных, измерения (сенсоры) и/или воздействия (актуаторы). Определение приведено в соответствии с фундаментальной работой [28]. Примером наномашины может служить клетка, которая в своей структуре повторяет микроробот (или наоборот), что приведено на рис. 7.1 и соответствует рисунку из [28]. В классификации наносетей в настоящее время

выделяются наносети, в которых информация передается с помощью электромагнитных волн, и наносети, в которых информация передается путем перемещения микрочастиц вещества (молекулярные наносети).

7.2. Классификация молекулярных наносетей

Как уже отмечалось выше, передача информации в таких наносетях может осуществляться путем перемещения микрочастиц вещества. Молекулярные наносети в настоящее время классифицируются следующим образом [29]:

- 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 передачи 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 [28]. Использование феромонов потенциально позволяет передавать информацию на сотни метров и километры.

В соответствии с определением [81] 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 [7]. 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), аррестанты (феромоны останавливающие), стимулянты (феромоны активности), детерренты (феромоны тормозящие реакцию). Такая классификация феромонов позволяет принципиально реализовать на их основе функции создания кластеров по аналогии с беспроводными сенсорными сетями. На рис. 7.2 в качестве примера приведены экранные изображения формирования кластеров в беспроводных сенсорных сетях, детально рассмотренные в главе, посвященной алгоритмам выбора головного узла в сенсорных сетях.

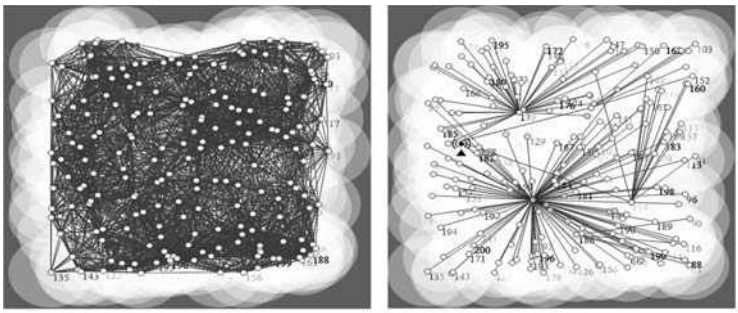

Рис. 7.2. Пример формирования кластера в беспроводных сенсорных сетях

Аттрактанты могут быть использованы для формирования кластера вокруг определенного головного узла, репелленты при ротации головного узла кластера, аррестанты 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 передачи информации с помощью перемещения мо-

лекул вещества такие химические соединения будем называть псевдоферомонами. Далее классифицируем возможные виды связи в наносетях с использованием феромонов для передачи информации. Классификация приведена в табл. 7.1.

Таблица 7.1. 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 создания искусственного приемника. Задачи синтеза феромонов во многом решены [14].

К настоящему времени синтезированы уже сотни феромонов. 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 – аттрактант самок тутового шелкопряда Bombix mori. 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.

Несмотря на кажущуюся простоту феромонов, 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 низкую температуру кипения и поэтому обладают высокой летучестью. 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 приемник под них, либо разрабатывать некий универсальный приемник, настраиваемый впоследствии на определение тех или иных феромонов или псевдоферомонов. Обе задачи нетривиальны, но их решение позволит дополнить существующие сети связи дополнительными ресурсами.

7.3. Приложения наносетей

В соответствии с классификацией видов связи 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 возможности стабильного энергоснабжения.

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.

И вместо заключения ко всей книге хотелось бы привести слова Уинстона Черчилля, представляющиеся авторам весьма уместными как для завершения этой главы, так и для всех затрагиваемых в книге аспектов пост-NGN в целом: «***Успех – не окончателен, неудачи – не фатальны: значение имеет лишь мужество продолжать***».

Литература

1. Гольдштейн А.Б., Гольдштейн Б.С. SOFTSWITCH. – СПб.: БХВ-Петербург, 2006.
2. Гольдштейн Б.С. Сигнализация в сетях связи. – Том 1, 4-е изд. – СПб.: БХВ-Петербург, 2005.
3. Гольдштейн Б.С. Протоколы сети доступа. — Том 2, 3-е изд. — СПб.: БХВ-Петербург, 2005.
4. Гольдштейн Б.С., Елагин В.С., Сенченко Ю.Л. Протоколы AAA: RADIUS и Diameter. Серия «Телекоммуникационные протоколы». Книга 9. — СПб.: БХВ-Петербург, 2011.
5. Гольдштейн Б.С., Зарубин А.В., Саморезов В.В. Протокол SIP. Справочник. Серия «Телекоммуникационные протоколы». — СПб.: БХВ-Петербург, 2005.
6. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: учебник для вузов. — СПб.: БХВ-Петербург, 2011.
7. Иванов В.Д. Феромоны насекомых. // Соросовский образовательный журнал. — 1998. — № 6.
8. Кох Р., Яновский Г.Г. Эволюция и конвергенция в электросвязи. — М.: Радио и связь, 2001.
9. Джеймс Ф. Куроуз, Кит В. Росс. Компьютерные сети. — 2-е изд. — СПб.: Питер, 2004.
10. Кучерявый А.Е., Кучерявый Е.А. От e-России к u-России: тенденции развития электросвязи. // Электросвязь. — 2005. — № 5.
11. Кучерявый А.Е., Цуприков А.Л. Сети связи следующего поколения. // ФГУП ЦНИИС. — 2006.
12. Кучерявый А.Е., Парамонов А.И., Кучерявый Е.А. Сети связи общего пользования. Тенденции развития и методы расчета. // ФГУП ЦНИИС. — 2008.
13. Кучерявый А.Е., Салим А. «Выбор головного узла кластера в однородной беспроводной сенсорной сети». — Электросвязь. — 2009. — № 8.
14. Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А. Самоорганизующиеся сети. — СПб.: Изд-во «Любавич», 2011.
15. Кучерявый Е. А. Управление трафиком и качество обслуживания в сети Интернет. — СПб.: Наука и техника, 2004.
16. Молчанов Д.А. Самоорганизующиеся сети и проблемы их построения. // Электросвязь. — 2006. — № 6.
17. Мочалов В.И. Разработка и исследование алгоритмов построения отказоустойчивых сенсорных сетей. Автореферат диссертации на соискание ученой степени кандидата технических наук. — М.: МТУСИ, 2011.
18. Яновский Г. Г. IP Multimedia subsystem: принципы, стандарты и архитектура. // Вестник связи. — 2006. — № 3.
19. Тихвинский В.О., Терентьев С.В. Сети мобильной связи LTE технологии и архитектура. — М.: Изд-во «Эко-Трендз», 2010.
20. 3GPP TS36.423 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 application protocol (X2AP), ver. Release 9, March 2010. [http://www.quintillion.co.jp/3GPP/Specs/36423-920.pdf].
21. Akkaya K. and Younis M. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, vol. 3, no. 3, 2005.
22. Akyildiz I.F. Key Wireless Networking Technologies in the Next Decade. NEW2AN 2006, St. Petersburg, Russia, June 2006. Keynote Speech.
23. Akyildiz F., Pompili D., Melodia T. Underwater acoustic sensor networks: research challenges. Ad Hoc Networks Journal, Elsevier, Volume 3, Issue 3, May 2005.
24. Akyildiz I.F., Vuran M.C., Akan O.B., Su W. Wireless Sensor Networks: A Survey revisited. Computer Networks Journal, 2005.
25. Akyildiz I.F. Key Wireless Networks Technologies in the Next Decade. WWIC 2005 Keynote Speech, Xanthi, Greece, May 2005.

26. Akyildiz I.F., Wang X., Wang X. Wireless mesh networks: a survey. Computer Networks and ISDN Systems, v.47, №4, March 2005.
27. Akyldiz I.F. Spectrum management in Cognitive Radio Networks. IEEE WiMob 2008 Conference. Proceedings. Avignon, France, 12-14 October, 2008.
28. Akyildiz I.F. at all. Nanonetworks: A new communication paradigm. Computer Networks, Elsevier, 2008.
29. Akyildiz I.F., Jornet J.M. The Internet of Nano-Things. IEEE Wireless Communications. December 2010, V.17, № 6.
30. Al-Karaki J.N. and Kamal A.E. Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications Magazine, vol. 11, no. 6, 2004.
31. Arboleda L.M., Nasser N. Comparison of Clustering Algorithms and Protocols for Wireless Sensor Networks. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Ottawa, May 2006.
32. Benmansour T., Moussaoui S. GMAC: Group Mobility Adaptive Clustering Scheme for Mobile Wireless Sensor Networks. International Symposium on Programming and Systems (ISPS). Proceedings, Algiers, Algeria, 25-27 April, 2011.
33. Bose P., Morin P., Stojmenovic I, Urrutia J. Routing with guaranteed delivery in ad hoc wireless networks. Wireless Networks, vol. 7, no. 6, 2001.
34. Borsani L, Guglielmi S., Redondi A., Cesana M. Tree-Based Routing Protocol for Wireless Sensor Networks. 8th International Conference on Wireless On-Demand Network Systems and Services, WONS'2011, Bardoneecchia, Italy, January 2011.
35. Chatterjee M. et al. WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks. Journal of Cluster Computing, V. 5/2, April, 2002.
36. Gorlatova M. and all. Energy Harvesting Active NetworkedTags (EnHANTs) for Ubiquitous Object Networking. IEEE Wireless Communications. December 2010, v.17, №6.
37. Chen B., Jamieson K., Balakrishnan H., Morris R. 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.
38. Chen H., Wu C.S., Chu Y. S., Cheng C.C., and Tsai L.K. 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.
39. Chong C.Y., Kumar S.P. Sensor Networks: Evolution, Opportunities and Challenges. Proceedings of the IEEE, vol. 91, issue 8, August 2003.
40. Chong C.Y., Mori S., Chang K.C. Distributed tracking in distributed sensor networks. American Control Conference, Seattle, WA, 1996.
41. Culler D.E., Hui J. 6loWPAN Tutorial. IP on IEEE 802.15.4 Low-Power Wireless Networks. Arch-Rock, 2007
42. Dahlman Erik, Parkvall Stefan, Johan Skeld. 4G LTE/LTE-Advanced for Mobile Broadband, Elsevier Academic Press, 2011.
43. T. von Deak. The role of remote sensing in disaster management. ITU News, №10, December, 2007.
44. ETSI TS 102 689. V.1.1.1. Machine – to - Machine Communications (M2M); M2M Service Requirements. August, 2010.
45. ETSI EN 302 665. Intelligent Transport Systems (ITS); Communications Architecture, v.1.1.1, September, 2010.
46. ETSI TS 102 636-1. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements, v.1.1.1, March, 2010.
47. ETSI TS 102 636-1. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios, v.1.1.1, March, 2010.
48. ETSI TS 102 636-1. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture, v.1.1.1, March, 2010.
49. ETSI TS 102 637-1. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications.; Part 1: Functional Requirements, v.1.1.1, September, 2010.

50. ETSI TS136.423 LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 Application Protocol, ver. 8.3.0 Release 8, October 2008.
51. FET: Future and Emerging Technology in Europe. Bio-ITC Convergence. January, 2008. European Commission Information Society and Media/DG-INFSO.
52. Garg V. Wireless Communications and Networking. Morgan Kaufmann, 2006.
53. Gupta G., M. Younis. Load-balanced clustering of wireless sensor networks. IEEE ICC 2003, vol.3, May 2003.
54. Hamalainen Seppo, Sanneck Henning, Sartori Cinzia. LTE Self-Organising Networks (SON): Network Management Automation for Operational Efficiency / – Чичестер, Великобритания: John Wiley & Sons, 2011.
55. Heinzelman W., Kulik J., Balakrishnan H. 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.
56. Heinzelman W., Chandrakasan A., Balakrishnan H. An application specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications 1 (4), 2002.
57. Heinzelman W., Chandrakasan A., Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. Proceedings 33rd Hawaii International Conference on System Sciences (HICSS), Wailea Maui, Hawaii, USA, Jan. 2000.
58. Hou Y.T., Shi Y., Pan J. «Lifetime-optimal data routing in wireless sensor networks without flow splitting,» in Workshop on Broadband Advanced Sensor Networks, San Jose, CA, 2004.
59. Huang H., Richa A.W., Segal M. Dynamic coverage in ad-hoc sensor networks. Mobile Networks and Applications. Springer Science + Business Media, 10, 2005.
60. Huang C., Tseng Y. The Coverage Problem in a Wireless Sensor Network. Mobile Networks and Applications, vol. 10, no. 4, Aug. 2005.
61. Hsieh T.T. Using sensor networks for highway and traffic applications. IEEE Potentials Volume 23, Issue 2, April-May 2004.
62. IEEE 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 1999.
63. IEEE 802.11a. Higher-Speed Physical Layer in the 5 GHz band. 1999.
64. IEEE 802.11в. Higher-Speed Physical Layer (PHY) Extension in the 2.4 GHz band.1999.
65. IEEE 802.11e. Medium Access Control (MAC) Quality of Service Enhancements. 2005.
66. IEEE 802.11g. Further Higher-Speed Physical Layer Extension in the 2.4 GHz band. 2003.
67. IEEE 802.11n. Enhancements for Higher Throughput. September, 2009.
68. IEEE 802.11s (draft). Extended Service Set Mesh Networking. 2009.
69. IEEE 802.11p. Wireless Access for the Vehicular Environment. July, 2010.
70. IEEE 802.16-2009. Air interface for Fixed and Mobile Broadband Wireless Access Systems. 2009.
71. IEEE 802.16m. Amendement to IEEE 802.16-2009. Advanced Air Interface with Data Rates of 100Mbit/s mobile and 1Gbit/s fixed. 2011.
72. IEEE 802.1p. Traffic Class Expediting and Dynamic Multicast Filtering. 2006.
73. IEEE 802.15.1-2005 Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs).
74. 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).
75. 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.
76. Iera A., Floerkemeier C., Mitsugi J., Morabito G. The Internet of Things. IEEE Wireless Communications. December 2010, v.17,№6.
77. IP multimedia subsystem (IMS). Handbook /Edited by Syed A. Ahson, Mohammad Ilyas/ CRC Press, 2009.

78. Intanagonwiwat C., Govindan R., Estrin D. 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.
79. Farooq Khan. LTE for 4G Mobile Broadband//Cambridge University Press. 2009.
80. Kansal A. et al. Sensing uncertainty reduction using low complexity actuation. ACM Information Processing in Sensor Networks (ISPN), April 2004.
81. Karlson P., M.Luscher. Pheromones: A new term for a class of biologically active substances. Nature, 183. 1959.
82. Kim B.-T. 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.
83. Kim D. and Chung Y. 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.
84. 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.
85. Koucheryavy Y., Jakubiak J. Research Challenges in Vehicular Ad hoc Networks. Proceedings, IEEE CCNC 2008, January 10-12, 2008. Las Vegas, USA.
86. Kwak K.S., Ullah S., Ullah N. 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.
87. Kwak K.S., Ameen M.A. Current Status of the Proposed IEEE 802.15.6 WBAN MAC Standardization.
88. Lindsey S. and Raghavendra C.S. PEGASIS: Power-efficient gathering in sensor information systems. Proceedings IEEE Aerospace Conference, vol. 3, Big Sky, Montana, USA, 2002.
89. Lindsey S., Raghavendra C., Sivalingam K. Data gathering in sensor networks using the energy delay metric. Proceedings, 15th International Parallel and Distributed Processing Symposium (IPDPS), San Francisco, USA, Apr. 2001.
90. Li Y., Wu V., Zhang J-Y., Peng J., Liao H-L., Zhang Y-F. A P2P based distributed services network for next generation mobile Internet communications. 18th International Conference on WWW. Proceedings, Madrid, Spain, April 20-24, 2009.
91. Marrocco G. Pervasive Electromagnetics: Sensing Paradigms by Passive RFID Technology. IEEE Wireless Communications. December 2010, V.17, № 6.
92. Myers C., Oppenheim A., Davis R., Dove W. Knowledgebased speech analysis and enhancement. The International Conference on Acoustics, Speech and Signal Processing, San Diego, CA, 1984.
93. Nam D.-H., Min H.-K. 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.
94. Nkwogu D.N., Allen A.R. Adaptive Learning and Reconfiguration in Wireless Sensor Actuator Networks for Control Applications. The 12th Annual Post Graduate symposium on the Convergence of Telecommunications, Networking and Broadcasting. Proceedings. Liverpool, Great Britain, 27-28 June, 2011.
95. Olsson Magnus, Sultana Shabnam, Rommer Stefan, Lars Frid, Catherine Mulligan. SAE and the Evolved Packet Core: Driving The Mobile Broadband Revolution/ Academic Press, 2009.
96. Poikselka M., Mayer G. The IMS: IP Multimedia Concepts and Services. 3rd Edition. J.Wiley&Sons, 2009.
97. Recommendation Y. 1541. Network Performance Objectives for IP-based Services. 2006.
98. Recommendation Y. 2021. IMS for Next Generation Network. ITU, 2006.
99. Recommendation Y. 2211. IMS-based Real-Time Conversational Multimedia Services over NGN. 2007.
100. Recommendation Y. 2221. Requirements for Support of Ubiquitous Sensor Network (USN) Applications and Services in the NGN Environment. 2010.

101. Recommendation (draft) Y.NGN-IoT-arch. Architecture of NGN for support of the Internet of Things. TD GEN697, NGN-GSI, May 9-20, 2011.
102. Recommendation ITU-T Y.2281. Framework of networked vehicle services and applications using NGN. ITU-T, 2011.
103. Recommendation (draft) Y.Terms-IoT (Internet of Things Related terminology). TD GEN749, NGN-GSI, May 9-20, 2011.
104. 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.
105. Recommendation (draft) Y.USN-arch. Functional Architecture for USN. TD GEN723, NGN-GSI, May 9-20, 2011.
106. Recommendation (draft) Y.UbiNet-hn. Framework of object-to-object communication using ubiquitous networking. TD GEN732, NGN-GSI, May 9-20, 2011.
107. Recommendation (draft) Y.WoT. Framework of Web of Things. TD GEN735, NGN-GSI, May 9-20, 2011.
108. RFC4919. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. 2007
109. Reynau L., Meddour D. An Open Architecture that Manages Quality of Service within Ad Hoc Networks. Proceedings, IEEE IWWAN, 2004.
110. Sarkar S.K., Basavaraju T.G., Puttamadappa C. Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications. Auerbach Publications, Boston, MA, USA, 2007.
111. Siva C., Murthy R., Manoj B.S. Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall, 2004.
112. Shelby Z. Embedded Web Services. IEEE Wireless Communications. December 2010, V.17, № 6.
113. Small T., Haas Z.J. The shared wireless infostation model: a new ad-hoc networking paradigm. Proceedings ACM Mobihoc, ACM Press, 2003.
114. Smart Ubiquitous Networks (SUN). TD PLEN193, SG13 ITU-T meeting, January 17-28, 2011.
115. Sohrabi K., Gao V, Ailawadhi V., and Pottie G.J. Protocols for self-organization of a wireless sensor network. IEEE Personal Communication Magazine, vol. 7, no.5.
116. Soro S. and Heinzelman W. B. Cluster head election techniques for coverage preservation in wireless sensor networks. Ad Hoc Networks, Elsevier, Volume 7, 2009.
117. SOSUS. http://www.pmel.noaa.gov/vents/acoustics/sosus.html.
118. Stojmenovic I. Handbook of sensor networks. Algorithms and architectures. John Wiley & Sons; 2005.
119. Tharini C., Ranjan V. An Energy Efficient Spatial Correlation Base Data Gathering Algorithm for Wireless Sensor Networks. International Journal of Distributed and Parallel Systems (IJDPS), v.2, №3, May, 2011.
120. Tiny OS webpages, http://www.tinyos.org.
121. Vision and Challenges for realizing the Internet of Things. European Commission. 2010.
122. Weiser M. Hot Topic: Ubiquitous computing. IEEE Computing. October 1993.
123. Wireless World Research Forum, July, 2009, №4.
124. Yao Y., Gehrke J. The cougar approach to in-network query processing in sensor networks. ACM SIGMOD Record, vol. 31, no. 3, 2002.
125. Younis O., Fahmy S. Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach. Proceedings, IEEE INFOCOM, Hong Kong, China, 2004.
126. YounisO., Krunz M., Ramasubramanian S. Node clustering in wireless sensor networks: Recent developments and deployment challenges. IEEE Network, vol. 20, no. 3, 2006.
127. Mark Wuthnow, Matthew Stafford, Jerry Shih. IMS. A New Model for Blending Applications/ /CRC Press, 2010
128. www.3gpp.org/specs/numbering.htm
129. www.zigbee.com.

Глоссарий

2G	Мобильные сети второго поколения, включая технологии GSM
2,5G	Усовершенствованное второе поколение систем подвижной связи
3G	Мобильные сети 3-го поколения, включая технологию UMTS
3GPP	Third Generation Partnership Project – партнерский проект ETSI по 3G
4G	4-е поколение сетей подвижной связи
6LoWPAN	Low energy IPv6 based Wireless Personal Area Networks protocol – сетевые структуры USN, построенные на базе протокола IPv6
AAA	Authentication, Authorization, Accounting – авторизация, аутентификация и учет
ABC	Always Best Connection – всегда выбирается лучшее соединение
AC	Access Category – категории обслуживания по стандарту IEEE 802.11e
ADSL	Asymmetrical Digital Subscriber Line – асимметричная цифровая АЛ
AMPS	Advanced Mobile Phone Service – улучшенная услуга речевой мобильной связи
AMR-WB+	Adaptive Multi-Rate-Wideband-i-codec – адаптивный многоскоростной широкополосный i-кодек
AN	Access Network – сеть доступа
ANSI	American National Standards Institute – национальный институт стандартов США;
API	Application Programming Interface – интерфейс прикладного программирования;
APN	Access Point Network – сеть точки доступа (реализована в шлюзе GGSN)
AS	Application Server – сервер приложений
AuC	Authentication Center – центр аутентификации
AWACS	Airborne Warning and Control System – посторонние объекты в воздушном пространстве – система предупреждения и контроля
BAN	Body Area Network – нательная сеть
BCCH	Broadcast Control Channel – однонаправленный канал для передачи широковещательной информации управления
BGCF	Breakout Gateway Control Function – функция управления шлюзами подсистемы IMS, обеспечивающая маршрутизацию вызовов и управление шлюзами взаимодействия подсистемы IMS с сетями коммутации каналов (например, GSM, ТфОП)
BNC	BAN Network Controller – контролер BAN
BRI	Basic Rate Interface – интерфейс базового доступа ISDN
BSC	Base Station Controller – контроллер базовой станции
CALM	Communications Architecture for Land Mobile environment
CAMEL	Customized Applications for Mobile network Enhanced Logic – специальные приложения для расширенной логики мобильной сети
CAP	CAMEL Application Part – подсистема приложений CAMEL
CCCH	Common Control Channel – канал, предназначенный для запроса доступа пользовательского терминала к сети LTE и используется при установлении соединения или при реализации иных процедур, требующих выделения индивидуального сигнального канала
CDMA	Code Division Multiple Access – многостанционный доступ с кодовым разделением каналов
CDR	Call Detail Record – учетная запись параметров вызова
CGF	Charging Gateway Function
CPP	Single Point Predictor
CQI	Channel Quality Indicators – индикаторы качества каналов в LTE

CS	Circuit Switching – коммутация каналов
CSCF	Call Session Control Function – функция управления сеансом связи
D2D	Device-to-Device – машина к машине или устройство к устройству
DARPA	Defense Advanced Research Projects Agency
DCA	Distributed Clustering Algorithm – распределенный алгоритм кластеризации
DCCH	Dedicated Control Channel – двунаправленный канал в LTE с конфигурацией точка-точка, используется для передачи индивидуальной сигнальной информации, если между пользовательским терминалом и сетью существует RRC-соединение
DHCP	Dynamic Host Configuration Protocol
DIAMETER	Протокол IP-сети – обеспечивающий аутентификацию, авторизацию и учет. Основан на протоколе RADIUS
DSLAM	Digital Subscriber Line Access Multiplexer – мультиплексор доступа для цифровых абонентских линий;
DTCH	Dedicated Traffic Channel – индивидуальный пользовательский канал с конфигурацией точка-точка, присвоенный пользовательскому терминалу в LTE
EDGE	Enhanced Data Global Evolution – повышение скорости передачи данных при глобальной эволюции. Проект, развивающий стандарт GSM и позволяющий увеличить скорость передачи данных до 384 кбит/с. Интерфейс EDGE надстраивается над существующим радиоинтерфейсом GSM
E-IMS	Enhanced IP Multimedia Subsystem – усовершенствованная мультимедийная IP-подсистема
EIR	Equipment Identity Register – регистр идентификации пользовательского оборудования
eNB	eNodeB, evolved NodeB – усовершенствованная базовая станция сети LTE
ENUM	tElephone NUmber Mapping – преобразование телефонного номера
EPC	Evolved Packet Core – новое поколение ядра пакетной сети
ePDG	Evolved Packet Data Gateway – пакетный шлюз взаимодействия сети SAE с «ненадежными» сетями доступа
EPC	Evolved Packet Core – эволюция ядра сети в LTE/SAE
EPS	Evolved Packet System – усовершенствованная пакетная система, термин объединяет сеть доступа и ядро EPC в LTE/SAE
ETSI	European Telecommunication Standardization Institute – Европейский институт телекоммуникационных стандартов
EVDO	Evolution, Data Only – стандарт 3G
FDD	Frequency Division Duplex – дуплексный режим с частотным разделением приема и передачи
FGN	Future Generation Network – сеть будущего поколения
FMC	Fixed-Mobile Convergence – конвергенция сетей мобильной и фиксированной связи
FTTx	Fiber To The «x» – волокно до точки «x». Собирательное название для ряда решений, как использовать кабель с оптическими волокнами в сети доступа
GERAN	GSM/EDGE Radio Access Network – сеть радиодоступа GSM/EDGE совместимая с UMTS
GGSN	Gateway GPRS Support Node – шлюзовой узел поддержки GPRS, маршрутизируюший пакеты данных, которые в него поступают из внешних пакетных сетей
GMSC	Gateway Mobile Switching Center – шлюзовой мобильный центр управления и коммутации

GPRS	General Packet Radio Service – технология пакетной радиопередачи данных, модернизация стандарта GSM, позволившая организовать услугу передачи данных на базе технологии с коммутацией пакетов
GPS	Global Positioning System – глобальная система позиционирования
GSM	Global System for Mobile communication – глобальная система мобильной связи, цифровой стандарт для сотовых систем мобильной связи, использующих диапазоны частот 900, 1800 и 1900 МГц и функционирующих по принципу TDMA
GTP	GPRS Tunneling Protocol – протокол формирования туннелей в GPRS
gsmSCF	GSM Service Control Function
HANET	Home Ad Hoc Networks – домашние сети Ad Hoc
HBC	Human Body Communication – уровень связи человеческого тела
HFC	Hybrid Fiber Coax – гибридная оптико-коаксиальныя линия
HLR	Home Location Register – сетевая база данных, в которой хранятся справочные данные о постоянно зарегистрированных абонентах (адреса, информация об услугах и др.), в том числе информация о местонахождении, позволяющая MSC обеспечить маршрутизацию вызовов
HSDPA	High-Speed Downlink Packet Access – высокоскоростной нисходящий пакетный доступ от базовой станции к мобильному терминалу
HSPA	High-Speed Packet Access – высокоскоростной пакетный доступ
HSS	Home Subscriber Server – сервер абонентов домашней сети
HSUPA	High Speed Uplink Packet Access – высокоскоростной восходящий пакетный доступ
HTTP	HyperText Transport Protocol – протокол передачи гипертекста
IaaS	Infrastructure as a Service – инфраструктура как услуга или служба
IASA	Inter-Access System Anchor – единый узел привязки базовой сети EPC
IBCF	Interconnect Border Control Function) – эта функция обеспечивает управляемость на границе между сетями разных провайдеров
I-BGF	Interconnect Border Gateway Function – управляет передачей данных на 3-м и 4-м уровнях через границу сетей провайдеров, играет роль межсетевого экрана и NAT в TISPAN, защищает ядро сети провайдера, фильтруя пакеты на основании информации транспортного уровня
ICE	In Case of Emergency – в случае крайней необходимости
I-CSCF	Interrogating Call Session Control Function. Опрашивающий сервер, являющийся граничным элементом подсистемы IMS, с которым устанавливает контакт внешняя сеть
IETF	Internet Engineering Task Force – инженерная рабочая группа Интернета
IM	Instant Messaging
IMEI	International Mobile Equipment Identity – международный уникальный идентификатор оборудования мобильной станции
IM-MGW	IP Multimedia Media Gateway – медиа шлюз, обеспечивающий передачу данных между подсистемой IMS и сетями коммутации
IMS	IP Multimedia Subsystem – мультимедийная IP-подсистема
IMSI	International Mobile Subscriber Identity – международный идентификатор мобильного абонента
IMT-2000	International Mobile Telecommunications-2000 – международная программа ITU создания систем подвижной связи 3G
IN	Intelligent Network – Интеллектуальная сеть
IM-SSF	IP Multimedia Service Switching Function – позволяет использовать в IMS услуги CAMEL4
INAP	Intelligent Network Application Protocol – прикладной протокол ОКС7 для Интеллектуальной сети
IoT	Internet of Things – Интернет вещей

IP	Internet Protocol – протокол (семейство протоколов) Интернет; текущая версия — IPv4, новая — Ipv6
IPCC	International Packet Communication Consortium – Международный консорциум пакетной связи
ISC	IMS Service Control, управление услугами подсистемы IMS;
ISDN	Integrated Services Digital Network – цифровая сеть интегрального обслуживания
ISIM	IP Multimedia Services Identity Module – модуль идентификации абонента мультимедийных услуг IP
ISUP	ISDN User Part – протокол стека ОКС7, поддерживающий сигнализацию телефонной сети, сети передачи данных и ISDN
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector – Международный союз электросвязи – сектор стандартизации в области связи телекоммуникаций
IWF	Inter-Working Function – обеспечивает взаимодействие протокола SIP сети IMS с сигнальным протоколом H.323 или с реализациями SIP в IP-сетях других провайдеров
I-CSCF	Interrogating Call Session Control Function – опрашивающий сервер, являющийся граничным элементом подсистемы IMS, с которым устанавливает контакт внешняя сеть
LBS	Location Base Services – услуги определения местонахождения абонентов
LEACH	Low Energy Adaptive Cluster Hierarchy – адаптивная иерархия кластеров, обеспечивающая малое потребление энергии
LMSI	Local Mobile Station Identity – локальный идентификатор мобильного абонента
LTE	Long Term Evolution – система мобильной связи нового поколения
M2M	Machine-to-Machine – сети схема связи машина-машина
MAC	Medium Access Control – протокол контроля доступа к среде
MANET	Mobile Ad Hoc Network – мобильная сеть Ad Hoc
MBAN	Medicine Body Area Networks – медицинские сети
MBMS	Multimedia Broadcast Multicast Service – широковещательные или многоадресная мультимедийная услуга
MCCH	Multicast Control Channel – однонаправленный канал в LTE с конфигурацией точка-много точек, передает информацию управления для MBMS от сети к терминалам пользователей
MDT	Minimization of Drive Tests, минимизация в сотовых сетях тестирования с испытателями на автодвижущихся средствах
ME	Mobile Equipment – мобильное устройство
MG	Media Gateway – медиашлюз
MGCF	Media Gateway Control Function – функция управления медиашлюзами
MGW	Media Gateway – медиашлюз
MIMO	Multiple Input Multiple Output – многократный ввод и многократный вывод в LTE
MIT	Massachusetts Institute of Technology – Массачусетский технологический институт
MME	Mobility Management Entity – модуль управления мобильностью в сети SAE
MOC	Machine Oriented Communications – межмашинные коммуникации
MRF	Media Resource Function – функции медиасервера в IMS
MRFC	Media Resource Function Controller – функция контроллера ресурсов мультимедиа, управляет доступом к ресурсам
MSC	Mobile Switching Center – центр коммутации мобильной связи

MSIN	Mobile Subscriber Identity Number – идентификационный номер подвижного абонента
MSISDN	Mobile Station International ISDN Number – международный ISDN-номер мобильного терминала
MSRN	Mobile Station Roaming Number – роуминговый номер подвижного абонента
MT	Mobile Terminated – вызываемый абонент
MTCH	Multicast Traffic Channel – однонаправленный канал от eNB к терминалу пользователя
NAI	Network Access Identifier – идентификатор вида username @ operator. com, определенный в RFC 2486
NASS	Network Attachment SubSystem – назначает IP-адреса в релизе 1 TISPAN
NB	Narrowband – узкополосный
NE	Network Element – сетевой элемент
NM	Network Management, эксплуатационное управление сетью;
NGN	Next Generation Network – сеть следующего поколения
NMT	Nordic Mobile Telephony– стандарт мобильной связи
OAM&P	Operations, Administration, Maintenance, Provisioning – основные функции NM;
OFDM	Orthogonal Frequency Division Multiplexing – мультиплексирование с ортогональным разделением частот;
OSA-SCS	Open Service Access – Service Capability Server – интерфейс к серверу приложений OSA, функционирует как сервер приложений со стороны S-CSCF и как интерфейс между сервером приложений OSA и OSA API – с другой стороны
OSI	Open Systems Interconnection – взаимодействие открытых систем
OSS	Operation Support System – система поддержки эксплуатации сети связи
PaaS	Platform as a Service – платформа как услуга (или служба)
PCCH	Paging Control Channel – однонаправленный канал, который переносит информацию для поиска абонента в LTE, этот канал используется, если сеть не знает соты, в которой в данный момент находится абонент
PCEF	Policy and Charging Enforcement Function – функция применения сетевой политики и правил начисления платы
PCRF	Policy and Charging Rules Function – функция политики сети и правил начисления платы
P-CSCF	Proxy Call Session Control Function – прокси-сервер SIP-протокола, являющийся первым сетевым элементом подсистемы IMS, с которым устанавливает контакт абонентский терминал UE
PDF	Policy Decision Function – функция стратегического решения
PDP	Packet Data Protocol – протокольный блок данных
P-GW	Packet Gateway – пакетный шлюз базовой сети EPC
PON	Passive Optic Network – пассивная оптическая сеть
PRI	Primary Rate Interface – интерфейс первичного доступа ISDN
PrUI	Private User Identity – основной идетификатор пользователя в IMS
PSC	Personal Communication Services – услуги персональной связи
PSI	Public Service Identity – идентификатор в IMS, присваивается не пользователям, а услугам, размещенным на серверах приложений
P-TMSI	Packet-Temporary Mobile Subscriber Identity – временный пакетный идентификатор
P-TMSI	Packet-Temporary Mobile Subscriber Identity, временный пакетный идентификатор мобильного абонента;

PuUI	Public User Identity – каждому PrUI в IMS Оператор ставит в соответствие один или несколько PuUI
QoS	Quality of Service – качество обслуживания
RACS	Resource and Admission Control Subsystem – подсистема управления доступом в TISPAN
RAN	Radio Access Network – сеть радиодоступа
RFC	Request for Comments – технические спецификации и стандарты IETF
RFID	Radio Frequency IDentification – радиочастотная идентификация
RG	Residental Gateway – шлюз в домашней сети Ad Hoc
RTP	Real-time Transport Protocol – протокол передачи пакетов данных в реальном времени
RNC	Radio Network Controller, контроллер радиосети;
RTP	Real-time Transport Protocol, протокол транспортировки пакетов в реальном времени;
SaaS	Software as a Service – программное обеспечение как услуга
SAE	System Architecture Evolution – архитектура базовой пакетной сети нового поколения, включающая в себя базовые сети EPC и систему управления
SAE Anchor	System Architecture Evolution Anchor – узел привязки (якорь) сети SAE
SAE GW	SAE Gateway – шлюз, который включает в себя два сетевых элемента: Serving Gateway, который отвечает за управление мобильностью между системами доступа GSM и UMTS, и PDN Gateway, осуществляющий взаимодействие с сетью Интернет и локальными сетями и обеспечивающий мобильность абонента между LTE и не-3GPP сетями
SBC	Session Border Controller – пограничный контроллер
SCP	Service control point – узел управления услугами Интеллектуальной сети
S-CSCF	Serving-Call Session Control Function – центральный обслуживающий сервер подсистемы IMS
SEG	Security Gateway – шлюз защиты в IMS
SGSN	Serving GPRS Support Node – сервисный узел поддержки GPRS
S-GW	Serving GW – обслуживающий шлюз
SGW	Signaling Gateway – шлюз обеспечения сигнального обмена между подсистемой IMS и внешними сетями с коммутацией каналов
SHANET	Shopping Ad Hoc Network
SHDSL	Single-pair High-speed DSL – симметричная высокоскоростная цифровая АЛ на одной витой паре
SIM	Subscriber Identity Module – модуль идентификации абонента
SIP	Session Initiation Protocol – протокол инициирования сессий
SIP URI	Session Initiation Protocol – Uniform Resource Indicator – универсальный идентификатор ресурса протокола инициирования сессий
SLA	Service Level Agreements – соглашения об уровне обслуживания
SLF	Subscriber Location Function – функция местонахождения абонента
SON	Self-organizing network – самоорганизующаяся сеть
SSF	Service Switching Function – функция коммутации для услуг
SSP	Service switching point – узел коммутации услуг Интеллектуальной сети
STP	Signaling transfer point – транзитный пункт сигнализации
SUN	Smart Ubiquitous Networks – разумные всепроникающие сети
TDD	Time Division Duplex – дуплексный режим с временным разделением приема и передачи

THIG	Topology Hiding Internetwork Gateway – скрывающая межсетевой шлюз топология
TMSI	Temporary Mobile Subscriber Identity – временный уникальный идентификатор мобильного абонента
TS	Technical Specifications – две буквы, характеризующие тип документа для технических спецификаций
TXOP	Transmission Opportunity – интервал возможности передачи без конкуренции по стандарту IEEE 802.11e
U	Ubiquitous – всепроникающее
UICC	Universal Integrated Circuit Card – идентификационная карта IMS-терминала, хранит один PrUI и, как минимум, один PuUI
UMTS	Universal Mobile Telecommunications System – универсальная система мобильной связи третьего поколения
USIM	Universal Subscriber Identity Module – модуль идентификации абонента в сети UMTS
USN	Ubiquitous Sensor Networks – всепроникающие сенсорные сети
UTRAN	UMTS Terrestrial Radio Access Network – наземная радиосеть доступа к сети UMTS
UWB	Ultra WideBand – сверхширокополосный
VANET	Vehicular Ad Hoc Networks – сети транспортных средств
VDSL	Very High-speed Digital Subscriber Line – суперскоростная цифровая АЛ
VLR	Visitor Location Register – визитный регистр местонахождения абонента
VoIP	Voice over IP – технология передачи речевого трафика по IP-сетям, IP-телефония;
WaaS	Web as a Service – Вэб как услуга
WBAN	Wireless Body Area Network – нательные беспроводные сети
WCDMA	Wideband Code Division Multiple Access – широкополосный многостанционный доступ с кодовым разделением каналов
WiMAX	Worldwide Interoperability for Microwave Access
WoT	Web of Things – Вэб вещей
xDSL	eXtended Digital Subscriber Line – расширенная абонентская цифровая линия – технология высокоскоростной связи
ЕСЭ РФ	Единая сеть электросвязи Российской Федерации
ИТС	Интеллектуальна транспортная система
ЛОНИИС	Ленинградский отраслевой НИИ связи
ЛЭИС	Ленинградский электротехнический институт связи
МККТТ	Международный консультативный комитет по телеграфии и телефонии
СПбГУТ	Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича;
СПС	Сеть подвижной связи
ТфОП (PSTN)	Телефонная сеть общего пользования
ФГОС	Федеральный образовательный стандарт
ЦСИО	Цифровая сеть интегрального обслуживания
ЧНН	Час наибольшей нагрузки

Гольдштейн Борис Соломонович
Кучерявый Андрей Евгеньевич

Сети связи пост-NGN

ИБ № 3004 ЛР № 065953 от 15.08.98

Формат 60x90 1/8.
Бумага офсетная.
Гарнитура прагматика. Печать офсетная
Объем 20 печ. л.
Доп. тираж
«БХВ-Петербург», 191036, Санкт-Петербург, Гончарная ул., 20

Первая Академическая типография «Наука»
199034, Санкт-Петербург, 9 линия,12/28

Авторы почти в одно и то же время родились, учились, с медалями окончили школы (разные), с отличием окончили ВУЗ (один и тот же) – факультет автоматической электросвязи Ленинградского электротехнического института связи им. проф. М.А. Бонч-Бруевича (ныне Санкт-Петербургский государственный университет телекоммуникаций, СПбГУТ), с которым фактически более не расставались и не расстаются по сей день.

Оба по распределению пришли на работу в Ленинградский отраслевой НИИ связи, где и проработали последовательно на всех мыслимых и немыслимых должностях более 70 лет (на двоих), а сегодня продолжают делать то же самое, но уже в разных местах: Андрей Кучерявый – на кафедре «Сетей связи» и в институте ГИПРОСВЯЗЬ – Северо-Запад, а Борис Гольдштейн – на кафедре «Систем коммутации и распределения информации» СПбГУТ и в Научно-технических центрах АРГУС, ПРОТЕЙ и СЕВЕНТЕСТ группы компаний ЭКРАН.

Без отрыва от основной работы оба в одно и то же время окончили аспирантуру, защитили кандидатские, а затем и докторские диссертации по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Опубликовали на двоих более полутысячи научных статей и докладов (за подавляющее большинство из которых им и сегодня не стыдно), получили более полусотни авторских свидетельств и патентов на изобретения (некоторые из которых – с моральным и даже материальным эффектом), издали несколько десятков книг по разным аспектам телекоммуникаций (и к своей радости иногда встречали экземпляры этих книг, если не зачитанные до дыр, то, как минимум, весьма потрепанные). Эти книги и статьи позволили авторам набрать вполне приличный индекс цитируемости, особенно если суммировать его, как и все вышеперечисленное, на двоих.

Авторы принимали и принимают участие в работе Исследовательских комиссий Международного союза электросвязи, в IEEE, в оргкомитетах целого ряда Международных конгрессов, симпозиумов и конференций, в подготовке выпусков журналов «IEEE Communications Magazine», «IEEE Selected Areas of Communications» и др., в редакционных коллегиях многих отраслевых журналов, в Международной академии связи, в Международной академии информатизации, в профильных ученых и диссертационных советах и др.

Значительную часть времени и сил авторы посвящают преподаванию в СПбГУТ им. проф. М.А. Бонч-Бруевича, заведуют ведущими кафедрами этого университета, подготовили десятки аспирантов, почти никто из которых не дал повода почувствовать горечь предательства, зато почти каждый предоставил множество оснований гордиться своими успехами на самых разных предприятиях и в самых разных странах.

Так что с учениками авторам повезло. Именно поэтому они и решились написать эту книгу, которая, с одной стороны, посвящена светлой памяти их учителя, директора и друга Анатолия Николаевича Голубева, а с другой стороны, адресована молодым инженерам, аспирантам, студентам, которым предстоит работать в этих самых инфокоммуникациях 2010-х и последующих лет интереснейшей эпохи пост-NGN.

Авторы взяли на себя смелость изложить самые последние идеи и подходы к инфокоммуникациям, основные ре(э)волюционные технологии и архитектуры, включая такие разные векторы развития инфокоммуникаций как Интернет вещей (IoT – Internet of Things) и сети мобильной связи 4G поколения SAE/LTE-Advance, всепроникающие сенсорные сети (USN – Ubiquitous Sensor Networks) и мультимедийная IP-подсистема (IMS – IP Multimedia Subsystem), сети для транспортных средств (VANET – Vehicular Ad-Hoc Networks) и молекулярные наносети.

Книга будет одинаково полезна топ-менеджерам, инженерам, студентам, аспирантам и всем специалистам, работающим в сегодняшних бурно развивающихся инфокоммуникациях.

ISBN 978-5-9775-0900-8

http://www.niits.ru/