

Знакомство с современными беспроводными технологиями. Многошаговые беспроводные сети: принципы построения и открытые задачи *

Е.М. Хоров

Назначение беспроводных многошаговых самоорганизующихся сетей

Беспроводные широкополосные сети резко расширили область своего применения на рубеже тысячелетий благодаря актуальности двух задач, известных как задача *последней мили* и задача построения *децентрализованных сетей*.

Задача *последней мили* заключается в организации доступа к сервисам традиционной проводной инфраструктурной сети для конечных пользователей. Для ее решения в проводную сеть включается специальное устройство – точка доступа, или базовая станция, к которой по беспроводному каналу подключаются клиентские станции конечных пользователей. В рамках такой архитектуры «клиент-сервер» доступ к среде может осуществляться централизованным или распределенным методами. В первом случае точка доступа монополично управляет доступом к среде, предотвращая коллизии (одновременную передачу пакетов разными станциями), причем, так как в отсутствие точки доступа клиентские станции все равно не могут подключиться к проводной сети, наделение ее монопольными правами не снижает надежности сети в целом. Во втором случае доступ к среде осуществляется на конкурентной основе, и все клиентские станции, а также сама точка доступа соревнуются за право передать свои пакеты.

Децентрализованные сети, или сети класса ad hoc, – это самоорганизующиеся сети, создаваемые из равнозначных станций тогда, когда это необходимо, без проводной инфраструктуры. Задача построения таких сетей также может быть решена с помощью выделения в сети некоторого устройства-координатора и наделения его полномочиями «сервера» по отношению к остальным устройствам, играющим роль «клиентских» станций, но это нецелесообразно. В отличие от задачи последней мили, при решении которой архитектура «клиент-сервер» является естественной, искусственное назначение станциям ролей «клиентов» и «сервера» при решении задачи построения децентрализованных сетей снижает надежность сети. Действительно, выход из строя устройства-координатора прерывает работу сети, несмотря на то, что это устройство не выполняет никаких функций, которые не могли бы выполнять другие станции. Вот почему при решении задачи построения децентрализованных сетей предпочтительно использование исключительно распределенного управления доступом к каналу.

Отказ от архитектуры «клиент-сервер» при построении сетей класса ad hoc делает решения задачи последней мили и решения задачи построения децентрализованных сетей существенно разными, что наиболее ярко отражено в разработанном международным комитетом IEEE 802¹ стандарте IEEE 802.11 [1] беспроводных локальных сетей, известных под торговой маркой Wi-Fi, – в стандарте описаны два типа сетей: инфраструктурные сети и сети ad hoc.

Технология инфраструктурных сетей (Wi-Fi Hotspot) широко известна по миллионам точек беспроводного доступа, развернутых во всем мире. Опираясь на проводную инфраструктурную сеть, точки доступа предоставляют клиентским станциям, как правило, выход в Интернет. Благодаря своему широкому распространению и простоте технология Wi-Fi Hot Spot хорошо изучена и в данной статье рассматриваться не будет.

Сети ad hoc, не требующие инфраструктуры, в рамках базового стандарта IEEE 802.11 являются одноранговыми сетями, в которых каждая станция находится в зоне непосредственного радиоприема всех остальных

*Статья подготовлена в рамках работ по гранту Министерства образования и науки (Соглашение №8330 от 17.08.2012)

¹В рамках комитета IEEE 802 LAN/MAN Standards Committee (Комитет Института инженеров электротехники и электроники по стандартам локальных и городских сетей) оформились в виде стандартов такие технологии, как Ethernet, Token Ring, Wi-Fi, Bluetooth и WiMAX.

станций. Однако с момента начала работы над стандартом появилось множество новых задач, связанных с развертыванием таких беспроводных сетей, как:

- домашние, офисные и заводские сети;
- сети университетских городков;
- муниципальные и коммерческие публичные сети;
- сети транспортных узлов (автомобилей, а в последние несколько лет и самолетов);
- сети, развертываемые в зонах чрезвычайных ситуаций;
- сети военного назначения.

Эти задачи требовали расширения зоны покрытия сети и обеспечения бесперебойной работы движущихся станций.

Расширение зоны покрытия сети означает, что, хотя сеть в целом остается связной, некоторые станции находятся вне зоны радиоприема друг друга, поэтому для доставки пакетов между ними требуется ретрансляция пакетов через промежуточные станции. Таким образом, расширение зоны покрытия сети приводит к переходу от одношаговой сети к многошаговой.

Движение же станций означает, что топология сети меняется со временем и станции могут в течение своей работы находиться то в зоне непосредственного радиоприема друг друга, то за пределами этой зоны. Технологиями, призванными расширить зону покрытия сети и обеспечить бесперебойную работу движущихся станций, стали технология самоорганизующихся мобильных ad hoc сетей MANET [2], оформленная в виде спецификаций организации IETF (англ.: Internet Engineering Task Force – Инженерный совет Интернета), и технология сетей Wi-Fi Mesh [3], разработанная в комитете IEEE 802 LAN/MAN Standards Committee.

Сети MANET

Сети MANET (англ.: Mobile Ad hoc NETwork – мобильная децентрализованная сеть) представляют собой сети, координация которых осуществляется на сетевом уровне, а доступ к каналу осуществляется с помощью одной из уже существующих технологий, допускающей построение децентрализованных сетей. Наибольшее развитие и известность получили сети MANET, построенные на базе технологии Wi-Fi ad hoc, и использующие для многошаговой доставки пакетов протоколы маршрутизации, работающие на сетевом (IP) уровне.

Особенности распределенного метода доступа к среде в сетях Wi-Fi ad hoc

Стандарт IEEE 802.11 определяет набор правил передачи пакетов, которые позволяют обеспечить распределенный конкурентный доступ к среде. В сетях ad hoc базовым механизмом доступа к среде является *режим распределенного управления DCF* (англ.: Distributed Coordination Function), в основе которого лежит метод множественного доступа с контролем несущей и избеганием коллизий CSMA/CA (англ.: Carrier Sense Multiple Access with Collision Avoidance).

Механизм DCF работает следующим образом [4].

Пусть в *непустую* очередь станции поступил пакет.

Этот пакет будет ожидать в очереди, пока не будет обслужен предыдущий пакет. После этого станция инициализирует счетчик отсрочки случайным целым числом из конкурентного окна – интервала $[0, CW_{min}]$. Пока среда свободна, значение счетчика отсрочки уменьшается на 1 каждый слот (интервал длительностью *slot*). Когда среда становится занятой, счетчик отсрочки замораживается; возобновление отсчетов слотов происходит после того, как среда освободится на определенный интервал. В качестве этого интервала выступает *EIFS* (англ.: Extended interframe space – увеличенный межкадровый интервал), если передавался сигнал, который станция не смогла декодировать, и *DIFS* (англ.: DCF interframe space – межкадровый интервал DCF) – если сигнал был декодирован.

Станция может начать передачу пакета при соблюдении обоих условий:

- среда оставалась свободной в течение интервала *DIFS* или *EIFS* (выбор интервала описан выше);
- значение счетчика отсрочки равно 0.

Пакет может предназначаться одной или нескольким станциям. Получение пакетов, предназначенных нескольким станциям (широковещательная передача), в текущей версии стандарта [1] не подтверждается, и обслуживание таких пакетов отправителем прекращается сразу же после его отправки. Если же пакет предназначен одной станции (одноадресная передача), то она должна сразу же подтвердить его получение. Для этого, по истечении короткого интервала *SIFS* (англ.: Short Interframe Space – короткий межкадровый интервал) после приема пакета станция-приемник отправляет короткий кадр-подтверждение АСК (англ.: acknowledgement – подтверждение). Если отправитель пакета получает АСК в течение интервала *AckTimeout* после отправки пакета, то на этом передача (обслуживание) пакета прекращается, пакет считается успешно переданным.

Если попытка передачи была неудачной и лимит *RL* (англ.: Retry Limit – ограничение числа повторов) количества повторных попыток передачи одного пакета не достигнут, станция начинает новую попытку передачи. Новая попытка предваряется выбором нового интервала отсрочки из увеличенного интервала $[0, CW_{new}]$: новое значение CW_{new} зависит от предыдущего CW_{old} согласно следующей формуле:

$$CW_{new} = \min \{2(CW_{old} + 1) - 1, CW_{max}\}, \quad (1)$$

где CW_{max} – максимальный размер конкурентного окна.

Если попытка передачи была неудачной, и был достигнут лимит *RL*, то станция прекращает обслуживания пакета.

Завершение обслуживания пакета всегда сопровождается инициализацией счетчика отсрочки случайным числом из минимального конкурентного окна $[0, CW_{min}]$.

Если пакет поступил в очередь, когда станция не занята обслуживанием какого-либо пакета, то она может начать его передачу сразу, как только счетчик отсрочки, взведенный после предыдущей передачи, обнулится и среда будет свободной в течение интервала *DIFS* или *EIFS*.

Очевидно, что методы DCF оказывается эффективным, только когда все станции находятся в зоне уверенного радиоприема друг друга. В этом случае станции, имеющие пакеты для передачи, отсчитывают счетчики отсрочки синхронно. Таким образом, коллизия может возникнуть, только если счетчики одновременно обнулятся. Вероятность этого тем меньше, чем больше размер конкурентного окна, которое увеличивается, если происходят коллизии.

В многошаговой беспроводной сети возможны явления, которые не наблюдаются в одношаговых сетях, например, *эффект скрытых станций*. Скрытыми называют станции, которые находятся вне зоны радиоприема друг друга, но имеют при этом общую соседнюю станцию. На рис. 1 это станции А и С.

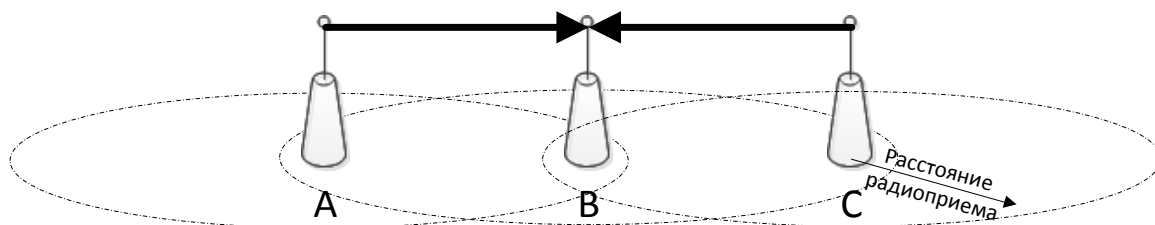


Рис. 1. Скрытые станции в многошаговых сетях

Поскольку скрытые станции не слышат радиопередачу друг друга, они считают слоты отсрочки независимо друг от друга, и одна станция может начать передачу в то время, как другая уже передает пакет. Произойдет коллизия, и станция *B* не сможет корректно принять ни пакет станции *A*, ни пакет станции *C*. Вероятность этого события существенно выше вероятности одновременного начала передачи пакета. Как показано в работах [6], наличие скрытых станций приводит к существенному снижению скорости передачи в сети, а в некоторых случаях – к блокировке соединений между станциями, что может приводить не только к падению производительности сети, но и к нарушению ее связности.

Таким образом, распределенный метод доступа, используемый в сетях Wi-Fi, оказывается неэффективным в многошаговых сетях и может приводить к низкой вероятности успешной передачи пакета, что необходимо принимать во внимание при разработке протоколов маршрутизации.

Маршрутизация в сетях MANET

Одной из ключевых задач в многошаговых сетях является задача поиска маршрута между двумя станциями, известная как задача маршрутизации. Ранние протоколы маршрутизации в сетях MANET, такие как OLSR [7] (англ.: Optimized Link State Routing – оптимизированная маршрутизация, использующая информацию о соединениях), AODV [8] (англ.: Ad hoc On-Demand Distance Vector Routing – реактивный протокол маршрутизации, использующий информацию о длинах маршрутов) и DSDV [9] (англ.: Destination-Sequenced Distance Vector – проактивный протокол маршрутизации, использующий информацию о длинах маршрутов), представляют собой слегка адаптированную кальку с протоколов маршрутизации, разработанных для проводных сетей. Например, протокол OLSR очень похож на протокол OSPF (англ.: Open Shortest Path First – маршрутизация с использованием коротких путей), применяемого для маршрутизации в проводных сетях.

Работая на сетевом уровне, простые протоколы маршрутизации никак не взаимодействуют с канальным уровнем. Таким образом, им недоступна информация о вероятности искажения пакетов помехами и коллизиями, о свойствах сигнально-кодированных конструкций, используемых на каждом из соединений, а также о методе доступа к каналу и параметрах механизма повторов непринятых пакетов. Следовательно, эти протоколы не могут определить вероятность успешной передачи пакета по соединению, а также пропускную способность соединения, а маршруты, найденные с их помощью, обладают малой пропускной способностью и часто пропадают [6, 10]. Кроме того, протоколы маршрутизации зачастую не учитывают такие особенности беспроводной среды, как:

- высокую вероятность потери пакета при широкополосной передаче, что приводит к частой потере служебной информации;
- экспоненциальный рост вероятности потери пакета при увеличении его длины, что накладывает ограничения на возможности агрегирования пакетов;
- влияние передачи пакета одной станцией на передачу пакетов соседними с ней станциями и т. д.

Из-за этого сети MANET, работающие под управлением простых протоколов, обладают низкой производительностью (см., например, [11]), и возможности их использования весьма ограничены.

Сети Wi-Fi Mesh стандарта IEEE 802.11s

Для повышения эффективности протоколов маршрутизации в сетях MANET потребовалось снабдить их информацией о канальном уровне, например, о качестве соединений с помощью метрики маршрутизации. Такой подход следует устоявшейся парадигме, что маршрутизация должна выполняться на сетевом уровне. Однако при его воплощении в жизнь разработчики сталкиваются с проблемой межуровневого взаимодействия: для повышения пропускной способности и отказоустойчивости многошаговой сети необходимо, чтобы протоколы маршрутизации использовали весьма специфичную информацию с канального уровня и управляли передачей пакетов на канальном уровне. Таким образом, протоколы должны учитывать возможности сетевых карт определенного производителя и определенной марки.

Устранить проблему межуровневого взаимодействия можно, решая задачу маршрутизации на канальном уровне. По этому пути пошел комитет по стандартам IEEE 802 LAN/MAN Standards Committee. В 2004 г. этот комитет создал отдельную группу для разработки стандарта беспроводных многошаговых самоорганизующихся сетей. В стандарте IEEE 802.11s [3], опубликованном в конце 2011 г., такие сети получили название сетей Wi-Fi Mesh.

В качестве примера механизмов, используемых в сетях Wi-Fi Mesh, рассмотрим новый метод доступа к каналу, описанный в стандарте этих сетей [3].

Детерминированный метод доступа к среде для многошаговых сетей Wi-Fi Mesh

Как было отмечено выше, методы случайного доступа к среде, разработанные для одношаговых сетей, оказываются неэффективными в многошаговых сетях из-за эффекта скрытых станций, поэтому для защиты пакетов от коллизий, наряду с традиционным случайным (конкурентным) методом, в сетях Wi-Fi Mesh может применяться опциональный детерминированный метод – МССА (англ.: Mesh coordination function Coordinated Channel Access – Метод доступа для mesh-сетей).

МССА основан на предварительном резервировании интервалов времени, называемых МССАОР (англ.: Mesh coordination function Coordinated Channel Access Opportunity), в течение которых возможны бесконку-

рентная передача данных от станции-владельца резервирования к станции-адресату резервирования и доставка кадра подтверждения получения данных в обратном направлении. Чтобы при этом не возникло коллизий, соседние станции владельца и адресата резервирования не должны вести передачу в течение всего зарезервированного интервала. Для обеспечения синхронизации информации о существующих зарезервированных интервалах каждая станция периодически рассылает рекламу: информацию о своих резервированиях, а также о резервированиях своих соседей.

Учитывая накладные расходы при установлении резервирования, а также при его рекламе, установление резервирования для передачи единственного пакета оказывается невыгодным. Поэтому МССА следует использовать для управления резервированиями, каждое из которых состоит из нескольких зарезервированных интервалов.

МССА-резервирование определяется тремя параметрами:

- длительностью (MCCAOP duration) каждого зарезервированного интервала;
- периодичностью (MCCAOP periodicity) – числом зарезервированных интервалов в течение одного DTIM-интервала².
- смещением (MCCAOP offset) первого зарезервированного интервала от начала DTIM-интервала.

Стандарт ограничивает суммарную долю *MAF* (англ.: MCCA Access Fraction – доля МССА) временных ресурсов сети внутри одного DTIM-интервала, которая может быть занята под МССА-резервирования, с помощью параметра *MAFLimit*. Если при создании нового резервирования суммарная доля *MAF* интервалов времени зарезервированного под детерминированный метод доступа превышает *MAFLimit* на самой станции или на соседних станциях, станция отказывается от установления резервирования.

Хотя метод МССА и позволяет бороться с эффектом скрытых станций, он удобен лишь при доставке потоковых данных постоянной интенсивности, например, голосовых данных. Таким образом, в многошаговых сетях по-прежнему остается конкурентный метод доступа к среде, и проблемы, связанные с его использованием, не исчезают.

Несмотря на очевидные достоинства метода детерминированного доступа, он сложен в реализации, поэтому в стандарте он отмечен как опциональный, т.е. некоторые станции могут его не поддерживать. Если станция не поддерживает МССА, то она сама резервирования не устанавливает, а в течение интервалов времени, зарезервированных другими станциями, осуществляет доступ к среде на конкурентной основе. Таким образом, метод МССА оказывается эффективным для станции, которая его использует, только в том случае, когда остальные станции его поддерживают.

Другие многошаговые сети

Создание mesh-сетей возможно не только на базе технологии беспроводных локальных сетей. В рамках комитета IEEE 802 LAN/MAN Standards Committee были разработаны стандарты IEEE 802.15.1, IEEE 802.15.3, IEEE 802.15.4 и IEEE 802.15.5 [12–15], в которых регламентируется возможность организации персональных многошаговых сетей, а также стандарт IEEE 802.16 [16] городских беспроводных сетей, известных под маркой WiMax, который включал в себя механизм образования mesh-сетей с централизованным или распределенным управлением. Кроме того, организацией Etsi International (англ.: European Computer Manufacturers Association) была создана технология сверхвысокоскоростных персональных mesh-сетей WiMedia (стандарт ECMA-368 [17]). Из-за того, что они получили значительно меньшее распространение, чем сети IEEE 802.11s, в данной статье они не были рассмотрены.

Открытые задачи

Несмотря на высокий интерес к многошаговым беспроводным сетям со стороны исследователей и разработчиков, все еще остается множество открытых задач.

Первая группа задач связана с методом доступа к среде. Хотя МССА и позволяет снизить вред, наносимый скрытыми станциями, он не гарантирует надежную передачу данных, поэтому важно разработать методы,

²DTIM-интервал станций определяется как интервал времени между двумя последовательными биконами, содержащими информационный элемент DTIM (англ.: Delivery Traffic Indication Message – сообщение-индикатор трафика, который необходимо доставить).

повышающие надежность МССА. Кроме того, необходимы алгоритмы, позволяющие определить объем ресурсов, которые надо зарезервировать для передачи потоковых данных. Особый интерес представляет передача мультимедийных данных, накладывающая ограничения на время доставки и долю потерянных данных.

Вторая группа задач связана с разработкой протоколов маршрутизации, строящих маршруты с учетом требований к качеству обслуживания передаваемых данных, а также принимающих во внимание тот факт, что доступ к среде может осуществляться разными методами: случайным и детерминированным.

Список литературы

- [1] IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.
- [2] Mobile Ad-hoc Networks (manet) : Rep. : IETF, 2008. — URL: <http://www.ietf.org/html.charters/manet-charter.html>.
- [3] IEEE 802.11s STANDARD for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment: Mesh Networking [Electronic resource], 2011.
- [4] Е.М. Хоров. Метрика маршрутизации для трафика, чувствительного к задержкам // Труды конференции «Информационные технологии и системы». — 2010. — С. 11–19.
- [5] Bianchi G. Performance Analysis of the IEEE 802.11 Distributed Coordination Function // IEEE Journal on Selected Areas in Communications 18(3). — 2000. — P. 535–547.
- [6] Lyakhov A., Pustogarov I., Gudilov A. IEEE 802.11 Direct links: Interference Classification and Modeling // Selected Lectures on Multiple Access and Queueing Systems. Revised Selected Papers from International Workshop on Multiple Access Communications (MACOM-2008). — Saint-Petersburg, Russia, 16–17th June, 2008. — P. 15–24.
- [7] Jacquet Philippe, Clausen Thomas. — Optimized Link State Routing Protocol (OLSR). — IETF, 2003. — October. — URL: <http://www.ietf.org/rfc/rfc3626.txt>.
- [8] Ad Hoc On-Demand Distance Vector Routing Protocol : Rep. / IETF MANET Working Group : 2003. — July 2003. — URL: <http://www.ietf.org/rfc/rfc3561.txt>. — Expiration: August 17, 2003.
- [9] Perkins Charles E., Bhagwat Pravin. DSDV Routing over a Multihop Wireless Network of Mobile Computers // Ad Hoc Networking / Ed. by Charles E. Perkins. — Addison-Wesley, 2001. — P. 53–74.
- [10] Ляхов А.И., Пустогаров И.А., Гудиллов А.С. Проблема неравномерного распределения пропускной способности канала в сетях IEEE 802.11 // Информационные процессы. — 2008. — Т. 8, № 3. — С. 149–167.
- [11] А.А. Сафонов, Е.М. Хоров, А.Н. Красилов. Анализ эффективности протокола OLSR в канале 5МГц // Труды конференции «Информационные технологии и системы». — 2010. — С. 11–19.
- [12] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN), 2005.
- [13] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN), 2003.
- [14] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs), 2006.
- [15] IEEE Recommended Practice for Information technology– Telecommunications and information exchange between systems– Local and metropolitan area networks– Specific requirements Part 15.5: Mesh Topology Capability in Wireless Personal Area Networks (WPANs), 2009.
- [16] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems, 2004.
- [17] High Rate Ultra Wideband PHY and MAC Standard, Standard ECMA-368, 2nd ed, [Electronic resource], 2007.