

## МЕТОДЫ МНОЖЕСТВЕННОГО ДОСТУПА В МОБИЛЬНЫХ РАДИОСЕТЯХ

Одной из проблем управления мобильными радиосетями (МР) — сетями MANET — является эффективное разделение их ресурсов между множеством независимо функционирующих узлов, что предполагает применение на канальном уровне соответствующих методов доступа (МД), к которым *предъявляются следующие основные требования: децентрализованное функционирование, высокая пропускная способность, малая задержка передачи, а также ряд дополнительных — передача неоднородного (данные, речь, видео) и приоритетного трафика, использование направленных антенн, управление очередностью передач в МР* [1].

Методы доступа можно классифицировать по следующим признакам (рис. 1):

- ◆ по организации сети и процесса передачи сообщений — централизованные, децентрализованные и зонавые; синхронные или асинхронные, с выделенным каналом управления или без него; с квитированием или без него;

- ◆ по способу разделения канала — детерминированные (статические или динамические), случайные (неконтролируемые и контролируемые) и гибридные (их комбинация);

- ◆ по количеству и типу используемых радиоканалов в сети — одноканальные и многоканальные, симметричные и асимметричные;

- ◆ по использованию в узлах сети оборудования позиционирования (координатные и некоординатные) и антенн с изменяющейся диаграммой направленности (направленные или ненаправленные);

- ◆ по реализации функций (дополнительных сервисов) — энергосбережение; ширококвещательная (групповая) передача; передача с заданным качеством обслуживания (QoS); передача приоритетного трафика, безопасность.

Рассмотрим предложенную классификацию более подробно.

Классификация и анализ *централизованных* МД в беспроводных сетях приведены в [1–3]. Зонавая организация сети, предполагающая разбиение ее на зоны (кластеры) с выделением в каждой зоне главных и простых узлов, а также шлюзов (для связи между зонами), является комбинацией централизованного (в зонах) и децентрализованного (между главными узлами) способов управления.

МР могут функционировать в *синхронном* или *асинхронном* режиме. Синхронизация предполагает, что радиоканал сегментирован на дискретные интервалы времени (слоты), объединенные в повторяющиеся фрагменты. Регулярность и однородность слотов позволяет реализовать передачу с заданным качеством обслуживания (QoS), так как задержка, пропускная способность и джиттер легко управляются посредством назначения временных слотов. Сложность процесса синхронизации зависит от организации сети. В централизованной сети узлы каждой соты легко синхронизируются базовой станцией, которая ширококвещательно передает сигнал, указывающий на начало временного фрагмента. В МР процесс синхронизации значительно сложнее и может быть осуществлен за счет временных сигналов глобальной



Рис. 1. Классификация методов доступа в МР

системы позиционирования (GPS). В свою очередь, асинхронный режим не предполагает глобальной синхронизации узлов и поэтому не требует дополнительного оборудования, однако определяет сложность в передаче данных (например, интегрального трафика) из-за случайного характера обмена информацией.

Организация сети тесно взаимосвязана со способами разделения канала: *детерминированным, случайным и гибридным*.

Реализация *детерминированных методов доступа* заключается в планировании (резервировании) ресурса сети для передачи сообщений. В качестве ресурса могут выступать частота (FDMA), время (TDMA), коды (CDMA), пространство (SDMA) или их сочетание (гибридные МД, например TDMA/CDMA или STDMA). Планирование может осуществляться как с учетом, так и без учета текущей топологии сети.

*Статические детерминированные МД* являются централизованными (предполагают наличие информации о всей сети) и осуществляют фиксированное планирование ресурсов сети до начала передач узлов. Данная задача относится к классу NP-полных, и с увеличением размерности сети для ее решения применяют эвристические алгоритмы [3].

*Динамические детерминированные МД* для планирования используют информацию о нагрузке и топологии сети. Здесь задача распределения ресурсов усложняется из-за отсутствия глобальной информации о сети (обычно каждый узел собирает информацию на расстоянии  $k$ -ретрансляций), поэтому предлагаемые МАС-решения для МР в указанной области имеют целью получение субоптимальных децентрализованных решений [3; 4].

Большинство известных детерминированных МД ориентировано на распределение временного ресурса, что возможно только в синхронных сетях. Соответствующие методы являются преимущественно бесконфликтными, т. е. длина передаваемого пакета меньше длительности слота (последние могут иметь фиксированную или переменную длину). Функционирование динамических детерминированных МД предполагает два этапа: на первом резервируются слоты, а на втором осуществляется непосредственно передача [3; 4]. Примерами реализации детерминированных МД являются технологии Bluetooth и HiperLan [5].

Рассмотрим *случайные МД*, большинство из которых функционируют в условиях асинхронной сети. Исторически первым считается метод *ALOHA*, не предполагающий взаимной координации узлов. Любой узел  $i$ , подготовив пакет к передаче узлу  $j$ , в произвольный момент времени начинает передачу. Передав пакет, узел  $i$  определенное время ожидает прием квитанции от узла  $j$ . Если квитанция не получена, то через случайный промежуток времени передача начинается вновь. Очевидно, что вероятность столкновений у этого метода очень велика (максимальная пропускная способность для полносвязной сети  $S = 0,18$  [2]). Повысить пропускную способность сети можно сегментированием сети — *S-ALOHA* ( $S = 0,36$  [3]).

Для снижения вероятности столкновений пакетов применяют методы доступа с контролем несущей (МДКН) или CSMA, т. е. методы, основанные на предварительной проверке состояния радиоканала. В простейшем случае перед передачей пакета узел контролирует состояние канала (наличие несущей или самой передачи). Если канал занят, узел откладывает передачу на более позднее время. При освобождении канала его передача может начинаться различными способами: сразу («жесткий» МДКН), через случайный интервал времени («мягкий»), с вероятностью  $p$  ( $p$ -настойчивый) или с рандомизацией времени передачи на сегменты [2].

Основным препятствием успешной передаче пакета при МДКН являются так называемые проблемы скрытого и открытого терминалов, т. е. возможность столкновения пакетов из-за распределенности процесса принятия решения на передачу (рис. 2). Проблема «скрытого терминала» (рис. 2, а) заключается в том, что узел  $a$  не находится в пределах радиосвязности с узлом  $c$  и, соответственно, не может прослушивать его передачи. Поэтому при передаче пакета от узла  $a$  к узлу  $b$  узел  $c$  в это же время может передать свой пакет (например, узлу  $d$ ). В результате возникает столкновение пакетов. В данном случае узел  $c$  является скрытым узлом относительно узла  $a$ .

Проблема «открытого терминала» (рис. 2, б) такова: узел  $c$  передает пакет узлу  $d$  и блокирует на время передачи узел  $b$ , который намеревается осуществить передачу узлу  $a$  (хотя процесс данной передачи бесконфликтен).

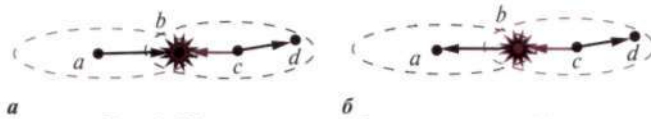


Рис. 2. Иллюстрация проблем «скрытого» (а) и «открытого» (б) терминалов

Для решения названных проблем предложен ряд методов (протоколов) множественного доступа с контролем несущей и предотвращением столкновений (CSMA/CA). Наиболее известные — это MACA [6], MACA-BI [7], FAMA [8], MACAW [9], DBTMA [10] и IEEE 802.11 DCF [5]. Применением перечисленных методов канал временно резервируется до момента передачи информационного пакета DATE с помощью диалога короткими служебными пакетами между получателем и отправителем: запрос на передачу отправителя (RTS) и согласие получателя (CTS).

MACA осуществляет 3-этапный процесс передачи RTS/CTS/DATE (рис. 3, а). MACA-BI улучшает характеристики MACA за счет исключения RTS. В этом случае передача (ее инициирует получатель посылкой RTR) осуществляется за два шага — RTR/DATE (рис. 3, б).



Рис. 3. Функционирование MACA (а) и MACA-BI (б)

Метод FAMA аналогичен MACA за исключением того, что длительность пакета CTS значительно больше RTS, что позволяет всем соседям узла *b*, обнаружив шум после передачи своего RTS, сделать вывод о занятости канала (рис. 4, а).

Для повышения надежности доставки пакетов MACAW дополнительно использует квитанцию ACK, подтверждающую правильный прием информации — RTS/CTS/DATA/ACK (рис. 4, б). Кроме явного квитирования в МР может использоваться пассивное или эхоквитирование — узел, передавший пакет, «слышит» его ретрансляцию соседом. Недостаток явного квитирования — дополнительная нагрузка на сеть в виде служебной информации. Что же касается пассивного квитирования, то оно позволяет уменьшить служебный трафик, но, в свою очередь, имеет следующие недостатки: последняя ретрансляция предполагает явное квитирование; возникает значительная задержка передачи пакета, определяемая задержкой в очереди ретранслятора; ощущаю повышение вероятность столкновений информационного пакета по сравнению с квитанцией (длительность квитанции намного меньше длительности информационного пакета); невозможность использования в системах с кодовым разделением канала. Отметим, что

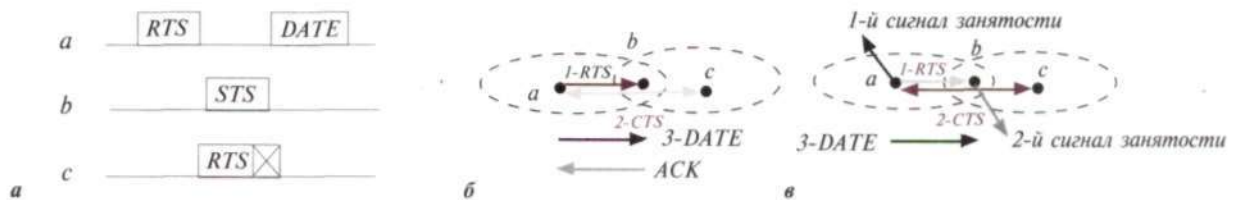


Рис. 4. Функционирование методов FAMA (а), MACAW (б) и DBTMA (в)

механизм квитирования на канальном уровне не реализуется в МР с однонаправленными каналами. В этом случае квитирование осуществляется сетевым уровнем за счет инкапсуляции квитанции в пакет сетевого уровня и его передачи по альтернативному маршруту.

Метод DBTMA разделяет выделенную полосу частот на два канала: в одном передаются данные, а в другом — служебная информация и (на отдельных частотах) сигналы занятости отправителя и получателя (рис. 4, в).

Децентрализованный режим работы протокола IEEE 802.11 DCF развивает схему резервирования MACAW (RTS/CTS/DATA/ACK) (рис. 5). Перед передачей RTS узел ожидает определенный период DIFS +  $cw$  (DCF указывает наибольшее время ожидания, а следовательно, приоритет доступа и окно состязаний). Если RTS принято без ошибок, получатель через короткий промежуток SIFS посылает пакет CTS. Получив разрешение на передачу, отправитель (по истечении времени SIFS) посылает пакет данных DATE. Адресат, проверив безошибочность приема пакета, через интервал SIFS посылает отправителю квитанцию ACK.

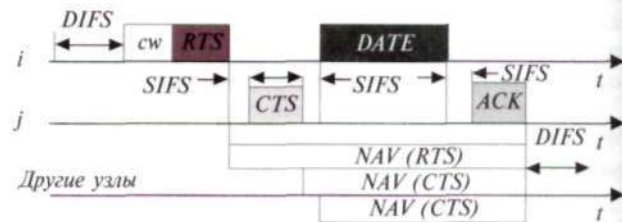


Рис. 5. Протокол IEEE 802.11 DCF

Для реализации бесконфликтных передач (исключения передач соседних узлов отправителя и получателя) используется специальный механизм NAV, предполагающий, что каждый из передаваемых пакетов содержит информацию о своей длительности (см. рис. 5). Поэтому соседи отправителя и получателя, принимая их, запрещают свои передачи на данный период.

Управление последовательностью доступа к каналу согласно протоколу IEEE 802.11 DCF осуществляется за счет динамического изменения размера окна состязаний  $cw$  (первоначально устанавливается его минимальное и максимальное значение, например  $cw_{min} = 7$  и  $cw_{max} = 255$ ). При занятости среды узел ожидает начала передачи (DIFS) и вступает в фазу состязаний (рис. 6). Каждый узел выбирает случайный временной сегмент (в пределах окна состязаний), в течение которого ожидает освобождения среды. Если канал занят, узел должен пропустить данный цикл доступа и подождать следующей возможности, пока среда не освободится (по крайней мере на время DIFS). Чем больше окно состязаний, тем меньше вероятность выбрать одинаковые сегменты начала передачи, а значит, вероятность кон-

фликта снижается. Однако при небольшой нагрузке малое окно состязаний обеспечивает меньшее время задержки доступа. Управляя выбором временного сегмента и размерами окна состязаний, можно обеспечить приоритетное обслуживание (принцип передачи «с максимальным усилием»).

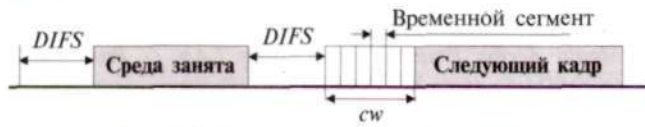


Рис. 6. Окно состязаний и время ожидания

Приведем (в виде таблицы) общую характеристику протоколов канального уровня, предложенных для использования в радиосетях.

Анализ таблицы позволяет сделать вывод о том, что в условиях высокой мобильности узлов, характерной для МР, предпочтителен протокол IEEE 802.11, хотя и он далек от совершенства. В качестве недостатков можно отметить следующие: неэффективен для протоколов транспортного уровня (например, для TCP) и широко-вещательной (групповой) передачи пакетов, невозможна передача трафика с заданным качеством обслуживания, несовершенны алгоритмы энергосбережения и др. [11].

Поэтому в настоящее время продолжается разработка новых МД, реализующих дополнительные функции и/или использующих дополнительное оборудование (позиционирования, направленные антенны и др.) по следующим направлениям.

♦ **Управление энергосбережением.** Беспроводные устройства питаются от батарей, и, следовательно, необходимо минимизировать расход их энергии. Соотношение расходуемой мощности в зависимости от режимов работы узла «сон»/поиск/прием/передача для современных беспроводных карт (например, для Lucent IEEE 802.11 WarePC Card) составляет 0,025:1:1,2:1,6 Вт. Поэтому возможным решением может быть отключение приемников или уменьшение передаваемой мощности. Так, в протоколе IEEE 802.11 DCF реализован режим периодического отключения узлов, правда в предположении полносвязной сети. В протоколе PAMAS используется режим «сна» — узел, обнаружив, что передаваемый пакет предназначен не ему, отключается на время передачи данного пакета [13]. При другом подходе (PCM) отправитель и получатель передают RTS и CTS с одинаковой мощностью, однако передача DATA и ACK осуществляется минимальной мощностью, необходимой

для безошибочного приема [14]. Уменьшить потребляемую мощность позволяет также применение эхо-квирования.

♦ **Широковещательная передача.** Для повышения надежности широковещательной передачи предложен протокол BSMA [15] (используется при зондовой и волновой маршрутизации). Его особенность состоит в уменьшении столкновений пакетов за счет приема отправителем CTS от всех соседних узлов.

♦ **Кодовое разделение каналов** позволяет решить проблемы скрытых и открытых абонентов, но при этом возникает проблема выравнивания мощностей в точках приема и децентрализованного распределения кодов [15].

♦ **Использование направленных антенн** в МР увеличивает пропускную способность радиоканала за счет пространственного разнесения процесса передачи (передачи между соседними узлами не мешают друг другу), а также энергетику (потенциал радиолинии) в отношении получателя. Однако это усложняет решение проблемы скрытого терминала, а также порождает новую, касающуюся определения соседних узлов и их местоположения (направления относительно данного узла). Возможным решением является применение в узлах GPS-приемников и/или периодическая передача каждым узлом сообщений присутствия [16].

♦ **Наличие оборудования позиционирования** позволяет синхронизировать сеть, а также использовать информацию позиционирования для регулировки направленности антенн и/или взаимодействия узлов по регулировке мощности передачи для построения топологии максимальной производительности [17].

♦ **Многоканальные МР** значительно уменьшают вероятность столкновений пакетов для случайных методов, но усложняют решение задачи распределения ресурсов при детерминированных МД [18].

♦ **Приоритетный доступ** для передачи сообщений различного приоритета обеспечивается за счет изменения длительностей интервалов передачи (DIFS и SIFS) и управления окном состязаний [19].

♦ **Передача интегрального трафика** возможна при синхронной организации сети и детерминированных протоколах доступа. Однако существуют решения, позволяющие получать приоритетный доступ к радиоканалу в зависимости от типа передаваемой информации [20].

♦ **Управление скоростью передачи** в радиоканале в зависимости от расстояния между абонентами, мощности передатчика и других параметров физического уровня [22].

Характеристика	Протокол канального уровня			
	IEEE 802.11	HomeRF	HiperLAN 2	Bluetooth
Частота, ГГц	2,4 / 5,1	2,4	5,1	2,4
Расстояние, м	100...1000	50	100...250	10...100
Скорость передачи в канале, Мбит/с	1 / 2 /; 11 / 54	11	54	0,7...1
Метод доступа к каналу	DFWMAC (CSMA/CA)	TDMA / TDD	Polling / TDD	
Тип управления, организация сети	Децентрализованное, все узлы равноправны		Зоновое (кластеризация сети), централизованное управление ресурсами (Master/Slave) в каждой зоне (пикосети)	
Мобильность узлов	Легко реализуется на сетевом уровне		Затруднена, требует перестраивания зон сети	
Пропускная способность сети	Ограничена взаимными помехами и возможными перегрузками		Определяется конфигурацией сети. Время реконфигурации сети значительное	
Возможность волновой передачи	Существует		Затруднена	

♦ *Обеспечение безопасности* на канальном уровне осуществляется аутентификацией и шифрованием. Отметим, что механизмы безопасности, применяемые в проводных и сотовых сетях связи, являются централизованными и поэтому неприемлемы для МР. В целом решение проблемы безопасности передачи информации в МР требует отдельного рассмотрения [22] и выходит за рамки данной статьи.

Анализ методов доступа [3; 4] показал их различную эффективность в зависимости от условий функционирования сети. Например, при малой входной нагрузке наиболее эффективны методы доступа с контролем несущей, при сильной — детерминированные (TDMA) при непременном решении задач временной синхронизации и динамического пространственного распределения слотов между узлами. При генерации злоумышленником ложного трафика эффективны методы случайного доступа типа ALOHA.

Проведенный анализ показал следующее:

1. Эффективность метода доступа в МР зависит не только от входной нагрузки, но и от мобильности узлов, используемого метода маршрутизации и текущей топологии сети.

2. Не существует единого метода доступа (или комбинации метод доступа/метод маршрутизации), обеспечивающего эффективное функционирование сети при различных условиях.

3. Выбор (синтез) необходимого метода доступа нельзя рассматривать изолированно от других уровней эталонной модели взаимодействия открытых систем. Он определяется параметрами МР (размерностью, мобильностью, оснащением узлов оборудованием позиционирования, направленными антеннами), информационной нагрузкой и требованиями к ее передаче, а также принятыми решениями на других уровнях эталонной модели.

4. Для эффективного использования ресурсов сети необходимо предусмотреть возможность применения метаметодов, т. е. совокупности методов доступа в узлах сети. Выбор конкретного метода доступа зависит от текущей цели управления сетью, состояния последней и принятых решений на других уровнях эталонной модели. Для окончательного решения в пользу конкретного МД (при отсутствии полной информации о состоянии сети) целесообразно использовать методы нечеткого ситуационного управления.

#### Литература

1. Chandra A., Gummala V., Limb J. O. *Wireless Medium Access Control Protocols* // *IEEE Communications Survey*, 2000.
2. Бунин С. Г., Войтер А. П. *Вычислительные сети с пакетной радиосвязью*. — К.: Техника, 1989. — 223 с.
3. *Труды института инженеров по электронике и радиотехнике (ТННЭР)*. — 1987. — Т. 75, № 1.
4. Pond L., Li V. *A Distributed Timeslot Assignment Protocol for Mobile Multi-hop Broadcast Packet Radio Networks* // *In Proceedings of MILCOM'89*. — 1989. — Vol. 1. — P. 70–74.
5. Шиллер Й. *Мобильные коммуникации*.: Пер. с англ. — М.: Издат. дом «Вильямс», 2002. — 384 с.
6. Karn P. *MACA — a new channel access method for packet radio* // *ARRL/CRRL Amateur Radio 9<sup>th</sup> Computer Networking Conference*, 1990.

7. Talucci F., Gerla M., Fratta L. *MACA-BI (MACA By Invitation): A Wireless MAC Protocol for High Speed Networking* // *In Proceedings IEEE ICUPC'97*, 1997.

8. Fullmer C., Garcia-Luna-Aceves J.J. *Floor Acquisition Multiple Access (FAMA) for packet radio networks* // *Computer Communication Review*. — 1995. — Vol. 25, no 4.

9. Braghavan, Demers A., Shenker S., Zhang L. *MACAW — A Media Access Protocol for Wireless LAN* // *Proc. ACM SIGCOMM Conference*, 1994. — P. 212–225.

10. Deng J., Haas Z. *Dual Busy Tone Multiple Access (DTBMA): A New Medium Access Control for Packet Radio Networks* // *In Proceedings ICUPC*, 1998.

11. Xu S., Saadawi T. *Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?* // *IEEE Communication Magazine*. — 2001. — Vol. 39, no 6. — P. 130–137.

12. Sihgh S., Ranghavana C.S. *PAMAS — Power Aware Multiple-Access Protocol with Signaling for Ad hoc networks* // *ACM Computer Communication Review*, July 1998.

13. Jung E.-S., Vaidya N.H. *A Power Control MAC Protocol for Ad Hoc Networks* // *In Proceedings of MOBICOM'02*, 2002.

14. Tang K., Gerla M. *Random Access MAC for Efficient Broadcast Support in Ad Hoc Networks* // *In Proceedings WCNC'00*, 2000.

15. Muqattash A., Krunz M. *CDMA-Based MAC Protocol for Wireless Ad Hoc Networks* // *In Proceedings MOBIHOC'03*, 2003.

16. Korakis T., Jakllari G., Tassioulas L. *A MAC protocol for full exploitation of Directional Antennas in Ad-hoc Networks* // *In Proceedings MOBIHOC'03*, 2003. — P. 98–107.

17. Миночкин А. И., Романюк В. А. *Управление топологией мобильной радиосети* // *Зв'язок*. — 2003. — № 2. — С. 28–33.

18. Li J., Haas Z., Sheng M., Chen Y. *Performance Evaluation of Modified IEEE 802.11 MAC for Multi-Chanel Multi-Hop Ad Hoc Networks* // *In Proceedings of AINA'03*, 2003.

19. Pallot X., Miller L. *Implementing Message Priority Policies over an 802.11 Based Mobile Ad Hoc Networks* // *In Proceedings of IEEE MILCOM'01*, 2001.

20. Sheu J.-P., Liu C.-H., Wu S.-L., Tseng Y.-S. *A Priority MAC Protocol to Support Real-time Multimedia Traffic in Ad Hoc Networks* // *In Proceedings EuroWireless'02*, 2002.

21. Holland G., Vaidja H., Bahl P. *A Rate-Adaptive MAC Protocol for Wireless Networks* // *In Proceedings ACM/IEEE MOBICOM'01*, July 2001.

22. Papadimitratos P., Haas Z. J. *Secure Data Transmission in Mobile Ad Hoc Networks* // *In Proceedings Second ACM Workshop on Wireless Security (WiSe'03)*, 2003.

23. Barlett C., Drozda m., Marathe A. *Analysis Interaction Between Networks Protocols, Topology and Traffic in Wireless Radio Networks* // *In Proceedings WCNC'03*, 2003.

24. Миночкин А. И., Романюк В. А. *Протоколы маршрутизации в мобильных радиосетях* // *Зв'язок*. — 2001. — № 1. — С. 31–36.

25. Леоненков А. *Нечеткое моделирование в среде MATLAB и fuzzyTECH*. — Спб.: БХВ-Петербург, 2003. — 736 с.