

# Neighbor Node Discovery

для беспроводной самоорганизующейся  
одноранговой сети типа Ad-hoc

**Обнаружение «соседнего узла» является важным шагом в инициализации беспроводной самоорганизующейся одноранговой сети типа сети Ad-hoc. В статье продемонстрированы и проанализированы несколько вариантов алгоритмов для обнаружения соседних узлов в беспроводных Ad-hoc-сетях.**

**Снехал В. Амбаткар  
(Snehal V. Ambatkar)**

**Правин Кулкарни  
(Pravin Kulkarni)**

**Перевод: Владимир Рентюк**

## Вступление

Беспроводные одноранговые Ad-hoc-сети (сенсорные сети), как правило, не используют какую-либо коммуникационную инфраструктуру и должны настроить себя сами непосредственно сразу после их развертывания. Естественно, что при таком варианте их организации сразу после развертывания каждый отдельный узел сети не имеет информации о других соседних узлах в зоне своей передачи. И для того, чтобы общаться с другими узлами сети, сначала ему требуется обнаружить своих соседей. Обнаружение соседнего узла является первым необходимым шагом в инициализации беспроводной сети, так как знание ближайших One-Hop соседей (One-Hop — буквально: «в пределах одного прыжка») имеет важное значение для протоколов доступа к среде управления, протоколов маршрутизации и эффективной технологии управления алгоритмами, что в сумме позволяет сети работать эффективно и правильно. Neighbor Discovery Node (NND, «обнаружение соседнего узла») представляет собой семейство протоколов, предназначенных для поиска ближайших соседних узлов, и является тем самым первым шагом в инициализации беспроводных сенсорных сетей WSN. Кроме того, информация, полученная с помощью протоколов обнаружения соседних узлов, является чрезвычайно полезной для выполнения дальнейших операций, таких как организация доступа к среде передачи данных, хранилищам информации и маршрутизации.

Существующие протоколы NND могут быть разделены на три категории: детерминированные; многопользовательские протоколы обнаружения соседних узлов; рандомизированные. Детерминированные протоколы обычно используют назначенных лидеров (серверы) для всех передающих узлов, а также используют протоколы обнаружения многопользовательской идентификации соседей на основе их предопределенных аутентичных подписей. По сравнению с первыми двумя категориями,

для организации NND наиболее часто используются рандомизированные протоколы. В рандомизированных протоколах узлы передают сообщения для обнаружения в произвольно выбранные временные интервалы. Это связано с необходимостью уменьшить вероятность столкновения (конфликтов или коллизий) с другими узлами. Так что алгоритмы обнаружения соседнего узла можно разделить на две категории, а именно: рандомизированные (на основе случайной последовательности событий) или детерминированные (на основе заданной последовательности событий).

При использовании рандомизированного алгоритма каждый узел осуществляет передачу в промежутки времени, которые выбраны случайным образом, и он обнаруживает всех имеющихся на данный момент времени своих соседей с некой достаточно высокой степенью вероятности. С другой стороны, при использовании детерминированного алгоритма каждый узел осуществляет передачу в соответствии с заранее определенным графиком (последовательностью), что позволяет ему обнаружить всех своих имеющихся на данный момент времени соседей с вероятностью, равной единице. В распределенных сетях такой детерминизм часто практикуется за счет увеличения времени работы на передачу и, в частном случае, для обнаружения соседних узлов, как правило, требует таких нереалистичных для большинства сетей предположений, как наличие синхронизации и априорное знание числа соседних узлов в своем окружении.

Исходя из вышеизложенного, в данной работе мы будем исследовать исключительно рандомизированные алгоритмы обнаружения соседних узлов (рис. 1–3).

## Мобильный компьютеринг

В сетевой компьютерной технологии под понятием мобильного компьютеринг (mobile computing — буквально «мобильные вычисления»), но в современных условиях этот термин

получил более широкое толкование) подразумевают совершенно разные вычислительные идеи, но в общем виде — это подключение в некоторые периоды времени некоторого числа компьютеров в систему через вид сетевой связи, подобной паутине Интернета.

### Идентификаторы узлов

Мы предполагаем, что все узлы имеют локальные (привязанные к месту расположения) уникальные идентификаторы, т. е. в сети для данного узла нет двух соседей, которые имеют один и тот же идентификатор. Например, идентификатор может быть как MAC-адресом узла, так и привязан к его местоположению.

### Модель радиопередачи

Каждый узел оснащен приемопередатчиком, что позволяет узлу либо передавать, либо получать сообщения, но он не может выполнять обе эти операции одновременно (т. е. используется полудуплексный режим).

### Модель коллизий

В рамках данной статьи мы делаем допущение, что, когда два узла (или более) имеют общий приемник, то при передаче конфликт происходит именно в приемнике. Кроме того, мы предполагаем, что такая коллизия является единственным источником потери пакетов, то есть мы будем игнорировать потери пакетов, возникающие из-за таких эффектов, как экранирование трассы передачи и замирания (фединг), которые имеют место и наблюдаются в любых беспроводных каналах передачи. Такая модель коллизий, пусть и идеализированная, позволит нам получить достаточно глубокое понимание проблемы обнаружения соседних узлов и даст ценную информацию для разработки практических алгоритмов обнаружения соседнего узла.

### Симметричное распределение

Размещение соседних узлов предполагается симметричным, т. е. они имеют одинаковое расстояние от рассматриваемого узла.

## Архитектура мобильного компьютеринга для NND

Типичная сенсорная беспроводная сеть состоит из статических и мобильных узлов. Расположение мобильных узлов будет меняться непрерывно по времени. В результате топология сети не может быть заранее определена. Следовательно, соединения между узлами будет прерываться, а сами узлы — перемещаться за пределы диапазона связи узла. Таким образом, проблема обнаружения соседних узлов — это не что иное, как обнаружение подвижных узлов в пределах дальности охвата связью одного узла. При этом информация о местоположении узлов с течением времени должна соответствующим образом обновляться. Также необходимо учитывать, что получать одновременный доступ к точке целевого назначения для нескольких узлов недопустимо, и в то же время необходимо избегать потери пакетов и ошибок при приеме/передаче.

Одной из самых сложных проблем сетей MANET (Mobile Ad-hoc Network — беспроводные децентрализованные самоорганизующиеся сети,

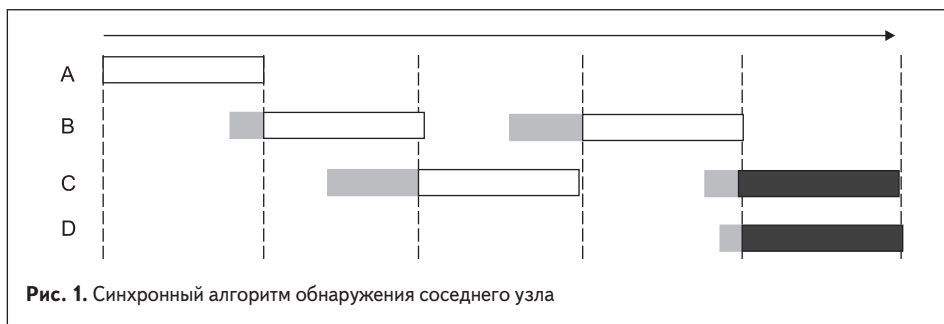


Рис. 1. Синхронный алгоритм обнаружения соседнего узла

состоящие из мобильных устройств), как известно, является проблема наличия так называемых скрытых узлов, которая решается с использованием RTS/CTS-сообщений (Request To Send/Clear To Send — запрос на отправку/разрешение отправки). Однако такое решение не может быть взято на вооружение для устранения аналогичной проблемы в сенсорных сетях. Дело в том, что узлы (станции), которые находятся в сенсорных сетях, являются либо первичными (серверами), либо вторичными (клиентами). В сенсорных сетях включение комбинированных станций является очень дорогостоящим. Сети, в которых узлы не синхронизированы друг с другом, будут иметь частые разъединения, что связано с тем, что из-за динамического поведения узлов информация об их местоположении будет постоянно изменяться, а следовательно, меняться и связи между ними. Но узлы могут эффективно общаться только при наличии стабильной связи между ними. Кроме того, необходимо учитывать, что в большинстве таких сетей источником питания для узлов являются батареи. С практической точки зрения выполнить замену или перезарядку этих батарей очень сложно, так что тут возникают определенные ограничения. То есть энергия, потребляемая узлами, должна использоваться в максимально возможной степени экономно. Потребление мощности, которая используется для связи и обработки сообщений, должно быть сведено к минимуму. С другой стороны, большое количество энергии также потребляется и в то время, когда узлы простаивают в режиме ожидания. Так что в течение периода прослушивания канала связи заряд батареи узла также будет тратиться впустую.

В следующем разделе мы представим на ваш суд наш метод обнаружения соседнего узла, который

позволяет узлу эффективно отслеживать соседей в пределах его коммуникационной досягаемости. Изучение и анализ производительности общих протоколов обнаружения узлов были выполнены в следующем заранее установленном порядке. В ходе анализа мы рассматривали сеть как блок графа, в котором любая пара узлов, которая попадает в область их зоны передачи, считается и принимается как соседние узлы. Снижение общего потребления электроэнергии управляется путем введения значительных изменений в режимы бодрствования и сна узлов. Поскольку рассматриваемая сеть носит динамический характер, то будет предпочтительнее использовать протокол маршрутизации, выполненный на основе административно установленного значения расстояния, назначенного для каждого пути в сети. Это позволит значительно уменьшить конечную задержку и накладные расходы протокола маршрутизации.

### Детерминированный или синхронизированный алгоритм

А. Кешаварзяном (A. Keshavarzian) в статье Energyefficient link assessment wireless sensor networks (IEEE INFOCOM. 2004. Vol. 3) был предложен детерминированный алгоритм обнаружения соседнего узла. Здесь каждый узел передает запрос на обнаружение в соответствии с заранее определенным графиком передачи, что позволяет ему обнаружить всех своих соседей на данный момент времени с вероятностью, равной единице. В распределенных сетях такой детерминизм часто практикуется за счет увеличения времени работы и, в частном случае, для обнаружения соседних узлов, как правило, требует таких нереалистичных предположений, как наличие синхронизации и априорное знание числа соседей в окружении.

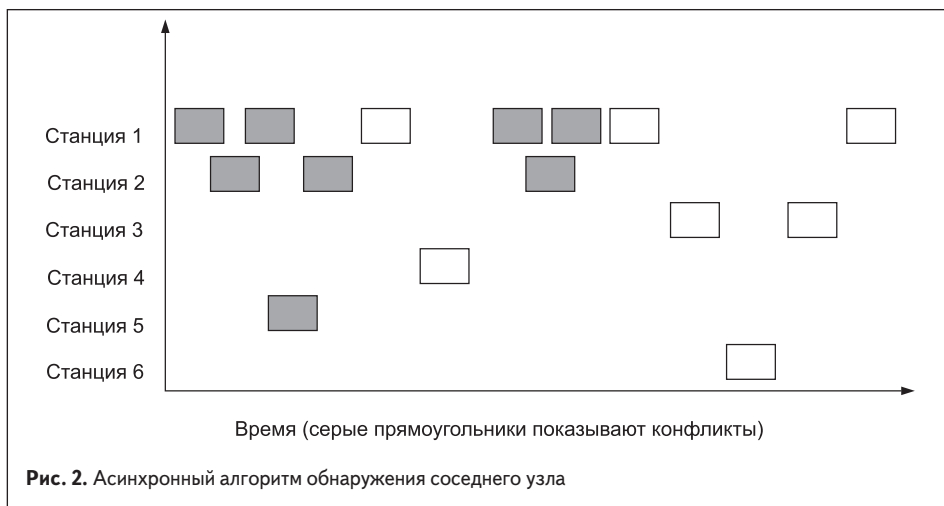


Рис. 2. Асинхронный алгоритм обнаружения соседнего узла

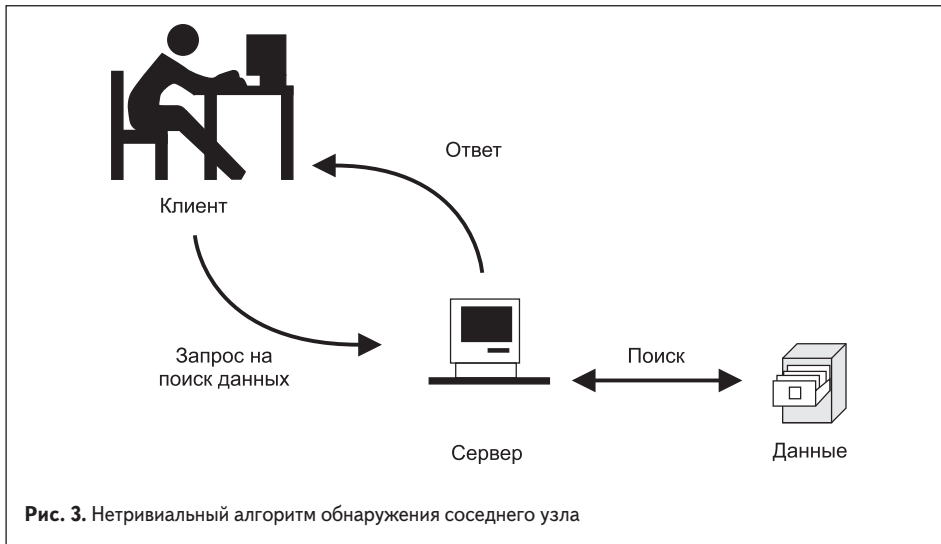


Рис. 3. Нетривиальный алгоритм обнаружения соседнего узла

**Случайный алгоритм**

При использовании рандомизированного алгоритма обнаружения соседнего узла каждый узел осуществляет передачу в промежутки времени, которые выбраны случайным образом, и он обнаруживает всех своих соседей на данный момент времени с некой достаточно высокой степенью вероятности.

Здесь проблема нахождения соседнего узла нетривиальна по нескольким причинам:

1. При обнаружении соседнего узла необходимо решить проблему коллизий в виде столкновений. В идеале алгоритму обнаружения соседнего узла необходимо свести к минимуму вероятность коллизий

и при этом еще свести к минимуму время обнаружения соседних узлов.

2. Во многих практических распределенных сетях узлы не имеют информации о числе соседних узлов, что делает решение проблемы коллизий еще более сложным и трудным.
3. Когда узлы не имеют доступа к глобальным часам, они вынуждены работать в асинхронном режиме, но все еще должны быть в состоянии эффективно обнаруживать свои соседние узлы.
4. В асинхронных системах узлы могут потенциально начать обнаружение соседей в самое разное время и, следовательно, могут пропустить передачу друг друга.

5. Когда число соседних узлов неизвестно, узлы не знают, когда и каким образом прервать и завершить процесс обнаружения соседних узлов.

**Заключение**

Представленные в статье эффективные алгоритмы обнаружения соседнего узла не требуют оценки плотности узлов и позволяют выполнять операции обнаружения асинхронно. Кроме того, алгоритмы позволяют узлам начать выполнение обнаружения в разное время и обнаружить завершение поиска узлов. Наш анализ показывает, что между нижней и верхней границами затрат времени для обнаружения соседей в сетевом пространстве имеется зазор.

Очевидно, что поиски оптимального алгоритма соседнего узла сети остаются интригующей перспективой. Особый интерес представляет вопрос о том, могут ли алгоритмы на основе обратной связи, которые являются оптимальными в случае с одноузловыми (single-hop) сетями, быть расширены для распределенных многоузловых сетей и при этом быть более эффективными, чем Алоха-подобные алгоритмы. Другим направлением для изучения является вопрос расширения различных алгоритмов и их анализа на представленных в данной работе моделях беспроводных каналов, которые включают такие явления, как замирания и экранирование радиосигнала. ■

*Оригинал статьи опубликован в International Journal of Computer Science and Network. 2016. V. 5. www.IJCSN.org.*