Информационные процессы, Том 12, № 3, 2012, стр. 198–212.

ПЕРЕДАЧА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Анализ совместного использования проактивного и реактивного методов распространения сетевой информации в многошаговых беспроводных сетях[1]

А.И. Ляхов, П.О. Некрасов, Д.М. Островский, А.А. Сафонов, Е.М. Хоров

Институт проблем передачи информации им. А.А. Харкевича РАН, Москва, Россия
Поступила в редколлегию 14.08.2012

Аннотация—Ряд протоколов маршрутизации в беспроводных самоорганизующихся сетях выбирают маршруты, основываясь на имеющейся на станции информации о топологии сети, поэтому используемый этими протоколами метод распространения служебной информации значительно влияет на производительность сети в целом. Неудачный выбор метода может привести к большому объему служебного трафика и использованию устаревшей информации. Это снижает производительность сети и не позволяет передавать с требуемым качеством мультимедийные данные реального времени, что является актуальной задачей. В работе предложен новый протокол маршрутизации, использующий совместно проактивный и реактивный методы распространения информации о топологии сети, и показана его эффективность в широком наборе сценариев при доставке мультимедийных данных реального времени.

КЛЮЧЕВЫЕ СЛОВА: маршрутизация, MANET, mesh-сети, качество обслуживания, мультимедийный трафик реального времени.

1. ВВЕДЕНИЕ

Несмотря на то, что децентрализованные сети, или сети класса ad hoc, существуют уже не один десяток лет, интерес к ним исследователей не уменьшается и сегодня. Это обусловлено не только потребностью в сетях, создаваемых при необходимости из равнозначных станций без какой-либо заранее развернутой инфраструктуры, но и новыми задачами, возникшими перед разработчиками таких сетей.

Традиционно используются одношаговые ad hoc сети, в которых каждая станция находится в зоне непосредственного радиоприема всех остальных станций. Для расширения зоны покрытия сети и обеспечения бесперебойной работы движущихся станций были разработаны несколько технологий, позволяющих доставлять пакеты между источником и адресатом не только напрямую, но и через промежуточные станции – ретрансляторы, и, таким образом, превратившие одношаговые ad-hoc сети в многошаговые.

Наибольшее распространение получили следующие технологии.

– Технология mesh-сетей (с маршрутизацией на канальном уровне). На сегодняшний день наиболее проработанными и исследованными являются сети WiFi Mesh на базе стандарта IEEE 802.11s[1].

[1] Работа выполнена в рамках проекта «Методы обеспечения качества обслуживания при доступе к широкополосным мультимедийным услугам в беспроводных самоорганизующихся сетях» в соответствии с грантом Министерства образования и науки России (заявка №2012-1.2.1-12-000-2006-009).

– Технология сетей MANET (с маршрутизацией на сетевом уровне). Хотя стандарты сетей MANET [2] допускают использование различных технологий канального уровня, наибольшее развитие получили сети MANET на базе Wi-Fi [3].

Несмотря на существование различных подходов к созданию многошаговых беспроводных самоорганизующихся сетей, принципы работы и возникающие при использовании этих сетей задачи одинаковы.

Поскольку обе технологии используют Wi-Fi, их применение сопряжено с рядом трудностей, обусловленных особенностями распределенного случайного метода доступа к среде (CSMA/CA). Даже когда все станции находятся в области радиоприема друг друга, этот метод доступа приводит к тому, что две или более станции могут начать передачу пакетов в один и тот же момент времени, в результате чего приемник не в состоянии получить ни один из этих пакетов. В таких случаях говорят, что произошла *коллизия*. Коллизии и шумы в канале делают беспроводную среду ненадежной для передачи данных, поэтому в таких сетях используется механизм повторов пакетов, значительно повышающий вероятность доставки пакета до получателя. Этот механизм применяется только для одноадресной (англ.: unicast) передачи, оставляя широковещательную (англ.: broadcast) передачу ненадежной в сетях WiFi.

В многошаговых сетях вред от коллизий значительно возрастает из-за так называемого эффекта *скрытых* станций. Скрытыми называют такие станции, которые находятся вне зоны радиоприема друг друга, но имеют при этом общую соседнюю станцию (на рис. 1 – это станции A и C). Поскольку A и C не «слышат» радиопередачу друг друга, станция A может начать передачу станции B в то время, когда станция C уже передает B пакет, в результате чего происходит коллизия. Как показано в работах [4, 5], наличие скрытых станций приводит к существенному снижению емкости сети, а в некоторых случаях и к блокировке соединений между станциями, что может привести не только к падению производительности сети, но и к нарушению ее связности.

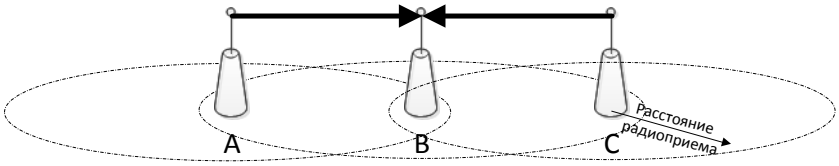

Рис. 1. Скрытые станции в многошаговой сети

Особенность беспроводной среды, заключающаяся в низкой вероятности успешной передачи пакета (в то время как в проводных сетях эта вероятность близка к единице), не позволяет использовать для надежной доставки данных хорошо изученные протоколы маршрутизации, разработанные для проводных сетей. Кроме того, в последние годы разработчики беспроводных сетей сталкиваются с новыми трудностями, связанными с необходимостью обеспечения требуемого качества обслуживания при передаче данных реального времени, что важно, например, для оказания услуги передачи мультимедийной информации, спрос на которую в последние годы значительно увеличился [6]. Это предъявляет новые требования к протоколам маршрутизации и делает проблему надежной доставки мультимедийных данных реального времени в беспроводных сетях актуальной.

Известные протоколы маршрутизации, как правило, включают в себя механизмы, отвечающие за следующие задачи:

– обнаружение соседних станций;
– оценку качества канала между соседними станциями (так или иначе, связанную с определением значения метрики маршрутизации на соединении);
– распространение сетевой информации;
– выбор на основании полученной сетевой информации маршрутов для передачи;
– ретрансляцию пакетов по выбранным маршрутам.

Высокая вероятность потери пакетов при широковещательной передаче делает выбор механизма распространения сетевой информации критическим для функционирования сети, поэтому в данной работе рассматривается именно эта задача.

Сетевая информация может представлять собой:

– *информацию о топологии* (о соединениях с соседними станциями) – в протоколы класса Link-State (англ.: состояние соединения): OLSR [7] (англ.: Optimized Link State Routing Protocol), HSLS [8] (англ.: Hazy-Sighted Link State Routing Protocol), ZRP [9] (англ.: Zone Routing Protocol) и др.;
– *информацию о длинах маршрутов* между всеми возможными парами станций – класс протоколов Distance-Vector: AODV [10] (англ.: Ad hoc On-Demand Distance Vector), DSDV [11] (англ.: Destination-Sequenced Distance Vector) и др.

При использовании протокола класса Link-State каждая станция получает информацию о топологии всей сети и, основываясь на этой информации, строит маршрут. В протоколах класса Distance-Vector поиск маршрута происходит распределенно; тем не менее, они проще в реализации и показывают хорошую эффективность в сетях с малым числом станций. Протоколы класса Link-State, как правило, сложнее, но при этом обладают лучшей масштабируемостью: их эффективность слабее зависит от числа станций, поэтому в крупных сетях чаще всего используются именно они [12].

Сетевая информация может распространяться *проактивно* (регулярно, вне зависимости от существующих потоков данных в сети) и *реактивно* (по запросу). Эффективность того или иного метода распространения сетевой информации существенно зависит от рассматриваемого сценария. Проактивное распространение обеспечивает бóльшую производительность сети в неподвижных сетях при большом числе потоков данных. Реактивное – наоборот, в мобильных сетях с небольшим числом потоков [13].

При создании протокола маршрутизации важно обеспечивать эффективность его работы в широком диапазоне сценариев, поэтому естественно для увеличения области применимости протокола маршрутизации воспользоваться гибридным подходом, суть которого состоит в том, что каждая станция использует информацию, полученную проактивно, пока не обнаружит, что эта информация неверна. Тогда станция запускает реактивный сбор сетевой информации. Такой подход применяется в частности в протоколе HWMP (англ.: Hybrid Wireless Mesh Protocol – гибридный протокол для беспроводных меш-сетей) многошаговых сетей стандарта WiFi Mesh. Протокол HWMP относится к классу Distance-Vector, и согласно стандарту, он предназначен для работы в сетях, в которых число станций не превосходит нескольких десятков. Очевидно, что подобный подход может использоваться и в протоколах класса Link-State, предназначенных для работы в сетях с большим числом станций.

Протоколов класса Link State, которые бы использовали гибридный метод распространения сетевой информации, долгое время не существовало. В [14] предлагается добавить в протокол OLSR механизм реактивного поиска маршрута, который бы позволял получать информацию, необходимую для построения маршрута, в том случае, когда станции недостаточно имеющейся у нее сетевой информации для определения маршрута. Однако предложенный подход не

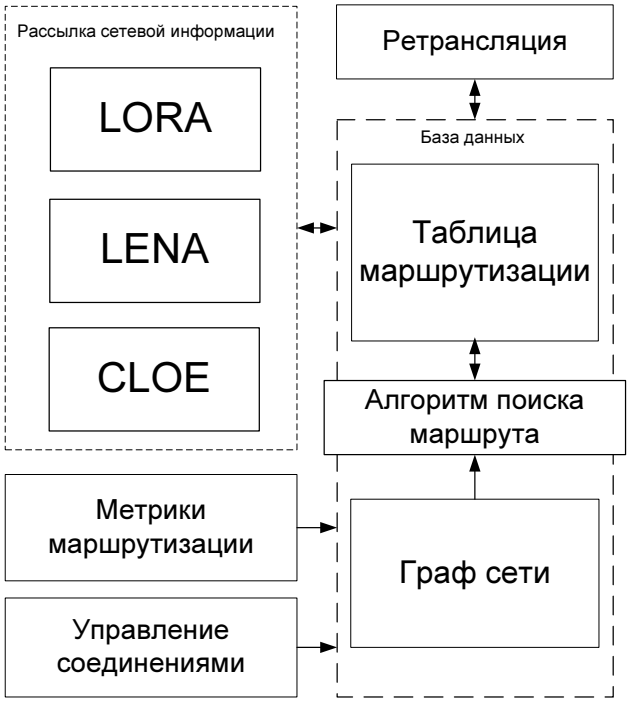

Рис. 2. Структурная схема протокола FRP

позволяет в значительной мере улучшить работу протокола маршрутизации по причинам, изложенным в [15], где исследуются ошибки маршрутизации, возникающие в протоколах класса Link State, на примере протокола OLSR. Авторы показали, что значительная доля таких ошибок связана не с недостатком сетевой информации, а с ее некорректностью (из-за устаревания), поэтому необходимы методы, позволяющие определить, что некоторая информация устарела и должна быть реактивно обновлена.

В данной работе предлагается новый гибридный протокол маршрутизации Flexible Routing Protocol (FRP) класса Link State, в основу которого положен протокол RA-OLSR, описанный в ранних версиях спецификации mesh-сетей IEEE 802.11s, и проводится анализ различных методов распространения сетевой информации, которые могут использоваться в этом протоколе.

2. ПРОТОКОЛ МАРШРУТИЗАЦИИ FRP

Гибридный протокол FRP класса Link-State с пошаговой ретрансляцией работает на канальном уровне, совместим с протоколами стека IEEE 802.11s и может быть использован в качестве замены стандартного для mesh-сетей IEEE 802.11s протокола маршрутизации HWMP.

Приведем упрощенное описание протокола FRP, уделив особое внимание методам распространения сетевой информации.

Протокол состоит из модуля управления соединениями, модуля оценки качества соединений (метрики маршрутизации), модулей распространения информации о соединениях и ошибках маршрутизации [15] (CLOE, LORA и LENA), алгоритмов поиска маршрута и механизма ретрансляции, которые обмениваются информацией посредством базы данных, состоящей из таблицы маршрутизации и *графа сети*, отражающего ее топологию (см. рис. 2). Вершинами графа являются станции сети, а дугами – соединения между станциями сети, причём вес дуг определяется значениями метрики маршрутизации на соединении. В отличие от популярных протоколов маршрутизации, таких как OLSR, HWMP, AODV, DSR и ZRP, протокол может

использовать одновременно несколько метрик маршрутизации, что, как было показано в [16], необходимо для эффективной маршрутизации мультимедийных потоков. Протокол различает потоки, передаваемые между станциями, и выбирает маршруты для каждого потока, исходя из его требований к качеству обслуживания. Для выбора маршрута в простейшем случае может использоваться алгоритм Дейкстры, запускаемый на графе сети. Кроме того, могут применяться и более сложные алгоритмы (см., например, [16]). Найденные маршруты сохраняются в таблице маршрутизации, на основании которой выполняется ретрансляция пакетов.

Каждая запись в таблице маршрутизации (т.е. каждый маршрут) идентифицируется следующей тройкой:

- адрес s станции-источника;
- адрес d станции-адресата;
- категория q трафика, для которой маршрут был построен.

Кроме идентификатора запись содержит поля, описывающие маршрут:

- адрес n следующего ретранслятора маршрута;
- значение m метрики маршрута;
- время t_{inv}, после которого запись становится неактуальной и маршрут должен быть пересчитан;
- время t_{del}, после которого запись должна быть удалена;
- множество P предыдущих ретрансляторов (*предыдущим ретранслятором* в маршруте по отношению к станции X будем называть станцию, которая недавно передавала пакеты трафика категории q с адресом источника s и адресом получателя d станции X).

Назначение этих полей пояснено далее в ходе описания основных механизмов протокола FRP.

Для обнаружения соседей, установления и поддержания соединений с ними FRP использует описанный в спецификации 802.11s [1] протокол PMP (англ.: Peering Management Protocol), или аналогичный ему.

Для каждого открытого соединения между соседними станциями протокол определяет значение метрики маршрутизации (или вектор значений, если используются несколько метрик).

Информация об установленных соединениях и значениях метрик этих соединений может распространяться по сети с помощью проактивного модуля CLOE (англ.: Configurable Link-state prOactive Entity) и реактивных модулей: LENA (англ.: Link Error Notification Add-on) и LORA (англ.: Link-State On demand Routing Add-on).

2.1. Модуль CLOE

Принцип действия проактивной компоненты CLOE заключается в *периодической* широковещательной рассылке по всей сети информации о соединениях между станциями, в результате которой станции получают информацию о топологии сети. Каждая станция с периодом TU_SLOT генерирует широковещательное сообщение TU (англ.: Topology Update), в которое включает адреса соседних станций и значения метрик соединений с ними. Во избежание повторной обработки все сообщения TU последовательно нумеруются. Получив сгенерированное станцией j сообщение TU, не являющееся дубликатом, станция i удаляет из графа сети все дуги, соответствующие соединениям станции j, информация о которых была получена ранее, и добавляет в граф сети дуги, соответствующие соединениям, описанным в полученном TU. Кроме того, станция j ретранслирует сообщение, подчиняясь правилам ретрансляции сообщений TU, описанным ниже.

Правила ретрансляции предназначены для уменьшения объема служебного трафика и основаны на методах MPR (англ.: Multi-Point Relay) и FS (англ.: Fuzzy Sight).

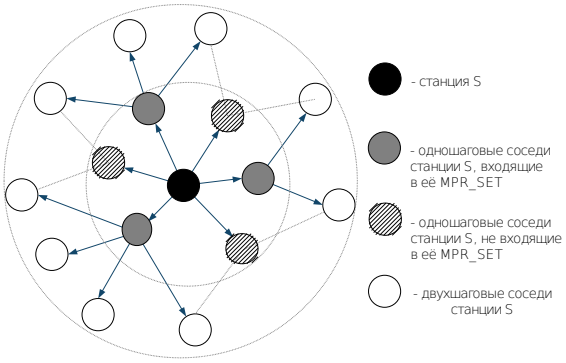

Рис. 3. Пример выбора MPR_SET

Принцип работы метода MPR заключается в уменьшении множества ретрансляторов широковещательных сообщений TU. На основании информации о множестве своих двухшаговых соседей каждая станция выбирает подмножество MPR_SET множества своих одношаговых соседей, т. е. станций, с которыми у нее установлены соединения, таким образом, чтобы каждый двухшаговый сосед данной станции являлся одношаговым соседом по крайней мере одной из станций, включенных в MPR_SET. На рис. 3 проиллюстрирован выбор множества MPR_SET станцией S. Уменьшение интенсивности обмена сетевой информацией достигается благодаря следующему правилу: станция i, получившая сообщение TU от станции j, ретранслирует его в том и только том случае, если i находится в MPR_SET станции j. Как показано в [17], применение этого правила в несколько раз снижает объем трафика при широковещательной рассылке информации.

Построенное подмножество MPR_SET может быть использовано для еще большего снижения объема рассылаемой информации так, как это сделано, например, в протоколе маршрутизации OLSR [18]. В этом протоколе станция i рассылает информацию не обо всех соединениях между собой и соседними станциями, а только о тех соединениях, которые установлены с соседями, поместившими i в свой MPR_SET. Таким образом присходит «прореживание» графа сети; иными словами, в результате рассылки информации о соединениях каждая станция сети получает информацию не обо всем графе сети, а лишь о его подграфе. Доказано [19], что в случае использования единичной метрики маршрутизации (англ. hop count) оптимальный маршрут, построенный на таком подграфе, совпадает с маршрутом, построенном на полном графе сети. Однако для доставки данных с заданным требованием к качеству обслуживания знания о подграфе сети недостаточно: при «прореживании» из графа, как правило, удаляются соединения между близко расположенными станциями. Таким образом, в нем остаются только соединения с низкой вероятностью успешной передачи по ним. Поэтому в протоколе FRP «прореживание» графа сети не используется и станции включают в генерируемые TU-сообщения информацию о соединениях со *всеми* своими соседями.

В основе метода FS лежит идея о том, что сообщение TU с сетевой информацией может рассылаться не по всей сети, а только по некоторой окрестности станции-источника TU. Радиус этой окрестности задается значением в поле TTL (англ.: Time To Live) заголовка сообщения. При каждой ретрансляции сообщения значение в поле TTL уменьшается на 1. Если оно равно 0, то пакет не ретранслируется. Так как окрестность бóльшего радиуса включает окрестность

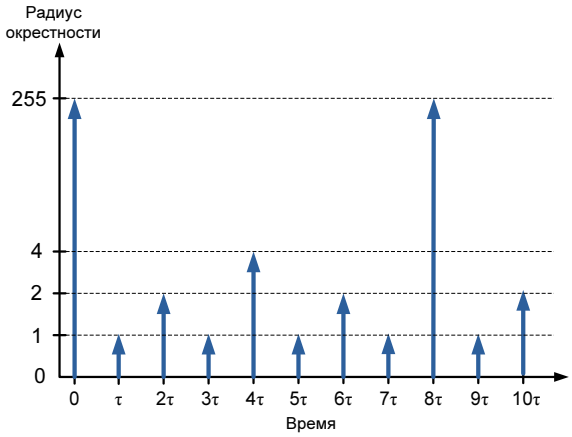

Рис. 4. Пример выбора радиуса области распространения сетевой информации в методе FS

меньшего радиуса, то, периодически меняя значение радиуса рассылки, станция рассылает маршрутную информацию ближним станциям чаще, чем дальним.

Очевидно, что описанный метод снижает объем служебной информации и одновременно с этим уменьшает знания станций о топологии сети. Однако неточность сведений о дальних станциях не является критичной. Поскольку ретрансляция выполняется пошагово, источнику достаточно лишь верно указать направление, в котором следует передавать пакет. Следующий ретранслятор, владеющий более точными сведениями о топологии сети в окрестности адресата, сможет скорректировать маршрут.

Формально правило выбора радиуса окрестности рассылки можно записать следующим образом. Пусть всего используется ρ радиусов рассылки. Обозначим множество радиусов окрестности рассылки как $\{r_n\}$, $n = \overline{1,\rho}$. Каждая станция регулярно через интервал τ рассылает сообщения с сетевой информацией, причем радиус изменяется циклически с длительностью цикла T, значение которой в протоколе принято равным $2^{\rho-1}\tau$.

В начале каждого цикла, т.е. в момент $t = 0$, информация рассылается по всей сети: $r(0) = r_\rho = \infty$ (на практике вместо ∞ используется достаточно большое число, заведомо превышающее возможный диаметр сети). В остальные моменты времени радиус выбирается следующим образом (см. рис. 4).

Пусть $i > 0$ – порядковый номер рассылки сетевой информации после начала последней рассылки по всей сети. Если $\exists n \in \mathbb{N}$ такое что $i = 2^{n-1}$, то радиус окрестности текущей рассылки i равен $r(i) = r_n$ (значение r_n определено ниже). Если $\nexists n \in \mathbb{N}$ такого, что $i = 2^{n-1}$, то определяется такое неотрицательное целое j, что $2^j < i < 2^{j+1}$, и радиус окрестности текущей рассылки выбирается равным $r(i) = r(i-2^j)$, где $r(i-2^j)$ определяется аналогичным образом.

Для значений радиусов окрестностей рассылок r_n ($n = \overline{1,\rho}$) в [8] найдены оптимальные значения:

$$r_n = \begin{cases} 2^n, & n = \overline{1,\rho-1}, \\ \infty, & n = \rho, \end{cases}$$

которые используются в работе. На рис. 4 проиллюстрирован пример выбора значений r_n, в котором $\rho = 4$ и $r_\rho = 255$.

Главной проблемой проактивного распространения является несвоевременное оповещение станций об изменении топологии в мобильных сетях, что приводит к неправильному пред-

ставлению станцией топологии сети и, как следствие, неправильно построенным маршрутам. Увеличение частоты рассылки сетевой информации может помочь решить эту проблему, однако приводит к росту объема служебного трафика, что сильно снижает пропускную способность сети, поэтому в протоколе FRP данная проблема решается иначе: используются модули LENA для обнаружения ошибок в построенных маршрутах и LORA для реактивного поиска маршрута.

2.2. Модуль LENA

Модуль LENA используется для оповещения ретрансляторов маршрута о возникновении следующих ошибок:

- закрытие соединения, являющегося составной частью актуального маршрута,
- возникновение цикла в актуальном маршруте, который детектируется при получении станцией пакета, который был уже ретранслирован ею ранее,
- невозможность построения маршрута.

Опишем работу модуля LENA более подробно.

Станция i, закрыв соединение с соседом j, обновляет граф сети, удаляя из него закрытое соединение.

После этого определяется множество R записей таблицы ретрансляции, у которых в поле n (адрес следующего ретранслятора) указан адрес станции j. Эти записи соответствуют тем маршрутам, которые стали некорректными. Для каждой такой записи станция i, основываясь на обновленном графе сети, осуществляет поиск соответствующего маршрута и, если он был найден, обновляет запись в таблице маршрутизации и удаляет ее из множества R. В результате этих действий в множестве R остаются записи о некорректных маршрутах, исправить которые станция не может исходя из имеющейся у нее информации о сети.

Записи из множества R помечаются как неактуальные по причине закрытия соединения и не используются для ретрансляции пакетов. Если эти записи использовались при ретрансляции пакетов от других источников, необходимо оповестить эти источники об отсутствии маршрута. Для этого станция i формирует сообщение PERR-C (англ.: Path ERRor – link Closed), в котором указываются идентификаторы записей из множества R, а также пара адресов (i, j); при этом адресатами этого сообщения указываются станции из объединения множеств P предыдущих ретрансляторов всех записей из множества R.

Станция, получившая такое сообщение PERR-C, обновляет граф сети, удаляя из него ребро (i, j), и записывает в множество R записи, идентификаторы которых указаны в PERR-C. Дальнейшие действия аналогичны действиям станции i.

При обнаружении цикла в некотором маршруте, исходя из имеющейся информации о топологии сети, станция i выполняет следующие действия. Станция i помечает запись r об этом маршруте в своей таблице маршрутизации как неактуальную по причине возникновения цикла. Затем она формирует сообщение PERR-L (англ.: Path ERRor – Loop), указывая в нем идентификатор записи r, и отправляет его предыдущим ретрансляторам, т.е. тем станциям, адреса которых указаны в множестве P записи r. Станции, получившие PERR-L, также делают запись неактуальной и передают PERR-L своим предыдущим ретрансляторам.

Если станция, получившая для ретрансляции некоторый пакет, не имеет маршрута до адресата этого пакета и не может его определить, исходя из информации в графе сети, она генерирует PERR-L аналогично случаю возникновения цикла.

2.3. Модуль LORA

Станции-источники маршрутов, записи которых помечены как неактуальные по причине перечисленных выше событий, инициируют реактивное распространение сетевой информации, чтобы исправить возникшие ошибки, для чего запускается модуль LORA, принцип работы которого состоит в следующем.

Чтобы инициировать реактивное распространение сетевой информации, необходимой для нахождения маршрута категории q от станции-источника s до адресата d, s формирует широковещательное сообщение PREQ (англ.: Path REQuest), указывая в нем идентификатор запроса и пустые поля, в которые по мере продвижения PREQ от станции к станции добавляются *прямой* и *обратный* пути от источника s до текущего ретранслятора PREQ.

Идентификатор запроса состоит из описанного выше идентификатора (s, d, q) запрашиваемого маршрута и порядкового номера запроса для данного маршрута, который увеличивается на 1 при каждой генерации запроса источником и не меняется в процессе ретрансляции запроса.

В качестве информации о *прямом* и *обратном* пути в PREQ заносятся адреса ретрансляторов данного маршрута и значения метрик маршрутизации для соединений между ними.

Ретрансляция PREQ выполняется по следующим правилам.

Станция, получившая PREQ, заносит в граф сети информацию обо всех соединениях, указанных в этом PREQ. Кроме того, если выполняется одно из условий:

- PREQ с таким идентификатором получен впервые, или
- прямой или обратный путь, указанный в новом PREQ, лучше соответствующего пути, указанного в старых PREQ с таким же идентификатором,

то станция, не являющаяся адресатом, запоминает адрес ретранслятора x, от которого PREQ был получен, и ретранслирует PREQ, включив в него информацию о соединении с x, а станция, являющаяся адресатом, отвечает сообщением PREP (англ.: Path REPly).

Если ни одно из условий не выполнено, то запрос игнорируется и никакие действия не производятся.

PREP ретранслируется к станции-источнику по самому лучшему пути: каждая станция-ретранслятор передает PREP той станции, от которой она получила PREQ с лучшей метрикой. По мере продвижения PREP к источнику в него заносится информация о соединениях лучшего прямого пути.

При ретрансляции сообщений PREQ и PREP содержащаяся в них информация об обратном и прямом пути, соответственно, заносится в таблицу маршрутизации каждого из ретрансляторов. Таким образом, когда PREP дойдет до станции-источниа, на всех станциях-ретрансляторах будут сделаны записи о маршруте до адресата, т.е. маршрут будет построен.

3. МЕТОДИКА ИССЛЕДОВАНИЯ

3.1. Показатель эффективности методов распространения сетевой информации

Для сравнения эффективности методов распространения сетевой информации необходимо определить критерий эффективности, отражающий степень удовлетворенности конечного пользователя качеством оказанной услуги. Поскольку в настоящее время быстрыми темпами растет спрос на широкополосные мультимедийные услуги, свяжем критерий эффективности с качеством передачи мультимедийной информации.

При проведении анализа рассмотрим сеть, нагруженную голосовыми потоками, качество передачи которых традиционно оценивается в соответствии с рекомендацией Международного

союза электросвязи ITU [20] с помощью так называемого R-фактора, зависящего от задержки получения пакета, ее вариации (джиттера) и доли доставленных пакетов, и измеряющегося по шкале от 0 до 100. Считается, что услуга доставки голосового потока оказана, если в течение времени наблюдения значение R-фактора не ниже 50. Разделим время наблюдения на непересекающиеся интервалы длительностью 1 с и для каждого такого интервала измерим значение R-фактора. Назовем *недоступностью NVA услуги доставки голосовых потоков* долю интервалов, на которых значение R-фактора ниже 50, и будем считать NVA показателем эффективности методов распространения сетевой информации: чем меньше NVA, тем метод эффективнее.

3.2. Среда имитационного моделирования

Для исследования различных методов распространения сетевой информации воспользуемся средой имитационного моделирования ns-3 [21], в которой реализуем разработанный протокол FRP.

3.3. Параметризация сценариев

Рассмотрим сеть, состоящую из $N = 50$ станций, и проведем исследование в различных сценариях работы сети, отличающихся мобильностью (скоростью движения станций), плотностью размещения станций, нагрузкой на сеть и значениями параметров протокола FRP.

Пусть станции двигаются согласно модели движения Random 2D Mobility Model [22]. Согласно этой модели, в начале эксперимента станции равномерно размещаются случайным образом внутри квадратной площадки, размеры которой будут определены ниже. Станции равновероятно выбирают направление движения и с заданной скоростью v перемещаются по выбранным прямолинейным траекториям внутри площадки. Достигнув границы площадки, станции равновероятно выбирают новое направление движения.

В работе приводятся результаты для 2 *степеней мобильности*:

- стационарная сеть – $v = 0$ м/с;
- мобильная сеть – $v = 20$ м/с.

Для каждой степени мобильности рассматриваются 2 значения *плотности размещения станций*:

- низкая плотность – размеры квадратной площадки выбираются таким образом, чтобы на площади R_0^2 в среднем находилось 2 станции, где R_0 – радиус уверенного приема – расстояние между двумя станциями, на котором вероятность успешной попытки передачи пакета от одной станции другой больше 0,5.
- высокая плотность – размеры квадратной площадки выбираются таким образом, чтобы на площади R_0^2 в среднем находилось 4 станции.

Сеть нагружается голосовыми потоками, сгенерированными аудио-кодеком G.729 [23]. Потоки имеют длительность 40 секунд и запускаются в случайные моменты времени таким образом, что для любого момента t интервала наблюдения длительностью 4000 с для числа потоков K выполняются соотношения $\lfloor \sigma N \rfloor \le K \le \lceil \sigma N \rceil$ и $\langle K \rangle_t = \sigma N$, где σ – средняя интенсивность трафика (отношение среднего за время наблюдения числа потоков к числу станций N).

Для каждого сценария проведем по 3 эксперимента. В первом эксперименте задействован только модуль CLOE, а модули LENA и LORA выключены. Это соответствует только проактивному распространению сетевой информации. Во втором эксперименте задействованы

Таблица 1. Основные параметры модели

Параметр	Значение
PHY/MAC	IEEE 802.11a
Ширина канала	20 МГц
Радиус R_0 уверенного приема	1125 м
Канальная скорость передачи,	6 Мбит/с
Метрика маршрутизации	Airtime link metric
Период τ генерации информации	1 с
Время устаревания информации о маршруте	16 с

модули LENA и LORA, а модуль CLOE выключен, что отвечает только реактивному распространению сетевой информации. Наконец, в третьем эксперименте задействованы все модули, что соответствует гибридному подходу.

В ходе предварительных экспериментов были установлены значения параметров протокола FRP, при которых только проактивное и только реактивное распространение сетевой информации дает наилучшие результаты в различных сценариях. Эти значения, а также значения основных параметров физического и канального уровней, использованные при моделировании, приведены в табл. 1.

4. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Приведем некоторые результаты имитационного моделирования.

График зависимости недоступности NVA услуги доставки голосовых потоков от интенсивности σ пользовательского трафика для неподвижной сети с низкой плотностью станций изображён на рис. 5а, с высокой плотностью станций – на рис. 5б[1].

Из рис. 5а видно, что в стационарной сети при низкой нагрузке на сеть (например, при $\sigma = 20\%$) реактивный метод распространения информации приводит к меньшей недоступности NVA услуги доставки голосовых потоков (4%), чем проактивный (8%). Это объясняется тем, что даже в случае неподвижных станций качество соединений может меняться со временем; более того, соединения между соседними станциями могут открываться и закрываться, что приводит к отказам маршрутов. Причиной изменения качества соединений являются коллизии, вызванные эффектом скрытых станций, вред от которого тем выше, чем больше нагрузка на сеть. При низком числе потоков реактивный метод распространения сетевой информации сразу же исправляет отказавший маршрут, в то время, как проактивный метод исправляет маршруты со значительной задержкой.

При увеличении числа голосовых потоков растет и объем служебного трафика, сгенерированного модулями реактивного распространения информации. Это еще больше увеличивает нагрузку на сеть и маршруты отказывают настолько часто, что LORA и LENA не успевают их исправить. Интенсивность же служебного трафика при проактивном распространении сетевой информации не зависит от числа потоков. По этим причинам при $\sigma > 20\%$ график $NVA(\sigma)$ на рис. 5а для реактивного распространения сетевой информации резко растет и в точке $\sigma \approx 44\%$ пересекает график $NVA(\sigma)$ для проактивного распространения.

Гибридный способ оказывается эффективней и проактивного, и реактивного распространения сетевой информации. Это обусловлено тем, что реактивные запросы запускаются только тогда, когда маршрут, найденный проактивно, отказал. Таким образом, даже при высокой нагрузке на сеть удается совместить низкий объем служебной информации проактивного метода с быстрым реактивным исправлением отказавших маршрутов.

[1] Число прогонов имитационной модели и длительность экспериментов выбираются таким образом, чтобы относительная ошибка при определении NVA не превосходила 5%.

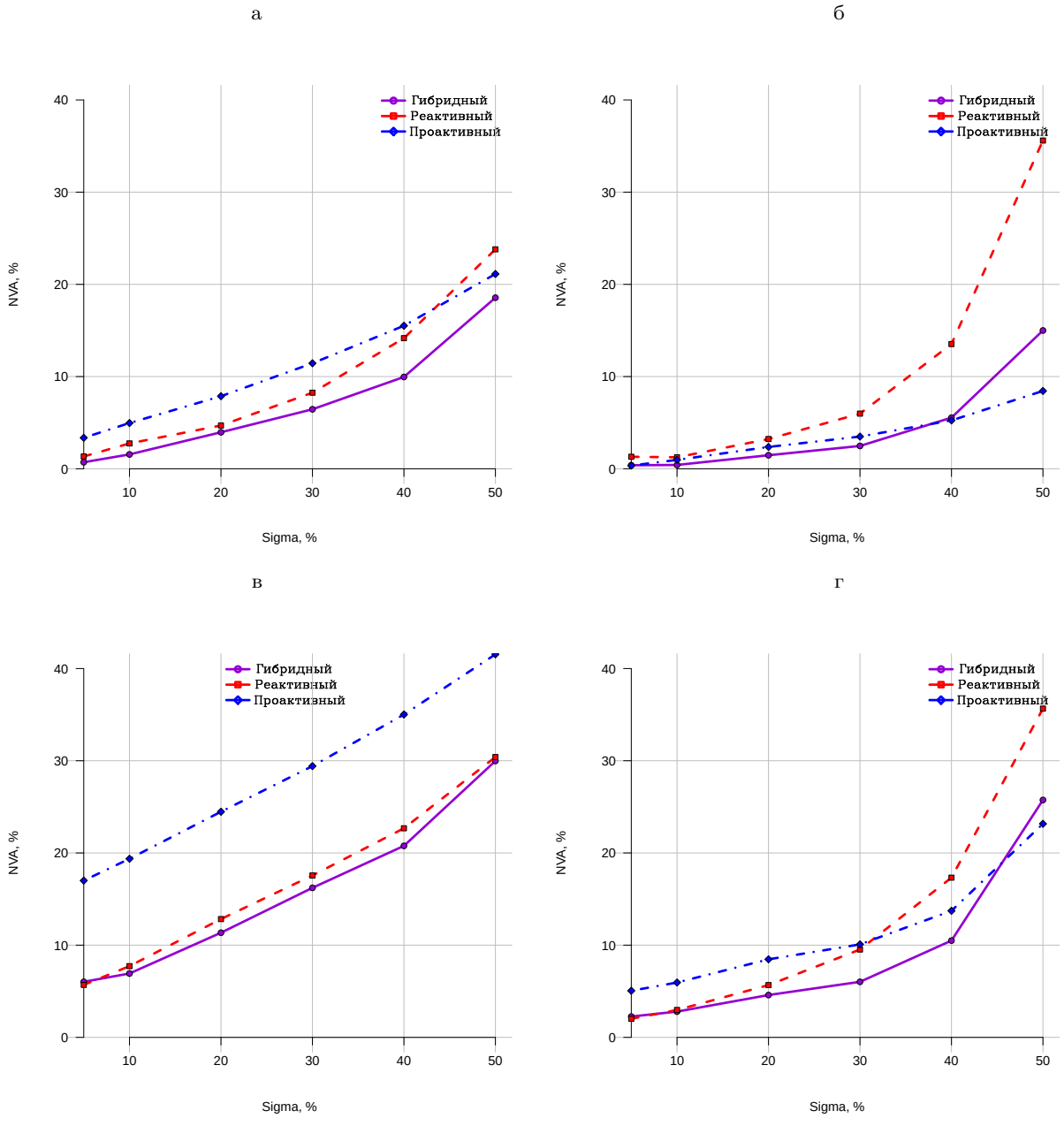

Рис. 5. Графики зависимости NVA от σ при различных методах распространения сетевой информации: а) для стационарной сети с низкой плотностью станций; б) для стационарной сети с высокой плотностью станций; в) для мобильной сети с низкой плотностью станций г) для мобильной сети с высокой плотностью станций.

Аналогичные выводы можно сделать и из рис. 5б, соответствующего стационарной сети с высокой плотностью станций. Однако в этом случае при высокой нагрузке на сеть $\sigma = 50\%$ гибридный метод показывает эффективность ниже, чем проактивный. Причиной этого являются реактивные запросы, интенсивность которых необходимо ограничивать.

В остальных случаях в стационарной сети использование гибридного метода распространения сетевой информации позволяет существенно понизить долю голосовых потоков, переданных с неудовлетворительным качеством обслуживания. Например, для стационарной сети с низкой плотностью при нагрузке $\sigma = 10\%$, гибридный метод обеспечивает $NVA \approx 1,5\%$, а проактивный – только $NVA \approx 5\%$. Иными словами, использование гибридного подхода в 3 раза снижает недоступность услуги доставки голосовых потоков.

Перейдем к исследованию мобильной сети. Для нее характерны постоянные открытия и закрытия соединений. График зависимости недоступности услуги доставки речевой информации для мобильной сети с низкой плотностью станций изображён на рис. 5в, с высокой плотностью станций – на рис. 5г. Видно, что из-за высокой скорости движения станций использование проактивного метода распространения информации приводит к высокой недоступности услуги доставки голосовых потоков: при низкой плотности станций – более 17%. В то же время реактивный метод распространения сетевой информации дает NVA ниже на 10-15%. Примечательно, что использование проактивного метода в дополнение к реактивному позволяет снизить NVA еще на несколько процентов (см. рис. 5в).

Поведение кривых $NVA(\sigma)$, изображенных на рис. 5г, при малых σ объясняются аналогично кривым на рис. 5б, а при больших σ – аналогично кривым на рис. 5в.

Проведенный в этом разделе анализ позволяет сделать вывод о высокой эффективности гибридного метода при передаче голосовых потоков в широком классе сценариев, что говорит о преимуществе данного метода распространения сетевой информации над проактивным и реактивным методами.

5. ВЫВОДЫ

В работе проведён сравнительный анализ проактивного, реактивного и гибридного методов рассылки сетевой информации. Показано, что использование только проактивного способа, как и использование только реактивного способа, эффективно лишь в определенных сценариях: в неподвижных сетях с высокой плотностью станций проактивный способ рассылки показывает высокий результат, в мобильных сетях с низкой плотностью станций реактивный способ эффективнее; при высокой загруженности сети пользовательским трафиком имеет смысл использование проактивного способа, при низкой – реактивного. Всё это говорит о том, что необходимо использовать гибридный способ рассылки сетевой информации, который бы объединял в себе реактивный и проактивный способы. В работе был разработан гибкий протокол маршрутизации, который может работать в различных режимах, в том числе – в режиме с проактивным распространением информацией, с реактивным распространением информации и с гибридным методом распространения сетевой информации. С помощью данного протокола показано, что предложенный гибридный подход эффективен в широком диапазоне сценариев: в сетях с различными плотностями и скоростями движения станций при различной нагрузке на сеть.

Такая универсальность является огромным преимуществом гибридного метода распространения сетевой информации. Будучи не привязанным к определённому классу сценариев, использование протокола маршрутизации с таким методом рассылки позволит добиваться высокого качества обслуживания независимо от условий использования сети, другими словами использование гибридного способа позволяет минимизировать зависимость его эффективности от выбора сценария.

СПИСОК ЛИТЕРАТУРЫ

1. IEEE 802.11s-2011 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 10: Mesh Networking. IEEE, 2007.
2. S. Corson, J. Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETF, January 1999. http://www.ietf.org/rfc/rfc2501.txt
3. IEEE 802.11-2007 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. IEEE, 2007.
4. А.И. Ляхов, И.А. Пустогаров, А.С. Гудилов. Проблема неравномерного распределения пропускной способности канала в сетях IEEE 802.11. Информационные процессы, 2008, т. 8, № 3, сс. 149–167.
5. A. Lyakhov, I. Pustogarov, A. Gudilov. 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, pp. 15–24.
6. Connect to the “Right” Network the “Right” Way – Presentated at AT&T Developer Summit (2011). 5th January 2011.
7. J.P. Macker, J.W. Dean. A study of link state flooding optimizations for scalable wireless networks. Proceedings of Military Communications Conference, (MILCOM 2003). October 2003.
8. C. Santivanez, R. Ramanathan. Hazy Sighted Link State (HSLS) Routing: A Scalable Link State Algorithm. BBN Technologies, 2008. http://www.ir.bbn.com/documents/techmemos/TM1301.pdf
9. Z. J. Haas, M. R. Pearlman, P. Samar. The Zone Routing Protocol (ZRP) for Ad Hoc Networks. IETF, July 2002 (Internet-Draft). http://www.ietf.org/proceedings/02nov/I-D/draft-ietf-manet-zone-zrp-04.txt
10. Ad Hoc On-Demand Distance Vector Routing Protocol. IETF, February 2003 (Internet-Draft). http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-13.txt
11. C. E. Perkins, P. Bhagwat. DSDV Routing over a Multihop Wireless Network of Mobile Computers. Ad Hoc Networking, 2001, ch. 3, pp. 53–74.
12. J. Haerri, F. Filali, C. Bonnet. Performance Comparison of AODV and OLSR in VANETs Urban Environments under Realistic Mobility Patterns. Proceedings of Med-Hoc-Net 2006, the 5th Annual Mediterranean Ad Hoc Networking Workshop. 14 June 2006.
13. A. Huhtonen. Comparing AODV and OLSR Routing Protocols. Presented at Telecommunications Software and Multimedia, 2004, pp. 1–9.
14. J. C. Wang, F. Safaei, M Abolhasan, D R. Franklin. OLSR-R3: Optimized link state routing with reactive route recovery. Proceedings of the 15th Asia-Pacific Conference on Communication (APCC 2009), pp. 359–362.
15. А.Г. Кирьянов, А.А. Сафонов, Е.М. Хоров. Методы исследования переходных характеристик протокола OLSR при включении/выключении узла сети. Труды конференции “Информационные технологии и системы” (ИТиС 2010), сс. 20–29. Геленджик, 2010.
16. E. Khorov, A. Safonov. Multiple metrics in MANET with end-to-end QoS support for unicast and multicast traffic. Proceedings of the Third international conference on Multiple access communications (MACOM-2010), pp. 251–262. Barcelona, Spain.
17. A. Busson, N. Mitton, E. Fleury. An analysis of the Multi-Point Relays selection in OLSR. INRIA, Research report 5468, January 2005.
18. P. Jacquet, T. Clausen. Optimized Link State Routing Protocol (OLSR). IETF, October 2003. http://www.ietf.org/rfc/rfc3626.txt

19. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot. Optimized link state routing protocol for ad hoc networks. Proceedings of Multi Topic Conference, 2001 (IEEE INMIC 2001), pp. 62–68.

20. ITU-T Recommendation G.107: The E-Model – A Computational Model In Use In Transmission Planning. ITU-T, March 2005.

21. The ns-3 network simulator. `http://www.nsnam.org`

22. M Izuan, M Saad, Z. A. Zukarnain. Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol. European Journal of Scientific Research, 2009, vol. 32, no. 4, pp. 444–454.

23. Recommendation G.729 – Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP). ITU-T, January 2007.

A study of a hybrid of reactive and proactive methods of topology information dissemination in wireless ad-hoc networks

E.M. Khorov, A.I. Lyakhov, P.O. Nekrasov, D.M. Ostrovsky, A.A. Safonov

A number of routing protocols for wireless ad-hoc networks select routes according to the network topology information obtained by a station. Thus, methods of routing information dissemination used by these protocols have a great impact on network performance. Bad choice of the method may lead to high overhead as well as the usage of outdated routing information. Both factors degrade network performance and do not allow to meet QoS requirements while transmitting multimedia real-time data streams which is in high demand. In this paper, we propose a novel routing protocol combining reactive and proactive methods of topology information dissemenation. Then we show its efficiency in a vast set of scenarios while transmitting multimedia real-time data.

KEYWORDS: wireless, ad-hoc, routing, QoS, hybrid method of network information dissemination, flexible routing protocol.