

Анализ эффективности метода доступа к каналу в сетях LoRaWAN*

Бабаев А.А., Банков Д.В., Хоров Е.М.

ИППИ РАН

babaev@phystech.edu, bankov@iitp.ru, khorov@iitp.ru

Аннотация

Недавно возникшая технология LoRa быстро приобретает репутацию перспективного решения для построения LPWAN-сетей. Данная технология использует протокол канального уровня LoRaWAN. Этот протокол ориентирован на передачу данных в беспроводных сенсорных сетях, с акцентом на низкое энергопотребление и на простоту конечных устройств. В данной работе исследуется метод доступа к каналу, описанный в стандарте LoRaWAN, указываются неточности в его описании и при помощи имитационного моделирования исследуется его производительность. Результаты моделирования показывают, что использование параметров, принятых в стандарте по умолчанию, приводит к тому, что сеть не способна обслужить даже несколько десятков активных устройств, подключенных к одному шлюзу. В работе также предлагаются возможные пути для улучшения производительности метода доступа к каналу.

1. Введение

Концепция Интернета вещей (англ. Internet of Things) давно интересует исследователей сетевых протоколов и производителей телекоммуникационного оборудования, и специалисты всё ближе подходят к её претворению в жизнь. Уже есть множество решений, позволяющих видеть эту концепцию в действии. Крупную нишу в реализации концепции Интернета вещей заняли LPWAN-технологии (англ. Low Power Wide-Area Network — энергоэффективная сеть дальнего радиуса действия), принцип которых заложен в следующем: при малой мощности устройство может производить передачу на большие расстояния, имея при этом существенные ограничения на скорость передачи. Упомянутые очевидные достоинства и недостатки LPWAN-технологий делают их перспективными для реализации сенсор-

ных сетей, в которых большое количество автономных устройств-сенсоров должны редко передавать небольшие порции данных. Уже существуют компании-производители готовых решений для промышленности и бизнеса на основе LPWAN-технологий, такие как LoRa [1], SIGFOX [2] и СТРИЖ [3], которые по праву первенства занимают ещё ненасыщенный рынок устройств и сервисов Интернета вещей.

Технология LoRa, о которой пойдёт речь в данной работе, основана на протоколе MAC-уровня LoRaWAN [4], разработанного специально для LPWAN-сетей. В протоколе LoRaWAN учтены особенности беспроводных сенсорных сетей, и общение между устройствами построено таким образом, чтобы автономные устройства тратили как можно меньше энергии на передачу данных. Экономия энергии достигается за счёт простоты протокола доступа к среде, который подобен неслотированной многоканальной системе АЛОХА [5].

Однако излишняя простота технологии может сильно ухудшить технические показатели сети, построенной на её основе. Пока не наблюдается повсеместное развёртывание сетей на основе LoRaWAN, и хотя по заявлениям производителей технология вполне работоспособна, неизвестно, может ли данная технология справиться с заявленной целью, а именно — с поддержкой большого числа устройств. Не меньший интерес представляет собой вопрос: каков предел возможностей данной технологии в терминах максимальной нагрузки на сеть и максимального числа станций, одновременно передающих свои данные?

В данной работе проведён анализ метода доступа к каналу для сети LoRaWAN и показано, что использование параметров протокола, заданных по умолчанию, приводит к неэффективному использованию канала, и что устройства, работающие по протоколу LoRaWAN, нуждаются в дополнительной настройке.

Дальнейшее изложение построено следующим образом. В разделе 2 описан метод доступа к каналу в сетях LoRaWAN, приведён исследуемый сценарий, и дана формальная постановка задачи. В разделе 3 приведён обзор литературы по теме работы. В разде-

*Исследование выполнено при финансовой поддержке РФФИ и Правительства Москвы в рамках научного проекта № 15-37-70004 мол_а_мос.

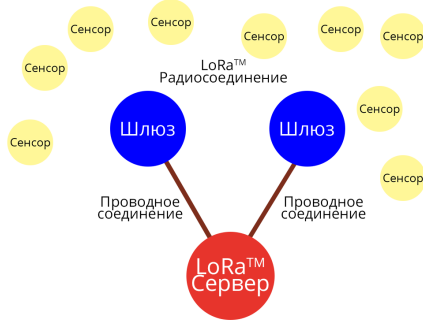


Рис. 1. Архитектура сети LoRaWAN

ле 4 представлен анализ процесса передачи данных в сети LoRaWAN. В разделе 5 показаны результаты имитационного моделирования сети. Раздел 6 содержит заключение и завершает работу.

2. Сценарий и постановка задачи

Сеть LoRaWAN имеет топологию «звезда» и состоит из сервера, к которому через (преимущественно проводную) IP-сеть подключены шлюзы, а к ним в свою очередь по беспроводному одношаговому соединению подключены сенсоры (см. рис. 1). Сервер собирает данные с сенсоров, а шлюзы играют роль ретрансляторов. В стандарте LoRaWAN описано три режима работы устройств: А, В и С, где А — стандартный режим работы, который организует передачу данных от сенсоров к шлюзу методом случайного доступа к каналу и должен быть реализован во всех сенсорах. Режим работы В предназначен для организации передачи данных от шлюза к сенсорам методом детерминированного доступа с периодической рассылкой расписаний. Режим работы С описывает работу устройств, не нуждающихся в экономии энергии, которые могут постоянно прослушивать канал. В этой работе исследуется взаимодействие устройств, работающих только в режиме работы А.

Устройства LoRaWAN могут работать в различных регионально-зависимых частотных диапазонах. Для примера будем рассматривать диапазон EU 869-870MHz ISM Band. При использовании данного диапазона устройства работают в нескольких частотных каналах (назовём их *основными* каналами), каждый из которых имеет ширину 125 кГц. Когда сенсор имеет данные на передачу, он выбирает случайным образом (равновероятно) канал, и в данном канале передаёт шлюзу кадр с данными (см. рис. 2). Спустя интервал времени T_1 сенсор слушает канал, в котором передавались данные, и в это время шлюз должен ответить сенсором кадром, в котором установлен флаг подтверждения.

Также, спустя интервал времени T_2 после приёма

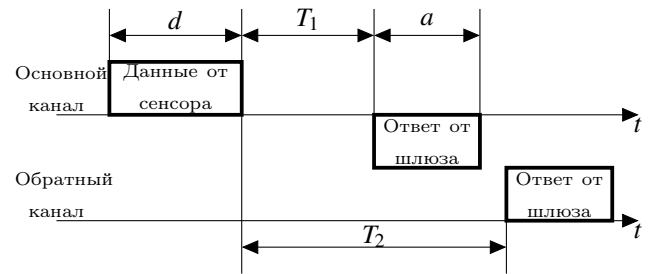


Рис. 2. Процесс передачи данных в сети LoRaWAN

кадра, шлюз должен передать сенсором кадр с подтверждением в специально указанном канале (назовём его *обратным* каналом). Сенсор должен прослушивать обратный канал, только если он не получил первое подтверждение. Получив хотя бы одно подтверждение, сенсор считает кадр успешно переданным.

В противном случае, прождав случайный интервал времени после того момента, когда должно было прийти второе подтверждение, сенсор делает новую попытку передачи по случайно выбранному основному каналу. Сенсор может начать новую передачу кадра только тогда, когда он успешно принял хотя бы одно подтверждение или когда истекло время передачи второго подтверждения.

Если два сенсора передают в пересекающиеся промежутки времени в одном канале с использованием одинаковой сигнально-кодовой конструкции, на принимающем шлюзе, если исключить эффект захвата канала, произойдёт коллизия кадров, и передача обоих сенсоров будет unsuccessful.

Рассмотрим сеть LoRa, в которой группа сенсоров подключена к одному шлюзу. Пусть на каждый сенсор данные на передачу поступают через экспоненциально-распределённый интервал времени после окончания предыдущей передачи. Передача данных ведётся по F основным каналам и одному обратному каналу. Все сенсоры передают кадры длины d , а шлюз отвечает им кадрами длины $a \leq d$.

Определим нагрузку на сеть как суммарную интенсивность передач кадров (включая ретрансмиссии), умноженную на длительность кадра. Исследуем, каким образом нагрузка на сеть связана с пропускной способностью сети, и как эта связь меняется с количеством станций и соотношением длины кадра к длине подтверждения.

3. Обзор литературы

LPWAN-технологии начали своё распространение совсем недавно, поэтому пока что существует очень мало работ, посвящённых их исследованию. Известны обзорные статьи [6] и [7], в которых про-

дится описание существующих на современном рынке LPWAN-технологий и их последующее сравнение без глубоких исследований их технических характеристик. В этих статьях содержится исключительно ознакомительный материал, который даёт понять, что такое Интернет вещей, и какие технологии используются для реализации сценариев Интернета вещей.

Пример аналитического моделирования LPWAN-сети можно найти в работе [8], где исследуется популярная LPWAN-технология — SIGFOX. Цель данной работы — найти оптимальное ограничение на число повторных передач для наиболее эффективной работы технологии. Данная работа является хорошим примером того, насколько примитивные решения для протоколов MAC-уровня используются в доступных на рынке LPWAN-технологиях.

В этой статье делаются первые шаги к изучению нового популярного решения в сфере Интернета вещей — LoRa, протокол MAC-уровня которой, как показывают результаты моделирования, при некорректной настройке (в частности, при использовании параметров, рекомендованных в стандарте) работает крайне неэффективно даже в случае, когда к шлюзу нужно подключать несколько десятков сенсоров.

4. Анализ

Прежде чем приступить к моделированию, рассмотрим некоторые неточности и недосказанности, которые можно заметить при внимательном изучении спецификации LoRaWAN. Спецификация в описании метода доступа к каналу лишь указывает, что после передачи кадра сенсор должен прослушивать канал в конкретные интервалы времени для получения подтверждения, и что шлюз должен отправить сенсор подтверждение в основном и в обратном каналах.

Возможна ситуация, когда два сенсора успешно отправили кадры в различных каналах в пересекающиеся интервалы времени. Шлюз может отправить этим сенсорам подтверждения в соответствующих каналах, однако подтверждение в обратном канале он может отправить только на один кадр. Будем считать, что в таком случае шлюз отправит в обратном канале подтверждение на самый ранний кадр.

4.1. Запрет на отправку подтверждений

Шлюз параллельно прослушивает основные каналы, ожидая отправку кадров от сенсоров. Получив кадр, шлюз должен через T_1 отправить подтверждение в канале, в котором передавался кадр. Но в спецификации не сказано, должен ли шлюз прослушивать канал в течение времени T_1 . Также в спе-

цификации не отмечено, что должен делать шлюз в случае, если в течение времени T_1 после приёма кадра в этом канале началась передача ещё одного кадра от другого сенсора. Должен ли шлюз отменить ожидаемую передачу подтверждения и принять новый кадр? С одной стороны, если шлюз запретит передачу такого подтверждения, то система будет лучше работать, поскольку таким образом можно будет избежать коллизии кадров лишь ценой потери одного подтверждения. Но с другой стороны, это повысит нагрузку на обратный канал, так как там будут отправляться подтверждения на все кадры. В данной работе приведены результаты моделирования для двух вариантов протоколов: в котором шлюз отменяет передачу подтверждения, и в котором шлюз передаёт подтверждение несмотря на передачу данных.

4.2. Выбор T_1

Интервал T_1 по умолчанию равен 1 с. Он должен быть достаточно большим, поскольку сенсоры нужно успеть переключиться с режима передачи на режим приёма. Вероятно, минимизировав T_1 можно увеличить пропускную способность сети, т.к. устройства будут тратить меньше времени на ожидание подтверждения. А с другой стороны, при рекомендованном в спецификации значении T_1 в период разрешения коллизии кадры могут вступать в коллизию не только друг с другом, но и с подтверждениями. Для избежания коллизии подтверждения с кадром нужно устанавливать T_1 большим, чем ширина интервала, из которого выбирается случайная отсрочка. Поэтому в данной работе разобраны предельные случаи $T_1 = 0$ и случай $T_1 = 3$ с.

4.3. «Снежный ком»

В спецификации указано, что после неуспешной передачи кадра сенсор должен сделать новую попытку передачи, прождав случайное время из множества 1, 2 и 3 с. При передаче с использованием самой надёжной сигнально-кодировой конструкции, длительность кадра данных варьируется от 0.4 с до 2.3 с в зависимости от размера полезной нагрузки. Для анализа, без ограничения общности будем считать, что длительность кадра данных $d = 1$ с, а длительность подтверждения равна $a = 0.5$ с.

Рассмотрим случай, когда имеется только один основной канал. Предположим, что две станции попали в коллизию так, что кадр от первой станции был отправлен на время $\tau \in (0, 1)$ с после кадра второй станции (см. рис. 3). Спустя $d + a + T_2$ каждый сенсор выберет случайное время, прождав которое будет сделана новая попытка передачи. Пусть b_1 — выбор первого сенсора, а b_2 — выбор второго сенсо-

ра. Тогда сенсоры, находившиеся в коллизии, успешно передадут данные при повторной попытке лишь при следующих значениях случайных чисел:

1. $b_1 = 3$ с, $b_2 = 1$ с;
2. $b_1 = 3$ с, $b_2 = 2$ с;
3. $b_1 = 2$ с, $b_2 = 1$ с;
4. $b_1 = 1$ с, $b_2 = 3$ с;

причём в зависимости от того, есть ли запрет на отправку подтверждений, кадр, передающийся позже, может вступить в коллизии с подтверждением на более раннюю передачу кадра данных.

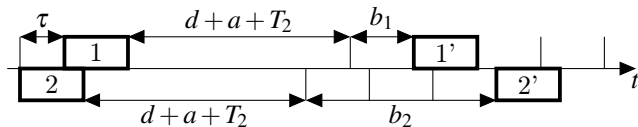


Рис. 3. Успешное разрешение коллизии в случае $b_1 = 1$ с, $b_2 = 3$ с

Значит, вероятность того, что сенсоры разрешат коллизии, меньше $\frac{4}{9}$, поскольку заново отправленные кадры могут войти в коллизии с кадрами, отправленными от других сенсоров. Такая маленькая вероятность разрешения коллизий является причиной возникновения явления «снежного кома», когда два кадра, попав в коллизии, после повторной передачи уведут в коллизии другие кадры, отправленные с остальных сенсоров. В результате сеть может успешно работать лишь при низкой входной нагрузке, так как иначе сенсоры постоянно находятся в состоянии разрешения коллизии, из-за чего растёт задержка при передаче данных.

Увеличение числа основных каналов с точки зрения разрешения коллизий эквивалентно увеличению интервала, из которого выбирается случайная отсрочка. Однако когда число каналов и интервал фиксированны, при большом числе станций вероятность разрешения коллизий всё-равно мала и избежать «снежного кома» нельзя. Правильным решением в данном случае является адаптивный подбор ширины интервала в соответствии с количеством передающих сенсоров, например, так, как это сделано в сетях Wi-Fi: сенсоры при каждой повторной коллизии удваивают интервал, из которого выбирают случайную отсрочку для повторной передачи, и сбрасывают ширину интервала в минимум после успешной попытки. Такое решение позволяет адаптивно для любого числа станций подобрать ширину интервала и намного быстрее разрешать коллизии, чем в случае, когда интервал фиксирован. Для иллюстрации эффективности данного решения, в разделе 5 приведены результаты моделирования сети LoRaWAN

для случая, когда сенсоры при коллизии выбирают отсрочку в экспоненциально растущем интервале. А именно, если раньше отсрочка всегда выбиралась из множества $\{1, 2, 3\}$ с, то в случае экспоненциального роста интервала отсрочки после каждой неудачной попытки передачи множество удваивается, и отсрочка выбирается уже из множества $\{1 \dots 6\}$ с, после второй неудачной попытки — из множества $\{1 \dots 12\}$ с, и т.д. до тех пор, пока передача не будет совершена, что вернёт множество в исходное состояние, и для следующего кадра в случае неудачной попытки передачи отсрочка будет выбираться из множества $\{1, 2, 3\}$ с.

5. Численные результаты

Проведём имитационное моделирование сети LoRaWAN для различного числа сенсоров, при этом используя временные параметры, предложенные в спецификации. Пусть параметры метода доступа настроены так, как рекомендовано в спецификации LoRaWAN. Рекомендуемые значения для интервалов между кадром и подтверждениями следующие: $T_1 = 1$ с и $T_2 = 2$ с. Число основных каналов $F = 3$. Рассмотрим подтверждения длиной $a = 0.5$ с, а длительность кадров от сенсоров — $d = \{0.5, 1, 2\}$ с. Рассмотрим случай, когда все сенсоры передают с использованием самой надёжной сигнально-кодировой конструкции DR0.

Результаты для случая, когда плюз не отправляет подтверждение, если оно пересечётся с начавшейся передачей кадра сенсором, представлены на рис. 4, 5, 6. На графиках показана зависимость нагрузки от пропускной способности сети (показана ветвь графика, которая соответствует устойчивому режиму работы). При низкой нагрузке графики для различного количества станций совпадают, что означает, что передачи кадров преимущественно успешны с первой попытки. При увеличении нагрузки пропускная способность растёт медленнее нагрузки и достигает своего максимального значения, которое тем больше, чем меньше количество подключённых к сети сенсоров. При дальнейшем увеличении нагрузки сеть становится неустойчивой, станции постоянно попадают в коллизии, пропускная способность падает, а длина очереди на передачу у станций стремится к бесконечности. Заметно, что максимальная нагрузка, соответствующая устойчивому режиму работы сети, тем меньше, чем больше число станций, так как с увеличением числа станций вероятность попасть в коллизии растёт.

Увеличение длительности кадра по отношению к длительности подтверждения даёт двойной результат. Для маленького числа станций, когда вероятность разрешения коллизии высока, максимальная пропускная способность сети растёт,

так как доля канальных ресурсов, потребляемых

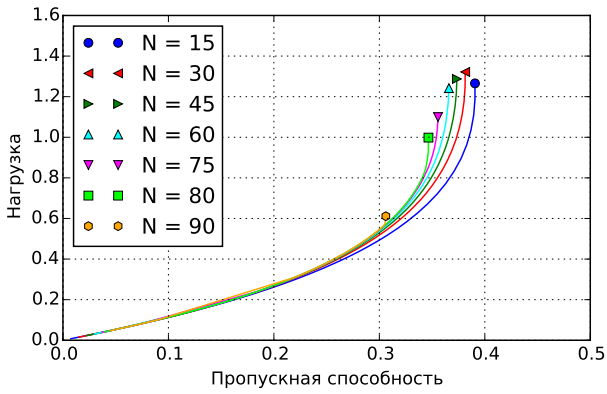


Рис. 4. Зависимость нагрузки от пропускной способности сети в случае $\frac{d}{a} = 1$

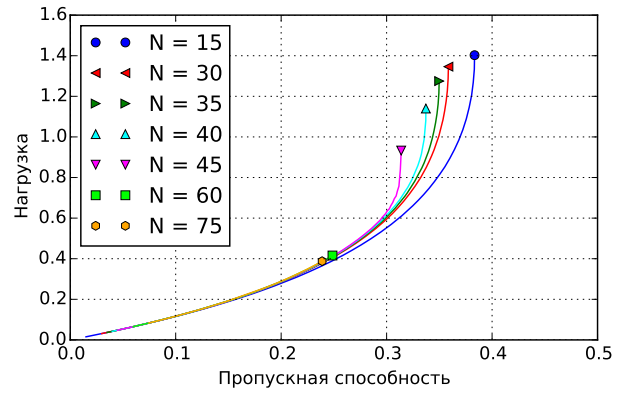


Рис. 7. Зависимость нагрузки от пропускной способности сети в случае $\frac{d}{a} = 2$, когда шлюз передаёт подтверждения несмотря на передачу кадра

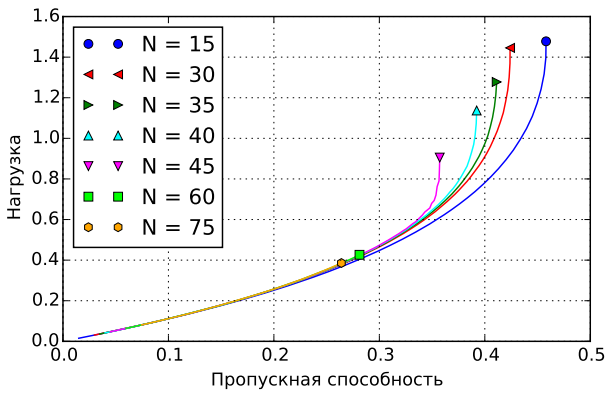


Рис. 5. Зависимость нагрузки от пропускной способности сети в случае $\frac{d}{a} = 2$

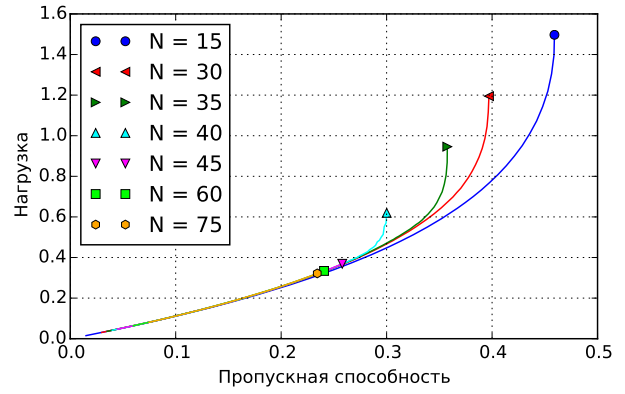


Рис. 8. Зависимость нагрузки от пропускной способности сети в случае $\frac{d}{a} = 2$ и $T_1 = 0$ с

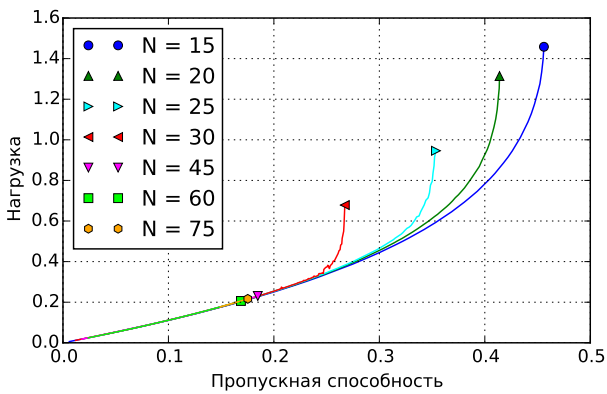


Рис. 6. Зависимость нагрузки от пропускной способности сети в случае $\frac{d}{a} = 4$

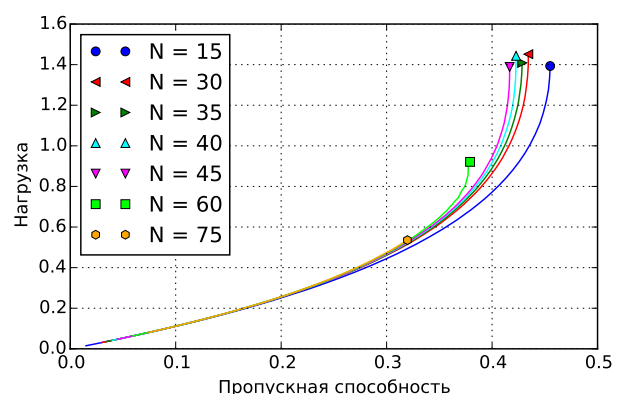


Рис. 9. Зависимость нагрузки от пропускной способности сети в случае $\frac{d}{a} = 2$ и $T_1 = 3$ с

подтверждениями, уменьшается. Для большого числа станций наблюдается противоположный эффект. Более длительные кадры приводят к высокой вероятности коллизии (как первой, так и повторной), из-за чего «снежный ком» образуется при меньших нагрузках.

На рис. 7 представлена зависимость нагрузки от пропускной способности для случая, когда шлюз не отменяет передачу подтверждения, если оно может пересечься с передачей кадра данных сенсором. Как видно, в таком случае пропускная способность падает примерно на 10% из-за коллизий подтверждений и кадров с данными.

На рис. 8 представлена зависимость нагрузки от пропускной способности для случая, когда задержка между отправкой кадра и соответствующим подтверждением минимальна. В случае, когда $T_1 = 0$ с, максимальная пропускная способность сети уменьшается, так как шлюз сразу же посылает подтверждение и не может отменить его для избежания коллизии с другим кадром данных. В результате происходит больше коллизий подтверждений с кадрами данных, чем при $T_1 = 1$ с.

Как показывают результаты моделирования, повторные коллизии оказывают существенный вклад в пропускную способность. Как и предполагалось, уменьшить вероятность повторной коллизии можно, установив T_1 больше ширины интервала, в котором выбирается случайный счётчик отсрочки, что подтверждается зависимостью, представленной на рис. 9. Увеличение T_1 приводит к увеличению пропускной способности и позволяет поддерживать большее количество активных сенсоров, избегая эффекта «снежного кома». Однако при достаточно большом числе станций это решение тоже оказывается неэффективным.

Все описанные до сих пор изменения приводят к незначительному увеличению пропускной способности. Рассмотрим следующее решение. На рис. 10 представлена зависимость нагрузки от пропускной способности для случая экспоненциально-растущего интервала отсрочки, описанного в подразделе 4.3. Такое решение позволяет адаптивно для любого числа станций подобрать ширину интервала и намного быстрее разрешать коллизии, чем в случае, когда интервал фиксирован. При этом по графику видно, что максимальная пропускная способность практически в два раза превосходит пропускную способность, достижимую при фиксированном интервале, принятом по умолчанию.

6. Заключение

Стремление минимизировать затраты энергии на передачу данных в сенсорных сетях приводит к значительному упрощению используемых при

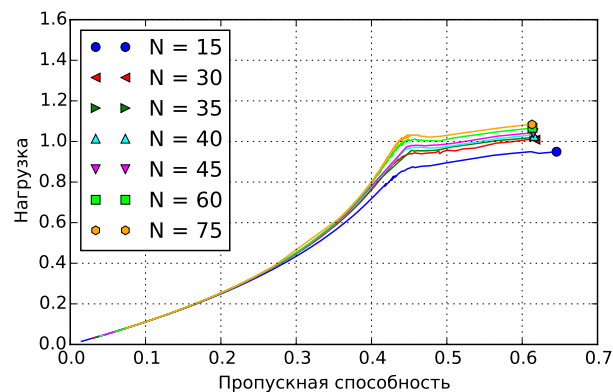


Рис. 10. Зависимость нагрузки от пропускной способности сети в случае $\frac{d}{a} = 2$ и экспоненциально-растущего интервала отсрочки

этом протоколов, в частности, метода доступа к каналу. Так, в популярной технологии LoRaWAN, метод доступа к каналу является разновидностью многоканальной АЛОХИ, в которой подтверждения на принятые кадры отправляются в основном и вспомогательном каналах. Протокол LoRaWAN нацелен на поддержку сетей из большого числа сенсоров, однако при неправильной настройке и даже при использовании стандартных параметров он не в состоянии поддерживать даже десятки активных сенсоров в сети. В данной работе указаны основные недостатки стандартного подхода к доступу к каналу, из которых главным является предлагаемый алгоритм разрешения коллизий, использование которого приводит к эффекту «снежного кома», когда пара сенсоров, вступив в коллизию, «собирает» в повторные коллизии все остальные сенсоры. Предварительные результаты показывают, что экспоненциальное увеличение отсрочки при повторных передачах кадра позволяет избежать этого эффекта, увеличить пропускную способность сети почти в два раза и обеспечить поддержку большого числа устройств. Разработка способа разрешения коллизии, эффективного не только с точки зрения пропускной способности сети, но и с точки зрения энергопотребления, является направлением для дальнейших исследований.

Список литературы

- [1] LoRa Alliance — Wide Area Networks for IoT <https://www.lora-alliance.org/>
- [2] SIGFOX — The Global Communications Service Provider for the Internet of Things <https://www.sigfox.com/>
- [3] Беспроводная LPWAN технология связи для Интернета вещей «СТРИЖ» <http://strij.net/>

- [4] LoRaWAN Specification — LoRa Alliance
<http://www.lora-alliance.org/portals/0/specs/LoRaWANSpecification1R0.pdf>
- [5] Abramson N. THE ALOHA SYSTEM: another alternative for computer communications //Proceedings of the November 17-19, 1970, fall joint computer conference. – ACM, 1970. – C. 281-285.
- [6] Centenaro, M., Vangelista, L., Zanella, A. and Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios // 2015.
- [7] Vangelista L., Zanella A., Zorzi M. Long-Range IoT Technologies: The Dawn of LoRa™ //Future Access Enablers of Ubiquitous and Intelligent Infrastructures. – Springer International Publishing, 2015. – C. 51-58.
- [8] Mo Y. et al. Optimization of the predefined number of replications in a Ultra Narrow Band based IoT network //2016 Wireless Days (WD). – IEEE, 2016. – C. 1-6.