

Банков Дмитрий Викторович

**Исследование механизмов случайного доступа к
каналу
в нелицензируемом диапазоне радиочастот
в сетях Интернета вещей**

05.12.13 – Системы, сети и устройства телекоммуникаций

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Работа прошла апробацию в *Федеральном государственном автономном образовательном учреждении высшего образования «Московский физико-технический институт (национальный исследовательский университет)»*

Научный руководитель: **Хоров Евгений Михайлович**
кандидат технических наук.

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов»

Защита состоится 25.09.2020 года в 10:00 на заседании диссертационного совета ФРКТ.05.12.13.004 по адресу 141701, Московская область, г. Долгопрудный, Институтский переулок, д.9.

С диссертацией можно ознакомиться в библиотеке и на сайте Московского физико-технического института (национального исследовательского университета) <https://mipt.ru/education/post-graduate/soiskateli-tekhnicheskie-nauki.php>.

Работа представлена «5» июня 2020 г. в Аттестационную комиссию федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (национальный исследовательский университет)» для рассмотрения советом по защите диссертаций на соискание ученой степени кандидата наук, доктора наук в соответствии с п.3.1 ст. 4 Федерального закона «О науке и государственной научно-технической политике».

Общая характеристика работы

Актуальность работы. С развитием концепции Интернета вещей всё большее значение приобретают беспроводные сенсорные сети (БСС). Они уже активно используются для наблюдения за окружающей средой и автоматизации сбора данных с измерительных приборов, таких как датчики температуры и счётчики электроэнергии, применяются в медицине и в промышленности. БСС преимущественно являются инфраструктурными сетями, в которых присутствуют базовые станции, координирующие процесс передачи и часто выполняющие роль шлюза во внешнюю сеть. Также в отличие от обычных беспроводных сетей, БСС преимущественно осуществляют передачу данных в направлении от конечных устройств — сенсоров — к базовой станции. Сенсоры в этом случае генерируют трафик низкой интенсивности и не чувствительный к времени доставки. Одним из требований к сенсорным устройствам является возможность автономной работы без подзарядки до 10 лет, в связи с чем передача данных в БСС должна быть организована таким образом, чтобы минимизировать энергопотребление. Для снижения стоимости и времени развёртывания инфраструктуры часто применяются технологии БСС, использующие нелицензируемые диапазоны радиочастот. В сценариях типичных для Интернета вещей к одной базовой станции может быть подключено много сенсоров, которые генерируют трафик в случайные моменты времени. Случайный характер трафика, необходимость экономии энергии, использование нелицензируемых радиочастот и требуемая дешевизна (и, следовательно, простота устройства) сенсоров обуславливают важность использования механизмов случайного доступа к каналу для передачи данных в БСС, а большое количество устройств в таких сетях означает, что эти механизмы должны быть эффективными в сценариях с высокой нагрузкой.

Для реализации БСС использующих нелицензируемые радиочастоты с учётом их особенностей разрабатывается и внедряется множество технологий, примером которых являются LoRaWAN, Wi-Fi HaLow, SigFox и ZigBee. Технология ZigBee была создана более 10 лет назад и является хорошо изученной, а SigFox не имеет открытого стандарта. По перечисленным причинам ZigBee и SigFox либо в настоящий момент представляют ограниченный интерес для исследования механизмов случайного доступа, либо их исследование затруднительно. В то же время LoRaWAN и Wi-Fi HaLow имеют открытые стандарты, опубликованные в 2015 и 2017 гг., соответственно. Из-за того, что данные технологии были созданы недавно, а их стандарты описывают лишь принципы работы сетей, и выбор многих параметров сети оставляют на усмотрение производителя оборудования, всё ещё остаётся ряд открытых вопросов по реализации и настройке сетей LoRaWAN и Wi-Fi HaLow, связанных с механизмами случайного доступа к каналу.

Методы случайного доступа к каналу можно поделить на два основных класса: без прослушивания несущей и с прослушиванием несущей. Метод доступа без прослушивания несущей, в частности, разновидность метода доступа к каналу «асинхронная Алоха» используется в LoRaWAN, и позволяет упростить и снизить стоимость конечных устройств. В LoRaWAN данный метод имеет ряд особенно-

стей. Во-первых, квитирования от центрального узла сети передаются как в том же канале, что и кадры от устройств, так и в дополнительном канале. Во-вторых, при неудачной попытке передачи устройства выполняют повторную попытку через случайное время, распределённое равномерно на интервале, длина которого сравнима с длительностью кадра данных. В-третьих, используемые сигнально-кодовые конструкции (СКК) имеют свойство ортогональности, то есть кадры, передаваемые в одном канале на различных СКК могут быть приняты центральным узлом сети одновременно. Также устройствам LoRaWAN свойствен эффект захвата канала: устройство, принимающее кадр в некотором частотном канале, может в процессе приёма переключиться на приём более мощного кадра, передаваемого в том же канале. При проектировании таких сетей возникает задача настройки сети и определения максимальной нагрузки, при которой сеть может гарантировать заданную вероятность доставки данных или время доставки для большого числа устройств.

Разновидность метода случайного доступа с прослушиванием несущей и избеганием коллизий, используется в Wi-Fi HaLow. В данной технологии, несмотря на наличие множества механизмов для управления процессом передачи и организации эффективного доступа к каналу по расписанию, в некоторых ситуациях устройства вынуждены использовать только методы случайного доступа для передачи кадров, например, при подключении устройств к сети, когда множество подключающихся устройств неизвестно. Передача запросов и ответов на подключение методом случайного доступа приводит к конкуренции устройств за доступ к каналу и снижает эффективность его использования. Для ограничения конкуренции при присоединении устройств к сети, в стандарте данной технологии представлены два протокола для централизованного и распределённого управления процессом присоединения. Данные протоколы представлены в стандарте как инструменты, с помощью которых можно повысить эффективность работы сети, однако настройка данных протоколов для поддержки большого числа устройств в сети выходит за рамки стандарта и является нетривиальной задачей.

Таким образом, для обеих технологий LoRaWAN и Wi-Fi HaLow актуальна проблема использования механизмов случайного доступа для передачи данных в сетях, состоящих из большого числа сенсоров. Поскольку механизмы случайного доступа в этих технологиях принципиально разные в диссертации рассматриваются обе технологии.

Степень разработанности темы. Случайный доступ к каналу является глубоко изученной темой, однако исследование механизмов случайного доступа с учётом специфики технологий LoRaWAN и Wi-Fi HaLow является открытой задачей. Исследованиям случайного доступа и смежных проблем беспроводных сетей посвящено значительное количество работ, среди которых следует особо отметить работы российских и зарубежных учёных: С.Д. Андреева, Н.Д. Введенской, Ю.В. Гайдамака, А.В. Дворковича, В.В. Зяблова, Е.А. Крука, Н.А. Кузнецова, А.Е. Кучерявого, Е.А. Кучерявого, А.И. Ляхова, А.А. Мальцева, К.В. Михайлова, А.Н. Рыбко, К.Е. Самуйлова, О.Д. Соколовой, С.Н. Степанова, В.Л. Стефанюка, А.М.

Тюрликова, Е.М. Хорова, И.И. Цитовича, Б.С. Цыбакова, В.В. Шахова, Ю.В. Шевчука, А.Н. Юргенсон, G. Bianchi, M. Centenaro, J. Haxhibeqiri, J. Famaey, J. Hoesbeke, S. Latré, I. Moerman, J. Petäjäjärvi, N. Shahin, P. Sthapit, I. Tinirello, L. Vangelista и др. Среди этих работ часть посвящена анализу технологии LoRa и сетей LoRaWAN с точки зрения различных уровней стека протоколов, в том числе представлены математические и имитационные модели метода доступа к каналу. Однако математические модели сетей LoRaWAN, существующие на момент публикации результатов диссертации, построены в предположении пуассоновского потока пакетов в канале, не описывают передачу данных в режиме с подтверждениями, не рассматривают метод повторных передач и пренебрегают наличием эффекта захвата канала, в результате чего эти модели переоценивают производительность сетей LoRaWAN, а настройка параметров сети на основе данных, полученных с помощью таких моделей, может привести к некорректной работе сетей. Таким образом, актуальным являются построение математических моделей метода случайного доступа в сетях LoRaWAN, лишённых перечисленных недостатков и позволяющих более точно описать работу сетей.

В ряде работ, посвящённых анализу процесса присоединения устройств к сетям Wi-Fi HaLow, исследуются алгоритмы выбора параметров протокола централизованного управления процессом присоединения устройств к сети. Следует отметить, что описанные на момент публикации результатов диссертации алгоритмы не учитывают уровень конкуренции за доступ к каналу при выборе параметров протокола и обладают низкой эффективностью. Также на момент публикации результатов диссертации отсутствовали исследования протокола распределённого управления процессом присоединения устройств. Поэтому актуальными являются дополнительный анализ процесса присоединения устройств к сетям Wi-Fi HaLow, разработка моделей процесса присоединения устройств и разработка решений, позволяющих снизить время присоединения.

Целью диссертационной работы является повышение эффективности механизмов случайного доступа в сетях Wi-Fi HaLow и LoRaWAN в сценариях с большим количеством устройств Интернета вещей.

Для достижения поставленной цели в диссертации ставятся и решаются следующие задачи:

1. Разработка математической модели передачи данных в сети LoRaWAN при использовании стандартного метода повторных передач кадров и наличии эффекта захвата канала, позволяющей оценить долю потерянных пакетов и время доставки пакетов.
2. Разработка алгоритма управления параметрами протокола централизованного управления процессом присоединения к сети Wi-Fi HaLow, позволяющего снизить среднее время присоединения устройств в сравнении с решениями, описанными в литературе.
3. Разработка математической модели протокола распределённого управления процессом присоединения к сети Wi-Fi HaLow, позволяющей выбрать параметры протокола, минимизирующие среднее время присоединения устройств

к сети.

Методы исследования. В диссертации используются методы теории телекоммуникационных сетей, теории вероятностей, теории случайных процессов, теории цепей Маркова, стохастической геометрии и комбинаторного анализа. При имитационном моделировании используется среда имитационного моделирования ns-3.

Научная новизна. В диссертации впервые:

- Разработана математическая модель сети LoRaWAN, учитывающая наличие подтверждений, отправляемых в том же канале, что и кадры данных, использование стандартного метода повторных передач пакетов, а также наличие эффекта захвата канала. Данная модель позволяет найти вероятность неуспешной передачи пакета, вероятность потери пакета и распределение времени доставки при передаче пакета.
- Разработан и исследован алгоритм управления порогом присоединения для протокола централизованного управления процессом присоединения к сети Wi-Fi HaLow, учитывающий уровень конкуренции за доступ к каналу при выборе параметров протокола с целью снижения времени присоединения устройств.
- Разработаны модели протокола распределённого управления процессом присоединения к сети Wi-Fi HaLow, позволяющие оценить влияние параметров протокола на среднее время присоединения устройства к сети.

Практическая ценность и реализация результатов. Использование теоретических результатов, полученных в диссертации, позволит уменьшить время присоединения устройств к сетям Wi-Fi HaLow, повысить надёжность и снизить время доставки при передаче данных в сетях LoRaWAN.

Результаты работы внедрены и используются на практике, что подтверждено соответствующими актами. В частности, разработанные модели и методы использованы в НИР, выполняемых ИППИ РАН по проектам: ОНИТ РАН «Анализ и синтез алгоритмов управления очередью и обслуживания пакетов в беспроводных сетях с гетерогенным трафиком», РФФИ «Повышение эффективности беспроводных сетей в сценариях Индустриального Интернета вещей» (№ 18-37-20077 мол_а_вед), РНФ «Цифровые технологии и их применение» (№ 14-50-00150), Мегагрант Правительства Российской Федерации «Облачные беспроводные сети пятого и последующих поколений» (договор № 14.W03.31.0019), а также для организации учебного процесса на кафедре проблем передачи информации и анализа данных МФТИ в ИППИ РАН.

Основные положения, выносимые на защиту:

1. Разработанная математическая модель сети LoRaWAN учитывает наличие эффекта захвата канала и позволяет определить максимальную интенсивность трафика в сети, при которой вероятность потери пакета и время их доставки не превышают заданных значений.
2. Разработанный алгоритм управления порогом присоединения для протокола централизованного управления процессом присоединения к сети Wi-Fi

HaLow позволяет достичь среднего времени присоединения устройств до 10 раз меньшего в сравнении с решением, предложенным в комитете по стандартизации IEEE 802 LAN/MAN.

3. Разработанная математическая модель протокола распределённого управления процессом присоединения к сети Wi-Fi HaLow позволяет найти среднее время присоединения станции к сети в зависимости от параметров протокола и количества присоединяющихся станций.

Апробация работы. Основные результаты диссертации докладывались и обсуждались на ведущих международных и российских конференциях: European Wireless (Венгрия, 2015 г.), IEEE International Symposium «Problems of Redundancy in Information and Control Systems» (REDUNDANCY) (Россия, 2016 г.), IEEE International Conference on Engineering and Telecommunication (EnT) (Россия, 2016 г.), IEEE International Conference on Communications (ICC) (Франция, 2017 г.), IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) (Макао, 2017 г.), IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (Канада, 2017 г.), «Информационные технологии и системы» в 2015–2017 гг., а также на семинарах ИППИ РАН.

Публикации. Материалы диссертации опубликованы в 13 печатных работах, из них 2 статьи [1, 2] — в рецензируемом журнале, индексируемом базами данных Scopus и Web of Science и по состоянию на конец 2019 года входящем в первый квартиль (Q1) журналов по импакт-фактору Web of Science, 7 статей [3–9] — в иных рецензируемых изданиях, входящих в перечень ВАК (в том числе 6 статей [3–8] в сборниках, индексируемых базами данных Scopus и Web of Science), а также 4 статьи [10–13] — в сборниках трудов иных конференций. Подготовка к публикации полученных результатов проводилась совместно с соавторами. Алгоритмы и модели, являющиеся результатами диссертации, разработаны диссертантом лично. Диссертантом были лично разработаны математические и имитационные модели сети LoRaWAN представленные в работах [1, 4–6, 12]. Также диссертантом были лично разработаны математические и имитационные модели сети Wi-Fi HaLow, представленные в работах [8–10]. Диссертантом были лично разработаны имитационные модели сети Wi-Fi HaLow и алгоритмы управления параметрами сети, представленные в работах [2, 3, 7, 11, 13]. Во всех приведенных работах вклад соавторов заключался в постановке задач, частичном анализе литературы и частичном получении и анализе численных результатов.

Структура и объем диссертации. Диссертация состоит из введения, 3 глав, заключения, библиографии и приложения. Общий объем диссертации 109 страниц, включая 36 рисунков и 4 таблицы. Библиография включает 82 наименования.

Содержание работы

Во Введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе рассматриваются особенности наиболее известных технологий для построения БСС, приводится обзор работ, посвящённых теме диссертации и формулируются задачи диссертации.

Технология LoRaWAN является технологией энергоэффективных сетей дальнего радиуса действия (англ. Low Power Wide Area Network, LPWAN) и позволяет создавать БСС. Типичная сеть LoRaWAN состоит из сервера, шлюзов и конечных устройств (далее называемых сенсорами). Шлюзы имеют быстрое и надёжное соединение с сервером (например, через сеть Ethernet) и соединяются с сенсорами по беспроводному каналу, играя роль ретрансляторов.

В сетях LoRaWAN данные между шлюзом и сенсорами передаются при помощи технологии LoRa. Используемая в этой технологии модуляция является разновидностью линейной частотной модуляции. Данная модуляция характеризуется параметром, называемым показателем расширения SF (англ. Spreading Factor), от которого зависит длительность символов и количество бит, передаваемых одним символом. Чем выше SF , тем ниже скорость передачи данных, но тем выше при этом чувствительность приёмника и надёжность передачи.

Важное свойство СКК LoRa состоит в том, что при определённых условиях приёмник LoRa может принять два сигнала, одновременно передаваемых в одном частотном канале, если эти сигналы используют разные показатели расширения. Более того, в реальных устройствах при передаче двух сигналов с одним показателем расширения, приёмник может различить более мощный при условии, что разность в мощности сигналов превышает 6 дБ.

Базовый механизм доступа к каналу, используемый в сетях LoRaWAN, основан на методе доступа «асинхронная Алоха» и работает следующим образом. Сеть LoRaWAN использует для передачи несколько частотных каналов: основные и один служебный. Для передачи данных устройство случайным образом выбирает один из основных каналов и передаёт кадр данных. Спустя время T_1 после окончания передачи кадра данных, сенсор должен прослушать выбранный основной канал в течение интервала времени, достаточного для детектирования начала передачи кадра от сервера (не менее, чем 6 символов на используемой СКК). Также спустя время T_2 после окончания передачи кадра, сенсор должен прослушать служебный канал. В течение интервалов, когда сенсор прослушивает канал, сервер может отправить сенсору какие-либо данные, а также подтвердить успешную передачу, установив соответствующий флаг в передаваемом кадре. Если сенсор не получает подтверждения ни в одном окне, то он делает повторную попытку передачи. Стандарт LoRaWAN рекомендует делать новую попытку передачи спустя случайное время, выбранное из интервала $[T_r, T_r + W]$ после окончания второго интервала времени, где $T_r = 1$ с, $W = 2$ с.

Сервер может назначать сенсорам СКК, используемые для передачи данных, причём алгоритм назначения СКК не описан в стандарте. По умолчанию, кадр от сервера, передаваемый в первом интервале, передаётся на той же, СКК на которой передавался соответствующий кадр от сенсора. Кадр, передаваемый в служебном канале, передаётся на одинаковой СКК для всех сенсоров, по умолчанию — на

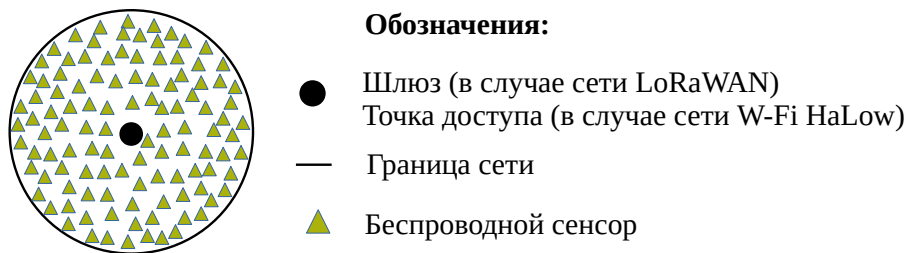


Рис. 1. Схематическое изображение исследуемой сети

самой медленной и надёжной СКК.

При исследовании механизма случайного доступа к каналу в технологии LoRaWAN рассматривается типичный сценарий работы БСС. Рассматривается сеть, изображённая на рис. 1, состоящая из множества сенсоров, равномерно распределённых в круге, в центре которого находится шлюз. Радиус круга не превышает 500 м, а количество сенсоров в сети — до 10000. Сенсоры генерируют данные порциями, которые могут быть переданы один кадром LoRaWAN (до 51 байта), и передают их на шлюз. Сенсоры генерируют новые пакеты согласно потоку Пуассона так, что средний интервал времени между генерацией новых пакетов одним сенсором составляет от 1 до 200 часов. Сеть использует 3 основных частотных канала и один дополнительный, шириной 125 кГц каждый. При этом устройства могут передавать данные используя набор СКК, определённый в стандарте LoRaWAN. Мощность передатчика на устройствах составляет 14 дБм. В канале имеется случайный шум, из-за которого передаваемые пакеты могут быть потеряны. Вероятность потери пакета из-за шума не превосходит 0,01.

Базовый механизм случайного доступа в сетях LoRaWAN реализует метод случайного доступа «асинхронная Алоха», математические модели которого подробно представлены в научной литературе. Однако данный механизм имеет ряд особенностей, связанных со спецификой технологии LoRaWAN, а именно: наличие ортогональных СКК, использование нескольких частотных каналов, эффект захвата канала, отправления двух подтверждений и метод повторных передач. С учётом этих особенностей технологии LoRaWAN возникает задача определения максимальной нагрузки, при которой сеть может гарантировать требуемую вероятность доставки данных и задержку, а также возникает задача назначения СКК устройствам с целью обеспечения требуемой задержки при доставке пакетов и вероятности доставки данных.

Технология Wi-Fi HaLow является адаптацией широко используемой технологии Wi-Fi к сценариям Интернета вещей и реализует дополнение к стандарту сетей Wi-Fi IEEE 802.11ah. Сети Wi-Fi HaLow передают данные в нелицензируемых диапазонах частот ниже 1 ГГц, использует узкие частотные каналы, шириной 1, 2, 4, ..., 16 МГц, и одна точка доступа Wi-Fi HaLow может обслуживать в пределах своей сети до ≈ 8000 устройств. Для поддержки большого числа устройств в технологии Wi-Fi HaLow имеется множество новых механизмов, позволяющих повысить эффективность использования канальных ресурсов в БСС. Проблема

поддержки большого числа устройств становится особенно важной в моменты, когда устройства присоединяются к сети, так как при этом точке доступа сети не известны количество устройств и поддерживаемый ими функционал.

В сетях Wi-Fi HaLow, как и в обычных сетях Wi-Fi, процесс присоединения устройств к сети состоит из двух этапов: аутентификации и ассоциации, и обычно начинается после того, как станция узнаёт о существовании сети, получив бикон — кадр, периодически рассылаемый точкой доступа для синхронизации сети и рассылки служебной информации. Для аутентификации станция передаёт точке доступа запрос на аутентификацию (кадр AuthReq, англ. Authentication Request), на который точка доступа должна ответить ответом на аутентификацию (кадр AuthRep, англ. Authentication Response).

После аутентификации станция может провести процедуру ассоциации с точкой доступа. Для этого станция отправляет ей запрос на ассоциацию (кадр AReq, англ. Association Request), на который точка доступа отправляет ответ на ассоциацию (кадр ARep, англ. Association Response). Только после пройденной процедуры ассоциации станция может отправлять и принимать кадры данных.

При передаче всех вышеупомянутых кадров станция и точка доступа используют стандартный метод случайного доступа Enhanced Distributed Channel Access (EDCA), который является разновидностью множественного доступа с контролем несущей и избеганием коллизий. В сети Интернета вещей возможна ситуация, когда большое количество станций одновременно начинают процедуру присоединения, например, когда группа станций получает бикон после перезагрузки точки доступа. В таком случае, станции одновременно начинают отправлять кадры AuthReq, что приводит к высокой конкуренции за доступ к каналу между устройствами. Производительность стандартного метода случайного доступа значительно падает при большом количестве конкурирующих станций. По этой причине в дополнении к стандарту IEEE 802.11ah представлены два протокола управления присоединением: протокол централизованного управления присоединением (ПЦУП) и протокол распределённого управления присоединением (далее ПРУП) — позволяющие точке доступа снизить конкуренцию между станциями за доступ к каналу на этапе аутентификации.

При использовании ПЦУП, точка доступа управляет долей числа станций, которым разрешено запрашивать аутентификацию. Для этого точка доступа в биконах передаёт порог аутентификации (англ. Authentication Threshold) — целое число от 0 до 1023. При включении, станция выбирает случайное целое число, равномерно распределённое от 0 до 1022 и ждёт бикон с порогом аутентификации. Если выбранное число меньше либо равно порогу, станция ждёт следующий бикон. В противном случае станция генерирует запрос на аутентификацию и начинает его отправку методом случайного доступа EDCA. Если станция в течение заданного интервала времени с момента генерации запроса не получает ответ, то станция ждёт следующий бикон и повторяет вышеописанную процедуру заново.

Стандарт IEEE 802.11ah не описывает процедуру выбора порога аутентификации точкой доступа. Однако выбор данного параметра имеет большое значение

для времени установки соединения. Например, когда количество станций мало, порог присоединения нужно устанавливать равным 1023 для минимизации времени присоединения. В то же время, при большом количестве станций, порог следует постепенно увеличивать от минимального значения к максимальному, позволяя небольшим группам станций получать доступ к каналу. Так возникает задача разработки алгоритма адаптивного выбора порога присоединения.

При исследовании механизмов случайного доступа к каналу в технологии Wi-Fi HaLow, среди прочих, рассматривается сценарий работы сети, изображённой на рис. 1, состоящей из множества сенсоров, равномерно распределённых в круге, в центре которого находится точка доступа. Радиус круга не превышает 200 м, количество сенсоров — до 8000. Мощность передатчика на устройствах составляет 16 дБм, что соответствует типичным параметрам сети Wi-Fi HaLow. В начальный момент времени сенсоры начинают процесс присоединения к точке доступа, используя заданный протокол (централизованного или распределённого) управления процессом присоединения.

При использовании ПРУП, интервалы между последовательными биконами (бикон-интервалы) разделяются на подынтервалы, называемые слотами управления аутентификацией (англ. Authentication Control Slot, ACS). Для того, чтобы ограничить конкуренцию при отправке запросов на аутентификацию, станции используют следующую процедуру, основанную на двоичной экспоненциальной отсрочке. Каждая станция задерживает попытку аутентификации на случайное время, состоящее из m бикон-интервалов и l ACS. Значение l выбирается равномерно из интервала $[0, L]$, где $L = \lfloor \frac{BI}{T_{AC}} \rfloor$, где T_{AC} — длительность слота. Значение m выбирается равномерно из интервала $[0, TI_\rho]$, где ρ — счётчик попыток аутентификации и

$$TI_\rho = \begin{cases} TI_{min}, & \rho = 0, \\ \min \{2TI_{\rho-1}, TI_{max}\} & \rho > 0. \end{cases}$$

Параметры TI_{min} , TI_{max} и T_{AC} определяются точкой доступа. Внутри слота, станция передаёт запрос на аутентификацию согласно стандартному методу случайного доступа. Если станция в течение заданного интервала времени не получает ответ, то она увеличивает счётчик попыток аутентификации ρ , генерирует новые m и l и заново выполняет описанную выше процедуру.

Согласно стандарту, максимальное значение для параметра T_{AC} равно примерно 130 мс, а для параметров TI_{min} и TI_{max} равно 255, но выбор значений этих параметров, позволяющих достичь наименьшего времени присоединения устройств, неочевиден. Так возникает задача разработки моделей ПРУП и выбора оптимальных значений параметров протокола.

Во второй главе разрабатывается математическая модель передачи данных в сети LoRaWAN при использовании стандартного метода повторных передач кадров и наличии эффекта захвата канала. В модели рассматривается сеть LoRaWAN, состоящая из сервера, шлюза и N сенсоров, использующих F основных

и один служебный канал для передачи. Устройства используют СКК $0, 1, \dots, M$, ортогональные друг другу и устанавливаемые сервером.

Работу сети можно моделировать как совокупность N систем с повторными заявками, в каждую из которых первичные заявки поступают согласно пуассоновскому потоку интенсивности λ/N , а вероятность повторной заявки определяется интегральными характеристиками остальных $N - 1$ систем. Однако, следуя классическому подходу для анализа системы «асинхронная Алоха», для вычисления численных характеристик сети процесс передачи данных рассматривается как набор из $F \times (M + 1) + 1$ временных осей, на которых случайным образом располагаются полуинтервалы, соответствующие передаваемым кадрам. Вероятность успешной передачи кадра рассчитывается через вероятность того, что соответствующий кадру полуинтервал не пересекается с другими, или, в случае пересечения, вероятность того, что на протяжении всей длительности кадра мощность сигнала превышает мощность шума и интерферирующих сигналов как минимум на CR , где CR — параметр захвата канала (6 дБ). Данная вероятность находится методами стохастической геометрии. При рассмотрении вероятности успешной передачи также учитывается, что кадр с вероятностью q может быть искажён случайным шумом.

Если из-за коллизии или шума сенсор не получает подтверждение от шлюза, он делает повторную попытку передачи, число которых ограничено значением RL (по-умолчанию, равным 8), по достижении которого сенсор отбрасывает кадр. Также в силу того, что сенсоры должны быть устроены максимально простым образом, предполагается, что у них ограничен размер буфера кадров на передачу. Если во время передачи кадра сенсор генерирует новый кадр, то после окончания попытки передачи сенсор перейдёт к обслуживанию нового кадра, даже если предыдущая попытка передачи была неуспешной.

В модели первые и повторные попытки передачи рассматриваются отдельно. Учитывается, что интенсивность потока повторных попыток передачи меньше интенсивности потока первых попыток передачи. Как следствие, при выводе вероятности успеха при первой попытке передачи пренебрегается коллизиями с повторными попытками, а также считается, что в коллизиях, приводящих к повторной попытке передачи, участвуют не более двух кадров.

Далее приводятся основные формулы модели, вывод и подробное описание которых содержатся в диссертации.

Для описания первых попыток передачи используется модификация распространённого подхода для моделирования метода доступа «асинхронная Алоха», учитывающая передачу подтверждений и наличие эффекта захвата канала. Первая попытка передачи является успешной с вероятностью:

$$P_i^{S,1} = P_i^{Data} P_i^{Ack}, \quad (1)$$

где P_i^{Data} — вероятность успешной передачи кадра от сенсора на СКК i , а P_i^{Ack} — вероятность того, что хотя бы одно подтверждение от сервера будет принято сенсором при условии, что данные были переданы успешно.

В рамках предположений модели, вероятность успешной передачи кадра от сенсора на СКК i находится как

$$P_i^{Data} = V_{i,0}^G e^{-(2T_i^{Data} + P_i^{Data} T_i^{Ack}) r_i} + \sum_{k=1}^{N-1} \frac{(2r_i T_i^{Data})^k}{k!} e^{-2r_i T_i^{Data}} V_{i,k}^G, \quad (2)$$

где T_i^{Data} и T_i^{Ack} — длительности кадра данных и подтверждения, соответственно, на СКК i , r_i — интенсивность трафика, приходящаяся на СКК i и на один основной канал, а $V_{i,k}^G$ — вероятность того, что мощность интерферирующих сигналов от k сенсоров меньше чем мощность сигнала от рассматриваемого сенсора плюс CR дБ, а также того, что кадр не был потерян из-за случайного шума.

Вероятность доставки хотя бы одного подтверждения находится как

$$P_i^{Ack} = P_i^{Ack1} + P_i^{Ack2} - P_i^{Ack1} P_i^{Ack2}, \quad (3)$$

где P_i^{Ack1} и P_i^{Ack2} — вероятности доставки первого и второго подтверждения, соответственно, при условии, что данные были переданы на СКК i .

Вероятность передачи первого подтверждения имеет вид, аналогичный (2):

$$P_i^{Ack1} = V_{i,0}^S e^{-(\min(T_1, T_i^{Data}) + T_i^{Ack}) r_i} + \sum_{k=1}^{N-1} \frac{(r_i T_i^{Ack})^k}{k!} e^{-r_i T_i^{Ack}} V_{i,k}^S, \quad (4)$$

где $V_{i,k}^S$ — вероятность того, что мощность интерферирующих сигналов от k сенсоров меньше чем мощность сигнала от шлюза плюс CR дБ, а также того, что кадр не был потерян из-за случайного шума.

Вероятность успешной доставки второго подтверждения находится как

$$P_i^{Ack2} = V_{0,0}^S e^{-T_0^{Ack}(\lambda - r_i)}. \quad (5)$$

В то же время, этот подход нельзя использовать для описания повторных попыток передачи, так как они не представляют собой поток Пуассона, и для их описания предложен другой способ учесть повторные попытки передачи. При повторной попытке передачи вероятность доставки кадра находится как:

$$P_{i,Re}^{Data} = \frac{P_{i,1}^S \frac{\zeta}{1-\zeta} + \left(1 - \frac{P_{i,1}^S}{1-\zeta}\right) \times [V_i^O (1-\zeta) + (V_i^O \zeta + V_i^B) \times (1 - P_i^c)]}{P_{i,1}^S \frac{\zeta}{1-\zeta} + \left(1 - \frac{P_{i,1}^S}{1-\zeta}\right) \times (1 - V_{i,1}^G)} P_i^{Data}, \quad (6)$$

где ζ — вероятность того, что повторная попытка передачи вызвана шумом и её осуществляет только один сенсор, V_i^O — вероятность того, что при пересекающейся во времени передаче двух сенсоров мощность сигнала одного сенсора настолько превосходит мощность сигнала другого сенсора, что его передача может быть принята шлюзом успешно, V_i^B — вероятность такого соотношения мощностей сигнала

лов сенсоров, что оба кадра не могут быть приняты шлюзом, а P_i^c — вероятность того, что после коллизии двух кадров произойдёт повторная коллизия.

Кадры передаются с одинаковой мощностью, а мощность сигнала при распространении затухает согласно модели Окамуры-Хата. Вероятности типа V_*^* приёма сигналов на фоне интерферирующих сигналов находятся методами стохастической геометрии. Их вывод, а также вывод других величин, входящих в выражения (1)–(6) приведён в тексте диссертации.

Полная вероятность успеха при повторной попытке передачи $P_i^{S,Re}$ получается согласно уравнению (1), где вместо P_i^{Data} используется $P_{i,Re}^{Data}$.

В модели вероятность PER неудачи при попытке передачи кадра находится как дополнение к вероятности успешной передачи кадра с первого раза или при повторной попытке передачи:

$$PER = 1 - \sum_{i=0}^M p_i \left(P_{1,i} P_i^{S,1} + (1 - P_{1,i}) P_i^{S,Re} \right), \quad (7)$$

где суммирование ведётся по всем СКК, p_i — вероятность того, что сенсор передаёт на СКК i а $P_{1,i}$ — вероятность того, что кадр передаётся впервые.

Вероятность потери кадра находится исходя из того, что кадр теряется в случае, если его не получается доставить за RL попыток передачи. Это может произойти если сенсор совершает RL коллизий подряд или если во время передачи кадра генерируется новый кадр. Чтобы найти данную вероятность нужно вычесть из единицы вероятность успешной передачи после любого возможного количества попыток передачи:

$$PLR = 1 - \sum_{i=0}^M p_i \left(P_i^{S,1} + (1 - P_i^{S,1}) P_i^G P_i^{S,Re} \sum_{r=1}^{RL-1} \left(P_i^G (1 - P_i^{S,Re}) \right)^{r-1} \right). \quad (8)$$

В данной формуле производится суммирование по всем СКК, и для каждой СКК учитывается вероятность передачи кадра с первой попытки, а также вероятность того, что при неуспешной первой попытке передачи сенсор передаёт кадр успешно после r повторных попыток передачи. При этом учитывается P_i^G — вероятность того, что во время повторной попытки передачи сенсор не генерирует новый кадр (в противном случае он должен отбросить текущий кадр).

Распределение задержки задаётся похожим выражением:

$$F_d(x) = \sum_{i=0}^M p_i \left(F_{0,i}^d(x) P_i^{S,1} + (1 - P_i^{S,1}) P_i^G P_i^{S,Re} \sum_{r=1}^{RL-1} F_{r,i}^d(x) \left(P_i^G (1 - P_i^{S,Re}) \right)^{r-1} \right), \quad (9)$$

где $F_{r,i}^d(x)$ — это распределение задержки на r -ю попытку передачи кадра.

Коллизиям в сетях LoRaWAN свойствен эффект «снежного кома», состоящий в том, что когда два или более сенсора делают неуспешные попытки передачи, при повторной попытке вероятность коллизии для них становится гораздо

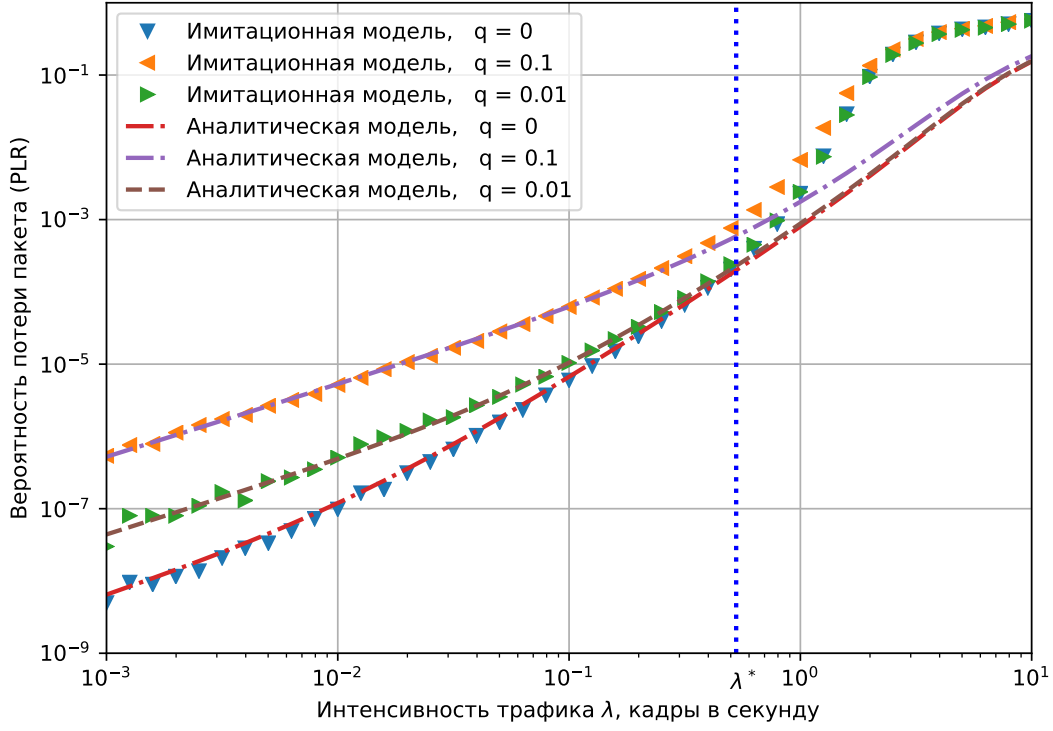


Рис. 2. Зависимость вероятности потери пакета от нагрузки сети

выше, и эти устройства с большой вероятностью вовлекают в коллизии другие устройства. Данный эффект становится заметным при интенсивности генерации новых кадров, когда каждая повторная попытка передачи приводит к коллизии с новым кадром. Чтобы её найти, нужно число каналов F поделить на среднюю длительность повторной попытки передачи:

$$\lambda^* = F \left(\sum_{i=0}^M p_i \left(T_i^{Data} + T_2 + T_0^{Ack} + T_r + \frac{W}{2} \right) \right)^{-1}, \quad (10)$$

где $T_2 = 1$ с — интервал времени, до отправки второго подтверждения. Данная нагрузка используется как граница применимости разработанной модели.

На рис. 2 показана зависимость вероятности потери кадра PLR от нагрузки сети. На графике приведены значения для параметра захвата канала $CR = 6$ дБ, СКК от 0 до $M = 6$, характеристики которых приведены в разделе 1.2 диссертации, количества основных каналов $F = 3$. При этом рассматривается вероятность потери кадра из-за шума равная 0, 0,1 и 0,01. Как видно, при нагрузке ниже λ^* результаты, полученные при помощи математической модели, незначительно отличаются от результатов имитационной модели.

При низкой нагрузке на сеть получается, что даже при достаточно высоком уровне шума ($q = 0,1$) метод повторных передач в сети LoRaWAN достигает низкой вероятности потери кадра, однако при высокой нагрузке данный метод становится неэффективным из-за слишком малого значения W — окна, из которого выбирается случайное время для повторной передачи.

Далее в разделе 2.3 диссертации приводятся примеры того, как разработанная математическая модель может быть использована при планировании сети LoRaWAN. В первом примере рассматривается задача минимизации вероятности неуспешной попытки передачи кадра PER . Минимизация PER осуществляется путём распределения СКК между сенсорами — выбора доли p_i сенсоров в сети, передающих на СКК i , используя уравнение (7). Согласно полученным численным результатам, назначение СКК так, чтобы доля сенсоров, использующих СКК i , равнялась p_i , позволяет в два раза снизить вероятность неуспешной передачи по сравнению с равномерным распределением СКК.

Во втором примере рассматривается задача планирования гетерогенной сети LoRaWAN, в которой присутствуют несколько групп сенсоров, каждая из которых генерирует трафик заданной интенсивности и имеет заданные требования на максимальную вероятность потери пакета. При равномерном распределении всех устройств в сети по СКК получается, что требования ни одной группы не могут быть удовлетворены. В то же время разработанную модель можно использовать для того, чтобы для каждой группы устройств определить максимальную нагрузку для каждой СКК, при которой достигается заданное ограничение на вероятность потери пакета — ёмкость сети для заданной СКК и категории устройств. Данная величина тем больше, чем большую вероятность потери пакета допускают устройства и чем более быстрая СКК рассматривается. Далее самая медленная СКК назначается такому числу сенсоров из группы устройств, имеющей наиболее строгие требования, чтобы генерируемый ими трафик имел интенсивность, равную ёмкости сети для данной СКК. Если ещё не всем устройствам из данной группы была назначена СКК, такая же процедура производится для следующей, более быстрой СКК и так далее. Затем аналогичным образом назначаются СКК следующей группе устройств, с тем ограничением, что при назначении устройству СКК не должны нарушаться требования на качество обслуживания учётом для устройств, которым уже назначена данная СКК. Использование данного подхода позволяет разделить устройства разных групп по СКК так, чтобы их требования к качеству обслуживания выполнялись.

В третьей главе исследуются механизмы случайного доступа к каналу при присоединении устройств к сети IEEE 802.11ah. Сначала рассматривается сеть Wi-Fi HaLow, состоящая из точки доступа и группы из N сенсоров, начинающих одновременно процесс присоединения к сети. В качестве меры эффективности механизмов случайного доступа рассматривается время присоединения группы устройств к сети при использовании ПЦУП и ПРУП. Для исследования данных механизмов использовалась среда имитационного моделирования ns-3.

В третьей главе проведено исследование ПЦУП, для которого разработаны и исследованы алгоритмы управления порогом присоединения.

В первую очередь, для ПЦУП разработан алгоритм Оракул, позволяющий найти оценку для минимального времени присоединения устройств при использовании ПЦУП. Данный алгоритм предполагает априорное знание точкой доступа количества присоединяющихся станций N , а также количества станций k_{opt} ,

которым нужно разрешать доступ к каналу в начале бикон-интервала, чтобы к концу бикон-интервала количество присоединившихся станций было максимальным. Для того, чтобы присоединить станции к сети за кратчайшее время, точка доступа начинает с порога присоединения равного нулю и сдвигает порог с шагом $\Delta = 1023 \frac{k_{opt}}{N}$. Таким образом точка доступа стремится в каждом бикон-интервале присоединять к сети в среднем максимальное количество станций. Следует отметить, что данный алгоритм не предполагается использовать в реальных устройствах, поскольку в реальных условиях точке доступа заведомо неизвестно количество присоединяющихся станций. Он используется только как инструмент для оценки эффективности других алгоритмов.

Поскольку в реальных условиях точке доступа заведомо неизвестно число станций и то, скольким станциям нужно разрешать доступ к каналу в бикон-интервале, далее разрабатывается алгоритм адаптивного выбора порога присоединения. Разработанный алгоритм рассматривает длину очереди ответов у точки доступа и изменяет значение порога на Δ . В то же время, значение Δ не является постоянной величиной, а изменяется согласно интенсивности поступления новых запросов на присоединение и отправки ответов на них.

Алгоритм может выполняться в трёх режимах и начинает работу в режиме *ожидания*. В данном режиме точка доступа устанавливает максимальный порог и отслеживает состояние очереди по окончании каждого бикон-интервала.

Если по окончании бикон-интервала в очереди остаются кадры AuthRep, точка доступа устанавливает порог равным 0 и ожидает, пока очередь ответов не опустеет. После этого точка доступа переходит в режим *обучения*, устанавливает порог и Δ равным 1.

В режиме обучения точка доступа по окончании каждого бикон-интервала увеличивает порог на Δ . Если по окончании бикон-интервала очередь точки доступа оказывается пустой, точка доступа удваивает значение Δ . Когда очередь окажется непустой, известно, что текущее значение Δ слишком велико, а предыдущее (в два раза меньшее) — меньше либо равно оптимальному. На этом шаге точка доступа делит Δ на 2 и переходит в режим *работы*.

В режиме работы, на каждом бикон-интервале точка доступа увеличивает порог присоединения на Δ если очередь пуста и не меняет порог в противном случае. Также точка доступа производит процедуру уточнения значения Δ . Для этого точка доступа увеличивает Δ на 1 по окончании бикон-интервалов. Такое уточнение выполняется только тогда, когда взведён флаг *tune*. Этот флаг сбрасывается, если очередь оказывается непустой по окончании бикон-интервала, так как это означает, что найденная оценка Δ слишком велика. Данный флаг взводится когда алгоритм переключается из режима *обучения* в режим *работы*, а также тогда, когда очередь ответов пребывает пустой в течение e бикон-интервалов подряд, где e — параметр алгоритма.

Когда порог достигает максимального значения, алгоритм снова переключается в режим *ожидания*.

Было проведено сравнение эффективности разработанного алгоритма с алго-

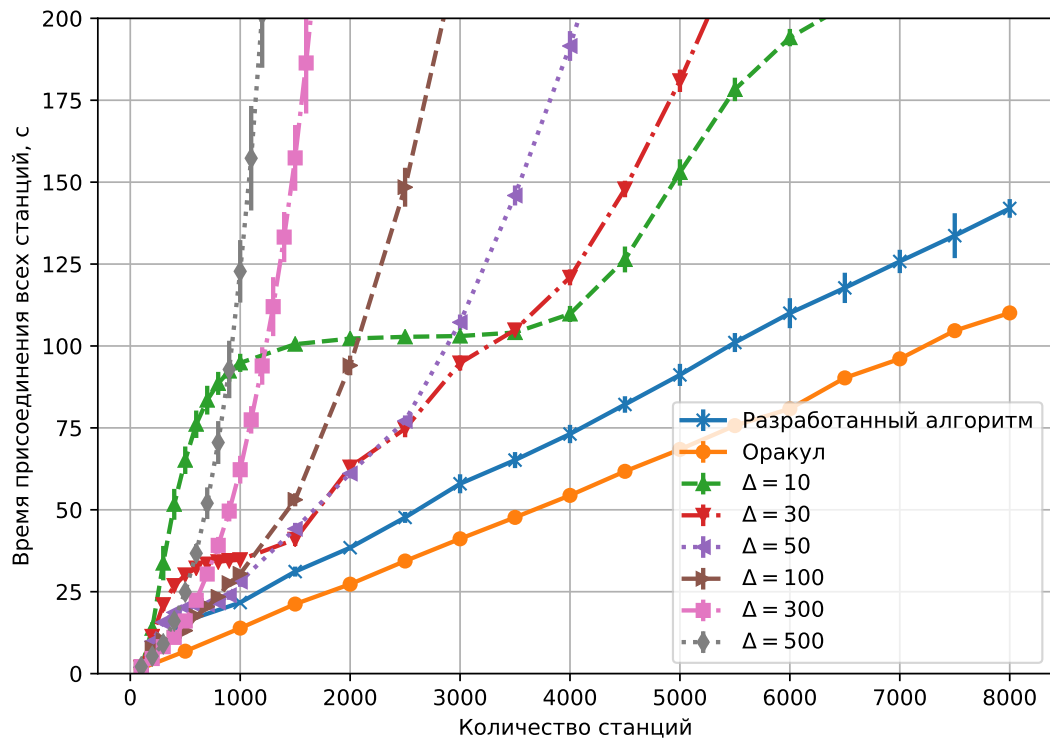


Рис. 3. Зависимость среднего времени присоединения сенсоров от их количества

ритмом, предложенным в комитете по стандартизации IEEE 802 LAN/MAN. При использовании данного алгоритма точка доступа увеличивает порог на Δ , если по окончании бикон-интервала число кадров в очереди ответов меньше Δ . либо уменьшает после каждого бикон-интервала Δ в противном случае, точка доступа уменьшает порог на Δ . При этом параметры Λ и Δ являются фиксированными, но в литературе отсутствуют рекомендации по их выбору.

На рис. 3 приведены результаты моделирования, в которых разработанный алгоритм сравнивается с алгоритмом Оракул и с алгоритмом, известным из литературы (кривые $\Delta = \dots$), при разных значениях параметра Δ и при $\Lambda = 0$. Как видно, для алгоритма, известного из литературы, время присоединения устройств значительно зависит от выбора параметра Δ . В то же время, разработанный алгоритм значительно превосходит по времени присоединения устройств алгоритм, известный из литературы, и проигрывает по времени присоединения алгоритму Оракул не более чем на 25%.

Далее в третьей главе проведено исследование ПРУП, для чего данный протокол реализован в среде имитационного моделирования ns-3.

Исследование влияния параметра T_{AC} — длительности слота управления аутентификацией — на эффективность ПРУП показало, что данный протокол практически не чувствителен к значению данного параметра. Такое отсутствие чувствительности связано с тем, что согласно стандарту IEEE 802.11ah, станции не ограничивают передачу запросов на аутентификацию выбранным слотом управления аутентификацией. В начале выбранного слота станция лишь генерирует кадр AuthReq и начинает процедуру случайного доступа к каналу. Однако

если канал занят или в случае коллизий, станция может совершить передачу кадра за пределами слота. В результате попытки передачи запросов не локализованы внутри соответствующих слотов управления аутентификацией, но распределены во времени независимо от значения T_{AC} .

Гораздо значительно на эффективность ПРУП влияет выбор параметра TI_{min} — начального окна, из которого сенсоры выбирают бикон-интервал, в котором начинают присоединение к сети. Значение TI_{min} , минимизирующее время присоединения устройств, зависит от количества присоединяющихся станций. Когда станций немного, они могут присоединиться к сети с первой попытки, и в среднем время присоединения составляет TI_{min} бикон-интервалов. Получается, что в таком случае использование больших TI_{min} является избыточным и приводит к высокому времени присоединения. В то же время, если присоединяющихся станций много, то когда TI_{min} мало, первые попытки аутентификации в основном оказываются неуспешными, что приводит к новым попыткам аутентификации и увеличивает время присоединения. Выбирая большое значение TI_{min} можно повысить вероятность успеха при попытках аутентификации.

Сравнение ПЦУП с ПРУП показало, что ПЦУП с алгоритмом Оракул достигает наименьшего времени присоединения устройств к сети, причём ПРУП позволяет достичь данное время только если параметр TI_{min} заранее выбран оптимальным образом, соответствующим количеству присоединяющихся сенсоров. Однако при фиксированном значении TI_{min} время присоединения к сети минимизируется лишь для небольшого диапазона количества сенсоров, а для другого числа сенсоров ПРУП может почти в два раза проигрывать по времени присоединения. В то же время ПЦУП с разработанным алгоритмом достигает примерно на 30% большего времени присоединения сенсоров чем ПЦУП с алгоритмом Оракул, но тоже для широкого диапазона числа сенсоров позволяет достичь меньшего времени присоединения чем ПРУП.

ПЦУП и ПРУП также сравнивались в менее благоприятных для присоединяющихся сенсоров сценариях. В данных сценариях помимо сенсоров в сети присутствуют пользовательские устройства, которые в начальный момент времени уже присоединены к сети и в режиме насыщения передают точке доступа кадры данных. Эти устройства создают конкуренцию присоединяющимся сенсорам и препятствуют отправке запросов на присоединение и ответов на них. В таком сценарии ПРУП гораздо менее эффективен, чем ПЦУП, и разница во времени для разных значений параметра TI_{min} становится незначительной. В то же время ПЦУП с разработанным алгоритмом управления порогом присоединения практически так же эффективен, как и ПЦУП с алгоритмом Оракул. Данный результат объясняется тем, что ПЦУП с разработанным алгоритмом позволяет точке доступа эффективнее чем ПРУП подстраивать количество присоединяющихся сенсоров под условия в канале, и время, необходимое для обучения алгоритма является незначительным по сравнению с временем присоединения устройств к сети.

Сравнение ПЦУП и ПРУП в других сценариях: в сценарии, в котором пользовательские устройства полностью скрыты от сенсоров, и в сценариях, в которых

присутствует эффект захвата канала, показывает аналогичные результаты.

Далее в третьей главе описывается схема для повышения эффективности протоколов управления процессом присоединения за счёт передачи части кадров, необходимых для присоединения устройств к сети, без конкуренции за доступ к каналу. Данная схема основана на том, что, получив запрос на аутентификацию, точка доступа не передаёт сразу ответ, а ждёт следующий бикон-интервал. В начале бикон-интервала точка доступа использует стандартный механизм виртуальной занятости среды, который позволяет внутри передаваемого кадра указать время, в течение которого среда будет занята, и все устройства сети не должны будут передавать кадры. Точка доступа может использовать данный механизм для того, чтобы гарантировать передачу ответа на запрос аутентификации, последующего запроса ассоциации и соответствующего ответа без конкуренции за доступ к каналу для всех сенсоров, запросивших аутентификацию за предыдущий бикон-интервал. Таким образом, во время присоединения к сети станция должна будет получать доступ к каналу только один раз — при передаче первого кадра — а передача следующих кадров будет защищена от коллизий точкой доступа.

Для ПРУП с применением предложенной схемы построена математическая модель процесса присоединения сенсора к сети, позволяющая найти среднее время присоединения сенсора. Рассматривается сценарий, когда одновременно N сенсоров начинают процесс присоединения. Процесс передачи запроса на присоединение сенсором описывается как случайный процесс с дискретным временем, единицей которого является один бикон-интервал. В качестве состояния процесса рассматривается количество попыток присоединения r , выполненных рассматриваемым сенсором к текущему бикон-интервалу. В модели предполагается, что все устройства в сети находятся в зоне видимости друг-друга, все устройства равноправны, и кадры в канале могут быть потеряны только в случае коллизии.

В модели рассматриваются последовательные бикон-интервалы и находится вероятность $TX_{t,r}$ того, что выбранный сенсор в интервале номер t будет передавать запрос, при условии, что за прошедшие t интервалов он совершил r попыток присоединения, и ни одна из них не была успешной:

$$TX_{t,r} = \begin{cases} \frac{1}{TI_{min}}, & r = 0, t < TI_{min}, \\ 0, & r = 0, t \geq TI_{min}, \\ \frac{1}{TI_r} \sum_{i=\max(t-TI_r, r-1)}^{t-1} C_{i,r-1}, & r > 0, \end{cases} \quad (11)$$

где $S_{t,r}$ и $C_{t,r}$ — вероятность успешной и неуспешной попытки присоединения при попытке передачи r в бикон-интервале t , соответственно, причём $T_{t,r} = S_{t,r} + C_{t,r}$. Первое и второе равенство означают, что первую попытку присоединения сенсор осуществляет равновероятно в одном из первых TI_{min} бикон-интервалов. Третье равенство соответствует попытке передачи r , которая наступает после попытки передачи $r - 1$ в случае неуспеха в одном из TI_r предыдущих слотов.

Из данной вероятности можно найти $TX_t = \sum_{r=0}^t TX_{t,r}$ того, что любой

другой сенсор совершает попытку присоединения в бикон-интервале t .

Далее вероятность успешной передачи запроса сенсором находится как

$$S_{t,r} = TX_{t,r} \sum_{k=0}^{N-1} \binom{N-1}{k} TX_t^k (1 - TX_t)^{N-k-1} \sum_{s=1}^k p_{s|k+1} \frac{s}{k+1}. \quad (12)$$

Вероятность успеха задаётся вероятностью того, что выбранный сенсор сделает попытку передачи, вероятностью того, что из $N - 1$ других сенсоров будут передавать k сенсоров и вероятностью $p_{s|k+1}$ того, что из $k + 1$ передающих сенсоров s сенсоров присоединятся успешно, а выбранный сенсор будет среди них. Вывод вероятности $p_{s|k+1}$ приводится в разделе 3.4.1 диссертации. Далее суммированием получается вероятность успеха в бикон-интервале t : $S_t = \sum_{r=0}^t S_{t,r}$.

Среднее время присоединения выбранного сенсора находится как сумма среднего времени, необходимого сенсорам на отправку запроса на аутентификацию и времени, затрачиваемого точкой доступа на обмен кадрами AuthRep-AReq-ARep со станциями, запросившими аутентификацию до выбранного сенсора.

$$\mathbb{E}(T) = T_{BI} \sum_{t=0}^{\infty} t S_t + \frac{N}{2} T_h, \quad (13)$$

где T_{BI} — длительность бикон-интервала, а T_h — время, необходимое на передачу последовательности кадров AuthRep-AReq-ARep.

Согласно результатам моделирования (см. рис. 4), ПРУП с предложенной схемой при $TI_{min} = 8$ достигает примерно такой же эффективности как ПЦУП с использованием алгоритма Оракул. Таким образом, использование предложенной схемы для бесконкурентного доступа к каналу позволяет значительно повысить эффективность ПРУП и достичь времени присоединения устройств, близкого к минимальному. При этом, если у точки доступа имеется оценка числа присоединяющихся станций, например, когда в случае перезагрузки точка доступа сохраняет информацию о том, сколько станций было к ней присоединено, то разработанная модель может быть использована для нахождения параметров ПРУП, для заданного количества станций минимизирующих среднее время присоединения.

В Заключение сформулированы основные результаты диссертации.

В Приложение включены акты о внедрении результатов диссертации.

Основные результаты

В данной диссертации проведены разработка и моделирование механизмов случайного доступа к каналу в беспроводных сенсорных сетях. В частности:

1. Разработана математическая модель сети LoRaWAN, учитывающая наличие подтверждений, отправляемых в том же канале, что и кадры данных, использование стандартного метода повторных передач пакетов и наличие эффекта захвата канала.

2. Разработано решение с использованием алгоритма «Оракул», позволяющее найти минимальное время присоединения устройств к сети Wi-Fi HaLow, дости-

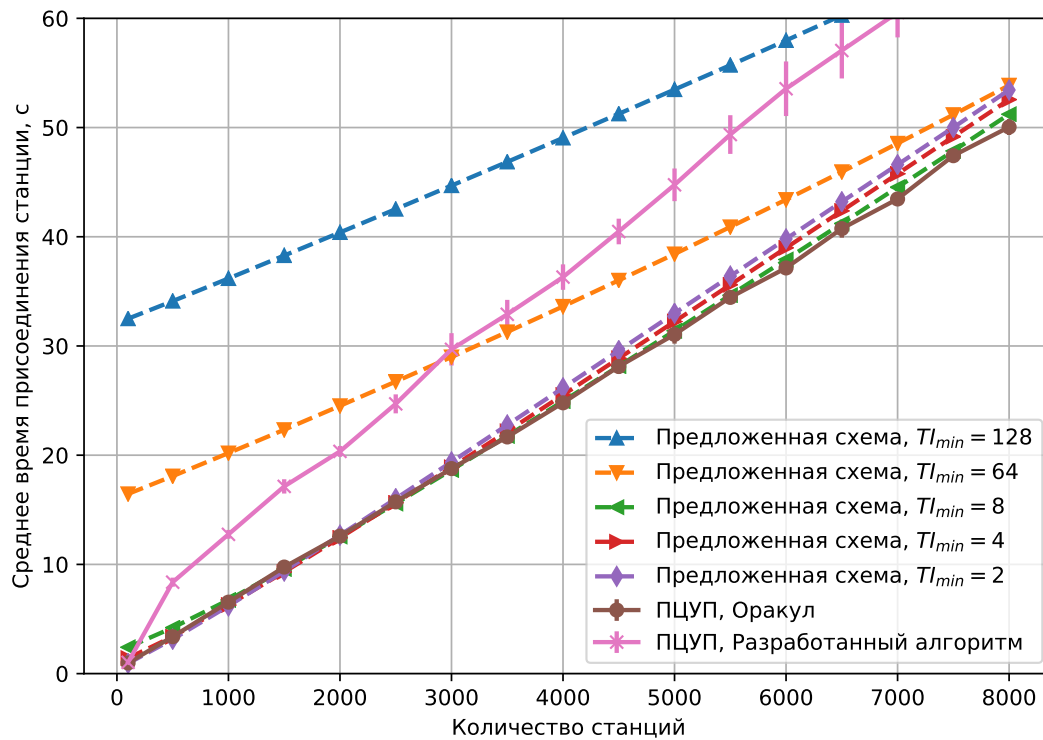


Рис. 4. Зависимость среднего времени присоединения станции от количества сенсоров

жимое при использовании протокола централизованного управления процессом присоединения.

3. Разработан и исследован при помощи имитационного моделирования в среде ns-3 алгоритм управления порогом присоединения для протокола централизованного управления процессом присоединения к сети Wi-Fi HaLow.

4. Разработана имитационная модель протокола распределённого управления процессом присоединения к сети Wi-Fi HaLow, позволяющая оценить эффективность протокола при наличии таких факторов, как эффект захвата канала и присутствие скрытых станций.

5. Разработана математическая модель протокола распределённого управления процессом присоединения к сети Wi-Fi HaLow, позволяющая оценить влияние параметров протокола на среднее время присоединения устройства к сети.

Список публикаций

1. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. LoRaWAN Modeling and MCS Allocation to Satisfy Heterogeneous QoS Requirements // Sensors. 2019. Vol. 19, no. 19. Pp. 1–23.
2. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey et al. What is the Fastest Way to Connect Stations to a Wi-Fi HaLow Network? // Sensors. 2018. Vol. 18, no. 9. Pp. 1–18.
3. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey, Stepanova Ekaterina. Fast Centralized Authentication in Wi-Fi HaLow Networks // Communications (ICC), 2017 IEEE International Conference on / IEEE. 2017. Pp. 1–6.

4. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. Mathematical Model of LoRaWAN Channel Access // A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2017 IEEE 18th International Symposium on / IEEE. 2017. Pp. 1–3.
5. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. Mathematical Model of LoRaWAN Channel Access with Capture Effect // Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on / IEEE. 2017. Pp. 1–5.
6. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. On the Limits of LoRaWAN Channel Access // Engineering and Telecommunication (EnT), 2016 International Conference on / IEEE. 2016. Pp. 10–14.
7. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. The Study of the Centralized Control Method to Hasten Link Set-up in IEEE 802.11 ah Networks // European Wireless 2015; 21th European Wireless Conference; Proceedings of / VDE. 2015. Pp. 1–6.
8. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. The Study of the Distributed Control Method to Hasten Link Set-Up in IEEE 802.11ah Networks // Problems of Redundancy in Information and Control Systems (REDUNDANCY), 2016 XV International Symposium / IEEE. 2016. Pp. 13–17.
9. Банков Дмитрий Викторович, Хоров Евгений Михайлович, Ляхов Андрей Игоревич. Исследование протокола централизованного управления процессом присоединения устройств в сетях IEEE 802.11ah // Информационные процессы. 2016. Т. 16, № 1. С. 27–40.
10. Красавина Татьяна Алексеевна, Банков Дмитрий Викторович, Хоров Евгений Михайлович. Исследование протокола распределенного управления процессом присоединения устройств при отсутствии помех в канале // Сборник трудов 39-й междисциплинарной школы-конференции ИППИ РАН «Информационные технологии и системы 2015». 2015. С. 1074–1085.
11. Степанова Екатерина Алексеевна, Банков Дмитрий Викторович, Хоров Евгений Михайлович. Исследование протокола централизованного управления процессом присоединения устройств в сетях IEEE 802.11ah при наличии интерференции // Сборник трудов 40-й междисциплинарной школы-конференции ИППИ РАН «Информационные технологии и системы 2016». 2016. С. 660–666.
12. Бабаев Алипаша Алияр оглы, Банков Дмитрий Викторович, Хоров Евгений Михайлович. Анализ эффективности метода доступа к каналу в сетях LoRaWAN // Сборник трудов 40-й междисциплинарной школы-конференции ИППИ РАН «Информационные технологии и системы 2016». 2016. С. 688–694.
13. Степанова Екатерина Алексеевна, Банков Дмитрий Викторович, Хоров Евгений Михайлович. Сравнение протоколов присоединения устройств в сетях межмашинного взаимодействия на основе технологии Wi-Fi // Сборник трудов 41-й междисциплинарной школы-конференции ИППИ РАН «Информационные технологии и системы 2017». 2017. С. 1–16.