

Анализ эффективности метода доступа к каналу в сетях NB-Fi¹

Д.В. Банков^{*,**}, П.А. Левченко^{*,***}, А.И. Ляхов^{*,**}, Е.М. Хоров^{*,**}

^{*} Институт проблем передачи информации им. А.А. Харкевича РАН, Москва

^{**} Национальный исследовательский университет «Высшая школа экономики», Москва

^{***} Московский физико-технический институт (национальный исследовательский университет),
Москва

Поступила в редколлегию 05.11.2021 г.

Аннотация—Вследствие стремительного развития Интернета вещей появляется все больше технологий энергоэффективных сетей дальнего радиуса действия. Одна из них — технология NB-Fi — принята в качестве предварительного национального стандарта Российской Федерации и планируется к широкому использованию. Однако на данный момент исследования технологии NB-Fi практически не представлены в научной литературе, и открытой задачей является исследование её возможностей, потенциальных преимуществ и недостатков. В этой работе приведен обзор протокола NB-Fi с точки зрения методов доступа к каналу. Также в работе исследована вероятность потери пакета и задержка в зависимости от интенсивности трафика, выявлены факторы, которые могут привести к снижению эффективности протокола, и предложены способы улучшения производительности сети.

КЛЮЧЕВЫЕ СЛОВА: NB-Fi, LPWAN, Интернет вещей, беспроводные сенсорные сети, метод доступа к каналу

DOI: 10.53921/18195822_2021_21_4_231

1. ВВЕДЕНИЕ

Интернет вещей стремительно развивается и с каждым годом приобретает всё большую долю во всемирной сети. Согласно прогнозам, к 2023 году половина соединений в Интернете будет относиться к межмашинному взаимодействию (англ.: Machine-to-Machine, M2M) [1] — автоматизированному обмену данных между «умными» устройствами: сенсорами, датчиками, активными элементами и сетевыми серверами, причём из этих соединений 14% будет относиться к энергоэффективным сетям дальнего радиуса действия (англ.: Low Power Wide Area Networks, LPWANs). Технологии LPWAN позволяют, хоть и с небольшой скоростью (по сравнению со скоростями, достижимыми в сотовых сетях или в сетях Wi-Fi), передавать данные большого числа устройств на большие расстояния при малых затратах мощности. Благодаря таким свойствам, технологии LPWAN рассматриваются как перспективное решение для реализации сенсорных сетей. Одной из таких технологий является технология NB-Fi.

В 2019 году стандарт протокола NB-Fi был утверждён в качестве предварительного национального стандарта Российской Федерации ПНСТ 354-2019 [2]. Протокол NB-Fi стал первым отечественным стандартизированным решением, которое планируется к широкому применению в сценариях мониторинга экологической ситуации, сбора данных для ЖКХ, городского планирования и управления инфраструктурой. Протокол NB-Fi регламентирует работу сетей LPWAN, в которых высокая дальность передачи при малом потреблении энергии достигается за счёт использования узкополосной модуляции радиосигналов, и имеет ряд сходств с

¹ Исследование осуществлено в рамках Программы фундаментальных исследований НИУ ВШЭ.

протоколами таких известных технологий LPWAN, как Sigfox [3, 4] и LoRaWAN [5, 6]. Однако протокол NB-Fi имеет и множество отличительных особенностей, из-за которых большая часть результатов исследований, посвящённых другим LPWAN-технологиям, неприменима для сетей NB-Fi, а подробных исследований протокола NB-Fi в научной литературе не представлено — NB-Fi упоминался ранее только в обзорных статьях, например [7, 8]. В то же время, поскольку планируется массовое применение сетей NB-Fi в народном хозяйстве, задача исследования и оптимизации протокола NB-Fi является актуальной.

В данной работе протокол NB-Fi исследуется с точки зрения эффективности метода доступа к каналу: рассматриваются особенности, которые могут повлиять на пропускную способность сети и вероятность потери пакета, выделяются «узкие места», и предлагаются решения для того, чтобы избежать потери эффективности.

Дальнейшее изложение построено следующим образом. В разделе 2 приводится описание протокола NB-Fi. В разделе 3 описывается исследуемый сценарий работы сети NB-Fi. В разделе 4 приведены результаты моделирования сети NB-Fi и их анализ. Заключение работы содержится в разделе 5.

2. ОПИСАНИЕ ПРОТОКОЛА

Беспроводные сети стандарта NB-Fi являются сетями класса LPWAN, которые характеризуются высокой энергоэффективностью передачи данных и высокой емкостью сети. Технология NB-Fi создана для работы в нелицензируемых диапазонах частот, в которых установлены ограничения на излучаемую мощность, например, в диапазоне 868,7–869,2 МГц, где максимальная излучаемая мощность составляет 100 мВт.

Сеть NB-Fi состоит из оконечных устройств, базовых станций и единого сервера. Передача данных между базовыми станциями и оконечными устройствами осуществляется через беспроводной канал по протоколу NB-Fi. По стандарту базовые станции обязаны осуществлять приём и передачу многих сигналов одновременно и принимать сигналы на любых частотах в пределах рабочей полосы частот. В то же время, базовые станции соединены с сервером через широкополосный канал связи.

2.1. Модуляция

В сетях NB-Fi используется относительная двоичная фазовая манипуляция несущей для пакетов восходящего направления (UPLINK-пакетов) и относительная двоичная фазовая манипуляция несущей или двоичная фазовая манипуляция несущей для пакетов нисходящего направления (DOWNLINK-пакетов).

Сигналы можно передавать с четырьмя разными скоростями: 50, 400, 3200 и 25600 бит/с. В силу соотношения неопределенности сигналы, передаваемые на разных скоростях, будут занимать разный диапазон по частоте, иметь разные мощности сигналов, при которых возможен приём, и, соответственно, разные максимальные дальности передачи.

Предельная чувствительность приёма в зависимости от скорости передачи показана в табл. 1. Значения чувствительности (S_{crit}) определяются как

$$S_{crit} = 10 \log_{10} kT\Delta f + N_{base} + SNR_{BER}, \quad (1)$$

где N_{base} — входной коэффициент шума, SNR_{BER} — отношение сигнал-шум для заданной частоты ошибок по битам (англ.: bit error rate, BER), k — постоянная Больцмана, T — температура, Δf — ширина полосы частот, занимаемая сигналом. Таким образом, подставив значения: $T = 290\text{К}$, $BER = 10^{-5}$, $SNR_{BER} = 5$ дБ, $N_{base} = 2$ дБ, получим предельную чувствительность приёма для разных скоростей передачи.

Таблица 1. Предельная чувствительность приёма.

Скорость передачи, бит/с	Предельная чувствительность приёма, дБм
50	-150
400	-141
3200	-132
25600	-123

2.2. Режимы работы

Конечные устройства NB-Fi могут работать в трёх режимах работы. При использовании режима без приема (англ.: No RX) устройство передает данные при необходимости, остальное время устройство находится в режиме «сон». При этом, устройства не могут принимать данные. При работе в режиме прерывистого приёма (англ.: Discontinuous RX) устройство передает данные при необходимости и переходит в режим приёма на непродолжительное время сразу после окончания передачи. Сервер буферизирует все запросы на отправку данных устройству и выполняет передачу данных во время «открытия» временного «окна», когда устройство переходит в режим приёма. При использовании режима непрерывного приёма (англ.: Continuous RX) устройство передает данные при необходимости, в остальное время находится в режиме приёма.

2.3. Формат кадра

Данные от оконечных устройств к базовой станции передаются в UPLINK-пакетах. Рассмотрим формат UPLINK-пакета. Он начинается (см. рис. 1) с преамбулы длиной 4 байта, которая служит для обнаружения пакета. В восходящем направлении преамбула фиксирована для всех устройств и в шестнадцатеричном виде равна 0x97157A6F.

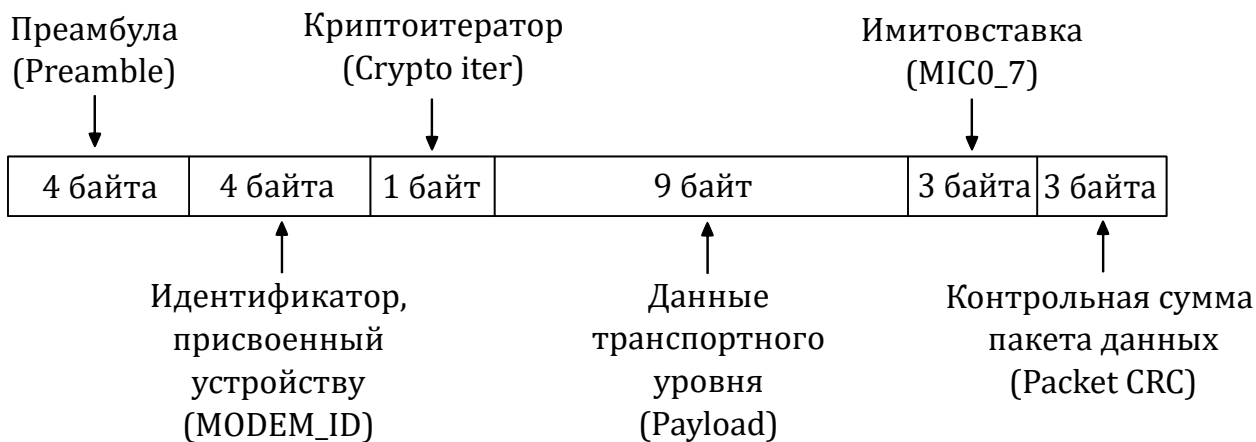


Рис. 1. Структура UPLINK-пакета.

Далее следуют данные, закодированные помехоустойчивым кодом. Стандарт NB-Fi предусматривает использование несистематических полярных и сверточных кодов со скоростью кодирования 5/8 для UPLINK-пакетов.

Входные данные для кодера, имеющие размер 20 байт, начинаются с 32 бит Modem_ID — идентификатора, присвоенного устройству. Далее следует восьмибитное поле Crypto Iter (криптоитератор), используемое для реализации механизма защиты данных, поле Payload (данные транспортного уровня) длиной 9 байт, поле MIC0_7 (младшие 3 байта имитовставки), необходимое для реализации механизма защиты данных и выбора центральной частоты передачи в восходящем направлении. Имитовставка вычисляется при помощи алгоритма

симметричного блочного шифрования «Магма» на основе зашифрованных полей Modem_ID, Crypto Iter, Payload. После этого идёт поле Packet CRC (контрольная сумма пакета данных) длиной 24 бита. Итоговый размер данных, закодированных помехоустойчивым кодом, равен 32 байтам.

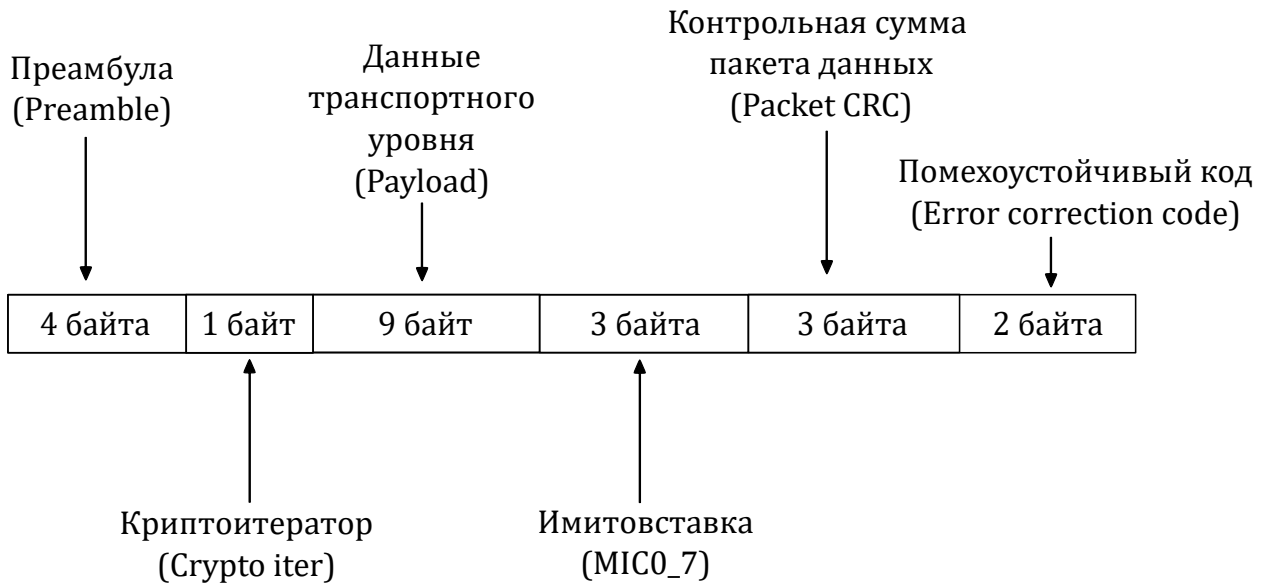


Рис. 2. Структура DOWNLINK-пакета.

Данные от базовой станции к конечным устройствам передаются в DOWNLINK-пакетах. В отличие от UPLINK-пакета, в DOWNLINK-пакете отсутствует идентификатор устройства. Также в DOWNLINK-пакетах преамбула не фиксирована, а вычисляется по алгоритму, основанному на итерационной генерации псевдослучайных чисел с идентификатором модема в качестве стартовой позиции генератора. После преамбулы передаются криптоитератор, данные транспортного уровня, имитовставка и контрольная сумма пакета данных. Все эти поля (кроме преамбулы) служат входными данными для кодера: в нисходящем направлении используется ZIGZAG-код со скоростью кодирования 1/2. В конце DOWNLINK-пакета передаются проверочные биты ZIGZAG-кода. Структура кадра показана на рис. 2.

2.4. Метод доступа к каналу

Сети NB-Fi работает с нелицензируемыми частотами. Для восходящего направления по стандарту должна быть выделена рабочая полоса шириной не менее 51,2 кГц, а для нисходящего направления — не менее 102,4 кГц. Каждому устройству назначается центральная частота в нисходящем направлении, которая зависит от скорости и идентификатор устройства. Центральная частота для передачи в восходящем направлении выбирается при каждой передаче (в том числе и повторной) и зависит от скорости, идентификатора устройства и MIC0_7. Рассмотрим подробнее метод выбора центральной частоты передачи в восходящем направлении.

Частота передачи UPLINK-пакета равна:

$$F_{UL} = \begin{cases} F_{base} + O_{UL,band} + O_{UL,channel}, & id \bmod 2 = 1, \\ F_{base} + O_{UL,band} - O_{UL,channel}, & id \bmod 2 = 0, \end{cases} \quad (2)$$

где id — идентификатор устройства, F_{base} — базовая частота передачи UPLINK-пакетов, $O_{UL,band}$ — смещение рабочей полосы частот относительно базовой, и $O_{UL,channel}$ — смещение несущей

частоты, которое зависит от содержания пакета. Последние две величины зависят от набора параметров.

Смещение рабочей полосы частот относительно базовой вычисляется по формуле:

$$O_{UL,band} = BW_{UL} \times O_{UL} \times S_{UL}, \tag{3}$$

где $BW_{UL} = 6400 \times 2^{W_{UL}}$, а O_{UL} , S_{UL} , W_{UL} — заданные параметры, обозначающие, соответственно, значение и направление смещения рабочей полосы передачи UPLINK-пакетов, относительно базовой частоты и ширину рабочей полосы передачи UPLINK-пакетов. Их характерные значения: $W_{UL} = 0, \dots, 7$, $O_{UL} = 0, \dots, 63$, $S_{UL} = \pm 1$.

Смещение несущей частоты заданного пакета вычисляется по формуле:

$$O_{UL,channel} = \frac{((id + MIC0_7) \bmod 256) \times G_{UL}}{255}, \tag{4}$$

где G_{UL} — полоса перестройки несущей частоты передачи UPLINK-пакетов, которая в зависимости от скорости передачи (BR) равна:

$$G_{UL} = \begin{cases} \frac{BW_{UL} - 2 \times BR - 2000}{2}, & \text{если } BW_{UL} > BR \times 2 + 2000, \\ G_{UL} = 0, & \text{если } BW_{UL} \leq BR \times 2 + 2000. \end{cases} \tag{5}$$

Таким образом, получаем метод вычисления центральной частоты передачи в восходящем направлении. Центральная частота в нисходящем направлении вычисляется аналогичным образом с одним изменением: отсутствует $MIC0_7$, поэтому центральная частота остаётся неизменной для всех передач одного устройства в нисходящем направлении.

2.5. Механизм подтверждения доставки пакета и повторной отправки

В технологии NB-Fi предусмотрен режим группового подтверждения доставки данных. Если он выключен, то кадры отправляются без подтверждения. В противном случае, в зависимости от выбранного режима, подтверждение должно поступать на каждый 2^n -й кадр, где $n = 0, \dots, 5$.

Данные транспортного уровня (см. рис. 3) содержат в себе заголовок (1 байт) и непосредственно полезные данные (8 байт). Заголовок состоит из четырех флагов: SYS, предназначенный для обозначения системных пакетов; ACK, информирующий о необходимости подтверждения пакета; MULTI, необходимый для групповой отправки и сигнализирующий, что вслед за этим пакетом будет отправлен следующий; ITER, изменяющийся в диапазоне 0-31 и информирующий о номере пакета в группе.

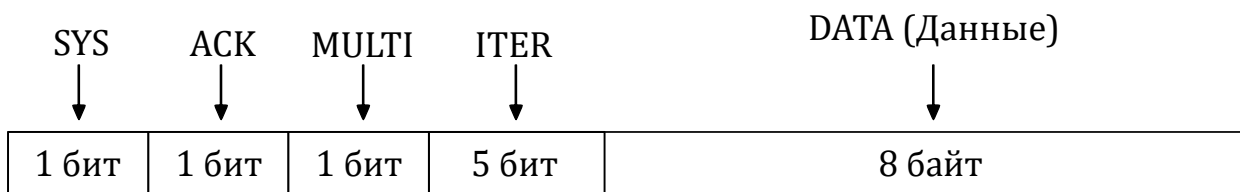


Рис. 3. Структура данных транспортного уровня.

При групповой отправки в последнем пакете из группы должен быть выставлен флаг ACK в заголовке пакета. Данный флаг сигнализирует, что необходимо в ответ отправить системный пакет ACK_P, где должны быть указаны номера полученных пакетов. Далее передающий

Таблица 2. Интервал для повторной передачи кадра.

Скорость передачи, бит/с	T_{delay} , мс	T_{listen} , мс	T_{rnd} , мс
50	5900	60000	5000
400	740	30000	1000
3200	95	6000	100
25600	15	6000	100

узел должен обработать пакет ACK_P и повторно отправить кадры, которые не были получены приёмником.

Если пакет ACK_P не был получен, то осуществляется повторная передача кадров в случайный момент времени в интервале:

$$(T_{delay} + T_{listen}; T_{delay} + T_{listen} + T_{rnd}), \quad (6)$$

где T_{delay} , T_{listen} и T_{rnd} зависят от скорости передачи в восходящем направлении. Их значения представлены в табл. 2. Стоит отметить, что параметры повторных передач кадров подобраны таким образом, что в случае коллизии кадра, передаваемого на скорости 50 бит/с с кадром, передаваемым на какой-либо другой скорости, повторная коллизия невозможна. Аналогично для кадра, передаваемого на скорости 400 бит/с.

Вновь обратим внимание на структуру UPLINK-пакета (см. рис. 1). Центральная частота передачи зависит от имитовставки и фиксированного идентификатора устройства. Имитовставка вычисляется следующим образом: сначала шифруются данные, а далее формируется имитовставка от них. Соответственно, так как при повторной передаче криптоитератор увеличивается, то меняется и имитовставка, а значит и выбирается новая центральная частота для передачи. Таким образом, повторная передача данных выполняется на частоте, отличной от частоты, на которой проводилась предыдущая попытка.

2.6. Алгоритм выбора скорости и мощности передачи

Устройства, работающие в режимах прерывистого и непрерывного приёма, должны оценивать качество радиосигнала и автоматически регулировать скорость и мощность передачи для UPLINK и DOWNLINK-пакетов. Решение о смене скорости и мощности передачи принимает оконечное устройство, которое оценивает соотношение сигнал-шум для DOWNLINK-пакетов непосредственно при их приёме, а для UPLINK-пакетов на основе информации от базовой станции из полей пакета ACK_P .

При достаточно высоком значении отношения сигнал-шум (больше либо равном $SNR_{UP} + SNR_{TX}$ для передачи в восходящем направлении и больше либо равном $SNR_{UP} + SNR_{RX}$ для передачи в нисходящем направлении) оконечное устройство должно выполнять перевод скорости на один уровень выше. Параметры SNR_{TX} и SNR_{RX} зависят от скорости передачи, их значения приведены в табл. 3. $SNR_{UP} = 15$ дБ для всех скоростей. Поскольку базовая станция обязана принимать сигналы на любой скорости, то смена скорости в восходящем направлении осуществляется без уведомления об этом сервера. При смене скорости передачи в нисходящем направлении устройство должно выполнить передачу системного пакета, содержащего параметры нового скоростного режима, с выставленным флагом ACK, означающим необходимость подтверждения приёма пакета. Кадр подтверждения должен быть отправлен на новой скорости. Если при смене скорости после определенного числа повторных попыток кадр с подтверждением не был получен, то устройство возвращает прежнюю скорость и осуществляет отправку системного кадра, не ожидая подтверждения. Скорость должна повышаться до тех пор, пока соотношение сигнал-шум не достигнет значения, не позволяющего выполнять повышение скорости, либо пока не будет достигнуто максимальное значение скорости.

Таблица 3. Пороговые значения соотношения сигнал-шум.

Скорость передачи, бит/с	SNR_{RX} , дБ	SNR_{TX} , дБ
50	0	0
400	9	9
3200	18	18
25600	27	27

Если при достижении максимального значения скорости соотношение сигнал-шум имеет достаточно высокое значение (больше либо равное $SNR_{UP} + SNR_{TX}$ для передачи пакетов в восходящем направлении и больше либо равное $SNR_{UP} + SNR_{RX}$ — в нисходящем), то выполняется постепенное снижение выходной мощности передатчика устройства (с шагом 3 дБ) для восходящего направления или посылается системный пакет с уведомлением о необходимости снижения выходной мощности передатчика базовой станции.

Если уровень соотношения сигнал-шум снижается ниже порогового значения ($SNR_{DOWN} = 10$ дБ), то выполняются обратные действия: сначала повышается выходная мощность передатчиков устройства или базовой станции, затем выполняется ступенчатое снижение скорости передачи, либо приема данных.

Механизм автоматического подбора скоростного режима и мощности передатчика может быть отключен.

3. ИССЛЕДУЕМЫЙ СЦЕНАРИЙ

Рассмотрим следующий сценарий работы сети NB-Fi. Сеть состоит из сервера, одной базовой станции и 1000 оконечных устройств, которые распределены равномерно в круге радиуса 1 км, в центре которого находится базовая станция. Устройства работают в режиме прерывистого приёма и передают пакеты на сервер. Пакеты на устройствах генерируются в соответствии с потоком Пуассона. В нисходящем направлении трафик отсутствует кроме пакетов с подтверждениями, которые отправляются на каждый полученный пакет данных от оконечных устройств. Скорости передачи назначаются устройствам при их инициализации, кадры подтверждения передаются на тех же скоростях, что и пакеты в восходящем направлении. На устройствах присутствует буфер, вмещающий один пакет. Если во время передачи пакета на устройстве генерируется новый пакет, то в случае неудачной попытки передачи пакет отбрасывается и устройство переходит к обработке нового пакета. Также если новый пакет генерируется, когда в буфере уже есть пакет, то старый пакет из буфера отбрасывается. Максимальное количество повторных попыток передачи одного кадра равно 7. Длина всех пакетов одинаковая и равна 288 битам. Длительность кадров для разных скоростей приведена в табл. 4.

Таблица 4. Длительность кадров.

Скорость передачи, бит/с	Длительность пакета, мс
50	5760
400	720
3200	90
25600	11,25

Устройства передают с мощностью 25 мВт. Для вычисления затухания мощности сигнала используется модель Окамуры-Хата. При рассматриваемых расстояниях мощность сигналов от сенсоров на базовой станции оказывается выше предельных значений, указанных в табл. 1. Передаваемый пакет принимается успешно, если соотношение мощности сигнала к мощности интерферирующих сигналов и шума в используемой полосе частот в течение передачи всего пакета оказывается выше 7 дБ (2 дБ — входной коэффициент шума базовой станции равен,

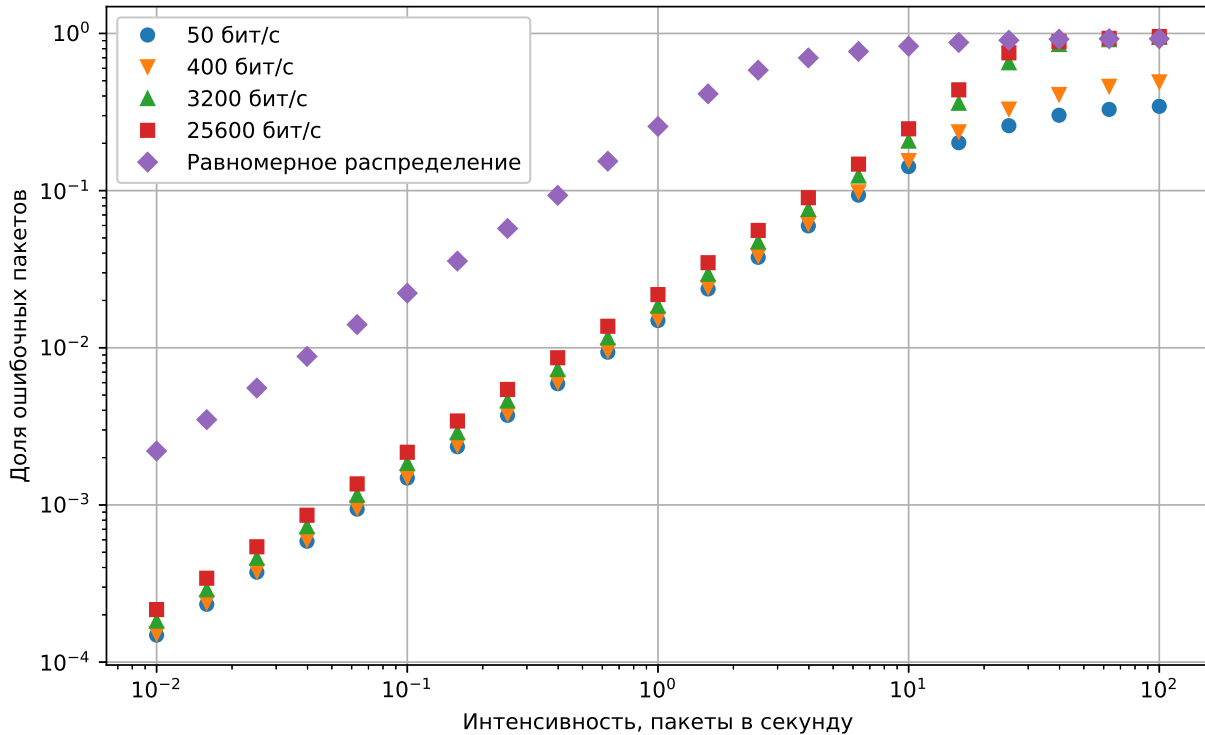


Рис. 4. Зависимость доли ошибочных пакетов от интенсивности трафика.

5 дБ — соотношение сигнал-шум для частоты ошибок по битам, при которой считается, что сигнал принимается достаточно надежно). При этом пренебрегаем потерями, вызванными случайными шумами — пакеты могут быть приняты неудачно только из-за коллизий с другими пакетами.

4. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

Для описанного сценария была реализована имитационная модель для исследования следующих показателей: доля ошибочных пакетов (англ.: packet error rate — PER), доля потерянных пакетов (англ.: packet loss rate — PLR) и средняя задержка в зависимости от интенсивности генерации кадров. Доля ошибочных пакетов — вероятность того, что передача пакета окажется неуспешной из-за того, что сам пакет не принят базовой станцией, или не было доставлено подтверждение на него от базовой станции. Доля потерянных пакетов — вероятность того, что сгенерированный пакет не будет доставлен, потому что либо было достигнуто максимальное число повторов, либо был сгенерирован новый пакет.

На рис. 4 показана зависимость PER от суммарной интенсивности трафика всех устройств для пяти разных способов назначения скоростей: в четырех случаях всем устройствам назначается одинаковая скорость, в пятом — скорости распределяются равномерно. Для интенсивностей меньше 1 с^{-1} , PER имеет практически одинаковые значения для сценариев, в которых все устройства передают с одинаковой скоростью. Схожесть значений объясняется тем, что при малых интенсивностях трафика PER практически полностью определяется вероятностью успеха при первой попытке передачи пакета, которая зависит от вероятности пересечения кадров по времени и по частоте. В случае, когда все устройства в сети передают на одинаковой скорости, эта вероятность практически не зависит от конкретной скорости передачи, потому что длительность кадра обратно пропорциональна ширине кадра по частоте. Таким образом,

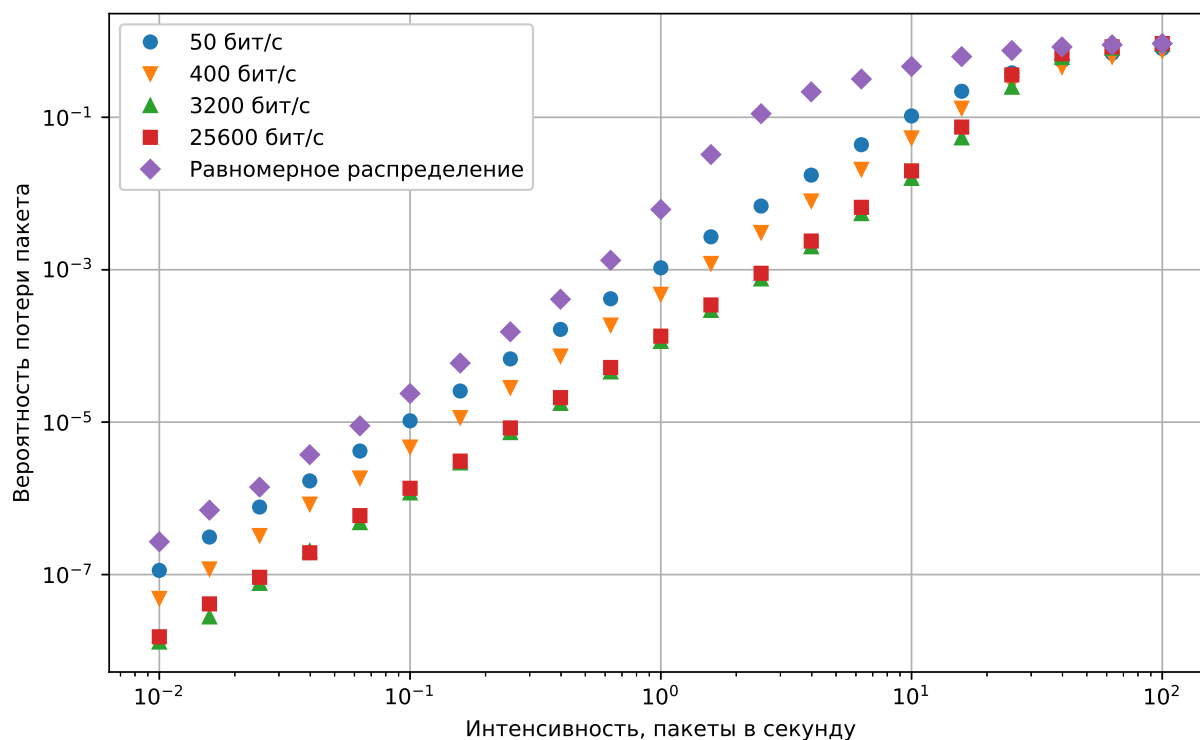


Рис. 5. Зависимость доли потерянных пакетов от интенсивности трафика.

при передаче на одинаковой скорости, чем больше вероятность пересечения кадров по времени, тем меньше вероятность их пересечения по частоте и наоборот. В то же время, если устройства в сети передают кадры на разных скоростях, то у них уже нет возможности компенсировать высокую вероятность пересечения по времени за счёт низкой вероятности пересечения по частоте и наоборот — поэтому PER для равномерного распределения скоростей намного выше, чем для случаев, когда все устройства в сети используют одну скорость. При большой интенсивности трафика оказывается, что PER ниже для низких скоростей. Это объясняется тем, что при большой интенсивности трафика вероятность пересечения кадров по времени очень близка к единице и вероятность коллизии определяется вероятностью того, что кадры разных устройств будут передаваться на разных частотах, и эта вероятность тем выше, чем ниже скорость.

Стоит отметить такой важный фактор, влияющий на PER, как доставка подтверждений. Частота для передачи в нисходящем направлении не зависит от передаваемого кадра и определяется идентификатором устройства, как описано в разделе 2.4. Если устройств в сети много, может возникнуть ситуация, когда базовой станции надо отправить подтверждения разным устройствам на пересекающихся частотных интервалах. В этом случае передача подтверждений некоторым устройствам может быть отложена, и если задержка отправки подтверждения превосходит время ожидания (T_{listen} в табл. 2), то подтверждение не будет доставлено. Возможным способом решения данной проблемы может быть отправление подтверждений не на каждый кадр, а на каждый 2^n -й кадр, как описано в разделе 2.5. При этом выбор значения n является открытой задачей и требует дополнительных исследований: увеличивая n можно снизить интенсивность трафика в нисходящем потоке, однако при этом возрастает задержка.

Рассмотрим зависимость вероятности потери пакета от интенсивности трафика (см. рис. 5). В отличие от PER, при малой интенсивности трафика PLR для разных скоростей получается

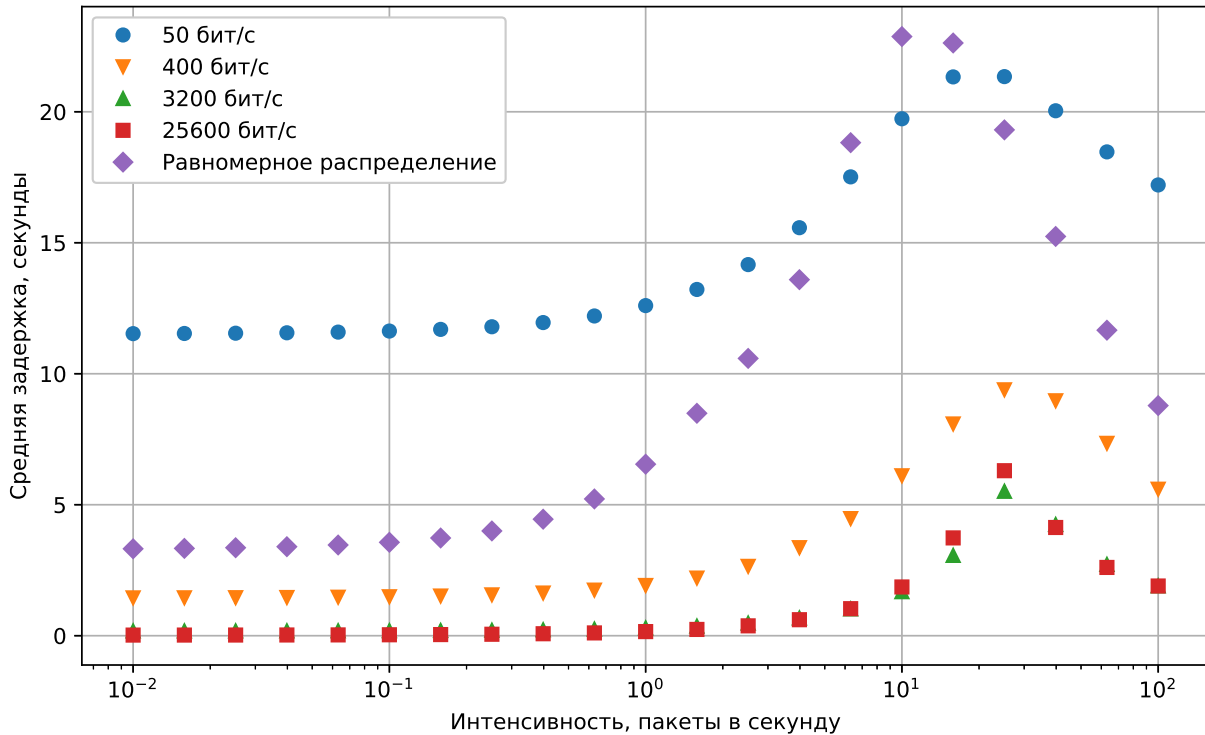


Рис. 6. Зависимость средней задержки от интенсивности трафика.

разным: самый низкий PLR получается для скоростей 25600 бит/с и 3200 бит/с. PLR определяется вероятностью того, что устройство отбросит пакет, что может произойти по достижении максимального числа повторных попыток передачи пакета или из-за генерации нового пакета за время передачи текущего пакета. PLR зависит от вероятности успеха при попытке передачи кадра, длительности кадра и времени ожидания перед повторной попыткой передачи. Чем дольше кадр и время ожидания повторной попытки, тем больше вероятность, что за время его передачи сгенерируется новый кадр и старый будет отброшен в случае неудачной попытки — это объясняет соотношение PLR для разных скоростей.

В отличие от PER, определяемого в основном вероятностью успешной передачи при первой попытке, на PLR большое влияние оказывает вероятность успеха при повторной попытке передачи. Часть повторных попыток передачи представляют собой попытки разрешения коллизии двумя и более устройствами. На вероятность успеха при таких повторных попытках влияет ширина кадра по частоте, а также отношение длительности кадра к длительности интервала, в котором устройство выбирает случайное время ожидания перед повторной попыткой (T_{rnd} в табл. 2). Обратим внимание на последнюю величину:

1. для скорости 50 бит/с отношение составляет 1,152,
2. для скорости 400 бит/с отношение составляет 0,72,
3. для скорости 3200 бит/с отношение составляет 0,9,
4. для скорости 25600 бит/с отношение составляет 0,1125.

Как видно, при скоростях 50 бит/с, 400 бит/с и 3200 бит/с данное отношение близко к единице. Это означает, что при коллизии двух кадров повторное пересечение кадров по времени произойдет с большой вероятностью, то есть рандомизация времени повторной передачи делается неэффективно. При этом у устройств есть возможность разрешить коллизию за счёт передачи

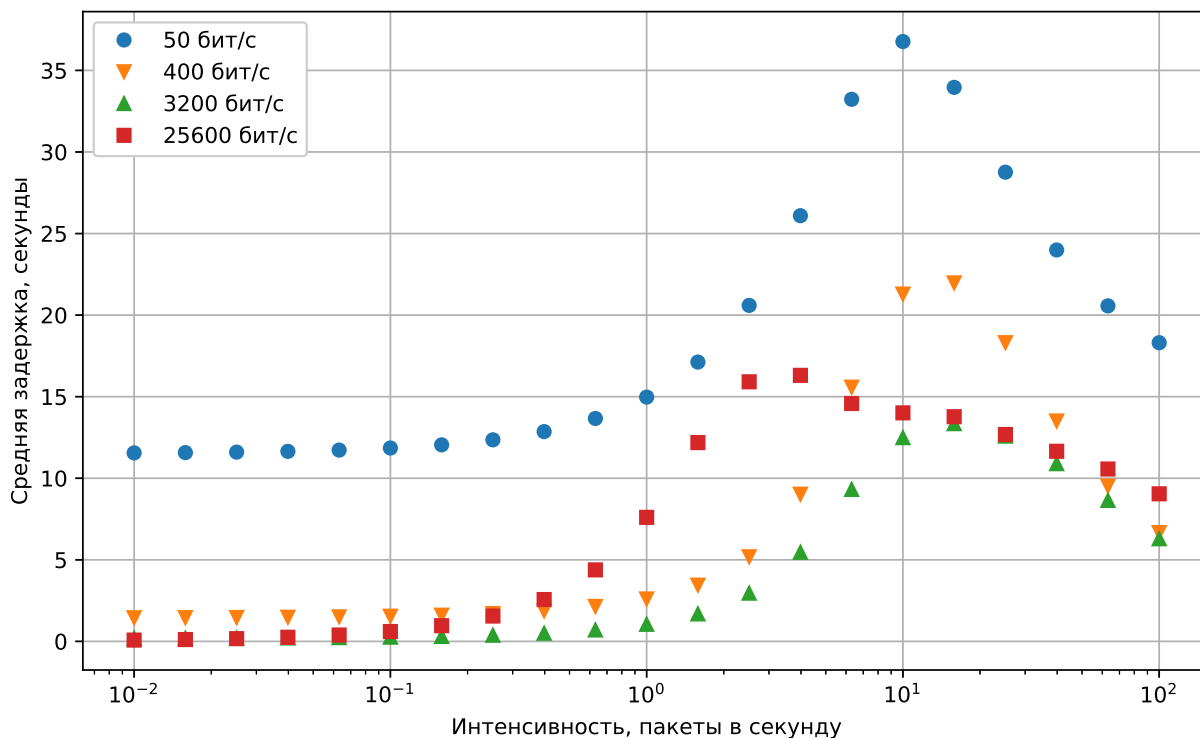


Рис. 7. Зависимость средней задержки от интенсивности трафика для равномерного распределения скоростей.

на разных частотах, однако возможно, что, выбирая ширину интервала T_{rnd} , можно было бы снизить PLR — данный вопрос требует дополнительных исследований.

Наконец, рассмотрим зависимость средней задержки при передаче пакета от интенсивности трафика (см. рис. 6). При малых интенсивностях задержка в первую очередь определяется круговой задержкой, обратно пропорциональной величине скорости. При увеличении интенсивности количество повторных попыток передачи, необходимых для доставки пакета, становится больше, следовательно, заметно увеличиваются задержки до некоторого максимального значения, после которого начинается спад, связанный с высокой долей потерь пакетов из-за того, что новые пакеты вытесняют старые — пакеты чаще всего либо доходят с небольшим числом повторных попыток, либо отбрасываются и не учитываются при подсчёте средней задержки.

На рис. 7 отдельно показана средняя задержка для каждой скорости в сценарии равномерного распределения скоростей. Задержки для каждой скорости при равномерном распределении значительно больше, чем при использовании только одной скорости вследствие большого PER для равномерного распределения. Заметим, что при низкой интенсивности трафика большей скорости соответствует меньшая средняя задержка, однако при интенсивности трафика порядка 1 с^{-1} соотношение средней задержки для скоростей 400, 3200 и 25600 бит/с изменится. Данный факт объясняется тем, что на среднюю задержку влияют как длительность передачи пакета, так и PER. При низкой интенсивности трафика PER мал и наибольший вклад в задержку вносит длительность передачи пакета, однако с ростом нагрузки PER тоже растёт, что приводит к тому, что средняя задержка для 25600 бит/с становится выше, чем для 3200 бит/с и 400 бит/с. При дальнейшем повышении интенсивности, выше 6 с^{-1} , начинает играть роль то, что в рассматриваемом сценарии при неудачной попытке передачи пакета и

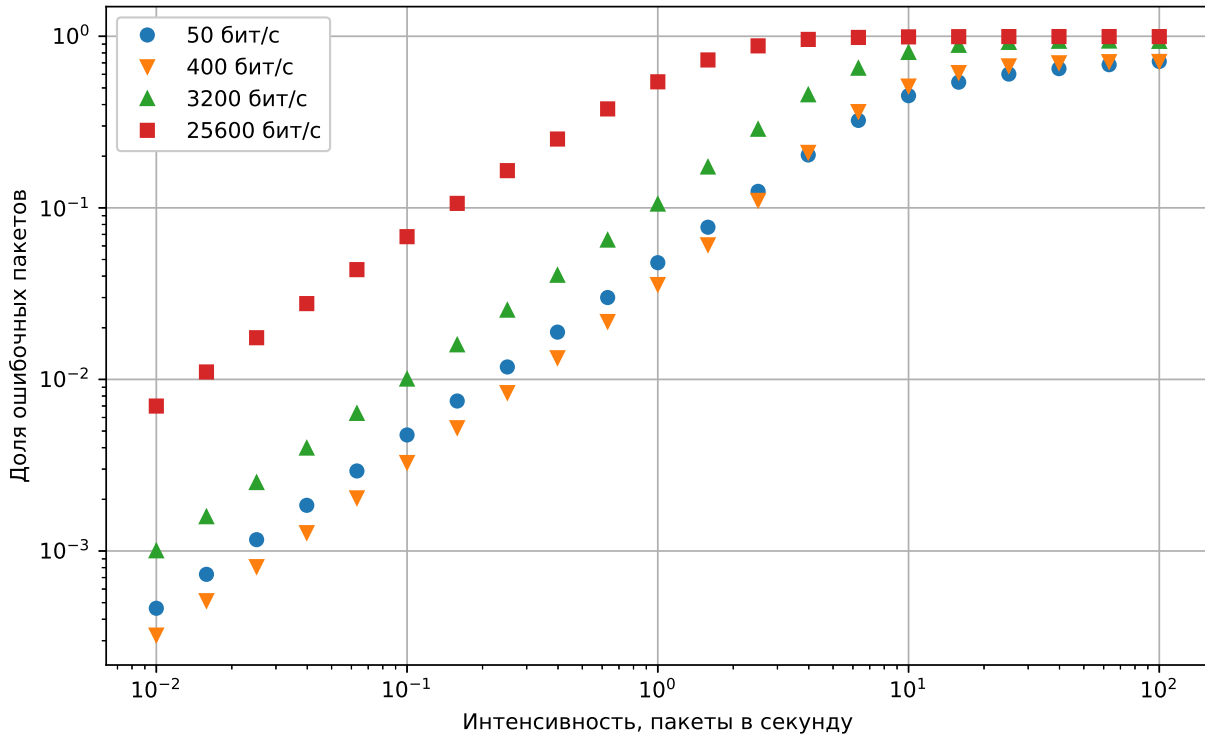


Рис. 8. Зависимость доли ошибочных пакетов от интенсивности трафика для равномерного распределения скоростей.

поступлении нового пакета, старый пакет отбрасывается и не учитывается при расчёте средней задержки. Отметим, что при равномерном распределении скоростей PER (см. рис. 8), соответствующий разным скоростям, получается разным. Наибольший PER соответствует самой высокой скорости, потому что широким по частоте кадрам соответствует большая вероятность пересечения с каким-либо другим кадром. В то же время, самый низкий PER наблюдается для скорости 400 бит/с, а не для скорости 50 бит/с, потому что при самой низкой скорости кадры имеют большую длительность и вероятность того, что за длительность кадра будет передан ещё какой-то кадр, пересекающийся с текущим, получается более высокой, чем для 400 бит/с.

Подводя итог полученным результатам, можно сделать следующие выводы. С точки зрения PLR и задержки, эффективнее всего использовать наиболее быстрые скорости: 25600 бит/с или 3200 бит/с, а одновременное использование разных скоростей в одной сети приводит к увеличению PLR, PER и задержки. В то же время, возможны ситуации, когда устройства вынуждены использовать более низкие скорости передачи, например, при плохих канальных условиях. В таких случаях было бы эффективно вводить дополнительное разделение по частотам для разных скоростей передачи, чтобы избежать пересечения сигналов на разных скоростях.

5. ЗАКЛЮЧЕНИЕ

В данной работе была рассмотрена технология NB-Fi, приведено описание протокола и для сценария с одной базовой станцией получены зависимости доли ошибочных пакетов, вероятности потери пакета и средней задержки при передаче данных от интенсивности общего трафика. Анализ численных результатов моделирования выявил несколько потенциальных факторов, снижающих эффективность работы сети, таких как пересечение сигналов на разных скоростях, потери подтверждений из-за недостаточной пропускной способности канала

в нисходящем потоке и из-за случайного пересечения частотных диапазонов, неэффективно подобранные интервалы, из которых выбирается случайное время для повторной попытки передачи. В дальнейшем планируется проведение исследований для решения данных проблем, разработка математических моделей сетей NB-Fi и алгоритмов выбора параметров с целью повышения эффективности сетей NB-Fi.

6. БЛАГОДАРНОСТИ

Авторы выражают благодарность Андрею Олеговичу Орлову, руководителю отдела цифровой обработки сигналов ООО «Телематические Решения», за консультацию по поводу протокола NB-Fi.

СПИСОК ЛИТЕРАТУРЫ

1. Cisco Annual Internet Report (2018–2023) White Paper. — 2020. — Access mode: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html> (online; accessed: 1 November 2021).
2. ПНСТ 354-2019. Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi) : 2019.
3. Goursaud Claire, Gorce Jean-Marie. Dedicated networks for IoT: PHY/MAC state of the art and challenges // EAI endorsed transactions on Internet of Things. — 2015.
4. Overview of cellular LPWAN technologies for IoT deployment: Sigfox, LoRaWAN, and NB-IoT / Mekki Kais, Bajic Eddy, Chaxel Frederic, and Meyer Fernand // 2018 IEEE international conference on pervasive computing and communications workshops (percom workshops) / IEEE. — 2018. — P. 197–202.
5. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. On the Limits of LoRaWAN Channel Access // Engineering and Telecommunication (EnT), 2016 International Conference on / IEEE. — 2016. — P. 10–14.
6. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. LoRaWAN modeling and MCS allocation to satisfy heterogeneous QoS requirements // Sensors. — 2019. — Vol. 19, no. 19. — P. 4204.
7. Low Power Wide Area Network Technologies for Smart Cities Applications / Pham Tung Lam, Nguyen Hoan, Nguyen Huy, Bui Van, and Jang Yeong Min // 2019 International Conference on Information and Communication Technology Convergence (ICTC) / IEEE. — 2019. — P. 501–505.
8. The IIoT/IoT device control model based on narrow-band IoT (NB-IoT) / Petrenko Alexey S, Petrenko Sergei A, Makoveichuk Krystina A, and Chetyrbok Petr V // 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) / IEEE. — 2018. — P. 950–953.

Performance Evaluation of Channel Access in NB-Fi Networks

Bankov D.V., Levchenko P.A., Lyakhov A.I., Khorov E.M.

The rapid growth of the Internet of Things gives rise to numerous Low Power Wide Area Network technologies, one of which — the NB-Fi technology — has been approved as a Preliminary National Standard of the Russian Federation and is planned for wide application. However, the scientific literature contains very few studies of NB-Fi, and the investigation of the possibilities and potential advantages and disadvantages of NB-Fi is an open issue. This paper provides a tutorial of the NB-Fi protocol with a focus on channel access methods. Also, the paper evaluates how the packet loss rate and delay depend on the network load, points out the factors that can reduce the protocol efficiency, and proposes some approaches to improve the NB-Fi network performance.

KEYWORDS: NB-Fi, LPWAN, Internet of Things, Wireless Sensor Networks, Channel Access