Расчет сетей беспроводного доступа IEEE 802.11 для пассажиров поездов

П. А. Плеханов

Петербургский государственный университет путей сообщения Императора Александра I

pavelplekhanov@gmail.com

Ю. Е. Арнадская

Петербургский метрополитен

arnadskaya@gmail.com

***Аннотация*. Представлено техническое описание стандартов беспроводного доступа IEEE 802.11 (Wi-Fi). Рассмотрены вопросы расчета сетей IEEE 802.11 (Wi-Fi) для обеспечения пассажиров поездов беспроводным доступом в Интернет.**

Ключевые слова: беспроводной доступ, IEEE 802.11, Wi-Fi, точка доступа, пассажирский поезд

I. Описание стандартов беспроводного доступа IEEE 802.11 (Wi-Fi)

Беспроводная связь на железнодорожном транспорте необходима не только для организации технологической голосовой связи работников и передачи данных управления движением, но также для обеспечения пассажиров привычными услугами подвижной связи, включая доступ в Интернет [1].

Учитывая планы по созданию в стране сети высокоскоростных железнодорожных магистралей со скоростями движения до 400 км/ч, для организации пассажирской связи будут требоваться специальные технические решения, в качестве которых сегодня рассматриваются технологии подвижной связи 5G/6G, спутниковой связи, а также Radio-Ethernet [2, 3]. При этом, наряду с решением вопроса организации радиоканала между движущимся поездом и инфраструктурой, немаловажной является оптимальная организация сети беспроводного доступа для пассажиров в вагонах, в том числе, за счет современных технологий беспроводных локальных сетей WLAN (Wireless Local Area Network) Wi-Fi на основе стандартов IEEE 802.11 (таблица) [4–6].

Таблица. Характеристика стандартов беспроводного доступа IEEE 802.11 (Wi-Fi)

Поколения Wi-Fi	Основные стандарты IEEE	Год принятия	Частотные диапазоны, ГГц	Максимальная скорость передачи данных (1), Гбит/с	Базовые технологии (2)
0	802.11	1997	2,4	0,002	DSSS (3) / FHSS (4)
1	802.11b	1999		0,011	DSSS
2	802.11a		5	0,054	OFDM (5)
3	802.11g	2003	2,4		
4	802.11n	2009	2,4 / 5	0,6	OFDM, MIMO (6)
5	802.11ac	2013	5	6,77	
6	802.11ax	2019	2,4 / 5 / 6	11	
7	802.11be	2024		23	
8	802.11bn	Ожидается 2028		Ожидается 100	В разработке

Примечания.
(1) Существенно зависит от используемой полосы частот и условий передачи (наличие помех, расстояние между передатчиком и приемником и т.д.)
(2) Изначально технология Wi-Fi (как и Ethernet на основе стандартов IEEE 802.3) основана на использовании метода множественного доступа с опознаванием несущей и обнаружением коллизий CSMA/CD (Carrier Sense Multiple Access with Collision Detection,): если во время передачи информационного сигнала узел сети обнаруживает сигнал от другого узла, занимающий канал связи, то он останавливает передачу, посылает специальный служебный сигнал и ждет в течение случайного промежутка времени перед тем, как снова отправить информационный сигнал
(3) Direct Sequence Spread Spectrum – Расширение спектра методом прямой последовательности, когда один импульс заменяется последовательностью из N более коротких импульсов, каждый из которых в N раз короче исходного, что позволяет расширить спектр сигнала (дополнительная защита информации) и снизить плотность мощности сигнала (повышение помехозащищенности)
(4) Frequency Hopping Spread Spectrum – Расширение спектра методом скачкообразной перестройки частоты, когда в разные временные интервалы используются разные частотные диапазоны
(5) Orthogonal Frequency Division Multiplexing – Ортогональное частотное уплотнение, когда передаваемый символ «расщепляется» и передается по частям при помощи ортогонально разнесенных поднесущих частот
(6) «Multiple Input – Multiple Output» – Антенная система «Много входов – Много выходов», обеспечивающая физическую реализацию метода множественного доступа с пространственным разделением каналов SDMA (Space Division Multiple Access), когда используется несколько передающих и приемных антенн, и радиоканал «раскладывается» на несколько независимых пространственных каналов: чем больше таких каналов, тем лучше характеристики (пропускная способность) радиоканала в целом

Начиная с поколения Wi-Fi 6, для борьбы с помехами используется технология BSS Coloring (Basic Service Set), основанная на использовании «цветовых» меток, которые точки доступа присваивают своим сетям, чтобы отличить их от соседних, работающих в тех же каналах: заголовки всех передаваемых в своей сети кадров сообщений помечаются своим «цветом», и если пользовательские устройства распознают кадр с этим «цветом», то они идентифицируют его как кадр своей сети и обрабатывают, а если «цвет» другой, то устройства такой кадр игнорируют.

Важным вопросом при проектировании сетей беспроводного доступа является обеспечение безопасности – конфиденциальности, целости и доступности передаваемых информационных сообщений. Одной из наиболее эффективных мер защиты является применение методов шифрования (криптографии), основанных на преобразовании входных данных в выходные при помощи алгоритма, который использует входные данные и ключ в качестве параметра. При этом, знание только выходных данных не дает возможности в течение приемлемого времени восстановить входные данные без знания ключа, также невозможно в течение приемлемого времени найти ключ, используя выходные данные, даже если входные данные известны.

В настоящее время, в стандартах IEEE 802.11 предусмотрено использование технологий шифрования WEP (Wired Equivalent Privacy – «Конфиденциальность как в проводных сетях»), WPA (Wi-Fi Protected Access – «Защищенный доступ Wi-Fi»), WPA2 и WPA3.

Протокол WEP, появившийся в 1997 году в первом оригинальном стандарте IEEE 802.11, шифрует трафик при помощи ключа длиной 40 или 104 бита. Поскольку данный ключ является статическим, то весь трафик, независимо от устройства, шифруется с помощью одного и того же ключа. WEP в настоящее время является устаревшим протоколом и используется для обеспечения обратной совместимости с устаревшими устройствами.

В 2003 году появляется технология WPA, которая использует протокол целостности временного ключа TKIP (Temporal Key Integrity Protocol), т.е. динамически изменяющий ключ, а также производит проверку целостности сообщений. В 2004 году, как обновление WPA, выходит технология WPA2. Она использует протокол блочного шифрования с имитовставкой и режимом сцепления блоков и счетчика CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), который основан на алгоритме расширенного стандарта шифрования AES (Advanced Encryption Standard) и является более надежным, чем протокол TKIP. Однако, технология WPA2 остается уязвимой, например, для атак с переустановкой ключа, позволяющих вредоносной сети имитировать реальную и вынуждать устройства подключаться к ней.

Наконец, в 2018 году приходит новая технология WPA3, в которой используются индивидуальное шифрование данных, протокол одновременной аутентификации равных SAE (Simultaneous Authentication of Equals) для создания безопасного «рукопожатия» устройства и точки доступа, а также усиленная защита от атак методом подбора пароля.

Для обеспечения требуемого уровня безопасности беспроводной сети важно знать, какая технология шифрования в ней используется, поскольку устаревшие протоколы являются более уязвимыми.

II. Проектирование сети беспроводного доступа IEEE 802.11 (Wi-Fi) в вагоне пассажирского поезда

Одним из ключевых этапов проектирования сети беспроводного доступа в пассажирских поездах является анализ устройств, подключаемых к инфраструктуре пассажирами. При анализе учитываются количество устройств, их категории, технические характеристики и функциональные возможности. В последние годы наблюдается устойчивый переход пользователей на более современные стандарты беспроводного доступа IEEE 802.11. Так, устройства с поддержкой 802.11n уже полностью вытеснили устаревшие решения на основе 802.11a/b/g, а сам стандарт 802.11n сегодня считается морально устаревшим, и активно растет число пользователей, использующих 802.11ac и 802.11ax.

Существует несколько подходов к проектированию сетей беспроводного доступа, каждый из которых может быть ориентирован на достижение определенных целей: максимальное расширение зоны покрытия, обеспечение высокой пропускной способности, а также поиск оптимального соотношения между этими параметрами. При этом, наибольшую практическую значимость представляет комбинированный подход, реализация которого требует предварительного анализа трафика и требований пользователей, что позволяет определить оптимальное количество точек доступа, обеспечивающих как текущие, так и перспективные потребности.

Для обеспечения лучшей производительности сети беспроводного доступа важно не только представлять общее количество пользовательских устройств, но и проанализировать работающие на их основе приложения, включая учет требований к пропускной способности канала связи и параметрам качества обслуживания QoS (Quality of Service).

Для примера рассмотрим установленную в электропоезде «Сапсан» типовую точку доступа Wi-Fi [7], между которой и пользовательским устройством пассажира (смартфоном или ноутбуком) организован канал связи максимальной протяженностью $D = 25$ м (примерная длина вагона «Сапсана») в диапазоне 2,4 ГГц в канале 6 (2426 … 2448 МГц) с центральной частотой $F = 2437$ МГц. В дальнейших расчетах будем использовать выражения из [8].

Рассчитаем линию связи в направлении от точки доступа к устройству. Исходя из характеристик оборудования, для точки доступа примем мощность передатчика $P_{tr} = 27$ дБм, потери в антенно-фидерном тракте $L_{tr} = 0$ дБ, коэффициент усиления антенны (в изотропных децибелах) $G_{tr} = 4$ дБи; для устройства примем потери в антенно-фидерном тракте $L_{recv} = 0$ дБ, коэффициент усиления антенны $G_{recv} = 3$ дБи, чувствительность приемника $P_{recv} = -64$ дБм.

Определим потери в свободном пространстве, приняв, для простоты расчетов, антенны устройств изотропными (здесь $K = -27{,}55$ – постоянная, необходимая для учета различных единиц измерения частоты и расстояния):

$$L_{bf} = 20\lg F + 20\lg D + K = \big(20\lg 2437 + 20\lg 25 + \\ + (-27{,}55)\big) \text{ дБ} = 68{,}25 \text{ дБ}.$$

Для неизотропных антенн необходимо также учитывать их коэффициенты усиления.

Определим запас на замирание сигнала SOM (System Operating Margin) как разность между реальным уровнем входного сигнала и чувствительностью приемника:

$$SOM = (P_{tr} - L_{tr} + G_{tr} - L_{bf} + G_{recv} - L_{recv}) - P_{recv} = \\ = \big((27 - 0 + 4 - 68{,}25 + 3 - 0) - (-64)\big)\ \text{дБ} = \\ = 29{,}75\ \text{дБ}.$$

Как правило, минимальная величина SOM должна быть не менее 10 дБ, однако на практике часто используют значение от 20 до 30 дБ.

Рассчитаем линию связи в обратном направлении (от устройства к точке доступа). Уровень потерь в свободном пространстве L_{bf}, при этом, не поменяется, потери в антенно-фидерных трактах L_{tr} смартфона и точки доступа также, для расчетов, останутся равными 0 дБ. Также, исходя из характеристик оборудования, для устройства примем мощность передатчика $P_{tr} = 17$ дБм, коэффициент усиления антенны $G_{tr} = 3$ дБи; для точки доступа примем коэффициент усиления антенны $G_{recv} = 4$ дБи, чувствительность приемника $P_{recv} = -65$ дБм.

Определим запас на замирание сигнала:

$$SOM = \big((17 - 0 + 3 - 68{,}25 + 4 - 0) - (-65)\big)\ \text{дБ} = \\ = 20{,}75\ \text{дБ}.$$

Из расчетов следует, что запас на замирание сигнала линии связи в обоих направлениях находится в рекомендуемом диапазоне значений, что говорит о достаточном энергетическом потенциале линии связи. При необходимости, также можно решить и обратную задачу: определить расстояние, при котором данная линия связи будет стабильно работать.

Как известно, для стабильного функционирования радиосвязи в диапазоне сантиметровых волн необходимо наличие прямой видимости между передающим и приемным устройствами. Для оценки допустимого уровня перекрытия и оптимизации условий распространения радиоволн используется понятие зоны Френеля (Fresnel zone) – области вокруг оси линии передачи, свободной от объектов, которые способны вызвать дифракцию или отражение и, тем самым, ослабить передаваемый сигнал. Ближайшая к оси линии передачи область называется первой зоной Френеля. Поскольку примерная длина вагона «Сапсана» составляет 25 м, то первая зона Френеля на таких дистанциях оказывается слишком мала, и определение ее радиуса можно не проводить. К тому же, в вагоне точки доступа можно расположить близко к потолку, чтобы обеспечить прямую видимость, а существующие препятствия (полки, сиденья, люди) не создают критичных перекрытий. Даже если первая зона Френеля оказывается частично перекрыта, то отраженные от стен, дверей, окон волны компенсируют потери.

Скорость передачи данных, указанная в технических характеристиках устройств беспроводного доступа, является теоретически максимально возможной и достигается при идеальных условиях работы оборудования. На практике фактическая скорость передачи пользовательского трафика гораздо ниже, что обусловлено, в том числе, необходимостью передачи служебной информации, количеством одновременно работающих пользовательских устройств, их удаленностью от точки доступа, наличием физических препятствий и помех и т.д. Применение механизмов, обеспечивающих стабильность соединения и защиту данных, также оказывает влияние на итоговую производительность сети беспроводного доступа, снижая ее на 30–50%.

Оценим среднюю пропускную способность C линии связи на одного пользующегося беспроводной сетью пассажира (считаем количество активных пользователей $n = 50$), приняв, исходя из характеристик оборудования, максимальную скорость передачи данных V точки доступа равной 1775 Мбит/с:

$$C = (V/2)/n = ((1775/2)/50)\ \text{Мбит/с} = \\ = 17{,}75\ \text{Мбит/с}.$$

Производительность сети беспроводного доступа становится меньше, если к точке доступа, поддерживающей, например, стандарт 802.11ax, подключится пользовательское устройство стандарта 802.11ac или 802.11n. Тогда передача данных будет осуществляться на максимально возможной для устройства скорости, поскольку, в противном случае, он не сможет корректно демодулировать сигнал. Когда к точке доступа подключается значительное количество таких устройств с ограниченной пропускной способностью, то общая производительность беспроводной сети снизится. Это связано с тем, что выполнение одних и тех же задач требует от «медленных» пользователей большего времени нахождения в эфире по сравнению с «быстрыми».

Пусть к точке доступа одновременно подключаются два пользовательских устройства стандартов 802.11ax и 802.11n в одном частотном диапазоне 2,4 ГГц. Рассчитаем время, необходимое пассажирам для использования приложений, требуемая пропускная способность C_{app} которых составляет, например, 5 Мбит/с. Скорость передачи двух пространственных потоков при ширине канала 20 МГц в 802.11ax равна 286,8 Мбит/с, а в 802.11n – 144,4 Мбит/с. Примем, для простоты расчетов, что средняя пропускная способность устройств C_{dev} в два раза меньше максимальной скорости передачи данных, т.е. 143,4 Мбит/с и 72,2 Мбит/с соответственно.

Процент времени, в течение которого канал используется для передачи сигналов (т.е. используемая доля пропускной способности канала), называется канальным временем или утилизацией канала связи η:

- для устройства 802.11ax:

$$\eta = (C_{app} \times 100\%)/C_{dev} = (5 \times 100\%)/(143{,}4) = \\ = 3{,}49\%;$$

- для устройства 802.11n:

$$\eta = (C_{app} \times 100\%)/C_{dev} = (5 \times 100\%)/(72{,}2) = \\ = 6{,}93\%.$$

Кроме того, существуют дополнительные издержки, связанные с отправкой приложениями служебных сообщений, с учетом которых фактическое время использования канала будет примерно в два раза больше, т.е. 6,98% – для устройства 802.11ax и 13,86% – для устройства 802.11n. Таким образом, «медленному» пассажиру понадобится в два раза больше времени на использование аналогичного приложения, чем «быстрому», что может привести к перегрузке беспроводной сети и, как следствие, к снижению ее производительности и увеличению средней задержки передачи. Это, в свою очередь, может снизить качество

работы чувствительных к задержкам приложений. По этой причине рекомендуется использовать двухдиапазонные точки доступа, при помощи которых «медленные» устройства будут работать в диапазоне 2,4 ГГц, а «быстрые» – в диапазоне 5 ГГц.

Таким образом, для определения необходимого количества точек доступа требуется оценить канальное время для пользовательских устройств и выполняющихся приложений. Возьмем пример вагона эконом-класса электропоезда «Сапсан», в котором одновременно находятся 60 пассажиров: из них около 15% (10 человек) не пользуются беспроводной сетью, а порядка 85% (50 человек) пользуются ей постоянно на протяжении всей поездки для просмотра видео, прослушивания музыки, обмена файлами посредством электронной почты и веб-серфинга. При этом, 80% (40 человек) получают доступ с помощью смартфонов, а оставшиеся 20% (10 человек) – с использованием ноутбуков. Тогда ориентировочные расчеты с использованием приведенных выше выражений для выбранной двухдиапазонной точки доступа, поддерживающей стандарты 802.11a/b/g/n/ac/ax, показывают, что на один вагон будет достаточно одной точки.

Проведем моделирование сети беспроводного доступа Wi-Fi вагона «Сапсана» с помощью программы Wi-Fi Planner PRO [9] для диапазонов 2,4 ГГц (рис. 1) и 5 ГГц (рис. 2) типовой точки доступа [10].

На основе исходных данных (план объекта, тип препятствий, технические характеристики точек доступа) определены – оптимальное место расположения точек доступа, их количество, а также цветовая карта покрытия беспроводной сети, отражающая уровень сигнала на разных расстояниях от точки в выбранном частотном диапазоне: чем более «теплыми» являются цвета (красный, желтый), тем выше уровень сигнала, а чем цвета более «холодные» (зеленый, голубой), тем уровень сигнала ниже. При моделировании была выбрана минимальная мощность передатчика точки доступа для исключения взаимных помех между точками соседних вагонов.

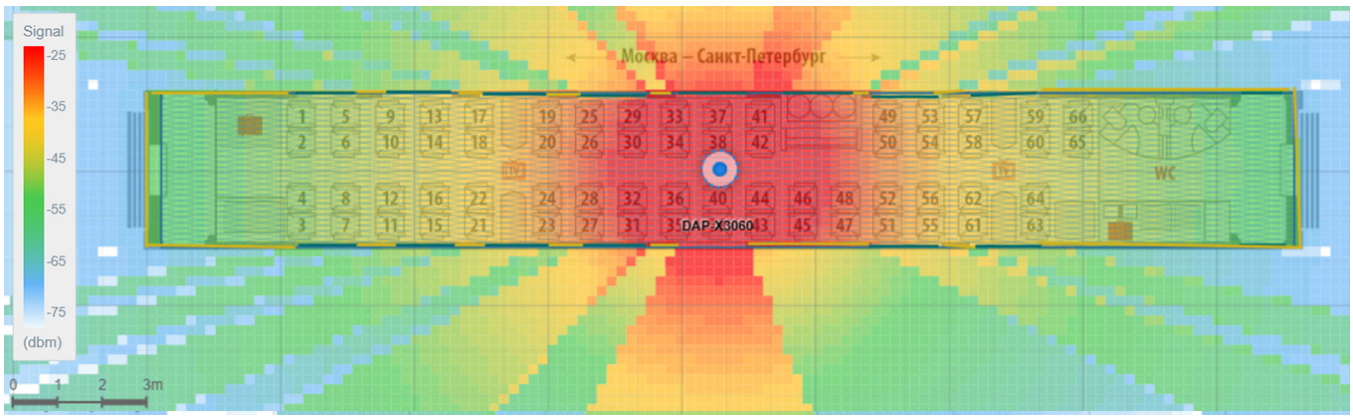

Рис. 1. Результаты моделирования сети беспроводного доступа Wi-Fi вагона «Сапсана» для диапазона 2,4 ГГц

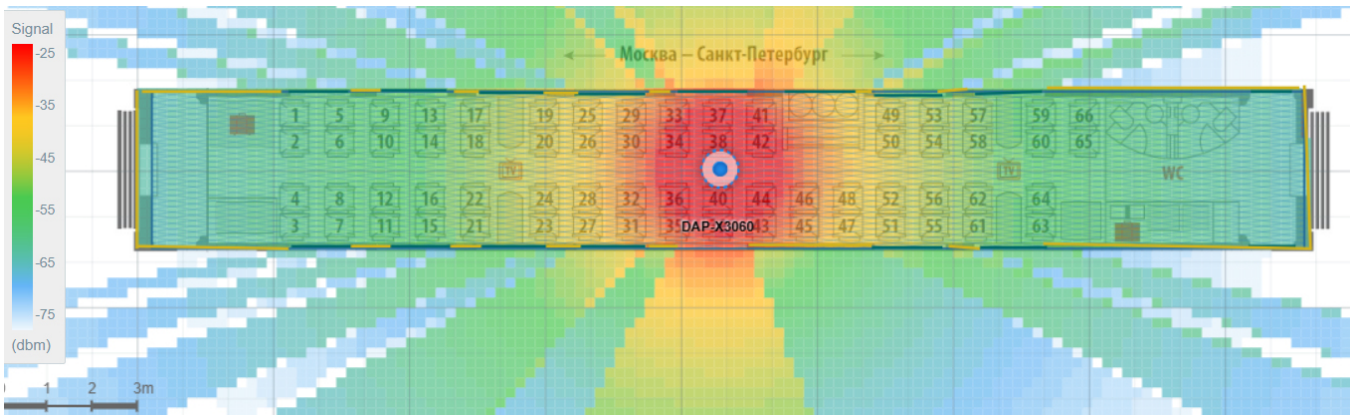

Рис. 2. Результаты моделирования сети беспроводного доступа Wi-Fi вагона «Сапсана» для диапазона 5 ГГц

При проектировании беспроводной сети уровень перекрытия зон обслуживания соседних точек доступа, работающих на неперекрывающихся каналах, определяется целевыми параметрами сети. В случае, если приоритетом является высокая производительность, перекрытие допускается на уровне сигнала около −67 дБм. Из результатов моделирования видно, что данное условие при выбранных параметрах и расположении точки доступа выполняется.

Список литературы

[1] Плеханов П.А., Арнадская Ю.Е. Проектирование беспроводных сетей в пассажирских поездах // Автоматика, связь, информатика. 2025. № 10. С. 18-21.

[2] Роенков Д.Н., Плеханов П.А. Радиосвязь для высокоскоростной железнодорожной магистрали Москва – Санкт-Петербург // Транспорт Российской Федерации. 2024. № 1. С. 58-61.

[3] Плеханов П.А., Роенков Д.Н. Перспективная подвижная связь // Автоматика, связь, информатика. 2024. № 1. С. 16-20.

[4] Плеханов П.А. Беспроводные инфокоммуникационные сети на железнодорожном транспорте. СПб.: ПГУПС, 2014. 55 с.

[5] Плеханов П.А., Роенков Д.Н. Цифровые системы подвижной связи на железнодорожном транспорте. СПб.: ФГБОУ ВО ПГУПС, 2020. 41 с.

[6] Плеханов П.А., Роенков Д.Н. БПЛА на службе железнодорожного транспорта // Автоматика, связь, информатика. 2023. № 9. С. 13-16.

[7] AirEngine 5761-11 Access Point [Электронный ресурс]. – URL: https://e.huawei.com/eu/products/wlan/indoor-access-points/airengine-5761-11. – Режим доступа: свободный (дата обращения: 20.03.2026).

[8] Технологии современных беспроводных сетей Wi-Fi: учебное пособие / Е.В. Смирнова, А.В. Пролетарский и др.; под общ. ред. А.В. Пролетарского. М.: Издательство МГТУ им. Н.Э. Баумана, 2017. 446 с.

[9] Wi-Fi Planner PRO [Электронный ресурс]. – URL: https://www.dlink.ru/tools/wi-fi/. – Режим доступа: свободный (дата обращения: 20.03.2026).

[10] DAP-X3060 [Электронный ресурс]. – URL: https://dlink.ru/ru/products/1366/2713.html. – Режим доступа: свободный (дата обращения: 20.03.2026).