

УЛУЧШЕНИЕ ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК ПРОТОКОЛОВ ИНКАПСУЛЯЦИИ 802.11

Юркин Д.В.¹, Исаченков П.А.², Патрикеев А.И.³

Статья посвящена исследованию и оптимизации информационного взаимодействия корреспондентов протокола инкапсуляции, который определяет параметры системы передачи данных, в рамках стандарта 802.11. В рамках исследования были поставлены задачи поиска наилучших параметров протокола инкапсуляции данных, исследованы зависимости среднего времени выполнения от длины кодового слова, произведены оценка влияния производительности радиооборудования на пропускную способность соединения, оценка влияния кадры на пропускную способность соединения, а также определено влияние отношения сигнал/шум на пропускную способность канала связи. В результате исследования было определено, что при максимальной длине кодируемого блока рекомендованной разработчиками стандартов, пропускная способность резко падает при ухудшении качества канала, в отличие от каналов хорошего качества, где максимальная длина кодируемого блока незначительно влияет на пропускную способность. Результаты исследования дают возможность построить приемо-передающий тракт, адаптируемый к вероятности ошибки, что позволит уменьшить потери пропускной способности в радиоканалах низкого качества и в полной мере использовать возможности среды передачи данных, а также ресурсы телекоммуникационного оборудования, при сохранении структуры инкапсуляции данных, определенной стандартом 802.11.

Ключевые слова: инкапсуляция, сети широкополосного радиодоступа, пропускная способность, вероятностно-временные характеристики, вероятность ошибки, отношение сигнал/шум, стандарт IEEE 802.11

Введение

При проектировании высокопроизводительных систем передачи данных, основывающихся на сетях широкополосного радиодоступа очень часто необходимо решать задачи оптимизации информационного взаимодействия корреспондентов-участников протокола инкапсуляции, определяющего параметры системы передачи данных, в рамках выбранного стандарта. Результатом данной работы являются рекомендации по улучшению временных характеристик протоколов установления и поддержки защищенных соединений в стандарте IEEE 802.11 [1].

Посредством предложенной методики повышения вероятностных характеристик системы показано влияние параметров приемо-передающего тракта, производительности телекоммуникационного оборудования и криптографических алгоритмов на эффективность использования пропускной способности телекоммуникационного оборудования.

Одной из основных целей исследований является методика улучшения вероятностных характеристик защищенных соединений, заключающаяся

в решении задач поиска минимального значения зависимости среднего времени передачи кадра от вероятности обнаруженной ошибки в канале связи и поиска максимального значения средней вероятности успешного завершения от вероятности обнаруженной ошибки.

Постановка задачи поиска наилучших параметров протокола инкапсуляции данных

Проанализируем зависимость среднего времени:

$$\bar{T} = (l, v_{form}, v_{send}, p_o, r) \quad (1)$$

выполнения протокола от вероятности ошибки в канале связи на примере самой простой модели канала связи ДСКБП.

Рассмотрим группу параметров, значения которых могут варьироваться для поиска оптимального значения функции :

l - длина кодируемого сообщения;

v_{form}, v_{send} - скорости формирования и передачи сообщения, соответственно;

p_o - вероятность битовой ошибки;

r - скорость кода.

1 Юркин Дмитрий Валерьевич, доцент, кандидат технических наук, доцент кафедры ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», г. Санкт-Петербург, dvurkin@ya.ru

2 Исаченков Павел Андреевич, студент ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», г. Санкт-Петербург, pais@tutaimail.com

3 Патрикеев Антон Игоревич, студент ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», г. Санкт-Петербург, antpat@rambler.ru

Основной областью применения методов оптимизации взаимодействия корреспондентов являются информационные схемы взаимодействия с вероятностным завершением. Основными оценками для которых являются вероятностные характеристики. Как было показано в [2], в каждом протоколе инкапсуляции имеется начальное, конечное состояние и промежуточные состояния. Для оценки было предложено использовать два, непосредственно связанных с алгоритмом протокола, параметра перехода из начального состояния в конечное состояние успешного завершения: среднее время успешного выполнения \bar{T} и вероятность успешного выполнения \bar{P} за определенное время.

Таким образом, можно сформулировать общий подход к оптимизации параметров СПДС:

$$\bar{T}(l, v_{form}, v_{form}, p_o, r) \rightarrow \min \quad (2)$$

1) необходимо определить такое разделение исходного сообщения m на i кодируемых блоков равной длины $l = l(m)/i, l \in [1, l(m)]$, при котором среднее время их передачи будет минимальным при заданной вероятности ошибки, скорости открытого канала и параметрах кодера $\{v_{form}, v_{form}, p_o, r\} = const$.

2) необходимо определить, такое отношение времен $h = \frac{t_{form}}{t_{send}}$, при котором среднее время передачи будет минимальным при определенной длине блока кодируемого сообщения, скорости кода и вероятности битовой ошибки в канале $\{l, p_o, r\} = const$.

3) необходимо определить, такое значение скорости кода r , при котором среднее время передачи будет минимальным при определенной длине блока кодируемого сообщения, скоростях формирования и передачи сообщения и вероятности битовой ошибки в канале $\{l, v_{form}, v_{form}, p_o\} = const$.

Исследование зависимостей среднего времени выполнения от длины кодового слова

Основные результаты моделирования протоколов инкапсуляции были изложены в [3], поэтому, основываясь полученных в результатах расчетов, оценим характер зависимости среднего времени выполнения от его параметров. При кодировании криптограммы зависимость $\bar{T}(p_o, l)$ будет иметь вид:

$$\bar{T}(p_o, l) = i(2-r)l(1-p_o)^{-(2-r)l}(v_{send}^{-1} + v_{form}^{-1}) \quad (3)$$

при $r \frac{m}{i}$ проверочных символов для каждого из i кодовых блоков (рис. 1).

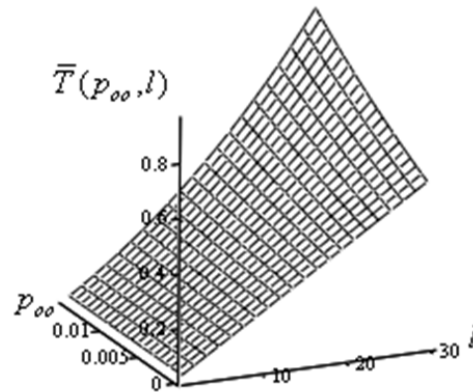


Рис. 1. Зависимость среднего времени передачи от длины кодового блока

Определим характер зависимости $\bar{T}(l)$. Найдем производную первого порядка $\frac{d}{dl} \bar{T}(l)$ (рис. 2):

$$\frac{d}{dl} \bar{T}(p_o, l) = (1-p_o)^{-(2-r)l} (v_{send}^{-1} + v_{form}^{-1}) \frac{1}{(1-\ln(1-p_o))(2-r)l} \quad (4)$$

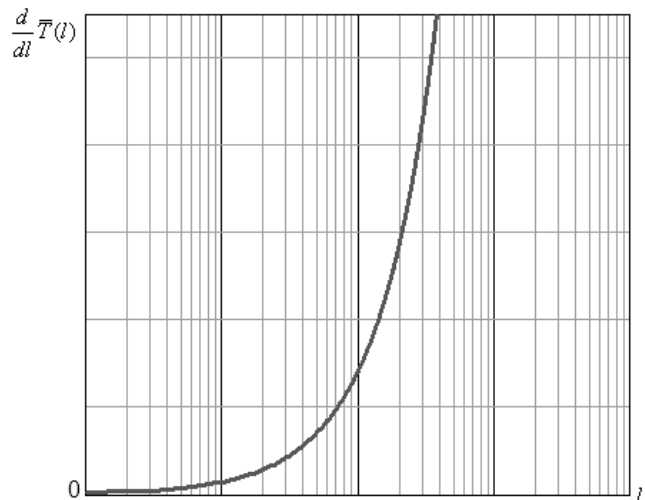


Рис. 2. Производная первого порядка зависимости среднего времени выполнения от длины кодового блока

Определим характер зависимости $\bar{T}(p_o)$ при заданной длине кодового блока l .

Найдем производную первого порядка

$$\frac{d}{dp_o} \bar{T}(p_o, l) \Big|_{l=const} \quad (\text{рис. 3}):$$

$$\frac{d}{dp_o} \bar{T}(p_o, l) = i((2-r)l)^2 (1-p_o)^{-1} (v_{send}^{-1} + v_{form}^{-1}) (1-p_o)^{-(2-r)l} \quad (5)$$

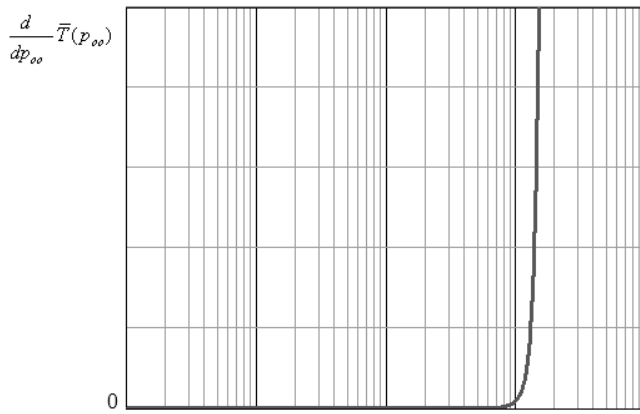


Рис. 3. Производная первого порядка зависимости среднего времени выполнения от вероятности ошибки

Проанализировав функции $\frac{d}{dp_o} \bar{T}(p_o, l)$ и $\frac{d}{dl} \bar{T}(p_o, l)$, можно сказать, что на всем диапазоне значений аргумента они не имеют корней. Функции $\frac{d}{dp_o} \bar{T}(p_o, l) > 0$ и $\frac{d}{dl} \bar{T}(p_o, l) > 0$, поэтому можно сказать, что зависимость $\bar{T}(p_o, l)|_{l=const}$ монотонно возрастает на интервале $p_o \in [0, 1]$, а зависимость $\bar{T}(p_o, l)|_{p_o=const}$ монотонно возрастает на интервале $l \in [1, l(m)]$.

Оценка влияния производительности радиооборудования на пропускную способность соединения

Покажем влияние скоростей формирования и передачи кадров на пропускную способность канала связи. Определим изменение пропускной способности относительно канала, образованного аппаратурой, не вносящей задержек при обработке сигналов:

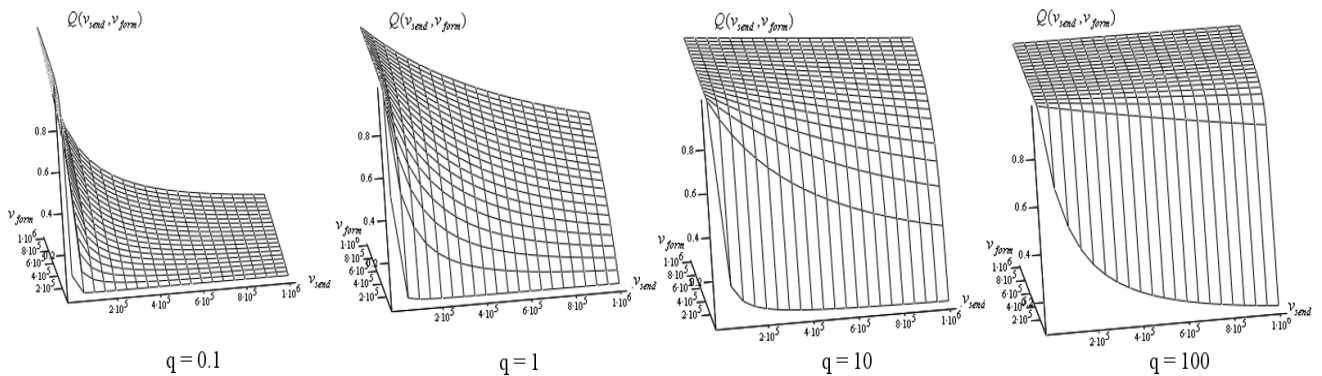


Рис. 4. Изменение пропускной способности от соотношения скоростей формирования и передачи сообщения

$$Q(p_o, r, l, v_{form}, v_{send}) = \frac{l \cdot i \cdot v_{send}^{-1}}{\bar{T}(p_o, r, l, v_{form}, v_{send})} \quad (6)$$

Рассмотрим случай, когда скорость битовая скорость канала связи остается неизменной, а меняется скорость обработки блока данных. В данном случае наиболее важную роль будет играть производительность радиоаппаратуры. Таким образом, время выполнения перехода из одной вершины вероятностного графа в другую было представлено как $t_{i \rightarrow i+1} = v_{send}^{-1} + v_{form}^{-1}$, но при более подробном рассмотрении времени формирования (время затрачиваемое на обработку кадра) $t_{form} = v_{form}^{-1}$, можно сказать, что большей частью оно определяет результирующую пропускную способность. Приведем зависимость среднего времени выполнения для различных величин v_{send} и v_{form} .

Построим поверхности для $Q(v_{send}, v_{form})$, описывающие зависимость изменения пропускной способности канала от скоростей формирования и передачи сообщения при отношении $q = \frac{t_{form}}{t_{send}} \in [10^{-1}, 1, 10^1, 10^2]$ (рис. 4).

Оценка влияния длины кадра на пропускную способность соединения

Для оценки вероятностно-временных характеристик воспользуемся методикой, изложенной в [4]. Зависимость среднего времени передачи $\bar{T}(p_o)$, для одного кадра от вероятности ошибки в канале связи при постоянной скорости кода будет иметь следующий вид: $\bar{T}(p_o, l) = (2 - r)l(1 - p_o)^{-(2-r)l}(v_{send}^{-1} + v_{form}^{-1})$, а зависимость изменения пропускной способности $Q(p_o)$ будет равна:

$$Q(p_o, r, l, v_{form}, v_{send}) = \frac{l \cdot v_{send}^{-1}}{\bar{T}(p_o, r, l, v_{form}, v_{send})} \quad (7)$$

Однако в исследуемом протоколе инкапсуляции кадра скорость кода является переменной и зависимость среднего времени передачи кадра будет $\bar{T}(p_o, l) = (l + l(h))((1 - p_o)^{-(l+l(h))} (v_{send}^{-1} + v_{form}^{-1}))$, где $l(h)$ - это длина заголовка кадра PDU MAC.

Построим поверхность (рис. 5), описывающую зависимость $Q(p_o, l)$ при следующих параметрах в соответствии с таблицей (табл. 1).

Таблица 1.

Параметры радиоаппаратуры

Скорость передачи кадра (бит/с)	Скорость формирования кадра (бит/с)	Количество служебной информации на кадр (бит)
10^7	$2 \cdot 10^9$	288

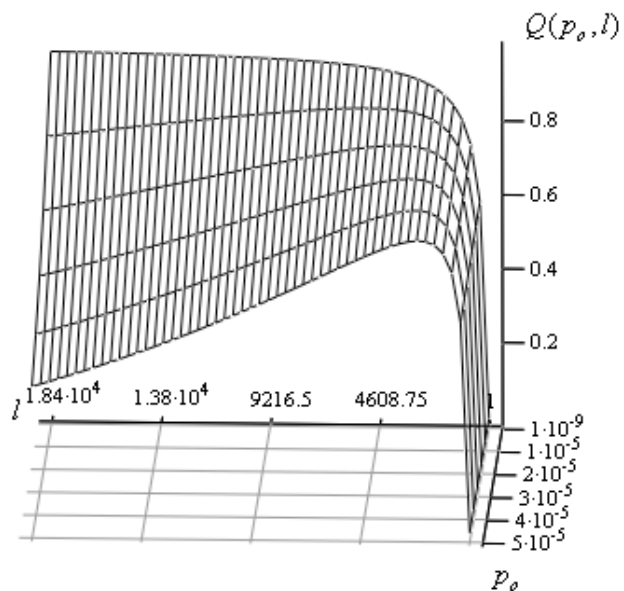


Рис. 5. Зависимость изменения пропускной способности канала связи от вероятности ошибки и длины информационной части кадра MAC

Стандартом определена компоновка кадров MAC, поэтому заголовок должен каждого кадра должен содержать такие поля как: управление кадром, идентификатор длительности соединения, адреса отправителя, получателя и передающей станции, управление очередностью, MSDU или фрагмент MSDU, поля отвечающие за работу службы QoS и результат помехоустойчивого кодирования. Размерность поля данных имеет переменную длину, для обнару-

жения ошибок в которой используется проверочная последовательность кадра, полученная с использованием циклического кода CRC-32 [5]. Согласно рекомендациям разработчиков стандарта, длина поля Frame Body является переменной и варьируется в пределах от 0 до 18432 бит при длине служебной части кадра 288 бит, однако вопрос выбора ее оптимальной длины в зависимости от вероятности битовой является открытым.

Найдем значение l_{opt} , удовлетворяющее условию $Q(l_{opt}) \rightarrow \max$, то есть оптимальное значение длины поля Frame Body. Исследуем на экстремумы зависимость изменения пропускной способности

$Q(p_o)$, для этого найдем корни зависимости $\left. \frac{d}{dl} Q(p_o, l) \right|_{p_o=const}$ производной первого порядка от пропускной способности по длине кодируемого сообщения l .

$$\frac{d}{dl} Q(l) = \frac{v_{send}^{-1} (v_{form}^{-1} + v_{send}^{-1}) (1 - p_o)^{-(h+l(h))} (l(h) + l(h) \ln(1 - p_o) l + l^2 \ln(1 - p_o))}{((1 - p_o)^{-(l(h)+l)} (l(h) + l) (v_{send}^{-1} + v_{form}^{-1}))^2} \quad (8)$$

Так как неотрицательный l_{opt} корень производной первого порядка от функции $\frac{d}{dl} Q(l)$ равен:

$$l_{opt}(p_o) = \left(-l(h) \cdot \ln(1 - p_o) - \left((l(h) \cdot \ln(1 - p_o))^2 - 4 \ln(1 - p_o) l(h) \right)^{\frac{1}{2}} \right) \cdot (2 \ln(1 - p_o))^{-1} \quad (9)$$

и функция $\frac{d}{dl} Q(l) > 0$, при $l \in (0, l_{opt})$, а при $l \in (l_{opt}, \infty)$ та же функция $\frac{d}{dl} Q(l) < 0$, то можно показать, что единственный экстремум l_{opt} , это максимум функции $Q(l)$.

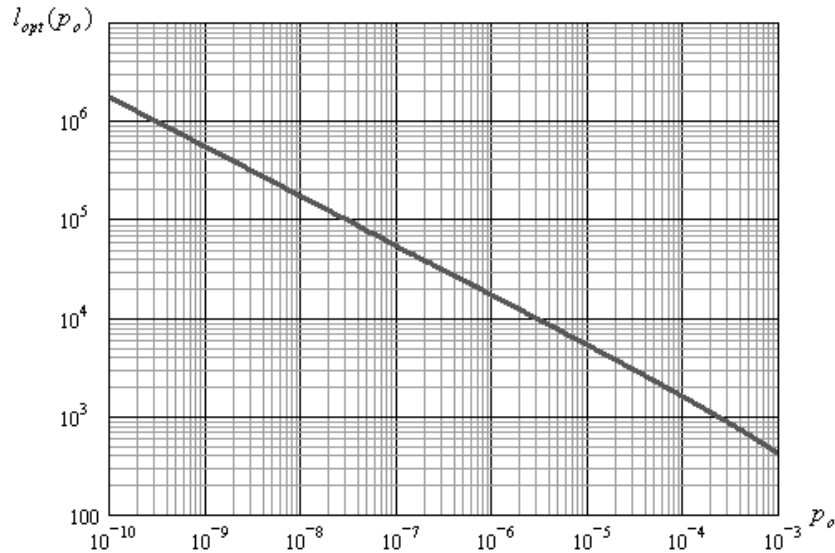


Рис. 6. Зависимость оптимальной длины поля данных от вероятности ошибки в канале связи

Построим зависимость $l_{opt}(p_o)$ оптимальной длины поля данных от вероятности битовой ошибки в канале связи для вышеизложенных параметров инкапсуляции (рис. 6).

Влияние отношения сигнал/шум на пропускную способность канала связи

Для сравнительной оценки пропускной способности предположим, что используется ранее упомянутая модель канала ДСКБП, а в качестве канальной модуляции BPSK. Тогда общий вид функции ошибки будет:

$$p_o = 0,5[1 - \Phi(2 - 0,5h)] \quad ()$$

где $h = \sqrt{E_s/N_0}$, это отношение сигнал/шум,

а $\Phi(x) = \frac{2}{\sqrt{2\pi}} \int_0^x e^{-t^2/2} dt$, это функция Крампа.

Поэтому пропускная способность ДСКБП определяется как:

$$C(p_o) = 1 - H(p_o) \quad (10)$$

где двоичная энтропия определена отношением:

$$H(p_o) = -x \log 2x - (1 - x) \log 2(1 - x) \quad (11)$$

Получим зависимости пропускной способности СПДС, работающей по ДСКБП, согласно изложенной методике оценки. Пропускная способность для СС с РОС определена отношением:

$$C(p_o) = \left((2-r)l((1-p_o)^{-(2-r)l} - 2^{-(1-r)l}) (v_{send}^{-1} + v_{form}^{-1})^{-1} v_{send}^{-1} \right) \quad (12)$$

Данная зависимость при различных видах модуляции от отношения С/Ш $C(h)$ будет иметь вид, показанный на рисунке (рис. 7).

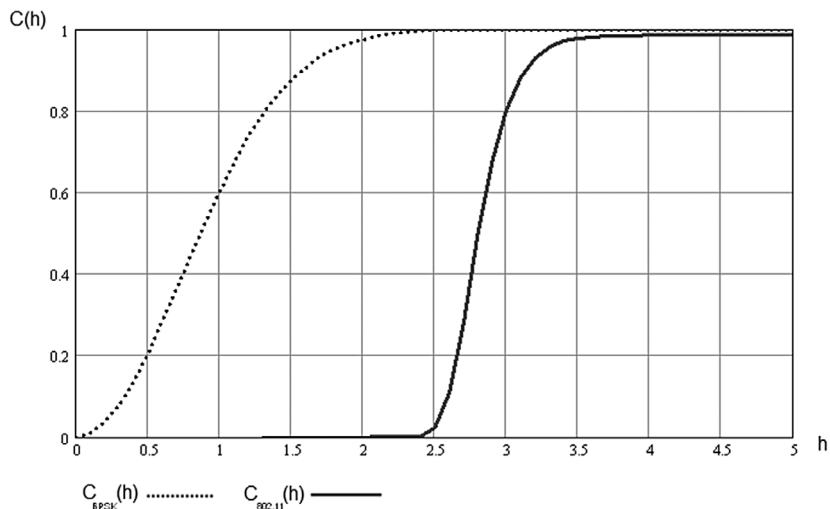


Рис. 7. Зависимости пропускной способности для ДСКБП фазовой модуляцией для инкапсуляции 802.11

Построим зависимости $C(h)$ (рис. 8) пропускной способности канала связи от вероятности битовой ошибки для адаптивной $C_{opt}(h)$, равной:

$$l_{opt}(p_o) = \left(-h \cdot \ln(1 - p_o) - \left((h \cdot \ln(1 - p_o))^2 - 4 \ln(1 - p_o) h \right)^{\frac{1}{2}} \right) \cdot (2 \ln(1 - p_o))^{-1} \quad (13)$$

и максимальной $C_{max}(h)$, равной 2304 окетам, длин поля данных кадра.

Покажем, насколько позволяет адаптация по длине кадра физического уровня повысить про-

пускную способность относительно системы связи с передачей кадров максимальной длины. Для этого построим зависимость (рис. 9):

$$\Delta C(h) = C_{opt}(h) - C_{max}(h) \quad (14)$$

Как видно по данной зависимости, разница пропускных способностей канала связи при максимальной оптимальной длина кадра имеет ярко выраженный экстремум при определенных отношениях С/Ш, поэтому целесообразно графически показать $\bar{l}(h)$ от отношения С/Ш в канале связи (рис. 10).

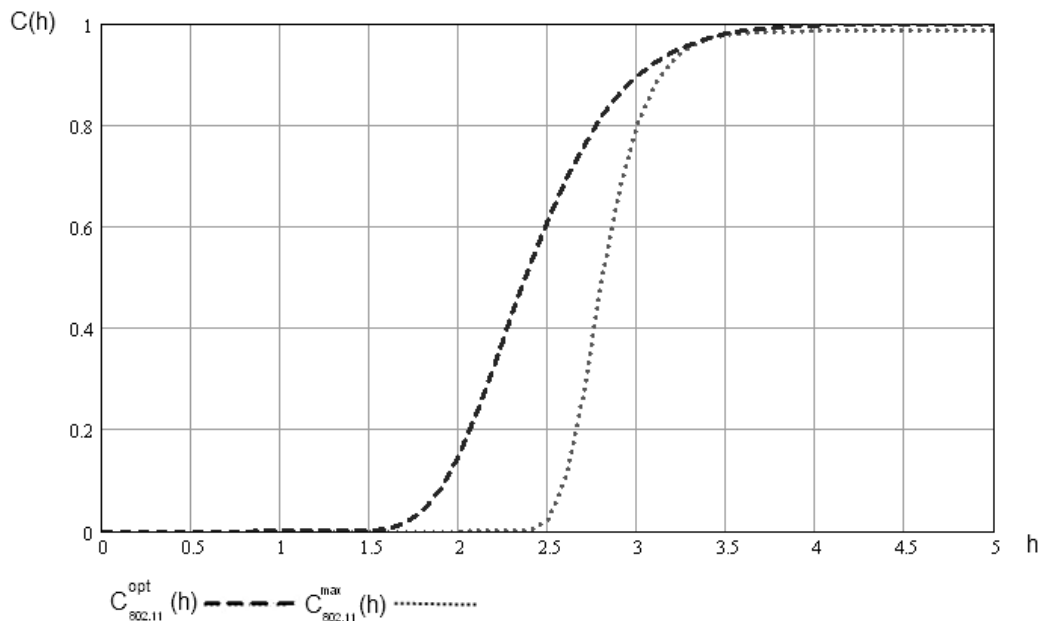


Рис. 8. Сравнение результатов оценки пропускной способности для ДСКБП и РОС при выборе различной длины кадра

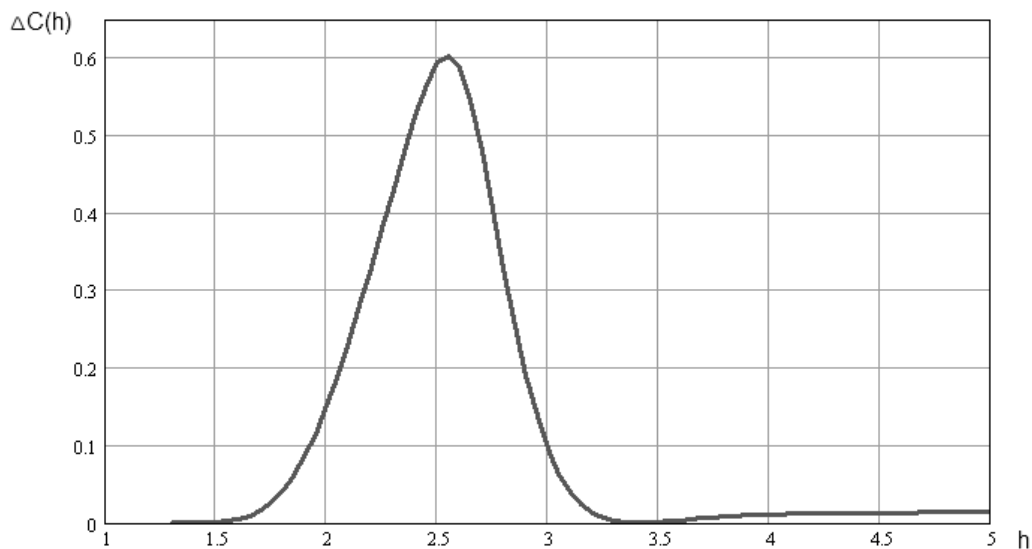


Рис. 9. Относительное изменение пропускной способности канала связи

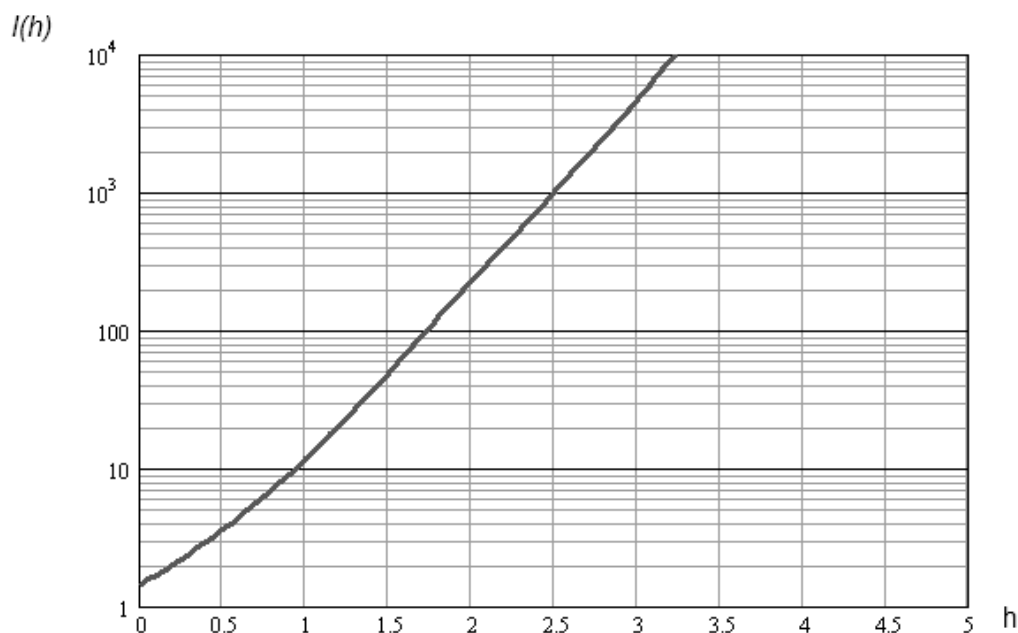


Рис. 10. Зависимость оптимальной длины кадра от отношения С/Ш.

Выводы

Проведенное исследование продемонстрировало, что в каналах хорошего качества влияние рекомендованной в стандарте максимальной длины кодируемого блока на пропускную способность является незначительным по причине небольшой вероятности поражения ошибками кадра, но с ухудшением качества канала пропускная способность резко падает, о чем был сделан вывод в [6].

Применение адаптивной длины информационной части кадра от вероятности обнаруженной ошибки позволяет существенно уменьшить потери пропускной способности в радиоканалах низкого качества. Это достигается посредством

оптимизации соотношения длин информационной и служебной частей кадра для заданной вероятности ошибки в канале. Решение задачи поиска оптимальной длины по критерию минимального среднего времени передачи кадра для СПДС работающей по каналу связи с ошибками позволяет оптимизировать пропускную способность во всем диапазоне вероятности обнаруженной ошибки.

Основываясь на приведенных выше результатах, можно построить адаптируемый к вероятности ошибки в канале приемо-передающий тракт, использующий в полной мере возможности среды передачи данных и производительность телекоммуникационного оборудования, сохраняя при этом структуру инкапсуляции данных.

Рецензент: Красов Андрей Владимирович, кандидат технических наук, профессор, заведующий кафедрой Защищённых систем связи, ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», г. Санкт-Петербург, krasov@inbox.ru

Литература:

1. IEEE Std 802.11-2007, IEEE Standard for Information Technology, Telecommunications and information exchange between systems, Local and metropolitan area network, Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
2. O. Isaksson, S. Keski-seppälä, S. D. Eppinger. Evaluation of design process alternatives using signal flow graphs, J. Eng. Design, 2000.
3. Никитин В.Н., Юркин Д.В. Анализ протоколов шифрования // Журнал Радиоэлектроники. 2009. №4. С. 7.
4. Nikitin V., Yurkin D., Chilamkurti N. The influence of the cryptographic protocols on the quality of the radio transmission, In Proc. of International Conference on Ultra Modern Telecommunications – ICUMT-2009, St.-Petersburg, Russia, pp. 1-5.
5. Castagnoli G.; Bräuer S.; Herrmann M. Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits, IEEE Transactions on Communications. 1993.
6. Юркин Д.В. Исследование и оптимизация защищенных каналов в сетях широкополосного радиодоступа. Диссертация на соискание ученой степени кандидата технических наук / Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича. Санкт-Петербург, 2010.

IMPROVING THE PROBABILITY-TIME CHARACTERISTICS OF THE 802.11-ENCAPSULATION PROTOCOLS

Yurkin D.V.⁴, Isachenkov P.A.⁵, Patrikeev A.I.⁶

This article is on the topic of the research and optimization of informational exchange between encapsulation protocol correspondents. This protocol defines the parameters of the data transmission system, as part of the IEEE 802.11 standard. During the research, the tasks were set to find the best parameters of data encapsulation protocol. Dependencies of the average execution time of the code word length, as well as the impact of radio equipment performance on bandwidth were investigated. Impact, caused by signal/noise ratio and the frame itself on the bandwidth were also studied. The study determined, that for the maximum recommended code block length, the bandwidth is significantly reduced while using the poor quality channels, whereas, using the high quality transmission channels can minimize the impact on the bandwidth. Research results make it possible to create a two-way transmission path, which is adaptable to the error probabilities. This could reduce the loss in the low-quality radio channels bandwidth and fully utilize the transmission medium capabilities as well as the resources of telecommunication equipment, while maintaining the data encapsulation structure, defined by the 802.11 standard.

Keywords: encapsulation, broadband radio access networks, bandwidth, probability-time characteristics, error probability, signal/noise ratio, IEEE 802.11 standard

References:

1. IEEE Std 802.11-2007, IEEE Standard for Information Technology, Telecommunications and information exchange between systems, Local and metropolitan area network, Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
2. O. Isaksson, S. Keski-seppälä, S. D. Eppinger. Evaluation of design process alternatives using signal flow graphs, J. Eng. Design, 2000.
3. Nikitin V.N., Yurkin D.V. Analiz protokolov shifrovaniya // Zhurnal Radioelektroniki. 2009. №4. S. 7.
4. Nikitin V., Yurkin D., Chilamkurti N. The influence of the cryptographic protocols on the quality of the radio transmission, In Proc. of International Conference on Ultra Modern Telecommunications – ICUMT-2009, St.-Petersburg, Russia, pp. 1-5.
5. Castagnoli G.; Bräuer S.; Herrmann M. Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits, IEEE Transactions on Communications. 1993.
6. Yurkin D.V. Issledovanie i optimizatsiya zashchishchennykh kanalov v setyakh shirokopolosnogo radiodostupa. Dissertatsiya na soiskanie uchenoy stepeni kandidata tekhnicheskikh nauk / Sankt-Peterburgskiy gosudarstvennyy universitet telekommunikatsiy im. M.A. Bonch-Bruевичa. Sankt-Peterburg, 2010.



4 Yurkin Dmitri, Ph.D., docent, Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruевич Saint - Petersburg State University of Telecommunications», Saint-Petersburg, dvyurkin@ya.ru
5 Isachenkov Pavel, Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruевич Saint - Petersburg State University of Telecommunications», Saint-Petersburg, pais@tutaimail.com
6 Patrikeev Anton, Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruевич Saint - Petersburg State University of Telecommunications», Saint-Petersburg, antpat@rambler.ru