

Повышение качества безопасности видеоконференции в сфере образования

В. С. Кизин^{1}, С. Н. Новиков^{1,2}*

¹ Сибирский государственный университет геосистем и технологий, г. Новосибирск,
Российская Федерация

² Сибирский государственный университет телекоммуникаций и информатики,
г. Новосибирск, Российская Федерация

*e-mail: pikachy159@gmail.com

Аннотация. В статье, направленной на применение безопасности сети связи для улучшения качества передачи образовательной видеоконференции, используется адаптивный алгоритм распределения ресурсов для оптимизации качества передачи по сети. Применение протокола для улучшения качества передачи видеоконференции может увеличить скорость передачи, снизить частоту ошибок по битам. Алгоритм минимизирует задержку, используя оптимизацию муравьиной колонии и кластеризацию, что в конечном итоге достигает цели снижения энергопотребления и повышение безопасности. Чтобы улучшить производительность системы, необходимо учитывать проблему распределения мощности при улучшении качества передачи образовательной видеоконференции. Путем анализа механизма адаптивного распределения ресурсов, применимого к безопасности сети при повышении качества передачи образовательной видеоконференции, были созданы условия для оптимизации распределения ресурсов.

Ключевые слова: видеоконференция, информационная безопасность, алгоритм распределения

Improving video conference security in education

V. S. Kizin^{1}, S. N. Novikov^{1,2}*

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

² Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian
Federation

* e-mail: pikachy159@gmail.com

Abstract. In article, which aims to apply communication network security to improve the transmission quality of an educational video conference, an adaptive resource allocation algorithm is used to optimize the transmission quality over the network. The application of the protocol to improve the transmission quality of a video conference can increase the transmission speed, reduce the bit error rate. The algorithm minimizes latency using ant colony optimization and clustering, which ultimately achieves the goal of reducing power consumption and improving security. In order to improve system performance, the problem of power distribution must be taken into account when improving the transmission quality of an educational video conference. By analyzing the adaptive resource allocation mechanism applicable to network security while improving the transmission quality of an educational video conference, conditions were created for optimizing resource allocation.

Keywords: video conferencing, information security, distribution algorithm

Введение

С быстрым развитием Интернет-технологий и IT-индустрии создание и распространение информации претерпели огромные изменения [1]. Система видеосвязи представляет собой удаленное интерактивное мультимедийное приложение в реальном времени на базе Интернета. Она обеспечивает хорошую операционную платформу для онлайн-классов, удаленных академических обменов и ежедневных рабочих встреч. Платформа для прямой трансляции видео принесла большое удобство многим сотрудникам и студентам. Развитие системы онлайн-видео в прямом эфире, несомненно, станет основным направлением развития индустрии образования в будущем.

Чтобы повысить производительность системы, при улучшении качества передачи видеосигнала в учебных заведениях необходимо учитывать проблему распределения мощности. В настоящее время основным методом решения этой проблемы является моделирование задачи оптимизации системы с последующим установлением уравнения лагранжевой оптимизации. Чтобы достичь разумного распределения ресурсов, этот алгоритм постоянно совершенствуется, уменьшая при этом помехи на совпадающей частоте, при этом максимизируя оптимальное распределение ресурсов. Из этого следует цель данной статьи: анализ существующих методов решения проблемы безопасного и гарантирующего QoS способа передачи видео в образовательной среде и разработка алгоритма адаптивного распределения ресурсов.

Материалы

Благодаря системе видеосвязи, конференции по удаленной работе в реальном времени и учебные курсы можно проводить в любое время через сеть, что значительно снижает стоимость обучения, сокращает затраты времени и значительно повышает эффективность общения и обучения. Использование системы видеосвязи позволяет родителям быть в курсе учебной ситуации студентов, укреплять общение и обмены с другими вузами, выдвигать предложения по их улучшению, полностью перейти на домашнее обучение [2]. Система видеосвязи, представленная на рис. 1, также включает относительно полное управление коммуникациями, управление персоналом и системы управления ресурсами.

Развитие информационных и нанотехнологий, методов и средств программирования, цифровой обработки сигналов и технологий распознавания образов привело, в свою очередь, к быстрому развитию средств защиты информации, информационных систем и сетей [3]. Международные опросы показывают, что в настоящее время 55 % корпоративных сетей не имеют собственных политик безопасности. Для обеспечения безопасности сети используются только простые меры безопасности [4]. Важным средством создания безопасной сетевой среды является внедрение системы безопасности одновременно с принятием превентивных мер [3]. С точки зрения формы и содержания риски безопасности разнообразны. Чтобы справиться с новыми угрозами, приложения для видеоконференций будут постоянно улучшаться [5]. Под систематизацией понимается, систе-

матизация сетевой безопасности с точки зрения технологий безопасности, показанной на рис. 2. Улучшение системы безопасности может сделать компьютерные сети более безопасными в комплексном плане. Сетевая модель клиента уже не так проста и уникальна, как раньше [6].

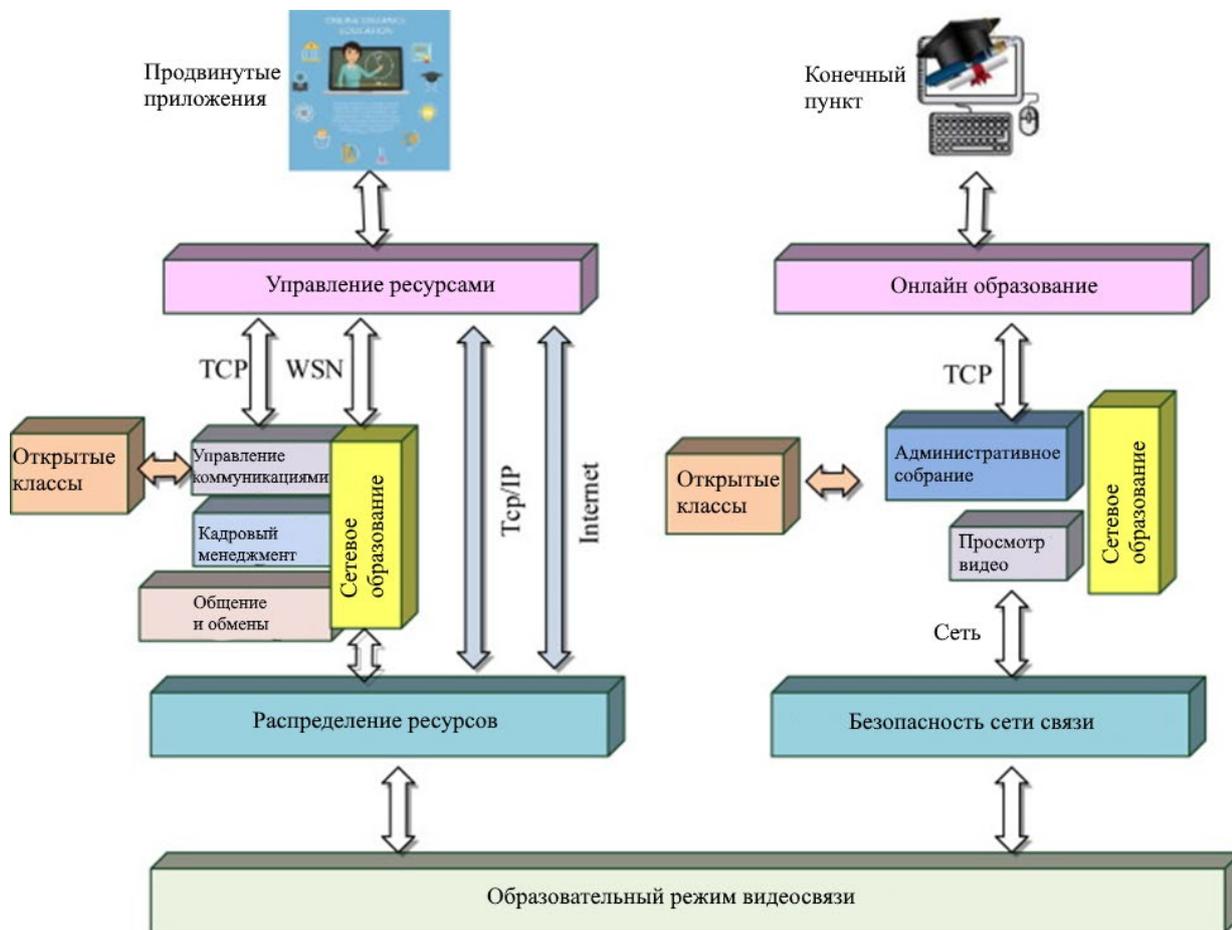


Рис. 1. Основы видеосвязи в сфере образования

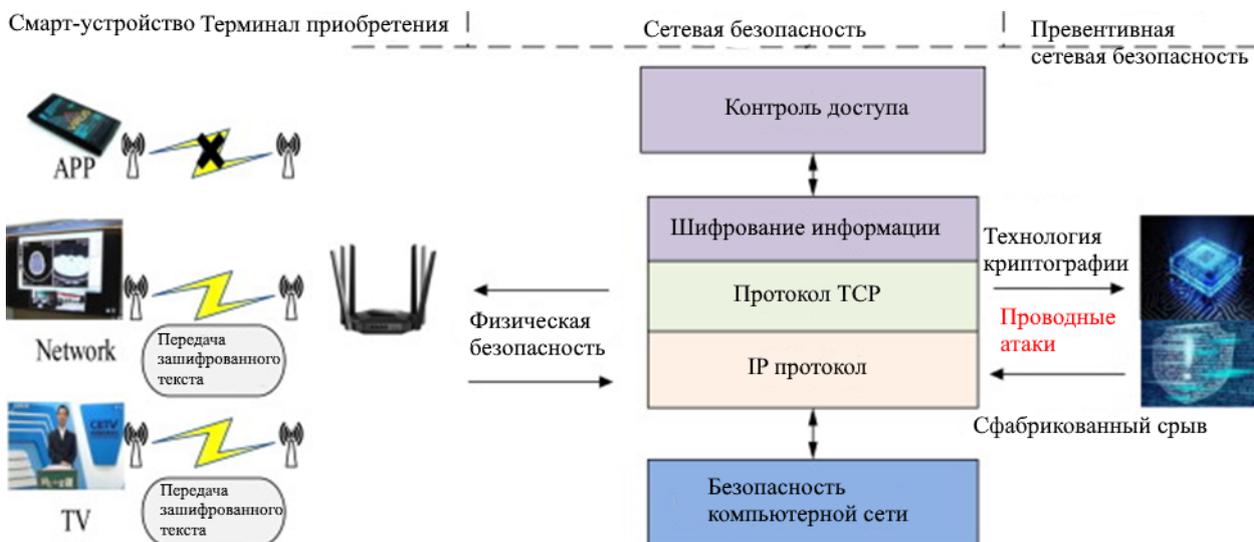


Рис. 2. Применение сетевой безопасности в сетевом протоколе связи

Система множественного доступа с ортогональным частотным анализом нисходящей линии связи состоит из q ячеек вместе, а коэффициент повторного использования частоты между ними равен 1.

Механизм адаптивного распределения ресурсов службы многоадресной, одноадресной рассылки может оценивать долю подкадра (каждый кадр состоит из 20 слотов длиной $T_{\text{slot}} = 15360 \times T_s = 0,5$ мс, которые пронумерованы от 0 до 19 [7]). Кроме этого, выделяется понятие подкадра (subframe), который состоит из двух соседних слотов. Структура кадра показана на рис. 3.

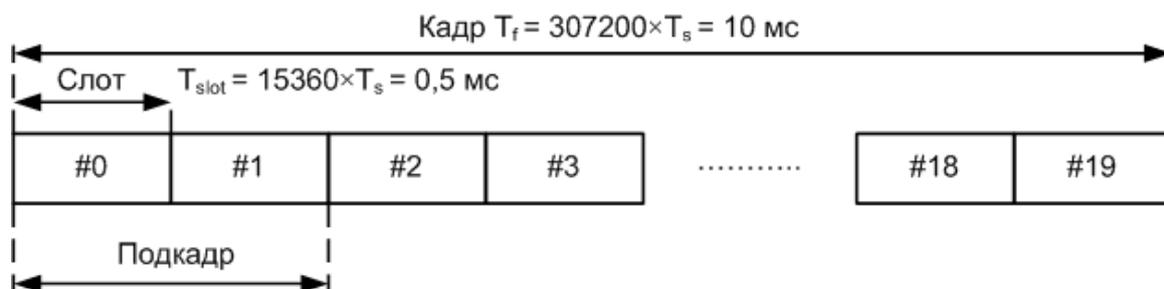


Рис. 3. Структура кадра

Этапы операции в основном включают в себя следующие моменты. Во-первых, соотношение подкадров в службе многоадресной рассылки вычисляется в течение периода выделения ресурсов [4]. Во-вторых, пороговое значение sinr получается в соответствии с требованием соотношения субкадров, а затем – многоадресной передачи. Эффективное значение службы сравнивается и анализируется с пороговым значением, чтобы определить, подходит или нет текущий подкадр для нужд службы многоадресной передачи и выполняется адаптивное выделение подкадров [6].

Во-первых, соотношение подкадров должно удовлетворять общую потребность в передаче данных службы многоадресной передачи в течение определенного времени передачи, а затем использовать это как количество подкадров, требуемых для определения распределения ресурсов службы многоадресной передачи [8].

Посредством вычисления доли подкадра в периоде ресурса соответствующий порог sinr может быть получен для адаптивного выделения подкадра.

Адаптивное выделение подкадра на рис. 4 связано с использованием ресурсов спектра и качеством служб многоадресной передачи, поэтому его необходимо выполнять в соответствии с определенными спецификациями [9]. Сначала следует определить пропорции подкадра.

Если требования соблюдены, то подкадры должны быть выделены одноадресной службе. Если требования не выполняются, то количество подкадров в подмножестве области передачи сети необходимо проанализировать, чтобы определить, удовлетворена ли область. Если это соответствует потребностям, то необходимо выделить подкадры для одноадресной службы. Кадры распределя-

ются по областям, требующим наибольшего количества подкадров [9]. Если оставшееся количество превышает спрос на службы многоадресной рассылки, то их необходимо снова выделить для служб одноадресной рассылки. Остальные кадры выделяются областям с наиболее востребованным подкадром в области распространения сети.

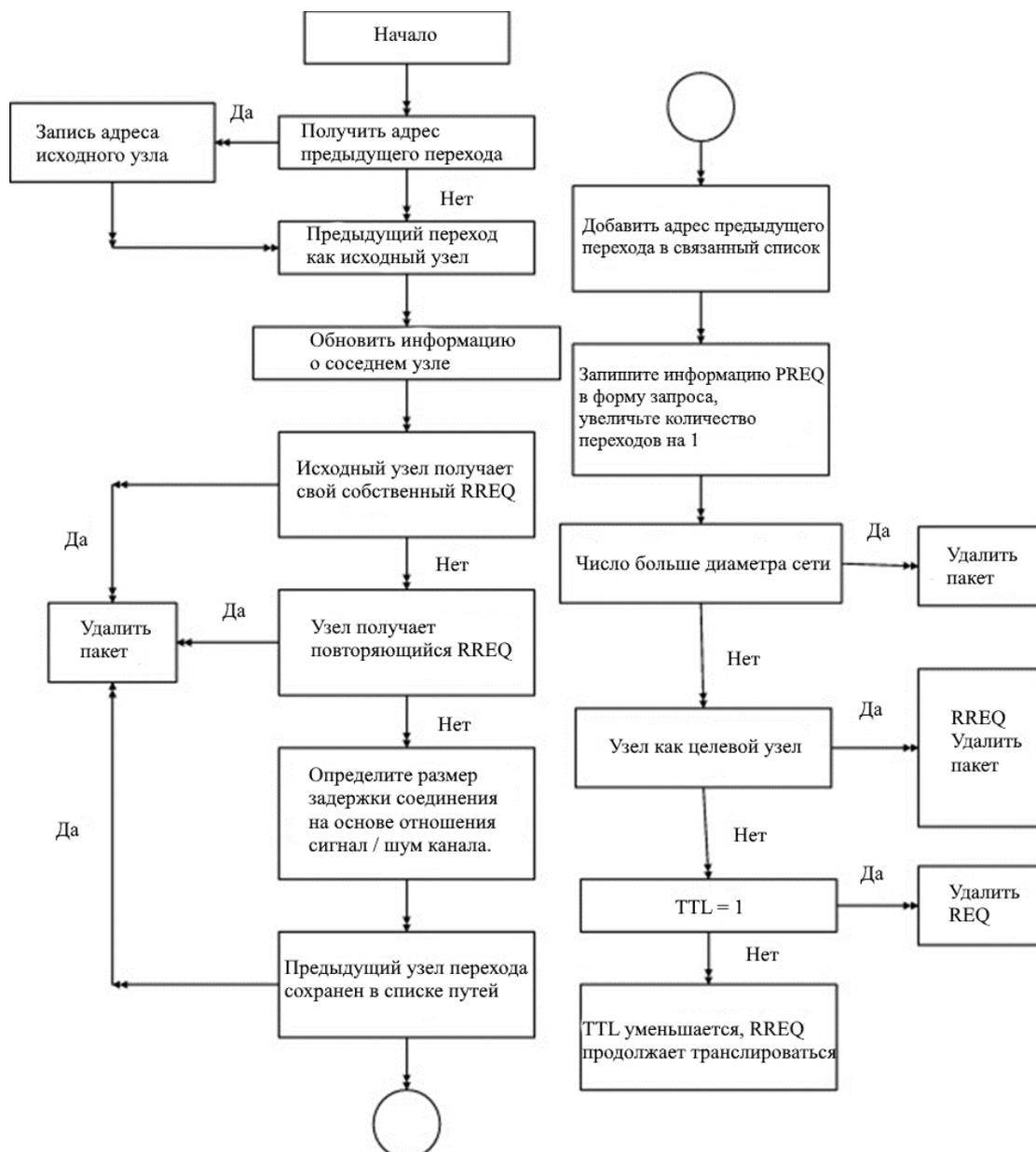


Рис. 4. Рабочий процесс модели сети

Результаты

Если набор всех областей распространения сети определен как $\{k\}$, где k служб необходимо передавать в пределах области распространения сети k ($k = 1, 2, \dots, M$), то будут использоваться те же ресурсы частотной области. Набор зон передачи передаваемой сети определяется как подмножество Z зон передачи сети [10].

Представляем трафик данных K пользовательских терминалов, поддерживаемых системой адаптивного распределения ресурсов нисходящей линии связи с базовой станцией. Базовая станция оснащена M передающими антеннами, и каждый пользовательский терминал имеет одну приемную антенну [11]. Предполагается, что, когда $K \geq M$ полоса частот разделена на N поднесущих. Можно считать, что матрица каналов не меняется в течение когерентного интервала. Принятый сигнал пользователя k на поднесущей где n можно выразить следующим образом:

$$y_{k,n} = h_{k,n}x_n + z_{k,n}. \quad (1)$$

где $h_{k,n} \in \mathbb{C}^{1 \times M}$ это канал матрица усиления пользователя k и записей $h_{k,n}$ считается одним и тем же независимой средней и единичной дисперсией, равной нулю; $x_n \in \mathbb{C}^{M \times 1}$ это символ, переданный из антенны базовой станции; $z_{k,n}$ это комплексный Гауссов шум, нулевая средняя и единичная дисперсия пользователя k .

На передающей стороне мы используем стратегию передачи с формированием диаграммы направленности с нулевым форсированием (ZFBF). В ZFBF передатчик выбирает активную группу пользователей и устанавливает значение $|S_n| \leq M$ этих данных для передачи $S_n \subset \{1, \dots, K\}$. Этот символ данных $S_{j,n}$ умножается на вектор формирования луча $W_{j,n}$ следующим образом:

$$X_n = \sum_{j \in S_n} \sqrt{P_{j,n}} W_{j,n} S_{j,n}. \quad (2)$$

Полученный сигнал (1) принимает следующий вид.

$$y_{k,n} = h_{k,n} \sum_{j \in S_n} \sqrt{P_{j,n}} W_{j,n} S_{j,n} + z_{k,n}. \quad (3)$$

В данной статье выбирается вектор формирования луча, удовлетворяющий условию нулевой интерференции, если $j \neq k$ $h_{k,n} W_{j,n} = 0$. $H_n(S_n)$ и $W_n(S_n)$ соответствующие значения подматрицы установлены на $H = [h_{1,n}^T, \dots, h_{K,n}^T]^T$, $W_n = [W_{1,n}, \dots, W_{K,n}]$.

Матрица формирования луча $W_n(S_n)$ можно просто получить, используя псевдообратное выражение $H_n(S_n)$ следующим образом:

$$W_n(S_n) = H_n(S_n)^+ = H_n(S_n)^* (H_n(S_n) H_n(S_n)^*)^{-1}. \quad (4)$$

Таким образом, может быть получено распределение мощности каждого пользователя на каждой поднесущей, а количество битов, переданных пользователем k на поднесущей n , может быть получено по формуле (6).

После того, как бит передачи пользователя на каждой поднесущей определен, алгоритм адаптивного распределения ресурсов выбирает наиболее подходящую поднесущую для пользователя на основе требований пользователя QoS и информации о состоянии очереди. Относительная скорость $r'_{k,n}$ пользователя k на поднесущей n , выраженная следующим образом:

$$r'_{k,n} = (r_{k,n} / \sum_N r_{k,n}) * r_{k,n}. \quad (5)$$

Относительная скорость $r'_{k,n}$ – представляет собой взвешенное значение, так же $r'_{k,n}$ не только отражает скорость передачи пользователя k на поднесущей n , но также отражает скорость передачи пользователя k на других поднесущих. Основная идея состоит в том, чтобы выделить каждую поднесущую соответствующему пользователю, не позволяя пользователю k вытеснять поднесущие, полезные для других пользователей. Коэффициент планирования используется для характеристики приоритета пользователя. Чем больше значение коэффициента планирования, тем выше уровень пользователя. Приоритеты пользователей для разных типов служб определяются следующим образом:

$$P_{r_k}(t) = \begin{cases} \beta_{rtpt} * r_{k,\min}(t) * r'_{k,n} * \max(1, W_k(t) / D_k(t))rtPS, \\ \beta_{nrtp} * r_{k,\min}(t) * r'_{k,n} * \max(1, Q_k(t) / \psi_k(t))nrtpS, \end{cases} \quad (6)$$

где β – параметр приоритета для разных типов пользователей; $r_{k,\min}(t)$ – минимальная скорость, требуемая для пользователя k ; $W_k(t)$ – время ожидания пакетных данных в очереди пользователя k ; $D_k(t) = \tau_k - W_k(t)$ – оставшаяся часть требуемой максимальной задержки для пакетных данных в k -м времени службы реального времени; ψ_k – пороговое значение пользовательской очереди не в режиме реального времени [12]. Высшее значение $Q_k(t)/\psi_k(t)$ указывает, что буфер k -очереди пользователя вот-вот переполнится, поэтому у пользователя должен быть более высокий приоритет. Приоритет службы установлен на -1, что означает, что выделение ресурсов службы учитывается только тогда, когда соблюдается минимальная скорость обслуживания служб в реальном времени и не в реальном времени, а ресурсы остаются. Когда минимальные скорости обслуживания для всех служб в реальном времени и не в реальном времени соблюдены, пользователь с лучшими условиями канала выбирается для распределения оставшихся ресурсов для максимизации пропускной способности системы.

Заключение

Создание видео коммуникаций с «удаленными, интерактивными и совместными» функциями стало тенденцией в развитии видеоприложений в сфере образования [13]. Кибербезопасность применяется во всех сферах жизни. В данной статье был разработан метод адаптивного распределения ресурсов для повышения качества передачи образовательного видео и применение безопасности сети

связи для повышения качества передачи образовательного видео. Этот алгоритм является подходящим методом распределения ресурсов между кластерами. По сравнению с другими алгоритмами разные пакеты служебных данных пересылаются по разным путям, что снижает потребление энергии при передаче данных для требуемых служб с малой задержкой и улучшает баланс нагрузки всей сети. Алгоритм реализации схемы состоит из двух частей: стратегии динамического выделения кэша и алгоритма адаптивного выделения ресурсов. Эта стратегия учитывает характеристики канала сети связи и общую мощность передачи базовой станции, а также ограничения общего буфера. По сравнению с существующими алгоритмами этот алгоритм повышает информационную безопасность, гарантируя многопользовательское и мульти сервисное QoS, а также значительно повышает пропускную способность системы и скорость потери пакетов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Gandotra P. Sector-based radio resource allocation (SBRRRA) algorithm for better quality of service and experience in device-to-device (D2D) communication / P. Gandotra, R. K. Jha, S. Jain // IEEE Trans. Veh. Technol. – 2018 – 67(7) – С. 5750-5765.
2. Зубов Г.Н. Диагностика аутентичности видеофонограмм, способы и признаки модификации, критерии оценки / Г.Н. Зубов – М., 2018.
3. Нгуен Динь Минь. Критерии оценки качества сжатых изображений // Известия вузов, специальный выпуск. – М.: МИИГАиК, 2017 - С. 27-29.
4. Gandotra P. A survey on device-to-device (D2D) communication: Architecture and security issues / P. Gandotra, R. K. Jha, S. Jain // J. Network Comput. Appl. – 2017 – 78 – С. 9-29.
5. Behrens W. Development of a questionnaire for the screening of communication processes in transdisciplinary research alliances / W. Behrens, C. Joob, A. Richert, S. Jeschke // Automation, Communication and Cybernetics in Science and Engineering – 2016 – 1 – С. 665-676.
6. Оков И.Н. Аутентификация речевых сообщений и изображений в каналах связи. Военная академия связи. СПб, Издательство Политехнического университета/ И.Н Оков. – 2006. – С. 300-303.
7. Володин, А.А. Обработка видео в системах телевизионного наблюдения / А.А. Володин, В.Г. Митько, Е.Н. Спинко // Вопросы защиты информации. – 2002. - №4(59). – С. 34-47.
8. Лопухов И. Резервирование промышленных сетей Ethernet на втором уровне OSI: стандарты и технологии / И. Лопухов // Современные технологии автоматизации. – 2009 -№3 – С. 16-32.
9. Chen X. Ant colony learning method for joint MCS and resource block allocation in LTE Femtocell downlink for multimedia applications with QoS guarantees / X. Chen, L. Li, X. Xiang // Multimedia Tools Appl – 2017 – 76(3)- С. 4035-4054.
10. Токарев Д.А., Стародубцев П.Е., В.Г. Грибунин. Решения по перехвату и чтению информации, передаваемой по защищенным сетевым протоколам. Известия института инженерной физики. Серпухов: Изд-во МОУ «ИИФ» 2018г. - №2 – С. 10.
11. Анин Б.Ю. Защита Компьютерной информации / Б.Ю. Анин. СПб.: БВХ - Петербург, 2000. – С. 384-388.
12. Мартимов Р.Ю. Классификация методов защиты целостности видеоданных. Т38 Технические науки: проблемы и перспективы: материалы III Междунар. науч. конф. (г. Санкт-Петербург, июль 2017 г.). – СПб.: Свое издательство, 2017 г. – С. 15-18.
13. Независимый российский информационно-аналитический центр : [сайт]. – Москва, 2005. – URL: <https://www.anti-malware.ru/practice/methods/Employee-Remote-Work-Cybersecurity> (дата обращения: 15.02.2022).