



УДК 061.68

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ VPN В SDN-КОНТРОЛЛЕРЕ В СЕТЯХ ЭЛЕКТРОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

С. С. ВРУБЛЕВСКИЙ,
старший инженер кафедры связи, к. т. н.

А. А. БЫСОВ,
доцент, начальник цикла кафедры связи, к. т. н.

Военная академия Республики Беларусь

Предложен способ управления туннелями виртуальных частных сетей (Virtual Private Network, VPN) в сетях электросвязи специального назначения (СЭСН) путем реализации концепции программно-конфигурируемых сетей (Software Defined Network, SDN). Представлена математическая модель виртуальной частной сети, применение которой в SDN-контроллере позволяет определять минимально необходимую величину буфера обмена виртуального маршрутизатора в оптимальном маршруте VPN-туннеля.

Ключевые слова: сеть электросвязи специального назначения, виртуальные частные сети, программно-конфигурируемый контроллер.

ВВЕДЕНИЕ

Сегодня в СЭСН наблюдается значительный рост объемов передаваемого трафика за счет необходимости предоставлять такие услуги, как видео-конференц-связь, IP-телефония, электронная почта, геоинформационные сервисы, удаленное управление устройствами, передача видеопотока и команд управления с беспилотного летательного аппарата, что подразумевает использование больших пропускных способностей каналов связи, а также усложняет управление устройствами в сети [1, с. 46–48].

Следует отметить, что сетевые технологии в СЭСН развиваются параллельно с сетями электросвязи общего пользования. Это подразумевает рост применения современных телекоммуникационных технологий. Одной из них является технология VPN, которая обеспечивает как разделение каналов, так и защищенное соединение абонентов.

Управление сетями VPN – сложная задача, однако иерархическая структура СЭСН позволяет осуществлять администрирование сетей VPN централизованно и эффективно. С этой целью в [2] для администрирования VPN-туннелей предложены соответствующие сервер и алгоритм. Конфигурация и управление

VPN-туннелями – непростой процесс, что при масштабировании сети и росте числа услуг существенно повысит нагрузку на процессоры коммутационных устройств.

Одно из эффективных решений данной задачи – использование программно-конфигурируемых сетей (SDN). Сеть SDN – это сеть передачи данных, в которой функции управления сетью и передачи данных разделены за счет применения центра управления (SDN-контроллер).

По структуре сети SDN подразделяются:

- на инфраструктурный уровень – набор коммутационных устройств второго уровня (в соответствии с моделью открытых информационных систем) и каналов передачи данных;
- уровень управления – сетевая операционная система с установленными сетевыми приложениями, обеспечивающая сетевые сервисы и прикладной программный интерфейс (Application Program Interface) для управления сетевыми устройствами и сетью;
- уровень приложений (для гибкого и эффективного управления сетью).

Анализ современных работ, исследующих возможности интеграции SDN в СЭСН, показывает, что SDN позволит повысить не только степень интеллектуализации управления телекоммуникационным оборудованием и самым значительно увеличить гибкость и масштабируемость СЭСН, но и уровень информационной безопасности [1, 3].

Применение SDN-контроллера позволяет повлиять на информационную безопасность за счет реализации следующих инструментов: централизованное управление политиками безопасности, интеграция с системами безопасности (система обнаружения вторжений, межсетевой экран),

ОСНОВНАЯ ЧАСТЬ

Имея возможность гибкого конфигурирования виртуальных коммутационных устройств, можно изменить их свойства, влияющие на несколько основных аспектов QoS: задержку передачи и вероятность потери пакета.

Изменения величины буфера обмена виртуальных маршрутизаторов (далее – величина буфера) позволит косвенно оказывать влияние на величину задержки передачи пакета в оптимальном маршруте VPN. Определение величины буфера может возлагаться на SDN-контроллер.

Один из способов решения данной задачи – совершенствование математической модели виртуальной частной сети в СЭСН и реализация ее функций в SDN-контроллере [6]. Предполагаемая схема применения SDN-контроллера в СЭСН представлена на рисунке 1.

Данная модель позволяет оценить ресурс сети, выраженный в пропускной способности канала связи, при учете задержки передачи пакета. Модернизацией математической модели виртуальной частной сети является внесение возможности расчета величины буфера и вероятности потери пакетов.

В математической модели VPN СЭСН представлена в виде ориентированного графа $G=(X, E)$,

динамическое управление трафиком и анализ его в режиме реального времени. Однако в вопросах обеспечения информационной безопасности технология SDN не является абсолютным решением [4].

Виртуализация сетевых устройств (виртуальных маршрутизаторов) также позволит эффективно решать задачу балансировки нагрузки в сети, чтобы поддерживать принцип равномерного распределения трафика на каждое коммутационное устройство. Решение данной задачи способствует выполнению требований по качеству обслуживания пользователей (Quality of Service, QoS) в соответствии с [5, с. 18–19].

где X – множество вершин (маршрутизаторы в моделируемой сети), E – множество ребер (соединительных линий). Оптимальные маршруты в математической модели виртуальной частной сети определяются посредством алгоритма Дейкстры, что соответствует применяемому на сегодняшний день в маршрутизаторах СЭСН протоколу Open Shortest Path First (OSPF).

Введем матрицу минимально необходимых величин буферов для каждого маршрута

$$B_{opt\ ij} = \begin{bmatrix} b_{opt\ 11} & b_{opt\ 12} & \dots & b_{opt\ 1X} \\ b_{opt\ 21} & b_{opt\ 22} & \dots & b_{opt\ 2X} \\ \vdots & \vdots & \vdots & \vdots \\ b_{opt\ X1} & b_{opt\ X2} & \dots & b_{opt\ XX} \end{bmatrix}, \quad (1)$$

где $b_{opt\ ij}$ – минимально необходимая величина буфера (данное соответствие представлено авторами в [7]) в оптимальном маршруте между i и j и определяется как

$$b_{opt\ ij} = w_{opt\ ij} \cdot q_{opt\ ij}, \quad (2)$$

где $w_{opt\ ij}$ – двухсторонняя задержка передачи пакета между i и j ($i=1, \dots, X, j=1, \dots, X$); $q_{opt\ ij}$ – пропускная

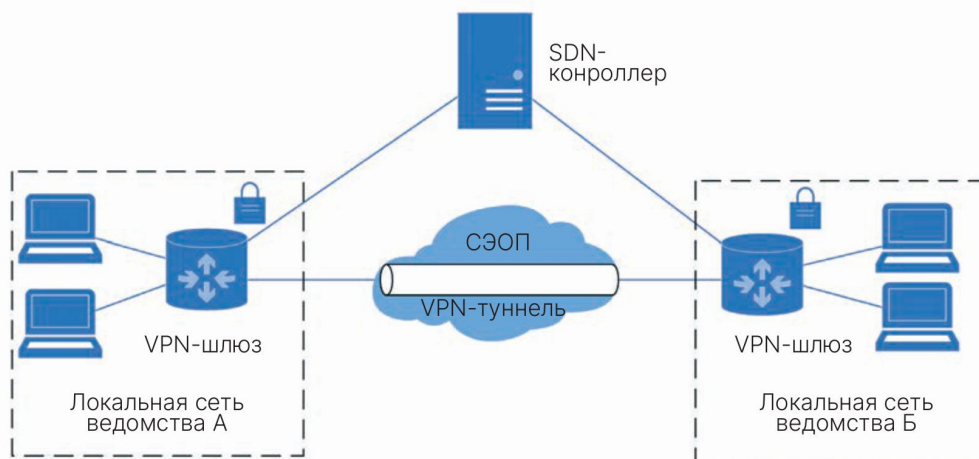


Рисунок 1. Схема применения SDN-контроллера

способность оптимального маршрута между i и j ; X – количество узлов [8].

Двухсторонняя задержка переадчи пакета $W_{\text{опт } ij}$ между маршрутизаторами i и j определяется как

$$W_{\text{опт } ij} = W_{\text{во } ij} + W_{\text{р } ij} + W_{\text{обр } ij} + W_{\text{с } ij} + W_{\text{о } ij}, \quad (3)$$

где $W_{\text{во } ij}$ – задержка внеузловой обработки пакета; $W_{\text{р } ij}$ – задержка распространения пакета; $W_{\text{обр } ij}$ – задержка обработки пакета маршрутизаторами; $W_{\text{с } ij}$ – задержка сериализации пакета; $W_{\text{о } ij}$ – задержка ожидания пакета в буферах маршрутизаторов.

Следует отметить, что в момент t_0 , когда терминальные устройства не генерируют трафик, суммарная задержка передачи пакета будет больше нуля, так как расчет $W_{\text{во } ij}$ и $W_{\text{р } ij}$ не зависит от значения интенсивности трафика. Следовательно, согласно выражению (2), даже в момент t_0 минимально необходимая величина буфера будет не нулевой.

Введем матрицу вероятностей потери пакетов в оптимальном маршруте между i и j

$$P_{\text{loss}} = \begin{bmatrix} P_{\text{loss } 11} & P_{\text{loss } 12} & \dots & P_{\text{loss } 1X} \\ P_{\text{loss } 21} & P_{\text{loss } 22} & \dots & P_{\text{loss } 2X} \\ \vdots & \vdots & \vdots & \vdots \\ P_{\text{loss } X1} & P_{\text{loss } X2} & \dots & P_{\text{loss } XX} \end{bmatrix}, \quad (4)$$

где $P_{\text{loss } ij} = r_{\text{опт } ij}^{b_{\text{опт } ij}}$ – вероятность потери пакетов в оптимальном маршруте между i и j ($i=1, \dots, X, j=1, \dots, X$), определяемая как загрузка канала связи в степени величины буфера обмена (данное соответствие представлено в [8], и авторы ссылаются на модель M/M/1 из классификации Кендалла – Башарина); $r_{\text{опт } ij} = \frac{\lambda_{ij}}{q_{\text{опт } ij}}$ – загрузка канала связи, равная отношению интенсивности трафика λ_{ij} к пропускной способности $q_{\text{опт } ij}$ оптимального маршрута [7]. Интенсивность трафика определяется в соответствии с математической моделью, представленной в [6].

На основе математической модели виртуальной частной сети в СЭСН с выражениями (1), (2), (4) исследовано влияние величины буфера на значения двухсторонней задержки передачи пакета (рисунок 2) и вероятности потери пакета (рисунок 3) при функционировании протокола OSPF.

На рисунках 2 и 3 показаны зависимости для оптимального маршрута между наиболее удаленными маршрутизаторами сети ($i=2, j=17$, т. е. $w_{\text{во } 217}$). Этот маршрут выбран как наихудший случай, поскольку он содержит максимальное количество промежуточных узлов, равное пяти (2–1–4–20–21–18–17). Данный критерий напрямую определяет максимальные значения задержки передачи пакета в рамках используемой модели, что делает пару маршрутизаторов 2-17 репрезентативными для анализа граничных характеристик сети.

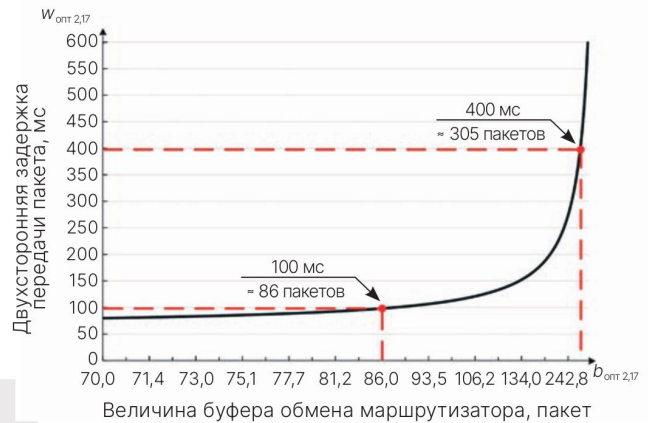


Рисунок 2. Зависимость двухсторонней задержки передачи пакета от величины буфера для загрузки канала 0,9

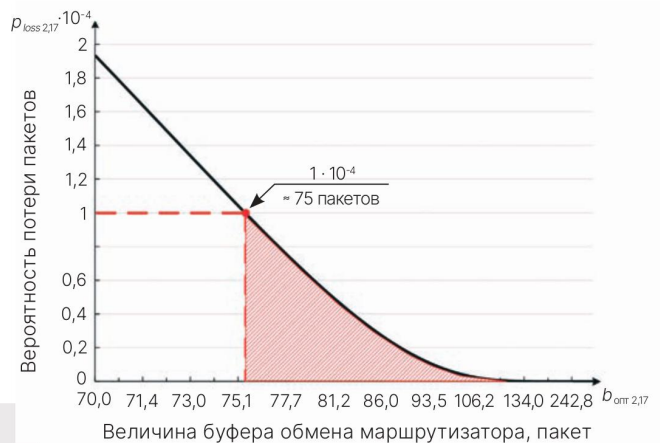


Рисунок 3. Зависимость вероятности потери пакетов от величины буфера обмена для загрузки канала 0,9

Исследование проведено при следующих условиях: задержка пакетизации – 20 мс (оптимальное значение для кодека G.711); кодек G.711 выбран ввиду того, что является основным для VoIP-трафика в СЭСН.

На рисунках 2 и 3 значение величины буфера изменяется в пределах от 70 (момент t_0) до 310,56 пакетов (момент, когда двухсторонняя задержка передачи пакета больше 400 мс).

Из анализа зависимости на рисунке 2 следует, что в рассматриваемой сети при выполнении требований QoS:

- для трафика класса 0-4 величина буфера при задержке передачи пакета в 100 мс равна 86 пакетам;
- для трафика класса 6-7 величина буфера при задержке передачи пакета до 400 мс не должна превышать значение в 305 пакетов (к классу трафика 5 требования по QoS не предъявляются).

Анализ зависимости, представленной на рисунке 3, показывает, что:

- вероятность потери пакета достигает значения, при котором выполняются требования

QoS для трафика класса 0-4, в 1×10^{-4} только при величине буфера в 75 пакетов;

- увеличение буфера позволяет значительно уменьшать вероятность потери пакета (так при величине буфера в 100 пакетов, вероятность потери пакетов достигает 1×10^{-6} , что соответствует требованию QoS к классам трафика 6-7).

При анализе полученных зависимостей сделан вывод: при росте величины буфера происходит не только уменьшение вероятности потери пакетов, но и увеличение двухсторонней задержки передачи пакета. Следовательно, слишком большая величина буфера позволит сохранить пакет (вероятность потери пакетов минимальна), но до конечного пользователя пакет придет с большой задержкой. Это ставит перед SDN-контроллером необходимость выбора буфера $b_{opt\ ij}$ между значениями $b_{opt\ ij}^{(100)}$ и $b_{opt\ ij}^{(400)}$, $b_{opt\ ij}^{(1 \cdot 10^{-6})}$ и $b_{opt\ ij}^{(1 \cdot 10^{-4})}$ при этом $b_{opt\ ij}^{(100)} \neq b_{opt\ ij}^{(1 \cdot 10^{-4})}$ и $b_{opt\ ij}^{(400)} \neq b_{opt\ ij}^{(1 \cdot 10^{-6})}$ (рисунок 4).

Для выполнения требования по QoS для различных классов трафика SDN-контроллеру необходимо решать следующую оптимизационную задачу:

$$\begin{cases} w_{opt\ ij}(b_{opt\ ij}), p_{loss\ ij}(b_{opt\ ij}) \rightarrow \min; \\ b_{opt\ ij} \in \Omega; \\ w_{opt\ ij} \leq w_{\pi}(k); \\ p_{loss\ ij} \leq p_{\pi}(k); \\ k = 0, 7; \\ i, j = 1, \dots, X; \end{cases} \quad (4)$$

где Ω – множество возможных альтернатив, рассматриваемых при поиске решения задачи; $w_{\pi}(k)$ – пороговое значение задержки передачи пакета для соответствующего класса трафика $k=0, 7$; $p_{loss\ ij}$ – вероятность потери пакета между маршрутизаторами i и j ; $p_{\pi}(k)$ – пороговое значение вероятности потери пакета для соответствующего класса трафика $k=0, 7$ [9, с. 42–45].

Согласно (4) для решения оптимизационной задачи необходимо найти такую величину буфера,

чтобы задержка передачи и вероятность потери пакета были минимальны. При этом они должны быть либо равны пороговым значениям для определенного класса трафика, либо меньше их.

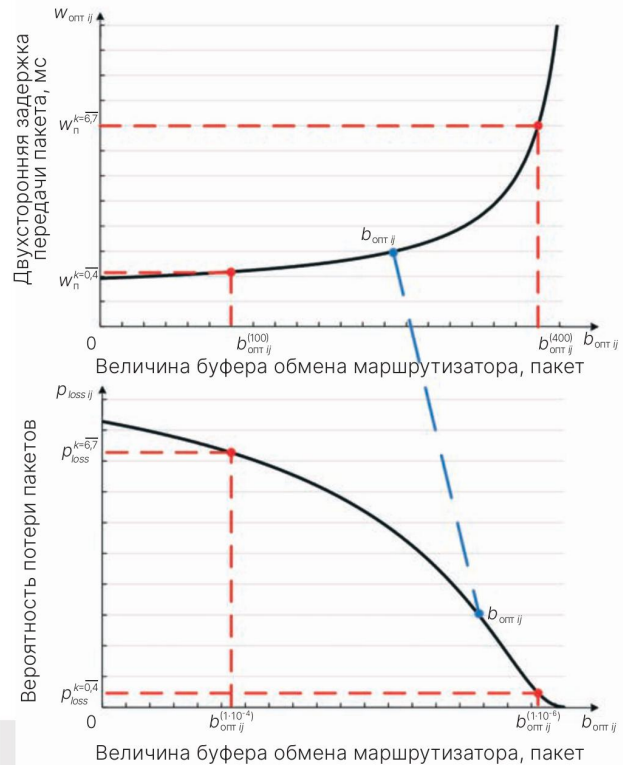


Рисунок 4. Схематичное описание выбора буфера для выполнения требований QoS в VPN-туннеле: $b_{opt\ ij}^{(100)}$ – величина буфера при минимальной задержке передачи пакета в 100 мс; $b_{opt\ ij}^{(400)}$ – величина буфера при максимальной задержке передачи пакета в 400 мс; $b_{opt\ ij}^{(1 \cdot 10^{-6})}$ – величина буфера при минимальной вероятности пакета в $1 \cdot 10^{-6}$; $b_{opt\ ij}^{(1 \cdot 10^{-4})}$ – величина буфера при значении максимальной вероятности пакета в $1 \cdot 10^{-4}$

ВЫВОДЫ

- ♦ Реализация программно-конфигурируемых сетей в СЭСН открывает новые горизонты для управления сложными сетевыми инфраструктурами. **Централизованный SDN-контроллер**, принимая на себя функции обработки маршрутизации и управления трафиком, **существенно разгружает коммутационные устройства, что особенно критично в условиях роста объема данных.**
- ♦ Применение граф-комбинаторной модели VPN демонстрирует свою эффективность в условиях динамически изменяющейся нагрузки. Например, в случае экстренного

развертывания сетей связи для аварийно-спасательных операций такая **модель позволяет оперативно перенастраивать маршруты, избегая перегруженных узлов и обеспечивая приоритетное обслуживание критически важного трафика.**

- ♦ Оптимизационная задача (4), решаемая SDN-контроллером, играет ключевую роль в балансировке между требованиями QoS и ресурсными ограничениями. Анализ зависимости задержки передачи от размера буфера маршрутизатора, представленный на рисунках 2 и 3, выявляет нелинейный

характер этой взаимосвязи. При малых значениях буфера (менее 50 МБ) наблюдается экспоненциальный рост вероятности потери пакетов из-за переполнения, тогда как увеличение буфера свыше 200 МБ приводит к неприемлемым задержкам, превышающим 400 мс. Это особенно критично для сервисов реального времени, таких как управление беспилотными системами, где даже кратковременная задержка может привести к потере управления или аварии. Таким образом, предложенная **модель определяет «золотую середину» буфера в диапазоне 80–120 МБ, что обеспечивает соблюдение пороговых значений задержки (не более 150 мс) при вероятности потерь пакетов ниже 0,1%.**

- ♦ **Внедрение SDN-технологий в СЭСН способствует усилению информационной безопасности.** Централизованный контроль трафика через SDN-контроллер позволяет реализовать продвинутые механизмы защиты, такие как динамическая сегментация сети для изоляции подозрительных узлов, автоматическое обновление правил фильтрации на основе анализа угроз в реальном времени, а также сквозное шифрование данных в VPN-туннелях. Например, в случае обнаружения DDoS-атаки SDN-контроллер может

перенаправить атакующий трафик в «песочницу», минимизируя воздействие на рабочую инфраструктуру.

Однако остаются и вызовы. Один из них – обеспечение совместимости SDN-контроллера с устаревшим оборудованием, которое до сих пор используется в некоторых сегментах СЭСН. Решение проблемы видится в разработке гибридных архитектур, где SDN-контроллер управляет современными устройствами через OpenFlow, а для legacy-оборудования используются шлюзы – переводчики протоколов. Кроме того, требуется дальнейшая работа по стандартизации интерфейсов взаимодействия между SDN-контроллерами разных производителей для беспрепятственного масштабирования решений. Предложенный подход решает текущие задачи управления VPN-туннелями в СЭСН и одновременно создает основу для внедрения инновационных технологий будущего, таких как квантовая криптография для защиты данных или нейроморфные вычисления для обработки сетевых событий. Это подтверждает, что интеграция SDN и математического моделирования является стратегическим направлением развития телекоммуникационных систем специального назначения, которое обеспечивает их соответствие вызовам цифровой трансформации. **ВС**

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Абазина, Е. С. Обоснование требований к пропускной способности канала связи для видеотрафика в перспективной мультисервисной сети специального назначения / Е. С. Абазина, А. В. Бусыгин, С. М. Одоевский // Труды воен.-косм. акад. им. А. Ф. Можайского. – 2020. – № 672. – С. 41–47.
2. Врублевский, С. С. Повышение пропускной способности VPN-туннелей в сетях электросвязи специального назначения / С. С. Врублевский // Вестник ВАРБ. – 2023. – № 3 (80). – С. 19–26.
3. Репин, Б. Г. Перспективы использования технологии SDN в системах связи специального назначения / Б. Г. Репин, Б. П. Репин, А. Н. Григорчук // Научная жизнь. – 2021. – № 1 (39). – С. 108–110.
4. Розендал, К. А. Средства информационной безопасности в программно-определяемых сетях / К. А. Розендал // Умная цифр. экономика. – 2022. – Т. 2, № 3. – С. 6–11.
5. Требования к сетевым показателям качества для служб, основанных на протоколе IP: Рекомендация Y.1541. – Женева: МСЭ, 2006. – 66 с.
6. Врублевский, С. С. Математическая модель VPN в сети электросвязи специального назначения, определяющая запас по пропускной способности, для планируемых VPN-туннелей с учетом класса передаваемого трафика / С. С. Врублевский, Е. В. Машкин, А. А. Бысов // Доклады БГУИР. – 2023. – № 4. – С. 93–100.
7. Kung, H. T. Sizing and Management of Roter Partners Buffers / H. T. Kung // Second Annual Sprint Applied Research Partners Advanced Networking (SPARTAN) Symposium. – 1998. – Vol. 1, № 9. – P. 34–37.
8. Афонцев, Э. В. О выборе размера буфера маршрутизатора компьютерной сети, нагруженного интенсивным трафиком реального времени / Э. В. Афонцев, М. К. Гребенкин, С. В. Поршнева // Известия Томского политехн. ун-та. – 2008. – Т. 313, № 5. – С. 106–109.
9. Аттенков, А. В. Методы оптимизации: учеб. пособие / А. В. Аттенков, С. В. Галкин, В. С. Зарубин. – Изд. 2-е – М.: Изд-во МГТУ им. Н. Э. Баумана, 2003. – 400 с.

The article proposes a method for managing virtual private network (VPN) tunnels in special-purpose telecommunications networks (SPTN) by implementing the concept of software-defined networks (SDN). A mathematical model of a virtual private network is presented, the use of which in an SDN controller allows for determining the minimum required virtual router exchange buffer size along the optimal VPN tunnel route.

Keywords: special-purpose telecommunications network, virtual private networks, software-defined controller.

Статья поступила в редакцию 30.01.2026.