УДК 061.68

Анализ характеристик качества обслуживания сети VPN на основе имитационной модели

Статья посвящена анализу характеристик качества обслуживания виртуальной частной сети на основе имитационной модели. Доказана необходимость маркирования пакетов VPN-трафика в сетях электросвязи специального назначения.

Е. В. МАШКИН,
кандидат технических наук, доцент, заместитель директора по развитию – первый заместитель директора ОАО «АГАТ-СИСТЕМ»

С. С. ВРУБЛЕВСКИЙ,
адъюнкт кафедры связи

А. А. БЫСОВ,
кандидат технических наук; начальник цикла кафедры связи

Военная академия Республики Беларусь

Ключевые слова:
сеть электросвязи специального назначения, виртуальная частная сеть, имитационная модель, характеристики качества обслуживания, алгоритм обработки очередей, класс трафика.

Введение. Виртуальная частная сеть (Virtual Private Network VPN) представляет собой способ и систему организации безопасного информационного пространства между локальными сетями и отдельными компьютерами, объединёнными через открытую среду передачи.

По виду технического решения VPN классифицируют:

- на виртуальные частные сети с удаленным доступом;
- ведомственные;
- межведомственные;
- локальные [1].

Ведомственные (корпоративные) сети VPN предназначены для обеспечения защищенного взаимодействия между подразделениями внутри организации или между группой организаций, объединенных корпоративными сетями связи (рисунок 1). Примером ведомственных сетей VPN могут служить сети электросвязи специального назначения (СЭСН), банковские сети и др.

Научно-методологический аппарат для анализа и синтеза сетей VPN в глобальных сетях не в полной мере применим для СЭСН ввиду того, что существующие методы анализа и синтеза сетей VPN, как правило, используются в системе «провайдер-пользователь», в которых качество обслуживания (Quality of Service (QoS)) обеспечивается путем расширения полосы пропускания, что не является допустимым в СЭСН с ограниченной полосой пропускания каналов связи.

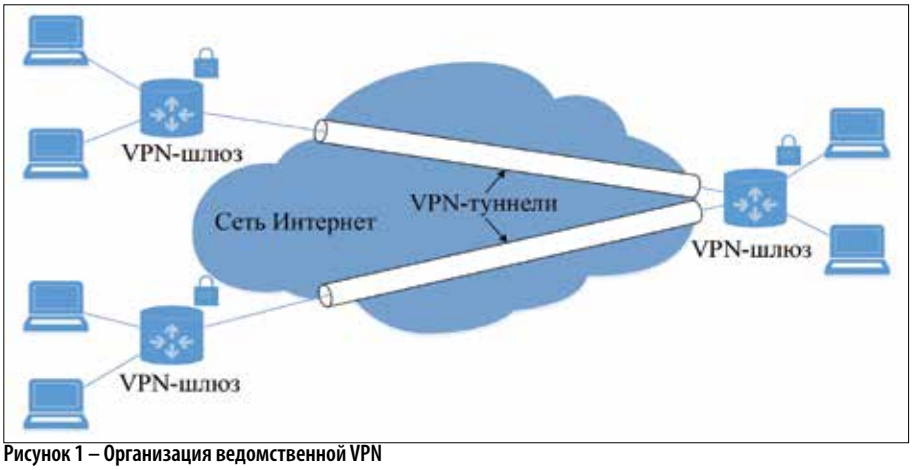

Рисунок 1 – Организация ведомственной VPN

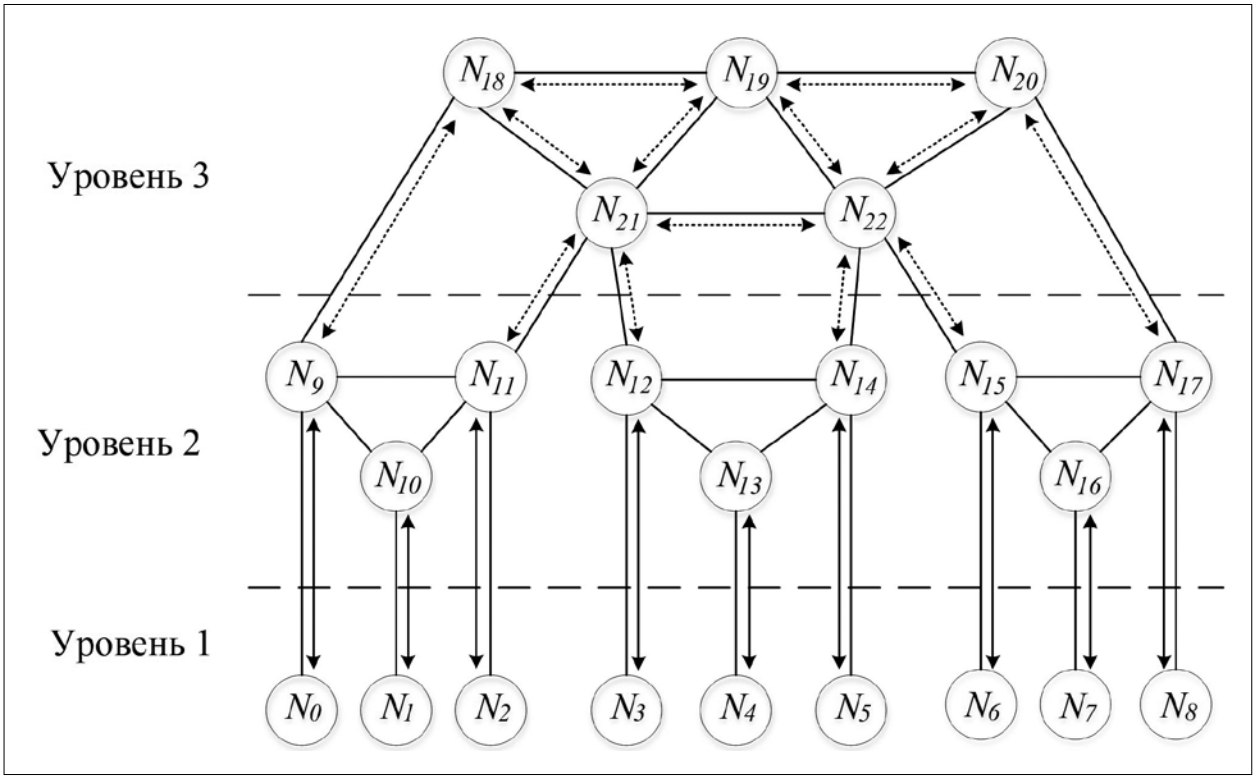

Рисунок 2 – Иерархическая структура СЭСН

Основная часть. Для определения неизвестных характеристик в сети, получения статистических данных разработана имитационная модель СЭСН с цифровыми средствами связи. СЭСН представляет многоуровневую систему взаимодействующих элементов, объединенные в подсистему из трех уровней, которые определены принципом иерархичности обеспечения управления (рисунок 2).

Данная модель СЭСН имитирует элементарные явления, составляющие процесс работы сети, с сохранением их логической структуры и последовательности протекания во времени [2].

Целями моделирования являются оценка характеристик качества обслуживания пользователей сети (задержка передачи пакетов, джиттер, вероятность потери пакетов) при использовании технологии VPN с существующими принципами их организации; получение статистических данных о работе СЭСН с использованием технологии VPN.

Характеристики маршрутизаторов и VPN-шлюзов, используемые в имитационной модели, представлены в таблицах 1 и 2.

Основным параметром, характеризующим коммутатор, является скорость коммутации, равная 72·106 пакетов/с.

Для выполнения этапа программной реализации модели был проведен анализ сред моделирования сетей: OPNet, OMNeT++, Network Simulator – 2 (NS-2), Network Simulator – 3 (NS-3). Сравнительный анализ сред моделирования представлен в таблице 3.

Каждая из сред моделирования предназначена для решения конкретных задач разной степени абстракции.

Таблица 1 – Характеристики маршрутизаторов

Уровень управления	Протоколы маршрутизации	Производительность, тыс. пакетов/с	Интерфейсы	Дисциплины обслуживания очередей	Метод борьбы с перегрузками
1	RIP	10	Fast Ethernet, SHDSL	FIFO, FQ, SFQ	RED
2					
3	OSPF (MPLS)	70-80			

Таблица 2 – Характеристики VPN-шлюзов

Уровень управления	Производительность, тыс. пакетов/с	Интерфейсы	Алгоритмы шифрования
1	10	Fast Ethernet	DES, AES (128, 192, 256-бит длина ключа)
2			
3	70–80		

Таблица 3 – Основные особенности сред моделирования

Особенности	OPNet	OMNeT++	NS-2	NS-3
Наличие библиотеки устройств	+	+	+	+
Пошаговая трассировка	–	+	+	+
Генерация отчетов	–	+	-	+
Стоимость, руб.	От 51 000	Бесплатно	Бесплатно	Бесплатно

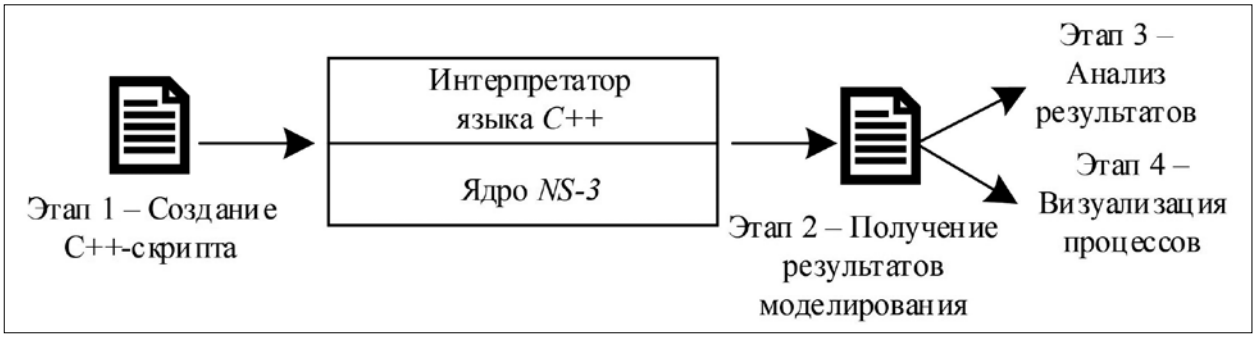

Рисунок 3 – Этапы программной реализации в NS-3

К достоинствам OPNet можно отнести:

- возможность планирования и оптимизации сети;
- создание аналитических моделей сети и протоколов связи.

Слабыми сторонами OPNet являются высокая стоимость базовой конфигурации, отсутствие трассировки моделей и недостаточная гибкость, что диктуется использованием собственной, нерасширяемой библиотекой устройств и ограничением наборов отчетов. В свою очередь недостатки OPNet могут решить среды моделирования OMNeT++ и NS-2, которые позволяют разрабатывать и моделировать телекоммуникационные системы любой сложности и степени абстракции, используют расширенный набор отчетов и т.д. Но в тоже время описание моделей происходит на двух языках программирования, что приводит к следующим ограничениям: сложности в обучение пользователей и сложности в реализации моделей и анализа результатов.

Для устранения ограничений NS-2 разработан NS-3, который представляет собой сетевой симулятор дискретного события с открытым исходным кодом, распространяемым под лицензией GNU GPLv2. Достоинствами данной среды моделирования являются:

- высокая степень абстракции;
- поддержка большого стека протоколов;
- высокое быстродействие исполнения рабочего скрипта модели (использование в качестве базового языка программирования для построения моделей C++);
- возможна работа с внешними инструментами для анализа данных (Wireshark) и визуализации работы сети (NetAnim) [3].

Анализ особенностей сред моделирования показал, что NS-3 способна в полной мере решить поставленные цели моделирования. Программная реализация в NS-3 включает в себя следующие этапы, представленные на рисунке 3.

Первым этапом программной реализации является создание скрипта, описывающего структуру и параметры сети, процесс циркуляции трафика и т.д.

При разработке скрипта были использованы следующие классы, имитирующие сетевые устройства, их функции, визуализацию и анализ работы всей сети (рисунок 4):

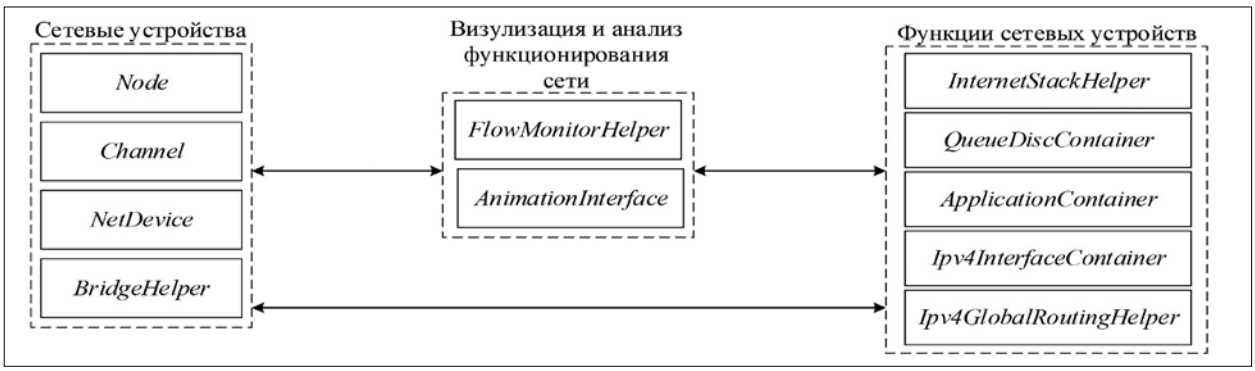

Рисунок 4 – Классы, используемые при разработке имитационной модели

- *Node – класс, описывающий узлы сети (коммутационные и терминальные устройства);*
- *Channel – класс, описывающий каналы связи (CsmaChannel, PointToPointChannel);*
- *NetDevice – класс, описывающий сетевые интерфейсы на устройстве (CsmaNetDevice, PointToPointNetDevice);*
- *BridgeHelper – класс, добавляющий функции коммутатора для узла сети;*
- *InternetStackHelper – класс, устанавливающий стек протоколов TCP/IP для устройств сети;*
- *QueueDiscContainer – класс, описывающий дисциплины обслуживания очередей;*
- *Ipv4InterfaceContainer – класс, присваивающий IP-адрес сетевым устройствам;*
- *ApplicationContainer – класс, имитирующий работу приложений на терминальных устройствах;*
- *Ipv4GlobalRoutingHelper – класс, реализующий протоколы маршрутизации.*

Анализ результатов и визуализация процессов моделирования осуществляется при помощи следующих классов:

AnimationInterface – класс, который визуализирует процесс функционирования сети, позволяет устанавливать положение устройств в сети, название, цвет узлов сети, а также добавление информации о пакетах;

FlowMonitorHelper – класс, позволяющий выводить результаты симуляции сети, автоматически обнаруживает все потоки, проходящие через сеть, и сохраняет о них сведения, которые могут потребоваться для анализа в виде файла формата .xml [4].

Оценка адекватности имитационной модели проводилась путем сравнения структуры и интенсивности трафика на входе маршрутизаторов, а также основных характеристик качества обслуживания (задержка передачи пакета, джиттер, вероятность потери пакетов), измеренных на участке реальной сети и имитационной модели. Для всех указанных параметров оценивался квадрат ошибки отклонения, который для рассматриваемых случаев был не более 5,2 %.

Исходя из проведенной выше проверки можно сделать вывод, что имитационная модель адекватна, описывает структуру сети и сетевые характеристики, что позволяет в полной мере проводить исследования сети.

Оценка результатов моделирования. В основу имитационной модели был положен вариант топологии СЭСН типовой структуры. На имитационной модели был произведен машинный эксперимент, целью которого являлось показать, что на сегодняшний день в СЭСН потоки данных, принадлежащие VPN-трафику, имеют низкие характеристики показателей качества обслуживания, которые могут быть повышены путем маркирования пакетов в соответствии с их классом трафика. Маркирование пакетов в модели осуществлялось VPN-шлюзом. Дальнейшая обработка маркированных пакетов проводилась при помощи алгоритма обработки очередей Priority Queuing (PQ – очередь с приоритетами). Для этого в используемом варианте СЭСН было установлено:

- 32 источника и приемника VoIP-трафика;
- 4 источника и приемника TCP-трафика.

Увеличение нагрузки на сеть производилось путем увеличения интенсивности трафика от 10 до 90 % загрузки сети, исходящего от источников VoIP-трафика на протяжении 60 секунд.

Поставленная цель достигалась получением и анализом зависимостей основных сетевых характеристик (задержка передачи пакета, джиттер, вероятность потери пакетов) от интенсивности для следующих алгоритмов обработки очередей с применением технологий VPN: First In First Out (FIFO – алгоритм обработки пакетов в порядке очередности); Random Early Detection (RED – алгоритм случайного раннего обнаружения перегрузок в сети); PQ.

Использование FIFO и RED в машинном эксперименте оправдано применением данных алгоритмов в маршрутизаторах, применяемых в СЭСН [5]. Результаты моделирования представлены на рисунках 5 – 7.

На рисунке 5 показано, что при значении интенсивности в 3,03 Мбит/с использование FIFO приводит к достижению 99,7 % задержки передачи пакета от максимально допустимого граничного значения,

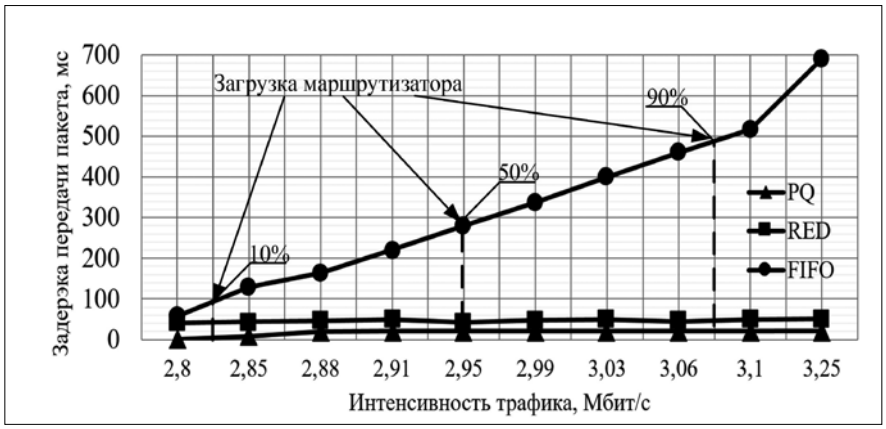

Рисунок 5 – Зависимости задержки передачи от интенсивности трафика при использовании VPN для PQ, RED, FIFO

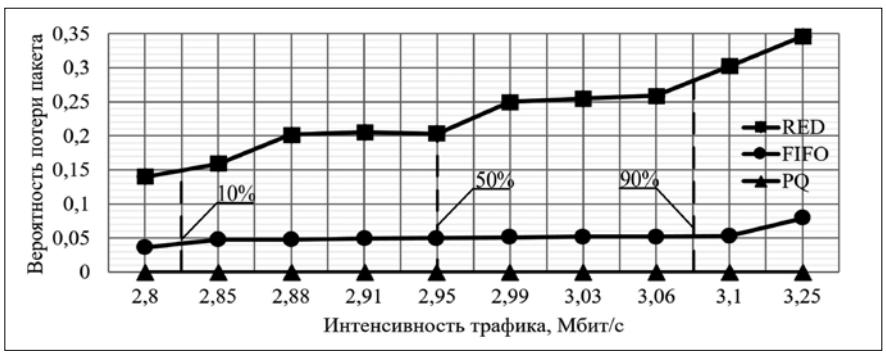

Рисунок 6 – Зависимости джиттера от интенсивности трафика при использовании VPN для PQ, RED, FIFO

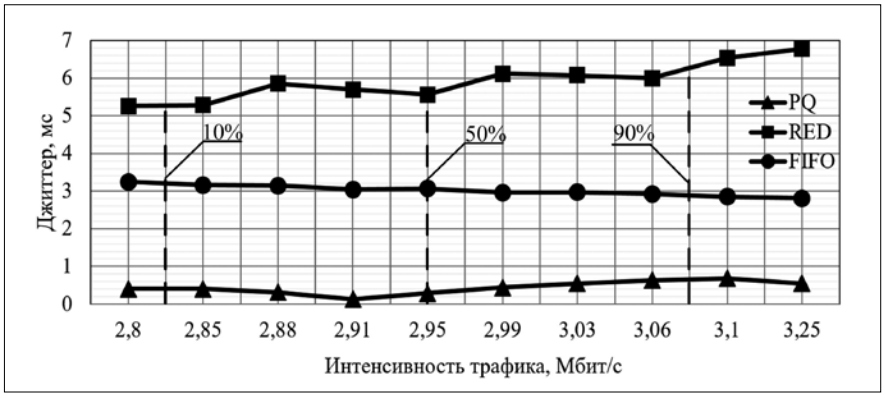

Рисунок 7 – Зависимости вероятности потери пакета от интенсивности трафика при использовании VPN для PQ, RED, FIFO

равного 400 мс [6], в то время как в RED – 12,3 %. Это объясняется тем, что при RED пакеты отбрасываются заранее, а не после переполнения буфера, как у FIFO.

При назначении пакетам VPN-потока меток с наивысшим приоритетом время ожидания пакета в буфере маршрутизатора значительно сокращается, тем самым уменьшая задержку передачи пакета, где при интенсивности в 3,03 Мбит/с значение задержки передачи пакета составляет 5,3 % от максимально допустимого значения.

Анализ зависимостей на рисунке 6 показывает, что при показателе интенсивности в 3,03 Мбит/с наименьшее значение джиттера составляет 1,1 % от максимально допустимого граничного значения, равного 50 мс [6], при использовании PQ, в свою очередь FIFO – 5,9 %, RED – 12,2 %.

На рисунке 7 показано, что приоритетная обработка пакетов, принадлежащих VPN-трафику, в маршрутизаторах приводит к их пересылке от одной конечной точки к другой с низкой вероятностью потери пакета. Так, для PQ при интенсивности 2,88 Мбит/с вероятность потери пакета достигает 0,001, в то время как в FIFO – 0,05, для RED – 0,2.

Выводы. Анализ данных характеристик приводит к следующим выводам:

- существующие механизмы обработки пакетов в СЭСН (применение FIFO и RED) не обеспечивают качество обслуживания пользователей сети;
- маркирование и последующая обработка пакетов VPN-трафика в СЭСН позволяют существенно повысить характеристики качества обслуживания сети. Следовательно, необходимо разрабатывать и применять механизмы, которые формируют определенные метки пакетов, в соответствии с классами трафика. Разработка данного механизма является дальнейшим направлением исследования.

ЛИТЕРАТУРА

1. **Давыдов, А. Е.** Защита и безопасность ведомственных интегрированных инфокоммуникационных систем / А. Е. Давыдов, Р. В. Максимов, О. К. Савицкий. – М.: Воентелеком, 2017. – 536 с.
2. **Шеннон, Р.** Имитационное моделирование систем – искусство и наука / Р.Шеннон; пер. с англ. под ред. Е. К.Масловского. – М.: Мир, 1978. – 418 с.
3. NS-3 Manual [Электронный ресурс]. – Режим доступа: https://www.nsnam.org/docs/manual/ns-3-manual.pdf (дата обращения: 20.03.2022).
4. NS-3 Model Library [Электронный ресурс]. – Режим доступа: https://www.nsnam.org/docs/models/ns-3-model-library. – Дата доступа: 20.03.2022.
5. Разработать и организовать производство аппаратно-программного комплекса средств коммутации и маршрутизации цифровых потоков для полевых систем связи: отчет об ОКР / ОАО «АГАТ-СИСТЕМ»; рук. В. М. Зайцев. – 2009. – 124 с.
6. Требования к сетевым показателям качества для служб, основанных на протоколе IP : Рекомендация Y.1541. – Женева: МСЭ, 2006. – 16 с.

Получено: 19.04.2022.