

УДК 061.68

Анализ математических моделей VPN и обоснование необходимости их применения в сетях электросвязи специального назначения

Статья посвящена анализу математических моделей виртуальных частных сетей. Указана особенность моделирования виртуальных частных сетей в сетях связи специального назначения.

Введение. В статье рассматриваются особенности применения виртуальных частных сетей в сетях электросвязи специального назначения, их математические модели: канальная, потоковая и комбинированная модели.

Основная часть. Виртуальная частная сеть (Virtual Private Network, VPN) представляет собой выделенную сеть передачи данных, построенную на инфраструктуре телекоммуникационной сети общего пользования (рис. 1), в которой конфиденциальность и защищенность информации пользователя обеспечиваются механизмами туннелирования и средствами информационной безопасности [1].

Виртуальные частные сети подразделяются:

на сети, построенные на оборудовании, которое устанавливается на стороне клиента и служит для его подключения к сети провайдера;

сети, построенные на оборудовании, которое устанавливается на стороне провайдера.

И те и другие подразделяются на три класса в зависимости от принципа организации связи пользователей сети:

ведомственные (внутрикорпоративные) сети VPN – как правило, строятся

на собственной сетевой инфраструктуре без использования ресурсов сети связи общего пользования;

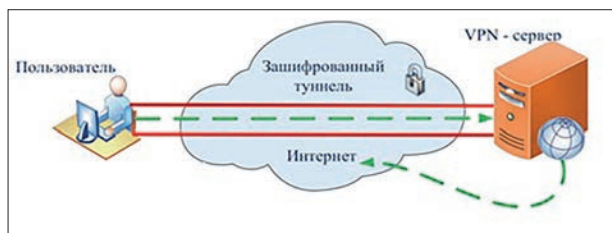


Рисунок 1 – Виртуальная частная сеть

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

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

С. С. ВРУБЛЕВСКИЙ,
адъюнкт кафедры связи

УО «Военная академия Республики Беларусь»

Ключевые слова:

сеть электросвязи специального назначения, виртуальная частная сеть, граф-комбинаторные алгоритмы, теория массового обслуживания, тензорный анализ, теория сетевого исчисления.

межведомственные (межкорпоративные) сети VPN – используют как собственную сетевую инфраструктуру, так и инфраструктуру сети провайдера;

сети VPN удаленного доступа – данный класс сетей VPN предполагает подключение пользователя к сети VPN при помощи специального аппаратного (криптомаршрутизаторы) и программного (Cisco AnyConnect Secure Mobility Client, Avast SecureLine VPN) обеспечения.

Создание ведомственных (замкнутых) сетей VPN оправдано при использовании аппаратуры IP-шифрования с целью разграничения общего и зашифрованного трафика. Примером ведомственных сетей VPN могут служить сети электросвязи специального назначения (СЭСН), банковские сети и др.

Виртуальные частные сети могут быть реализованы на базе протоколов модели OSI на следующих уровнях:

канальный – L2VPN (L2TP, PPTP, VPLS, VPWS);
сетевой – L3VPN (IPsec, GRE, BGP/MPLS, VPRN);
сеансовый – L5VPN [2].

Виртуальные частные сети, реализованные на базе протоколов третьего уровня, получили наибольшее распространение. Это обусловлено центральной ролью протокола IP в стеках протоколов модели OSI.

Сеть электросвязи специального назначения (СЭСН) – это сеть, предназначенная для обеспечения нужд государственного управления, национальной безопасности, обороны, охраны правопорядка, предупреждения и ликвидации чрезвычайных ситуаций [3].

Применение технологии VPN получило широкое распространение в СЭСН различных государств по следующим причинам:

- применение стандартных стеков протоколов (например, TCP/IP);

- использование средств IP-шифрования, для построения защищенных каналов (туннелей VPN);

- необходимостью разграничения трафика в зависимости от его класса и приоритета пользователей.

СЭСН специального назначения представляет многоуровневую систему взаимодействующих элементов, которые объединены в подсистемы различного уровня. В состав СЭСН специального назначения входят транспортные сети и сети доступа. Транспортная сеть состоит из центров коммутации СЭСН, включающих высокопроизводительные маршрутизаторы, а также средства каналаообразования (станции радиорелейной, тропосферной, спутниковой связи, мультиплексорное и модемное оборудование).

На сегодняшний день, СЭСН представляет совокупность двух сетей: сеть с коммутацией пакетов и сеть с коммутацией каналов.

Основным оборудованием сети с коммутацией пакетов являются коммутаторы и маршрутизаторы различного уровня (примеры сетевых устройств представлены на рис. 2).

Наличие средств коммутации и маршрутизации мультисервисного трафика предполагает решение задачи шифрования трафика при помощи технологии VPN.

Научно-методологический аппарат для анализа и синтеза сетей VPN общего назначения 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 статье проведен анализ подходов к моделированию сетей VPN.

На сегодняшний день существуют следующие классы моделей исследования сетей VPN, основанные:

- на граф-комбинаторных алгоритмах [4];

- математическом аппарате теории телетрафика [5];

- тензорном анализе [6];

- теории сетевых исчислений NC (Network Calculus) [7].

Наиболее широкое распространение получили модели, основанные на *граф-комбинаторных* алгоритмах.

К моделям, основанным на граф-комбинаторных алгоритмах относятся:

- канальная модель;

- потокосовая модель;

- комбинированная модель.

Канальная модель

Канальная модель VPN использовалась в сетях, построенных по принципу коммутации каналов (ATM и Frame Relay). Исследованием канальной модели посвящены работы Kelly F.P., Mitra D., Ramakrishnan K.G., Morrison J.A. [8]. Описание VPN канальной моделью предполагает знание конечной матрицы трафика, что чаще всего является неизвестным параметром.

Канальная модель VPN аппроксимирует VPN-туннель между двумя точками виртуальным каналом с заданной пропускной способностью (например, между точками А и В создан виртуальный канал с пропускной способностью 10 Мбит/с, а между А и В – 8 Мбит/с).

Данная аппроксимация нерационально расходует ресурсы сети, так как описание туннеля VPN виртуальным каналом с заданной полосой пропускания не позволяет осуществить статистическое мультиплексирование (передачу трафика от разных источников в одном канале).



а)



б)

Рисунок 2 – Внешний вид лицевой панели коммутатора П-215 и маршрутизатора П-320

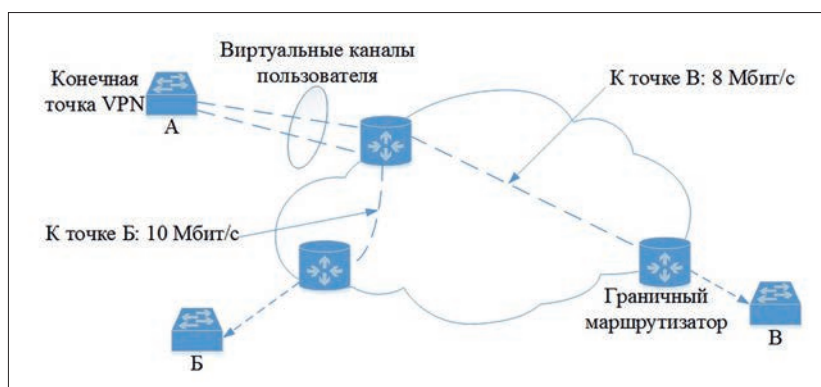


Рисунок 3 – Канальная модель VPN

Исходя из принципа формирования канальной модели следует, что ее применение эффективно в сетях связи, в которых трафик является однородным и предсказуемым (например, соединение двух VoIP сетей VPN-туннелем).

Потоковая модель

Потоковая модель была предложена группой исследователей: Duffield N. G., Goyal P., van der Merwe J. E., Ramakrishnan K. K., Mishra P. И впервые предложена в [9].

Данная модель аппроксимирует совокупность VPN-туннелей потоком с заданной полосой пропускания между граничными маршрутизаторами и конечными точками VPN. Такой подход позволяет описывать сеть VPN суммарным трафиком на входе и на выходе из конечной точки VPN, а не совокупностью каналов с требуемой полосой пропускания (рис. 4).

Основным достоинством данной модели является то, что для описания сети VPN не требуется знание матрицы трафика, так как задается только верхняя граница интенсивности суммарного трафика. Также данная модель позволяет динамически изменять полосу пропускания потока по требованию.

Недостатком данной модели является сложность ее реализации: с увеличением размеров сети растет количество всевозможных видов топологий VPN и вариантов распределения полосы пропускания. Эта задача является задачей NP-сложности, которая приводит к тому, что при помощи математического аппарата теории графов можно найти только распределение полосы пропускания в относительно небольших сетях с неизменной топологией.

Комбинированная модель

Комбинированная модель впервые была предложена в [4] и является модификацией потоковой модели. Данная модель решает задачу определения значения исходящего и входящего трафика для каждой точки виртуальной частной сети по отношению ко всем другим конечным точкам. Что делает возможным установление специфических требований по трафику от одной конечной точки к другой конечной точке или группе точек (рис. 5).

Комбинированная модель обладает следующими достоинствами:

- позволяет установить специфические требования по трафику от одной конечной точки до другой точки, что уменьшает сетевые ресурсы для реализации VPN;

- предоставляет возможность реализовать конфигурацию связи «точка – много точек»;

- для реализации VPN может использоваться частичная матрица трафика, но чем полнее будет информация о трафике, тем эффективней будет использована полоса пропускания сети.

Недостатком комбинированной модели является то, что данная модель накладывает ограничение на использование трафика, циркулирующего в рамках одной сети доступа. Применение данной модели предъявляет высокие требования к вычислительным ресурсам, ввиду хранения больших массивов данных.

Заключение. В настоящее время применение канальной модели для описания сетей VPN целесообразно в сетях с предсказуемым однородным трафиком (например, моносервисная сеть VoIP, что на практике редко реализуемо).

Применение потоковой модели для описания VPN в СЭСН ограничено изменчивостью

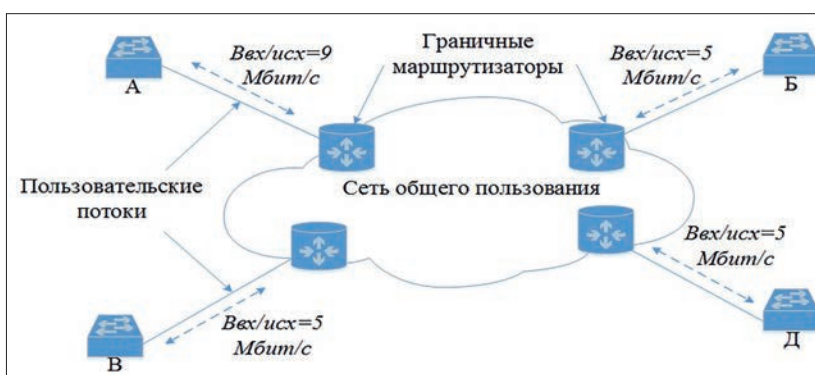


Рисунок 4 – Пример реализации потоковой модели VPN

топологии сети и возрастанием сложности задачи распределения полосы пропускания с увеличением ее размеров.

Комбинированная модель позволяет уменьшить сетевые ресурсы для реализации VPN, а также предоставляет возможность реализовать гибкие конфигурации сетей связи, однако накладывает ограничения на использования трафика, циркулирующего в рамках одной сети доступа.

Следовательно, применение существующих математических моделей сети VPN в СЭСН ограничено. Таким образом, разработка моделей, учитывающих особенности применения VPN в СЭСН, является актуальной задачей исследований в области инфокоммуникаций.

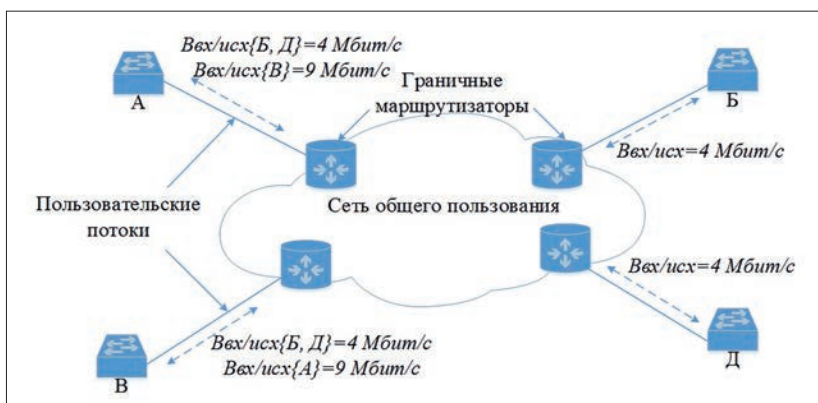


Рисунок 5 – Пример реализации комбинированной модели VPN

ЛИТЕРАТУРА

1. Mitra, D. Virtual Private Networks: Joint Resource Allocation and Routing Design / Mitra D., Morrison J. A., Ramakrishnan K. G. // Proc. of the 18th Annual Joint Conference of the IEEE Computer and Communications Societies. – 1999. – P. 480– 490.
2. Сапрыкин, А. В. Исследование и разработка методов анализа вероятностно-временных характеристик узлов сетей связи специального назначения: автореф. дис. ... канд. тех. наук: 05.12.13 / А. В. Сапрыкин; Поволжский гос. ун-т телекоммуникаций и информатики. – Самара, 2018. – 16 с.
3. Об электросвязи: Закон Респ. Беларусь от 19.05.2005 № 45-3; в ред. от 06.08.2007 № 277-3; с изм. и доп. от 24.05.2021 № 109-3. – Минск, 2021. – 34 с.
4. Росляков, А. В. Разработка моделей и методов анализа виртуальных частных сетей с учетом особенностей их практической реализации: автореф. дис. ... д-ра техн. наук : 05.12.13 / А. В. Росляков; Поволжский гос. ун-т телекоммуникаций и информатики. – Самара, 2008. – 32 с.
5. Гавлиевский, С. Л. Методы анализа мультисервисных сетей связи с несколькими классами обслуживания: автореф. дис. ... д-ра техн. наук.: 05.12.13 / С. Л. Гавлиевский; Поволжский гос. ун-т телекоммуникаций и информатики. – Самара, 2012. – 32 с.
6. Гаипов, К. Э. Применение тензорного метода двойственных сетей для анализа распределенных систем обработки информации [Электронный ресурс] / К. Э. Гаипов, М. К. Заленская // Журн. Современные проблемы науки и образования. – 2013. – № 4. – Режим доступа: <http://www.science-education.ru/110-9766>. – Дата доступа: 15.03.2021.
7. Росляков, А. В. Применение сетевого анализа к оценке характеристик динамических виртуальных частных сетей / А. В. Росляков, А. А. Хаёров // Т-Comm. Телекоммуникации и транспорт, 2012. – № 7. – С.178–179.
8. Mitra, D. Virtual private networks: joint resource allocation and routing design / D. Mitra, J. A. Morrison, K. G. Ramakrishnan // Proc. IEEE INFOCO. – New York, 1999. – № 99 – P. 480–490.
9. Duffield, N. G. A flexible model for resource management in virtual private networks / N. G. Duffield, [et al.] // ACM SIGCOMM Computer Communication Review. – 1999. – V. 29. – № 4. – P. 95 – 108.

The paper is devoted to the analysis of mathematical models of virtual private networks. The feature of modeling virtual private networks in communication networks is indicated special purpose.

Keywords: special telecommunication network, virtual private network, graph-combinatorial algorithms, queuing theory, tensor analysis, theory of network calculus.

Получено 31.08.21.