ОБЕСПЕЧЕНИЕ КАЧЕСТВА ОБСЛУЖИВАНИЯ В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ В СЛУЧАЕ ОТКАЗОВ

Нуштаев А.В.
Поволжская Государственная Академия Телекоммуникаций и Информатики

В настоящее время при упоминании о виртуальных частных сетях обычно имеются в виду VPNs на базе протокола IP. Традиционно вопрос обеспечения качества обслуживания для IP VPN имел второстепенное значение. Однако в последние годы появились такие технологии как RSVP, DiffServ, MPLS, которые делают возможным обеспечение качества обслуживание в VPN-сетях. Существует две популярные модели для обеспечения качества обслуживания QoS в контексте VPN-сетей:

- канальная (pipe) модель
- потоковая (hose) модель.

В канальной модели клиент VPN-сети определяет требования к QoS между каждой парой конечных точек VPN-сети. Иначе, канальная модель требует знать итоговую матрицу трафика, которая представляет собой нагрузку между каждой парой конечных точек VPN. Однако число конечных точек в VPN-сети постоянно увеличивается и соединение между конечными точками становится всё более и более затруднительным. В результате почти невозможно предсказать параметры трафика между парой конечных точек, требующихся для канальной модели. Отсюда недоиспользование сетевых ресурсов, резервируемых для VPN. Задача обеспечения VPN в канальной модели – это задача проектирования маршрутов «точка-точка» между сайтами VPN. Данная проблема достаточно изучена для VPN на основе виртуальных каналов (например, виртуальных каналов ATM или FR или путей коммутации меток MPLS) [1,2]. Суть данного подхода заключается в следующем. Имеется сеть, имеющая несколько узлов, соединенных двунаправленными звеньями с ограниченной симметричной полосой пропускания. На сети организуется несколько виртуальных частных сетей как совокупность маршрутов, соединяющих VPN сайты по принципу каждый с каждым с разделением трафика по нескольким путям. Пользователь, каждой VPN платит за резервированную на этих маршрутах полосу пропускания. Различные маршруты имеют различную стоимость для разных VPN. Задача – распределить доступную полосу пропускания так, чтобы общий доход, приносимый сервис-провайдеру пользователями всех VPN, был максимален. Данная задача есть задача нелинейного программирования. Существует и другой, более рациональный, подход [5], в котором для связности VPN сайтов между собой используется топология дерева. Сеть в данном случае представляется в виде графа с ребрами, имеющими неограниченную емкость (полосу пропускания). Задача обеспечения VPN – построение дерева имеющего минимальную стоимость, т.е. с минимумом зарезервированной полосы пропускания. Данная задача относится к классу задач NP-hard и решается эвристическими методами.

В потоковой модели клиент VPN-сети определяет требования к QoS в конечной точке VPN-сети, а не каждой пары конечных точек. Особенностью, связанной с каждой конечной точкой, является пара участков полосы пропускания – полосы пропускания входа и выхода. Полоса пропускания входа для конечной точки определяет входящий трафик ото всех других конечных точек VPN-сети в данную конечную точку, в то время как полоса пропускания выхода – это количество трафика, который можно передать из данной конечной точки в другие конечные точки VPN-сети. Таким образом, в потоковой модели провайдер предоставляет клиенту VPN-сети обслуживание с определённой гарантией для трафика, который передаётся из каждой конечной точки в другие и принимается из других конечных точек данной VPN-сети. Клиент не может определить, каким образом этот трафик распределён между другими конечными точками. В результате в отличие от канальной модели при использовании потоковой модели не требуется от клиента знать матрицу трафика, что в свою очередь меньше обременяет клиента, который хочет воспользоваться услугой VPN-сети. Обеспечение VPN требует идентификации подграфа соединений точек подключений к VPN и резервирования необходимой полосы пропускания на физических звеньях, используемых подграфом. Различные алгоритмы обеспечения VPN в потоковой модели рассмотрены в [3].

В целом для обеих моделей виртуальных частных сетей можно выделить следующую тенденцию: использование математического аппарата теории графов. Для связности сайтов VPN между собой используется структура дерева, которое может быть построено разнообразными способами [3]. Основная проблема при этом – вычислительная сложность алгоритмов обеспечения VPN.

Предположим, что дерево, обеспечивающее соединения конечных точек подключения к VPN, построено. Две конечные точки этого дерева могут быть соединены только по одному пути, и отказ одного ребра приведет к неработоспособности VPN в целом. Таким образом, другой, не менее важной проблемой обеспечения QoS в VPN является обеспечение защиты пользовательского трафика от потерь возникающих в случае отказа звеньев сети. При этом под отказом звена может пониматься и его перегрузка, в результате которой трафик пользователя не может быть им обслужен.

В контексте защиты трафика виртуальных частных сетей (восстановления VPN) от отказов можно выделить два подхода:

- защита звена;
- защита пути.

Пусть имеется сеть, представленная в виде графа G. На этом графе построено дерево VPN T с сайтами A, B, C и D (рис.1). Пусть (u,v) - отказавшее звено дерева T (показано точками). Тогда для защиты звена (u,v) (рис.2) необходимо определить путь p (пунктирная линия), связывающее вершины u и v и зарезервировать на нем необходимую полосу пропускания. Для защиты пути (рис.3) необходимо определить путь p' (пунктирная линия), который соединит поддеревья $T(u,v)$ и $T(v,u)$ (сохранившие частичную связность) и зарезервировать на нем необходимую полосу пропускания [6].

Восстановление в потоковой модели рассмотрено в [4]. Суть предлагаемого подхода заключается в следующем. Имеется исходное дерево VPN. Защита этого дерева от отказов единственного звена (т.е. в один момент времени может отказать только одно звено) формулируется как построение запасных путей таким образом, чтобы суммарная резервируемая полоса пропускания на низ была минимальной. Это задача есть задача поиска оптимальной аугментации для графа G (которая является задачей класса NP-complete) и решается методами аппроксимации. Под аугментацией понимается множество вершин и ребер графа G, такое чтобы объединение дерева T и аугментации A имеет двухзвенную связность. Защита пути не рассматривается.

Восстановление в канальной модели рассмотрено [5]. В данной работе предлагается строить два дерева – дерево действующих путей и дерево запасных путей, которое обеспечивает защиту от отказа пути. Эта задача аналогична построению направленного дерева Штейнера, связующего источник с точками назначения. Данная задача относится к классу задач NP-hard и решается эвристическими методами. Защита звена не рассматривается.

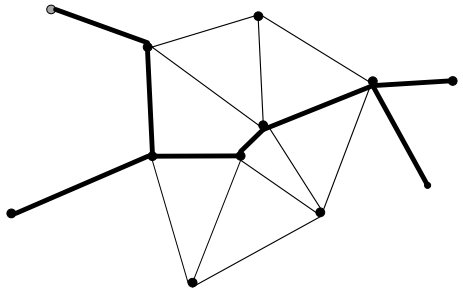

Рис. 1. VPN дерево

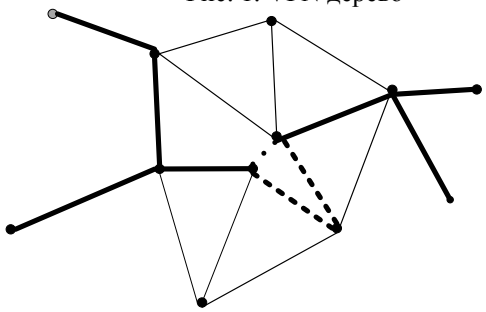

Рис. 2. Восстановление для звена

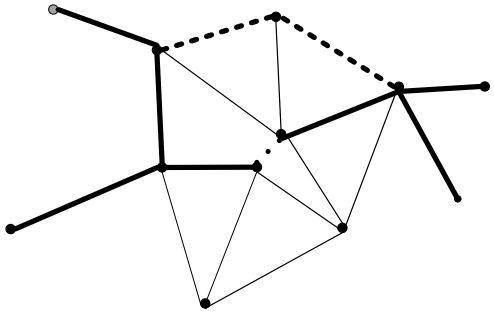

Рис. 3. Восстановление для пути

В целом можно сказать, что проблема восстановления в VPN сетях (как в канальной модели, так и в потоковой модели) не рассмотрена достаточно глубоко и требует более детального изучения.

Литература

1. Mitra D., Morrison J.A., Ramakrishnan K.G. Virtual Private Networks: Joint Resource Allocation and Routing Design // Proc. IEEE INFOCOM 99, 1999.

2. Mitra D., Morrison J.A., Ramakrishnan K.G. VPN DESIGNER: A Tool for Design of Multiservice Virtual Private Networks // Proc. 8th International Telecom. Network Planning Symp, NETWORKS 98, 1998, pp. 153-158.

3. Kumar A., Rastogi R., Silberschatz A., Yener B. Algorithms for provisioning virtual private networks in the hose model // in Proceedings ACM SIGCOMM, 2001.

4. Italiano G., Rastogi R., Yener B. Restoration Algorithms for Virtual Private Networks in the Hose Model // in IEEE INFOCOM, 2002.

5. Hota C., Jha S., Raghurama G., Restoration of VPNs with QoS Guarantees in the Pipe Model, Proceedings of the 6th International Workshop on Distributed Computing (IWDC 2004)

6. Balasubramanian A., Sasaki G. Bandwidth Requirements for Protected VPNs in the Hose Model, International Symposium on Information Theory, 2003.