Comparative Analysis of QoS VPN Provisioning Algorithm on Traditional IP based VPN and MPLS VPN using NS-2

Kusum Grewal
Assistant Professor
ITM University,
Gurgaon, Haryana

Ravinder Dangi
Sr. V&V Engineer
CurveBeam LLC,
Gurgaon, Haryana

ABSTRACT
A virtual private network (VPN) is a private network that uses a public network such as the internet or Multiprotocol Label Switching (MPLS) network to connect remote sites of same or different organizations/networks together. VPN provides similar level of privacy, security, quality of service and manageability that privately owned network provides.

This paper presents the comparative analysis of VPN provisioning algorithm, Modified Tree Routing Algorithm (MTRA), on traditional IP based VPN and MPLS technology based VPNs. MPLS based method of packet forwarding has many advantages over IP layer forwarding. Packets with the same destination arriving on different ports of the router can be assigned to different Forwarding Equivalence Classes (FEC). Conventional forwarding, on the other hand, can only consider information that travels with packet in the packet header. The simulator used to implement the algorithm is, Network Simulator version 2.30 (ns-2). NS-2 gives the packet level analysis of the network with animation.

General Terms
Networking

Keywords
VPN Provisioning, IP VPN, MPLS, MTRA, ns-2

1. INTRODUCTION
VPN has become an important part of corporate networking solutions. VPNs require at least two cooperating devices linked together via a secure tunnel wrapped with a series of functions, including authentication, access control, and data confidentiality and encryption, across an insecure Internet infrastructure.

There are several barriers to widespread deployment of VPNs. One of them is the lack of widely used quality of service (QoS) standards. To improve QoS of VPN, Hose Model was introduced in late 90's [1]. Then various algorithms were proposed and implemented for the provisioning purpose [3]. On line hose model provisioning algorithm MTRA is the latest algorithm proposed and it is the only algorithm that is capable of handling on-line requests on the basis of current network topology and resources available [4] [5]. It achieves minimum rejection ratio. Here we carried out work for implementation of this algorithm on MPLS backbone.

2. IMPLEMENTATION
For implementation, NS-2 Simulator is used in Linux environment.

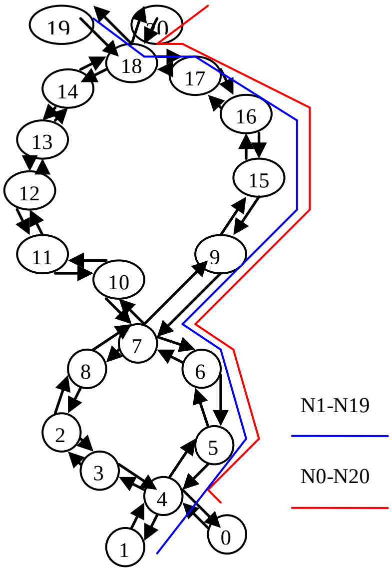
The following steps are taken for simulation of MPLS VPN and MTRA algorithm. Hence the Bandwidth Utilization per link of the VPN is calculated [2] [6]. We further calculated the rejection ratio using the formula:

$$rejection\ \ ratio = \frac{number\ \ of\ \ requests\ \ rejected}{total\ \ number\ of\ \ requests\ \ received}$$

1. Define topology
2. Assign BW, traffic rate, delay, type of routing and routing protocol and link failure protected bandwidth scenario.
3. Write tcl script for the above
4. Link tcl scripts with modified C++ code
5. Execute tcl script in ns-2
6. Get NAM file and trace files generated as a result of execution
7. Execution of trace file, generated above, for taking BW utilization graph for every link and animated analysis of NAM topology generator output.

2.1 Simulation Scenario
The simulation scenario is depicted in the Figure 1.

All the links have a transmission capacity of 5 Mbps. At the beginning of the simulation, no label-switched paths (LSP) are established and three traffic flows are forwarded according to Layer 3 routing protocol. The two flows have a Constant Bit Rate of 400 Kbps and all are forwarded along the same path. Since, at some points of time, the overall bit rate of the two flows exceed the link capacity, packet drops are experienced on the link between router11 and router4. So we decide to establish LSPs on alternative paths to avoid link congestion. Two LSPs are established respectively from router4 and router11 and all the routers between these are now labeled as LSR (Label Switch Router) to map the flow from node 0 to node 20 on the first LSP and the flow from 1 to 19 on the second LSP. Then a failure is forced on link between router 16 and router 17, so the first LSP is released and the first flow restart to be forwarded according to Layer 3 protocol. The simulation was started at 10 sec and ended at 60 sec. The link went down at 11 sec and went up at 40 sec.



Packet flow in MPLS
tunnel

Figure: 1 Topology and packet flow tunnel

2.2 Network Topology

The Figure 2 gives the network topology.

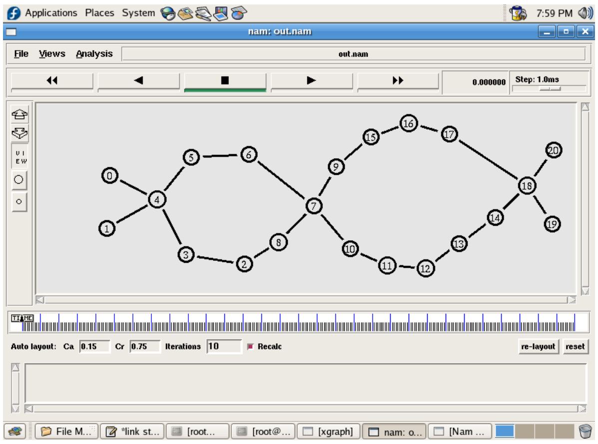


Figure 2: Snapshot view of Network topology in ns2 animator window

2.3 Link State Protocol Execution

The NAM snapshot given below (Figure 3) shows the run of MTRA algorithm for the collection of routing information and maintaining the routing table for VPN path allocations and establishing appropriate MPLS tunnel for data flow.

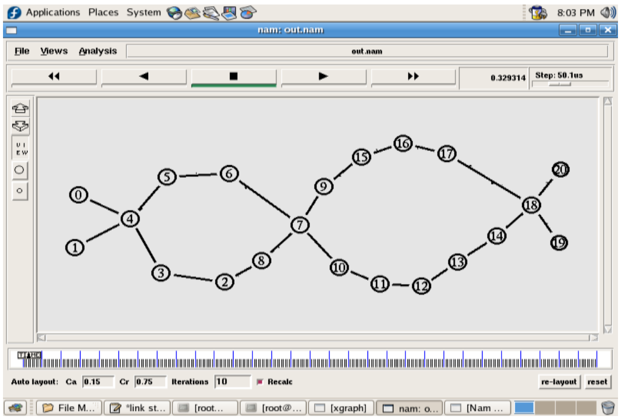


Figure 3: Snapshot view of getting the network information in ns2 animator window (First run of algorithm)

2.4 MPLS Tunnel Formation

The NAM snapshot given below (Figure 4) shows the established MPLS tunnel for data flow and the packets flowing through it at time 27.26 sec. It is showing two VPN requests established successfully between node n0-n20 and n1-n19 following the tunnel LSR4-LSR5-LSR6-LSR7-LSR9-LSR16-LSR17-LSR18. The red line encircles the packets.

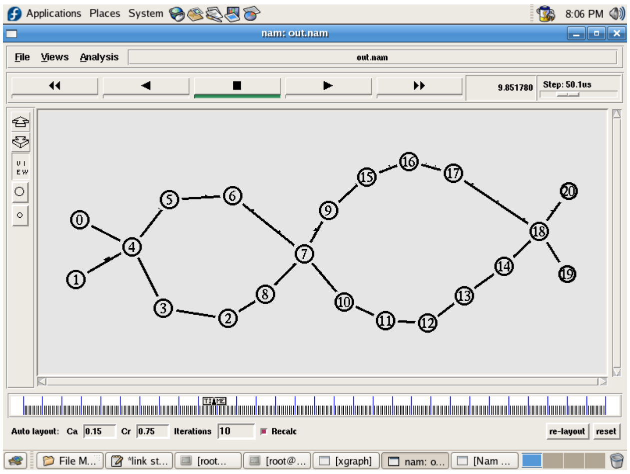


Figure 4: Snapshot view of data flow from node n0 to n19 & n1-n20 through MPLS tunnel in ns2 animator window (in case of MTRA)

2.5 Link Failure

The NAM snapshot given below (Figure 5) shows the link failure in established MPLS tunnel for data flow.

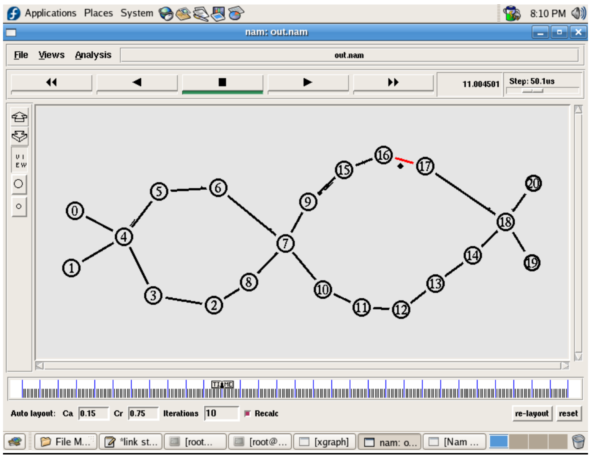


Figure 5: Snapshot view of data link failure through MPLS tunnel in ns2 animator window

2.6 Alternate Tunnel Formation

The NAM snapshot given below (Figure 6) shows the link failure in established MPLS tunnel for data flow[7]. It is showing two VPN requests established successfully between node n0-n20 and n1-n19 following the tunnel other than LSR4-LSR5-LSR6-LSR7-LSR9-LSR16-LSR17-LSR18 that is LSR4-LSR3-LSR2-LSR8-LSR7-LSR10-LSR11-LSR12-LSR13-LSR14-LSR18 (the longer one).

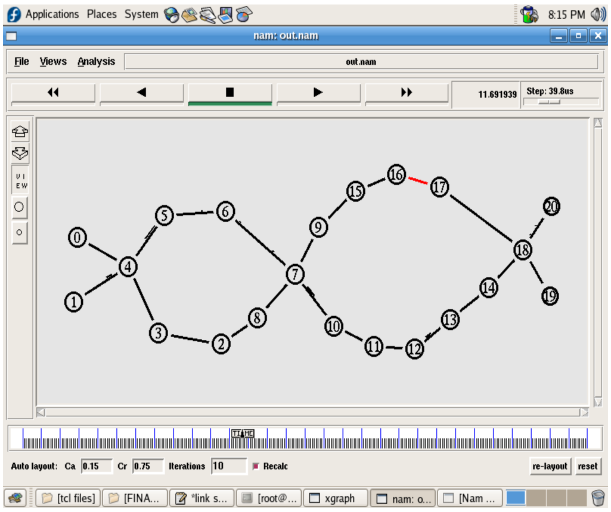


Figure 6: Flow of data through alternate path due to link restoration in case of on-line algorithm

3. RESULTS

For the network topology as mentioned in Figure 2, consists of 21 nodes out of which nodes n0, n1, n19 and n20 are simple IP nodes ,which carries IP traffic and the nodes in between them are label switching routers i.e. LSR nodes which carries MPLS traffic. The capacity of each link is 5Mb, delay of 10ms and drop tail queuing. Traffic source is attached to n0 and n1 and it sinks on n19 and n20 respectively. The traffic rates Tr1, Tr2 and Tr3 are used. The exponential traffic being used has following parameters:

1) Traffic rate 1 (Tr1)
Packet size of 100 bytes, 10 ms burst rate, 3 ms idle rate and 100k rate.

2) Traffic rate 2 (Tr2)
Packet size of 100 bytes, 10 ms burst rate, 3 ms idle rate and 200k rate.

3) Traffic rate 3 (Tr3)
Packet size of 100 bytes, 10 ms burst rate, 3 ms idle rate and 300k rate.

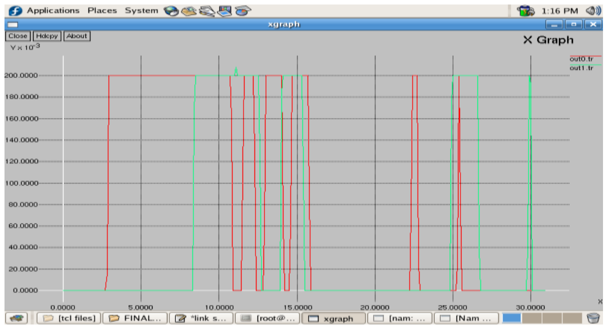


Figure.7 Throughput vs time graph for IP VPN and traffic rate Tr1

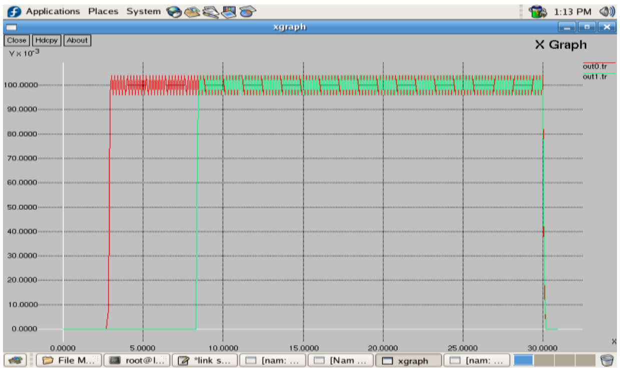


Figure: 8 Throughput vs time graph for MPLS VPN and traffic rate Tr1

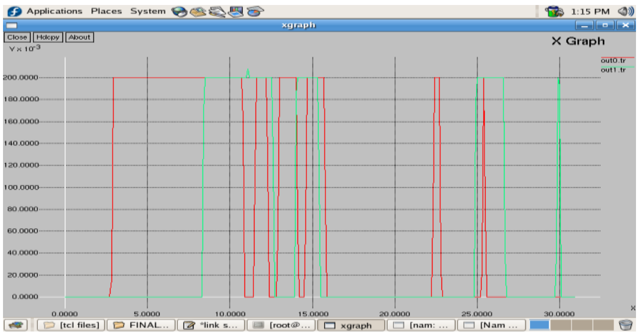


Figure: 9 Throughput vs time graph for IP VPN and traffic rate Tr2

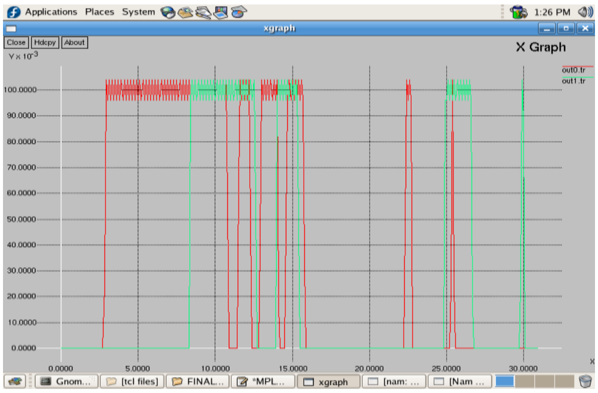


Figure: 10 Throughput vs time graph for MPLS VPN and traffic rate Tr2

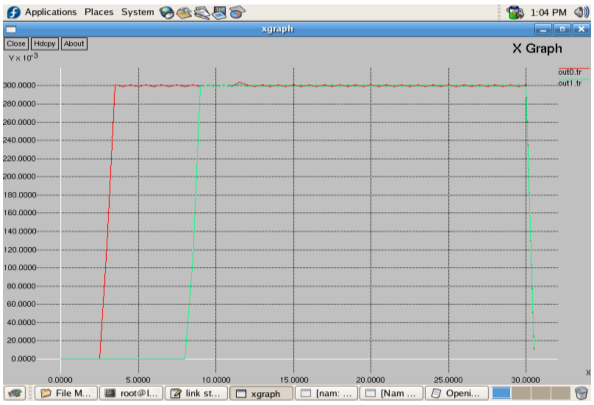


Figure: 11 Throughput vs time graph for IP VPN and traffic rate Tr3

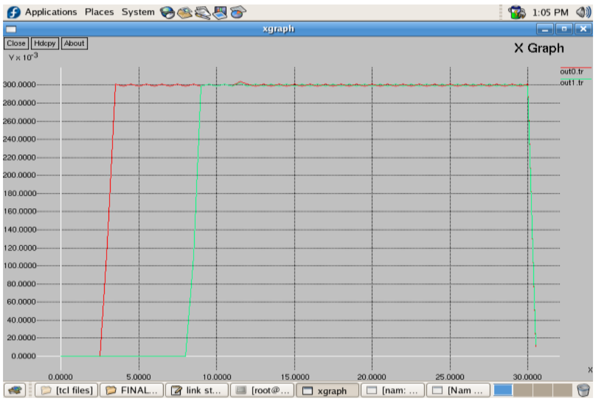


Figure: 12 Throughput vs time graph for MPLS VPN and traffic rate Tr3

Comparison of MPLS VPN with MTRA vs IP VPN with MTRA, Rejection Ratio:

Figure 13 shows the rejection ratio curve for MTRA algorithm. It shows that by using MPLS technology MTRA algorithm give lesser rejection ratio.

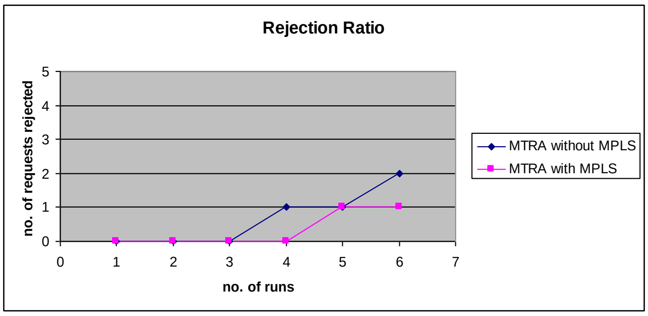


Figure13 Comparison of Rejection Ratio for MTRA algorithm on MPLS and without MPLS (IP) VPN

Various simulations are successfully done to see the effect of different traffic rates on the throughput, rejection ratio of the VPN. It is concluded that the rejection ratio is least in case of MTRA when we use MPLS technology compared to simple Layer 3 IP routing

4. CONCLUSION

After simulating the VPN setup for IP and MPLS backbone, at different traffic rates (Tr1, Tr2, Tr3) as mentioned above, It is concluded that the VPN performs well when we use MPLS technology compared to simple Layer 3 IP routing technique for the heavy traffic conditions. For normal traffic conditions their behavior is similar.

5. REFERENCES

[1] A. Gupta, J. Kleinberg, A. Kumar, R. Rastogi and B. Yener, "Provisioning a Virtual Private Network: A Network Design Problem for Multicommodity Flow", in Proc. of the 33rd Annual ACM Symposium on Theory of Computing (STOC), 2001.

[2] A. J ttner, I. Szab and Á Szentesi, "On Bandwidth Efficiency of the Hose Resource Management Model in Virtual Private Networks", in: Proceedings of IEEE INFOCOM, 2003.

[3] A. Kumar, R. Rastogi, A. Silberschatz and B. Yener, "Algorithms for Provisioning Virtual Private Networks in the Hose Model", IEEE/ACM Transactions on Networking, vol. 10, no. 4, August 2002

[4] N. G. Duffield, P. Goyal and A. Greenberg, "A Flexible Model for Resource Management in Virtual Private Networks", in: *Proc. of ACM SIGCOMM*, 1999.

[5] N. G. Duffield, P. Goyal, A. Greenberg, P. Mishra, K. K. Ramakrishnan and J. E. V. D. Merwe, "Resource Management with Hoses: Point-to-Cloud Services for Virtual Private Networks", IEEE/ACM Transactions on Networking, vol. 10, no. 5, pp. 565-578, October 2002.

[6] E. Horowitz, S. Sahni and S. Anderson-Freed, "Fundamentals of Data Structure in C", Computer Science Press, 1993.

[7] G. Italiano, R. Rastogi and B. Yener, "Restoration Algorithms for Virtual Private Networks in the Hose Model", in Proc. of IEEE INFOCOM, 2002.