JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY

www.IJTPC.org/Publications

Optimization of the tunnel VPN

Sanaa DIFAA, Mohamed Azouazi, Abdelaziz Marzak

Faculte des Sciences de Casa, Université Hasan II_Mohammedia, Maroc.

ABSTRACT

The data transmitted over the Internet is much more vulnerable than when running on an internal network in an organization. A good compromise is to use the Internet as a transmission medium using a protocol that transmits encrypted data. This is known as virtual private network (VPN Virtual Private Network). The VPN system therefore provides a secure connection at a lower cost, and based on an encapsulation protocol (tunneling) IPSec (Internet Protocol Security) uses cryptographic protection services, security protocols, and dynamic key management, these foundations ensure both power and flexibility for secure communications among computers of this network. In this paper we study the problem of robust optimization design of VPNs to solve the problem of bandwidth saturation. We formulate mathematical models of the problem and propose efficient heuristics based on local search techniques for solving

Keywords

Ant colonies, Optimization VPN IPSec, MPLS.

1. INTRODUCTION

A virtual private network (VPN, Virtual Private Network) is a solution that allows you to extend a private network operator by exploiting safely a public network:

- Confidentiality by encrypting communications
- The authenticity through mutual authentication of the correspondents and integrity control of data

So a VPN allows you to:

• Connect multiple entities;
• Secure connections from an ISP;
• Integrate private network of roaming users

Telecommunications operators offering the past few years, VPN (Virtual Private Network) services. Companies subscribing to these deals can have a private virtual infrastructure and long-distance communication.
The VPN client can connect various geographically distributed sites without having to invest in leased lines and without having to bear the costs related to the management and maintenance of such architecture.

The VPN architecture is described below in FIG. For now subscribing offer VPN, VPN nodes appear to be interconnected in a mesh topology completely through virtual links. In fact, the VPN nodes are directly connected to the operator network IP routers, and links correspond to the virtual paths between the routers in the IP network. [5]

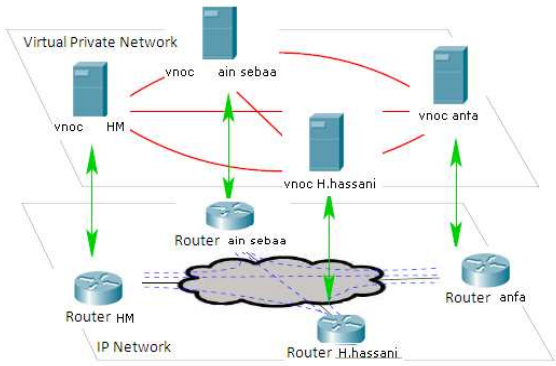

Figure 1: Diagram of a VPN

There are two technologies widely deployed by operators for the implementation of VPN services: MPLS VPN Technology [Multi Protocol Label Switching] and that based on the IP protocol (IPSec [Internet Protocol Security]).

In terms of network design, there is a significant difference between MPLS VPN and IP VPN.

Whereas with a VPN IP VPN virtual links can be routed to multiple paths based on routing metrics of the underlying network, each virtual link an MPLS VPN is routed on a single path using an LSP (Label Switched Path) in explicit routing. The VPN service provider can better control the placement of virtual links in the network using RSVP [Resource Reservation Protocol].

From the point of view of the client company, VPN should appear as a private network, offering the same quality of service that network of leased lines, but at a much lower price. [4]

For this, it is essential that the operator provides the bandwidth allocated to the virtual links of the VPN.

This implies first of all to specify the bandwidth required among the different nodes of VPN, Then to reserve the network operator along the paths corresponding to the virtual links using the RSVP protocol.

The evolution of the Internet, described in the previous sections, leading to a proliferation of services offered by the networks and a growing number of users and volume of traffic they generate.

In a society where information and communication have become so important, interruption of services offered by the network, or even a significant degradation of QoS are less acceptable. This raises the operators or ISPs new issues. [12] [13]

Initially, to cope with these problems, the operators or ISPs turned to the over sizing of equipment. The main sources of QoS degradation being congested areas of the network, reduce the risk of congestion by a significant increase of resources allows'' elapse traffic volumes while ensuring QoS requirements.

However, this approach is no longer economically viable. Competitive environment which induces low profit margins is no longer possible to improve the performance of IP networks by excessive over sizing equipment. From a technical point of view, this must be changed if we really want to control the evolution of the network.

Performance guarantees cannot be achieved without a new approach to network planning .Techniques of network planning, which adapt the network to the volumes of traffic and QoS requirements that it must endure.

They also incorporate the concepts of resilience not only to ensure proper use of resources in the home network, but also performance "acceptable" if the network is in a state of failure. Planning one's network also returns to anticipate the evolution of the overall traffic, for example the development of services in the network and the number of clients per service.

2. Network design

The problem of network design, known in the literature as the "Network Design" usually arises for operators wishing to set up a new communication infrastructure or replacing existing ones in order to meet new user requirements (communications intranet, extranet, internet ...). [10]

This problem consists, given a set of predefined locations for the installation of equipment'' and features (most often estimated) flows between sites, of selecting a subset of sites to find and activate a plan to connect at a lower cost. This case consists of the installation fees of equipment and connection sites. In general, the resulting network must meet certain standards of reliability and performance (Figure 2).

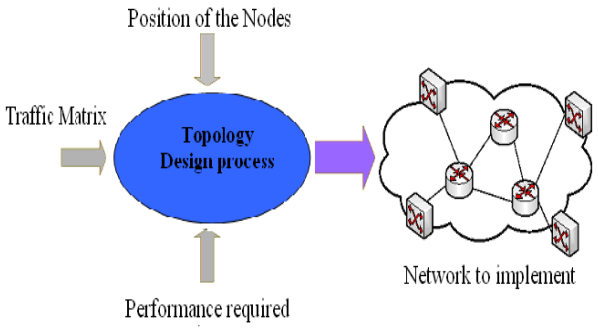

Figure 2: Process network design

A variant of the design problems for the network topology of the extension of a network. We assume that the network is recognized, but seeks to change its topology. For example, you can add new nodes to serve new points of presence. We may also want to remove some links and add others to meet the changing demand.

3. Planning Routing

As we have previously stated, the term routing refers to all mechanisms implemented in a network to determine routes that will route packets from a transmitting terminal to a receiving terminal.

Routing algorithms are useful of course for routing data but also for the allocation of resources along the paths.

The introduction of the service quality from start to end makes these routing problems complex.

The simplest approach for routing a flow between a given source and a destination is to choose the shortest path. This is the idea underlying routing best-effort IP networks that uses distributed algorithms for shortest path.

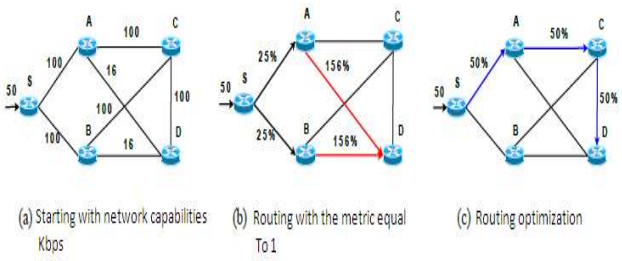

Figure 3: Examples of instances of routing optimization problem

This figure illustrates the importance of changes in the IP routing. Figure 1.7 (a) illustrates the topology of departure where all metrics are unitary. Capacity values interfaces are given in Figure Kbps and a single traffic demand 50 Kbps is issued between S and D.

Therefore, a first routing gives us two routes from S to D (see Figure 1.7 (b)).

Equitable sharing of distributed stream so 25 Kbps on each route. But these routes borrow the A / D and B / D interfaces that therefore cannot support all traffic (their capacity is 16 Kbps). Their use therefore worth 156%.

The operator is required to optimize the routing metrics by changing some links (or interfaces). If the operator keeps, for example, metrics interfaces S / A and A / C at 1 and increases the metric of the other interfaces, it obtains the routing scheme described in Figure 1.7 (c). Thus, the maximum use of interfaces decreases from 156% to 50%.

The aim is to deliver high quality customer service while maintaining the equipment costs and the lowest possible operation. The return on investment is obviously a key factor for business success.

Optimization problems that arise in the design or operation of networks are grouped in this document in the name of network optimization problems. [9]

4. Minimization of the total bandwidth reserved

The routing optimization problem is to establish a routing scheme flow to avoid equipment congestion to better distribute flows in the network. And to achieve this optimization, we will use the ant algorithm (ACS), inspired by foraging ants and aims to solve the problem of saturation of the bandwidth of VPN is to find a path minimum length that must borrow a VPN tunnel to establish connections with the various agencies and to exchange data reliably.

The contribution of this adaptation lies primarily in:

- Its simplicity.
- Its ease of implantation.
- Its effectiveness in planning to establish tunnels.

In order to solve this problem by the method of ant colonies, the problem must be represented as a graph whose vertices represent agents and arcs are tunnels between these agencies and the VPN server. [7] [8]

The evaluation of each arc is a function of time of connection to the receiving agency (Figure 4)

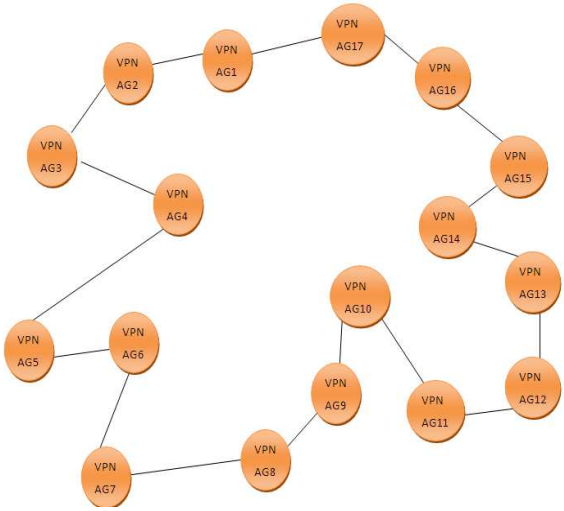

Figure 4: Graph 17 agencies representing the problem of the tunnel established by each agency once.

5. Resolution algorithm ants

We associate with each arc (i, j) of the graph two values τij Nij defined in the case of our problem as follows;

τij is the trace pheromones left by ants on arc (i, j).

ŋij the attractiveness of the arc (i, j) is equal in our case, unlike the connection time to the agency j.

This time consists of travel time, in minutes, an agency i to another j and service time in minutes in each service area, weighed by the number of spaces in each agency.

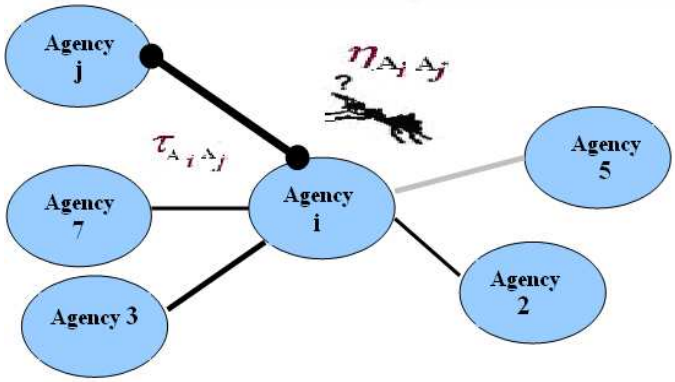

Figure 5: the evolution of arcs by two digital values

We can summarize the general operation of the ARS to solve our optimization problem of tunnels by the following algorithm:

For each segment, set τij to τ0

Randomly allocate an ant to each agency

For t=1 to tmax

For k from 1 to m

For each non-visited agency

Select a destination agency, within the remaining streets Jik, according to the formula:

$$j=\begin{cases}\operatorname{argmax}_{u\in J^k_i}\left\{[\tau_{iu}(t)][\eta_{iu}]^\beta\right\} & \text{if } q\le q_0\\ J & \text{else}\end{cases}$$

Where j is chosen according to the probability

$$P_{ij}^{k}(t)=\frac{(\tau_{ij}(t))^{\alpha}(\eta_{ij})^{\beta}}{\sum_{l\in J^k_i}(\tau_{il}(t))^{\alpha}(\eta_{il})^{\beta}}$$

$$\tau_{ij}(t)\leftarrow(1-\rho)\tau_{ij}(t)+\rho\tau_0$$

End for

Calculate the length Lk for each trip cycle of the ant k

If ant k totals the shortest length then store it in T+

For each segment (i,j) ∈ T+, calculate

$$\tau_{ij}(t)\leftarrow(1-\rho)\tau_{ij}(t)+\rho/L^{+}$$

End-For

Return T+ and its length L+

End-For

Co: parameters used

ρ = 0, tmax = 10, β = 2

6. Illustration with an example

After studying the different optimization algorithms were selected the most suitable and profitable to our situation, this is why we have implemented our

Solution using the programming language C + + object-oriented in order to compare the results of the solution present and those of our solution. [1] [2]

The graph below summarizes a real itinerary prepared by our VPN tunnel before implementing our solution cases:

- Current Situation

The graph below summarizes a real case of a delivery itinerary used by our Tunnel VPN

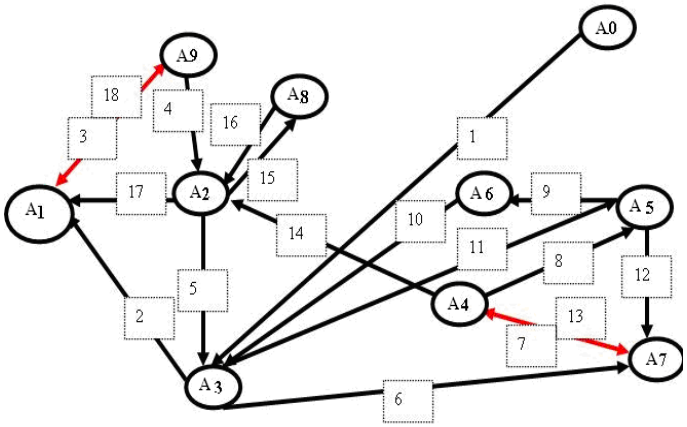

Figure ٦: Existing Delivery Itinerary

A0, A1… A9 designate the agency; and the values 1 to 18 designate the order of the tunnel between those agencies. The itinerary is:

A0->1 A3->2 A1->3 A9->4 A2->5 A3->6 A7->7 A4->8 A5->9 A6->10 A3->11 A5->12 A7->13 A4->14 A2->17 A1->18 A9

We notice that the VPN goes connected a agency more than once (example: A2 is connected three times). This redundancy generates an additional cost, a waste of time and saturation of the total bandwidth reserved.

- Solution suggested by our algorithm

We took the previous case and apply to it our algorithm to develop an optimized solution that we represent in fig 6. As parameters, we took m = 10, α=1.0, β = 2.0, ρ=0.5 and tmax=10 A;

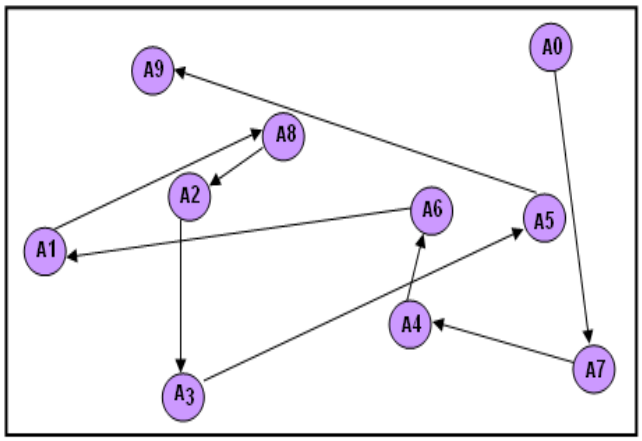

Figure 6: Itinerary suggested by our algorithm

Our solution suggests the following itinerary: A0-> A7-> A4-> A6-> A1-> A8-> A2->A3-> A5-> A9.

The current solution respects the criteria previously outlined and most notably gives a better itinerary. In fact,

1. the total time is reduced by 40%
2. the total bandwidth reserved is minimized by 35%

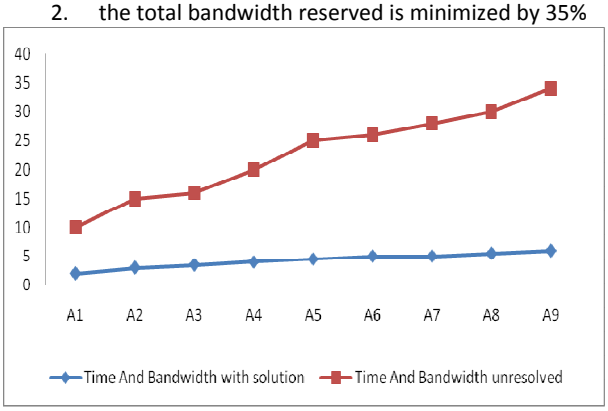

Figure ٧: the evolution of flow per unit time with and without solution

7. Conclusion

This study has shown how to carry meta-heuristic ant colony optimization to the problem of planning VPN tunnels. The final solution allowed to significantly improving realized tunnels between the agencies and the VPN server. This would

Result in cost savings and also minimizing the considerable bandwidth for the company and allows improving the efficiency of its operations. It should be mentioned that preset constraints are reliable over time. However, in practice, it is possible that one or more contingencies disrupt the routing previously established.

In other words, part of the problem depends explicitly on time; it affects real-time applications to the new server VPN depending on their availability and its queue. It is for this that connection becomes dynamic.

Research dynamic connection problems have been growing interestingly in the last few years, the evolution of various information technologies and communications, can now effectively address dynamic problems

8. REFERENCES

[1] P. Blaise : Tournées de véhicules d'une société coopérative: algorithmes séquentiels et parallèles : http://www.prism.uvsq.fr/rapports/1996/document_1996_6.ps.

[2] M.Dorigo, L.Maria Gambardella. Ant colony system : A cooperative Learning. Approch to the travelling Salesman Problem. IEEE Transactions on Evolutionary Computation, Vol.1, No.1, 1997

[3] J.K. Lenstra and A.H.G Rinnoy Kan : Complexity of vehicle routing and scheduling problems. Networks, 11 : 221-227, 19٩٩

[4] G.Laporte , M. Potvin, J.Y et F. Semet , Classical and modern heuristics for the vehicle routing problem, International Transactions in Operational Research, 2000

[5] B. Gleeson. Uses of IPsec with Provider Provisioned VPNs. PPVPN Working Group, August 2001. draft-gleeson-ipsec-ppvpn-00.txt, work in progress.

[6] Cisco Secure VPN Client Solutions Guide, 2002. Cisco Systems Inc., Number: OL-0259-02.

[7] G. Laporte,G. et I.H. Osman, Routing problems : A Bibliography, Annals of Operations Research, ٢٠٠٢

[8] Check Point Software Technologies Ltd. IPSec Versus Clientless VPNs for Remote Access, September 2002. white paper, http://www.checkpoint.com.

[9] V Cerf et R Kahn. A Protocol for Packet Network Intercommunication. IEEE Transactions on Communications, 22(5):637– 648, Jan ٢٠٠٣.

[10] P. Knight, H. Ould-Brahim, and B. Gleeson. Network based IP VPN Architecture using Virtual Routers. L3VPN Working Group, April 2004. draft-gleeson-ipsec-ppvpn-00.txt,work in progress.

[11] G. Laporte, Y. Nobert : An exact algorithms for the vehicle routing problem. Networks, 14, n°1, pp. 161-172, ٢٠٠٤

[12] Alexandre Alapetite ssh-tunnel-http 01 July 2012

[13] Thomas Firewall - VPN - SSL VPN, StoneSoft 13 December 2012