On Improving Communication System Performance in Some Virtual Private Networks

Tomasz Malinowski(✉) and Jan Chudzikiewicz(✉)

Faculty of Cybernetics, Military University of Technology,
ul. Gen. Witolda Urbanowicza 2, 00-908 Warszawa, Poland
{tomasz.malinowski,jan.chudzikiewicz}@wat.edu.pl
http://www.wat.edu.pl/

Abstract. The paper presents the procedure for determining the optimal set of hubs and spokes and thus the collection of tunnels in hub-and-spoke network. The subject of the study was a multi-departmental network, with security of transmission requirement, so DMVPN technology with IPSec-protected tunnels were used. The optimization of the hub/spoke set was intended to improve inter-departmental communication efficiency, which was to be confirmed by the analysis of simulation results. In the simulation studies, the quality of the chosen service (VoIP) was checked for the different structures of tunnel connections. Simulation tests were prepared and implemented in Riverbed Modeler environment.

Keywords: Optimal communication structure · Routing protocols
Dynamic tunneling in VPN

1 Introduction

This article is a continuation of the considerations on improving the reliability and performance of transmission in the networks based on hub-and-spoke logical architecture. The procedure for monitoring and maintaining a network of dynamic VPN tunnels was introduced in [1]. The idea of reconfiguration was intended to use a diagnostic theory to test the interoperability of branch boundary routers, which act as a tunnel brokers for other routers, to communicate branches networks using dynamic IPSec tunnels. The basis for this discussion was Cisco DMVPN technology.

The authors of this article focus on the method of centralized monitoring of communication parameters in DMVPN network with scattered departments and on calculation of the optimal set of hubs and spokes. Network structures in which inter-departmental communication takes place through hub routers and is secured by IPSec are considered. The task is to determine optimal set of border routers (single router can act as hub or spoke) and thus a minimal set of VPN tunnels.

P. Gaj et al. (Eds.): CN 2018, CCIS 860, pp. 64–73, 2018.
https://doi.org/10.1007/978-3-319-92459-5_6

This task belongs to the wide domain of determining the optimal allocation of resources and determining the optimal communication structure and is raised in many research works focused on improving reliability, performance, and usability of transmission systems (multiprocessor systems, military computer networks - wired and wireless networks of stationary or mobile nodes). A lot of research focuses on the problems of optimization of the hypercube structure and on the problems with location and relocation of network resources ([2–8]). In the era of IoT (Internet of Things), results of research on optimal and "energy-efficient" communication structures, prolonging the life time of the network with battery-powered nodes, are particularly important [9]. The research is focused on developing new routing protocols, efficient medium access protocols, selecting of nodes collecting and processing information from other nodes (sink nodes) and on indicating nodes of the meeting points (rendezvous points) or nodes acting as coordinators ([9–12]).

In our area of interest, i.e. dynamic tunneling in VPNs, research is focused on testing of the network performance in cases of utilization of various routing protocols [13].

In this paper we introduce a procedure for determining the optimal set of hubs and spokes in specific communication structure. We assume arbitrarily that the dynamic routing protocol, used for broadcasting of prefixes of branch network addresses, is OSPF (Open Shortest Path First). The result of the procedure is the graph of logical VPN connections between departmental border routers. Based on the graph we will be able to distinguish spoke and hub/spoke routers. We assumed that such structure of VPN tunnels will enable efficient and secure exchange of information between branches. We were looking for confirmation of assumptions in the results of the simulation studies.

This paper firstly presents short description and basic DMVPN problems. In Sect. 3, the structure of the analyzed network, the assumptions and formal description of the problem are given. Section 3 also deals with the procedure for determining the best tunneling structure between the border routers of our network. The last section shows the model of simulated network and results of simulation tests.

2 DMVPN Characteristics and Main Transmission Issues

DMVPN (Dynamic multipoint VPN) is a great technology to create scalable VPN. It is based on Multipoint Generic Routing Encapsulation protocol (mGRE), IPSec and Next Hop Resolution Protocol (NHRP). It makes possible build a communication structure connecting branches of the company through secure tunnels over WAN. Some of the tunnels are permanent, some of them are dynamically built-up, as needed, so using DMVPN makes it unnecessary to create and to manage large numbers of tunnel connections in big multi-site networks.

DMVPN consists border routers that function as hubs or spokes. In basic DMVPN form, inter-branch communication via hub nodes is offered (DMVPN

Phase-1) and is called spoke-hub-spoke communication. Another variant is the communication between boundary branch routers through dynamic tunnels, which are established after reconciling of tunnel parameters with the tunnel broker. Spoke is the reconciliation node, and hub is tunnel broker (DMVPN Phase-2, where branches are directly connected). In both cases it is possible to protect the tunnels by IPSec. Implementation of direct communication between branches with secured tunnels is DMVPN Phase-3 (spoke-to-spoke connections with IPSec).

The general shape of DMVPN was shown in Fig. 1.

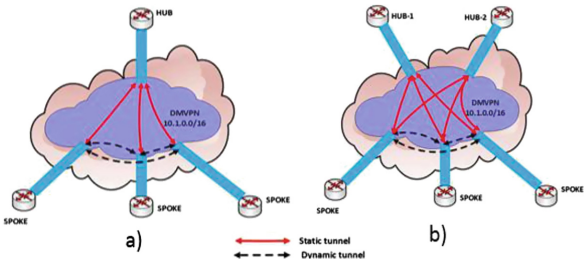

Fig. 1. DMVP with one HUB (a) and backup NHS server (b)

For reliability DMVPN can contain primary and backup hub (structure b on Fig. 1). Regardless of DMVPN structure, each spoke has to register itself in the primary hub or additionally in backup hub, which are called Next Hop Servers (NHS).

DMVPN technology has many advantages, but in various studies the shortcomings and problems that occur in networks with this solution are signaled. For example, for spoke-to-spoke communication (DMVPN Phase-3) a hub failure can directly impact spoke-to-spoke connectivity in those DMVPN networks where spokes can't establish direct IPSec sessions (due to NAT or other limitations).

Another example might be the problem discussed in the article [1]. The authors point out the fact, that the primary condition of successful tunneling is proper functioning of the spoke in hub registration mechanism, the polling mechanism about physical addresses of the final points of tunnels, but also mechanism of call's disconnecting in case of hub failure (connection with hub can be temporary loss, hub can be overloaded, hub's response time can be too long, etc.). In some cases of tunnel connections protected by IPSec, it is necessary to track hub's availability and to remove IPSec session after a period of temporary hub's unavailability (cleaning of IPSec Security Associations) [1].

Despite the fact that DMVPN technology is developed and improved over the years, it is still possible to indicate the situations in which network management procedures in situations of malfunction are useful.

3 Determining of Optimal VPN Communication Structure

Our considerations will be focused on the VPN and the network structure graph G_1, shown in the Fig. 2.

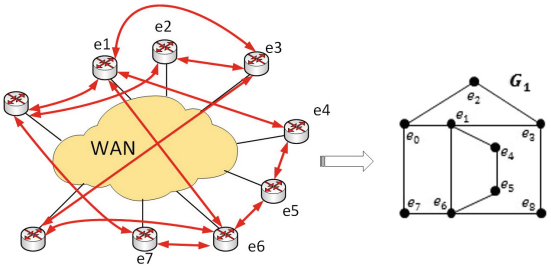

Fig. 2. Structure of potential VPN connections in a specific network

We assume that the analyzed structure of tunnel connections results from some technical limitations of border routers, which means that not every router can act as a hub. All routers, however, can be a spoke. Thus, the initial structure is not the structure of full-mesh tunnel connections but partial-mesh. Such a structure will be a subject of optimization, because we want to minimize the number of the tunnel connections.

The procedure for determining the optimal structure will be implemented centrally by the network management station. The assignation of such structure will involve uploading of the appropriate configuration to the border routers of DMVPN branches.

The network structure is described by graph $G = <E, U>$, for E – set of network nodes, and U – set of communication links (corresponding to DMVPN tunnels).

In the example network, nodes e_0 to e_8 are departmental border routers. Red lines (in Fig. 2) between nodes are potential IPSec tunnels. Graph G_1 shows VPN connections in a simpler form.

VPN topology in Fig. 2 are redundant connections structure, but not full-meshed. Graph G_1 is a subgraph of four-dimensional hypercube It is a redundant structure with high degree of redundancy, fulfilling the stringent requirements imposed on some networks. The issue of determining such subgraphs was discussed in [7].

Our first goal was to implement a procedure of acquiring by management station information about the quality of the transmission channels between nodes $e_0 - e_8$. Because Cisco routers are the border routers of our network, we use IP SLA probes. IP SLA is a great tool and is an embedded agent in Cisco IOS, designed to measure and monitor common network performance metrics like

jitter, delay, and packet loss. IP SLA has two components: the source and the target. The source generates packets, and the target functions as responder.

Simple IP SLA probe may look as follows:

ip sla 1
udp-jitter 10.0.0.1 codec g729a
frequency 40
ip sla schedule 5 life forever start-time now

On the recipient's side, we just turn on the responder using the command: *ip sla responder*

Statistics given by the probe is listed below (some lines are omitted).

WA#show ip sla statistics

Latest RTT: *192 milliseconds*
Source to Destination Latency *Min/Avg/Max: 2/75/244 milliseconds*
Destination to Source Latency *Min/Avg/Max: 2/214/423 milliseconds*
Source *to Destination Jitter Min/Avg/Max: 0/13/209 milliseconds*
Destination *to Source Jitter Min/Avg/Max: 0/23/314 milliseconds*
Packet Loss Values:
Loss Source to Destination: 0
Loss Destination to Source: 0
Out Of Sequence: 0 Tail Drop: 19
Packet Late Arrival: 0 Packet Skipped: 1
Voice Score Values:
Calculated Planning Impairment Factor (ICPIF): 14
MOS score: 4.00

We assume that the probes will be running on border routers, that can set up tunnels as in Fig. 2. The probes will assess the "quality of the tunnel connection". This parameter will be the key to determining the best communication structure of our network.

Because it is communication structure with permanent tunnels (DMVPN Phase-1), our intent is to choose "optimal minimum set" of hubs and spokes (in our case, providing the best VoIP service performance).

In general, let $d\,(e, e'\,|G\,)$ be the distance between nodes e and e' in a coherent graph G. This is the length of the shortest chain (in the graph G) connecting node e with the node e'.

Nodes of the structure G are characterized by a radius. Let $r\,(e\,|G\,) = \overset{max}{_{e' \in E(G)}}$ $d\,((e, e')\,|G\,)$ be the radius of a node. In the Table 1 radius for all nodes of G_1 were presented.

A basis for determining the communication structure is a dendrite, which provides the minimum number of communication lines.

Let $T = <E, U^*>$ be the dendrite i.e. such coherent acyclic partial graph of G that:

$$\exists\,\langle e',\ e''\rangle \in U \Rightarrow \langle e',\ e''\rangle \in U^* \Leftrightarrow [(d\,(e^*,\ e') \neq d\,(e^*,\ e'')) \wedge d\,(e',\ e'') = 1]$$

Table 1. The radius values for G_1

$e \in E(G_1)$	$r(e\,\vert G_1)$
e_0	3
e_1	2
e_2	4
e_3	3
e_4	3
e_5	4
e_6	3
e_7	4
e_8	4

for

$$r(e^*) = \underset{e \in E(G)}{max}\, r(e)$$

The algorithm for dendrite T determining was presented in [7]. The procedure described there gives, in the first step, a set of dendrites, illustrated in the Fig. 5.

For simplicity of calculation, it was assumed that distance between e and e', which are connected via VPN tunnel, is 1, but you can use all or some of the characteristics returned by the IP SLA probes and assign a metric according to your preferences. In a real network environment, we assume continuous (periodic) checking of various SLA parameters, and using them as a metric of inter-nodes tunnels.

The optimal structure is a dendrite determined for a node with minimal radius. For the structure G_1 the node e_1 (Table 1) has a minimal radius. The structure T_{OPT}, shown in Fig. 3, was chosen as the optimal communication structure for the G_1. Thus, the nodes e_2, e_5, e_6, e_7, e_8 are spokes, and the nodes e_0, e_1, e_3, e_4 are hubs.

After determining the optimal communication structure, the management station can perform appropriate reconfiguration of the boundary routers.

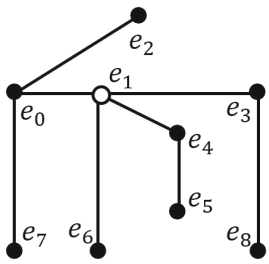

Fig. 3. The optimal communication structure T_{OPT} for the G_1

4 The Results of Simulation Studies

The procedure for determining the set of hubs, spokes and tunnels was verified by simulation tests. The study was conducted in the Riverbed Modeler simulation environment. The simulation model of our network is shown in the Fig. 4.

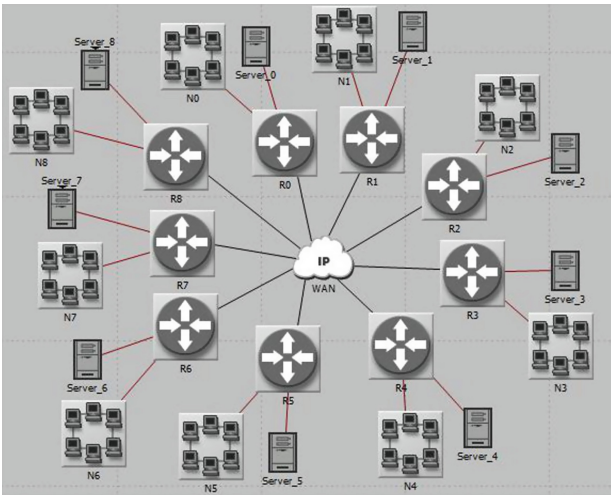

Fig. 4. Simulation model of DMVPN

There were nine branches attached to the WAN by border routers R0 – R8. The single branch was modeled as a LAN with 10 workstations and one http server. Branch workstations can communicate through WAN over VoIP and http (treated as background traffic). The observed service, as especially important for us, was VoIP.

The conducted simulation tests certainly do not serve to verify the design of any network. The tests were to authenticate the procedure for determining the optimal VPN communication structure. Therefore, we only took care of the homogeneity of links and network devices. What was important for us is that in the randomness of generating network streams and the randomness of client-server connections, the simulation results confirm the correctness of the theoretical arguments.

We were interested in the value of important VoIP service parameters like end-to-end delay and delay variation Network services have used the standard application models, available at Riverbed Modeler ("Heavy Browsing" http model and "PCM Quality Speech" voice model). Routers were connected to WAN over T1 links.

Simulation scenarios corresponded to the structures from Fig. 5. It was expected that the results of the simulations will confirm the choice of optimal hubs, spokes and tunnels collections (Fig. 2). Some interesting results Voice

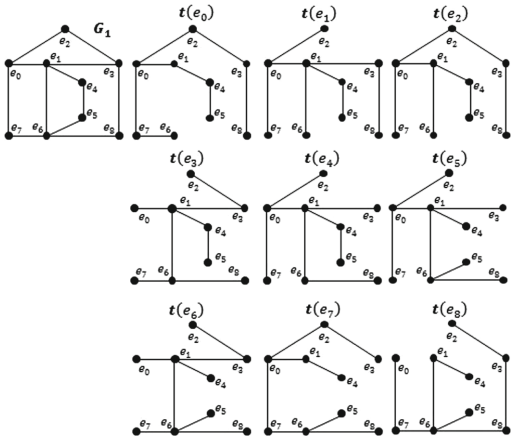

Fig. 5. Set of G_1's dendrites

End-to-End Delay and Voice Delay Variation, confirming the correctness of the procedure for determining the optimal VPN structure are shown in the figures below. *End-to-End Delay* is "average delay in seconds for all network nodes communicating each other under VoIP" and Voice Delay Variation is "average variance in seconds (for all voice workstations) among end to end delays for voice packets. It is measured from the time packet is created to the time it is received" [14]. Low values of these parameters are desirable.

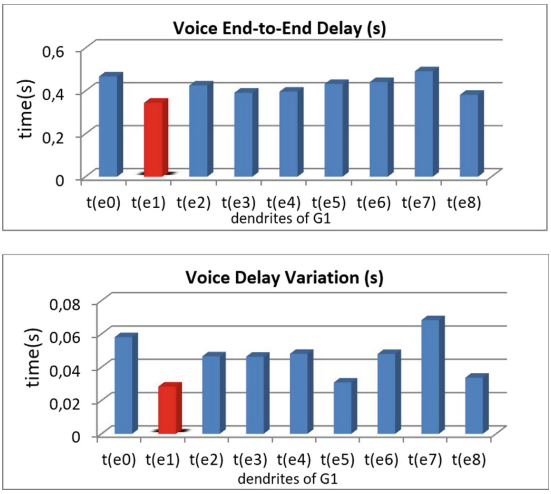

Fig. 6. Average values of *Voice End-to-End Delay* and *Delay Variation*

Complete set of results, in the form of a bar chart, for all G_1's dendrites are presented in Fig. 6. The highlighted bar refers to the best structure $t(e_1)$ (T_{OPT} from Fig. 3).

5 Conclusions and Future Work

Correctness of developed method and its usefulness was confirmed by simulation results. We are satisfied with the simulation results, as considered structures were rather simple and very similar to each other and we did not expect such unequivocal results, which would confirm the correctness of the analytical procedure for determining the optimal VPN structure.

Our next step is the practical implementation of the VPN connection management system. Despite the confirmation of usefulness of our procedure in a simulation environment, it will be interesting to implement and test the effects of continuous monitoring of VPN transmission channels and changing the configuration of routers in a real network environment.

References

1. Malinowski, T., Arciuch, A.: The procedure for monitoring and maintaining a network of distributed resources. In: Annals of Computer Science and Information Systems, Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, vol. 2, 7–10 September 2014, Warsaw, Poland (2014)
2. AlBdaiwia, B.F., Bose, B.: On resource placements in 3D tori. J. Parallel Distrib. Comput. **63**, 838–845 (2003)
3. AlBdaiwia, B.F., Bose, B.: Quasi-perfect resource placements for two-dimensional toroidal networks. J. Parallel Distrib. Comput. **65**, 815–831 (2005)
4. Bae, M.M., Bose, B.: Resource placement in torus-based networks. IEEE Trans. Comput. **46**(10), 1083–1092 (1997)
5. Imani, N., Sarbazi-Azad, H., Zomaya, A.Y.: Resource placement in Cartesian product of networks. J. Parallel Distrib. Comput. **70**, 481–495 (2010)
6. Moinzadeh, P., Sarbazi-Azad, H., Yazdani, N.: Resource placement in cube-connected cycles. In: The International Symposium on Parallel Architectures, Algorithms, and Networks, pp. 83–89. IEEE Computer Society (2008)
7. Chudzikiewicz, J., Zieliński, Z.: On some resources placement schemes in the 4-dimensional soft degradable hypercube processors network. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds.) Proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX. June 30 – July 4, 2014, Brunów, Poland. AISC, vol. 286, pp. 133–143. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07013-1_13
8. Chudzikiewicz, J., Malinowski, T., Zieliński, Z.: The method for optimal server placement in the hypercube networks. In: Proceedings of the 2015 Federated Conference on Computer Science and Information Systems. ACSIS, vol. 2, pp. 947–954 (2015). https://doi.org/10.15439/2014F159
9. Brindha, L., Muthaiah, U.: Energy efficient mobile sink path selection using a cluster based approach in WSNs. Int. J. Innovative Res. Comput. Commun. Eng. **3**(3) (2015)

10. Erzin, A.I., Plotnikov, R.V.: Using VNS for the optimal synthesis of the communication tree in wireless sensor networks. In: Electronic Notes in Discrete Mathematics, vol. 47. Elsevier (2015)
11. Ghotra, A., Soni, N.: Performance evaluation of ant colony optimization based rendezvous leach using for mobile sink based WSNs. Int. J. Eng. Res. Dev. **11**(07) (2015)
12. Baby, S., Soman, M.: Rendezvous based techniques for energy conservation in wireless sensor networks - a survey. J. Netw. Commun. Emerg. Technol. (JNCET), **3**(3) (2015)
13. Bahnasee, A., Kamoun, N.E.: Study and analysis of a dynamic routing protocols' scalability over a dynamic multi-point virtual private network. Int. J. Comput. Appl. (0975-8887), **123**(2) (2015)
14. Sethi, A.S., Hnatyshin, V.Y.: The Practical OPNET User Guide for Computer Network Simulation. Chapman and Hall/CRC (2012)