ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2009. No. 8(96)*
ELEKTRONIKA IR ELEKTROTECHNIKA

AUTOMATION, ROBOTICS
T 125
AUTOMATIZAVIMAS, ROBOTECHNIKA

Virtual Private Networks – Based Home System

R. Volner, V. Smrž
Department of Air Transport, Institute of Transport, Faculty of Mechanical Engineering, VŠB – Technical University of Ostrava, Dr. Malého 17, 701 00 Ostrava, e-mail: Rudolf.volner@vsb.cz

Introduction

Recent studies conclude that early and specialized pre-hospital patient management contributes to emergency case survival, especially in cases of serious injuries of the head, the spinal cord and internal organs. The delivery of high-quality quality pre-hospital medical care in emergency cases (such as accidents happened within a stadium) requires immediate access to a wide range of medical information (critical bio-signals, patient's medical history, etc). However, stadium's paramedic personnel who usually are the first to handle such situations do not have immediate access to such information, as well as the required advanced theoretical knowledge and experience. Since, for practical and financial reasons, stadiums cannot be manned by specialized physicians (enough to handle crisis situations) paramedic personnel can only rely on directions provided to them by experts. The above mentioned problem could be efficiently solved through the usage of a mobile device which would allow specialized physicians located at a hospital site, to coordinate remote paramedical staff via tele-diagnosis and interactive tele-consultation means.

Based virtual private networks (VPNs) are designed to provide services with security and QoS comparable to that of a private network [1, 2]. The QoS guarantee is accomplished through bandwidth specification and reservation in the network. Bandwidth specification of a VPN is provided by the VPN owner and is often done in the form of *service level agreements* (SLAs) that specify the type of services and the amount of bandwidth for each type.

In terms of bandwidth specification and requirement, we can divide VPNs into two types: *pipe-model* VPNs [3] and *hose-model* VPNs [4]. A pipe-model VPN needs to specify the bandwidth requirement between any two endpoints (i.e., the customer equipment (CE) in Fig. 1). If the number of endpoints of a VPN is large, a pipe-model VPN is not an efficient solution as it is difficult to precisely predict the bandwidth requirement for each source-destination pair. A hose-model VPN, on the other hand, only needs to specify the amount of ingress and egress traffic (i.e., the amount of traffic that can be sent to and received from the backbone network) at each endpoint. Bandwidth specification is obviously much easier than that of a pipe-model VPN.

Many hose-model VPN provisioning algorithms have been proposed recently. They focus on the bandwidth efficiency in the construction of a single hose-model VPN [3]. If we add the following constraints: single-path, tree-topology, symmetric ingress and egress bandwidth at each endpoint, and infinite link capacity, then a minimum-bandwidth VPN can be constructed in polynomial time [5, 6].

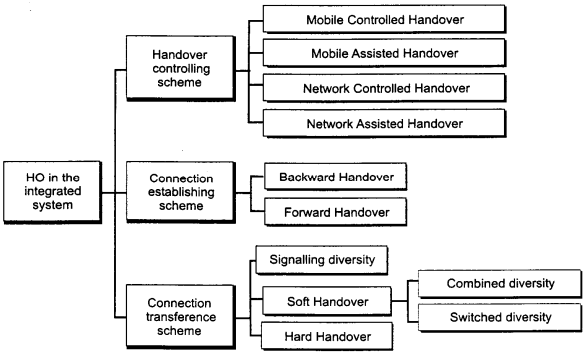

Fig. 1. Handover taxonomy for satellite/terrestrial network architecture

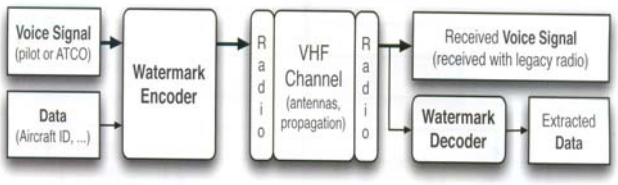

Fig. 2. Watermarking system for the aeronautic radio

Characterization of services, traffic sources and system teletraffic

Traditional traffic modeling of data sources assumed that the inter-arrival times of traffic packets were basically exponential in distribution and independent of one another, which means that the process is memory-less. However, recent studies of the behaviour of individual multimedia sources and system-level activity show that traffic traces are distributed in ways more complex than this.

Our analysis has aimed at improving the best-fitting model for a given traffic scenario when the underlying flow keeps changing over time and space. To be confident that the results are useful a model was sought that:

- was as simple as possible in a computational sense without compromising accuracy,
- had a physical explanation in the network context,
- can be related to real measurements for verification purposes by the operators.

The investigation focused on extensions that could retain tractability, in two steps as described below:

- statistical multiplexing,
- parameterization.

Traffic generation – if the traffic is memory-less, generation of traffic to support the simulations can be achieved simply by a negative exponentially distributed process to specify packet inter-arrival time.

Single VPN construction

Assume that the VPN to be added has endpoints and the ingress and egress bandwidth constraints at the VPN endpoints are given by the following vector

$$H = \left[(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)\right], \quad (1)$$

where α_i and β_i represent the VPN's ingress and egress bandwidth requested at node *i*, that is, α_i and β_i are the maximum amount of traffic that end node *i* can send into and receive from the MPLS backbone network.

Compared with a conventional traffic matrix

$$T = \{d_{ij}\}, \quad (2)$$

where d_{ij} represents the traffic rate from node *I* to node *j*, a hose-model VPN only provides the row sums

$$\sum_j d_{ij} = \alpha_i, \quad (3)$$

where α_i – the ingress traffic at node *i* and column sums

$$\sum_i d_{ij} = \beta_j, \quad (4)$$

where β_j – the egress traffic at node *j*. Conventional traffic engineering techniques are mostly based on the assumption that $T = \{d_{ij}\}$ is known and cannot be directly applied to a hose-model problem. In the following, we will present several linear programming formulations for constructing a single hose-model VPN.

If we can list every element in *D*, the problem of finding a routing scheme (i.e., x_{ij}^e) that minimizes the bandwidth reservation can be formulated as the following linear programming (LP) problem.

The approach outlined in formulation (1) has one problem - elements in *D* are too numerous to list. The problem is solved by the following property.

$$\begin{cases} \min \sum_{e \in E} y_e; \\ \sum_{e \in G^+(\upsilon)} x_{ij}^e - \sum_{e \in G^-(\upsilon)} x_{ij}^e = 0, \quad i, j \in R, \ \upsilon \neq i, j; \\ \sum_{e \in G^+(\upsilon)} x_{ij}^e - \sum_{e \in G^-(\upsilon)} x_{ij}^e = 1, \quad i, j \in R, \ \upsilon = i; \\ \sum_{e \in G^+(\upsilon)} x_{ij}^e - \sum_{e \in G^-(\upsilon)} x_{ij}^e = -1, \quad i, j \in R, \ \upsilon = j; \\ \sum_{i,j \in R} x_{ij}^e d_{ij} \leq y_e, \quad e \in E, \ T \in D; \\ 0 \leq y_e \leq c_e, \quad e \in E; \\ 0 \leq x_{ij}^e \leq 1, \quad i, j \in R, \ e \in . \end{cases} \quad (5)$$

This linear programming formulation has a polynomial number of variables and constraints. Once we have x_{ij}^e, the set of paths and the load splitting ratios among the paths can be obtained

Dynamic VPN construction

VPNs come and go. The dynamics of adding and deleting connections can have a significant impact on the scalability of the network. Current schemes for dynamic VPN construction are based on the constraint-based-routing framework where we first remove the bandwidth reserved for the existing VPNs before creating paths and reserving bandwidth for the new VPN. There are several problems with this approach:

- First, finding the optimal paths for a new VPN is not a trivial task and can be time consuming,
- Second, the number of paths inside the network grows with the number of VPNs,
- Third, each edge router needs to maintain the state information (like splitting ratios) of each individual VPN [2].

Because the number of VPNs can be very large in a high-speed network, maintaining the state information of each VPN can create a scalability problem. In the following, we solve the problem with a different approach.

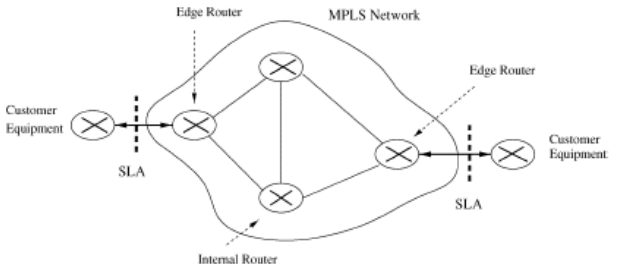

Fig. 3. MPLS back bone network

Conclusion

Provisioning VPNs in the hose model differs from that in the traditional pipe model in that the traffic demand matrix is unknown and only the maximum bandwidths of the traffic each VPN endpoint can send into and receive

from the network are given. Determining optimal routing and bandwidth reservation for VPNs in the hose model is a challenging problem because of the uncertainty of the point-to-point load distribution. Previous research work focuses on routing and bandwidth provisioning for single VPN.

The analytical techniques developed in the paper are general and can be used to tackle other network problems when traffic uncertainty is inherent. We will explore this issue in our future research.

References

1. **Rosen E., et al**.. Multiprotocol label switching architecture, RFC 3031, 2001.
2. **Rosen E., Rekhter Y.** BGP/MPLS VPNs RFC 2547, 1999.
3. **Jüttner A., Szabo I., Szentesi A**. On bandwidth efficiency of the hose resource management model in virtual private networks, in Proc. IEEE INFOCOM 2003, San Francisco, April 2003. – P. 386–395.
4. **Duffield N. G., Goyal P., Greenberg A., Mishra P., Ramakrishnan K. K., der Merwe J. E. V.** A flexible model for resource management in virtual private networks, in Proc. ACM SIGCOMM, San Diego, CA, August 1999. – P. 95–108.
5. **Kumar A., Rastogi R., Silberschatz A., Yener B**. Algorithms for provisioning virtual private networks in the hose model, in Proc. ACM SIGCOMM, Cambridge, MA, August 2001. – P. 135–146.
6. **Gupta A., Kleinberg J., Kumar A., Rastogi R., Yener B.** Provisioning a virtual private network: A network design problem for multicommodity flow, in Proc. ACM STOC, 2001. – P. 389–398.
7. **Volner R., Poušek L**. Wireless Biomedical Home Security Network – architecture and modelling", 38th Annual 2004 International Carnahan Conference on Security Technology. – Albuquerque, New Mexico, USA. – IEEE Catalog Number 04CH37572. – ISBN 0–7803–8506 – 3. – P. 69 – 76.
8. **Volner R., Poušek L**. Inteligence Security Home Network, 37th Annual 2003 International Carnahan Conference on Security Technology. – Taipei, Taiwan. – IEEE Catalog Number 03CH37458. – ISBN 0–7803–7882–2. – P. 30–37.
9. **Volner R**. Inteligence CATV – Traffic models, Design and Analysis, International Conference on Computer, Communication and Control Technologies CCCT'03 and The 9th International Conference on Information Systems Analysis and Synthesis ISAS 03. – Proceeding vol. IV. – Orlando, Florida, USA. – 2003. – ISBN 980–6560–05–1. – CD – ISBN 980–6560–10–8. – P. 340–345,
10. **Volner R., Boreš P.** Aviation Data Networks // Electronics and Electrical Engineering. – Kaunas: Technologija, 2005. – No. 7(63). – P. 22–26.

Received 2009 07 15

R. Volner, V. Smrž. Virtual Private Networks – Based Home System // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009. – No. 8(96). – P. 62–64.

The term security network intelligence is widely used in the field of communication security network. A number of new and potentially concepts and products based on the concept of security network intelligence have been introduced, including smart flows, intelligent routing, and intelligent web switching. Many intelligent systems focus on a specific security service, function, or device, and do not provide true end-to-end service network intelligence. True security network intelligence requires more than a set of disconnected elements, it requires an interconnecting and functionally coupled architecture that enables the various functional levels to interact and communicate with each other. Ill. 3, bibl. 10 (in English; abstracts in English, Russian and Lithuanian).

Р. Волнер, В. Смрж. Виртуальные персональные сети – основные домашние сети // Электроника и электротехника. – Каунас: Технология, 2009. – № 8(96). – С. 62–64.

Приведено понятие „охраны умной сети", которое широко применяется в персональных сетях связи. Приведено несколько новых и перспективных концепций и продуктов, основанных по принципах "охраны умной сети" , учитывая интелектуальные потоки информации, их маршруты, и переключения. Множество информационных систем, под воздействием сервиса охраны не представляет конечной информации. Правильная "охрана интелектуальной информации" требует больше контролируемых параметров, что создает возможности появиться внутреннему резервированию и функционально связанной архитектуре, которая позволяет связи на множестве функциональных уровней. Ил. 3, библ. 10 (на английском языке; рефераты на английском, русском и литовском яз.).

R. Volner, V. Smrž. Virtualūs privatūs tinklai – pagrindinis namų tinklas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2009. – Nr. 8(96). – P. 62–64.

Privačiuose ryšio tinkluose plačiai taikoma „sumanaus tinklo apsaugos" sąvoka. Straipsnyje pateikta keletas naujų potencialių koncepcijų bei produktų, paremtų sumanių tinklų apsaugos koncepcija, įskaitant protingus duomenų srautus, informacijos maršrutus ir perjungimus. Daugybė informacinių sistemų yra sąlygojamos konkretaus apsaugos serviso, funkcijų ar įrenginio ir nesuteikia galutinės informacijos. Teisingai sumanios informacijos apsaugai reikia daugiau parametrų, dėl to gali atsirasti vidinis rezervavimas ir funkcionaliai susieta architektūra, kuri įgalina bendrauti daugybe funkcijų lygių ir komunikuoti vienam su kitu. Il. 3, bibl. 10 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).