Efficient, Online Embedding of Secure Virtual Networks

Leonardo Richter Bays, Rodrigo Ruas Oliveira, Luciana Salete Buriol,
Marinho Pilla Barcellos, Luciano Paschoal Gaspary
Federal University of Rio Grande do Sul (UFRGS) – Institute of Informatics
{lrbays,ruas.oliveira,buriol,marinho,paschoal}@inf.ufrgs.br

I. Introduction

The use of network virtualization in large-scale, real environments depends on the ability to adequately map virtual network (VN) requests to physical resources, as well as to protect VNs against security threats. Although related work exists in the area of VN embedding [1]–[3], we were not aware of previous investigations aimed at reconciling efficient resource mapping and satisfaction of security requirements.

In this abstract, we briefly revisit a heuristic method we recently proposed that is capable of embedding large VNs with security support, in a time frame limited to the order of seconds. Our method leverages simulated annealing to iteratively search for possible VN mappings until a solution that meets certain quality criteria is found. In contrast to our previously developed ILP model [4], our novel heuristic approach features precise modeling of overhead costs of security mechanisms, and handles incoming VN requests in an online manner. The interested reader may refer to [5] for details about the work.

II. Proposed Solution

The proposed heuristic algorithm takes into account: the topology of physical and virtual networks; the capacity of physical routers and links, as well as the requirements of their virtual counterparts; the required security level of each VN[1]; processing and bandwidth costs of cryptographic algorithms; and the position of previously embedded VNs.

The algorithm builds an initial solution by semi-randomly placing virtual routers on physical routers. Virtual links are mapped to paths created using the Dijkstra's algorithm. The initial solution is then evaluated by calculating the aggregated bandwidth consumed by embedded VNs. Following this, the iterative search for solutions is started, ending when a maximum number of iterations is reached or the evaluation of the best found solution is better than a desired maximum. In each iteration, a new solution is generated by moving a virtual router to a different physical router, and recreating all links associated with this router. At the end of the iterative process, if the best found solution is feasible, the VN is embedded.

III. Evaluation

A number of experiments were performed in order to compare our novel heuristic algorithm with a new version of our ILP model[2]. Figure 1 shows that the heuristic method is able to find feasible mappings for environments using physical networks with up to 500 routers while remaining in the order of seconds. In contrast, the ILP model does not scale to physical networks with more than 100 routers. Figure 2, in turn, shows the bandwidth overhead of embedded VNs with different security requirements in one of the performed experiments. Clear differences in generated overhead are observed when certain security features are required, in particular when comparing these to VNs that do not require security provisions.

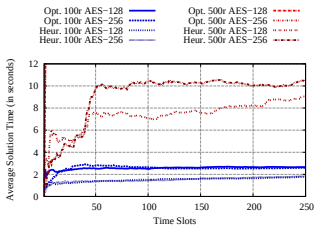

Fig. 1. Solution time in all performed experiments.

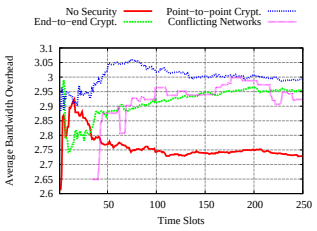

Fig. 2. Bandwidth overhead of different types of requests.

IV. Conclusions

Through our experiments, we were able to conclude that while the ILP model is better suited for smaller physical infrastructures, the heuristic algorithm is capable of scaling to larger substrate networks while still mapping VN requests in a timely manner. Further, the difference in overhead values of different types of VN requests highlights the importance of considering the impact of security mechanisms in terms of resource consumption in the VN embedding process. Failing to adequately consider this impact may lead to underprovisioning of resources, potentially causing performance issues on embedded VNs.

Acknowledgments

This work has been partially supported by FP7/CNPq (Project SecFuNet, FP7-ICT-2011-EU-Brazil), RNP-CTIC (Project ReVir), as well as PRONEM/FAPERGS/CNPq (Project NPRV).

References

[1] M. Yu, Y. Yi, J. Rexford, and M. Chiang, "Rethinking virtual network embedding: substrate support for path splitting and migration," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 17–29, Mar. 2008.

[2] N. Chowdhury, M. Rahman, and R. Boutaba, "Virtual network embedding with coordinated node and link mapping," in *INFOCOM 2009, IEEE*, april 2009, pp. 783 –791.

[3] G. P. Alkmim, D. M. Batista, and N. L. S. Fonseca, "Mapping virtual networks onto substrate networks," *Journal of Internet Services and Applications*, vol. 4, no. 1, p. 3, 2013.

[4] L. R. Bays, R. R. Oliveira, L. S. Buriol, M. P. Barcellos, and L. P. Gaspary, "Security-aware optimal resource allocation for virtual network embedding," in *Network and Service Management (CNSM), 2012 8th International Conference on*, 2012.

[5] L. R. Bays, "Efficient, online embedding of secure virtual networks," Master's thesis, Universidade Federal do Rio Grande do Sul, 2013.

[1] As in our previous publication, we consider three levels of security: end-to-end cryptography, point-to-point cryptography, and non-overlapping VNs.

[2] Our previous ILP model was updated in order to consider precise costs of security mechanisms and handle VN requests in an online manner.