Secure Virtual Network Embedding

Andreas Fischer and Hermann de Meer

University of Passau, Passau 94032, Germany,
{andreas.fischer, demeer}@uni-passau.de

Keywords: Network Virtualization, Virtual Network Embedding, Security

1 Introduction

Network virtualization has been recognized as an important technique to overcome the perceived ossification of the current Internet [1]. Several variations of network virtualization have already been discussed in the literature [3, 2]. These approaches use virtualization to partition and/or combine physical network resources into virtual network resources. An actual deployment of virtual networks then requires the network operator to perform a mapping of virtual resources onto physical resources. The question of how this mapping can be performed in an optimal way is commonly known as the Virtual Network Embedding (VNE) problem. Several algorithms to solve this problem have been proposed so far. These algorithms, however, focus on optimizing the use of resources with regard to performance. Security constraints to the VNE problem have not been investigated in depth, so far.

2 Secure Virtual Network Embedding

The mapping of virtual resources onto physical resources is subject to several security-related issues and concerns. The sharing of resources realized by virtualization opens up new vulnerabilities for side-channel attacks. Moreover, the virtualization software itself may be vulnerable to attacks, compromising the security of the hosted virtual resources. Finally, malicious operation of virtual resources may allow an attacker to gain unauthorized control over physical resources. To achieve a secure VNE, three types of constraints, therefore, have to be investigated:

- A virtual resource should not be mapped on physical resources that do not comply with the security requirements of the virtual resource.
- A critical physical resource should not be used to host virtual resources that are potentially harmful to its operation
- A critical virtual resource should not be co-hosted on the same physical resource as another potentially malicious virtual resource.

Implementation of these constraints in VNE algorithms is necessary to capture the trust relationships between different parties involved in the operation of

a virtualized network environment. In a multi-vendor network virtualization scenario, these constraints can, therefore, not be neglected. However, the adaption of VNE algorithms to incorporate these constraints in an appropriate manner is not trivial. Some algorithms may perform better than others under these constraints. In order to compare the modified algorithms, one has to define an appropriate set of metrics. Using those metrics, it becomes apparent which algorithms perform well under additional security constraints.

3 Conclusion and Future Work

Security constraints for the VNE problem have not been discussed in depth, so far. It is therefore necessary, to investigate the performance of existing algorithm, when operating with those additional constraints. One tool to investigate these issues is the ALEVIN software [4]. It provides an interface for easy implementation and evaluation of VNE algorithms. We are currently working on extending the software to incorporate arbitrary constraints for VNE algorithms.

Acknowledgements

The research leading to these results has received funding from the European Community's Seventh Framework Programme ([FP7/2007-2013] [FP7/2007-2011]) in the context of the ResumeNet and EuroNF projects (grant agreement no. 224619 and 216366, respectively).

References

1. Anderson, T., Peterson, L., Shenker, S., Turner, J.: Overcoming the internet impasse through virtualization. Computer 38(4), 34 – 41 (2005)
2. Berl, A., Fischer, A., de Meer, H.: Virtualisierung im Future Internet - Virtualisierungsmethoden und Anwendungen. Informatik-Spektrum 33(2), 186–194 (2010)
3. Chowdhury, N.M.K., Boutaba, R.: A survey of network virtualization. Computer Networks 54(5), 862 – 876 (2010)
4. Fischer, A., Botero, J.F., Duelli, M., Schlosser, D., Hesselbach, X., De Meer, H.: ALEVIN - A Framework to Develop, Compare, and Analyze Virtual Network Embedding Algorithms. Electronic Communications of the EASST 37, 1–12 (2011)