Toward Efficient Embedding of Survivable Virtual Networks

Rodrigo R Oliveira, Daniel S Marcon, Leonardo R Bays, Miguel C Neves,
Luciana S Buriol, Luciano P Gaspary, Marinho P Barcellos
Federal University of Rio Grande do Sul, Institute of Informatics, Porto Alegre, RS, Brazil
Email: {ruas.oliveira, daniel.stefani, lrbays, mcneves, buriol, paschoal, marinho}@inf.ufrgs.br

I. Introduction

Virtual Network Embedding is a procedure that maps virtual nodes and links to physical resources belonging to a substrate network. This procedure tends to increase the dependency on certain physical resources, allowing an attacker to launch DoS attacks on virtual networks by compromising nodes and links of the underlying physical substrate. High capacity physical links, in particular, are good targets since they may be important for a large number of virtual networks.

Previous research tackled this problem by setting aside additional resources as backup [1]–[3]. Although effective, this strategy may be unaffordable since backup resources cannot be used for new allocations, thus reducing the ability of the network to take new requests.

This paper presents a virtual network embedding approach which enables resilience to attacks and efficiency in resource utilization[1]. The proposed approach is composed of two complementary strategies: while a preventive strategy embeds virtual links into multiple substrate paths, a reactive strategy attempts to reallocate any capacity affected by a DoS attack.

II. Proposed Approach

The first strategy aims to provide resilience by embedding each virtual link into a set of substrate paths such that: (i) all capacity of links is distributed along the paths; and (ii) paths of the same virtual link have little or no similarity. This is achieved by splitting the capacity of virtual links into multiple paths. If the strategy is successful virtual links will remain operational – at a lower capacity – after disruptions.

The second strategy attempts to recover from disruptions by using the spare capacity of the substrate network. Whenever a physical link becomes inaccessible, a subset of the virtual links will be either fully or partially compromised. If the virtual link has no paths left, it means it was fully compromised. Otherwise, one or more paths remain available, and any spare bandwidth remaining on these paths can be used to restore the capacity of the virtual link.

III. Evaluation

Numerical experiments were performed with synthetically generated workload, similarly to related work. The physical network was composed of 50 nodes and around 200 links, while the virtual networks varied in size. The arrival rate of virtual networks followed a Poisson process with mean 7/100 rounds. Attacks followed a Poisson process with mean of 1/100 rounds and duration of 10 rounds.

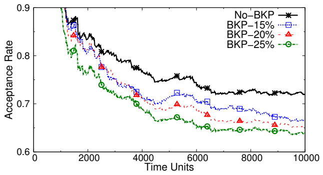

Figure 1. The use of backup resources reduces long-term acceptance rate.

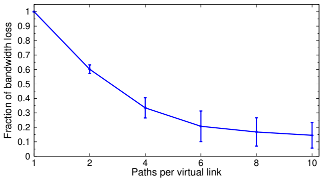

Figure 2. Bandwidth loss on scenarios with 1 to 10 paths per virtual link.

The proposed approach is denoted as No-Bkp, while backup-oriented schemes are denoted Bkp-X% (settings based on related work). Figure 1 shows that the use of backups decreases long-term acceptance rate. This difference tends to grow larger as more resources are used as backup.

Figure 2 shows that the proposed approach prevents bandwidth lost after disruption events. This loss is reduced by incrementing the number of paths, stabilizing at approximately 15%. The observed non-linear behavior is due to the capacity of the substrate network to provide disjoint end-to-end paths.

IV. Conclusion

This paper presented a novel approach for protecting virtual networks against disruptions in the substrate. Unlike previous work, our approach does not use backups. Rather, it employs multiple path virtual link embedding and opportunistic recovery to mitigate the impact of attacks. Results show that the proposed approach provides resilience to virtual networks with a higher long-term acceptance rate.

Acknowledgment

This work has been 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] H. Yu, C. Qiao, V. Anand, X. Liu, H. Di, and G. Sun, "Survivable virtual infrastructure mapping in a federated computing and networking system under single regional failures," in *Proc. GLOBECOM, IEEE*, 2010.

[2] T. Guo, N. Wang, K. Moessner, and R. Tafazolli, "Shared backup network provision for virtual network embedding," in *Proc. ICC, IEEE*, 2011.

[3] M. R. Rahman, I. Aib, and R. Boutaba, "Survivable virtual network embedding," in *NETWORKING 2010*, ser. LNCS, M. Crovella, L. Feeney, D. Rubenstein, and S. Raghavan, Eds. Springer Berlin / Heidelberg, 2010, vol. 6091.

[4] R. R. Oliveira and M. Barcellos, "Toward cost-efficient, DoS-resilient virtual networks with ORE: opportunistic resilience embedding," Master's Dissertation, Universidade Federal do Rio Grande do Sul, 2013.

[1] A full description of the proposed approach is available in [4]