Improving Resiliency Against DDoS Attacks by SDN and Multipath Orchestration of VNF Services

Onur Alparslan*, Onur Gunes†, Y. Sinan Hanay†, Shin'ichi Arakawa* and Masayuki Murata*
* Graduate School of Information Science and Technology, Osaka University, Japan
Email: {a-onur, arakawa, murata}@ist.osaka-u.ac.jp
† Department of Computer Engineering, TED University, Turkey
Email: {onur.gunes, sinan.hanay}@tedu.edu.tr

***Abstract*—We propose an architecture that increases the resiliency against DDoS attacks by leveraging virtual network functions (VNF) and software defined networking (SDN). In the first step, the proposed architecture places the virtual network functions (VNF) optimally by solving a linear program. In the second step, in order to add preemptive protection against DDoS attacks, special filter VNFs and secondary paths passing through these filter VNFs are set up by solving another linear program. Under a DDoS attack, SDN controller switches the routes affected by the attack to the secondary paths for filtering DDoS traffic in order to prevent over-utilization. The simulation results show that the proposed architecture can absorb higher amount of DDoS traffic with low impact on the average hop count.**

I. Introduction

A recent report by Akamai shows that distributed denial of service (DDoS) attacks over 100 Gbps have increased by 140% over the same period of the previous year [1]. As the frequency and complexity of DDoS attacks increase year by year, many networks have started to deploy protection and mitigation solutions against DDoS.

Recently, software-defined networking (SDN) has become popular in the networking community as it decouples data and control plane in the networks, and provides greater flexibility in network management. Along with the SDN development, network function virtualization (NFV) has been integrated to networks to replace high cost, inflexible hardware middleboxes by implementing network functions in the software.

DDoS attacks can be mitigated by redirecting traffic to cloud-based mitigation services, which filter DDoS traffic in the cloud. However, carrying the heavy DDoS traffic to another network can be costly and may cause congestion at the edge links of the network. Another possible solution is VNF-based filtering. Filter VNFs can filter traffic without sending the traffic to cloud. For example, an architecture called CoFence was proposed for dynamic load balancing using filter VNFs [2]. CoFence does filtering by a VNF called IPS (Intrusion Protection Service) placed in the same network and other domains (i.e. cloud). CoFence allows dynamic load balancing between multiple IPS servers in multiple domains. In another work, when an attack is detected at the edge node of a network, the traffic is forwarded to an OpenFlow controller implemented as a VNF, which filters the traffic and sends it back to the client through the edge node [3]. Both of these architectures are mainly for protecting networks against attacks that are coming from the outside. Moreover, the problem of optimum placement of VNFs, routes and the service chains for protection against DDoS attacks has not been addressed yet. We tackle this problem in this work. In this paper, we propose an architecture that leverages SDN and VNF technologies to increase the resiliency of networks against DDoS traffic sourcing from both the outside and inside of the network.

978-1-5386-0728-2/17/$31.00 © 2017 IEEE

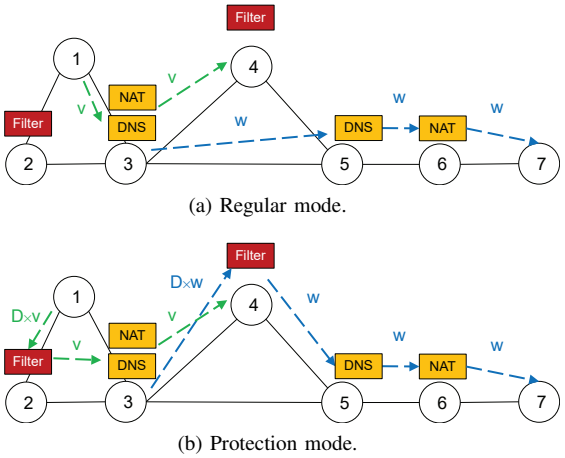
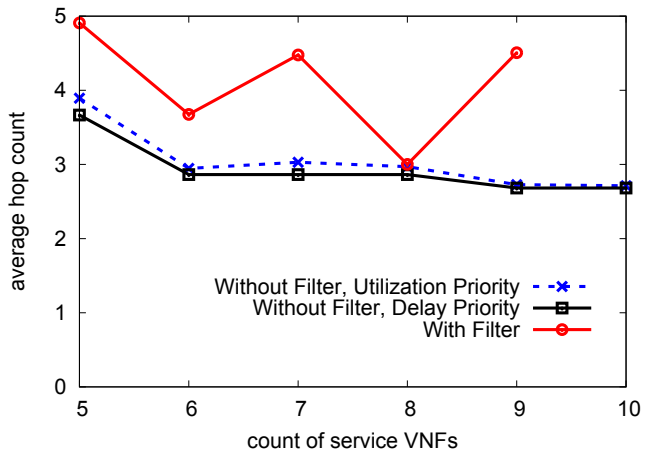


Fig. 1. The illustration of the network in "regular mode" and "protection mode". v and w denote the amount of traffic from node 1 to 4 and node 3 to 7, respectively. Under an attack, the flow from node 1 to 4 is redirected over node 2 instead of node 3, since node 2 has a filter VNF.

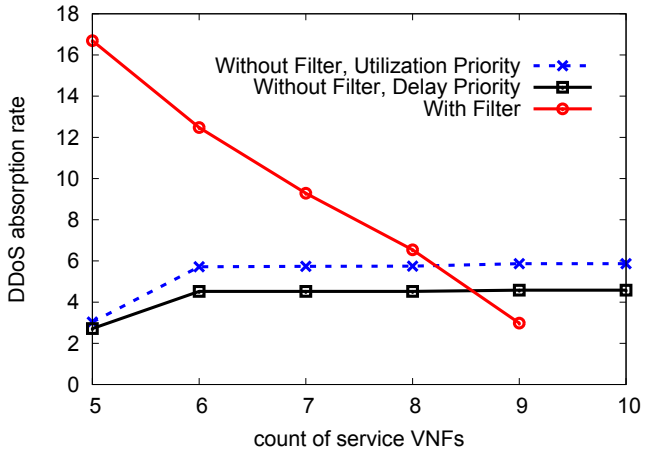
The rest of this paper is organized as follows. In Section II, we describe the proposed architecture. Then, we evaluate the performance of the architecture in Section III. We conclude this paper in Section IV.

II. Architecture

Our proposal aims to increase the resiliency against over-utilization when a DDoS attack large enough to disrupt the network services occurs, while minimizing the performance penalty incurred by the proposed methods when the network is not under a heavy DDoS attack. We assume that there is a network with SDN and VNF capability, with a list of service chain requests between nodes. In the first step, the proposed architecture calculates the placement of the service NFVs and the routes of the service chains in the network by solving a



(a) The effect on hop count.



(b) The effect on attack absorption rate.

Fig. 2. The effect of number of VNFs on hop count and absorption rate. Filter VNFs increase the DDoS absorption rate at the cost of increasing average hop counts. The line denoted by "With Filter" stops at x=9, because there must be at least one filter VNF resulting 9 service VNFs as the total number of VNFs is 10.

linear program according to the list of service chains and the performance objectives. Then, the network is set up according to the optimization result, which is called "regular mode". In the second step, in order to filter out possible DDoS traffic, specialized filter VNFs are established in the network. The placement of filter VNFs and the paths of secondary service chains for a "protection mode" network are calculated by another linear program. As a condition, the secondary paths of all service chains first pass through a filter VNF before other VNFs in order to prevent their over-utilization due to DDoS traffic. In the second step, the placement of the service VNFs calculated in the first step is kept.

Fig. 1 illustrates our approach. A network with 7 routers containing two kinds of service VNFs (i.e. DNS and NAT) is shown. Unless there is a heavy DDoS traffic causing congestion, the network operates in "regular mode" where service chains use the shortest paths without passing through the filter VNFs as shown in Fig. 1a.

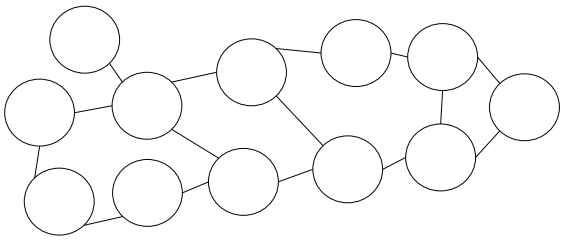


Fig. 3. Simulated topology

In the "protection mode", the mechanism is as follows. Assume that both service chains are under a heavy DDoS traffic with an average incoming traffic magnification of D. Assume that nodes 1, 3 and 5 cannot carry filter VNFs, After detecting a heavy DDoS traffic, the network switches to "protection mode", where the SDN controller changes the paths of service chains by applying the fast reroute mechanism to forward the traffic to the pre-calculated secondary paths, which pass through filter VNFs as shown in Fig. 1b. This way, DDoS attacks are prevented immediately without waiting for the calculation of new routes or establishing/moving VNFs. After the rerouting, some links carry the filtered and unfiltered traffic together, e.g., the traffic on the link from node 3 and 4 due to the service chains from node 1 to 7 and node 3 to 7 increases from v to $v + D \times w$. The main of objective of the linear program in the second stage of optimization is to calculate the secondary paths and the placement of filter VNFs that maximize the value of D without over-utilization.

An important part of this approach is to find the right number of filters. With many filters, the traffic passing through a single filter may not be enough to detect DDoS packets as sampling per filter VNF decreases as discussed in [4]. On the other hand, with few filters the performance of the network degrades as the secondary paths get even longer, which increases the delay of service chains and the utilization of the links.

III. Simulation Results

We implemented a linear optimization program for the proposed architecture in CPLEX by extending the formulation and the implementation in [5]. We simulated the 12-node Internet2 topology shown in Fig. 3 and the service chain traffic set using three service VNFs as given in [5]. The ladder-like topology limits the number of possible paths between the node pairs in the right and left side of the topology, so it is a challenging topology for multipath traffic engineering. In general, the processing limitations and the costs like license per VNF and energy consumption limit the number of VNFs in a network. In order to do a fair comparison, we limited the total number of service and filter VNFs established in the network to 10 and applied our algorithm to calculate the optimum placement of VNFs and the primary/secondary paths of the service chains by changing the ratio of service and filter VNFs.

Fig. 2 shows the effect on average hop count and DDoS absorption rate, which is the maximum average traffic multiplication rate due to DDoS that the network can carry without link over-utilization. The filters prevent DDoS traffic to reach service VNFs, so VNF over-utilization is not considered. The x-axis is the number of service VNFs. When 10 service VNFs are established, there is no protection against DDoS as there are no filter VNFs. The lines denoted by "without filter" show the performance when the network operates in the "regular mode". The result of two possible optimization objectives based on utilization and delay priority are shown. The line denoted by "with filter" shows the performance after the network switches to "protection mode" in the case of a heavy DDoS attack.

Fig. 2a shows that adding filters caused in a slow increase in the average hop count in "regular mode". Switching to "protection mode" increased the average hop count by around one hop. Fig. 2b shows that the maximum DDoS absorption rate of the "regular mode" was $5.8X$ when all VNFs are service VNFs and the network is optimized for minimizing the maximum utilization. Even though a challenging ladder-like topology was simulated, using 5 filter VNFs increased the absorption rate to $16.7X$ in "protection mode" at the expense of increasing the average hope count by around one hop in the "regular mode". Using a single VNF resulted in low absorption in the "protection mode" even less than "regular mode" due to long secondary paths.

IV. Conclusion

We proposed an architecture that increases the resiliency against DDoS attacks by leveraging SDN and multipath orchestration of VNF services. The architecture calculates the multipath VNF orchestration by a two stage linear programming optimization. The simulation results revealed that the architecture improves the DDoS traffic absorption rate, while minimizing the performance penalty when the network is not under heavy DDoS attack. As a future work, we will devise a heuristic solution for fast optimization of large topologies that cannot be solved by CPLEX.

Acknowledgment

This research was supported in part by Grant-in-Aid for Scientific Research (A) 15H01682 of the Japan Society for the Promotion of Science (JSPS) in Japan.

References

[1] "Akamai's State of the Internet," Tech. Rep., 2016. [Online]. Available: https://goo.gl/wq3Kad

[2] B. Rashidi and C. Fung, "CoFence: A collaborative DDoS defence using network function virtualization," in *12th International Conference on Network and Service Management (CNSM)*, 2016, pp. 160–166.

[3] K. Giotis, G. Androulidakis, and V. Maglaris, "A scalable anomaly detection and mitigation architecture for legacy networks via an OpenFlow middlebox," *Security and Communication Networks*, vol. 9, no. 13, pp. 1958–1970, 2016.

[4] T. Ha, S. Yoon, A. C. Risdianto, J. Kim, and H. Lim, "Suspicious flow forwarding for multiple intrusion detection systems on software-defined networks," *IEEE Network*, vol. 30, no. 6, pp. 22–27, November 2016.

[5] F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and O. C. M. B. Duarte, "Orchestrating virtualized network functions," *IEEE Transactions on Network and Service Management*, vol. 13, no. 4, pp. 725–739, Dec 2016.