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*
* Osaka University, Japan ** TED University, Turkey

Abstract

We propose a multipath VNF orchestration for optimum placement of VNFs and service chains by a two stage linear programming optimization that increases the resiliency against DDoS attacks

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 of links.

The simulation results show that the architecture increases the DDoS traffic absorption rate instantly, while the operator gains time to calculate and apply a solution specifically optimized for the DDoS pattern.

Introduction

As the frequency and complexity of distributed denial of service (DDoS) attacks increase year by year, many networks have started to deploy protection and mitigation solutions against DDoS

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. Moreover, VNF has many benefits like flexibility, scalability and elasticity

An optimum multipath placement of VNFs, routes and the service chains for protection against DDoS attacks has not been addressed yet.

We propose a two level multipath ILP formulation 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.

Architecture

Our proposal aims to increase the resiliency against over-utilization of links 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.

In the first step, the proposed formulation calculates the placement of the service NFVs and the routes of the service chains in the network by solving an ILP 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 ILP. It assumes that DDOS increases all traffic to ***D*** times in average. 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. The placement of the service VNFs calculated in the first step is kept.

Unless there is a heavy DDoS traffic causing congestion, the network operates in "**regular mode**" where service chains use the primary paths without passing through the 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.

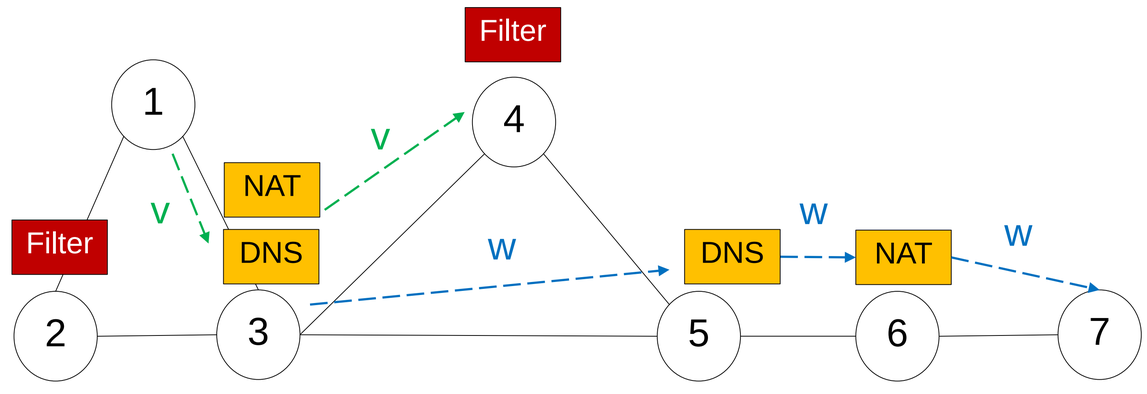

Fig. 1: Regular mode

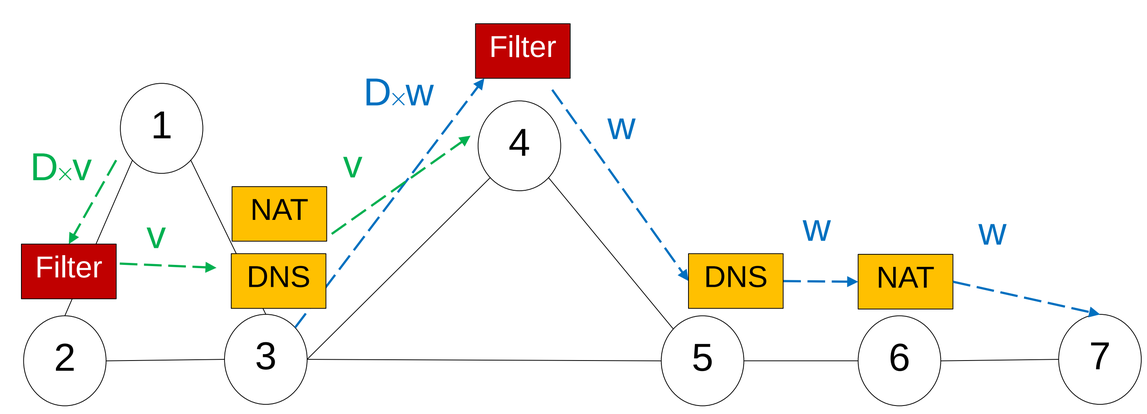

Fig. 2: Protection mode

Results

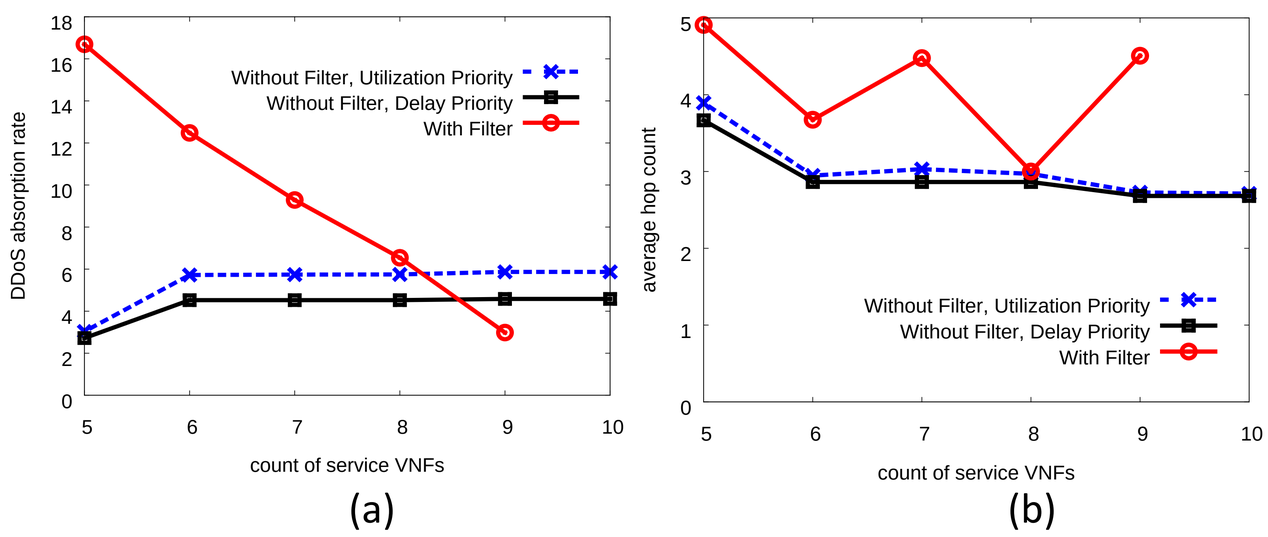

Fig. 3. Simulation results

Simulated the 12-node Internet2 topology and service chain traffic sets using three service VNFs. In order to do a fair comparison, we fixed 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. The objective is a weighted sum of delay and link utilization ratio.

Fig. 3 shows the effect on average hop count and DDoS absorption rate ***D***, which is the maximum average traffic multiplication rate due to DDoS that the network can carry without link over-utilization. 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 link utilization ratio 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. 3.a shows that the maximum DDoS absorption rate of the "regular mode" was D=5.8 when all VNFs are service VNFs and the network is optimized for minimizing the maximum utilization. Using 5 filter VNFs increased the absorption rate to D=16.7 in "protection mode".

Fig. 3.b 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.

Conclusions

The simulation results revealed that the architecture increases the DDoS traffic absorption rate instantly, while minimizing the performance penalty using secondary paths. As the severity of DDoS decreases, the operator gains time to calculate and apply a solution specifically optimized for the DDoS pattern.