Analyzing different Distributed Denial of Service attacks and its solutions in a Software Defined Networks

Supervisors:
Dr. Chhagan Lan
Prof. Mauro Conti

Author:
Dylan Durand
d.r.durand@student.tudelft.nl

I. What is a software defined network?

- Software-Defined Networking (SDN) is a relatively new network architecture (~2008).
- The data and control plane are separated to allow for a centralized controller (Fig 1.).
  - The switches (in the data plane) now only act as forwarding devices.
- The controller decides where the data goes by installing flow rules on the switches.

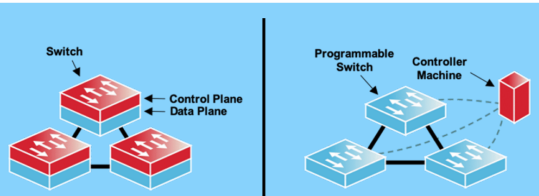

Figure 1: An simple illustration of a classical network and a Software Defined Network

II. What is a Distributed Denial of Service attack?

- When a network is flooded with unwanted traffic
- This is usually done by the attacker deploying a botnet - a group of internet devices that have been hijacked.
- This attack disrupts the server's processes and makes it unusable for the target users (Fig 2.).

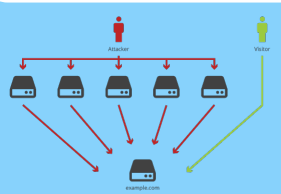

Figure 2: A simple illustration of how a DDoS attack is carried out

III. Motivation

- More networks will use the SDN architecture in the future, which creates a more significant demand to overcome the vulnerabilities in this network.
- **DDoS** attacks are one of the most uncomplicated attacks to be carried out. This creates the need for an analysis of the different attacks and their solutions to help keep the network safe.

IV. Research method

Find and read the latest literature
Analyze different forms of DDoS attacks
Compare solutions
Explain limitations in current mitigation techniques

V. SDN-related threats

- **Flowtable overflow -** Constant flooding of the data switches will use up its memory, so processing the incoming packets will become impossible. Therefore legitimate requests will not be handled either
- **Controller resource saturation -** The controller CPU and memory will be exhausted when handling flood requests. This will worsen the network's overall performance as legitimate requests will not be handled.

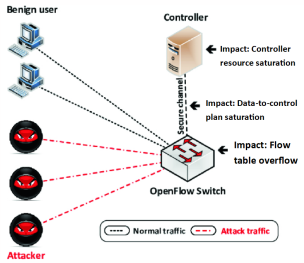

Figure 3: Highlighting the different impacts of a DDoS attack in a SDN

- **Data-to-control plane saturation -** Incoming packets are buffered within the switch, and only partial information is forwarded. However, when this buffer is full, the whole packet will be forwarded, which will congest the communication channel. In these situations, the network becomes unavailable to its users.

VI. State-of-the-art solutions

Solutions	Description
SVM [1]	SVM classifier used to detect DDoS packet
K-means [2]	K-means clustering algorithm is used to detect malicious traffic distribution
vSwitchGuard [3]	Evaluated different classifiers, combination of K-NN and variational autoencoder performed best
DETPro [4]	Modified decision tree used to detect DDoS packets
SAFETY [5]	Mapping of DNS requests and entropy is used
WisdomSDN [6]	Entropy method with a dynamic threshold is used
DAISY [7]	Uses different thresholds to identify a DDoS attack

VII. Conclusion and future work

Evaluation

- Machine learning-based solutions incur more significant overhead due to their complexity.
- All solutions proved to have a high detection rate in their evaluation.
- The combination of different machine learning classifiers leads to improved mitigation results.

Future work

- More combinations of machine learning classifiers should be experimented with.
- A potential new solution includes using an entropy-based method with a dynamic threshold to detect a potential DDoS attack. Furthermore, K-NN and variational autoencoder are used to classify the flow.

References:

[1] L. Yang and H. Zhao, "Ddos attack identification and defense using sdn based on machine learning method," in 2018 15th international symposium on pervasive systems, algorithms and networks (I-SPAN), pp. 174–178, IEEE, 2018.
[2] J. Cui, J. Zhang, J. He, H. Zhong, and Y. Lu, "Ddos detection and defense mechanism for sdn controllers with k-means," in 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC), pp. 394–401, IEEE, 2020.
[3] . Khamaiseh, E. Serra, and D. Xu, "vswitchguard: De- fending openflow switches against saturation attacks," in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 851–860, IEEE, 2020.
[4] . Chen, J. Pei, and D. Li, "Detpro: A high-efficiency and low-latency system against ddos attacks in sdn based on decision tree," in ICC 2019-2019 IEEE Inter- national Conference on Communications (ICC), pp. 1– 6, IEEE, 2019.
[5] . Kumar, M. Tripathi, A. Nehra, M. Conti, and C. Lal, "Safety: Early detection and mitigation of tcp syn flood utilizing entropy in sdn," IEEE Transactions on Network and Service Management, vol. 15, no. 4, pp. 1545–1559, 2018.
[6] . Abou El Houda, L. Khoukhi, and A. S. Hafid, "Bring- ing intelligence to software defined networks: mitigat- ing ddos attacks," IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2523–2535, 2020.
[7] M. Imran, M. H. Durad, F. A. Khan, and H. Ab- bas, "Daisy: A detection and mitigation system against denial-of-service attacks in software-defined networks," IEEE Systems Journal, vol. 14, no. 2, pp. 1933–1944, 2019.