Future of DDoS Attacks Mitigation in Software Defined Networks

Martin Vizváry, Jan Vykopal

AIMS 2014, Brno, July, 1st 2014

Current and Future Networking

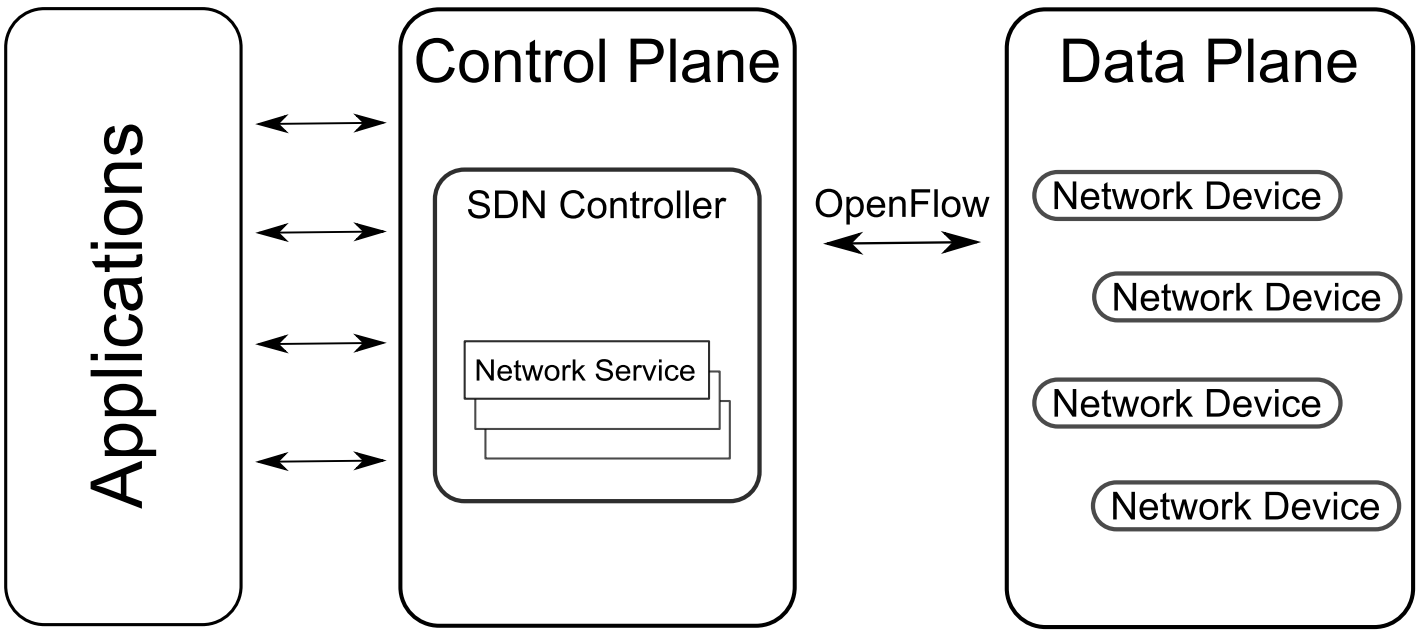
- Traditional networking principles remain mostly unchanged over the past decades.
- Clouds and Internet of Things demand scalable and dynamic networks.
- There are emerging new concepts of networking.
- DDoS attacks in networks remains a threat.

Current and Future Networking

- Traditional networking principles remain mostly unchanged over the past decades.
- Clouds and Internet of Things demand scalable and dynamic networks.
- There are emerging new concepts of networking.
- DDoS attacks in networks remains a threat.

What about DDoS attacks in Software Defined Networks?!

Software Defined Networks



Hypothesis

Software Defined Networks provides an ideal platform for distributed detection and mitigation of DDoS attacks.

Hypothesis

Software Defined Networks provides an ideal platform for distributed detection and mitigation of DDoS attacks.

Why?

Hypothesis

Software Defined Networks provides an ideal platform for distributed detection and mitigation of DDoS attacks.

Why?

- **The whole concept of SDN is flow based** – detection

Hypothesis

Software Defined Networks provides an ideal platform for distributed detection and mitigation of DDoS attacks.

Why?

- **The whole concept of SDN is flow based** – detection
- **There is a central point of knowledge** – mitigation

Hypothesis

Software Defined Networks provides an ideal platform for distributed detection and mitigation of DDoS attacks.

Why?

- **The whole concept of SDN is flow based** – detection
- **There is a central point of knowledge** – mitigation
- **Standardized API used for control and data plane communication** – mitigation

Research questions

I. ***What differences does SDN bring compared to traditional networks and its monitoring?***

Research questions

I. *What differences does SDN bring compared to traditional networks and its monitoring?*

II. *What are SDN specific security vulnerabilities both on the data and control plane?*

Research questions

I. *What differences does SDN bring compared to traditional networks and its monitoring?*

II. *What are SDN specific security vulnerabilities both on the data and control plane?*

III. *How to optimally mitigate DDoS attacks in Software Defined Networks?*

Research question I.

What differences does SDN bring compared to traditional networks and its monitoring?

- **Gain an thorough understanding of SDN.**
- **Compare the differences between SDN and current networks.**
- **Analyze flow monitoring possibilities in SDN.**

Research question II.

What are SDN specific security vulnerabilities abused by attackers in DDoS attacks both on the data and control plane?

- **Analyze possible abusive attributes of the data and control plane.**
- **Analyze open-source solution Open vSwitch.**
- **Analyze business SDN-ready devices.**

Research question III.

How to optimally mitigate DDoS attacks in Software Defined Networks?

- **Mitigation of the DDoS attack in SDN environment**
  - **Use all devices of company infrastructure in data plane for filtering DDoS.**
  - **Analyze trace-back possibilities in pure SDN environment and filter the attack closer to the source.**

Next Steps

- Create a state of the art in SDN network monitoring and security.
- Analyze attack, defense and monitoring mechanisms in current networks and the possibility of their deployment in SDN environment.
- Prepare a pure SDN testbed with set of synthetic and real traffic based data sets to verify our hypothesis.

Summary

I am in initial phase of a PhD study.

Goals:

- Obtain a thorough understanding of SDN in the context of security and monitoring in this environment.
- Find an optimal way of mitigation DDoS attacks using the benefits of SDN infrastructure.

Thank you for your attention.

I'd be happy to answer your questions, however I'd be happier to hear your advices.

Martin Vizváry, Jan Vykopal