Bohatei: Flexible and Elastic DDoS Defense

Seyed K. Fayaz*, Yoshiaki Tobioka*, Vyas Sekar*, Michael Bailey◆
*Carnegie Mellon University, ◆University of Illinois at Urbana-Champaign

Project Silver

Motivation

DDoS attacks are increasing in number, volume, and diversity.

DDoS defense today relies on proprietary hardware appliances deployed at fixed locations.

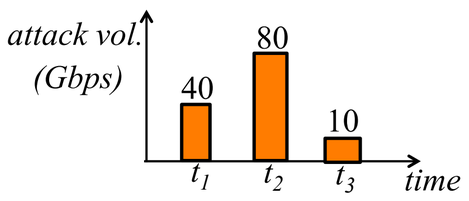
Fundamental limitations of the current approach:
1. High capital cost
2. Fixed capacity
3. Fixed functionality
4. Fixed location

High capital cost

Price of DDoS Defense Appliances

Bit Rate	Price
1Gbps	$11,000-$38,000
4Gbps	$68,000
12Gbps	$128,000

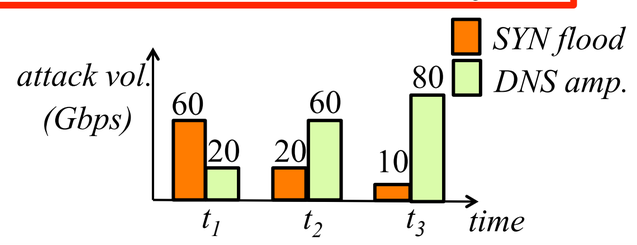
Fixed capacity



Today: Hardware appliance res. footprint=240Gbps

Ideal: Elastic scaling res. footprint=130Gbps

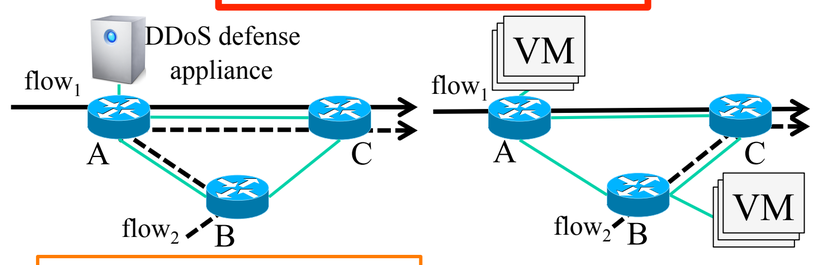
Fixed functionality



Today: hardware appliance res. footprint=420Gbps

Ideal: elastic scaling res. footprint=250Gbps

Fixed location



Today: traffic footprint given hardware appliance=3 hops

Ideal: traffic footprint given elastic scaling=2 hops

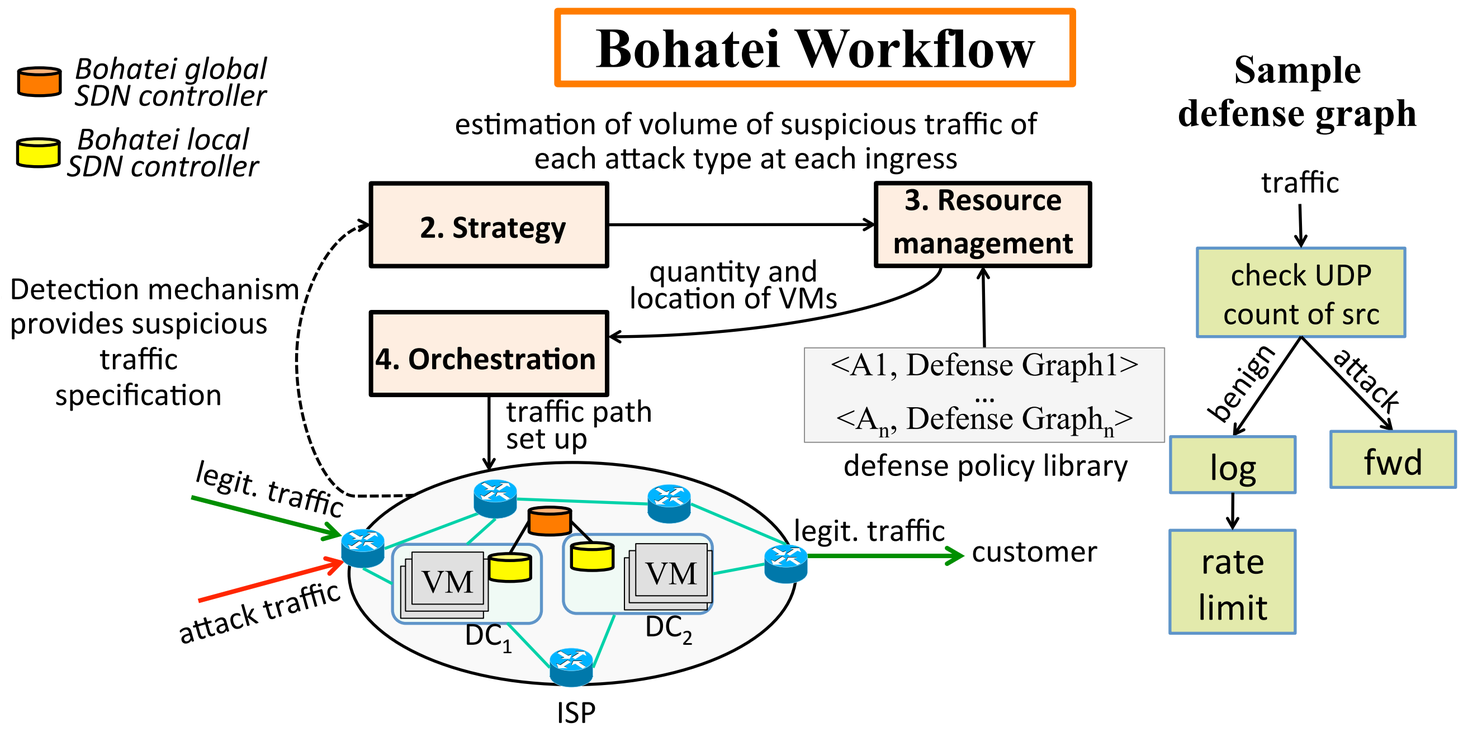
Vision: Enabling Flexible and Elastic Defense using Bohatei

Can we build a *flexible* and *elastic* DDoS defense platform that can handle attacks with varying type, volume, and location?

- Flexibility in traffic steering using SDN
- Elasticity in defense deployment using NFV

Bohatei envisions a four-step workflow:
1. Attack detection (using existing methods)
2. Estimation of volume of attack traffic
3. Resource management
4. Network orchestration

Bohatei Workflow



Sample defense graph

Bohatei Key Ideas

Challenges

1- Responsive resource management: Optimal decision making about the number and type of defense VMs takes hours.

2- Scalable network orchestration: The existing SDN approach to set up switch forwarding rules in a *per-flow* and *reactive* manner swamps the SDN controller.

3- Coping with dynamic adversaries that may quickly change the type, volume, and ingress of attack.

Ideas

1- Hierarchical optimization decomposition:
- The ISP-wide controller determines how many and what types of VMs to run in each datacenter
- Each per-datacenter controller determines the specific server on which each defense VM will run.

2- Proactive tag-based forwarding:
- Forwarding rules based on per-VM tags
- Pro-active switch configuration

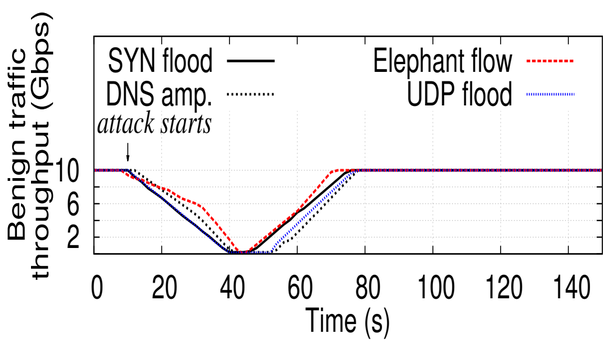
3- Online adaptation: A defense strategy adaptation approach inspired by online algorithms for minimizing *regret* (i.e., how much better we could have done in retrospect)

Key Results

Implementation

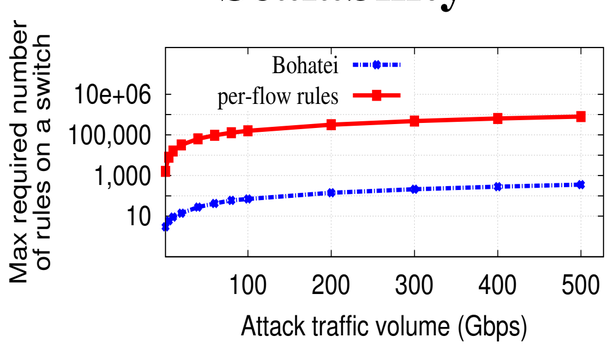
- Implementation of a Bohatei controller using OpenDaylight
- Use of open source tools (e.g., OpenvSwitch, Snort, Bro, iptables) as defense modules
- Evaluation on a real testbed as well as using simulations
- Code is made available

Responsiveness



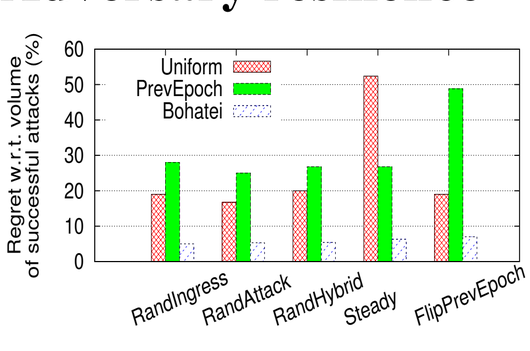
Bohatei responds rapidly (<1 min) to diverse attacks.

Scalability



Handling ~1Tbps attacks requires <1K rules on a switch

Adversary resilience



Bohatei's online adaptation achieves low regret

Carnegie Mellon University

project homepage

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

http://silver.web.unc.edu

Cloud Security Horizons Summit, March 2016