Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks

Kostas Giotis

Network Management & Optimal Design Laboratory (NETMODE)
School of Electrical & Computer Engineering
National Technical University of Athens

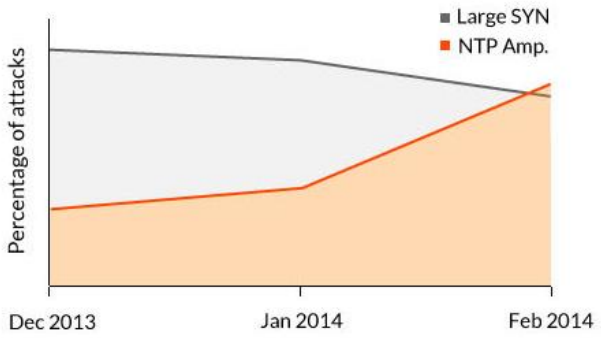
European Workshop on Software Defined Networks
September 3rd, 2014
Budapest, Hungary

Malicious traffic growth

- Companies, governments and institutions are increasingly targeted by surges of malicious traffic
  - **Target:** Service discovery & disruption

- DDoS attacks become more sophisticated
  - Exploitation of common protocols (DNS, NTP)
  - High traffic volumes, trough Amplification Techniques

DDoS attacks



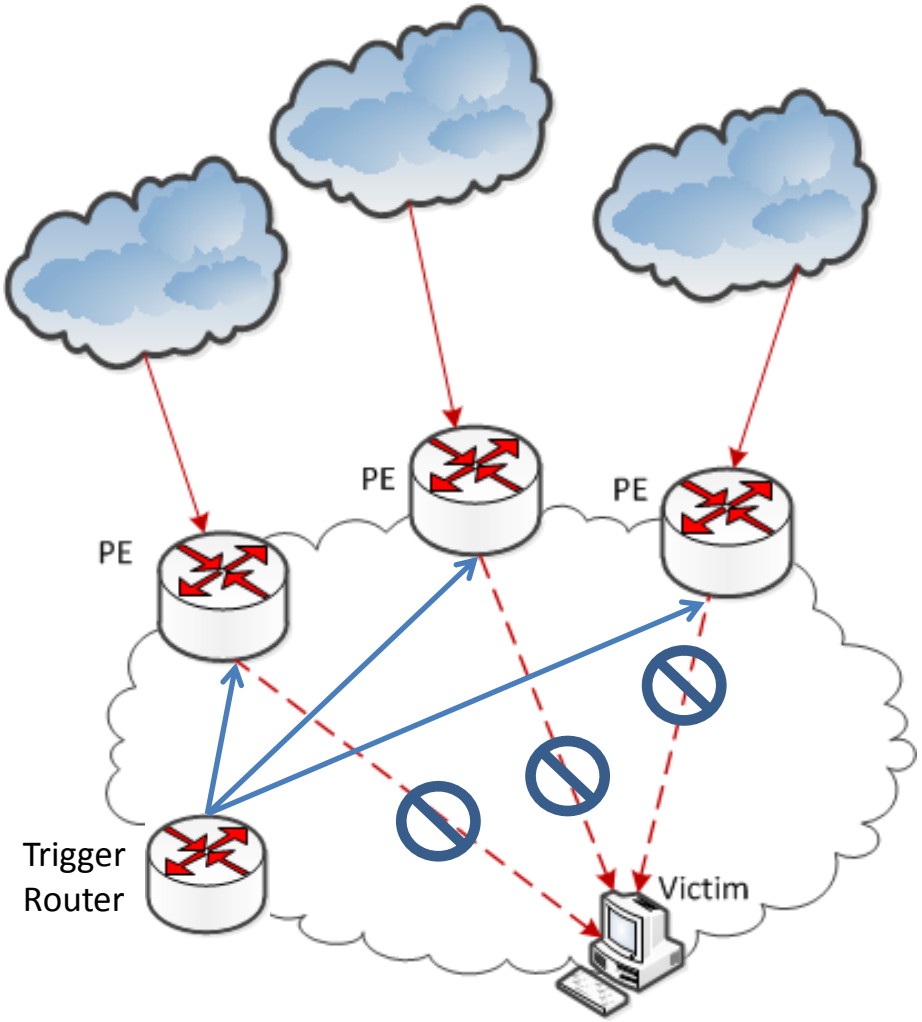
- The shift towards amplification attacks may point to a new trend.
- Amplification techniques produce attacks of higher volume

[1] http://www.incapsula.com/blog/ddos-threat-landscape-report-2014.html

Common Countermeasures:

- Access Control Lists
  - – Waste network resources
  - – High-end equipment
  - – High administrative costs
- Remote Triggered Black Hole (RTBH)
  - + Propagate a null route to all iBGP peers
  - + Requires less human intervention
  - – Victim becomes unreachable

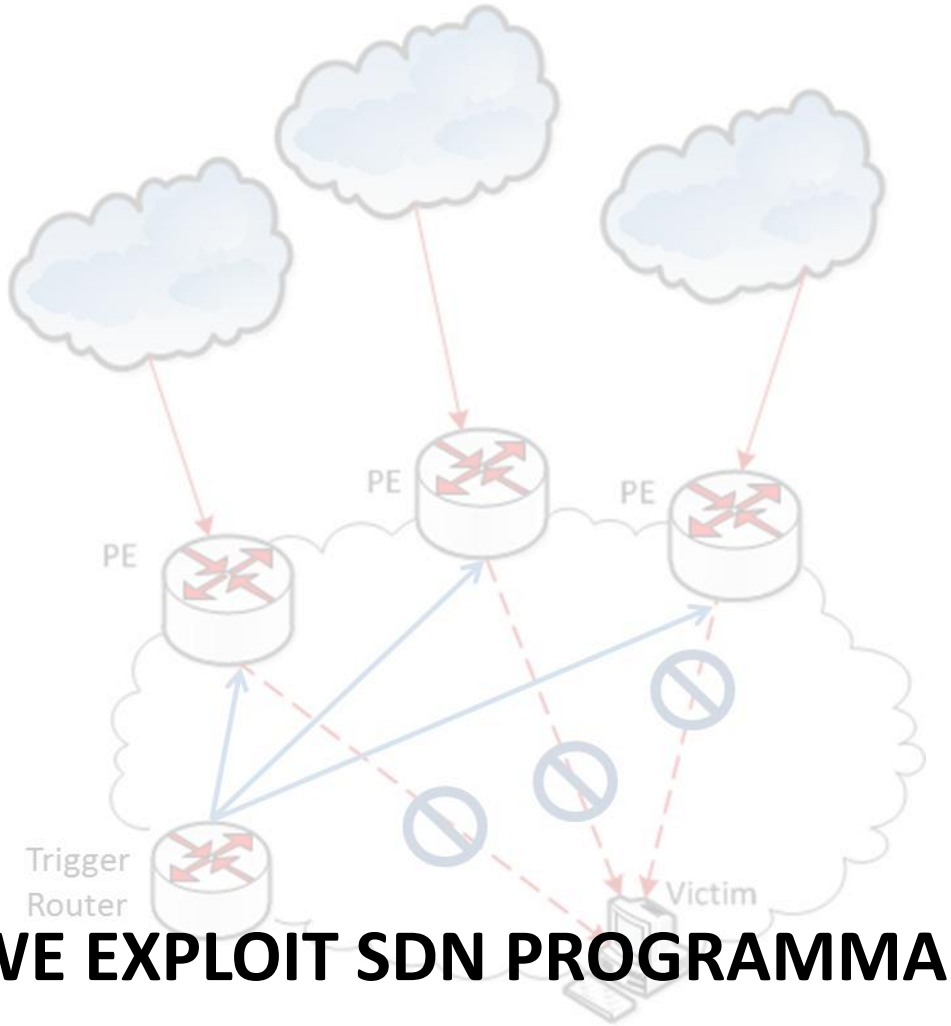
- ✓ Malicious traffic going to the Victim is dropped
- ✓ Prevent the waste of valuable resources, such as uplink bandwidth



- x Benign traffic is dropped as well
- x "Drop" is the only option
- x Matching is based on Destination IP

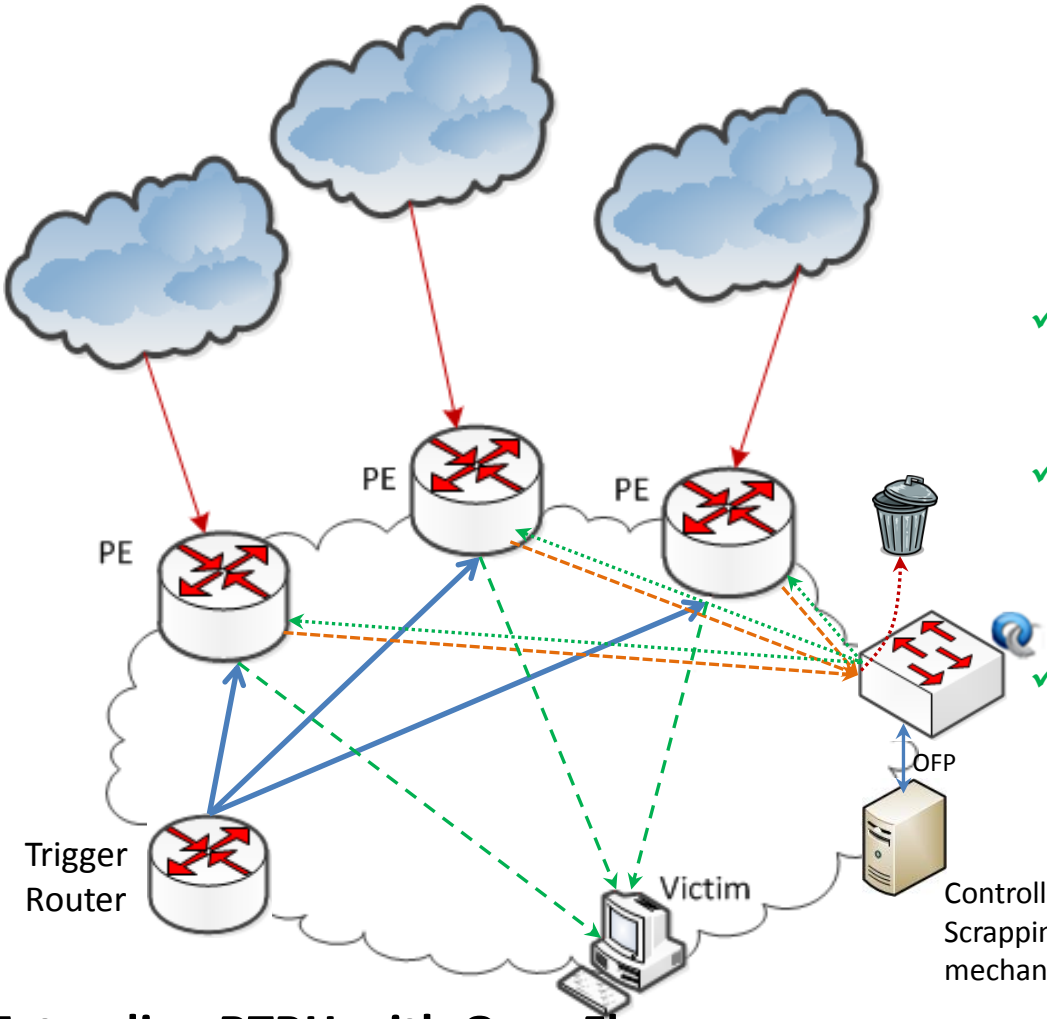
The RTBH Approach

Mitigate the attack and avoid collateral damage from malicious traffic



CAN WE EXPLOIT SDN PROGRAMMABILITY TO ACHIEVE BETTER MITIGATION RESULTS?

- ✓ Malicious traffic going to the Victim is dropped
- ✓ Prevent the waste of valuable resources, such as uplink bandwidth



- ✓ Matching traffic on a per-flow basis
- ✓ Benign Traffic is forwarded towards the Victim
- ✓ Preserve normal operation and reachability of the Victim

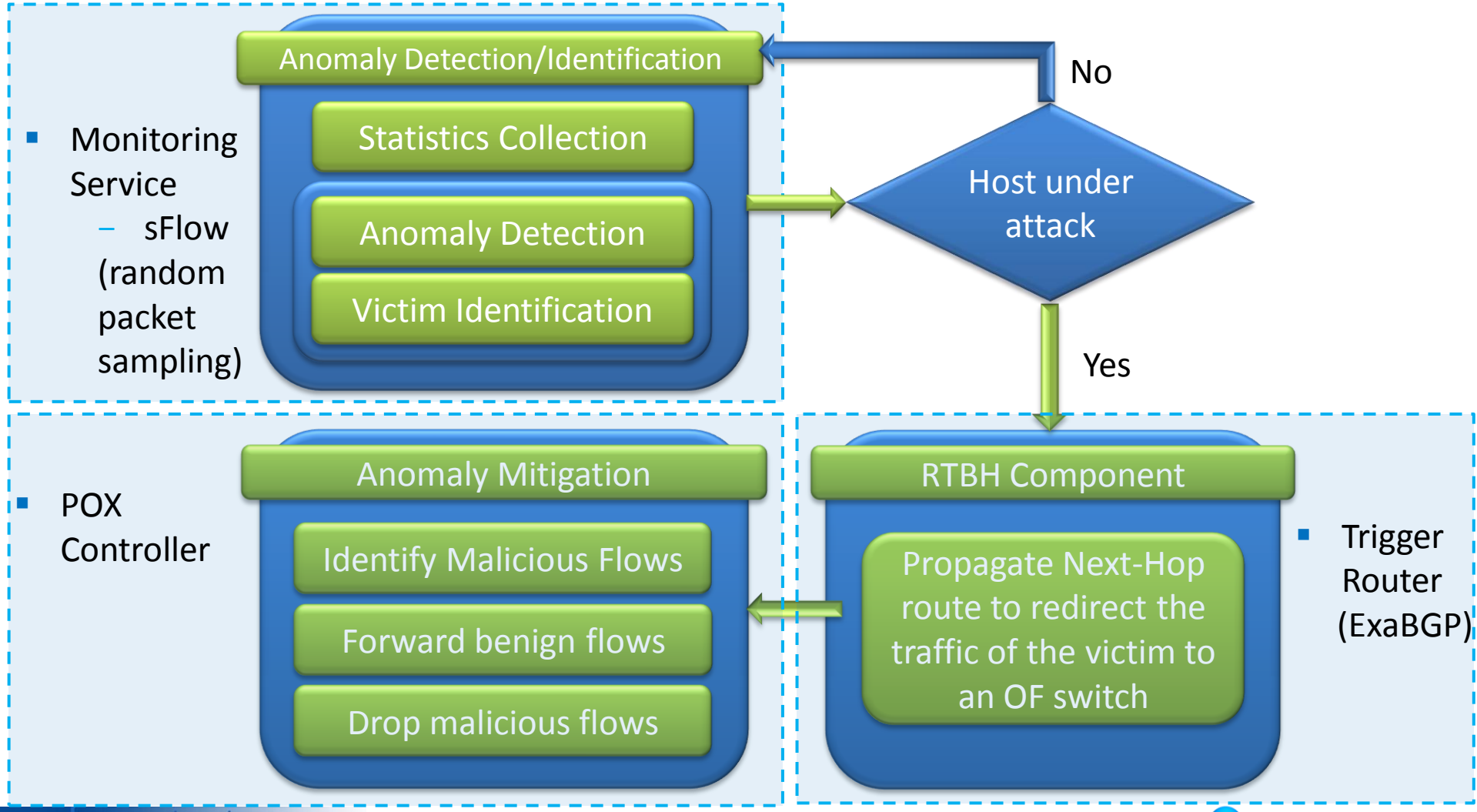
Extending RTBH with OpenFlow

- Victim's traffic is redirected to an OF switch
- Controller identifies malicious flows
- The Controller instructs the switch to drop malicious flows
- Benign Traffic is forwarded back, through the inport of the OF switch

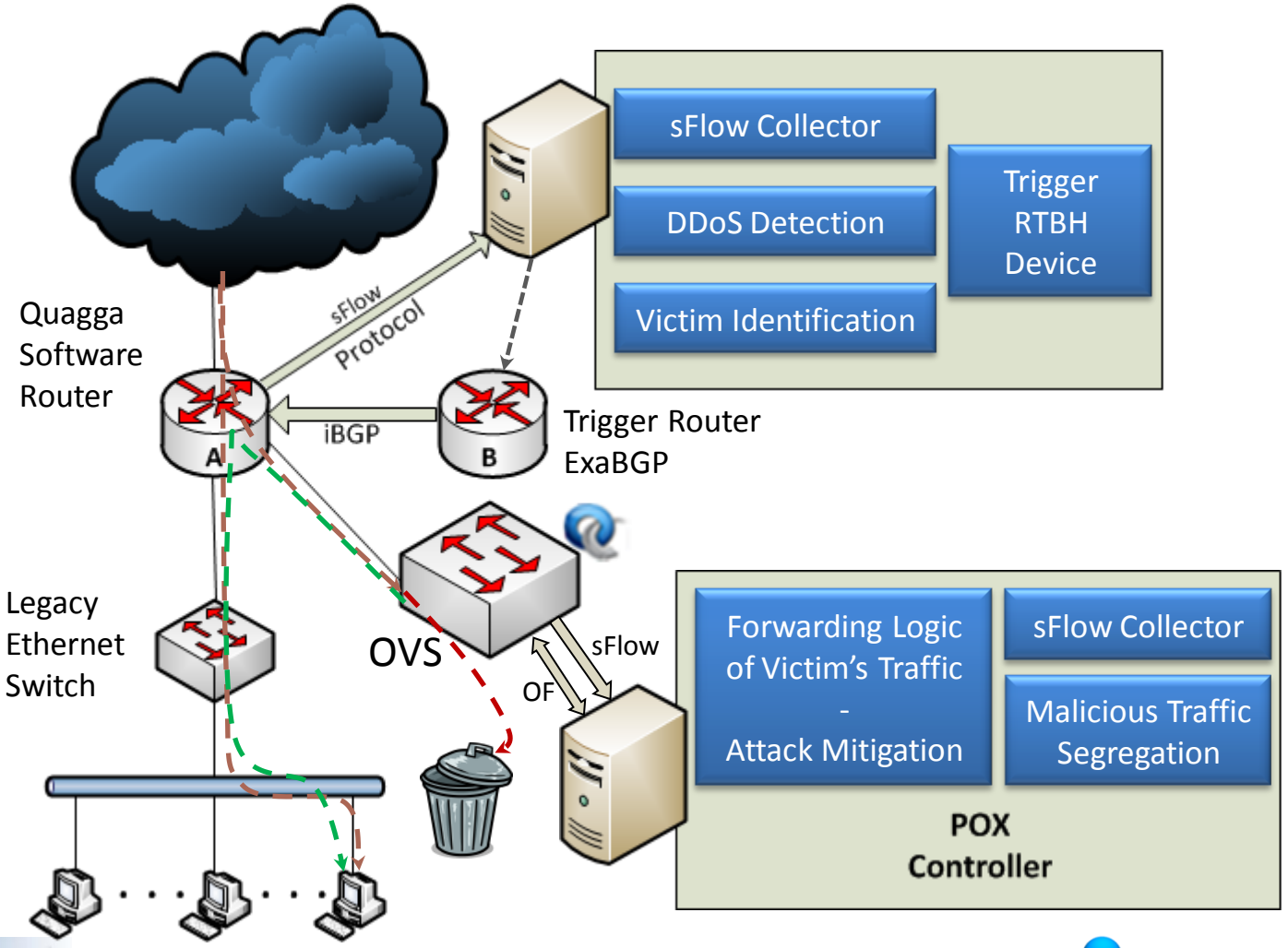
Key properties of the proposed approach

- Match offending traffic on a per-flow level
  - Benign packets are still delivered to the victim
- Modular architecture design
  - Decoupling of the required functions such as:
    - Data gathering
    - Anomaly Detection & Victim Identification
    - Attack Mitigation
- Automated Triggering of the RTBH device
  - Reduce administrative costs
- Packet sampling capabilities
  - Native OF statistics collection does not scale
  - High-end equipment is avoided

A **modular** architecture approach

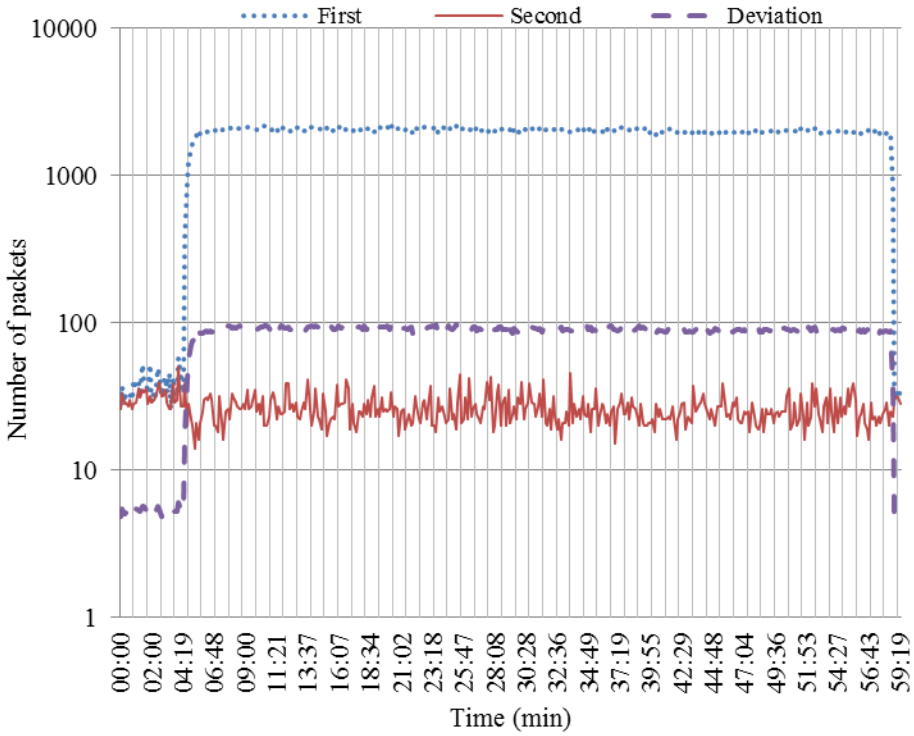


Experimental Setup



DDoS Detection & Victim Identification

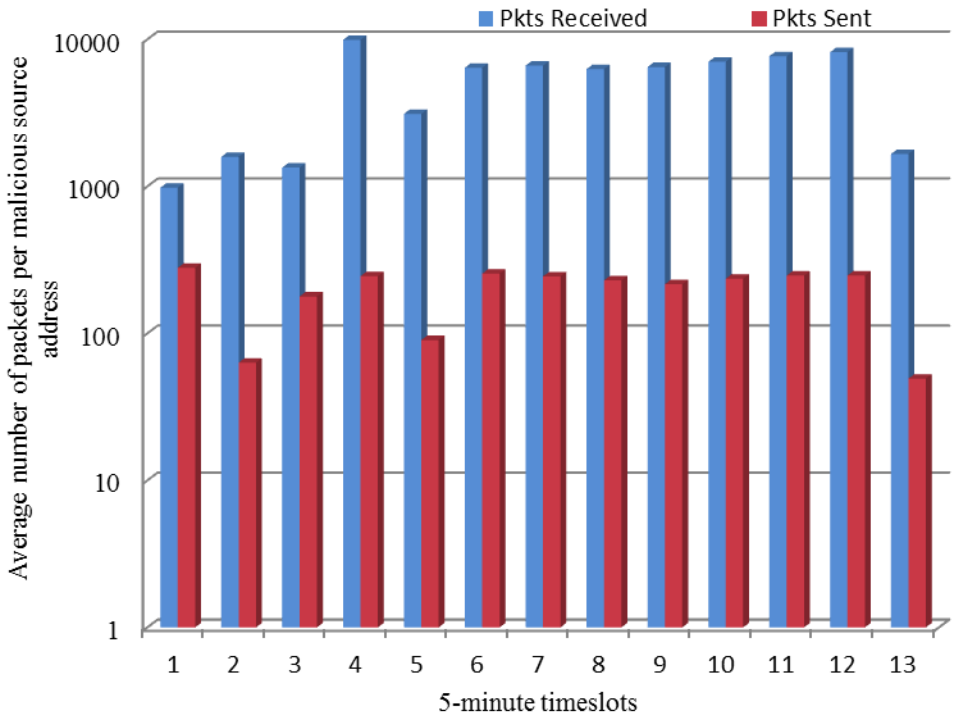
- Fine-grained DDoS Detection
  - Bidirectional count sketch algorithm
    - Efficiently store a summary of large data
    - Count sFlow samples based on Dst IP
- Victim Identification
  - Locate top Dst IP addresses with highly asymmetric communication pattern
  - Eliminate IP addresses that do not surpass a specific threshold



- Evaluation based on real traffic data
  - Captured DDoS attack
    - CAIDA DDoS Attack 2007 Dataset
  - Benign traffic captured from NTUA

Malicious Traffic Segregation

- Packet symmetry metric employed as proof of concept
  - you can choose your own algorithm
- For TCP connections: $1 \leq {}^{recv}/_{sent} \leq 4.5$
- For UDP traffic: similar approach, but site-dependent



We know the victim, we know the bad flows.. Now what ?

- OpenFlow offers Network Programmability
  - Control flows that were redirected to the OF switch
  - Malicious flows are dropped
  - Benign flows are forwarded back through the inport (OFPP_IN_PORT OpenFlow action)

	L1	L2			L3			L4		ACTION	PRIORITY
	In port	ETHER			IP			Port		Out Port	
		src	dst	type	src	dst	Prot	src	dst		
B	X	*	*	*	*	*	*	*	*	0xfff8	10
M	X	*	*	0x 0800	S	D	0x06	*	*	-	100

Does it scale? Still more to do..

- DDoS attacks involve thousands of malicious flows
  - Experiment with Hardware OF switches that use expensive TCAMs
  - Investigate a Longest Common Prefix approach to aggregate bad flows
- Deploy a multilevel Anomaly Detection method
  - We do not need detailed flow inspection all the time

Thank you !

Kostas Giotis

coyiotis@netmode.ntua.gr