Jaqen: A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches

Alan Zaoxing Liu

Joint work with Hun Namkung, Georgios Nikolaidis, Jeongkeun Lee, Changhoon Kim, Xin Jin, Vladimir Braverman, Minlan Yu, Vyas Sekar

BOSTON UNIVERSITY

intel

JOHNS HOPKINS UNIVERSITY

VE RI TAS HARVARD

Carnegie Mellon University

DDoS attacks are getting worse

- Increasing in *volume*
- Increasing in *diversity*
- Increasing in *cost to defend the attacks*

Surge in DDoS attacks targeting education and academic sector

9/15/2020 Infosecurity

CISA Warns of Increased DDoS Attacks

Security Experts Say Remote Workforce, Online Learning Create Opportunities

9/10/2020 U.S. CISA

DDoS Attacks Increase by 151% in First Half of 2020

9/16/2020 Neustar

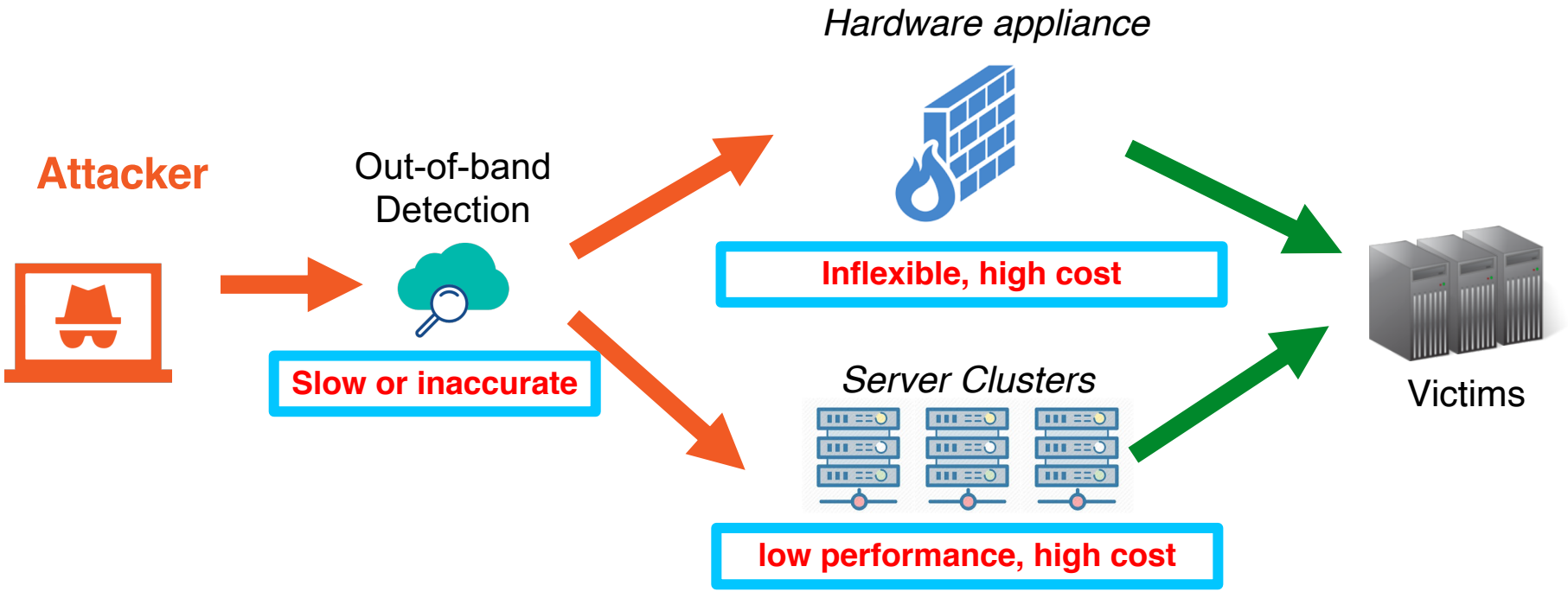
European ISPs report mysterious wave of DDoS attacks

9/3/2020 ZDNet

Requirements for DDoS Defense

- Performance:
  handle *large volumes* with *low latency*
- Flexibility:
  handle *diverse attack vectors*
- Cost-effectiveness:
  handle attacks with *low capital and operational costs*

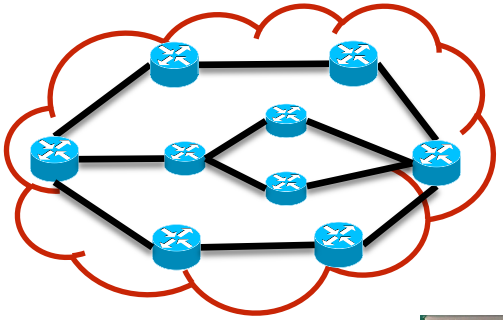
Current DDoS Solutions: Middleboxes



E.g., 100 servers for 1000Gbps mitigation. [Security'15]

Can we do better?

Trend: Network devices are more programmable



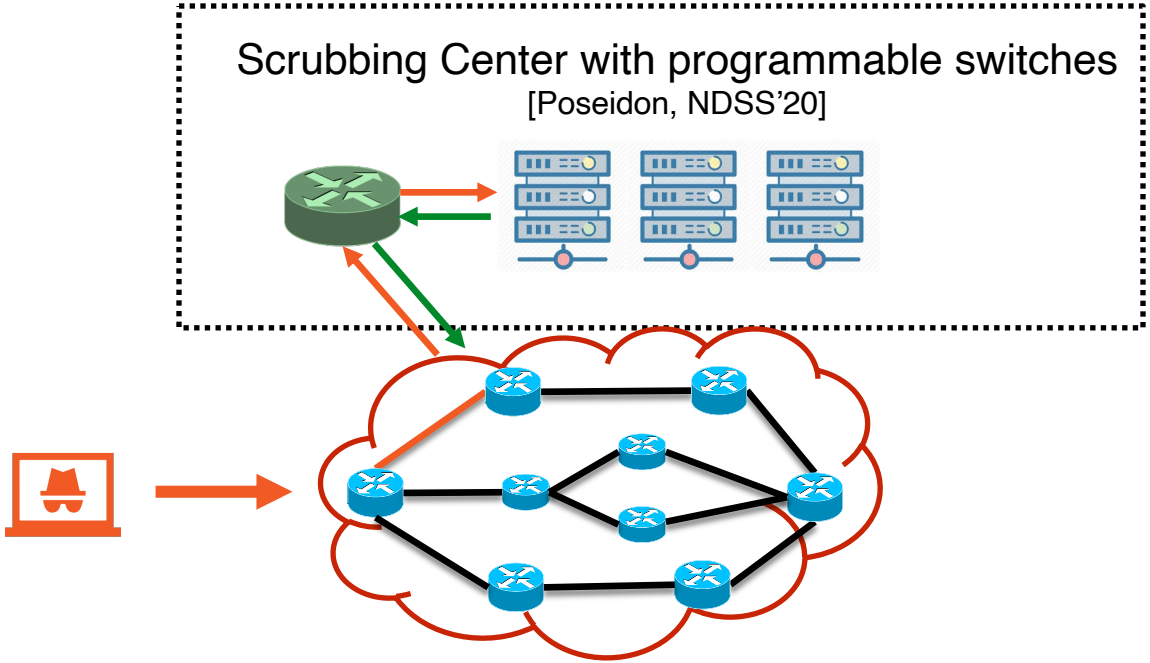
Increasing in-network *programmability* in ISP networks

Programmable Switch

Switch ASICs

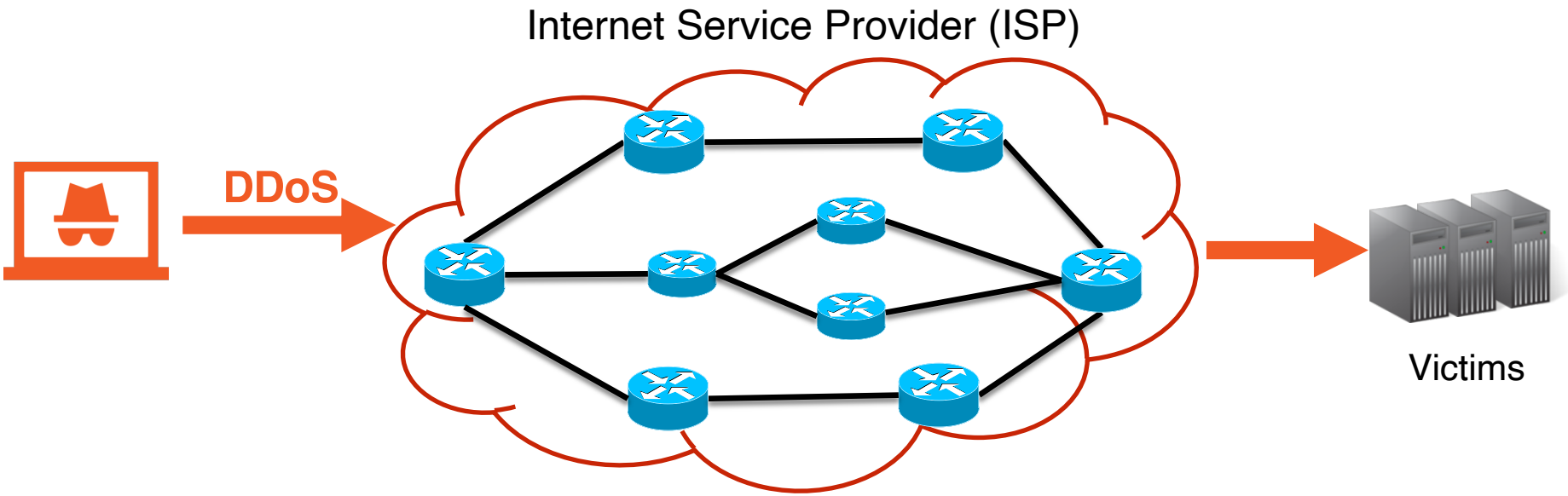
- High line-rate performance (e.g., Tbps)
- High programmability using high-level language (e.g., P4)
- Cost effective with similar cost as traditional switches

Current DDoS Solutions: Switches for Scrabbing



- Still need out-of-band detection.
- Scrubbing approach adds large latency.
- Unscalable mitigation functions (e.g., Server-like SYN Proxy)

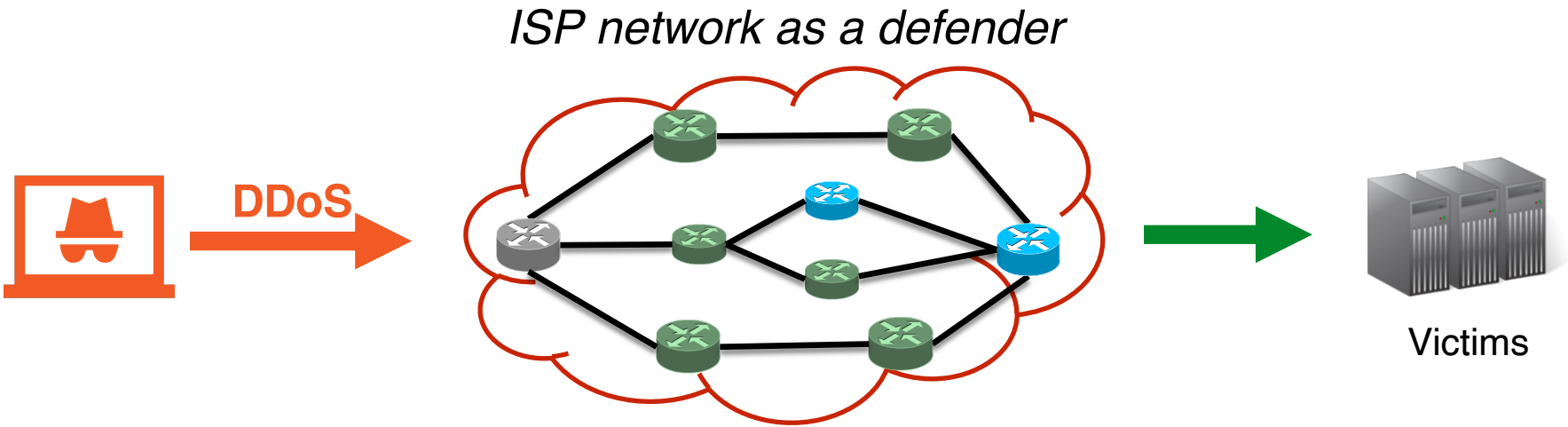
Opportunity: Programmable ISP Networks for DDoS Defense



- Near the source or victim of the attacks
- Provide defense-as-a-service to the clients

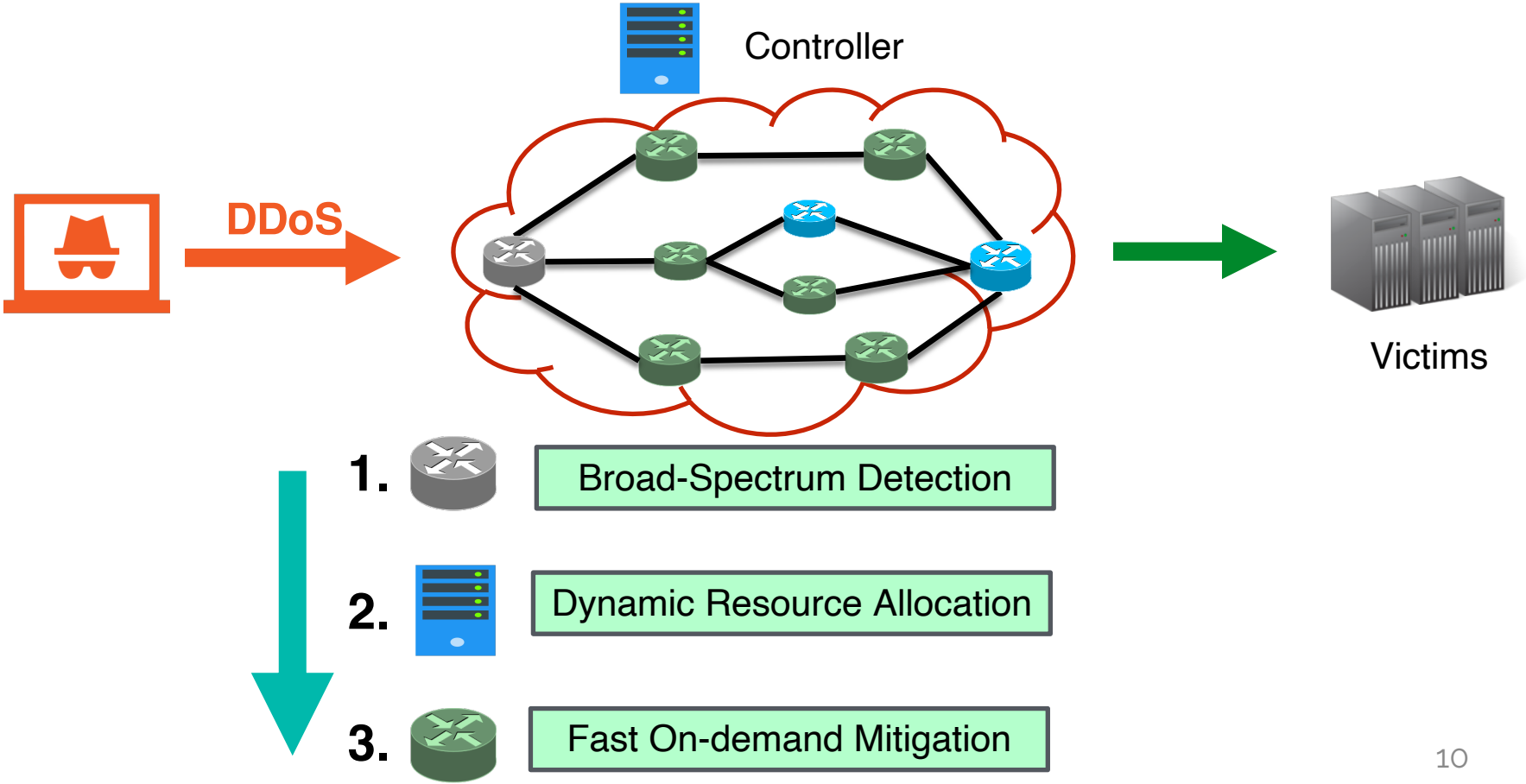
Can we design ISP-based DDoS defense that fully leverages programmable switches?

Jaqen: Switch-Native DDoS Defense for ISP

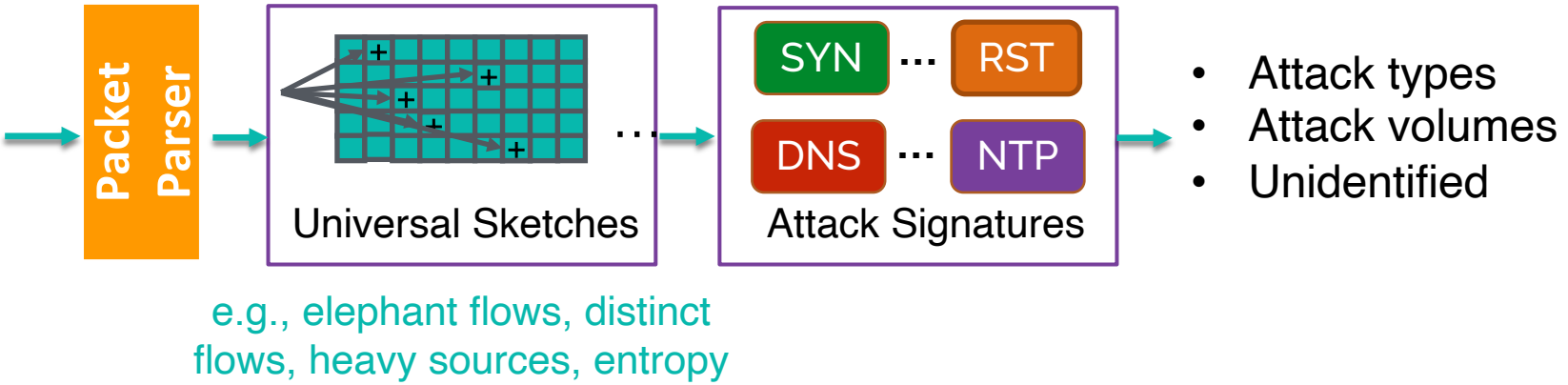


- Detection + Mitigation integrated “switch-native” solution.
- Designed for ISP networks where there are a LOT of switches.

Jaqen's Full Stack Design

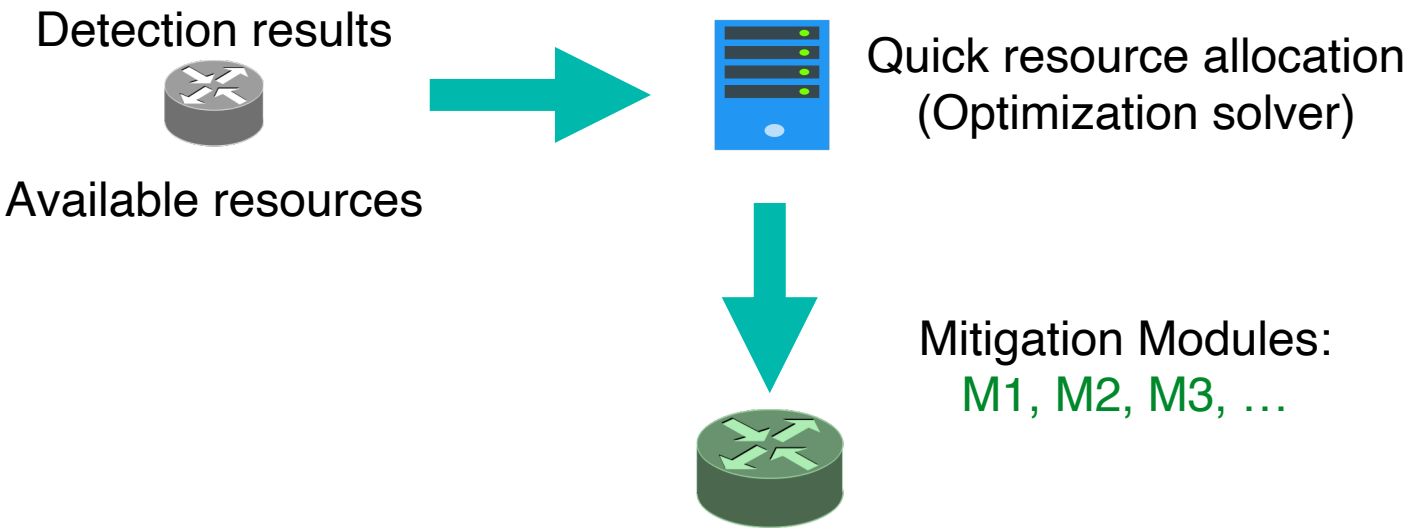


Broad-Spectrum and Always-On Detection



- A wide-spectrum detection of volumetric attacks.
- Compact design with future-proof universal sketches.
- Detection metric API: Query (proto, func, mode, freq)

Fast On-Demand Mitigation



- Cannot afford preloading all possible mitigation modules.

Switch-Optimized Mitigation Library

SYN Cookie/proxy
[BSDC'02, RFC4987]
Block-List [WDFIA'07]
Allow-List [WDFIA'07]
ICMP block
DNS filter
…

Sketches
Bloom filters
Counting bloom filters
SYN Proxy with filters
Exact-match table
Rater limiter
…

Mitigation API
RateLimit(identity,rate)
ExactBlockList(identity,size)
ExactAllowList(identity,size)
ApproxBlockList(identity,config)
ApproxAllowList(identity,config)
ActionAndTest(action,List(predicate))
HeaderHashAndTest(identity,action)
UnmatchAndAction(action,List(predicate))
KVStore(key,value,size)
ReportCtr(identity,type)
Recirculate(identity,type)

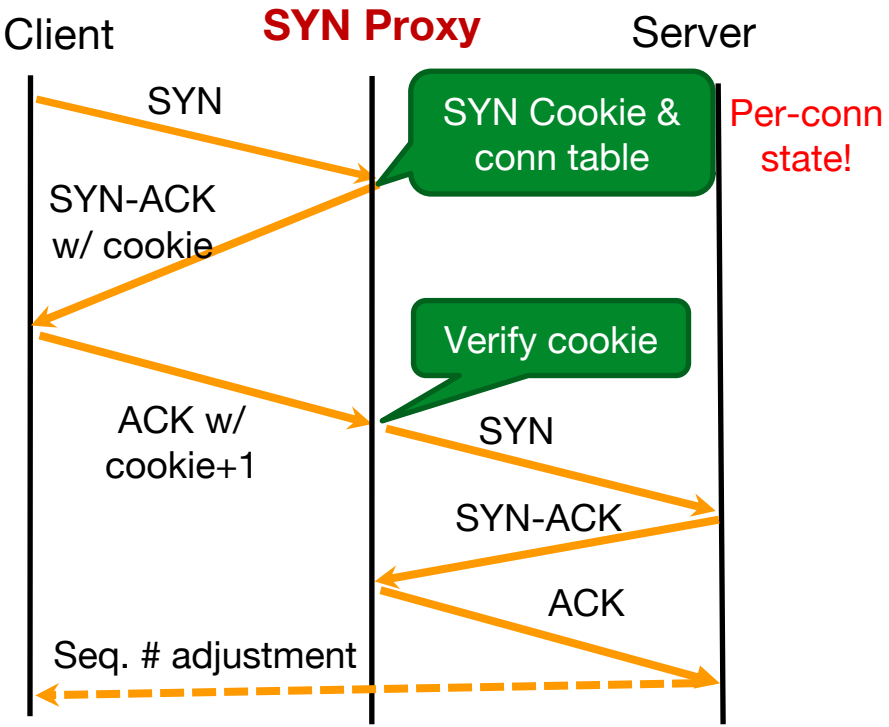
Best-practice mitigation

Switch-optimized library

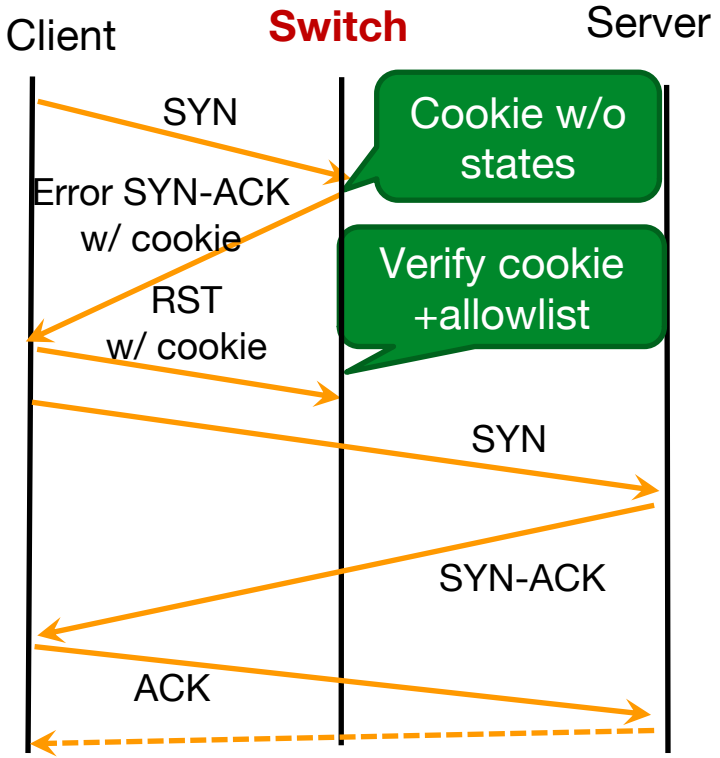
Mitigation API

- Preserve O(10 Million) legitimate connections with O(10 MB) on-switch memory.
- Support mitigation strategies on 21 attacks.

Switch-Native SYN Proxy



SYN Proxy [NDSS'20]



Jaqen SYN Proxy

Evaluation – Single Attack

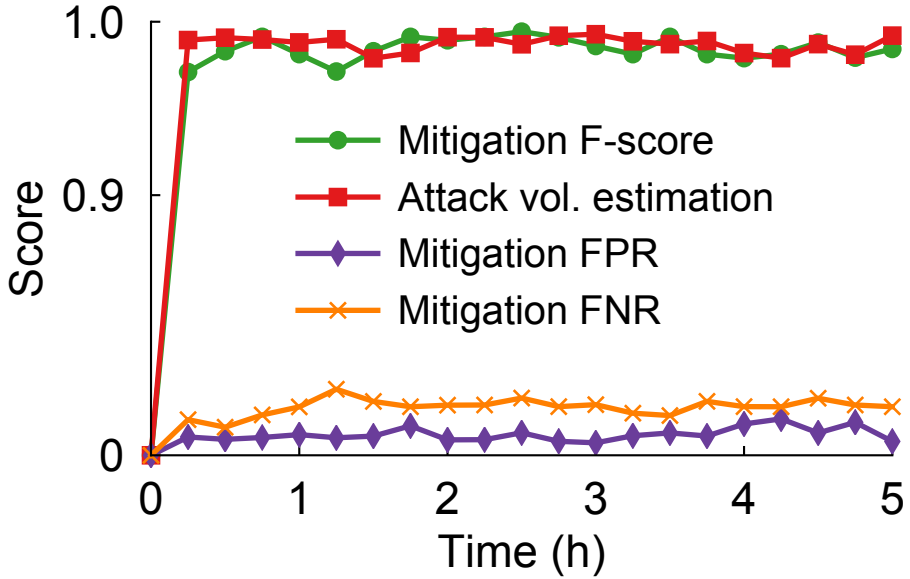
- Comparison with Poseidon [NDSS'20].
- Single Intel Tofino switch.
- 40Gbps attack traffic with 2M legitimate TCP connections.

Defense (40G)	Poseidon (FPR / FNR)	Jaqen (FPR / FNR)
SYN proxy	2M, 25.2% / 1.3%	2M, 0.0% / 1.3%
DNS/NTP defense	2M, 1.2% / 3.7%	2M, 0.7% / 3.1%

- Mitigation with probabilistic data structures is more scalable.

Evaluation – Dynamic Attacks

- 6 volumetric attacks (SYN, ICMP, UDP, DNS, NTP, Memcached)
- 380Gbps total volume, 3.2 Tbps Intel Tofino switch



High detection accuracy and high mitigation effectiveness

Conclusions

- ISP DDoS defense compromises performance, flexibility and cost-effectiveness.

- Appealing programmable network devices (e.g., programmable switches)
  * High line-rate packet processing
  * Full packet programmability with low cost

- Jaqen: Switch-native DDoS defense for ISP networks
  * Broad-spectrum detection integrated with on-demand mitigation
  * Network-wide resource management
  * Switch-optimized library for best practice mitigation

Contact: Alan Liu
zaoxing@bu.edu
http://zaoxing.github.io/