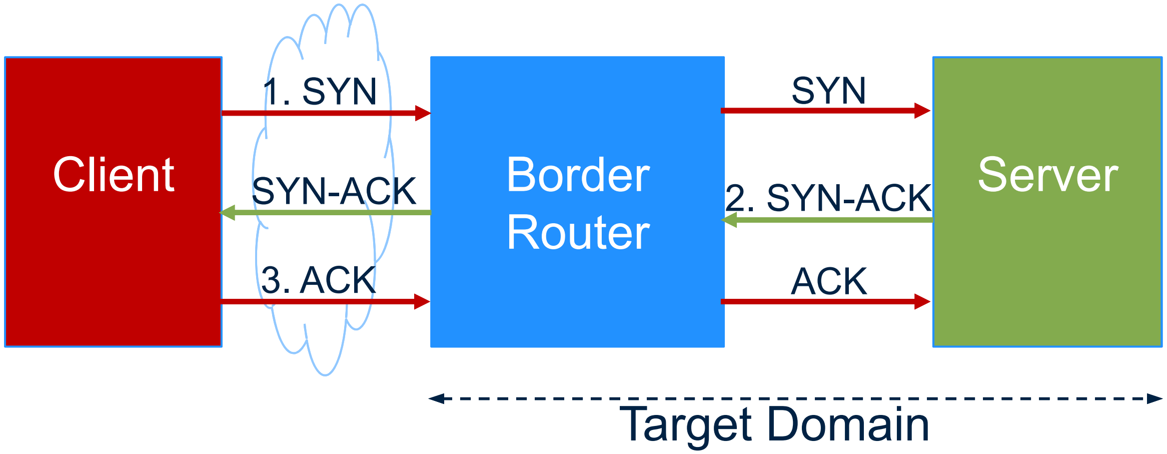
Analyzing the Vulnerabilities Introduced by DDoS Mitigation Techniques for SDNs

Rajendra V. Boppana 📢
Rajasekhar Chaganti
Vasudha Vedula

Department of Computer Science
University of Texas at San Antonio

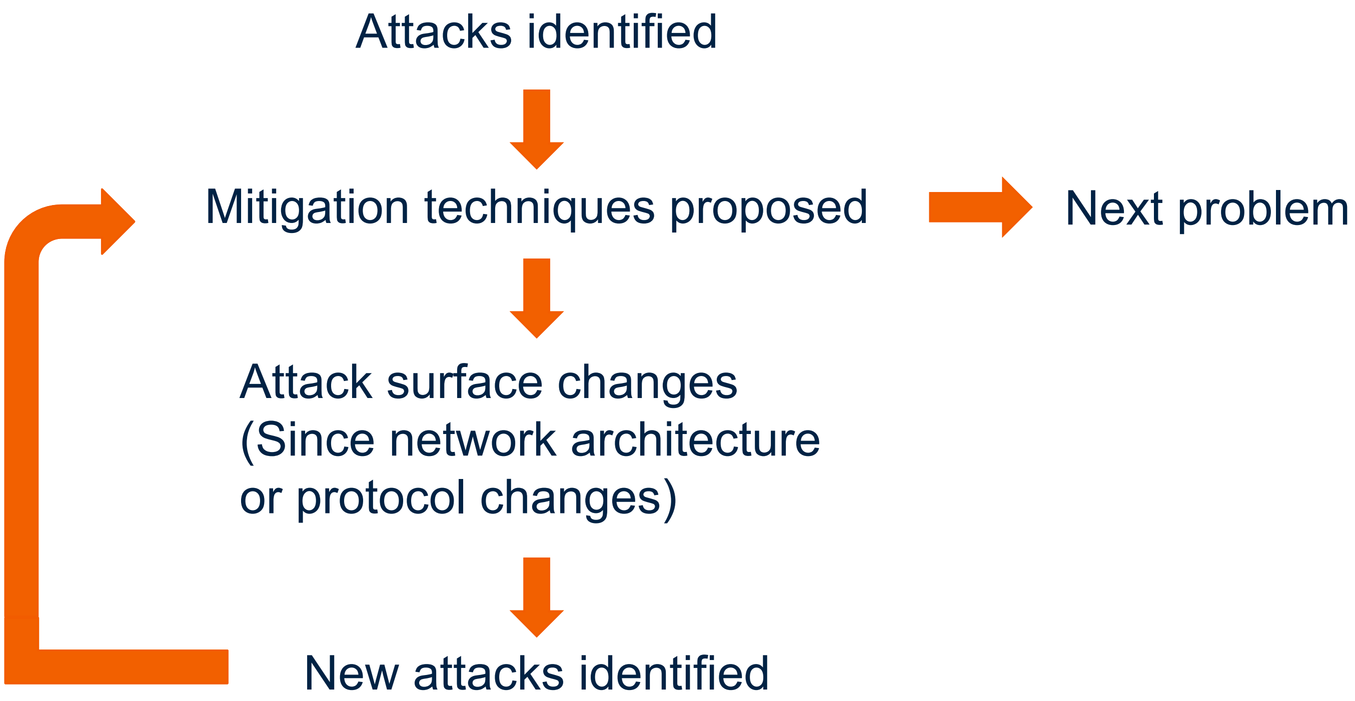
TCP SYN Flooding Attack

- TCP sets up a bidirectional, reliable connection between client and server prior to data exchange



- Denial of Service (DoS) Attack: send SYN packets and ignore server responses

Circle of Network Security



Attacks identified

Mitigation techniques proposed

Next problem

Attack surface changes
(Since network architecture
or protocol changes)

New attacks identified

Our Focus

- How do you analyze the new vulnerabilities introduced by mitigation techniques?
- Is there a checklist to identify the new vulnerabilities?
- How do you minimize new vulnerabilities?

Commonly Exploited Vulnerabilities and Limitations

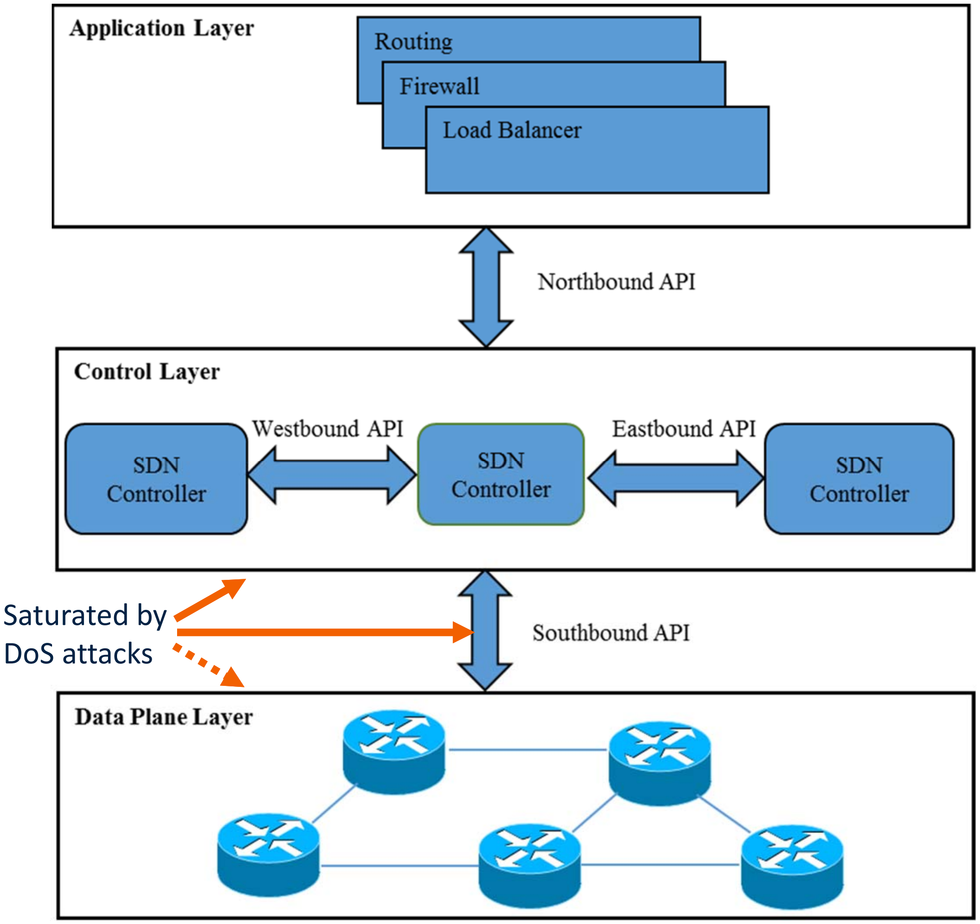
- Inherent in design/architecture/modification
- High memory/processing requirements
- Disproportionately large responses
- Accepting data/packets without verifying

Commonly Exploited Vulnerabilities and Limitations

- Using simplistic indicators to handle packets
- Blacklists
- Whitelists
- Responses that reveal configuration/security posture

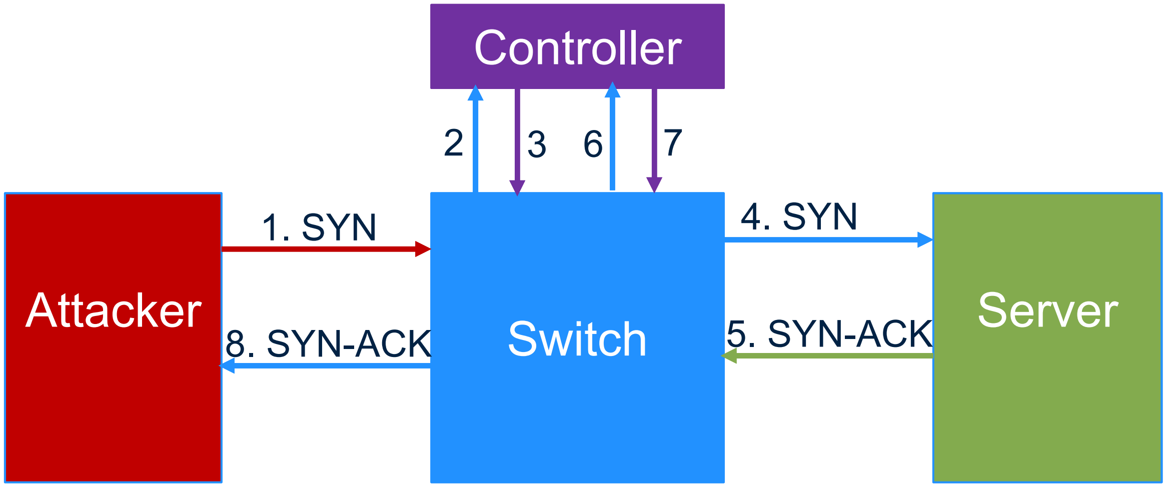
Software Defined Networking (SDN)

- Decouples the control and data planes of switches, routers
  - Centralized control
  - Better network management
  - Better security
  - Widely used in data center networks
- Introduces new vulnerabilities



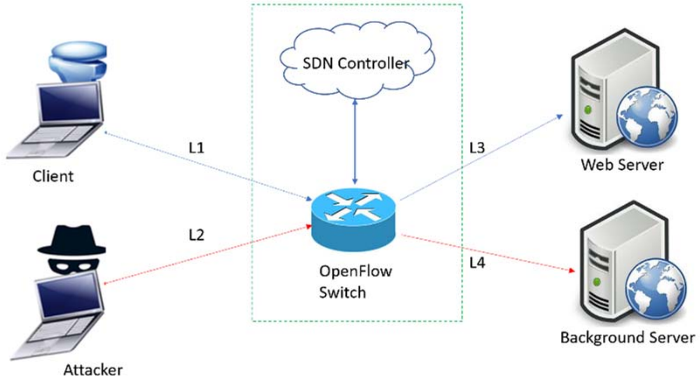
DoS Attacks on SDNs

- TCP SYN flooding attack
  - Attacker sends TCP SYN requests, but does not compete TCP connection setup
  - Four messages exchanged between data plane and controller; packet processing by the controller

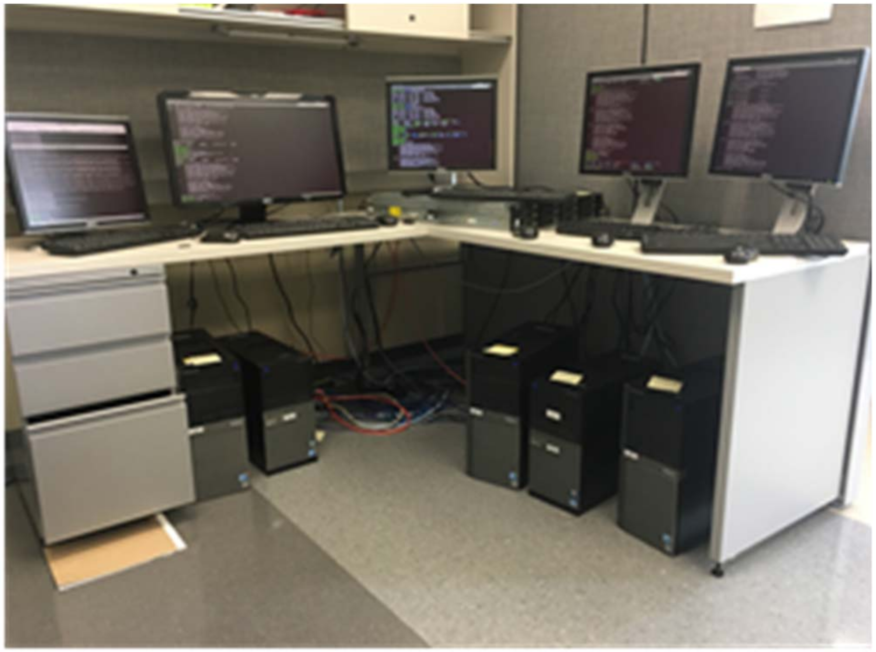


Experimental Setup

- The experimental setup consist of one Client, one Attacker, two HTTP Servers, Pox Controller and the modified Openflow Reference Switch, v1.0



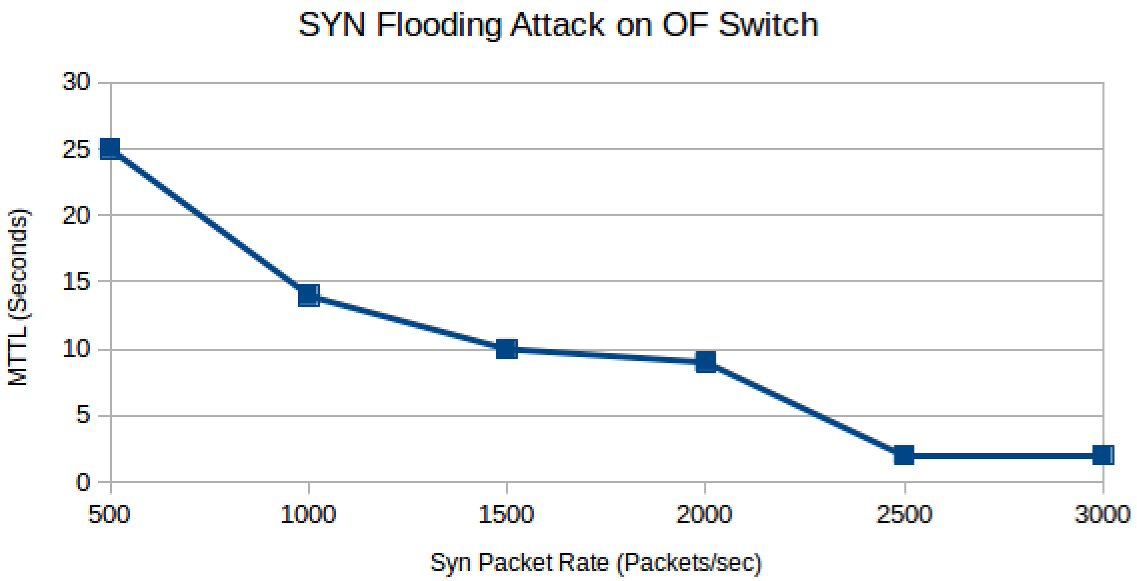
Experimental Setup (block diagram)



The 5-node Cluster used for experiments

Attack Tools
Hping3 (Syn flooding),
Bonesi (Syn flooding with spoofed IP addresses, Connection Flooding)

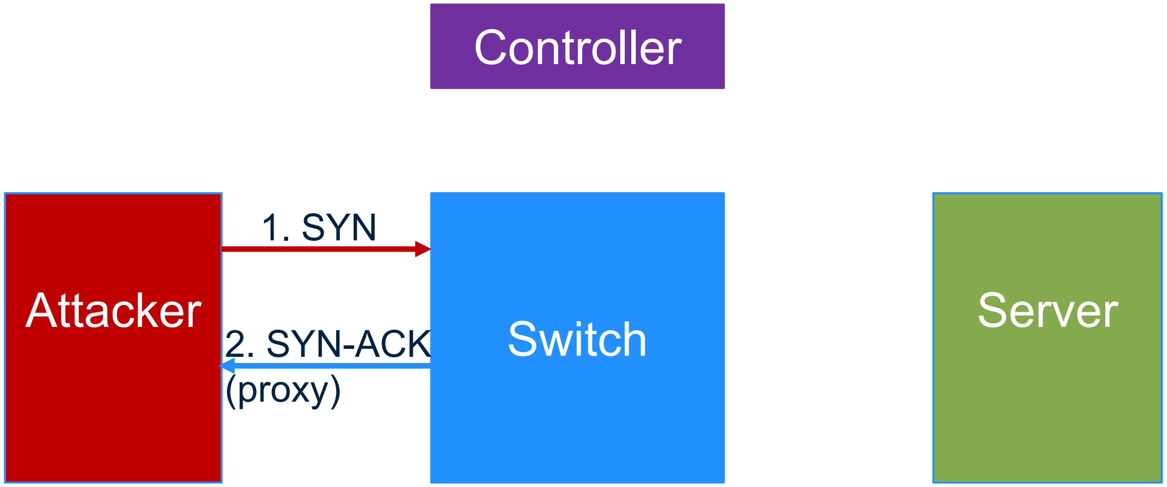
Impact of SYN Flooding Attack on SDNs



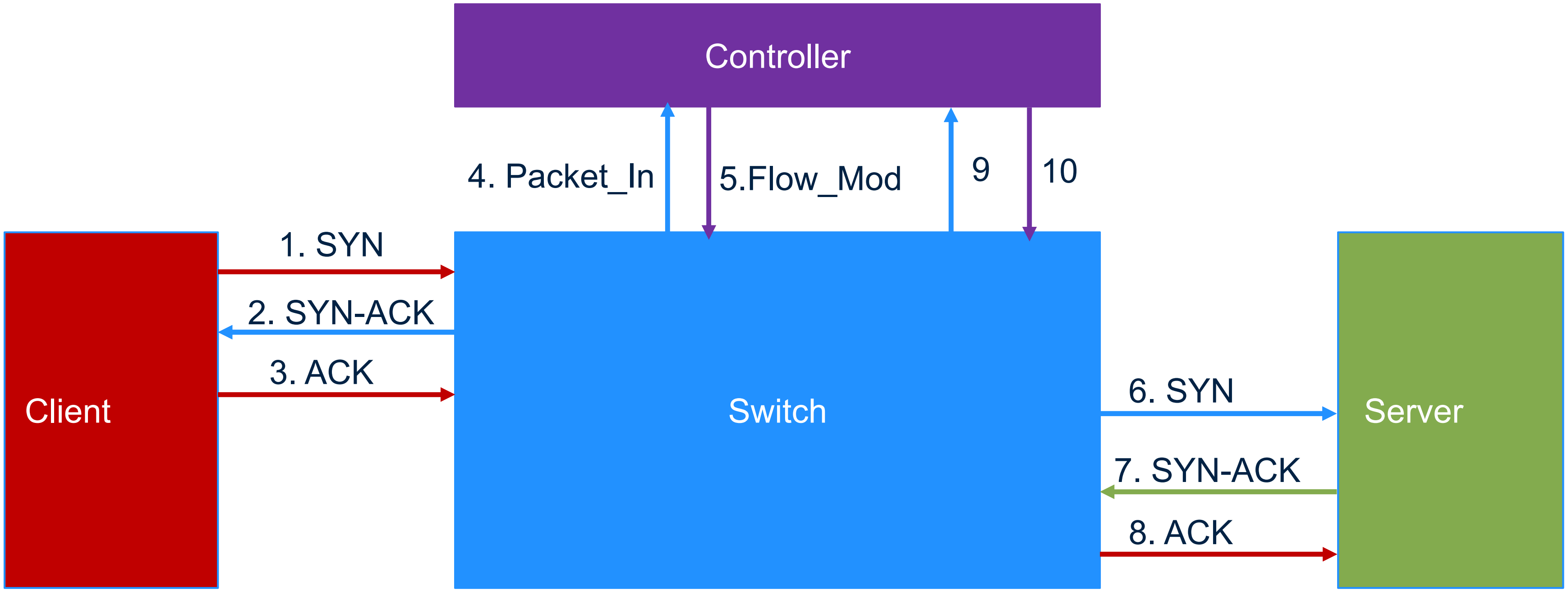
- Client downloads a 1 KB file from server back to back.
- Attack starts 30 seconds after the client starts.
- Experiment duration is 120 seconds
- Each data point is an average of 16 runs

SYN Proxy to Mitigate DDoS Attacks

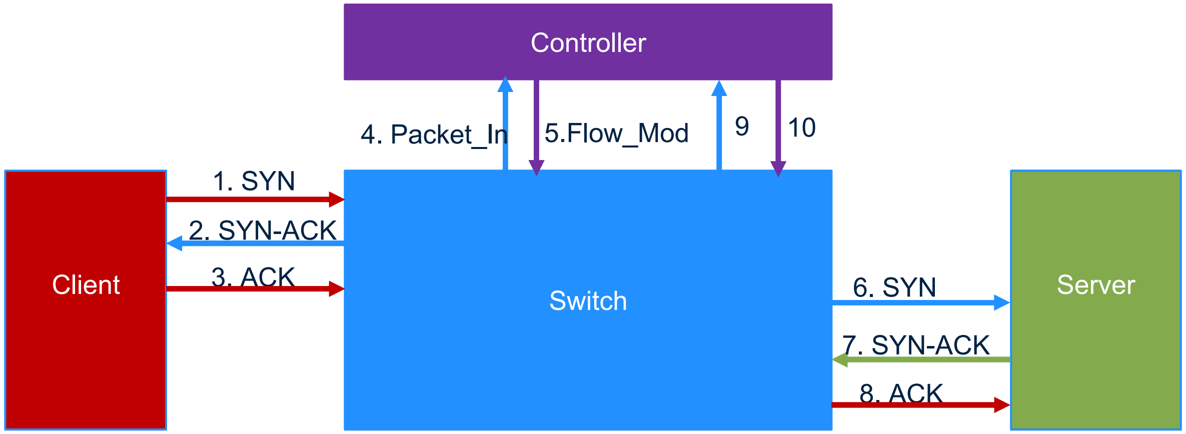
- Split TCP connection into two separate connections
  - Originally developed to make servers resilient to SYN floods
    - Avant-Guard (CCS, 2013)
    - LineSwitch (IEEE ToN, 2016)
    - Cisco and Juniper routers



Connection Migration



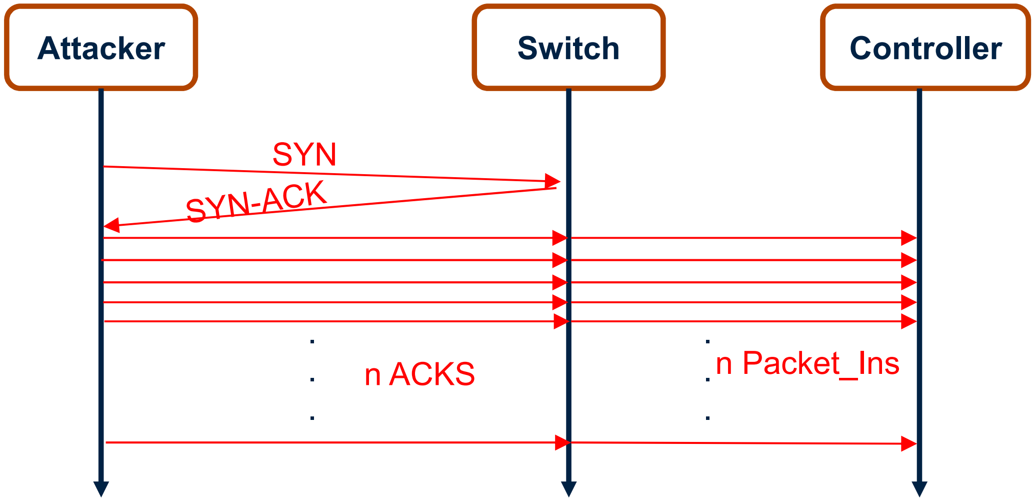
Connection Migration Vulnerabilities



Vulnerability List
Design/architecture
Memory/processing
Large responses
Not verifying data/packets
Simplistic indicators
Blacklists
Whitelists
Revealing configuration

- Switch translates packets headers between the connections
  - Header translation buffer can be saturated
- ACK triggers switch/controller processing
  - Attacker needs to send ACKs to make SYN floods work
  - **Ack flooding attacks**

ACK Flooding Attack


Attacker

Switch

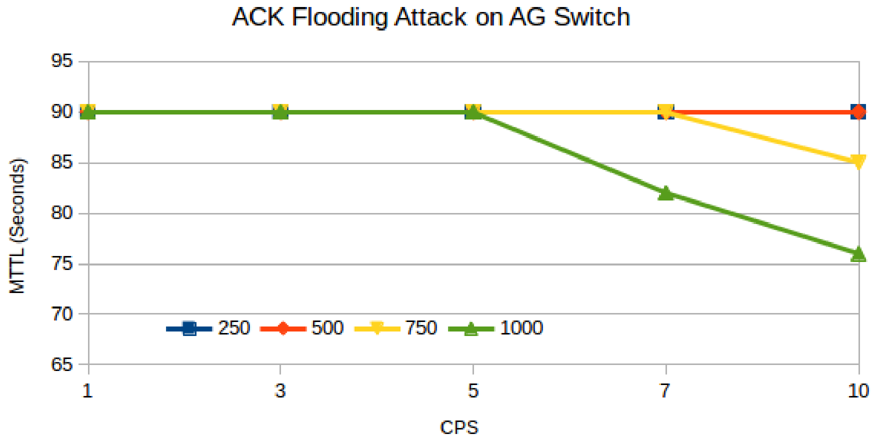
Controller

SYN

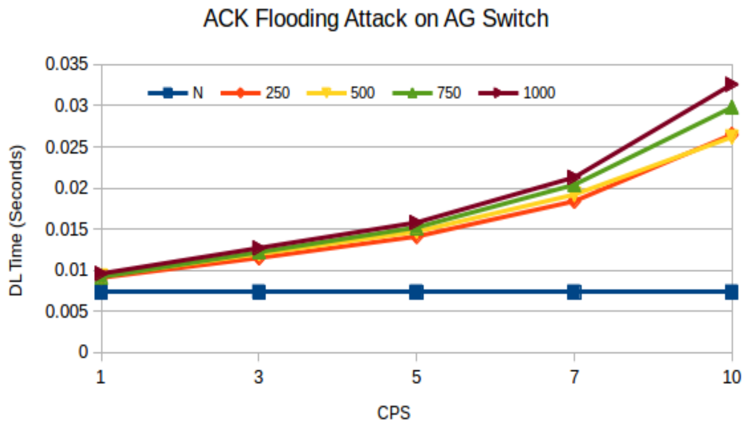
SYN-ACK

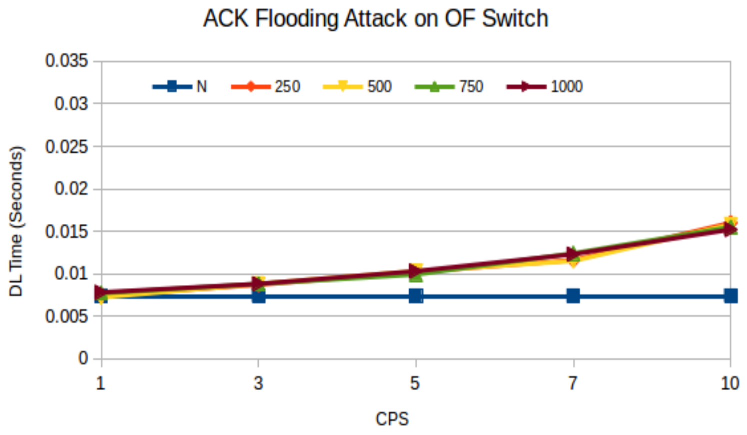
n ACKS

n Packet_Ins



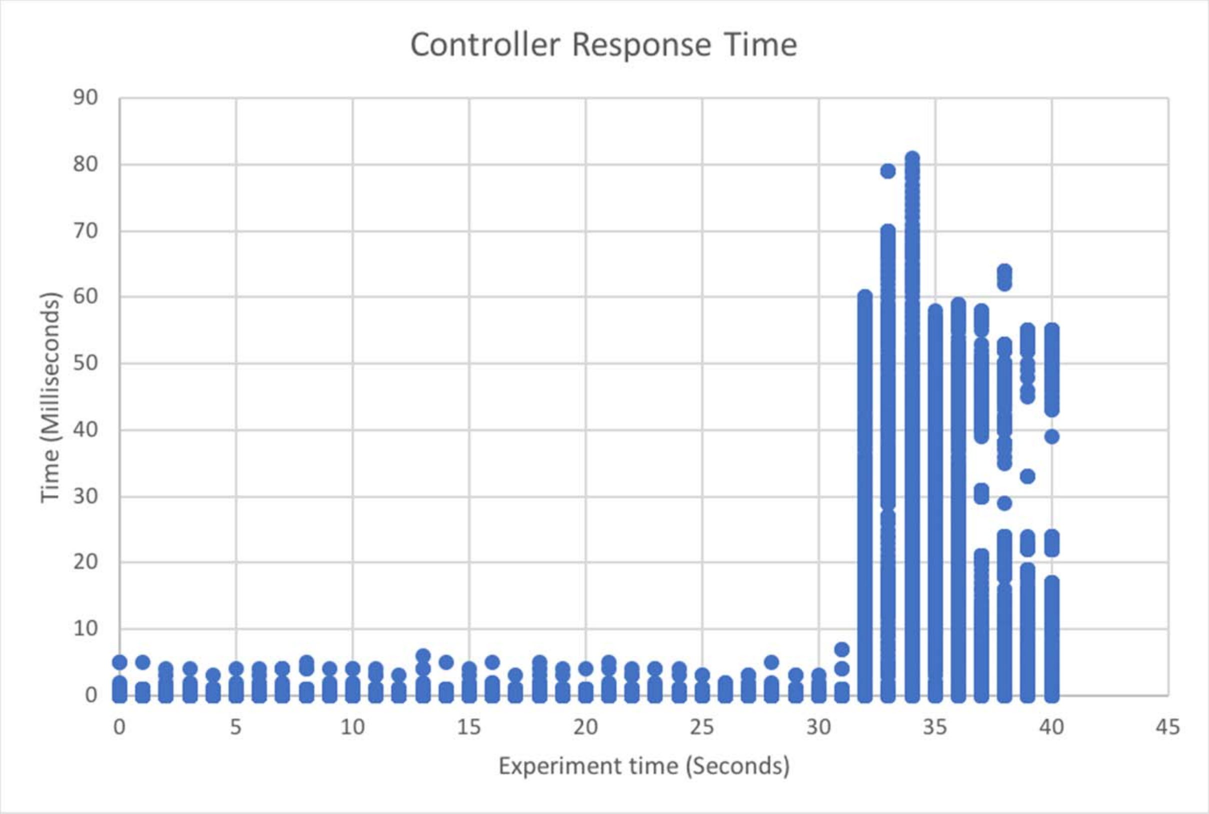
Server Response Time





- AG: SDN with AG SYN Proxy implemented
- OF: unmodified SDN switch
- DL: client’s time to download a file from server

Controller Response Time



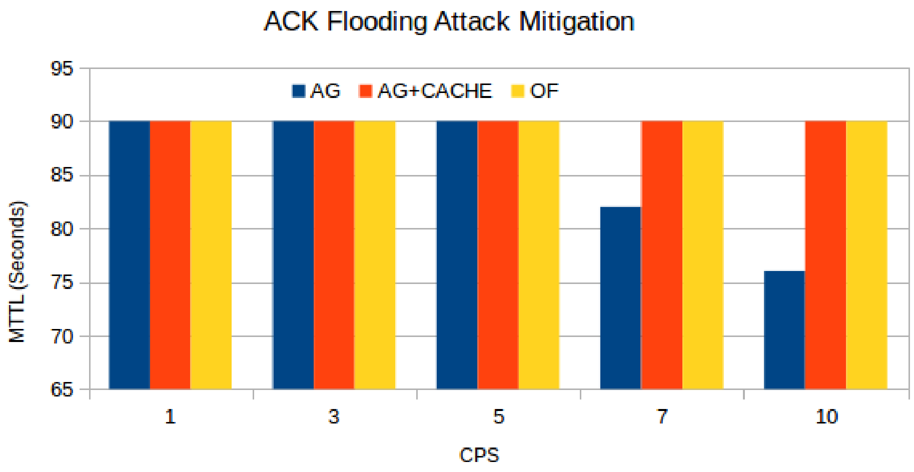
Attack rate: 500 ACKs/s (5 SYNs/s, 100 ACKs/SYN-ACK)

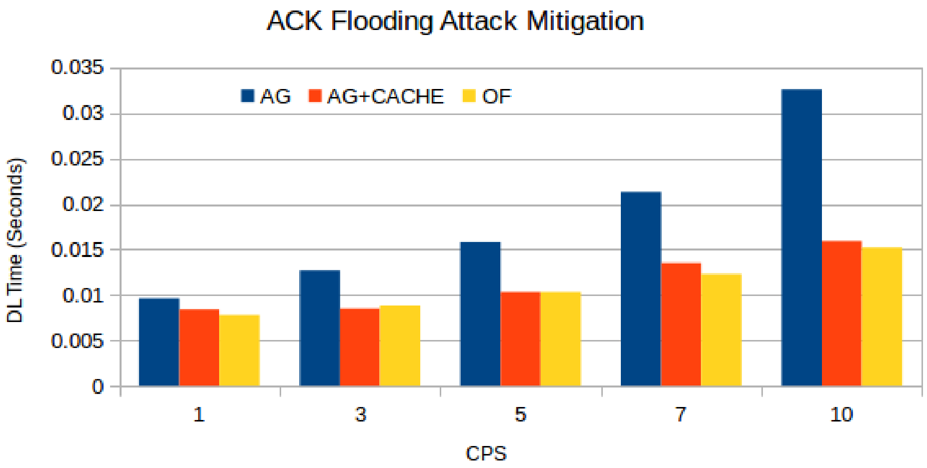
Attack starts after 30 seconds

ACK Cache

- Switch keeps track of received ACKs without flow entries
- ACK A with ‘a’ in its acknowledgment field is received; let s = a-1
- If s is found in the ACK cache, A is dropped
- Otherwise, s is verified to be a possible SYN cookie used in a recent SYN proxy by the switch
  - If the verification is successful, s is recorded in ACK cache, controller is requested for a flow entry
  - If the verification is not successful, A is handled using the default OF logic
- Even a 4 KB cache is sufficient

Effectiveness of ACK Cache





ACK Cache Vulnerabilities

- Blacklisting
  - SYN cookie is verified to modify the cache
- Simplistic indicators
- Memory/processing limitations
- False positives
  - Depend on the robustness of the cryptographic hash functions used for SYN cookie generation
- False negatives
  - Equivalent to conflict misses in a cache: two SYN cookies mapped to the same cache location

Vulnerability List

Design/architecture

Memory/processing

Large responses

Not verifying data/packets

Simplistic indicators

Blacklists

Whitelists

Revealing configuration

Conclusions and Further Work

- The vulnerability list is helpful in analyzing mitigation schemes and their vulnerabilities
- Evaluated the impact of ACK flooding on SDNs with SYN proxy
- Proposed a low-cost mitigation technique and analyzed its vulnerabilities
- Future work
  - Expand on the vulnerabilities list
  - Investigation vulnerabilities introduced by ML, entropy and statistical techniques
  - New solutions to TCP SYN flooding

Research is partially funded by National Security Agency through University of Arizona.