Fighting Fire with Light: Tackling Extreme Terabit DDoS Using Programmable Optics

Matt Hall
Grace Liu, Ram Durairajan, Vyas Sekar

{ mhall, ram } @ cs.uoregon.edu
{ guyuel, vsekar } @ andrew.cmu.edu
DDoS Attack Landscape is Changing

DDoS Attacks Hit Record 500 Gbps in 2015

Phil Muncaster
UK / EMEA News Reporter, Infosecurity Magazine

Email Phil
Follow @philmuncaster
DDoS Attack Landscape is Changing

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Mirai took advantage of insecure IoT devices in a simple but clever way. It scanned big blocks of the internet for open Telnet ports, then attempted to log in default passwords. In this way, it was able to amass a botnet army.
Amazon says it mitigated the largest DDoS attack ever recorded

An attack with a previously unseen volume of 2.3 Tbps

By Jon Porter | @JonPorty | Jun 18, 2020, 7:31am EDT

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Mirai took advantage of insecure IoT devices in a simple but clever way. It scanned big blocks of the internet for open Telnet ports, then attempted to log in default passwords. In this way, it was able to amass a botnet army.
Limitations with Current State-of-The-Art

- Static topologies
- Attack induced congestion
- Topology unaware defense
- No traffic isolation
- Costly scrubbing all traffic

Internet

Adaptive Reconnaissance
Access Denied
Adaptive Attacks
Our Goal

• Explore if DDoS defense system with programable optics can be beneficial and exciting to work on
• Illuminate two key benefits of such a system
  • Opportunistic reconfigurability
  • Physical separation of distinct traffic classes
• Present modeling results that quantify the performance benefit granted by programmable optics during a DDoS attack
An Untapped Resource

- Single-mode optical fiber underpins nearly all wide-area communications systems
- Reconfigurable Add/Drop Multiplexers enable the steering of individual wavelengths on a fiber rapidly
- Optical amplifier modeling efforts point to a rapidly reconfigurable backbone soon
What are Programmable Optics?

- Programmable optics enable bandwidth to be reallocated onto adjacent paths within a network through *transitions* between *network instances*
Opportunity 1

• Opportunistic Reconfigurability
Opportunity 1

• Opportunistic Reconfigurability
Opportunity 1

• Opportunistic Reconfigurability
Opportunity 1

• Opportunistic Reconfigurability
Opportunity 2

• Physical Separation
Opportunity 2

• Physical Separation
Opportunity 2

• Physical Separation
Opportunity 2

- Physical Separation
Optics-enabled In-Network defense for Extreme Terabit DDoS attacks

- Reconfigurable topologies
- Dynamic capacity
- Topology aware defenses
- Isolate and route benign traffic
- Scrubbing only suspicious traffic
- Adaptive Reconnaissance
- Adaptive Attacks

Internet
Performance limitation with Static Optics
Performance limitation with Static Optics

Throughput (Gbps)

Baseline  Scrubber

Attack Strength (Gbps)

Victim Server

Scrubber

Trusted

Suspicious
Performance gain with Programmable Optics
Performance gain with Programmable Optics
ONSET: The Road Ahead

• Demonstrate feasibility of ONSET against diverse DDoS attacks
  • Build an accurate modeling and simulation platform for ONSET
    • Model optical and electrical network components
    • Simulate fixed/variable rate attacks, volumetric, and protocol-conforming attacks
• Prototype ONSET
  • Demonstrate an ONSET system, characterized by optical switching time and performance guarantees for legitimate users during an attack
• ONSET for Advanced Cyber Attacks
  • Network reconnaissance is an ongoing threat
  • Transitioning network state between different optical layer connectivity graphs to thwart malicious reconnaissance campaigns
Questions