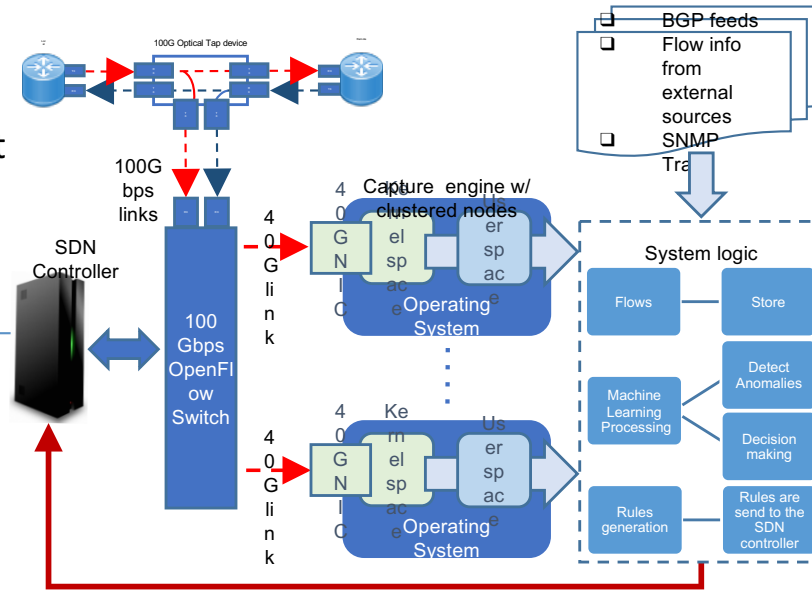# Quad Chart for: NetBrane: A Software-Defined DDoS Protection Platform for Internet Services

Challenge:

Build an effective, pro-active defense system for DDoS attacks at an Internet scale

Solution:

- High-speed capture (100Gbps and more)
- Traffic modeling using Machine Learning for low false positives and negatives, near real-time model fitting and classification
- Combination of network maps, BGP routing , vulnerable servers, etc, to proactively develop responses
- SDN technology for attack mitigation
- Hacker chatter capture, NLP processing, actionable alerts

100G Optical Tap device

100G bps links

SDN Controller

100 Gbps OpenFlow Switch

40G link

40G link

Capture engine w/ clustered nodes

Kernel space

User space

Operating System

BGP feeds
Flow info from external sources
SNMP Tra

System logic

Flows — Store

Machine Learning Processing — Detect Anomalies

Decision making

Rules generation — Rules are send to the SDN controller

What we need to TTP

- Access to operational traffic to develop accurate models
- Opportunities to deploy our prototype at IXPs

DHS D15PC00205
Colorado State University
PI: Christos Papadopoulos
Team: Stephen Hayne, Haonan Wang, Michalis Faloutsos

Value proposition:

- Unprecedented insight into traffic at a network via collection of very fine granularity information
- Distributed alert system to propagate strategic information to all networks
- Proactive defenses that minimize collateral damage
- Powerful SDN filters that support thousands of rules
- Hacker chatter alerts to plan defenses ahead of an attack

Contact us

- christos@colostate.edu
- Stephen.Hayne@colostate.EDU
- haonan.wang@gmail.com
- michalis@cs.ucr.edu