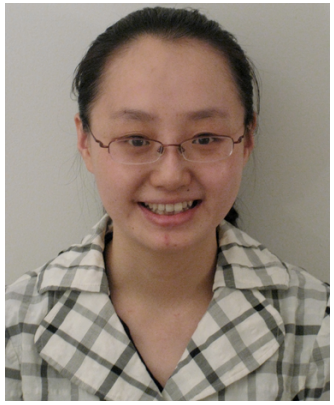
USC University of Southern California

facebook

Yale University

SENSS

Security Service for the Internet

Jelena Mirkovic (USC/ISI), Minlan Yu (USC), Ying Zhang (HP Labs), Sivaram Ramanathan (USC)

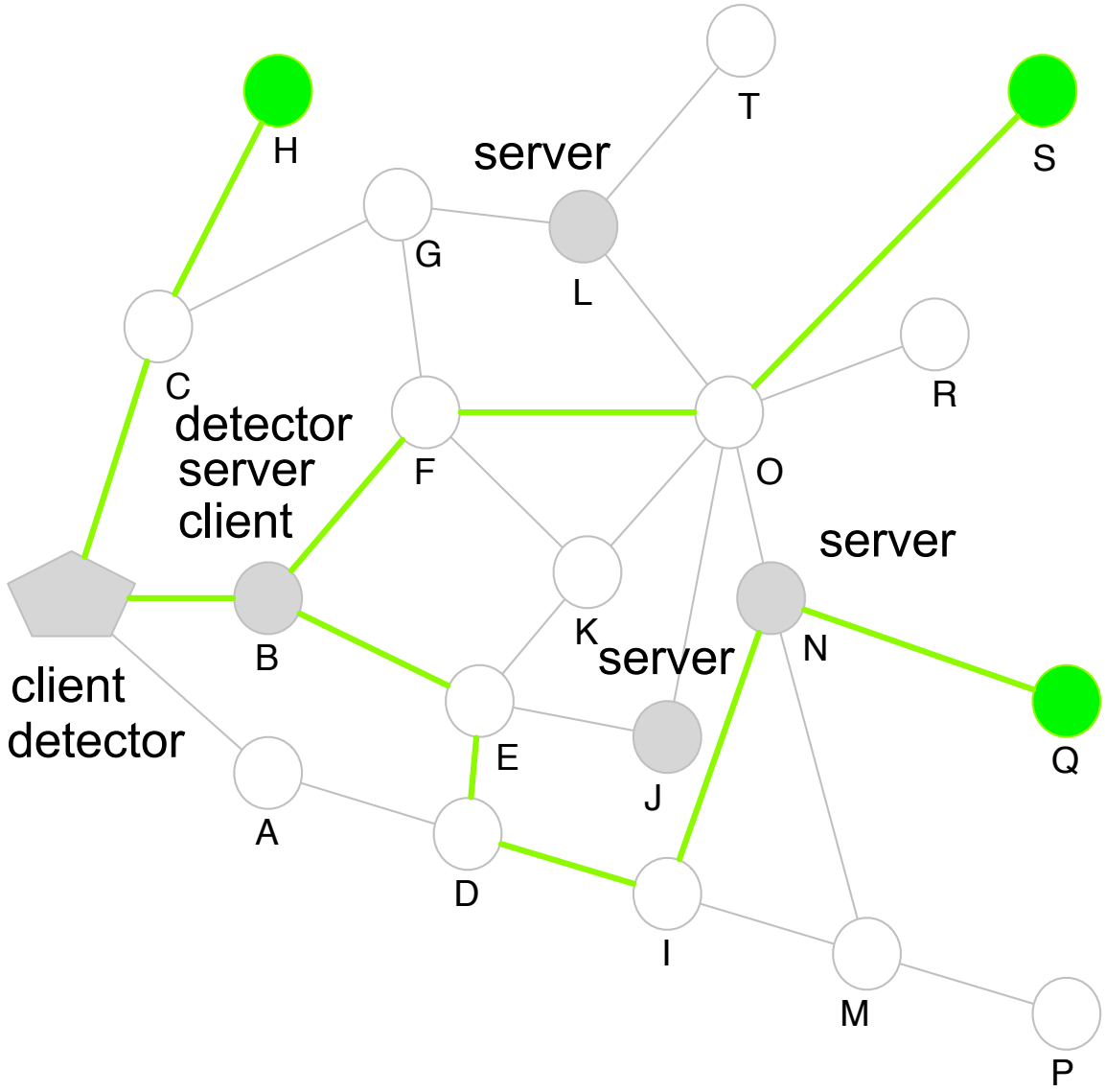
DDoS Attacks: Large and Powerful

- DDoS attacks are increasing in volume and frequency (new record 1.2 Tbps)
- Disproportionate power in hands of attacker
  - Attacks that bring down large, well provisioned victims often wielded by a single person or small group (Spamhouse, Dyn, OVH and Krebs)
  - No special experience or circumstance
  - Cheap for attacker, very expensive for the victim
- Enabled by large, distributed botnets
  - No single entity (centralized or distributed) can withstand this, distributed defenses a must

Our solution: SENSS

- Fully software solution – easy to deploy
- Enables any ISP to offer automated services for DDoS diagnosis and mitigation
  - Naturally distributed, secure, robust to misbehavior
  - Works with existing ISP infrastructure (SDN, Flowspec, Netflow)
- Victim queries its own ISP or remote ISPs
  - About its inbound traffic, routes to its prefixes
  - This helps detect best points for mitigation
- Victim asks select ISPs to:
  - Filter some of its inbound traffic (victim specifies header signature)
  - Demote a route that may contain a bottleneck

SENSS Modules



blacklist aggregator
proxy

SENSS APIs at ISPs

- Exposed as Web services
  - Leverage existing functionalities for robustness (replication), security (HTTPS), charging (e-commerce)

Type	Fields	Action/Reply
Traffic query	Flow, dir, obs_time	List of <tag, dir, volume>
Traffic filter/allow	Flow, dir, tag, duration	Deploy filter/allow actions
Route query	Prefix	List of best paths to prefix
Route demote	Prefix, segment, duration	Demote routes with given segment

- Message authentication: Proof of authority for a prefix
  - E.g., RPKI, a DB of known customers, prefixes and public keys
- TLS for communication security

How Can You Help?

- Deploy a passive module:
  - Detector – learn how often you experience DDoS or participate in it
  - Blacklist aggregator – get our feed of suspicious prefixes
- Deploy an active module:
  - Server – automate filter rule deployment in multiple switches
  - Client + Detector – leverage your ISP's DDoS solution and trigger it automatically
- Looking for:
  - Experiences from trenches, what do you do now for DoS?
  - One-time feedback on needs, deployability, concerns
  - 1h/month ongoing feedback from ops world
  - Sites to pilot our solutions

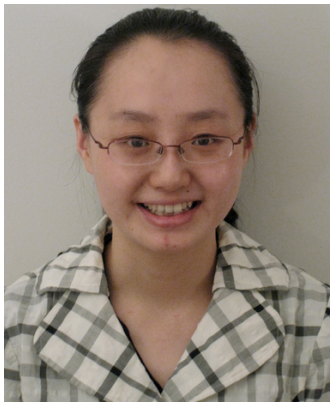
USC University of Southern California

Contact us

sunshine@isi.edu

http://steel.isi.edu/Projects/SENSS/

Jelena Mirkovic



Minlan Yu

Ying Zhang

Sivaram Ramanathan