USC University of Southern California

SENSS

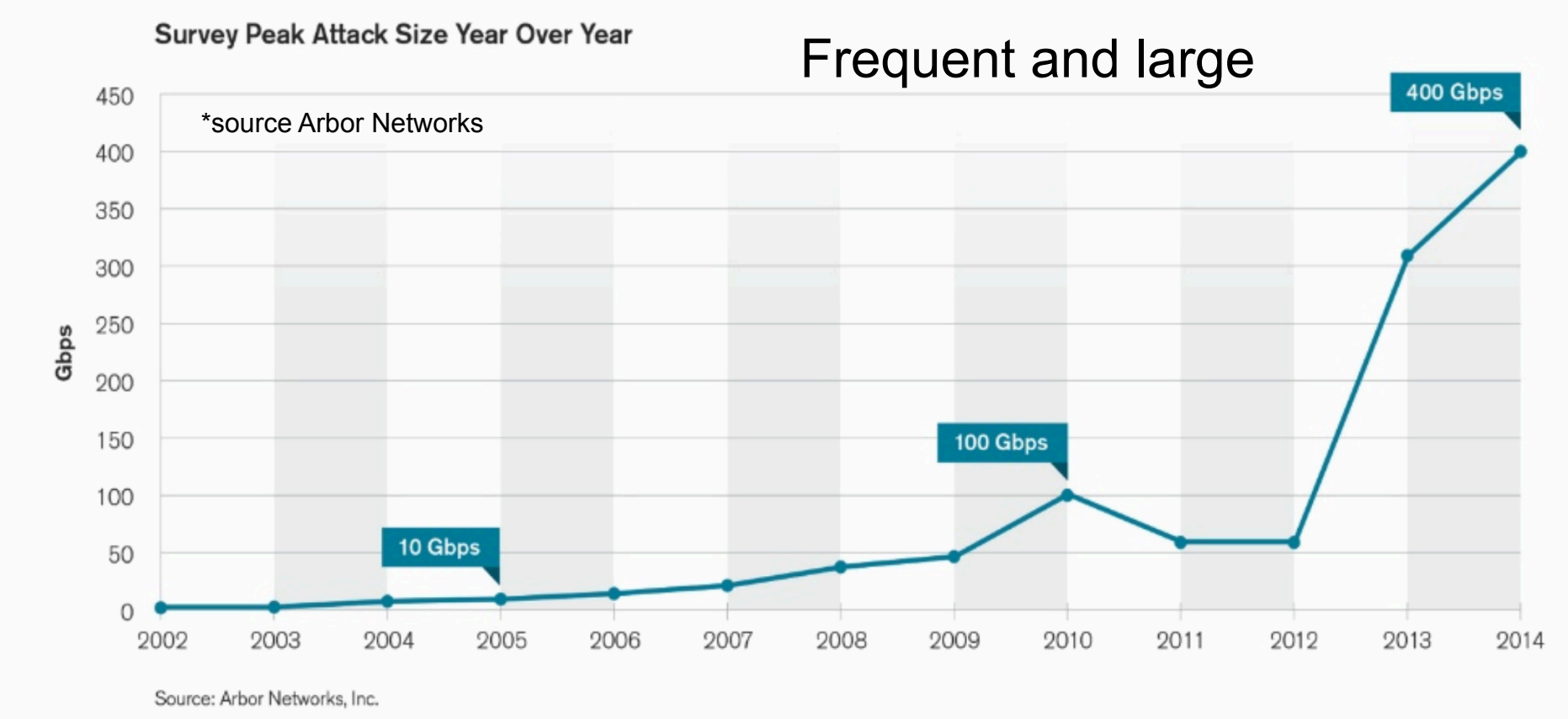
Security Service for the Internet

Jelena Mirkovic
sunshine@isi.edu
USC Information Sciences Institute

Joint work with Minlan Yu (USC),
Ying Zhang (HP Labs) and Abdulla Alwabel (USC)

Motivation and Insights

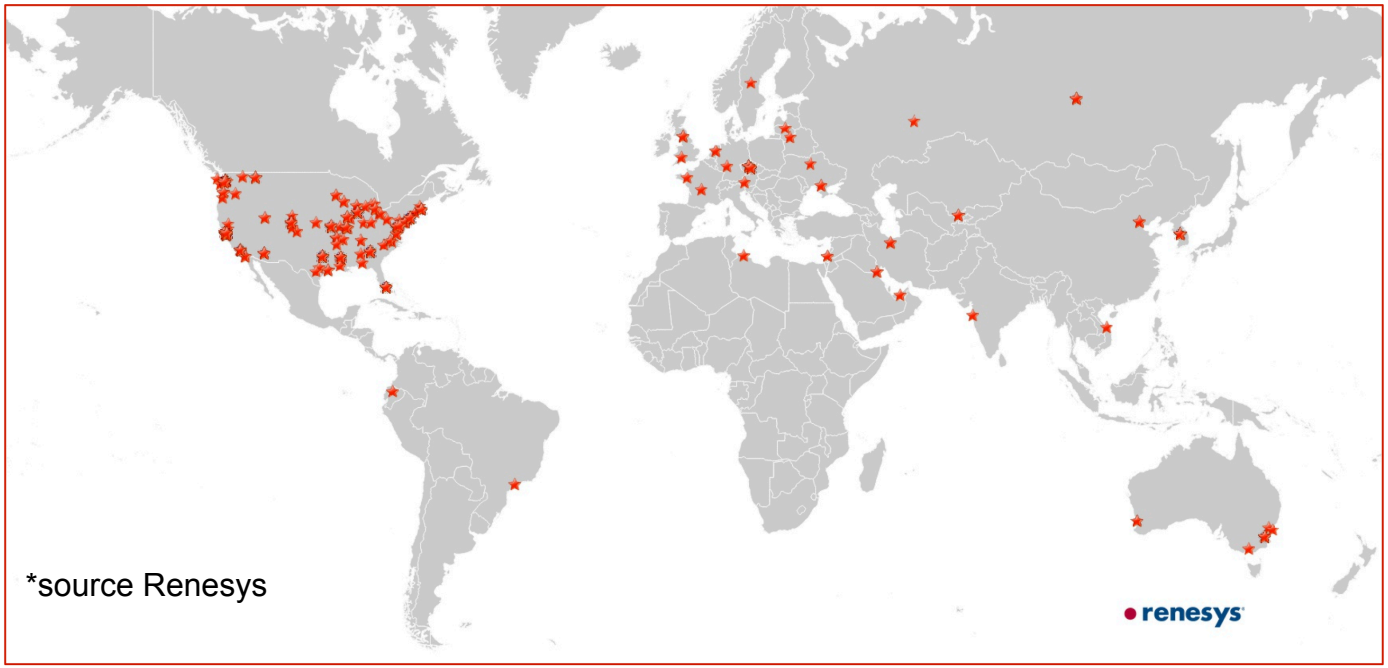
Growing DDoS Attacks*



2/3rd of respondents have experienced at least one DDoS attack

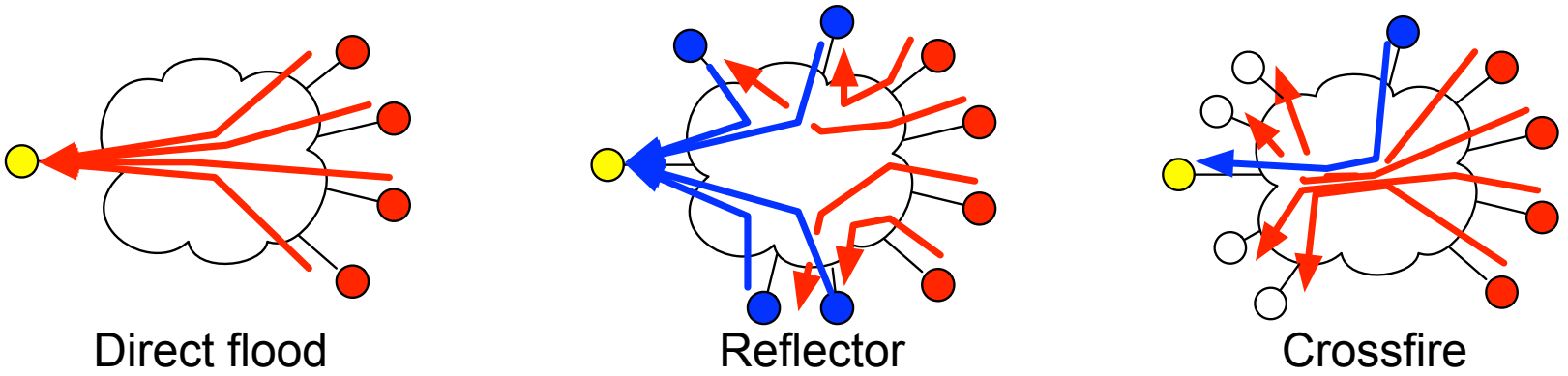
Growing BGP Prefix Hijacking*

- In 2013, hijacking affected 1,500 prefixes, in 150 cities
- Live interception attacks are on for more than 60 days
- Traffic from major companies, govs, ISPs diverted



Attack Variants

- DDoS



- BGP prefix hijacking
  - Attacker announces victim's prefix (origin) or short AS path to the victim (closeness)
  - Blackholing (drop traffic) or interception (sniff or modify then forward to victim)

Main Challenge

- The best locations for diagnosis and mitigation are often far from the victim
  - Victim cannot observe nor control traffic and routes at these locations
- Example: Reflector attack
  - Public servers see spoofed requests but don't know/care that they are spoofed
  - Victim has a challenge to separate legitimate from attack traffic
  - Attack must be filtered upstream due to high volume
- Example: Prefix hijacking
  - Networks far from victim accept and propagate route
- Mitigation should involve remote ISPs
  - Today: sustaining attacks not fixing the problems

SENSS Enables the Victim to

- … observe own traffic
  - Going to the victim' prefixes
  - Carrying sources from the victim's prefixes
- … observe own routes
  - For the victim's prefixes
- … control own traffic
  - Filter, allow, request bw guarantee
- … control own routes
  - Demote a route that may contain a hijacker or correct it

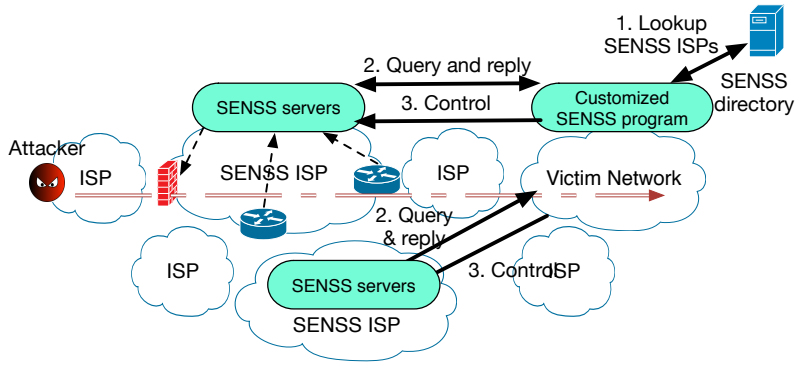
In any willing ISP (even non-neighbor)!

Aligns control with ownership of traffic/routes
Remote ISP must be able to verify the requestor's ownership of prefix

SENSS

Operation

- ISPs run SENSS servers
- Victim identifies ISPs to interact with using public SENSS directory
  - Sends to each a query
  - ISPs authenticate prefix ownership, process query, charge the victim and return replies
- Victim decides which control actions to apply and where
  - Sends messages about this to chosen ISPs
  - ISPs authenticate prefix ownership, charge the victim, implement requested actions



Key Design Decisions

1. Simple actions at ISPs, intelligence at victim
2. Direct victim-remote ISP communication

- Benefits
  - Incentives for ISPs (easy implementation)
  - Efficiency in sparse deployment
  - Robustness to misbehavior
  - Custom and evolvable attack handling

Comparison With State of Art

Approach	Collaboration	Requirements	Capabilities	Attacks handled
Pushback	Hop-by-hop	None	O/C traffic	DF detect/mit
Traceback	None	Marking	O traffic	DF detect
CloudFlare/ Prolexic	None	Middlebox	O/C traffic	DF, RF, CR detect/mit.
Flowspec	Peers	None	C traffic	DF mit.
Secure BGP	Hop-by-hop	Crypto	C routes	BL, IC origin/closeness detect/mit
RPKI	Victim-any AS	Crypto	C routes	BL, IC origin detect/mit
Looking glass	Victim-any AS	None	O routes	BL, IC detect
SENSS	Victim-any AS	RPKI	O/C traffic/ routes	DF, RF, CR detect/mit BL, IC origin/closeness detect/mit

SENSS APIs at ISPs

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

Type	**Message**	**Matching Fields**	**Reply/Action**
Traffic query	*traffic_query*	flow, direction, otime	a list of <tag, direction, #bytes/#pkts> for the flow
Route query	*route_query*	prefix	AS paths from the SENSS AS to the prefix
Traffic control	*filter/allow*	flow, duration	filter/allow all traffic matching the flow
	set_bw	flow, bw, dueation	guarantee *bw* for traffic matching the flow
Route control	*demote*	prefix, seg, duration	give lower priority to route to prefix w/ specified AS path seg
	mod	prefix, seg_1,seg_2, duration	modify the false AS path seg_1 to the correct seg_2

Tag = neighbor's AS number (+ geolocation)

Security

- RPKI to verify prefix ownership
- TLS for communication security
- Enabling communication during attacks
  - Victim may be flooded or its prefixes hijacked
    - Cannot receive replies, may not be able to send messages
  - Offload victim functionality to a proxy in another network
    - Use ROA to delegate prefix ownership
    - May set up proxies as backup service
    - Proxy monitors the victim operation, turns on

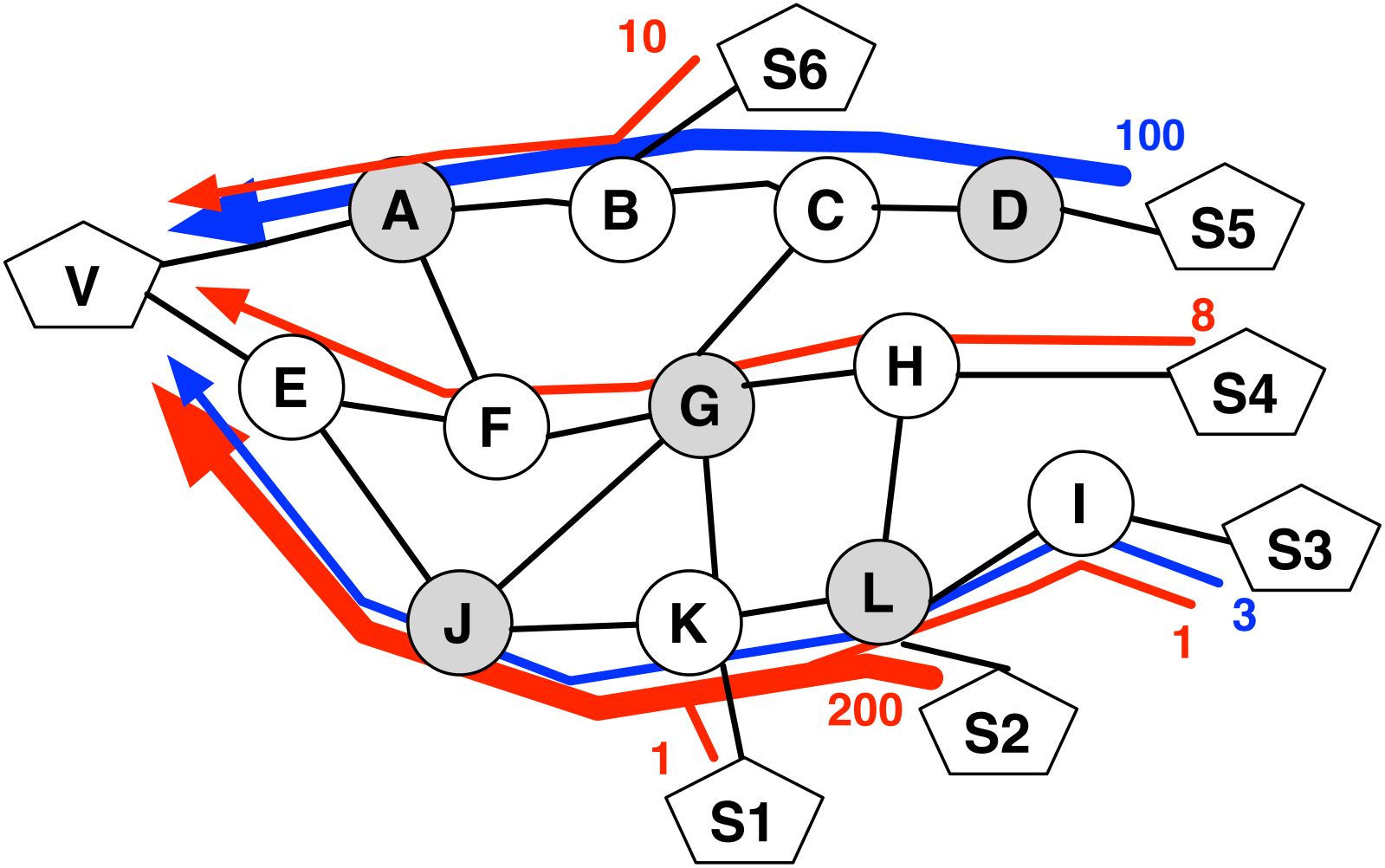
Using SENSS To Diagnose and Mitigate Attacks

just examples
victim can design custom programs

Direct Floods

- If there is TCP/IP signature
  - Send traffic filter messages to ISPs
- If there is no TCP/IP signature
  - Send traffic queries to ISPs with victim's prefix (before and during attacks)
  - Identify AS-AS links from replies that
    - Used to carry little or no traffic to the victim (threshold α)
    - Now carry a lot of traffic to the victim
  - Send traffic filter messages to ISPs for these AS-AS links
  - Works for attacks that deploy IP spoofing
- Iteratively deploy filters until attack below goal

Direct Floods



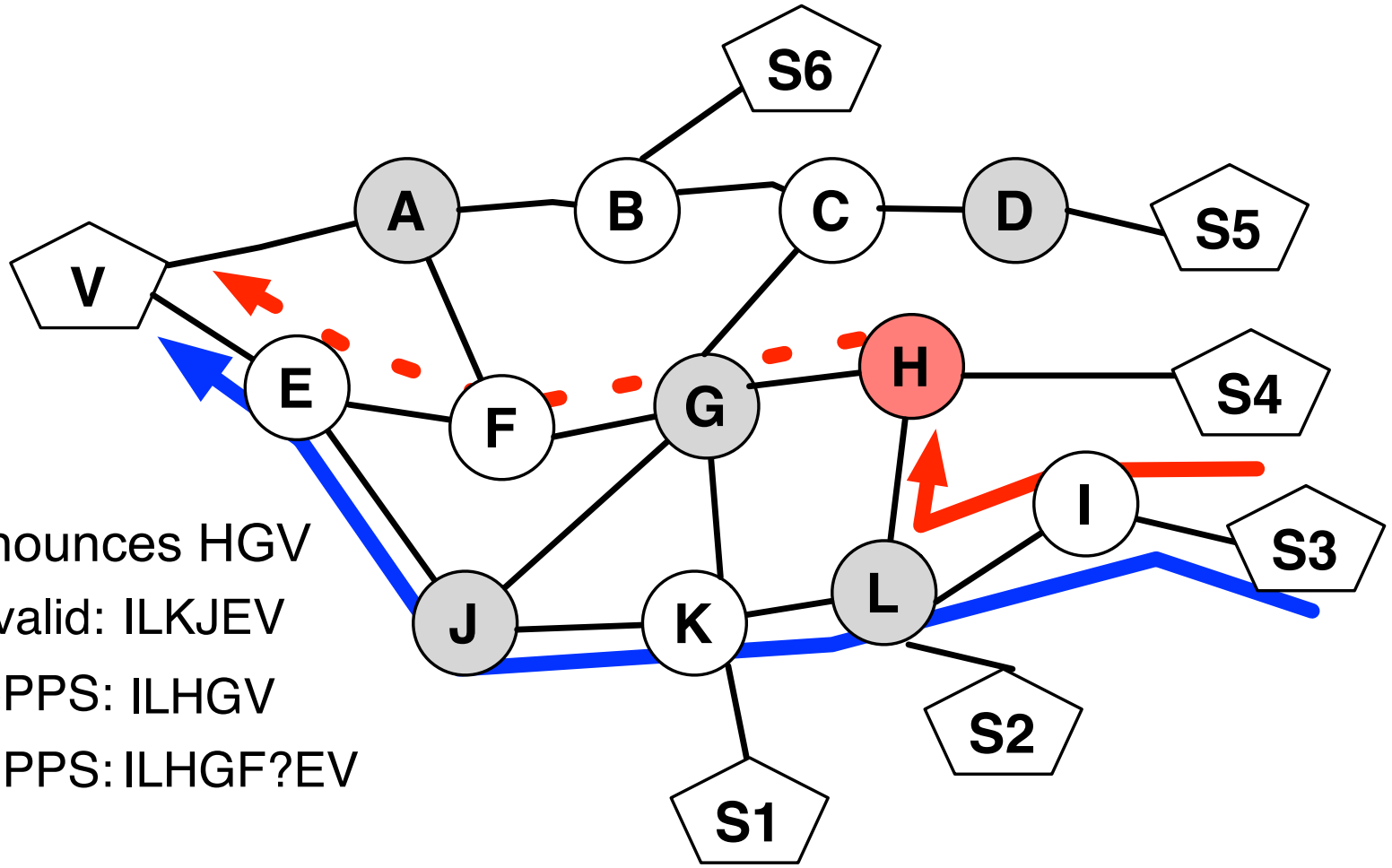
Reflector Attacks

- NAT all outgoing requests for port S (e.g., 53) using a range of source ports [a,b]
- Send two control messages to chosen ISPs
  - Allow traffic to IP of NAT, from port 53 to ports [a,b]
  - Drop all other traffic from port 53 to victim's prefixes
- Can change [a,b] dynamically

Interception

- RPKI takes care of origin attacks
- For closeness attacks
  - Ask ISPs for path to V in Control Plane - CPPS
  - Send traffic queries to ISPs on and off CPPS to learn Data Plane paths - DPPS
  - Find segments that appear in Control Plane but not in Data Plane
  - Send demote or mod messages to polluted ISPs
    - BGP realizes attack route is longer, reverts to good route

Interception



H announces HGV

valid: ILKJEV

CPPS: ILHGV

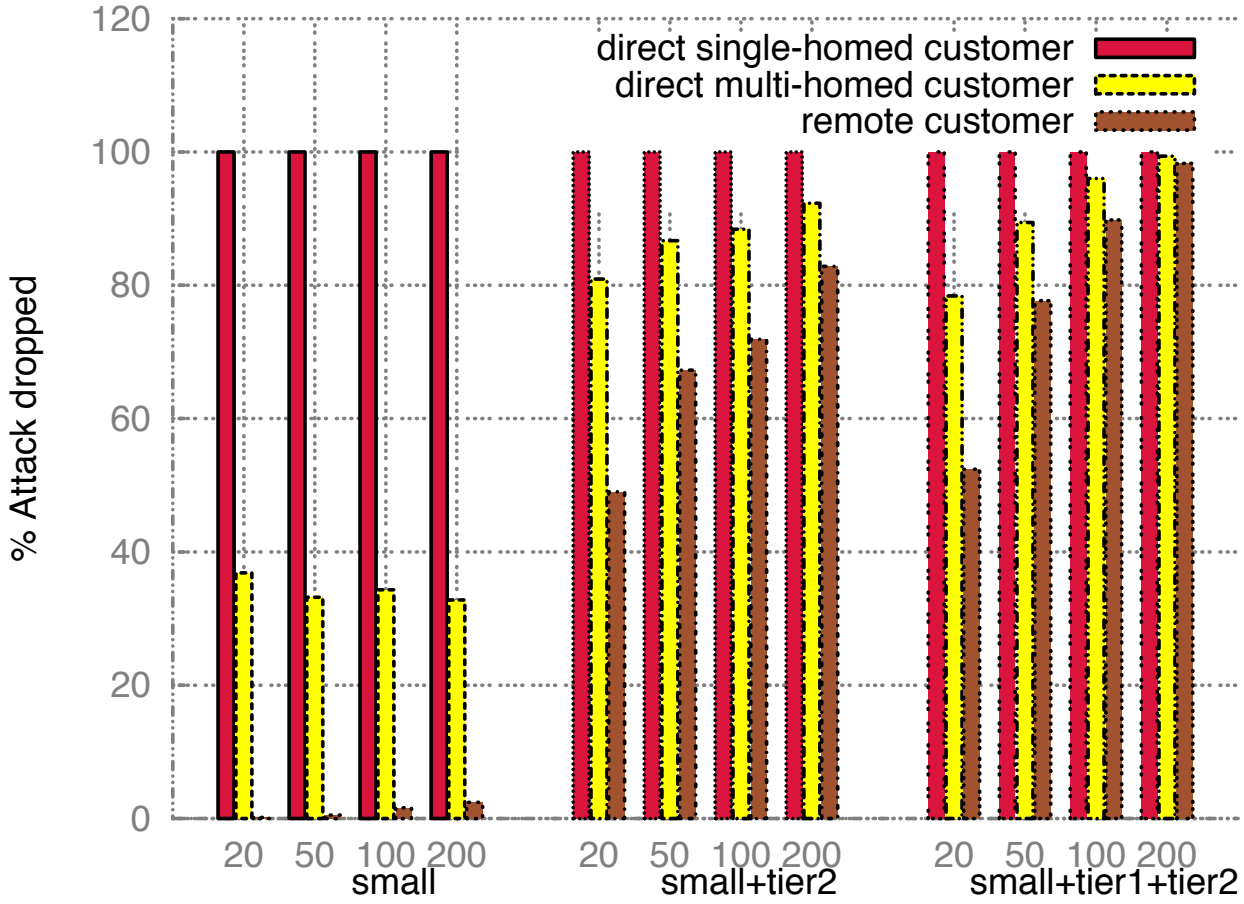
DPPS: ILHGF?EV

Evaluation

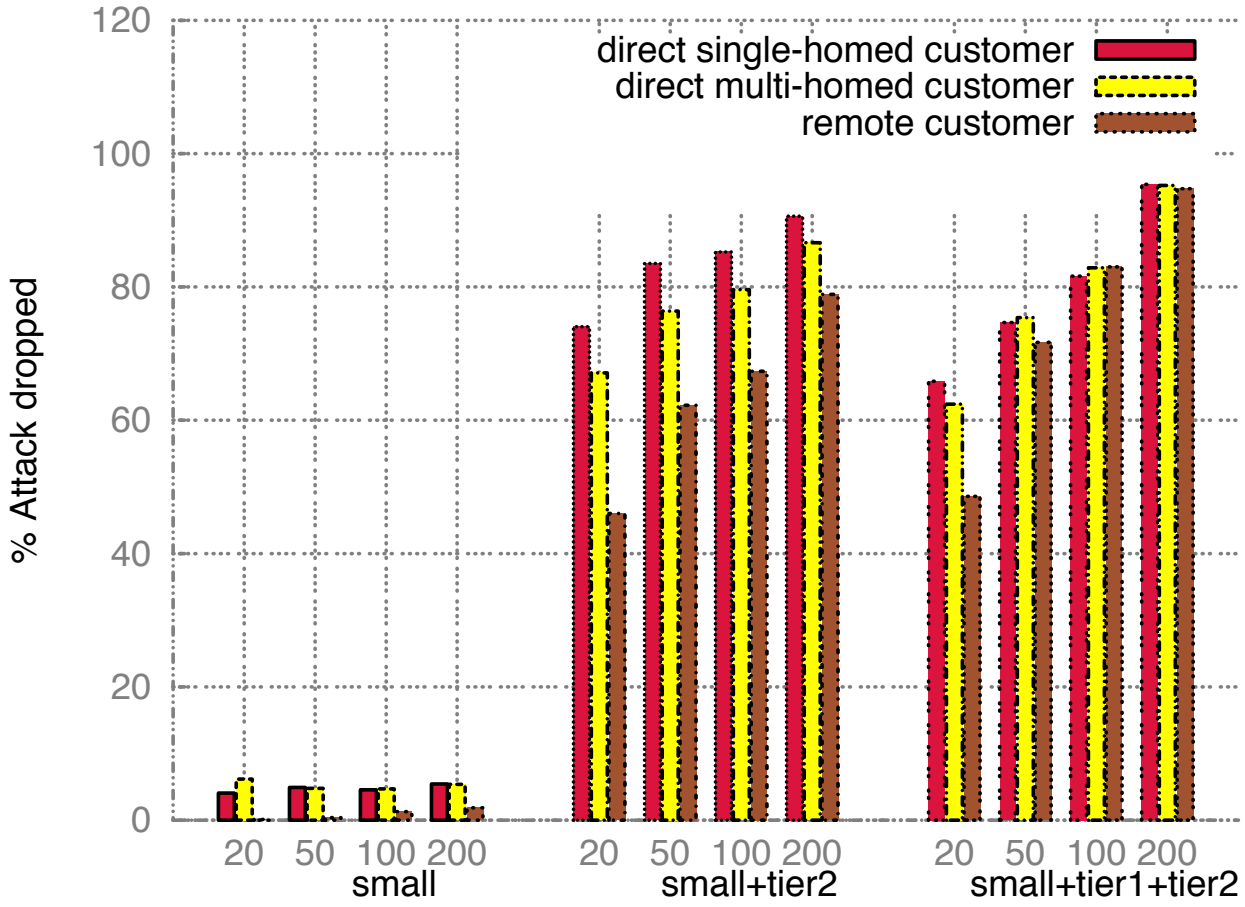
Simulation

- On AS topology
  - Using a month's worth of data from RouteViews
- Several partial deployment scenarios
  - On small ISPs
  - On mix of small, tier 2 and tier 1 ISPs (70:25:5 ratio)
  - Up to 200 ASes (~ 0.5% of the Internet, 15x fewer than ASes currently deploying RPKI)
- Legitimate traffic (for DDoS w sig)
  - Edgecast (all POPs)
- Attacker distribution
  - UCSD (two attacks by Storm botnet in 2007)
  - BARS (sources of attacks from 8 months in 2013)

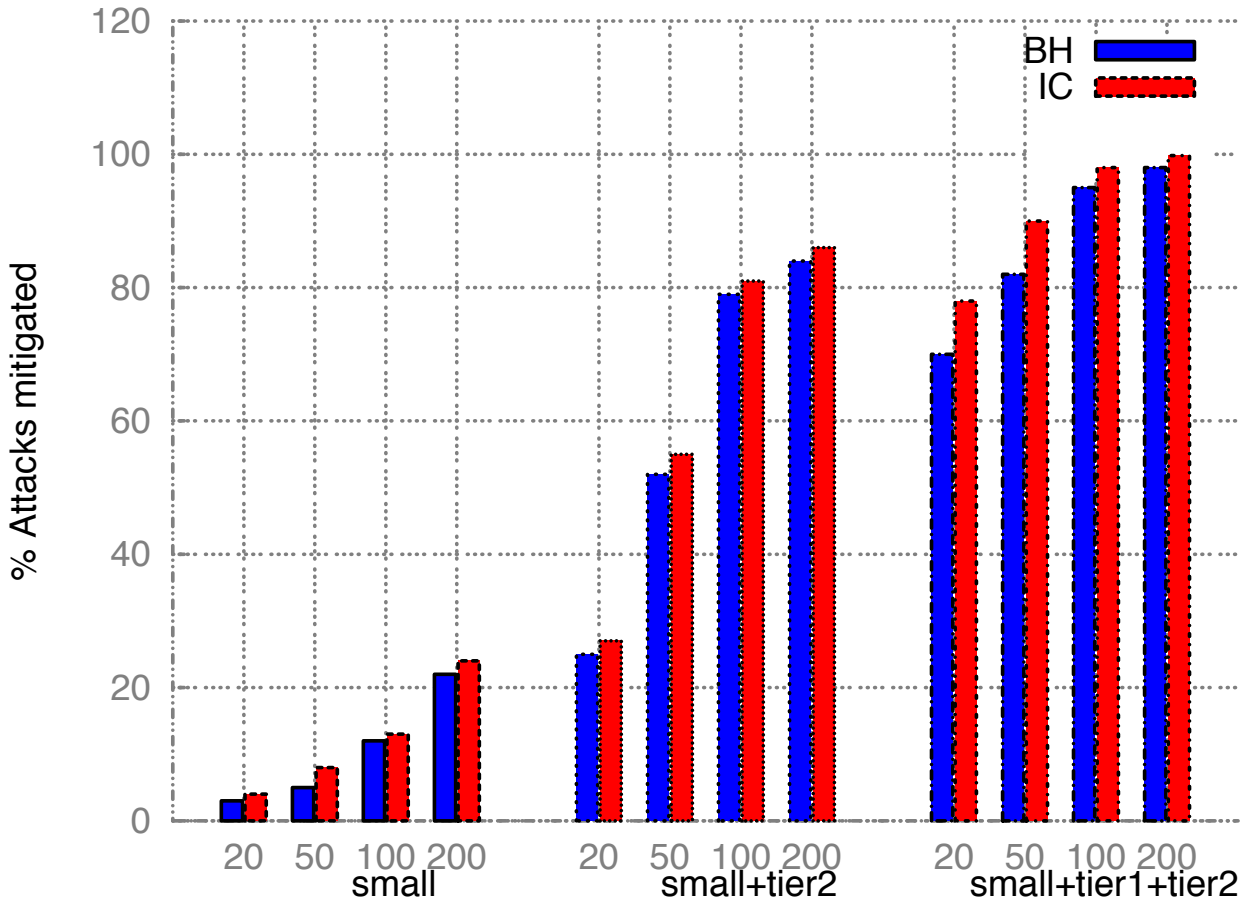
DDoS: Reflection and Flood with Signature



DDoS: Flood without Signature



Hijacking: Blackholing and Interception



Deployment Considerations

Privacy and Policy

- SENSS does not reveal sensitive info about ISP's business
- Routing info is already public
- Traffic distribution per neighbor can be anonymized or aggregated
  - For DDoS w/o sig we need traffic volume but not AS identity in tags; tags can be anonymized
  - For blackholing/interception we need aggregate (IN/OUT) traffic and AS identities
- ISPs can refuse to render services at will
  - For policy reasons or if too many queries by the same customer

Charging

- Fixed price or per service rendered
- Each ISP can come up with their own price per service
- When under attack the victim can register for SENSS service with an ISP on demand
  - Our Web service implementation enables this
  - No prior trust needed

Misbehaving ISPs

- For many scenarios the effect of lying is the same as if the liar is legacy AS
  - Attacker can only delay detection and response but cannot subvert them
- ISP may charge for control actions and not perform them
  - Victim can monitor for this; avoid non-performing ISPs

Conclusions

Conclusions

- Distributed attacks not handled well today
  - Redundancy to sustain attacks. Cost is still high and attack traffic still clogs the Internet
  - Smaller businesses can be affected for days
- SENSS can detect and mitigate distributed attacks in very sparse deployment
  - Good effectiveness, low cost, simple to deploy
  - Source of revenue for ISPs
- An infrastructure for ISP collaboration
  - Adding APIs to ISPs can be useful for many purposes

USC University of Southern California

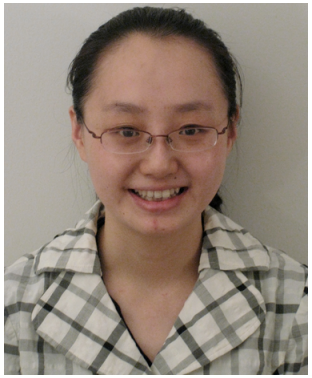
Thanks for coming!

Reach out if interested

sunshine@isi.edu

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

Jelena Mirkovic



Minlan Yu

Ying Zhang

Abdulla Alwabel

Need Community Feedback

- From ISPs
  - Would you be interested in deploying SENSS or just test-driving it?
  - What are your concerns?
  - Would you charge remote customers for SENSS services?
    - Flat rate or per request?
  - What other types of attacks should we look at?
- From end-networks/enterprises
  - Would you use SENSS if it were deployed?
  - What are your concerns?
  - What other types of attacks should we look at?

Reach out if interested

sunshine@isi.edu

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