SENSS: Software-defined Security Service

Minlan Yu

University of Southern California

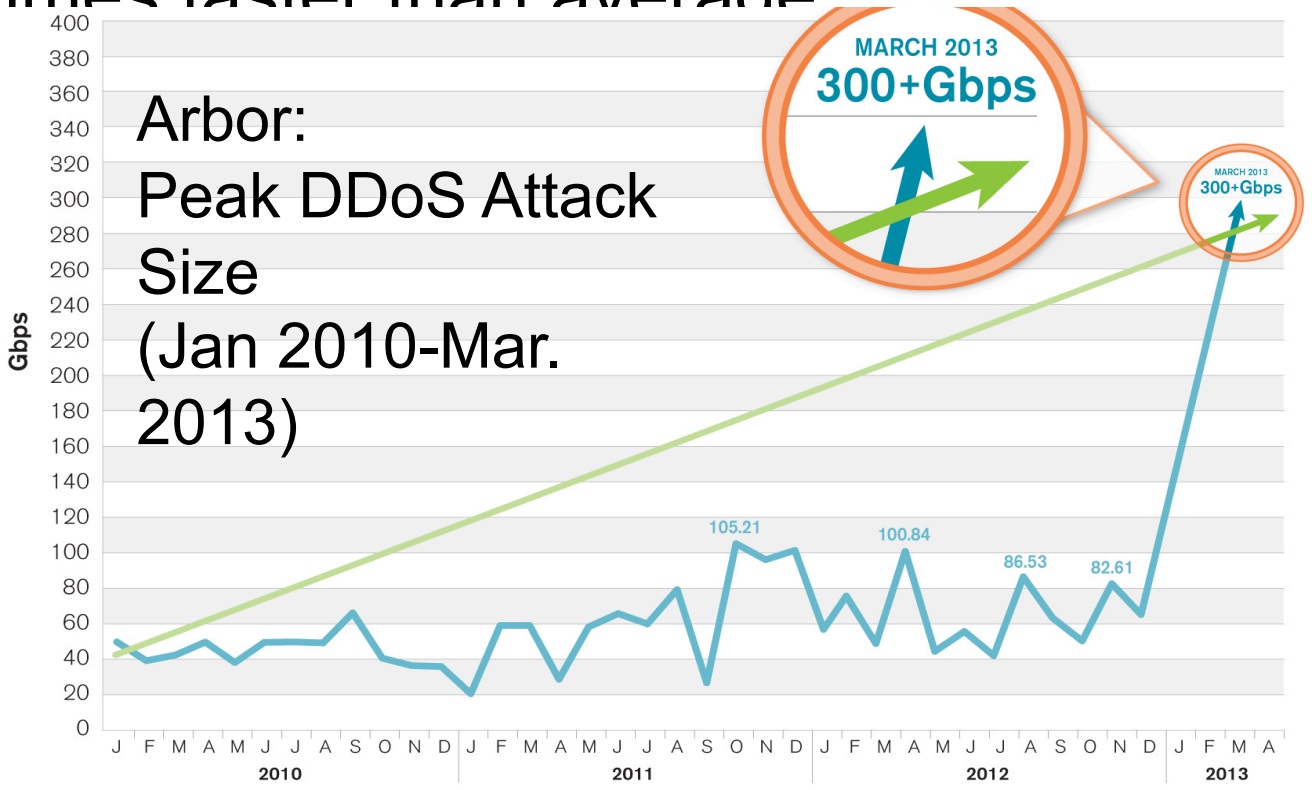
Joint work with Abdulla Alwabel, Ying Zhang, Jelena /ic

Growing DDoS Attacks

Average monthly size of DDoS attacks (Gbps)

Growing DDoS Attacks

At March 2013, DDoS flooded Spamhaus at 300Gbps,
200 times faster than average

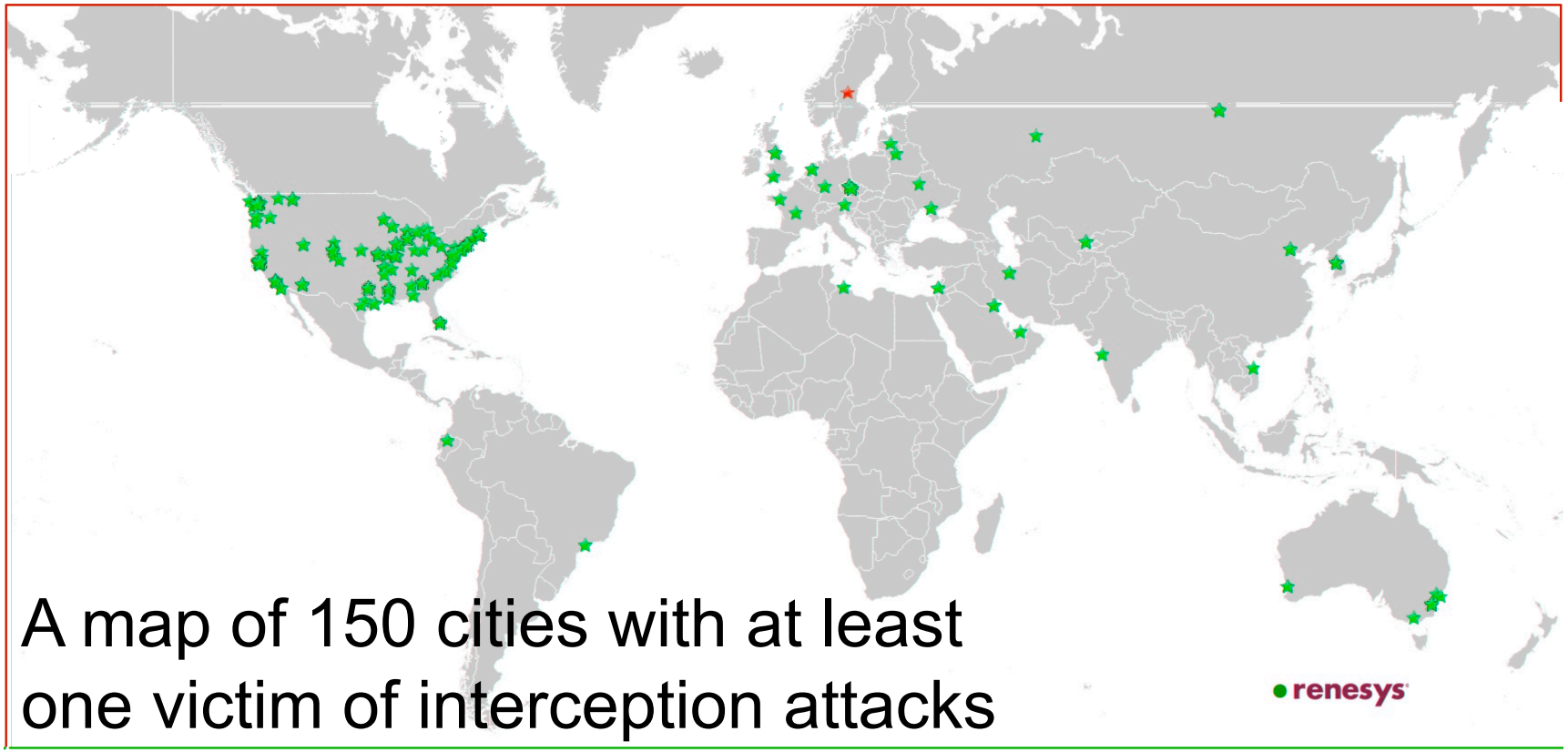


Growing Prefix Hijacking

In 2013, prefix hijacking affects 1,500 prefixes, 150 cities

Live interception attacks are on for more than 60 days

Traffic from major financial companies, govs, ISPs diverted



A map of 150 cities with at least one victim of interception attacks

Motivation

- Network attacks are more frequent and powerful
  - In Q1 2014: 47% increase in total DDoS attacks.
  - Attack size more than 300Gbps.
- Network attacks are more damaging
  - 71% of data center operators report DDoS attacks
  - DDoS on Bitcoin Exchanges lowered bitcoin price from 700$ to 540$
- Diverse attacks
  - Data plane: Direct flooding, reflector attacks
  - Control plane: Prefix hijacking, interception

Traditional Solutions

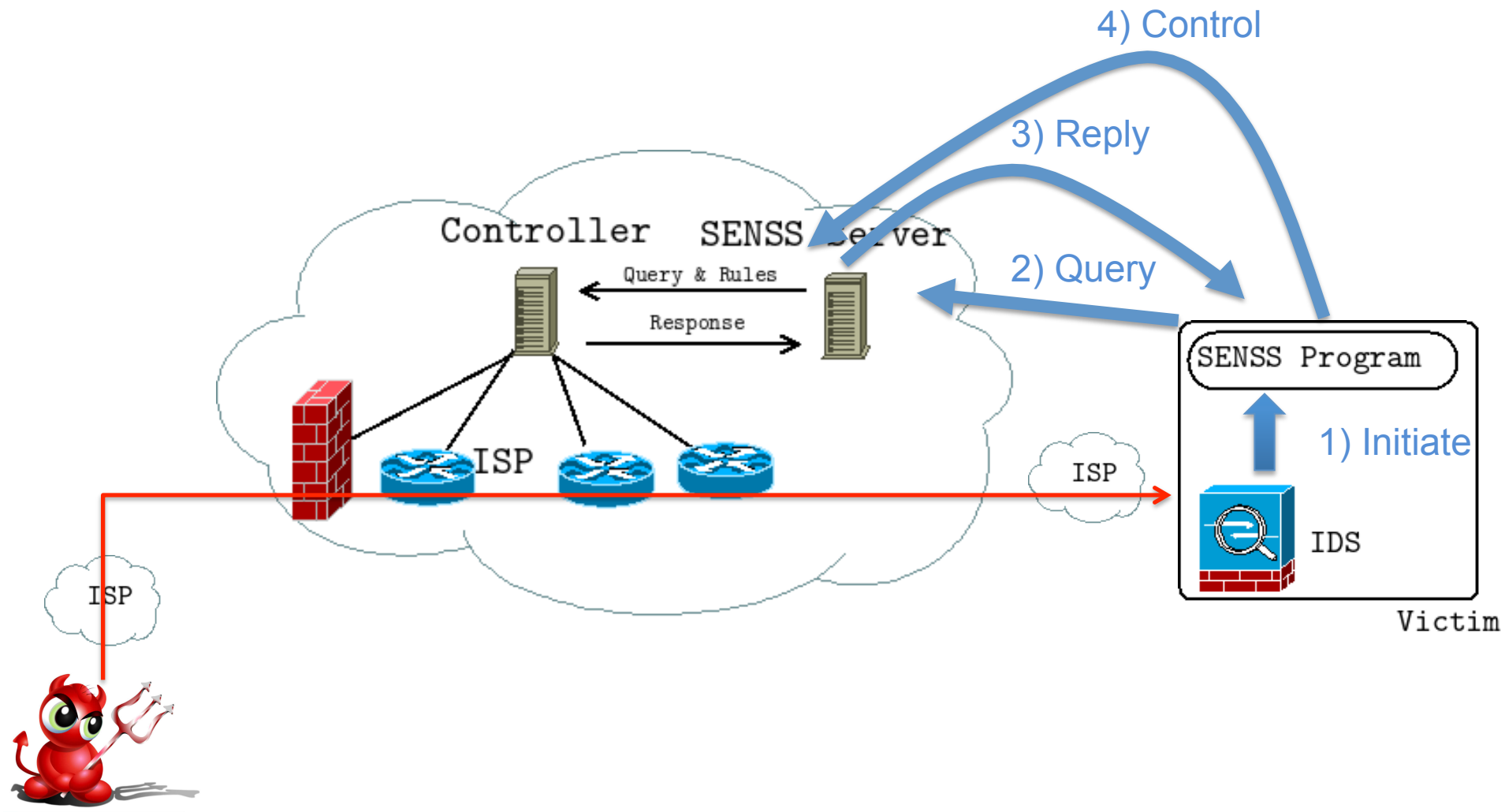
- Victim-based solutions are not sufficient
  - Leverage IDS boxes, or outsource to security services
  - Hard to diagnose remote root causes or trace sources
  - Have to manually call ISPs on the phone
- Research inter-ISP solutions are not adopted
  - Focus on individual attacks
  - Require complex changes on routers
  - No economic incentive for ISPs

Need a flexible, deployable solution for diverse attacks

Software-defined Security Service (SENSS)

- Victim-oriented programming for diverse attacks
  - Victims have the incentives
  - Victims have knowledge of their traffic and priorities
- Victims request help from remote networks
  - To observe and control their own traffic and routes
  - Using simple and expressive interfaces at ISPs, easily implemented in today's ISPs
- Difficult trade-offs: all the intelligence implemented at the victim

SENSS Design



SENSS is Practical

- ISPs
  - SENSS-needed interfaces already exist in their infrastructure
  - ISPs already provide manual support for victims
  - ISPs can charge victims for the security services
- Victims
  - Strong incentives to fix their own problems
  - Effective solutions even with partial deployment

Challenges

- What's the right interface at ISPs?
  - Easy to implement at today's ISPs
  - Useful for a wide variety of attack defenses
- How can victims program the defenses?
  - With SENSS deployment on a few ASes
  - Without missing information (spoofing, privacy, etc)
- Security and Privacy

Simple, Flexible Interfaces at ISPs

SENSS Interfaces: Traffic

- Traffic query
  - Query flows using TCP/IP header fields
  - Answer #bytes/pkts from/to each neighbor
- Traffic control
  - Filter, rate limit traffic matching a traffic flow
- Similar to OpenFlow rules
  - Only allow victims to query/control traffic to/from them

1. src=1.2.*.*, dest=3.4.5.* → query
2. src port=80, dest=3.4.*.* → filter

SENSS Interfaces: Routes

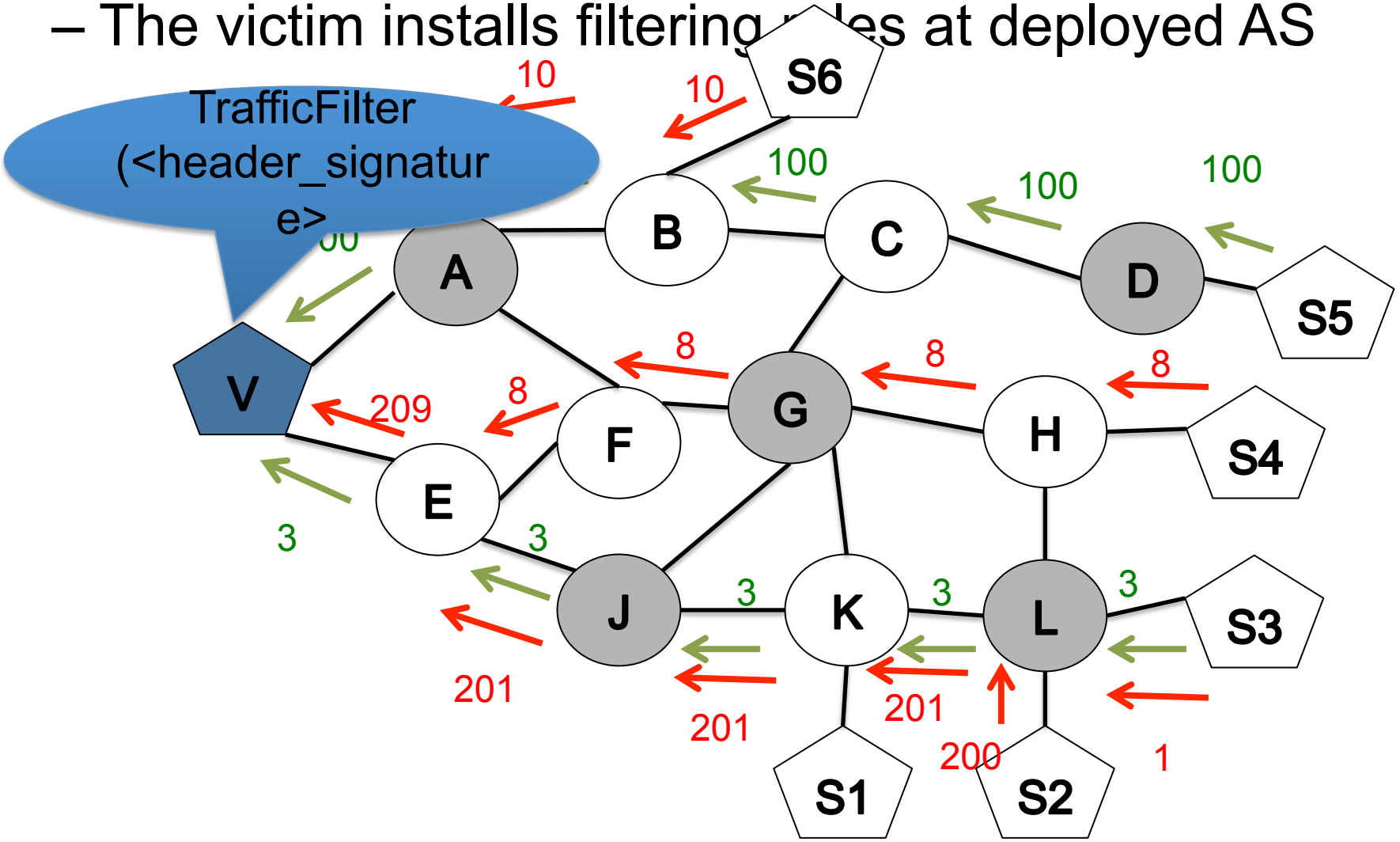
- Route query
  - Query the best route to the victim prefix
  - Similar to BGP route queries to neighbors
  - But we extend to remote ASes
- Route control
  - Modify the route from the AS to the victim
  - Demote all the routes with given AS segments
  - To get around the malicious/polluted ASes

Automated Detection/Mitigation at Victims

DDoS w/ Signature

– The victim identifies the attack and header signature

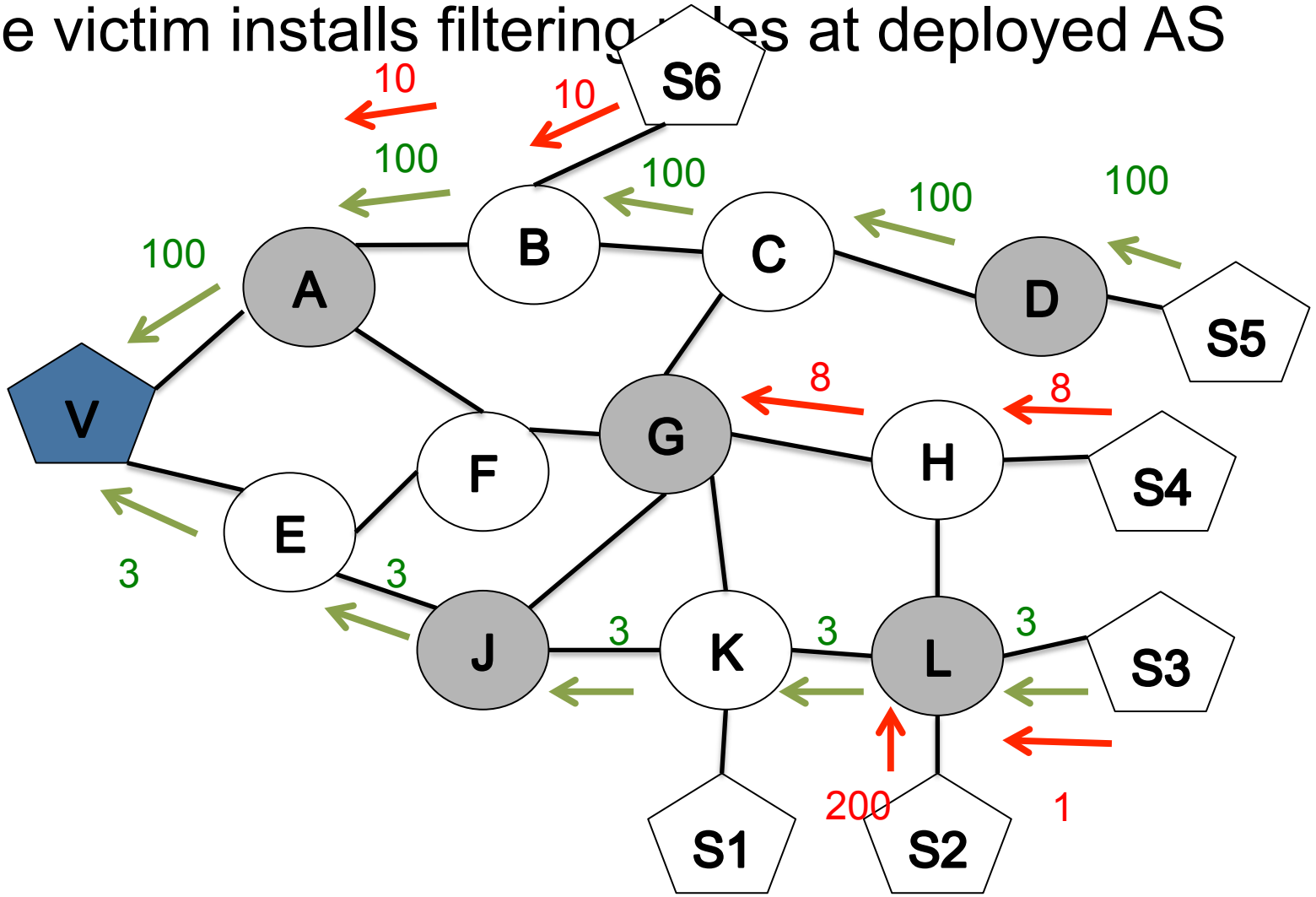
– The victim installs filtering rules at deployed AS



DDoS w/ Signature

– The victim identifies the attack and header signature

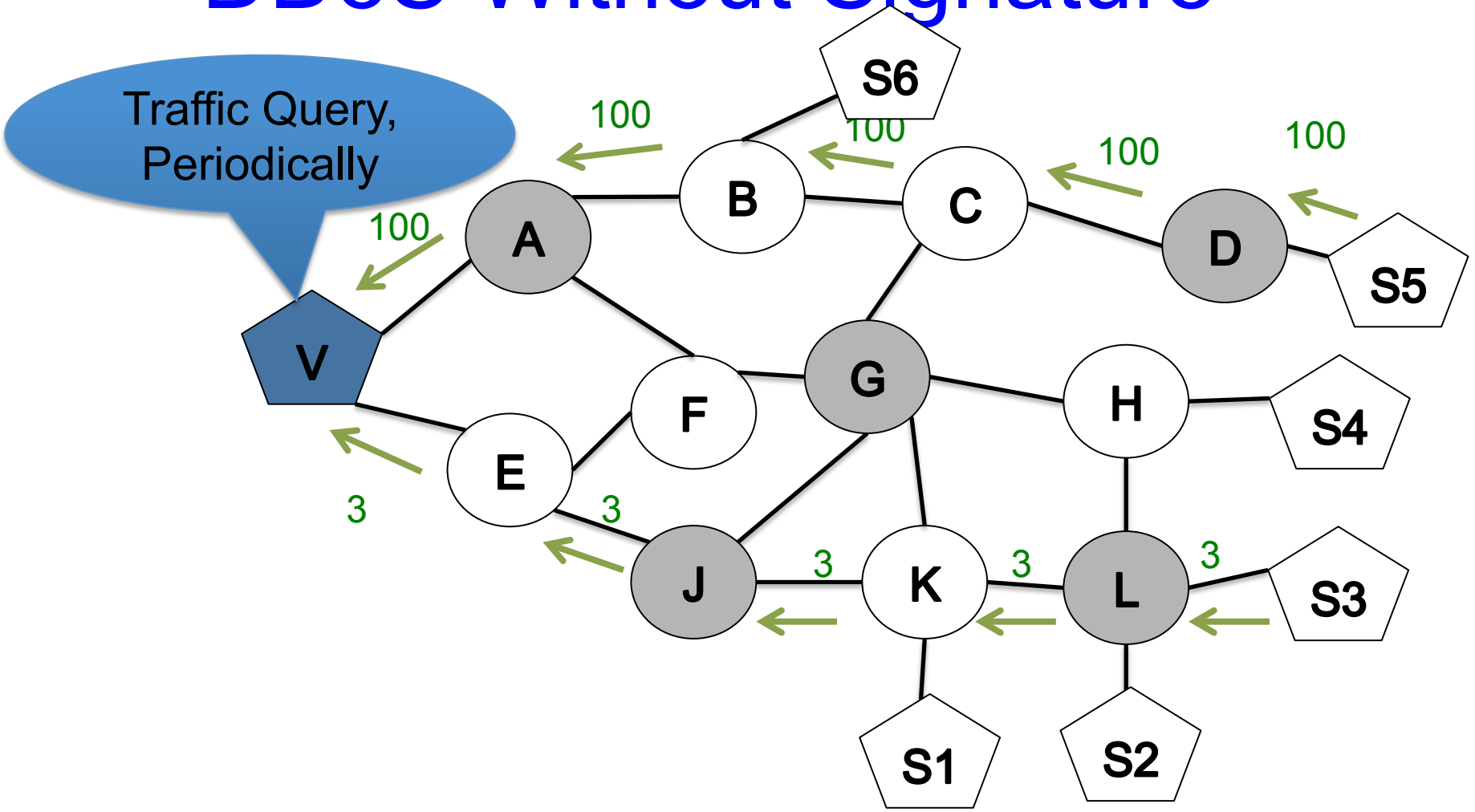
– The victim installs filtering rules at deployed AS



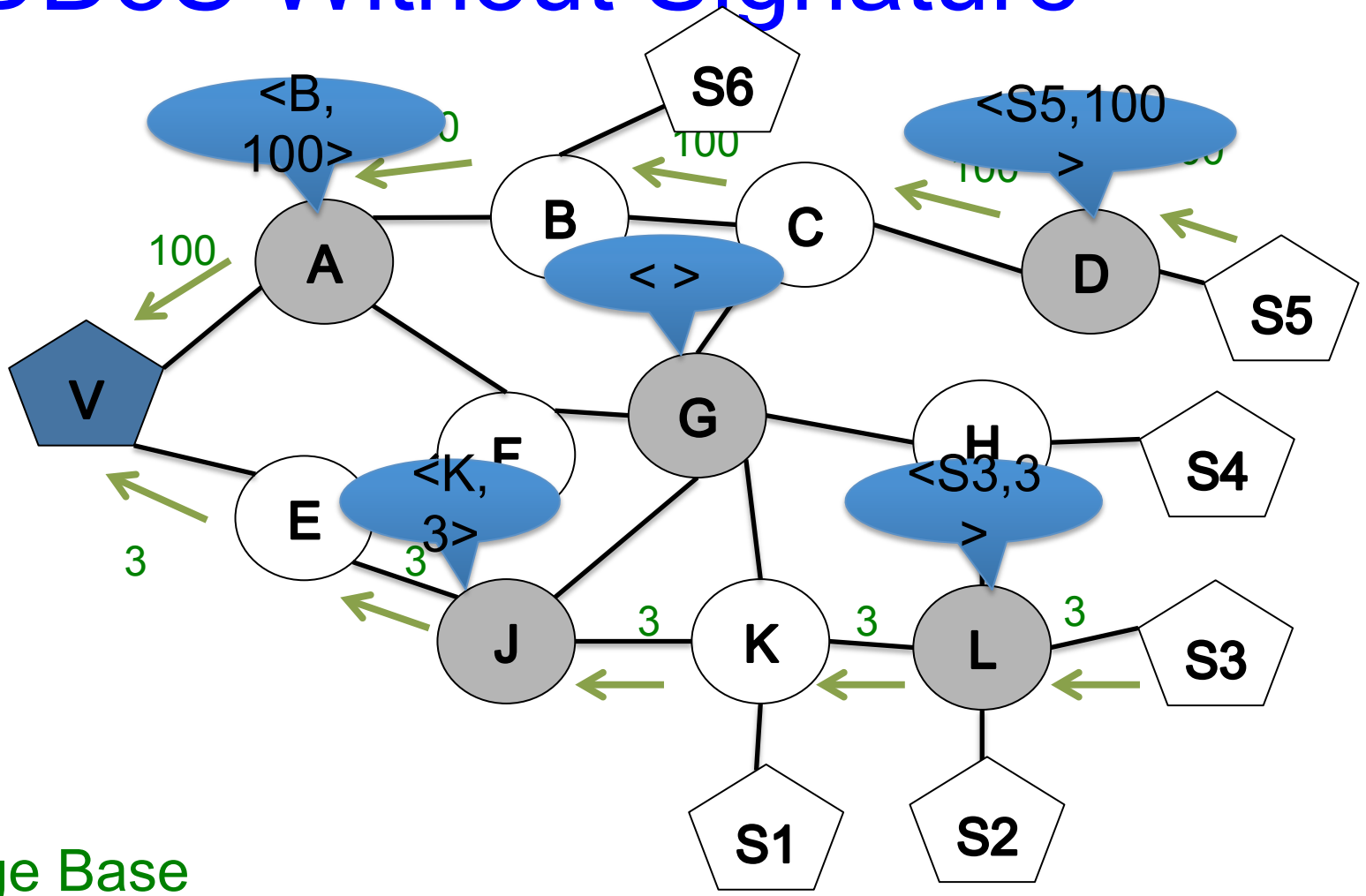
DDoS Without Signature

- Victims may not find a signature
  - Spoofing; randomize packet header and contents
- Cannot simply block high traffic aggregates
  - May lead to high collateral damage
- SENSS: Compare traffic distribution across ASes before and after the attack
  - Track normal traffic distribution periodically
  - Compare with traffic distribution during attack
  - Filter on those AS links with big traffic growth
  - Only victim can decide which collateral damage is OK

DDoS Without Signature



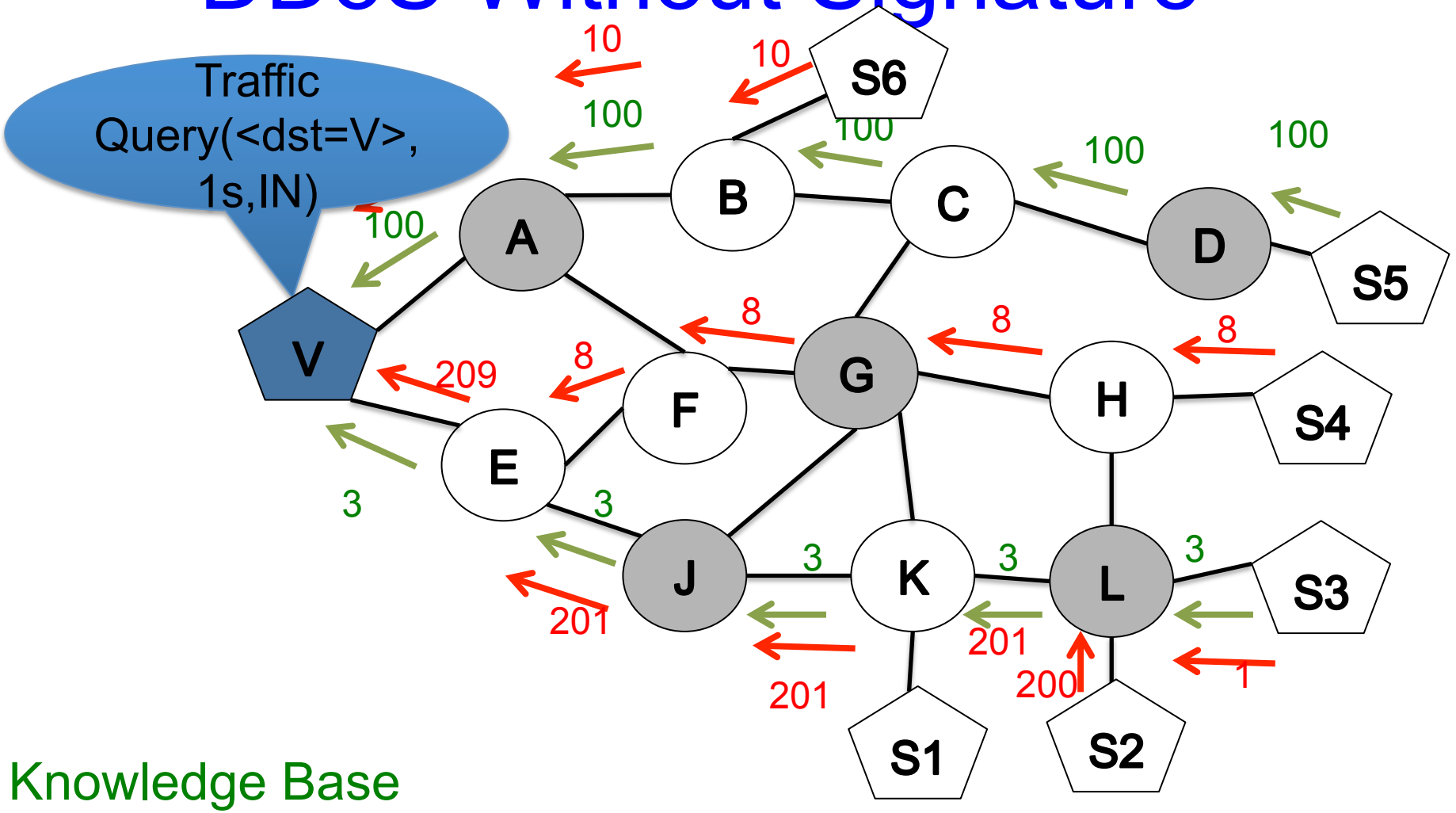
DDoS Without Signature



Knowledge Base

A:<B,100> D: <S4,100> G: <> J: <K,3> L: <S3,3>

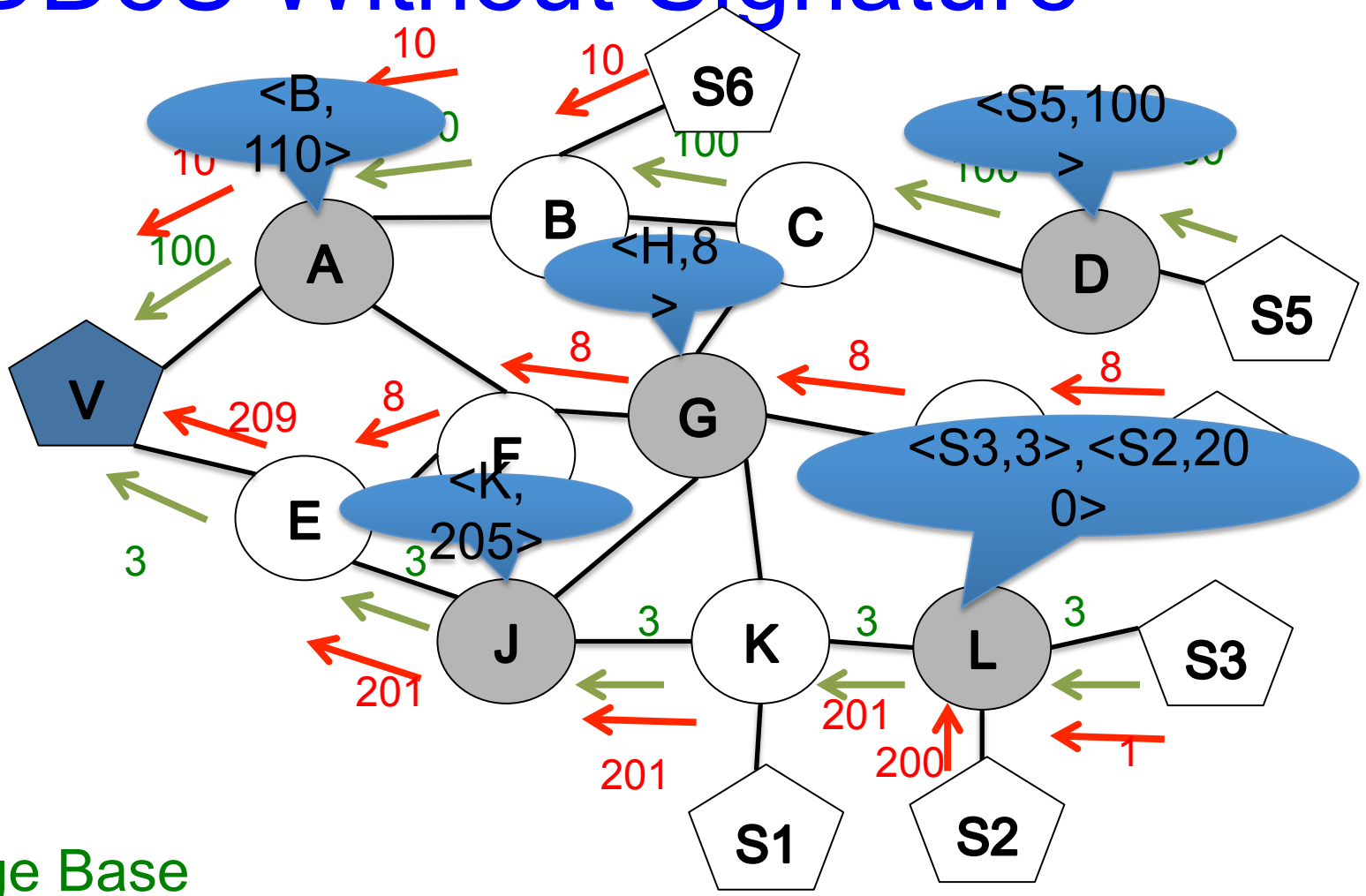
DDoS Without Signature



Knowledge Base

A:<B,100> D: <S4,100> G: <> J: <K,3> L: <S3,3>

DDoS Without Signature

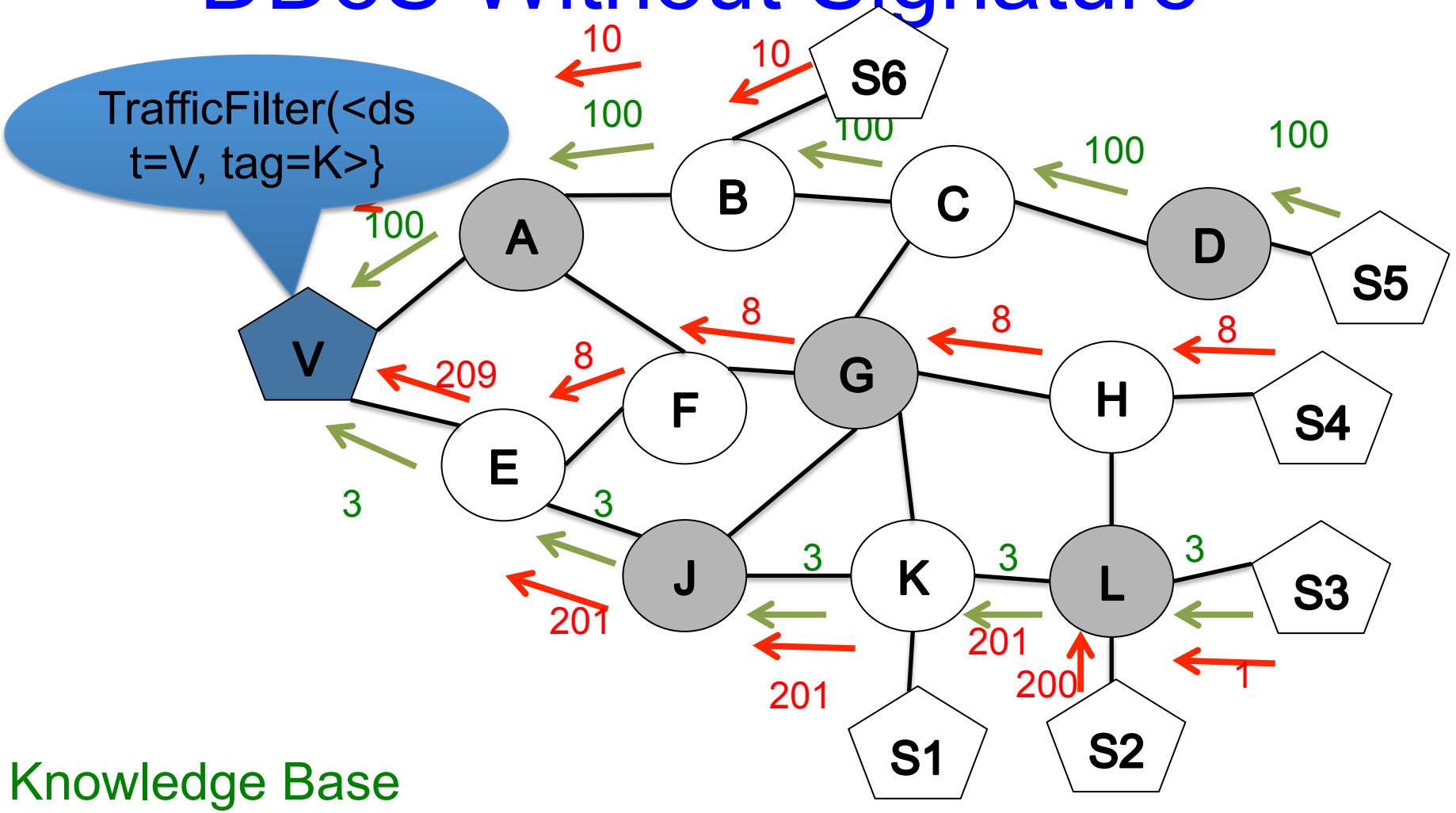


Knowledge Base

A:<B,100> D: <S4,100> G: <> J: <K,3> L: <S3,3>

~~A:<B,100>~~ D: <S4,100> G: <H, 8> J: <K,205> L: <S3,3> <S2, 200>

DDoS Without Signature

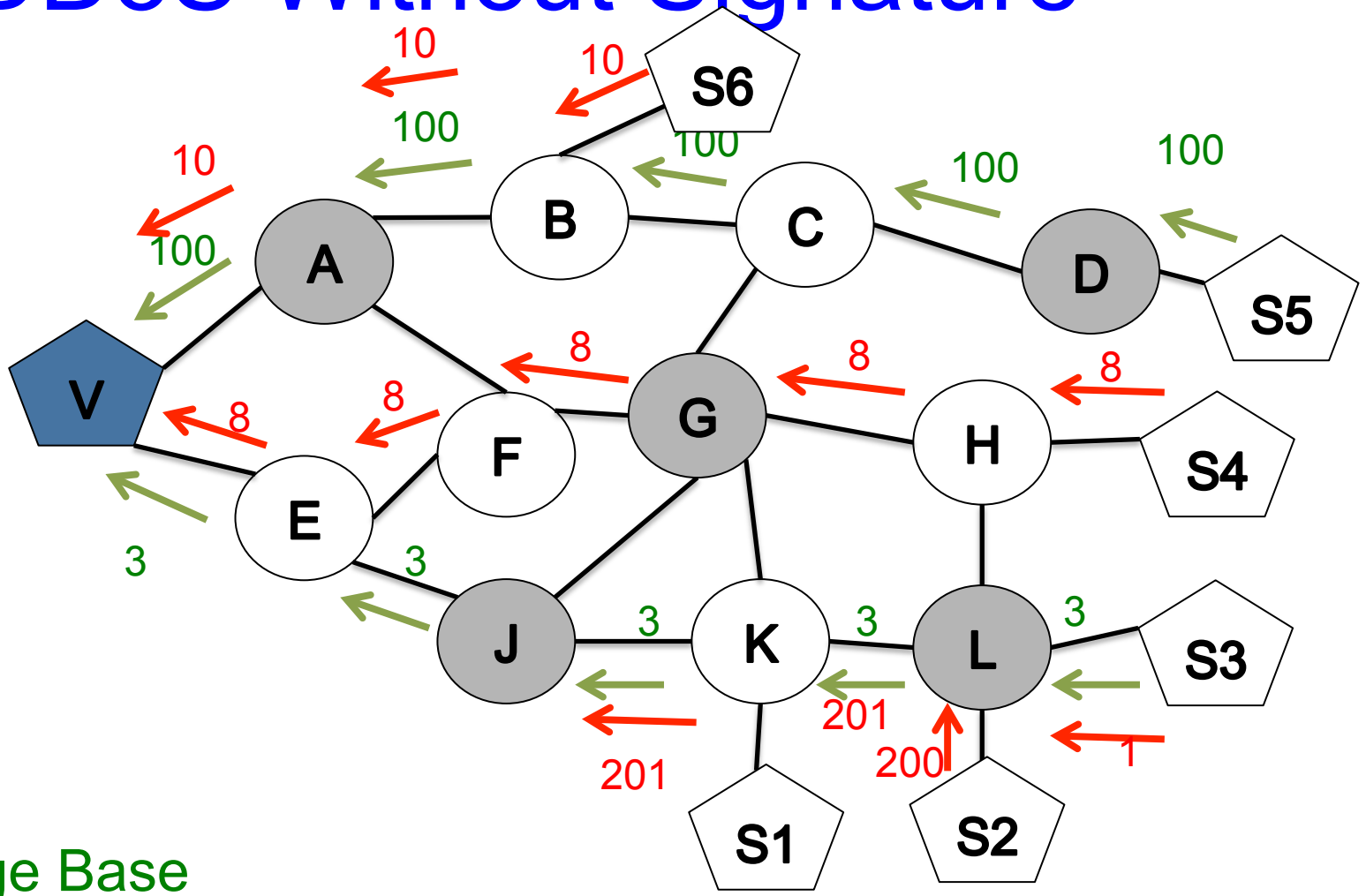


Knowledge Base

A:<B,100> D: <S4,100> G: <> J: <K,3> L:

A:<B,100> D: <S4,100> G: <H, 8> J: <K,205> L: <S3,3> <S2, 200>

DDoS Without Signature



Knowledge Base

A:<B,100> D: <S4,100> G: <> J: <K,3> L:

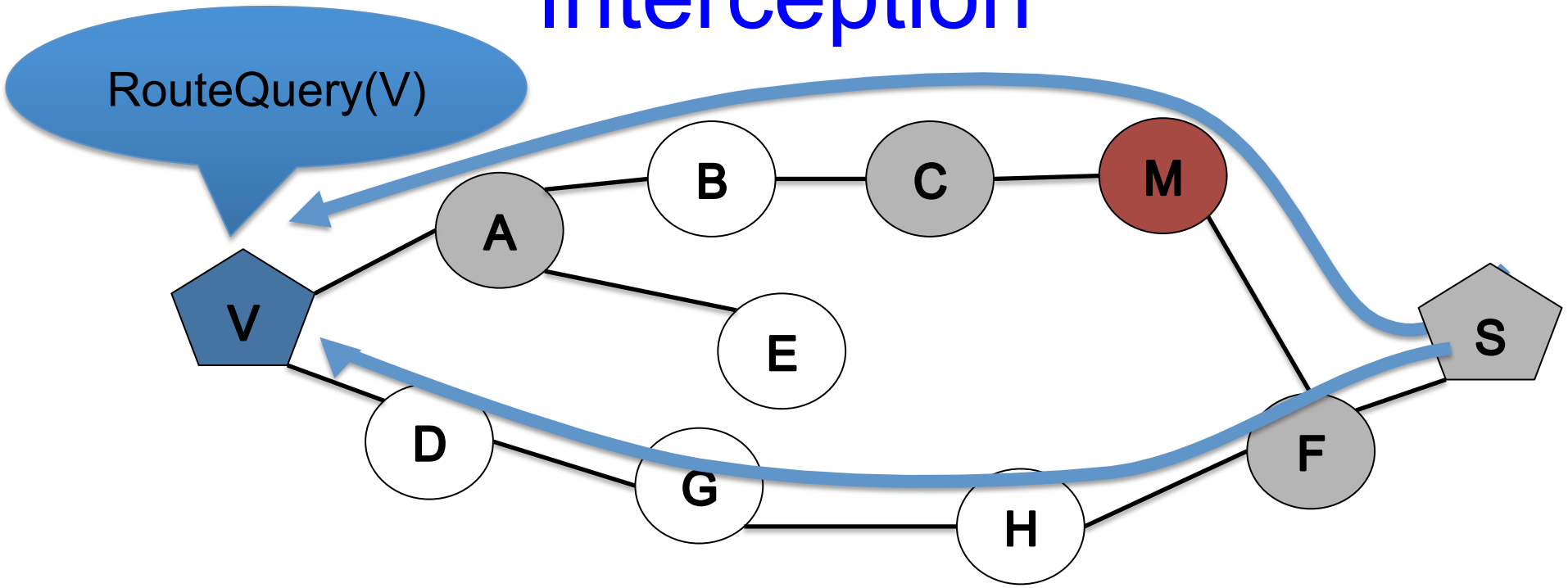
A:<B,100> D: <S4,100> G: <H, 8> J: <K,205> L: <S3,3>

<S2, 200>

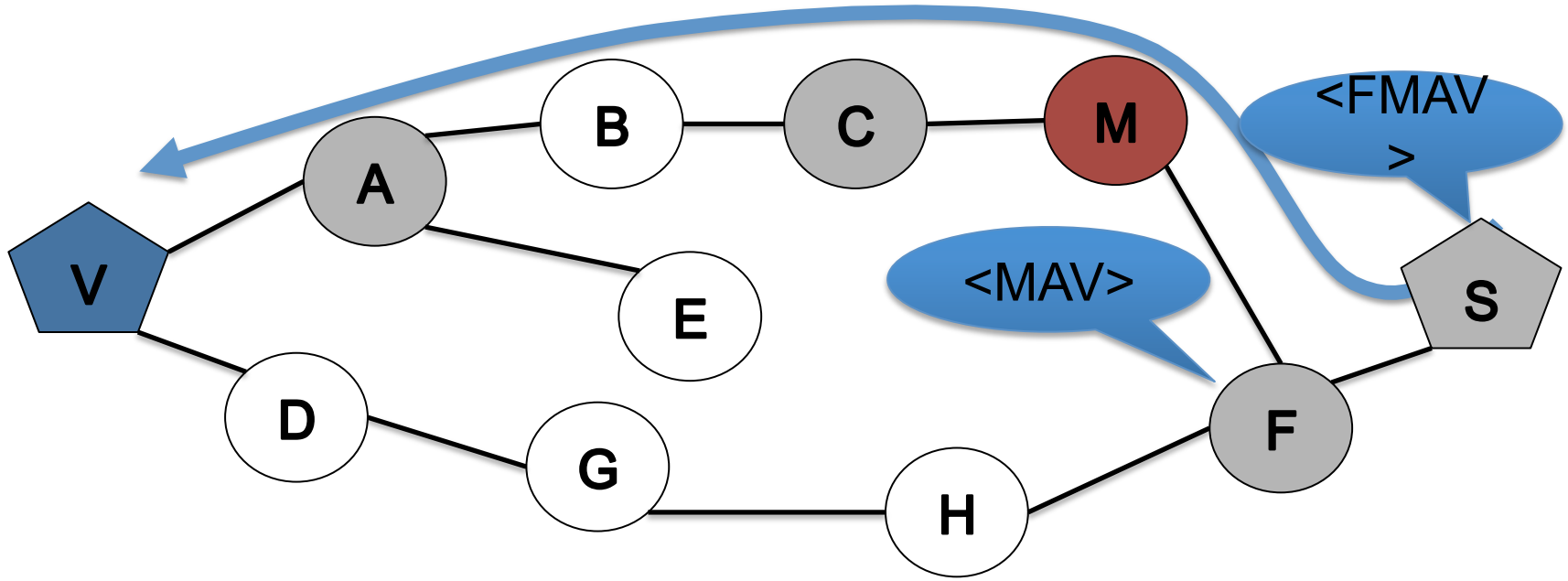
Interception Attacks

- Interception attacks
  - Introduce false information into the routing system
  - Claim shorter AS-PATH, hijack victim prefix
  - Traffic still reaches the victim
- Detection and mitigation
  - Data plane alone cannot reveal the root causes
  - Control plane info may be inaccurate or outdated
- SENSS: Check inconsistency between control and data planes via route and traffic query

Interception

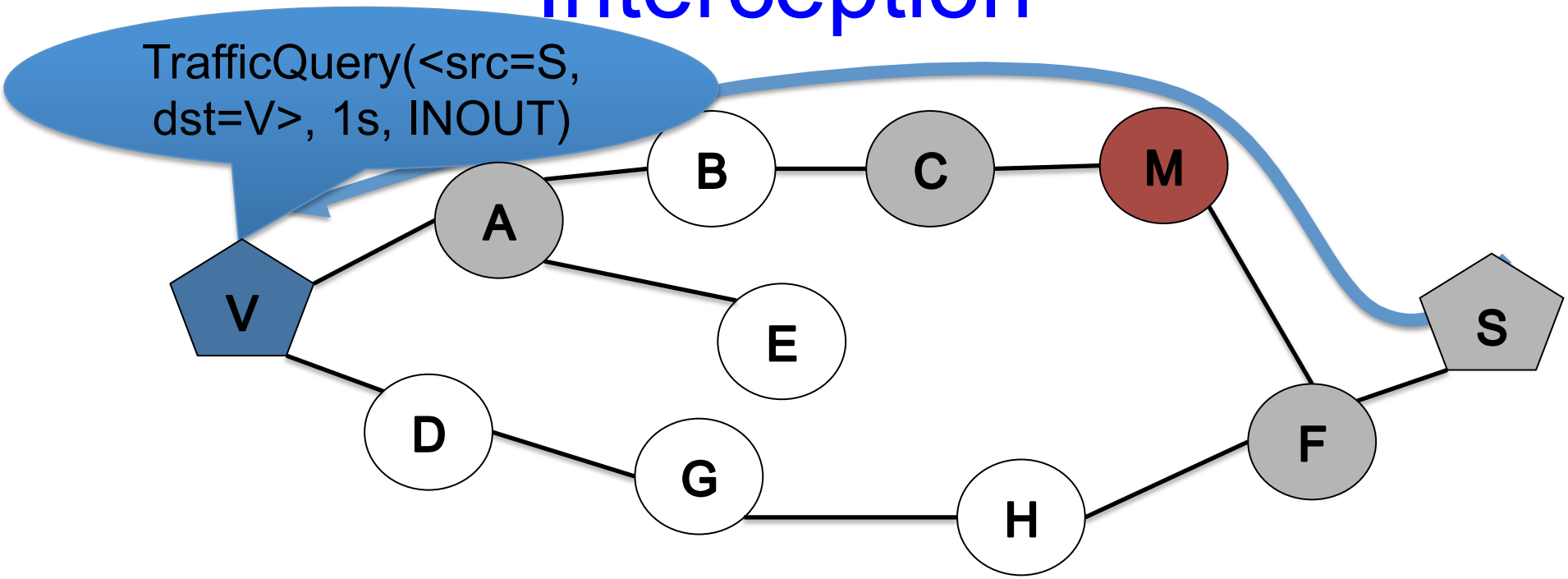


Interception



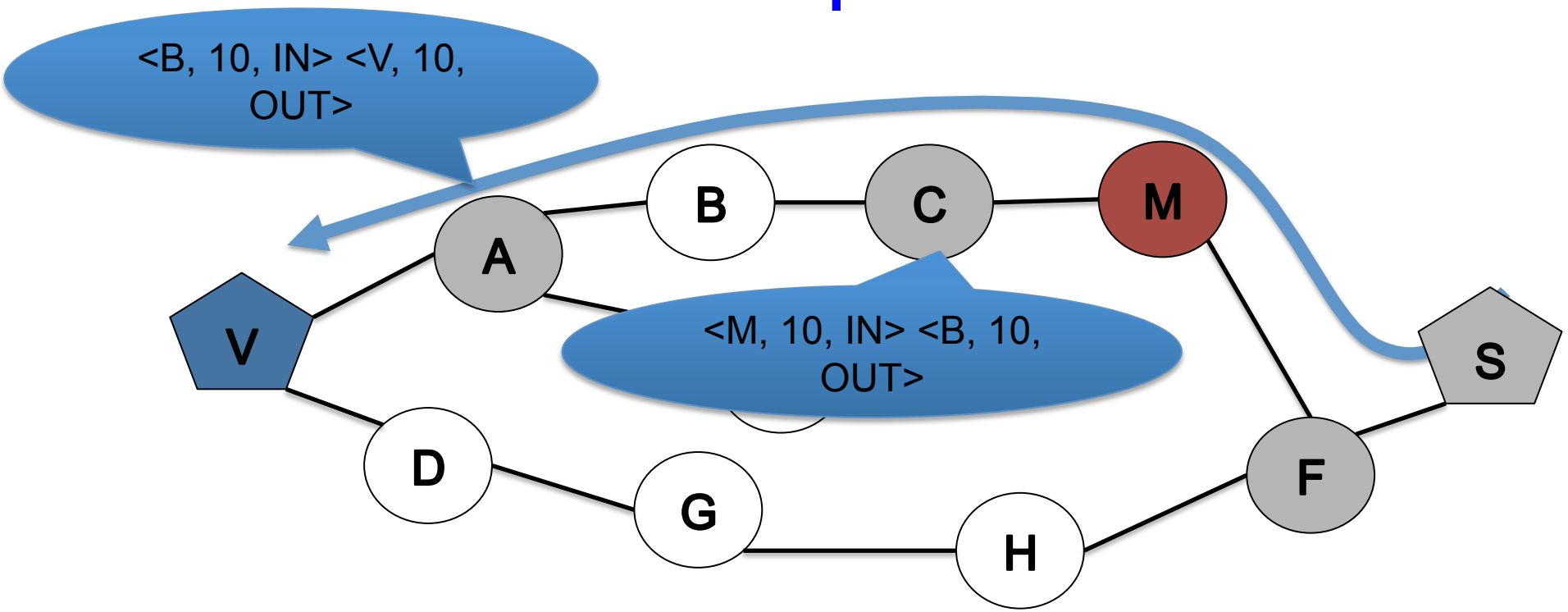
Knowledge Base
Control Plane
S to V: <FMAV>
F to V: <MAV>

Interception



Knowledge Base
Control Plane
S to V: <FMAV>
F to V: <MAV>

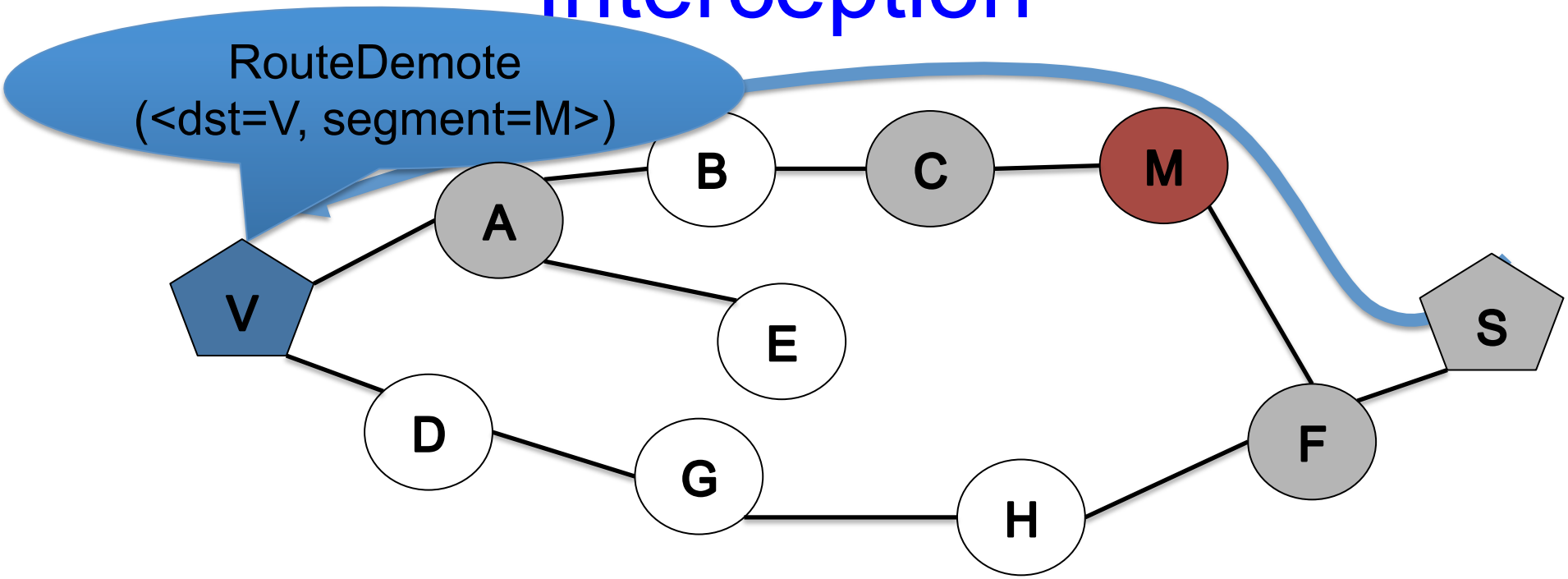
Interception



Knowledge Base
Control Plane
S to V: <FMAV>
F to V: <MAV>

Data Plane
Traffic from S to V passes through B and C!!

Interception



Knowledge Base

Control Plane

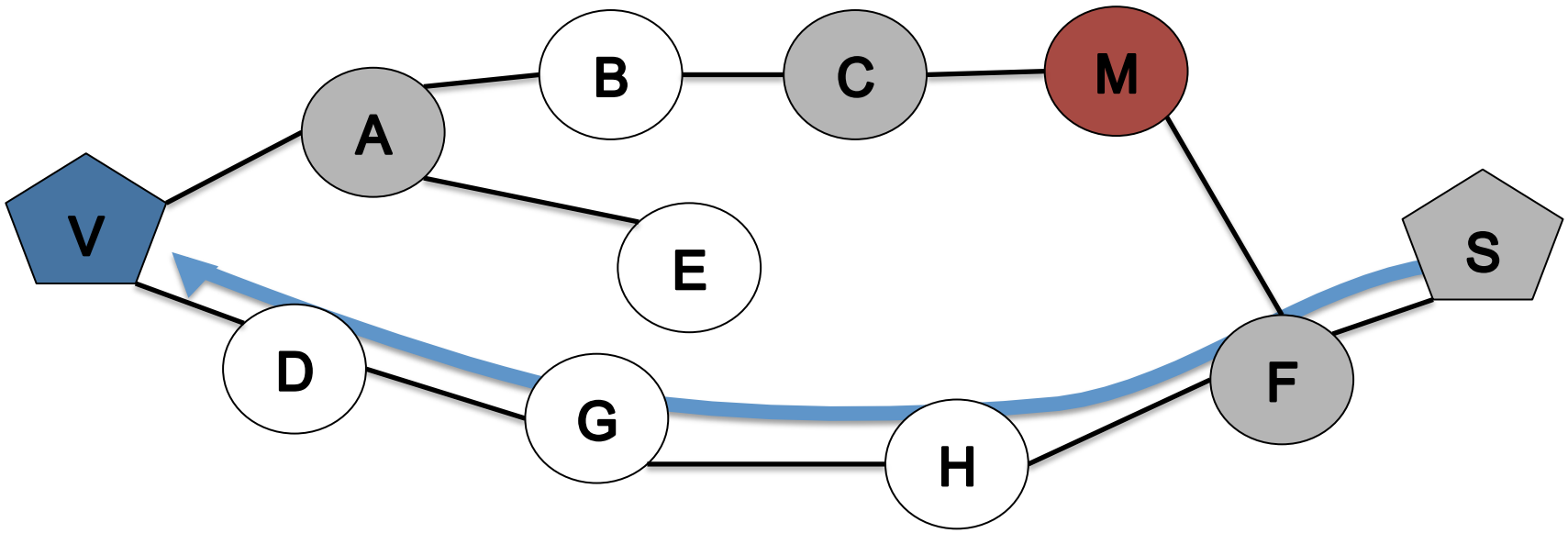
S to V: <FMAV>

F to V: <MAV>

Data Plane

Traffic from S to V passes through B and C!!

Interception



Knowledge Base

Control Plane

S to V: <FMAV>

F to V: <MAV>

Data Plane

Traffic from S to V passes through B and C!!

SENSS Use Cases

Attacks	Query	Control
DDoS w/ signature	Traffic queries	Traffic filter
DDoS w/o signature	Traffic queries	Traffic filter
DDoS reflection	Reduces to DDoS w/ or w/o signature	
Crossfire	Traffic queries	Bandwidth guarantees
Blackholing	Route queries	Route demotion
Interception	Route and Traffic queries	Route modification

Simulation Setup

- AS-Level Internet topology from RouteViews/ RIPE
  - 41K ASes with 92K links, including 11 Tier-1 ASes
- Simulate DDoS
  - Real traffic from CDN traces and DDoS attack traces
  - Simulated traffic with different distributions
- Simulate Prefix-Hijacking
  - Select victims and attackers from different tiers in the AS hierarchy

DDoS Results

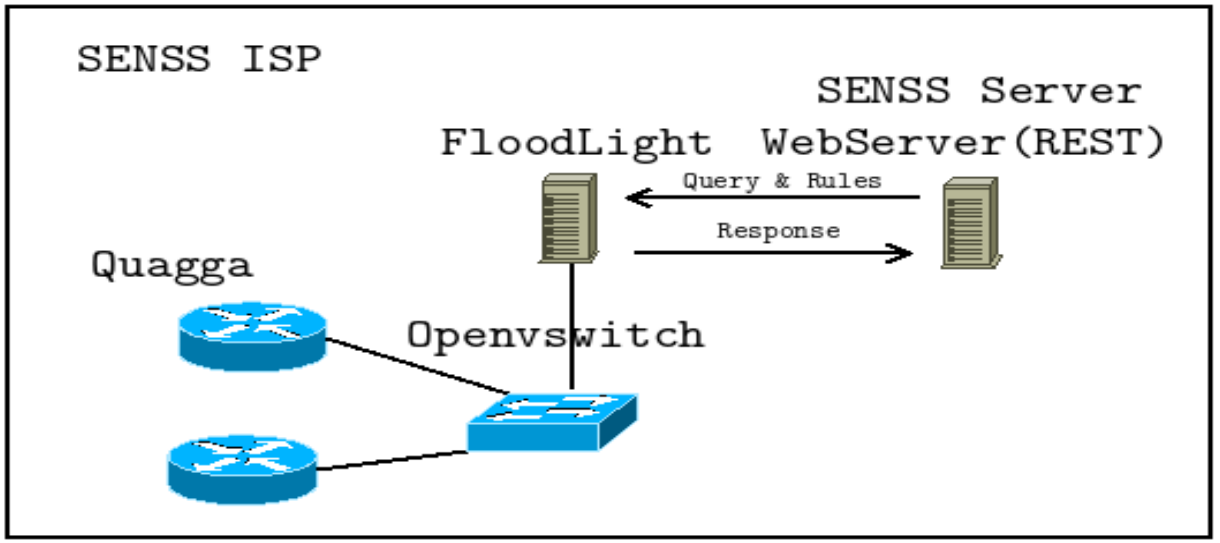
- Eliminate attack traffic
  - To eliminate 95% attack traffic
  - Need only 10-30 SENSS ASes
  - Less than 36 messages are needed
  - Hold for a wide range of traffic distributions
- Small collateral damage
  - Outperforms traceback solutions with the same # of deployed ASes

Prefix Hijacking Results

- Detection
  - With 30 ASes deployed, the detection accuracy can reach 90% for blackholing and 70% for interception
  - The median number of queries is 3-10 for blackholing and 6-15 for interception
- Mitigation
  - Correct > 80% of polluted Ases with 18 SENSS ASes

SENSS Implementation

- ISPs
  - Openvswitch as data plane, Quagga as control plane
  - Floodlight as controller for Openvswitch
  - Apache SENSS server
- Victim
  - Sends HTTPs requests to SENSS server
- Response time
  - 600 ms



Security and Privacy

- Security
  - Operations allowed on traffic from/to own prefixes and routes to own prefixes
  - Ownership verification via RPKI, communication via SSL
  - Outsource to cloud if victim has no path to SENSS server
- Privacy
  - ISPs only need to share traffic information for peer indexes, without revealing the actual peer
  - Routing information is already publicly available

Conclusion

- Software-defined security service
  - Simple, flexible interfaces at ISP
  - Victim-oriented programming for diverse attacks
- Practical security detection/mitigation services
  - Effective to mitigate large-scale attacks
  - Incentive for adoption from ISP and victims
  - Flexible for supporting new defenses for new attacks

Adopting SENSS

- We will release SENSS for deployment
  - Contact Minlan Yu (minlanyu@usc.edu)
- We want to hear from operators
  - What are your concerns in deploying SENSS?
  - Economics? Privacy? Effectiveness? Deployment?

http://www-bcf.usc.edu/~minlanyu/writeup/ons14-senss.pdf