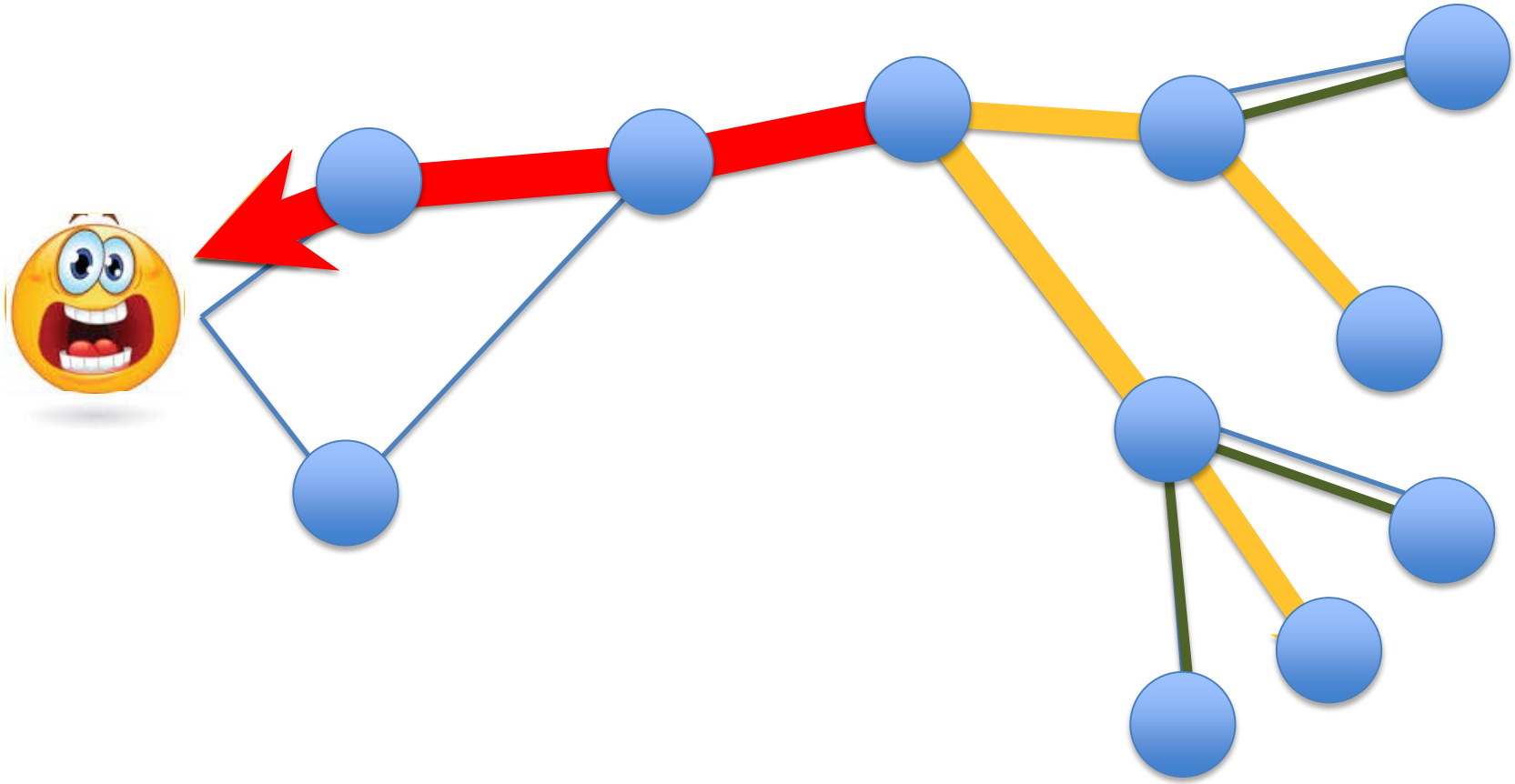
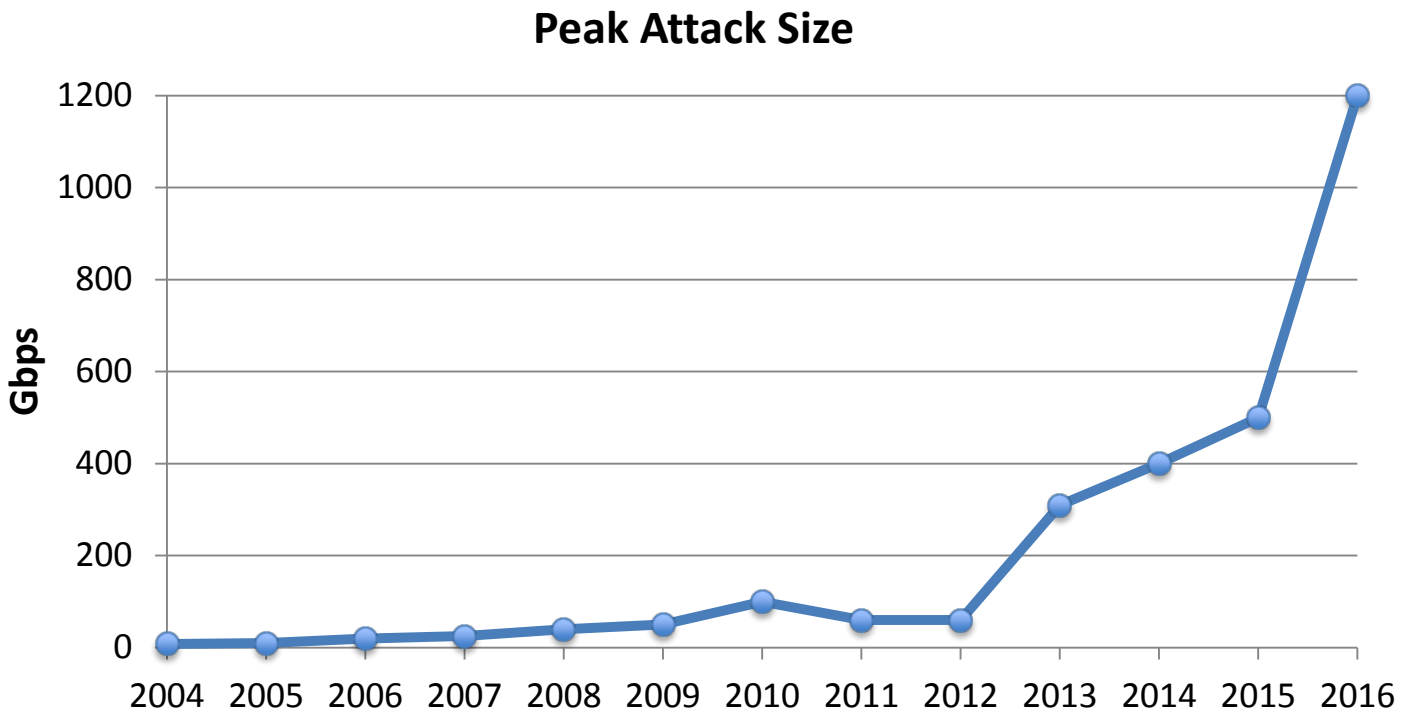
DDoS Defense for a Community of Peers

Jem Berkes (Project PI) and Adam Wick (Transition Lead)

About DDoS

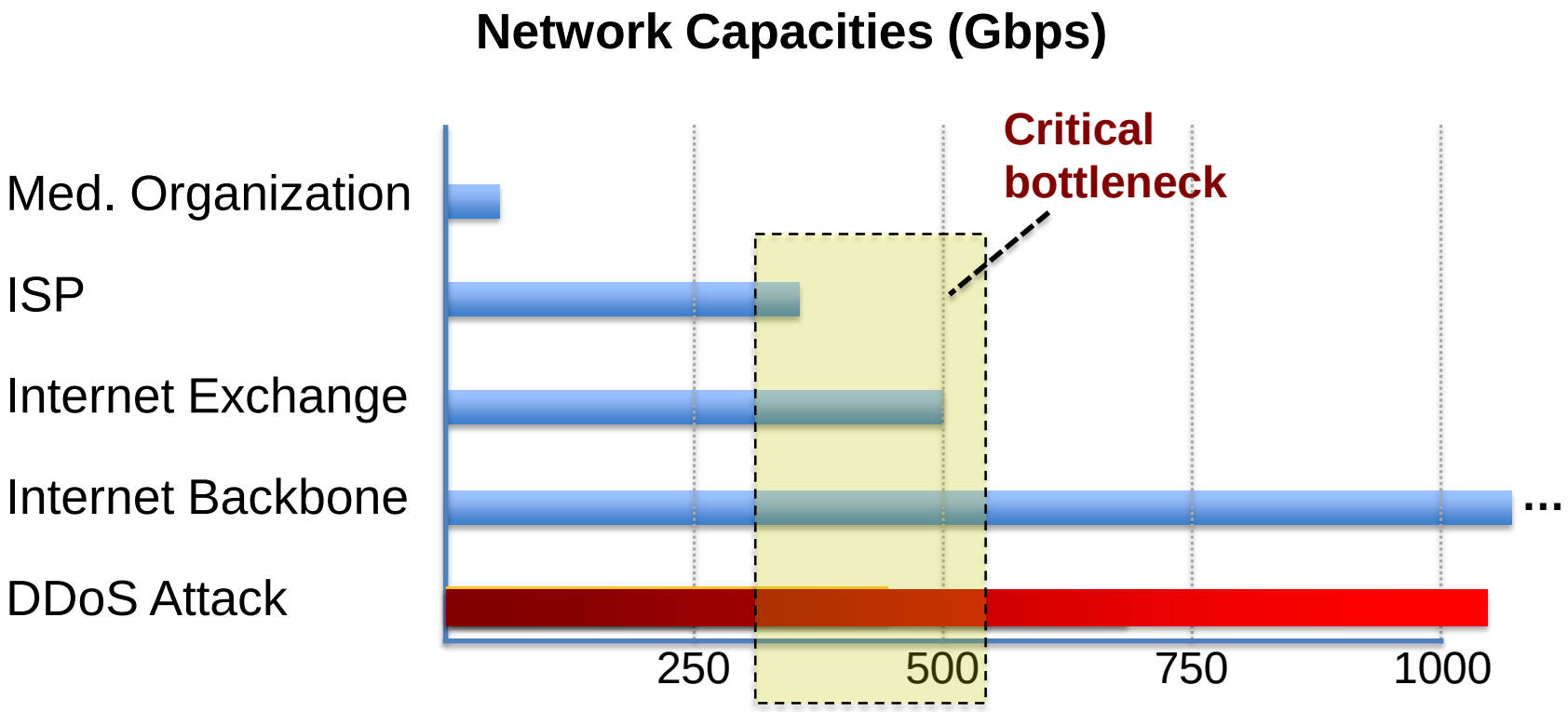
A DDoS Attack





Source data: Arbor Networks Worldwide Infrastructure Security Report, and recent media reports

When DDoS Becomes a Problem ...



Current Attacks Now Exceed Bottlenecks

- **Mirai / IoT botnets**
- **Enormous increase from 500 Gbps to 1,200+ Gbps**
- **Can’t stop this alone**
  - Tier 1 ISPs
  - Cloud providers – not immune
- **Aggregate, world-wide capacity is not the issue**

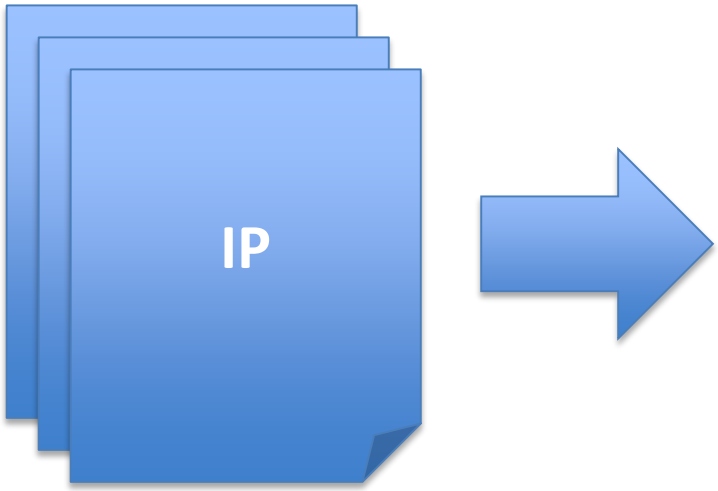
Networks Must Collaborate

- **Effective defense requires collaboration between networks**
- **Must stop traffic closer to sources**
- **Automate response/coordination under attack stress**

We're creating a tool to do this – 3DCoP

Handling DDoS with 3DCoP

Flow representation of traffic



SRCIP	SPORT	DSTIP	DPORT	PROTO	COUNT
…	…	…	…	…	…
…	…	…	…	…	…
…	…	…	…	…	…

- Big
- Packet bodies

- Compact summary
- NetFlow, IPFIX

Our approach

- **Decentralized collaboration between networks**
- **Share flow information (clues) from distributed sensors via P2P**
- **Use clues to compute**
  - Sources of attacks
  - Spoofed traffic
  - Optimal blocking

Decentralized P2P Network

- **Out-of-band P2P**
- **Can operate using cell phone tethering – during attack**
- **IPFS: Kademlia-based DHT swarm**
    - Every node has public key

What is shared?

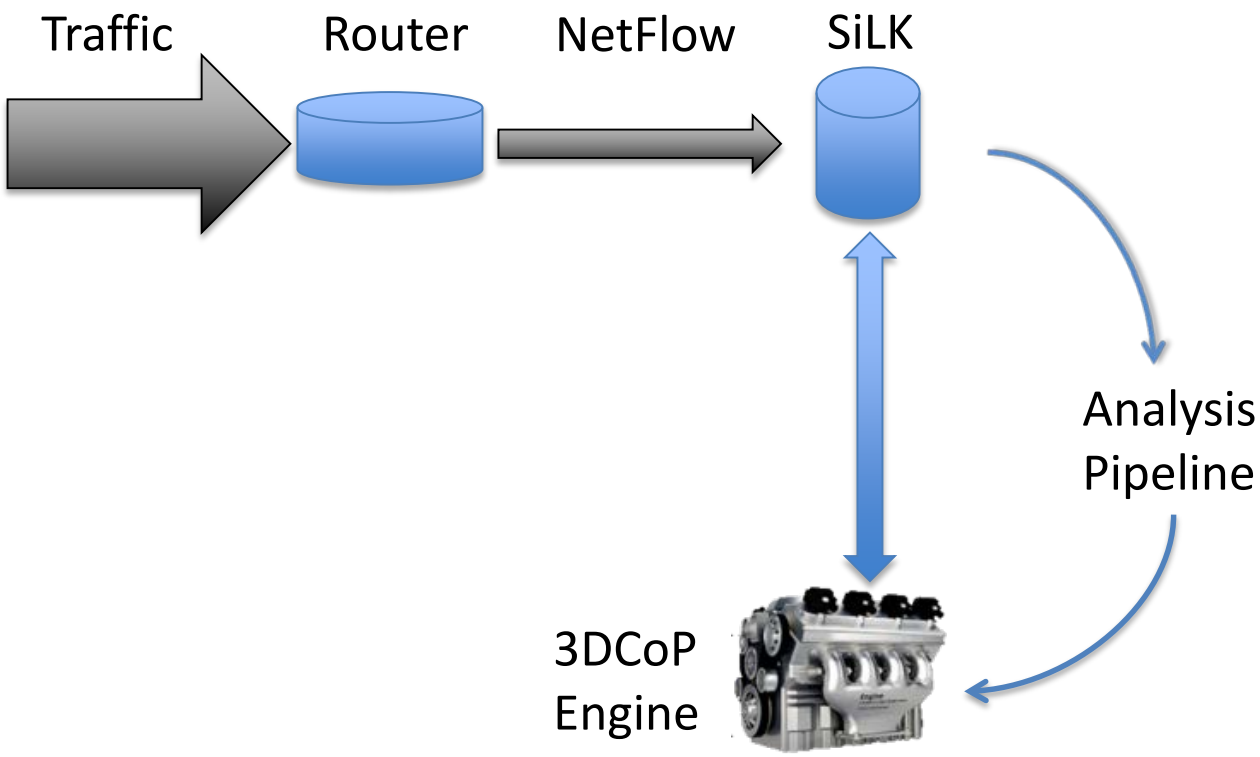
- **Subset of flow data, classified as**
  - Anomalies
  - Undesirable traffic (attacks)
  - Assertions: present or not present
- **Each node pushes data**
  - Decide what you want to share

Who is it shared with?

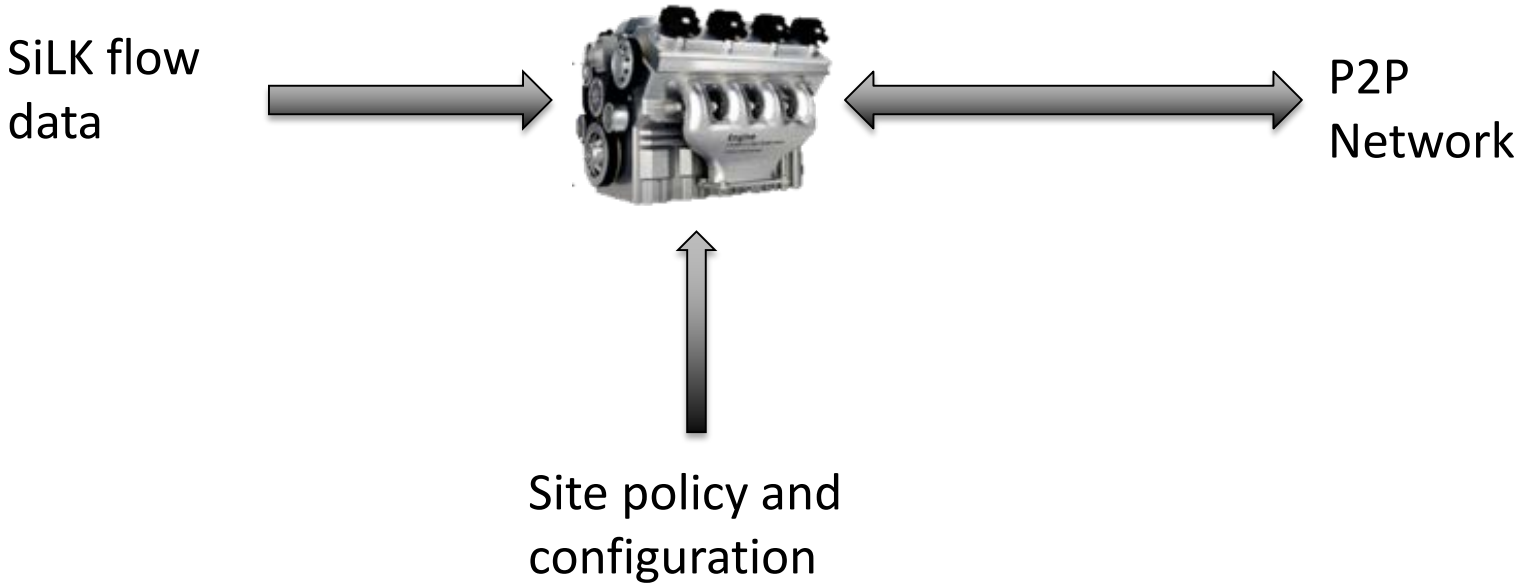
- **Strict/private mode**
  - Flow data only shared with owner of flow endpoint
  - Enforced with public key cryptography
- **Global announcements**
  - For very anomalous traffic, or attacks
- **Groups/associations**

Each site always controls what they share, and with whom

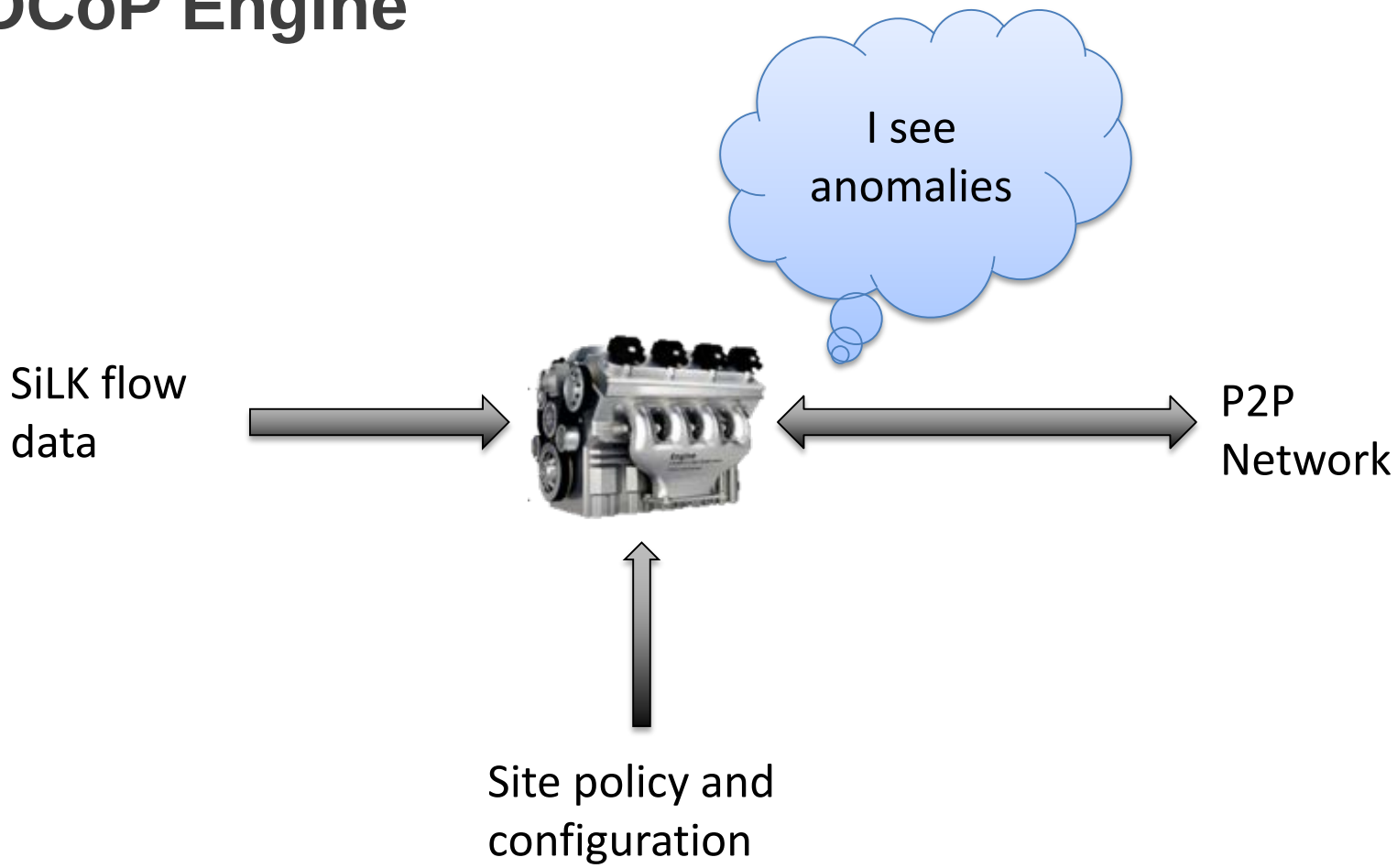
Data Processing



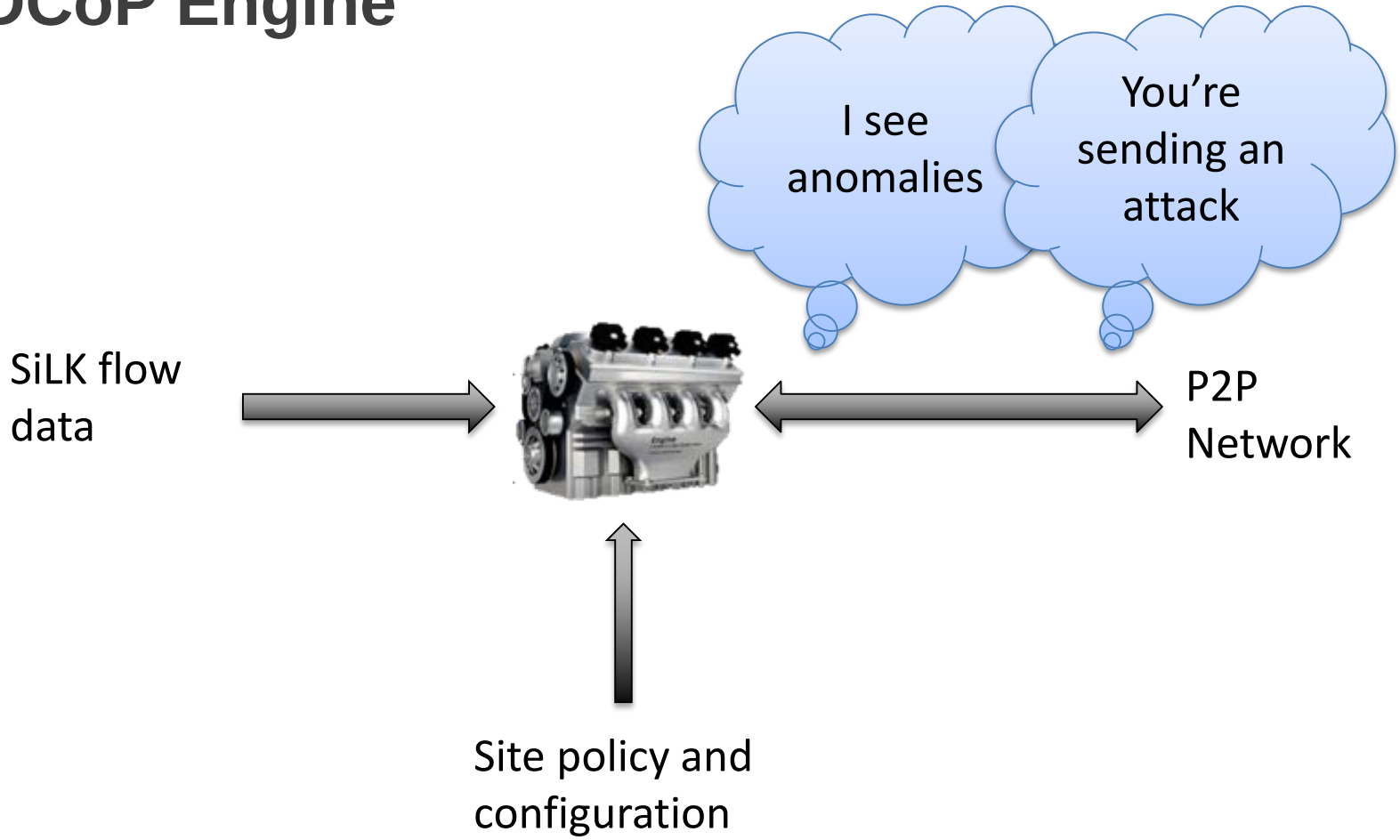
3DCoP Engine



3DCoP Engine



3DCoP Engine



Engine

- **State tables**
  - Local anomalies, peer-reported anomalies, etc.
- **Rules-based algorithm**
- **State iterations with real-time updates**
- **Automatic traffic analysis leading to actions**

Rules in the Engine

```
if I see anomalous outbound flows
   and others report anomalies from me
then

      increase oddness score for flows
```

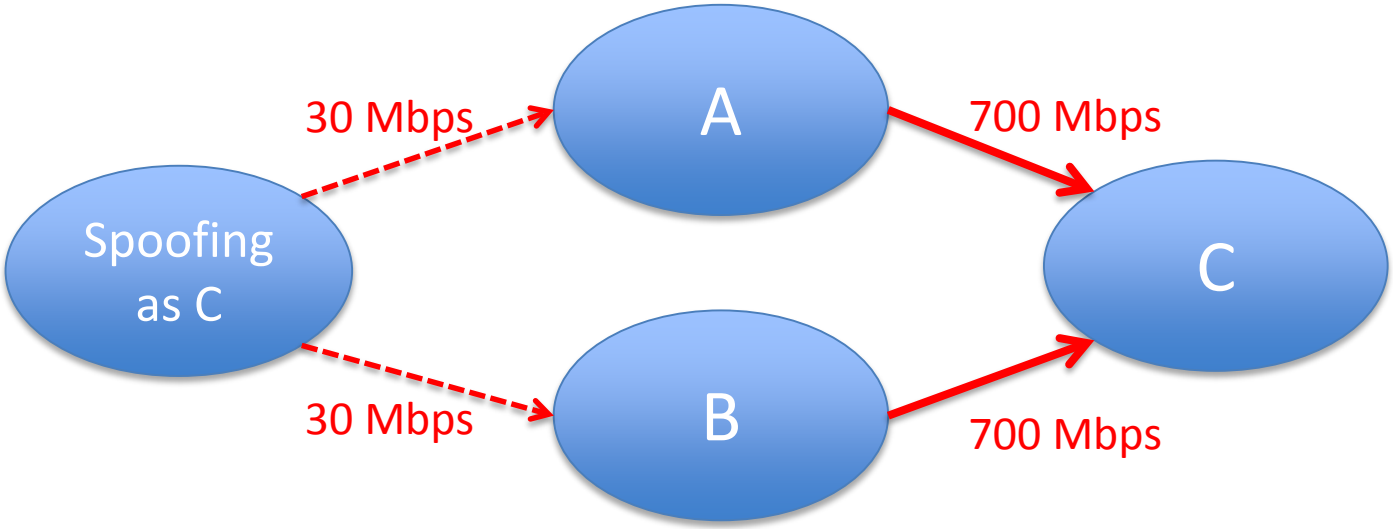
```
foreach anomalous flow

      if oddness score > THRESHOLD
         and network utilization is high
         and many src_ip are sending to few dst_ip
      then

                promote anomaly to attack
```

More Rules…

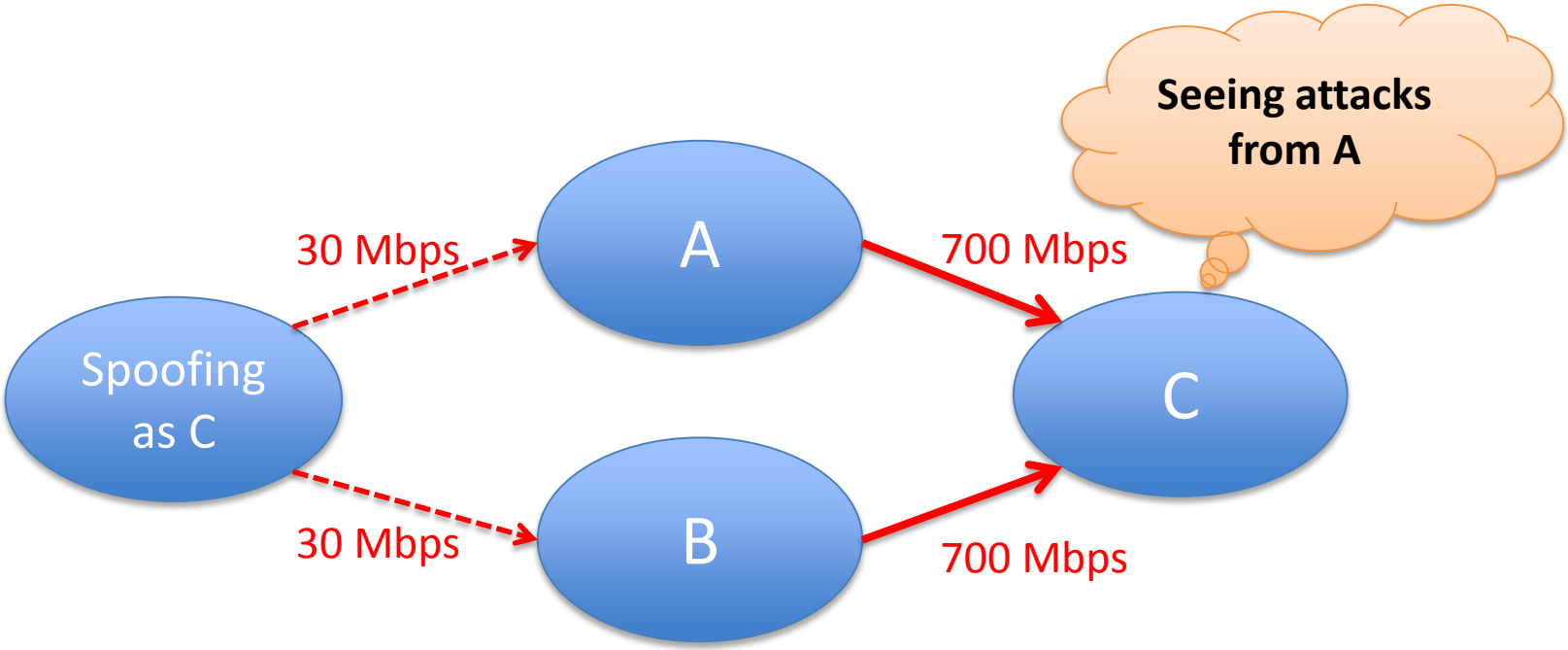
```
foreach peer-reported anomaly

        if local anomaly matches port number
        then
                // might be related attack
                if port is a known amplifier service
                then

                        increase oddness score
                        // we might all be part of
                        // the same DDoS attack
```

Example

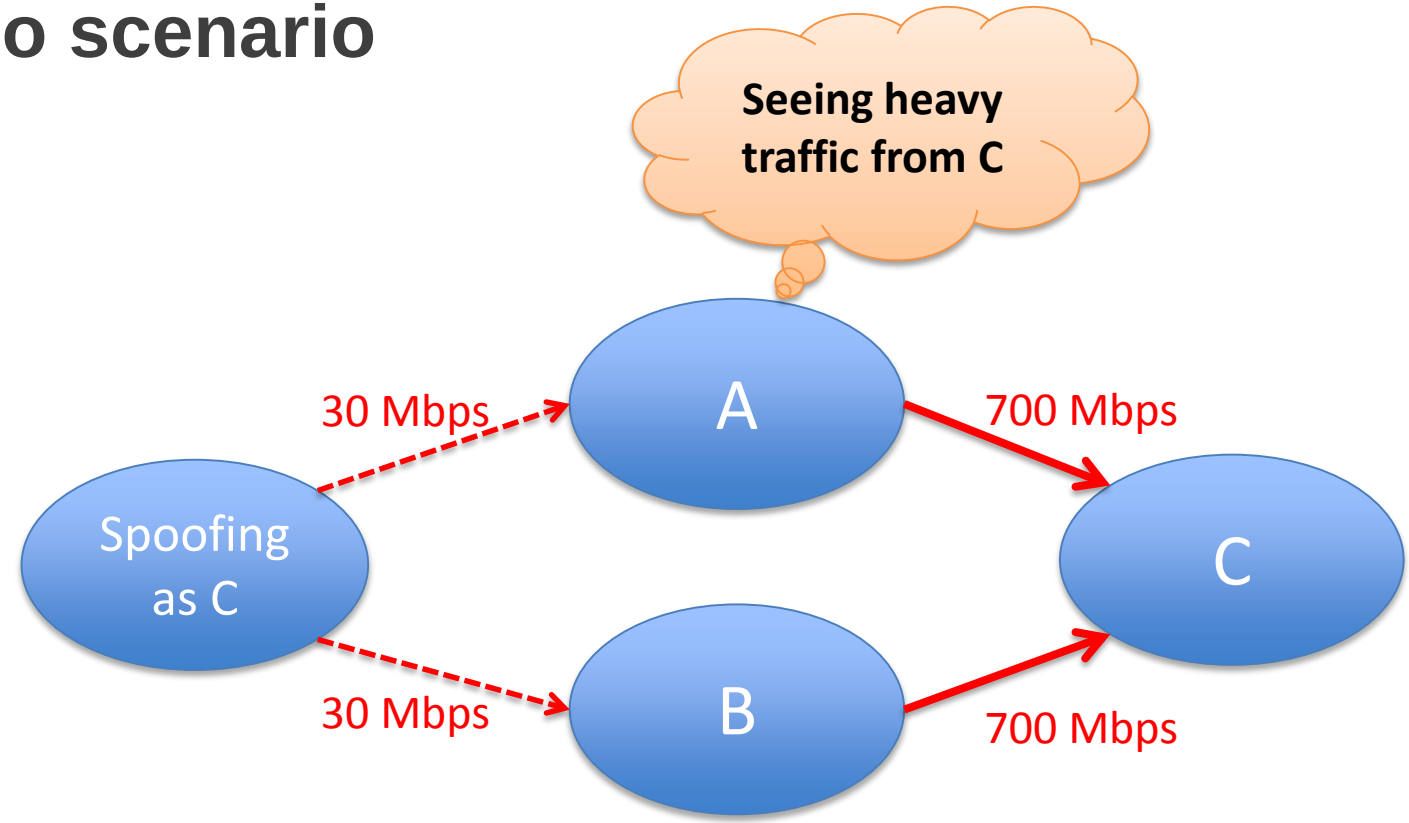
Demo scenario



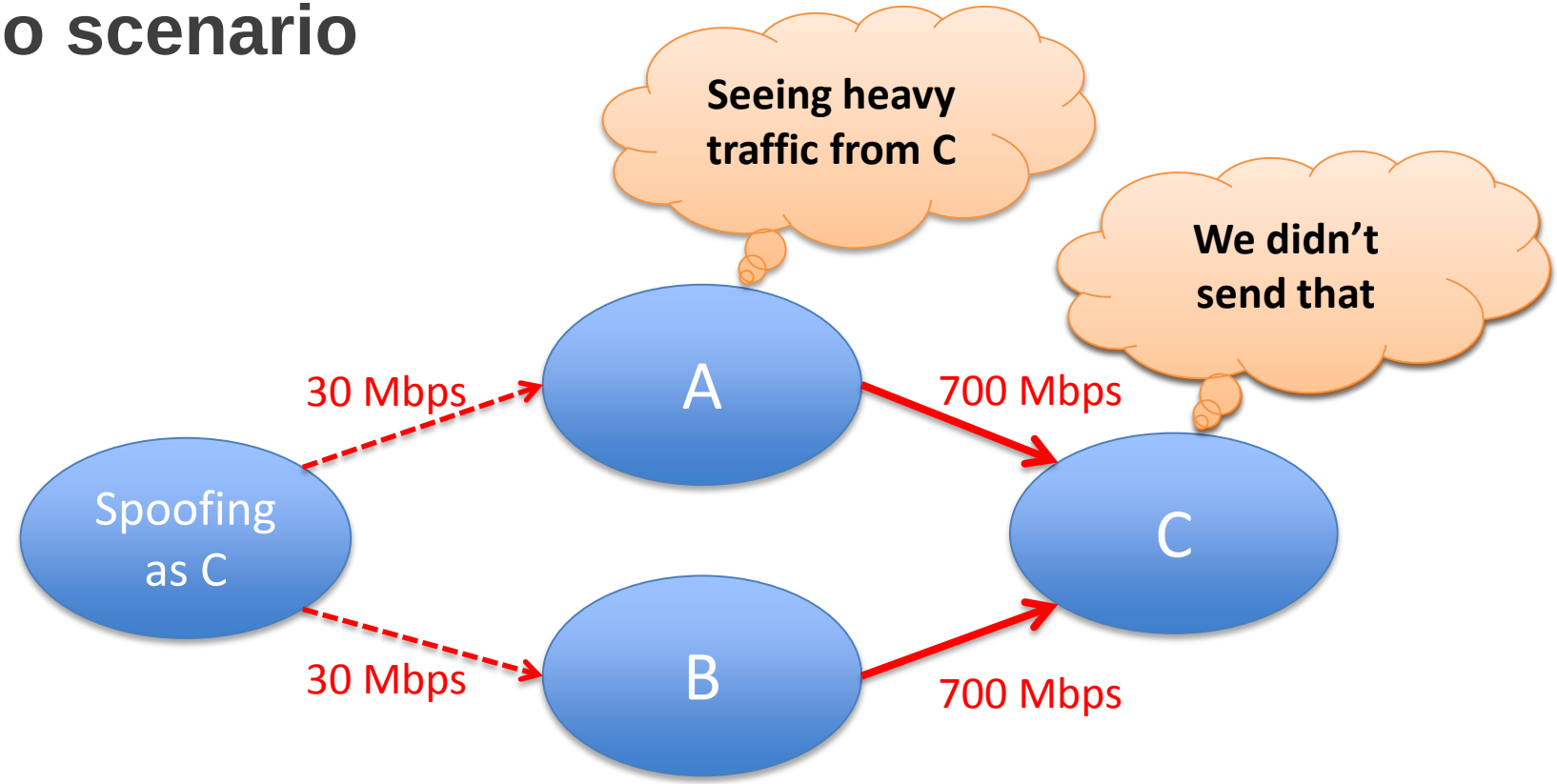
Demo scenario



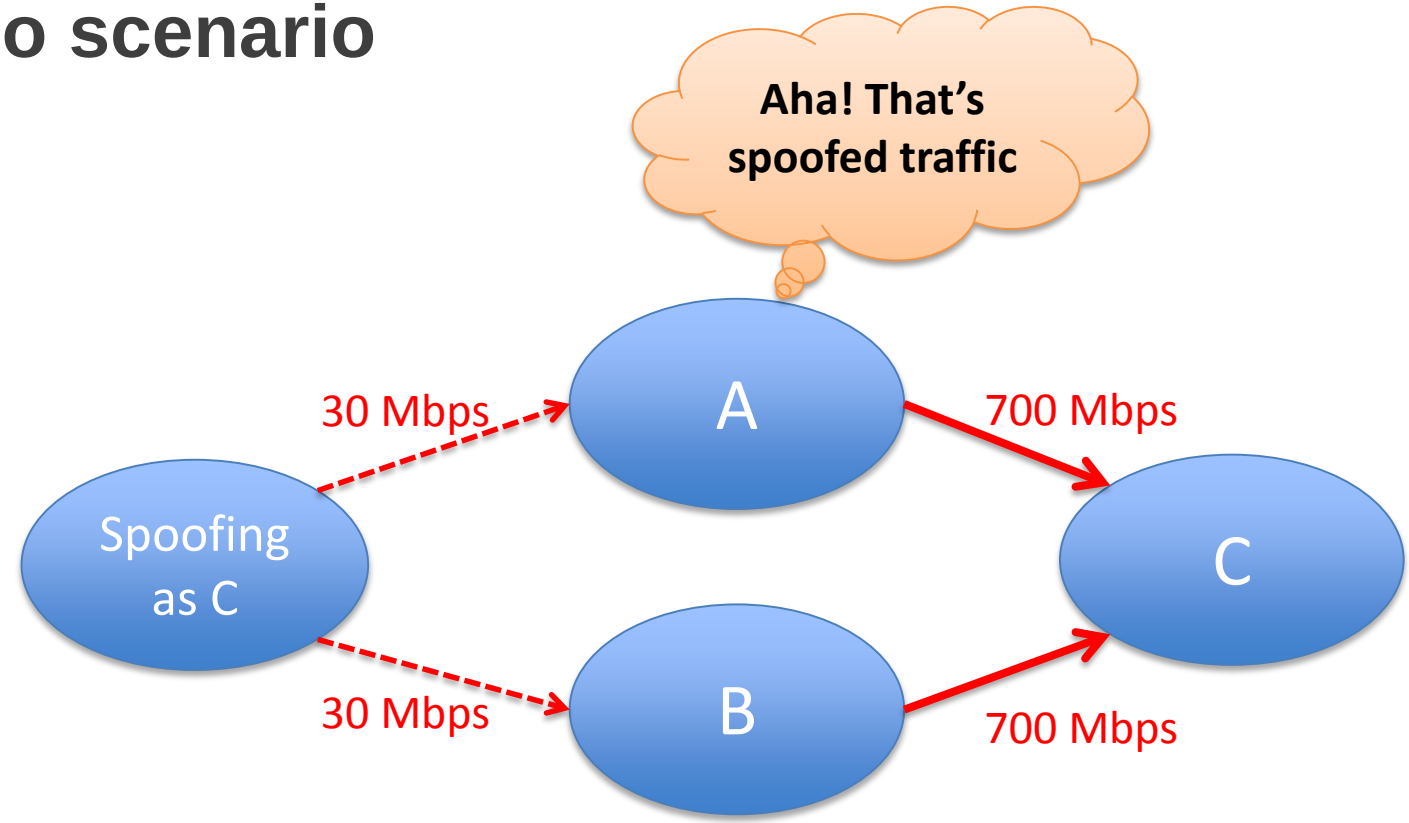
Demo scenario



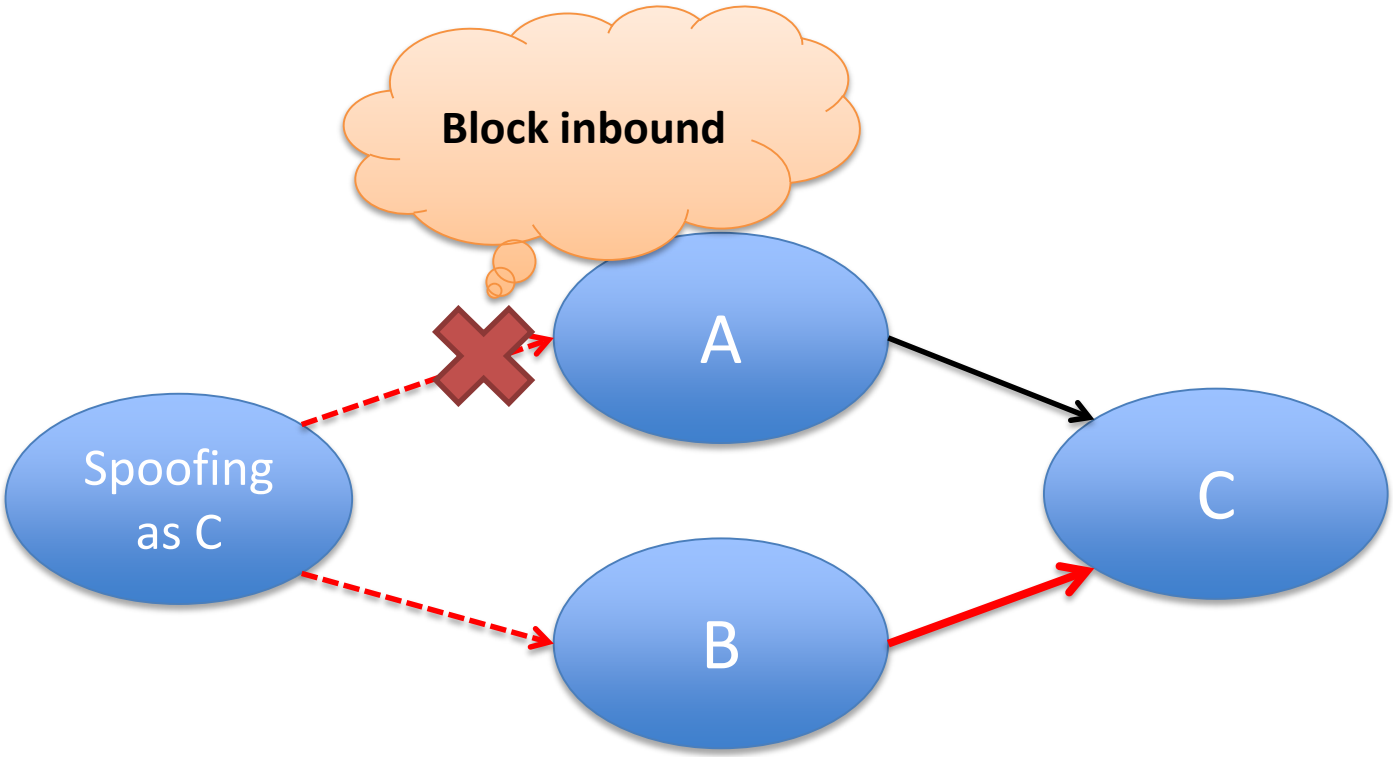
Demo scenario



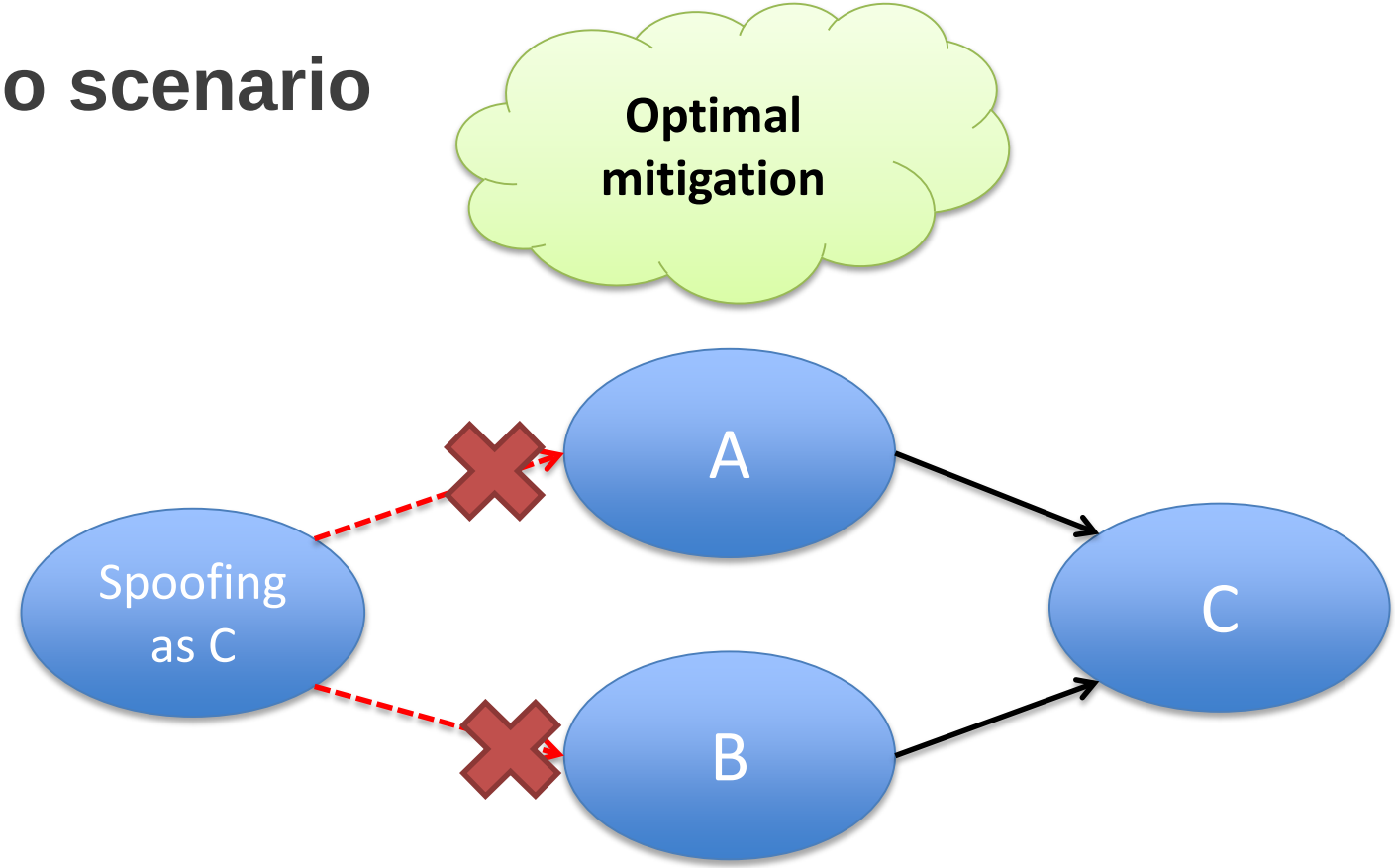
Demo scenario



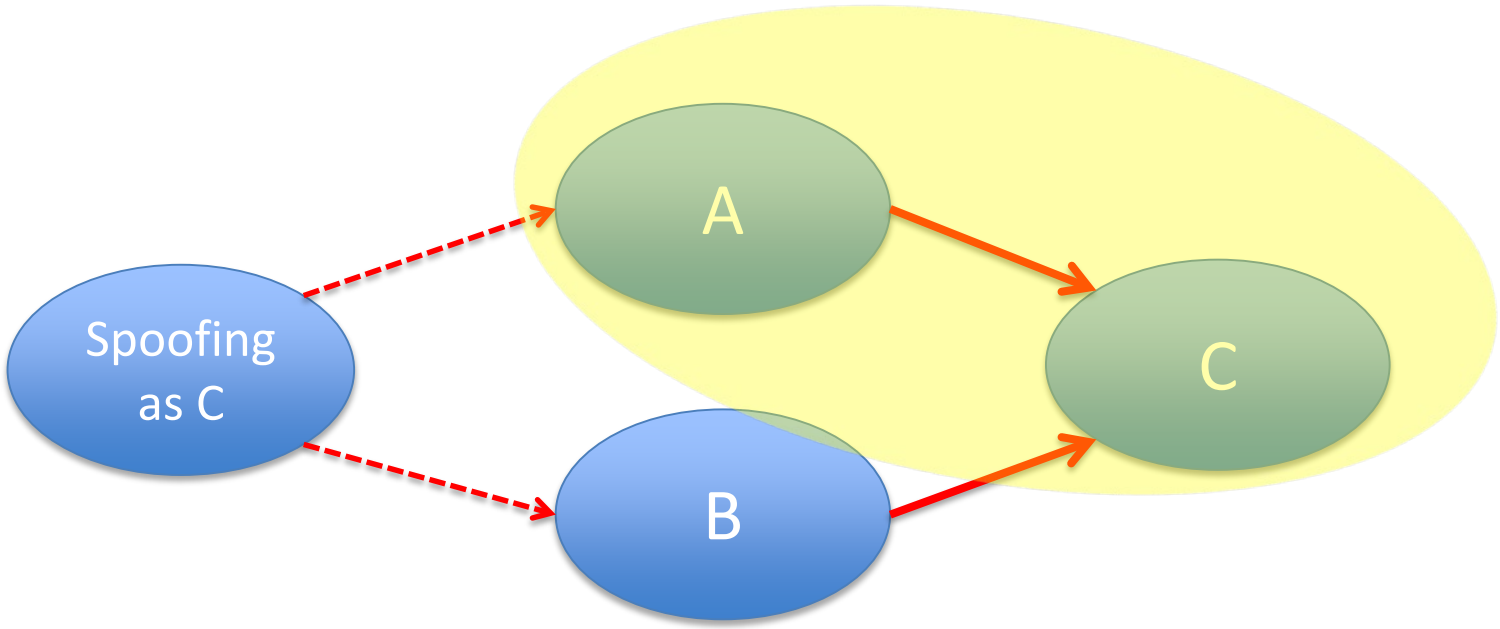
Demo scenario



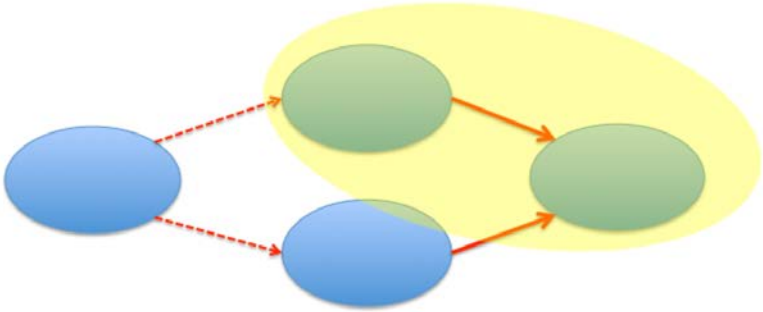
Demo scenario



Demo scenario

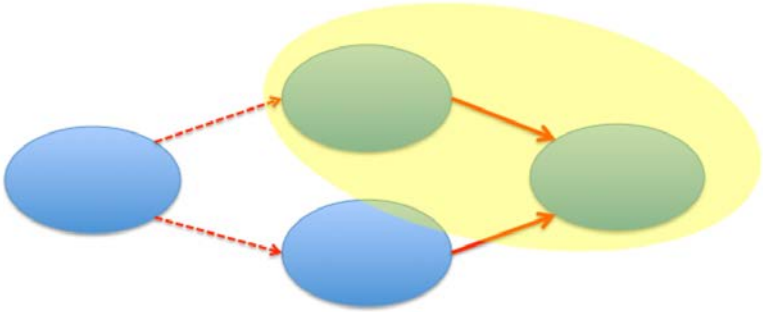


State Iterations



Network containing A (amplifier)	Network containing C (victim)

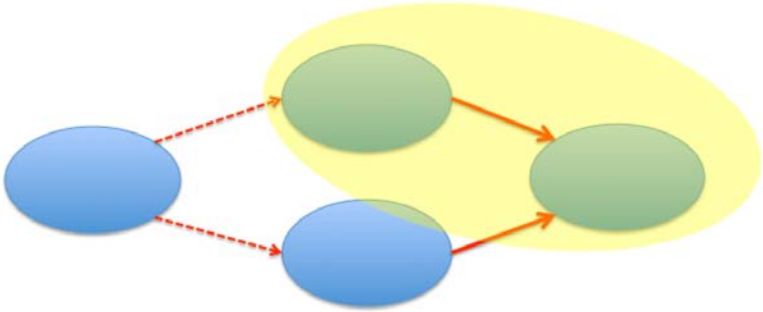
State Iterations



Network containing A (amplifier)
Inbound Anomalies C --> A Outbound Anomalies A --> C

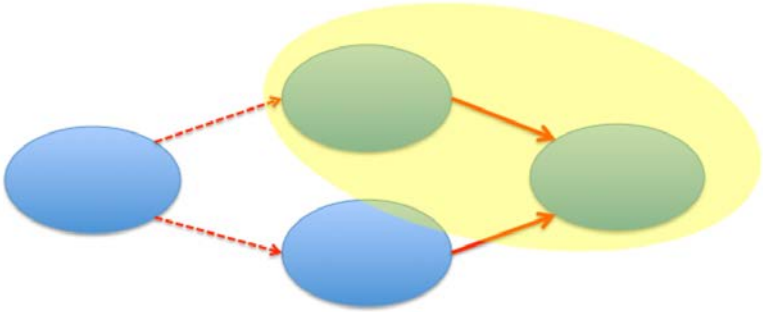
Network containing C (victim)
Inbound Attacks A --> C

State Iterations



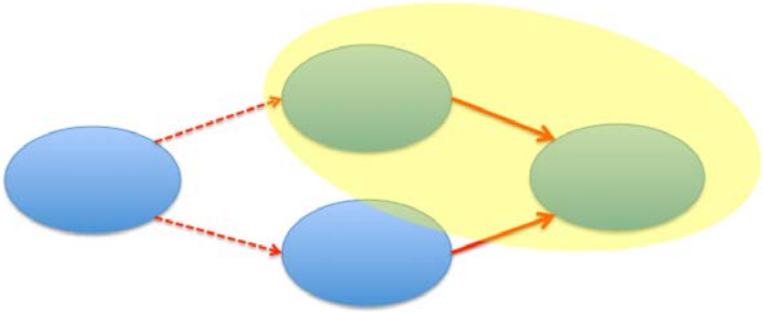
Network containing A (amplifier)	Network containing C (victim)
Inbound Anomalies C --> A Outbound Anomalies **A --> C**	Inbound Attacks **A --> C**

State Iterations



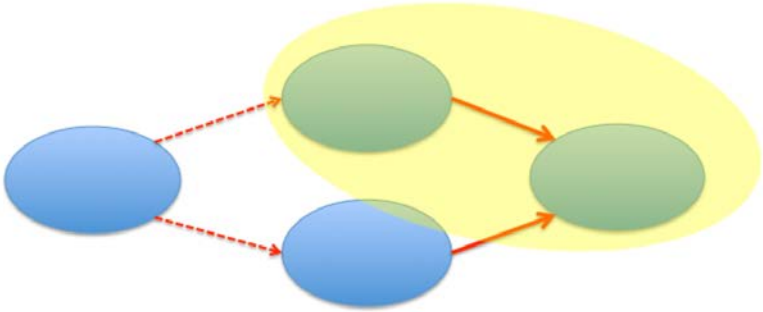
Network containing A (amplifier)	Network containing C (victim)
Inbound Anomalies C --> A Outbound **Attacks, Must Stop** A --> C	Inbound Attacks A --> C

State Iterations



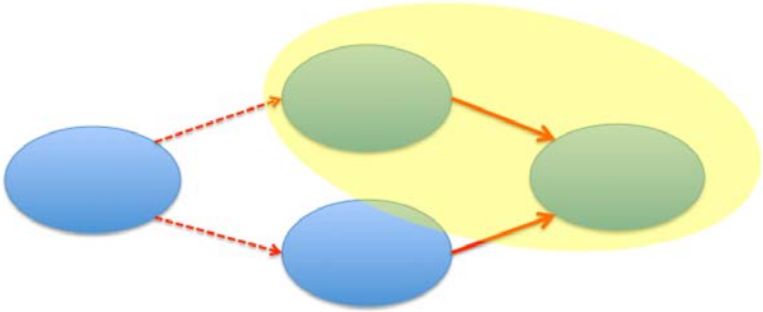
Network containing A (amplifier)	Network containing C (victim)
Inbound Anomalies C --> A Outbound Attacks, Must Stop A --> C	Inbound Attacks A --> C Check flow repository…

State Iterations



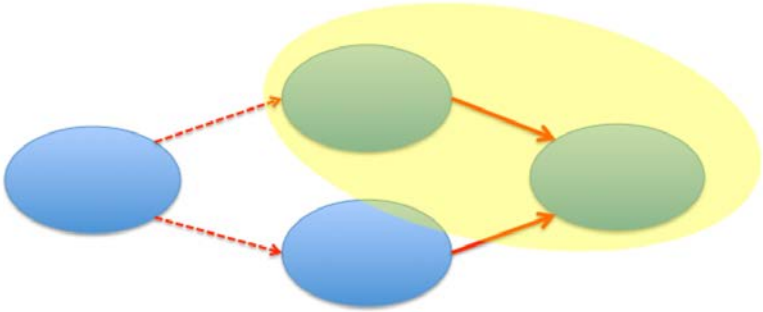
Network containing A (amplifier)	Network containing C (victim)
Inbound Anomalies C --> A Outbound Attacks, Must Stop A --> C **Assertions that Peers Did Not Send** **C --> A**	Inbound Attacks A --> C **Someone is spoofing my IP** **C --> A**

State Iterations



Network containing A (amplifier)	Network containing C (victim)
Inbound Spoofed Attacks C --> A Outbound Attacks, Must Stop A --> C Assertions that Peers Did Not Send C --> A	Inbound Attacks A --> C Someone is spoofing my IP C --> A

We’ve learned a lot!



Network containing A (amplifier)
Inbound Spoofed Attacks C --> A Outbound Attacks, Must Stop A --> C Assertions that Peers Did Not Send C --> A

Network containing C (victim)
Inbound Attacks A --> C Someone is spoofing my IP C --> A

We've learned a lot!

Network containing A (amplifier)
Inbound Spoofed Attacks C --> A Outbound Attacks, Must Stop A --> C Assertions that Peers Did Not Send C --> A

Vital information
learned through
collaboration

What About Mischief and Lies?

- **We have considered this**
- **Peers make statements about their own traffic**
  - “I don’t want this traffic”
- **Public key crypto ties ownership/responsibility**

Status

Status

- **Have an early prototype**
  - ***We are seeking pilot and evaluation partners.***
- **Correctly computes results with a simple attack**
  - Identifies attack sources
  - Identifies spoofed traffic

Next steps

- **Construct larger, more complex attack scenarios**
- **Develop the engine further**
  - Accuracy
  - Better reasoning

Contact Us!

Jem Berkes: jberkes@galois.com

Galois 3DCoP Team: ddos@galois.com

We are actively seeking evaluation partners for 3DCoP. Please contact us if you'd be interested in trying 3DCoP out in your organization.

This project is the result of funding provided by the Science and Technology Directorate of the United States Department of Homeland Security under contract number D15PC00185. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Department of Homeland Security, or the U.S. Government.