

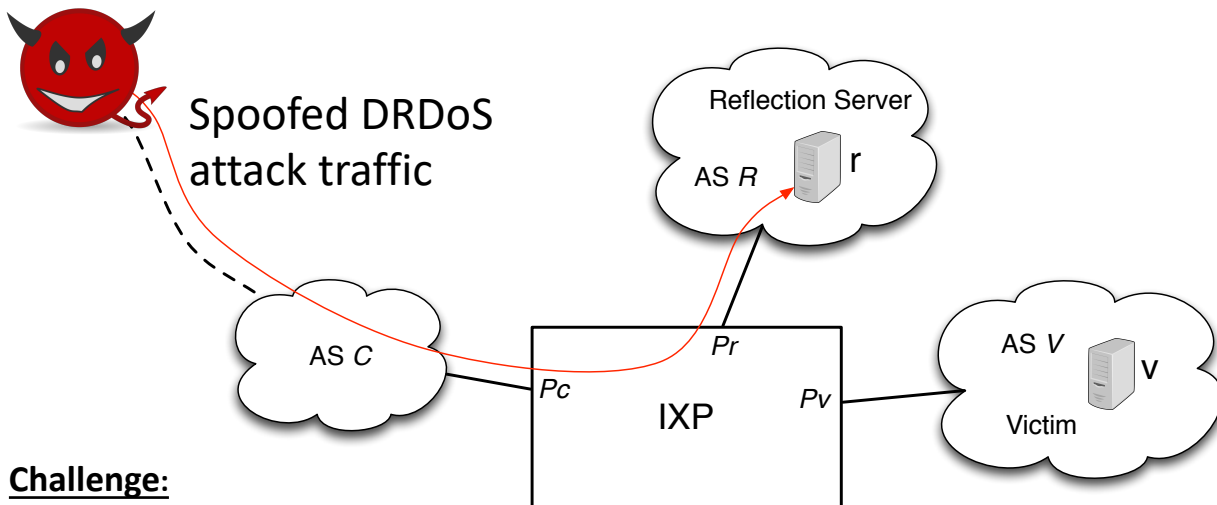
# EAGER: Collaborative: Leveraging High-Density Internet Peering Hubs to Mitigate Large-Scale DDoS Attacks



NSF CNS #1741608

UGA Lead PI: Roberto Perdisci ([perdisci@cs.uga.edu](mailto:perdisci@cs.uga.edu))

GaTech PI: Maria Konte ([mkonte@gatech.edu](mailto:mkonte@gatech.edu))



## Challenge:

- Volumetric DRDoS attacks can completely overwhelm a victim network
- How can we filter out DRDoS attack traffic upstream, so that the target AS's bandwidth is not exhausted?

## Solution:

- Build a DDoS defense that can be deployed at IXPs
- Filter DRDoS traffic at IXPs where the victim (or its upstream providers) peers with other networks

## Scientific Impact:

- Develop DRDoS defense based on anomaly detection
- Learn how traffic normally crosses the IXP
- Detect spoofed DRDoS traffic by detecting anomalous traffic routing paths
- Block DRDoS attack traffic before it reaches the victim (selective blackholing)

## Broader Impact:

- Open-source DRDoS defense system specifically for IXPs
- IXP operators can collectively defend DRDoS victims
- Significant contribution to improving Internet security

AS-to-Port Matrix

Before Spoofed Traffic

	Pc		Pv	
AS V	0	0	0	0

After Spoofed Traffic

	Pc		Pv	
AS V	0	0	0	0

Detailed description of the AS-to-Port Matrix: The matrix shows traffic flow between AS V and two peering paths, Pc and Pv. In the 'Before Spoofed Traffic' state, all traffic is zero. In the 'After Spoofed Traffic' state, traffic is introduced. On the Pc path, a red 'Y' appears in the cell for AS V, indicating spoofed traffic. On the Pv path, a blue 'W' appears in the cell for AS V, indicating legitimate traffic. The other cells remain zero.