**Real-time DDoS Defense**

**A Collaborative Approach**

### Problem:

What happens, if 400 Gbps are reaching the network? [1][2]

### Research Questions:

1. Is real-time and automatic mitigation at ISP level performed and if yes, how?
2. How can the effect of DDoS attack be limited?
3. How can the framework for real-time and automatic mitigation be validated?

### Approach:

To optimize mitigation and response capabilities and thus reduce potential damages caused by DDoS attacks, mitigation and response should move from the target network to the network of Internet Service Providers. Additionally, ISPs should collaborate and exchange information in context of network security.

This work proposes a framework for flow-based real-time and automatic mitigation of DDoS attacks in ISP networks.

---
