Distributed Denial-of-service

- Distributed denial-of-service (DDoS) attacks cause serious damage to network-based services and their users.
- DDoS attacks are performed by sending large volumes of garbage packets to their targets.
- Small- and medium-sized organizations lack the resources to withstand a very large DDoS attack.

Collaborative DDoS Defense

- Multiple entities exchange information about specific DDoS attacks.
- Collaborators make decisions on the roles on defense:
  - Initiation nodes
  - Mitigation nodes
  - Propagation nodes
- Attack traffic can be stopped early on before reaching the victim’s network.

How about motivation?

Costs:
- Dropping customers traffic will reduce the income
- Equipment costs
- Maintenance costs
- Relationship establishment

Benefits:
- Fulfill customers needs (happier customer)
- Reduce traffic on the paying links
- Good reputation
- Attracts more good traffic

Even with good solutions, ISPs may still not participate.

Game-theory Approaches

- Game theory approach can incorporate each organization’s motivation into consideration.
- Each combination of parameters can potentially lead to equilibriums (stable states) for defense deployment.
- By combining the simulation and theoretical analysis, this approach can produce predictions for the effectiveness deploying collaborative DDoS defense solutions, and provide optimization suggestions for motivating the deployment.