# PREVENT FLOODING ATTACK in NDN

Jack Kuo

2017.10.24 NDN Course

# Why

* Limited attention from the security community
* Related to my current plan -  Information Security Incubation Program (launched by Ministry of Education)
* We have lots of network facilities

# Related paper

## I have read

* Interest Flooding Attack in Named Data Networking: A Survey
* Interest Flooding Attack and Countermeasures in Named Data Networking

## I want to read

* A hybrid multiobjective RBFPSO method for mitigating DoSattacks in named data networking

# The second paper summary

## Three countermeasure method

**Token bucket with per interface fairness**

* Using token and extended PIT to control packet forwarding
* The worst of three

**Satisfaction-based Interest acceptance**

* Router randomly drop packet according to Interest satisfaction ratio
* Ranked in middle and has periodic dip in small-scale binary tree topology

**Satisfaction-based pushback**

* Router give quota to downstream one recursively
* The best one in small-scale and ISP-like scale

## Pros and Cons

**Prons**

* Some code he uses is shared on [GitHub](https://github.com/cawka) 

**Cons**

* Token bucket method may use “two rate three color marker” but paper doesn’t mention
* If attacker stop attacking, he’s still blocked by router

# What should I need?

* Lots of computers to run NDN router, Producer,  Consumer
* Skill to write script and build entire NDN network