Networking 2013: OMM session

Paper ID: A2-1

Paper title: Interest Flooding Attack and Countermeasures in Named Data Networking

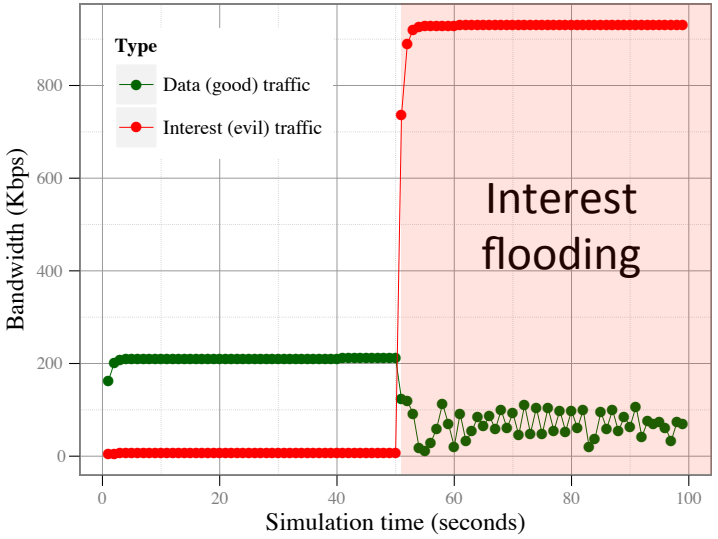
Author: Alexander Afanasyev

Motivation

- (Distributed) denial of service (DoS) attacks are significant threats to the current Internet

- NDN architecture prevents conventional (D)DoS attacks
  - impossible to spoof IP address or launch a reflector attack
  - not as easy to target a specific host

- NDN **may** be exposed to new types of attacks
  - interest flooding
    - network resource exhaustion
    - router's resource exhaustion



Solution using architecture's features

- NDN routers have all the information needed to be able to differentiate good interests from bad ones.
  - To be effective in DoS, bad interests need to be insuppressible and requesting non-existing content.
  - On the other hand, good interests will likely be satisfied with a content

- Keep per incoming interface, per prefix (FIB entry) interest satisfaction statistics in routers

- Use the statistics to detect and control bad traffic
  - "bad" interest can be pushed back to attackers