DoS and DDoS resiliency of NDN/CCN architecture

Alexander Afanasyev (UCLA), Ilya Moiseenko (UCLA), Ersin Uzun (PARC), Priya Mahadevan (PARC)

NDN vulnerabilities

- **Interest flooding / PIT overloading**
  - **target:** NDN routers, network channels
  - **action:** expressing a large number of Interests for (non-)existing Data from a specific namespace or a broad set of namespaces
  - **effect:** resource (CPU, memory, bandwidth, etc.) exhaustion, PIT overloading
- **Cache poisoning**
  - **target:** NDN routers
  - **action:** expressing a large number of Interests for unpopular Data
  - **effect:** evicting popular Data from caches
- **Content poisoning**
  - **target:** consumers, NDN routers, network channels
  - **action:** satisfying Interests with bogus (verifiable, but from bad publisher / non-verifiable) Data
  - **effect:** wrong content may be cached on the way and reach consumer, which will need to re-express Interest with appropriate exclude filter

Main research goals

- **Investigate resiliency of NDN architecture to Denial-of-Service (DoS) attacks**
  - applicability of existing IP-based attacks to NDN
  - effect and potential of NDN-specific attacks
  - quantify architectural resiliency of NDN to attacks
- **Investigate DoS detection techniques**
  - traffic pattern analysis
  - time series analysis
  - sequential change point detection
- **Investigate DoS prevention/mitigation techniques**
  - bandwidth-delay-product (BDP) based interest limits
  - dynamic per-face interest limiting
  - dynamic per-face per prefix interest limiting
  - PIT quotas and "replacement" policies
  - pushing "bad" Interests to the edges of the network

Scope of the work for Summer'12

- **Problem subset for the summer**
  - **Only networking-level attacks specific to NDN architecture**
    - no application-level or implementation-related attacks
    - code bugs (if any) are not inherent to NDN architecture
  - **Focus on interest flooding attacks**
    - the most (in IP packet flooding form) prevalent type of attack on the existing Internet
- **Research assumptions**
  - only static content in NDN network
  - client nodes can be malicious or compromised
  - no malicious or compromised routers
- **Future directions**
  - explore attacks possible on network with dynamic content
  - explore resiliency to colluding attackers
  - understand relation between DDoS attacks and fairness (per-source/per-prefix/per-face, etc.)

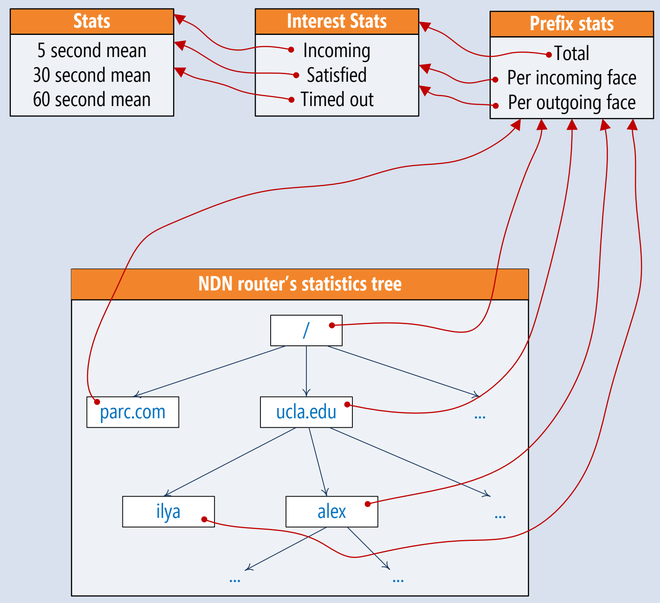
Methodology

- **Analysis**
  - analyze existing DoS and DDoS detection solutions
  - evaluate applicability of existing schemes to mitigate NDN-specific attacks
  - explore NDN-specific DoS mitigation methods
- **Evaluation**
  - **Simulation-based experimentation (ndnSIM)**
    - ndnSIM — module for NS-3 simulator
    - small-scale and complex large-scale (realistic) scenarios
  - **Emulation-based experimentation (DETER testbed)**
    - small-scale scenarios (~20 nodes)
    - verify fidelity of the simulation results
- **Evaluation goal**
  - **obtain metrics for analytics**
    - number of satisfied/unsatisfied interests vs. time
    - ratio of satisfied/unsatisfied to incoming interests vs. time
    - per-face per-prefix stats
  - **evaluate extent and effects of NDN-specific DoS attacks**
  - **evaluate DoS avoidance/mitigation methods**
    - adaptation of existing methods
    - NDN-specific methods

Evaluation details

- **Topologies**
  - **simple small-scale**
    - linear
    - one-level binary tree
    - two-level binary tree
  - **complex large-scale**
    - multi-level binary tree
    - realistic large-scale (Internet and ISP)
- **Attack scenarios**
  - **simple**
    - one producer, 50% consumers good, 50% bad
  - **advanced**
    - one producer, variable ratio good and bad consumers
    - multiple producers for the same prefix
    - multiple producers for different prefixes
- **Metrics (statistics) generation**
  - **multiple dimensions**
    - time, prefix, interface (incoming, outgoing)
  - **multiple granularities**
    - 5 sec, 30 sec, 60 sec (configurable)
    - per-prefix per-interface
    - per-prefix only, per-interface only

Statistics generation module



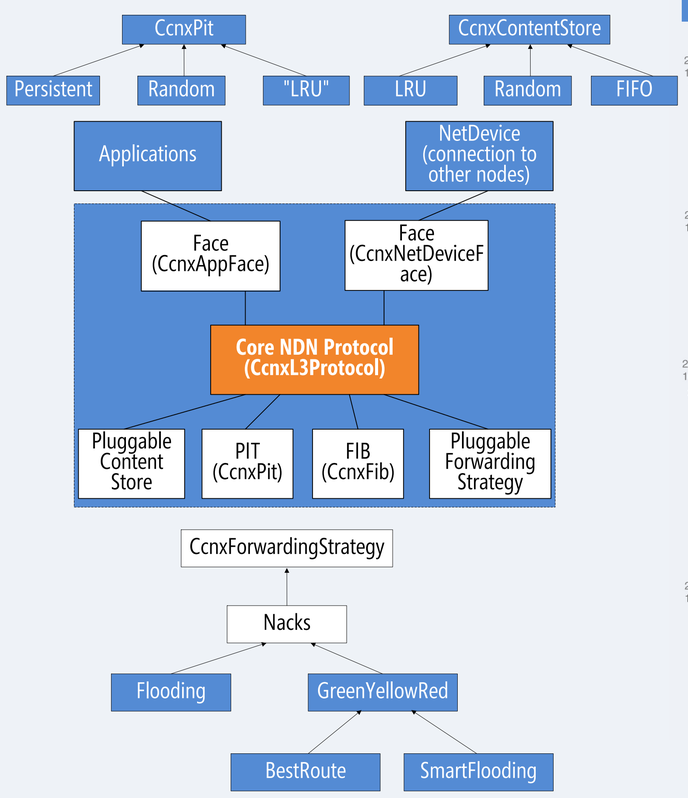
Properties of the implemented statistics tree:

- Child node statistics is periodically (every second) aggregated to the parent.
- Total statistics is aggregated at leaf nodes.
- Exponential decaying of stats data.
- Pruning zeroed nodes and branches.

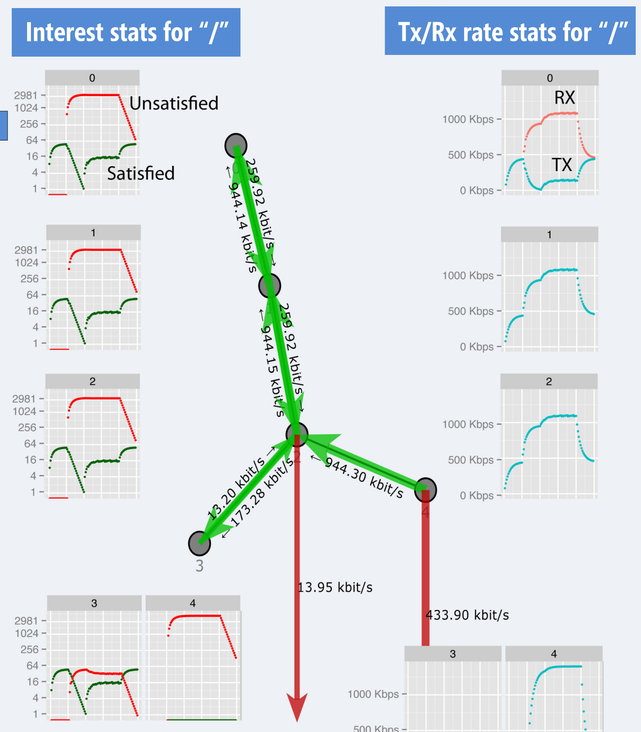
Work in progress

ndnSIM: NS-3 based NDN simulator

- **Modular & extensible architecture**
  - C++ classes for every NDN component
    - Face
    - PIT
    - FIB
    - ContentStore
- **Simulated basic NDN operations**
- **Pluggable modules**
  - Forwarding strategy
  - PIT
  - Content Store
- **Packet-level interoperability with CCNx implementation**



Linear topology



Simple tree topology