Backscatter from the Data Plane - Threats to Stability and Security in Information-Centric Networking

Matthias Wählisch, Thomas C. Schmidt, Markus Vahlenkamp

Hamburg University of Applied Sciences
Internet Technologies Group

December 19, 2012

Agenda

Introduction

Background

Internet use cases shift

- From *host-centric*

  Communicate via end-points (host/port)
- To *information-centric*

  Access content via the network itself

- The network should probably account stronger for content distribution

ICN aims for

- Scalable and efficient content-aware network infrastructure
- In-network storage / caching

General ICN building blocks

Publish / Subscribe paradigm

- Publish data in-network
- Receive data through subscription
- Match publication and subscription by rendezvous mechanism

Naming

- Via location independent identifiers

Caching

- At-the-edge on end-nodes
- In-network on content routers
  - On-path towards origin / off-path

General ICN building blocks

Security

- Secure content instead of communication channels
  - Data integrity (e.g. self-certifiability)
  - Author & origin authentication
- Popular to be coupled with content naming

Routing and Forwarding

- Immediate routing of content requests (one-step resolve/retrieve)
- Name Resolution Service (NRS) (two-step resolve/retrieve)

ICN concepts

Ongoing projects

- NDN / CCNx from PARC
- NetInf of the 4WARD and SAIL project
- PSIRP / PURSUIT project

Early projects

- TRIAD project of Stanford University (2001)
- Data Oriented Network Architecture (DONA) (2007)

NDN / CCNx

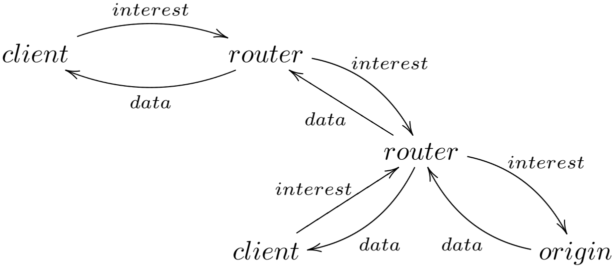
Overview

- Named Data Networking (NDN)
- Prototype implementation named CCNx
- Most popular Information-Centric Networking approach so far
- Research project of Palo Alto Research Center (PARC)

Naming structure

- Hierarchical & Aggregatable
- Human-friendly format
- Smallest addressable unit - file chunks
- Example: *ccnx:/parc/videos/intro.avi*

NDN / CCNx Routing



- Interest packets create soft-state (Pending Interest entry)
- Reverse Path Forwarding through use of Pending Interest Table (PIT)
- Soft-state timeout or clearing by corresponding data packet

Subsumption

- NDN / CCNx claims protection against many of today's network attacks e.g.
  - Content manipulation by signing
  - (D)DoS attacks by requiring subscription for data delivery
- Underlying paradigm largely different from today's Internet
  - Hop-by-Hop vs. End-to-End delivery
  - Publish / Subscribe vs. Sender-driven approach

Motivation

Motivation

- How stable is the ICN infrastructure?
- Does it scale at Internet size?
- Which security threats do still exist?
- Which new attack vectors arise?

- ICN opens control plane to content consumers and producers through
  - Publications
  - Subscriptions
- These data-driven states influence the network

Visible Issues

- Resource Exhaustion

  Exhaustion of FIB / PIT table space or CPU capacity
- State Decorrelation

  Unwanted traffic flows through failures in distributed state coherence
- Path & Name Infiltration

  Malicious attraction of name prefixes
- Cache Pollution

  Degrade regular cache performance through content hotness manipulating
- Cryptographic Breaches

  Large amounts of data & long lived signing keys provide increased attack surface

Examination

Examination

Methodology

1. Develop threatening scenarios
2. Define metrics to be collected during measurement
3. Select appropriate environment / approach to run measurement

Threatening scenario

➠ PIT attack

Create bulks of Interests

- Existing content
  PIT entry removed by arriving data
- Non-existing content
  PIT entry removed by timeout

Metrics of interest

- PIT Count

  Number of Pending Interests per node
- PIT / FIB management resources

  CPU time and memory consumption
- Interest retransmission rate

  Number of Interests suffering retransmission
- Network Throughput

  Amount of data that was transmitted per second
- Time-to-Deliver

  Time for a file transfer to complete

Testbed topology

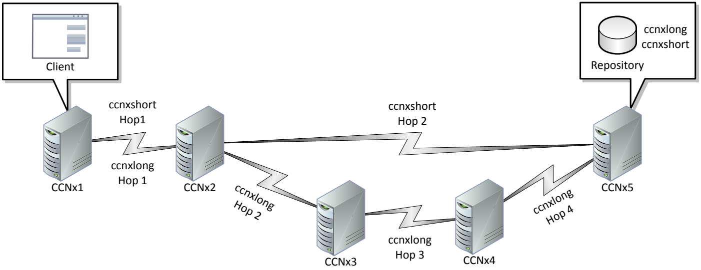
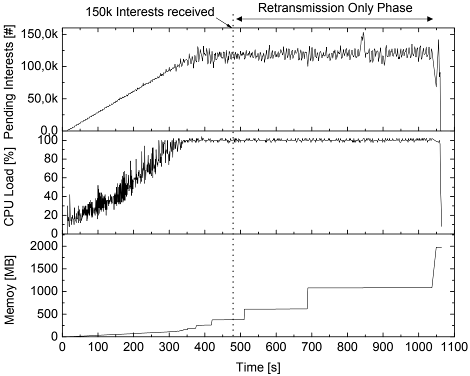


Figure: Testbed topology

Results

Rapid resource exhaustion

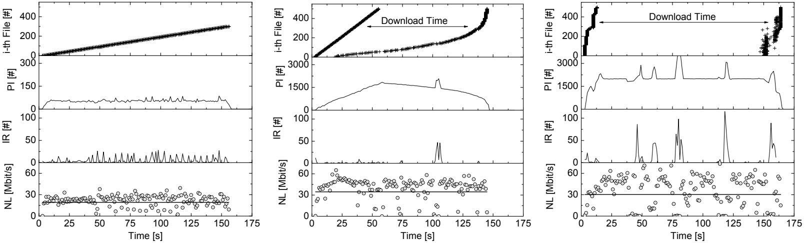
Load at first hop router, requesting non-existing content



- Issue 2000 Interests per 6s until 150k Interests are pending
- Resource load increases linearly
- System saturated at $\approx$ 120k Pending Interests

Chunk-based state multiplication

10 Mbit files parallel download

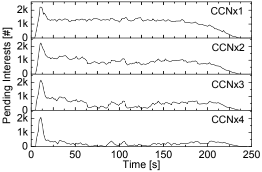


(a) 2 files per second (b) 10 files per second (c) 100 files per second

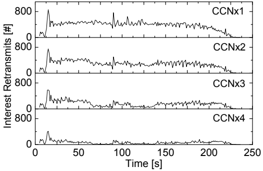
- Increased download times despite of underutilised link, caused by lack of processing & memory resources

Homogeneous chain of nodes

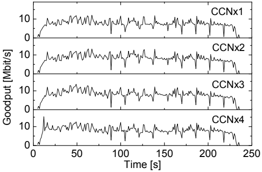
All nodes are equipped with similar CPU & memory capacity



(a) Pending Interests



(b) Interest Retransmits

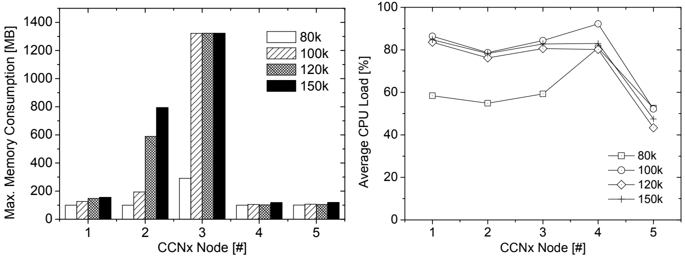


(c) Network Utilization

➠ PI's and IR's decrease towards content source due to propagation effects

Chained transmission with bottleneck

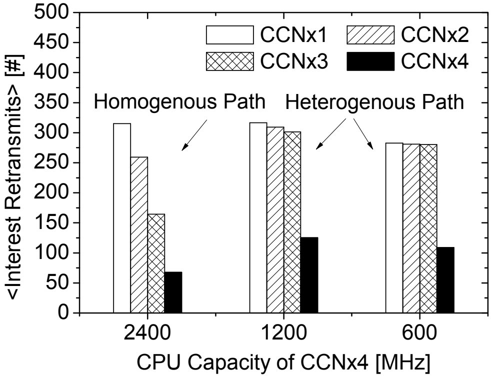
Node 4 equipped with just 25% CPU resources



(a) Memory Consumption (b) Average CPU Load

- Bottleneck node acts like a barrier
- Pre-bottleneck nodes suffer increased memory and CPU consumption

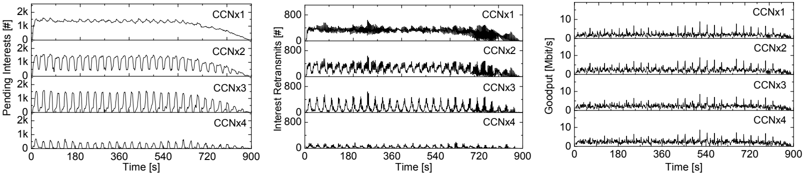
Router performance relating to Interest forwarding



- IR's drastically increase
- Network behaviour switches at occurrence of bottleneck - regardless of strength

Multiple fluctuating bottlenecks

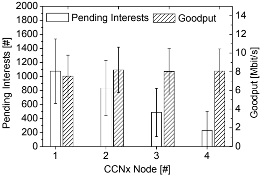
Shifted periodical CPU capacity reduction by 90% for 30s on every node



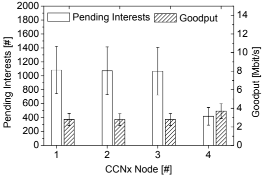
(a) Pending Interests (b) Interest Retransmits (c) Network Utilization

- Simulation of cross-traffic scenario
- Data transmission rates drop significantly
- Time-to-completion increased by factor of 3.6 to 900s

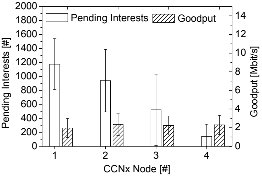
Conclusion



(a) Homogeneous Network



(b) Single Point of Weakness



(c) Alternating Resources

Conclusion

- Inhomogeneities drastically lower network efficiency
- State management follows maximal requirements
- Forwarding performance adopts to weakest node

Thanks for your attention!

References I

[1] The Named Data Networking Homepage.
http://www.named-data.net, 2012.

[2] The NetInf Homepage.
http://www.netinf.org, 2012.

[3] The PSIRP Homepage.
http://www.psirp.org, 2012.

[4] The PURSUIT Homepage.
http://www.fp7-pursuit.eu, 2012.

[5] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and Ohlmann, B.
A Survey of Information-Centric Networking (Draft).
Tech. Rep. 10492, Dagstuhl Seminar Proceedings, 2011.

References II

[6] Camara, D., Urbani, F., Lacage, M., Turletti, T., and Dabbous, W.
Experimentation with ccn.
Presentation, INRIA, Planète-Project, 2012.

[7] PARC.
The CCNx Homepage.
http://www.ccnx.org, 2012.

[8] Vahlenkamp, M.
Ccnx meassurement testbed implementation.
Tech. rep., HAW Hamburg, 2012.

References III

[9] Wählisch, M., Schmidt, T. C., and Vahlenkamp, M.
Backscatter from the Data Plane — Threats to Stability and Security in Information-Centric Networking.
Technical Report arXiv:1205.4778, Open Archive: arXiv.org, 2012.

[10] Wählisch, M., Schmidt, T. C., and Vahlenkamp, M.
Bulk of Interest: Performance Measurement of Content-Centric Routing.
In *Proc. of ACM SIGCOMM, Poster Session* (New York, August 2012), ACM, pp. 99–100.

[11] Zhang, L., Estrin, D., Burke, J., Jacobson, V., and Thornton, J. D.
Named Data Networking (NDN) Project.
Tech.report ndn-0001, PARC, 2010.