Threats in Information-Centric Networking

Seminar

Markus Vahlenkamp

Hamburg University of Applied Sciences
Master of Science
Computer Science

November 14, 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

Target

- Designing a scalable and efficient content-aware network infrastructure

NDN / CCNx Overview

- Most Popular Information-Centric Networking approach so far
- Research project of Palo Alto Research Center (PARC)
- Named Data Networking (NDN)[1]
- Prototype implementation named CCNx[4]

NDN / CCNx

Fundamental paradigms

- Publish / Subscribe
  - Publish data In-network
  - Receive data through subscription
  - Matching publication and subscription in network
- In-network content addressing by name
- Cache content everywhere

NDN / CCNx

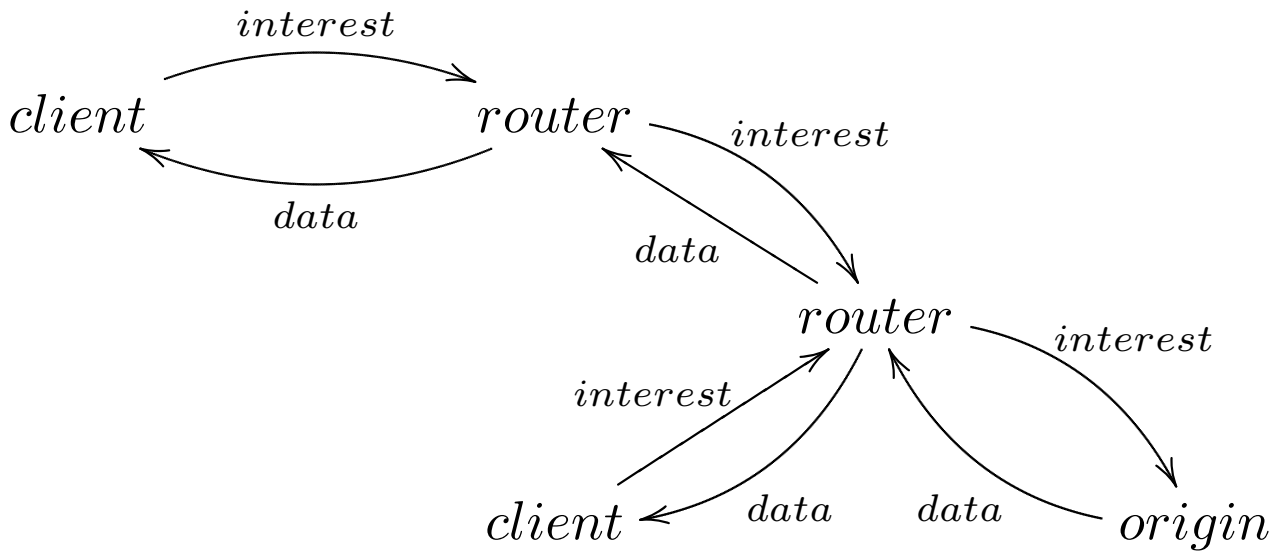

Figure: Abstract CCNx overview[2]

- Interest packets are routed towards sources
- Longest prefix match on content names

NDN / CCNx

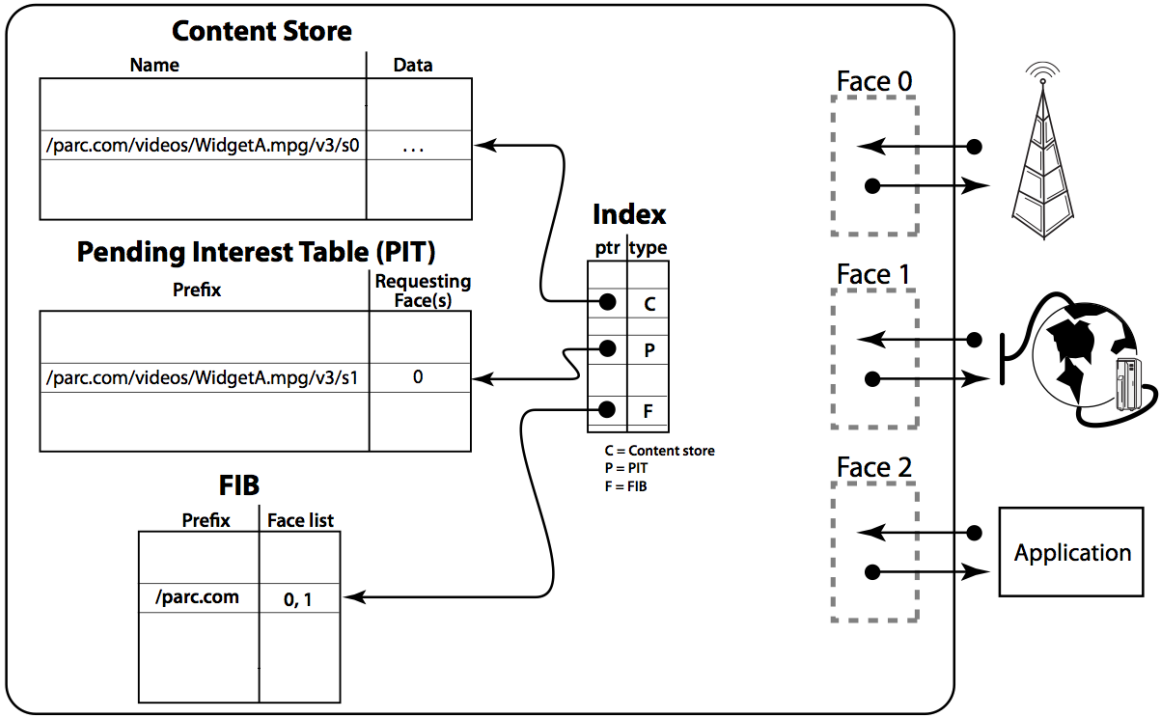

Figure: Conceptual CCNx router architecture[8]

Name resolution & routing

- Routing on content names
- Multiple distributed origins possible
- Interest packets create soft-state (PIT entries)
- Reverse Path Forwarding through use of Pending Interest Table (PIT)
- Soft-states time out or are cleared by corresponding data packets

NDN / CCNx

Security

- Secure content instead of communication channels
  - Data integrity (e.g. self-certifiability)
  - Author & origin authentication
- Data transfer purely receiver initiated
  - No data receipt w/o previous subscription

Subsumption

- Underlying paradigm is entirely different from today's Internet
- NDN / CCNx claims protection against many network attacks[3]

Research Questions

- General Questions
- Problem Space
- Detailed Questions

General Questions

Central Research Question

- Relating to the NDN / CCNx approach
  - Which security issues do still exist?
  - Which new attack vectors arise?

Research Question

- ✦ Problem Space

Problem Space

Anticipated vulnerabilities[6] I

- 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

Anticipated vulnerabilities[6] II

- Cache Pollution

  Degrade regular cache performance through content hotness manipulating

- Cryptographic Breaches

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

Research Question

- Detailed Question

Detailed Questions

Furthermore focus on

- Resource Exhaustion case

Detailed Questions

- Do the anticipated issues exist?
- System behaviour in case of appearance?
- Counter measures to eliminate or mitigate impact?

Methodology

- Scenarios
- Metrics
- Approaches

Methodology

Procedure

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

Threatening Scenarios

- PIT attack

  Create bulks of Interests

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

- FIB attack

  Create bulks of routing information

  - CPU stress through continuous SPF runs
  - Memory exhaustion through amount of routing entries

Methodology

- Metrics

Metrics of Interest I

- PIT Count

  Number of Pending Interests per node
- Interest Retransmission rate

  Number of Interests suffering retransmission
- FIB-Entry Count

  Number of name-based routing entries

Metrics of Interest II

- Memory Consumption

  Amount of memory consumed
- CPU Utilisation

  Amount of utilized CPU resources
- Network Throughput

  Amount of data that was transmitted per second

Methodology

- Approaches

Approaches

- Simulations

  Setup simulation tool, meter relevant data
- Testbed

  Setup network of CCNx nodes, meter relevant data
- Theoretical considerations

  Consider limitations, flaws and issues on theoretical basis

Approaches

Characteristics

Simulation	***Testbed***
Deterministic	Non-deterministic
Single node emulates network	Large number of nodes required
No real code execution[1]	Real code execution

[1] traditionally; see DCE

Approaches

Environment

Simulation	***Testbed***
Barely dependent on execution environment	Environment dependent execution
In-memory execution	Communication with other nodes

Approaches

Handling

Simulation	***Testbed***
➠ Simple scenario definition by code or descriptive	➠ Distributed node & state management required
➠ Simple linear event correlation	➠ Clock sync to obtain causal relation

Approaches

Resource Utilisation & Scaling

Simulation	***Testbed***
Light-weight implementation	Increased resource requirements
Analysis based on emulation of large, real-world topologies	Actual node and network utilisation
Limited by simulation node capacity	Limited by number of available testbed nodes

Progress, Conclusion & Outlook

Progress, Conclusion & Outlook

Actual progress

(✓) Testbed implementation
- PIT attack
- Up to 5 nodes
- Results presented in [5, 7, 6]

([2]) Simulation implementation
- PIT attack
- Hundreds of nodes

(-) Problem solution

Conclusion & Outlook

- Lot's of work forthcoming
- Still many threat analysis pending

[2] work in progress

Thanks for your attention!

References I

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

[2] 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.

[3] Jacobson, V., Smetters, D. K., Thornton, J. D., and Plass, M. F.
Networking Named Content.
In *Proc. of the 5th Int. Conf. on emerging Networking EXperiments and Technologies (ACM CoNEXT'09)* (New York, NY, USA, Dec. 2009), ACM, pp. 1–12.

References II

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

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

[6] 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.

References III

[7] 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.

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