Networking Named Content

Palo Alto Research Center

Motivation

How to retrieve content over a network?

- Traditional TCP/IP stack
- Retrieval based on *where* it is located

Motivation

These protocols were created with 1960s/70s use-cases in mind.

- A focus on *resource sharing*
- Host-to-host abstraction

These days the internet is about accessing a vast amount of content, regardless of location

Motivation

Three areas that the traditional model is ineffective

- Availability
- Security
- Location-dependence

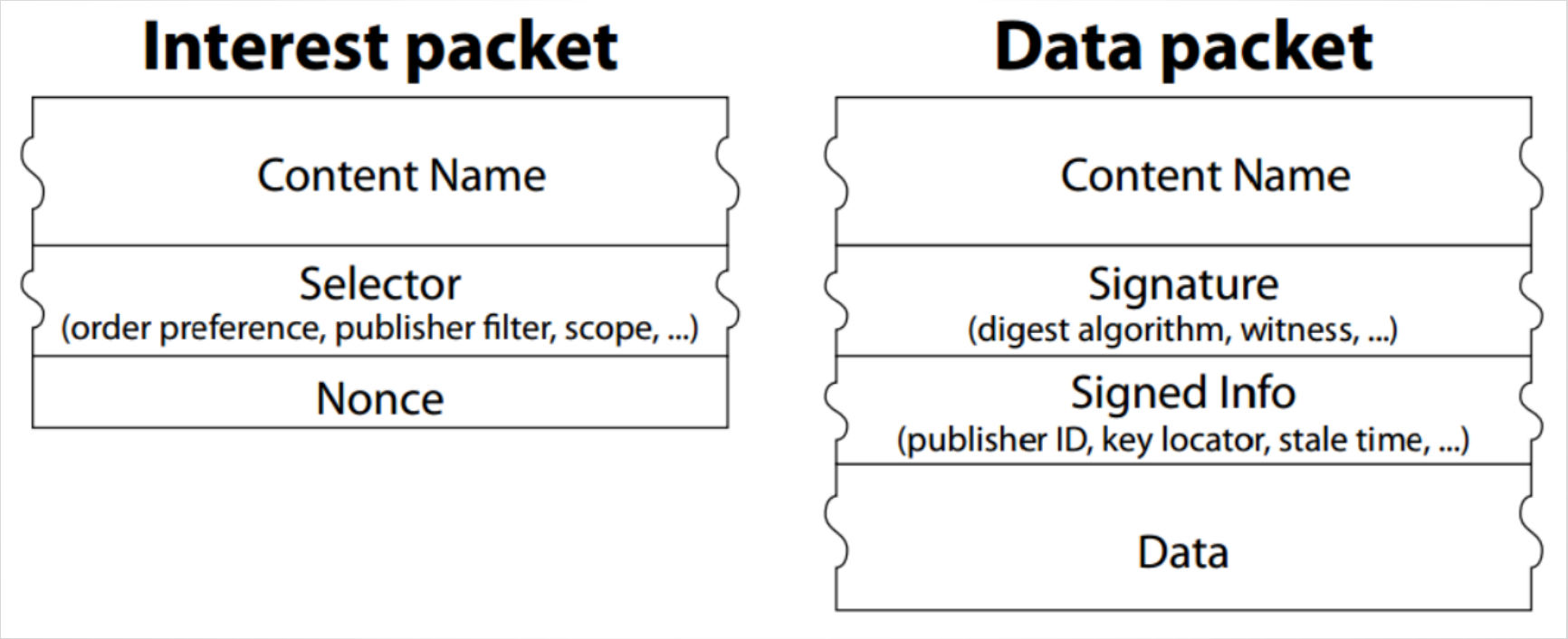
Model Overview

Content-Centric Networking (CCN)

A new networking stack with a focus on *what* the content is rather than *where* it is located.

Includes new transport and routing protocols as well as a built in security system.

Model Overview



Model Overview

- Consumers broadcast the content they want
- Any node can respond with content
- A request is satisfied if the “ContentName” is the same in the request and response
- ContentName examples:
  - /ThisRoom/projector
  - /Local/Friends

Model Overview

Packet Forwarding Engine; composed of:

- FIB (Forwarding Information Base)
  - Similar to IP FIB, but allows multiple destinations
- Content Store
  - Like buffer memory in IP router, but CCN “remembers” packets for as long as possible
- PIT (Pending Interest Table)
  - Stores Interest packets sent upstream to data sources

Model Overview

Transport

- Like TCP, hides failure (retries packets)
- Unlike TCP, it is stateless
  - It is the consumers responsibility to retry
- Flow control of Interests is modelled like TCP ack packets

Model Overview

Routing

- CCN's forwarding model is a strict superset of TCP's
  - Existing routing schemes should work on CCN
  - CCN can be deployed incrementally, using exsiting hardware
- CCN can support both existing Link-state Intra-domain and Inter-domain routing

Model Overview

Security

- Security is property of packets rather than the connection they travel through
- *All* content is digitally signed
- Consumers must validate the data they want
- Different to IP where trust of content is based on where and how it was obtained

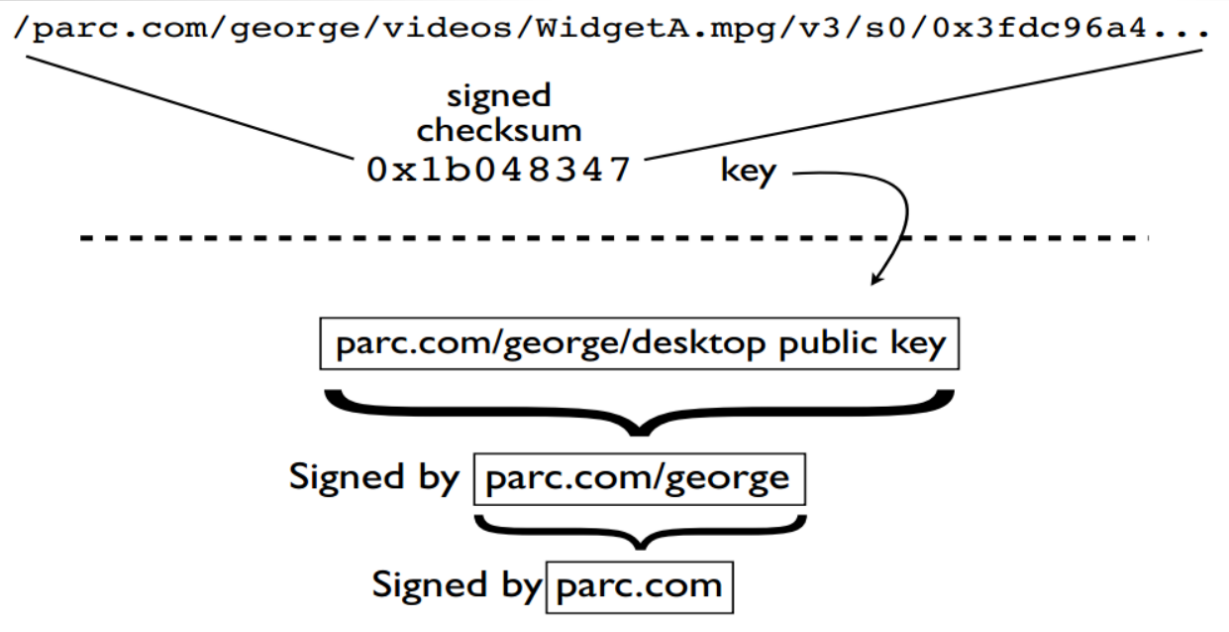
Model Overview

Security - Trust

- Signing of content is flexible
  - Legal document authorised by a court
  - A blog post verified by someone who signed other entries
- SDSI/SPKI model used to hierarchically map keys to identities via namespaces (next slide)

Model Overview

SDSI/SPKI example



Implementation

- Packets encoded in *ccnb* binary XML format
- CCN (*ccnd*) forwarder implemented as a C daemon
- Security layer is implemented as a C & Java library
- Runs on all widely used operating systems
- Currently v0.8.1 https://github.com/ProjectCCNx/ccnx

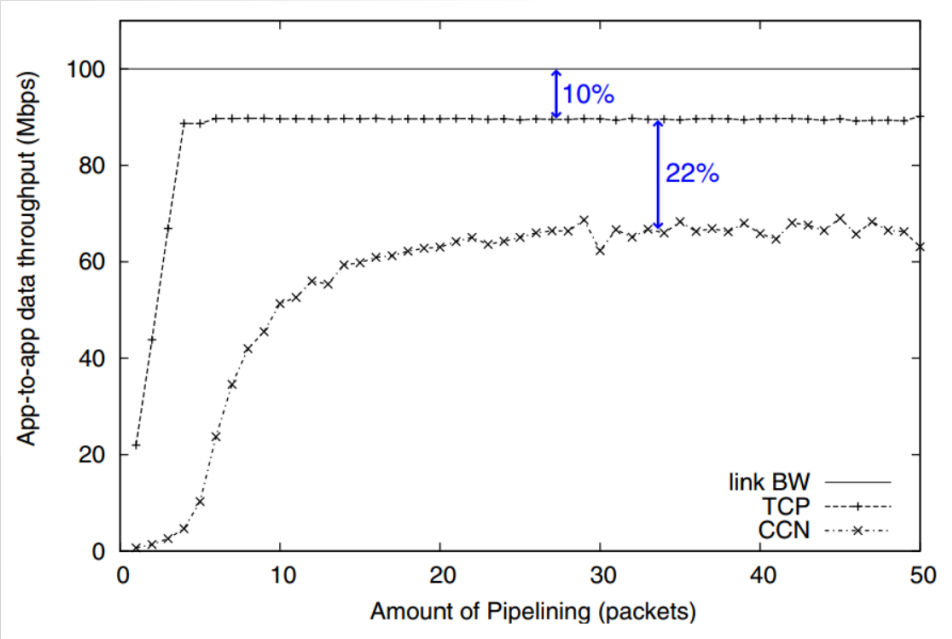
Evaluation

Tested 3 key areas:

- Data Transfer Efficiency
  - File downloading vs TCP
  - Web page downloading vs HTTP/HTTPS
- Content Distribution efficiency
- Voice-over-CCN

Evaluation

File downloading performance vs TCP



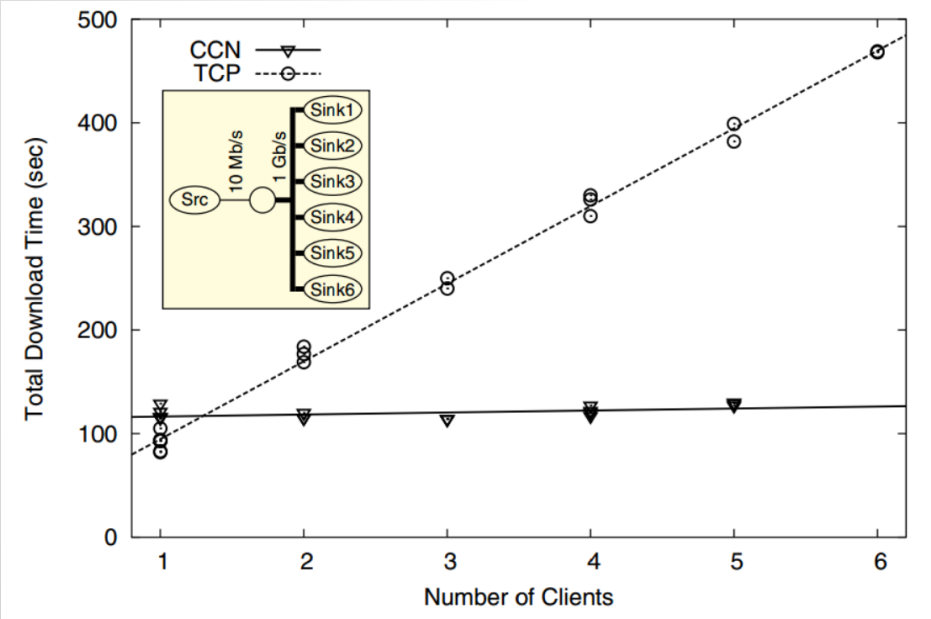
Evaluation

Web Page Download Comparison

	Bytes (packets)		Overheads	
	Sent	Received	Encap	Transact
Web page (6429 bytes)				
HTTP	723 (9)	7364 (9)	15%	11%
CCN/ETH	811 (8)	8101 (6)	26%	13%
CCN/UDP	325 (3)	6873 (5)	7%	5%
Secured Web page (16944 bytes)				
HTTPS	1548 (16)	21232 (22)	25%	9%
CCN/ETH	1791 (16)	20910 (14)	23%	11%
CCN/UDP	629 (5)	18253 (14)	8%	4%

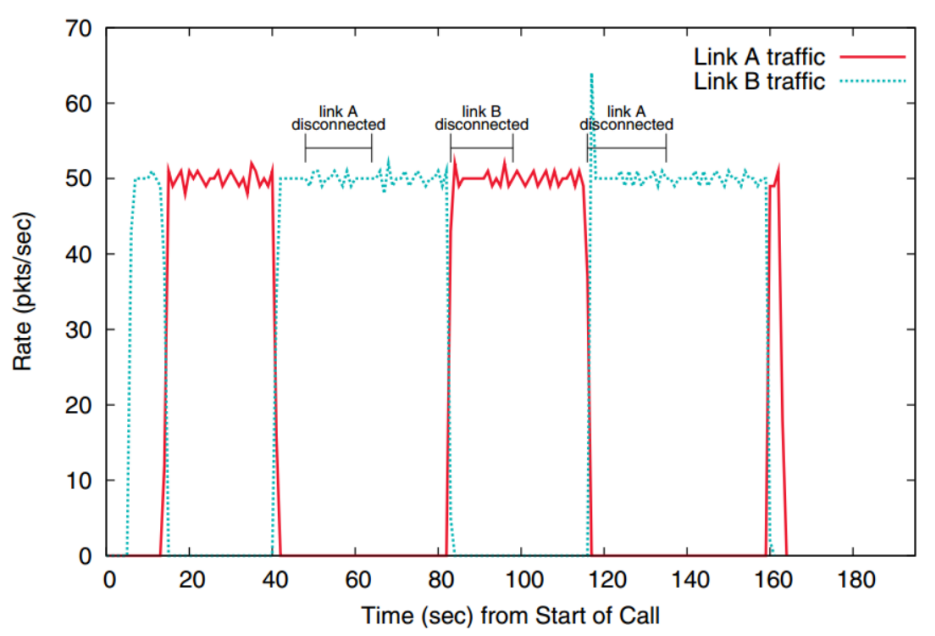
Evaluation

Content Distribution vs TCP



Evaluation

Voice-over-CCN with dropping links



Discussion

- Doesn’t seem hard to beat TCP/IP, real question is whether it can disrupt such an entrenched system
- In general a very ambitious project, but there is backwards compatibility support
  - It can run alongside TCP/IP

Recent Developments

- Android implementation
- Seem to be promoting mainly in more niche areas:
  - Medical devices
  - Home media networks
  - Lighting control systems
- Roadmap for v1.0 released Dec 2013

Questions?