CCN

CCNx 1.0 Security Overview

Computer Science Laboratory
Networking & Distributed Systems

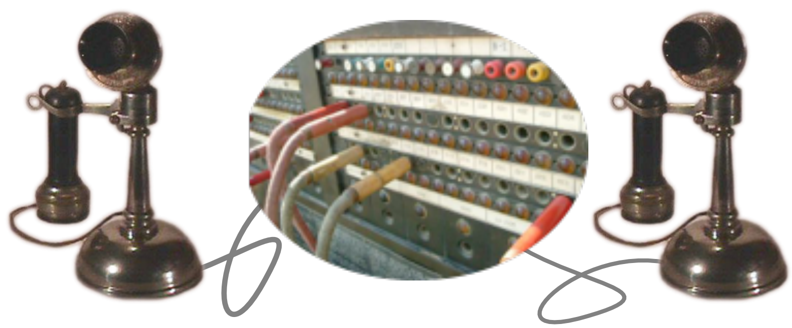
March 2014

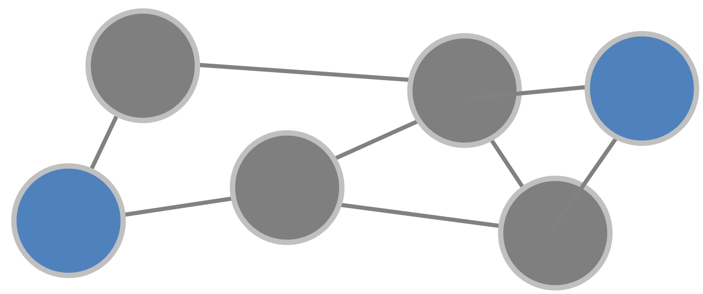
parc
A Xerox Company

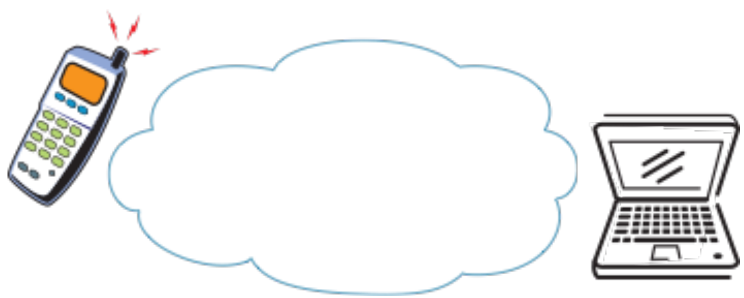
Agenda

- Motivation
- CCN Overview
- CCN Security/Privacy

- For 150 years, ‘communication’ has meant a wire connecting two devices.





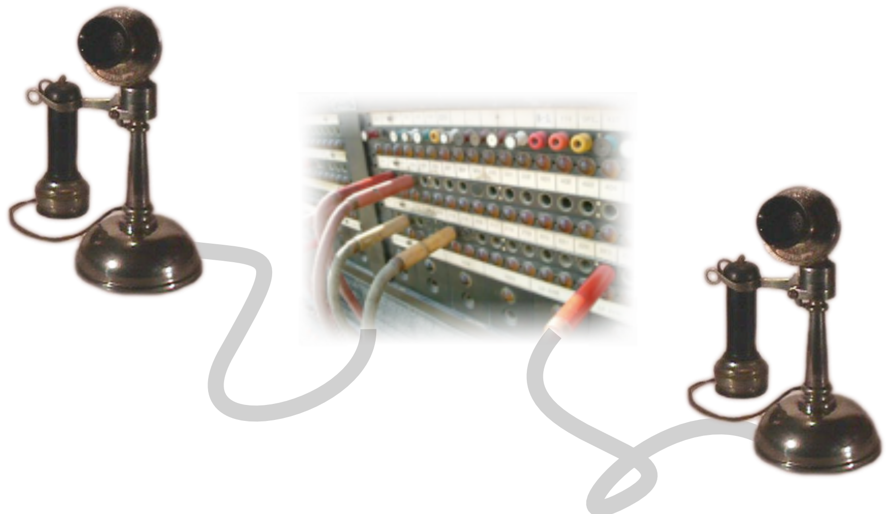


- For users, the Web forever changed that: Content matters, not the host it came from.

- Networking helped to create today's world of content, but was not designed for it:
  - The fundamental communication model is a point-to-point conversation between two hosts.
  - The central abstraction is a host identifier.

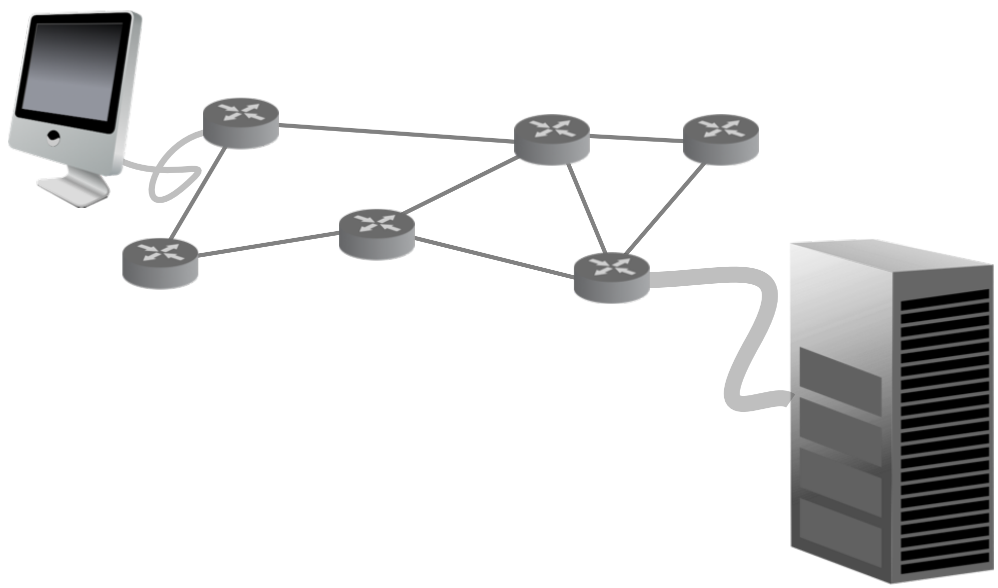
Challenges

- Massive scale of data dissemination
- Computing devices increasingly mobile
- Ad-hoc networking, disruption-tolerant networking
- Internet of things
- Robust data delivery
- Security and Privacy



1876

2012




0:31 / 4:13
HD
PSY - GANGNAM STYLE (강남스타일) M/V
officialpsy · 60 videos
1,812,207,517

1.8B Views

DN $\neq$ CN

Today we have a Communications Network,
not a Distribution Network.

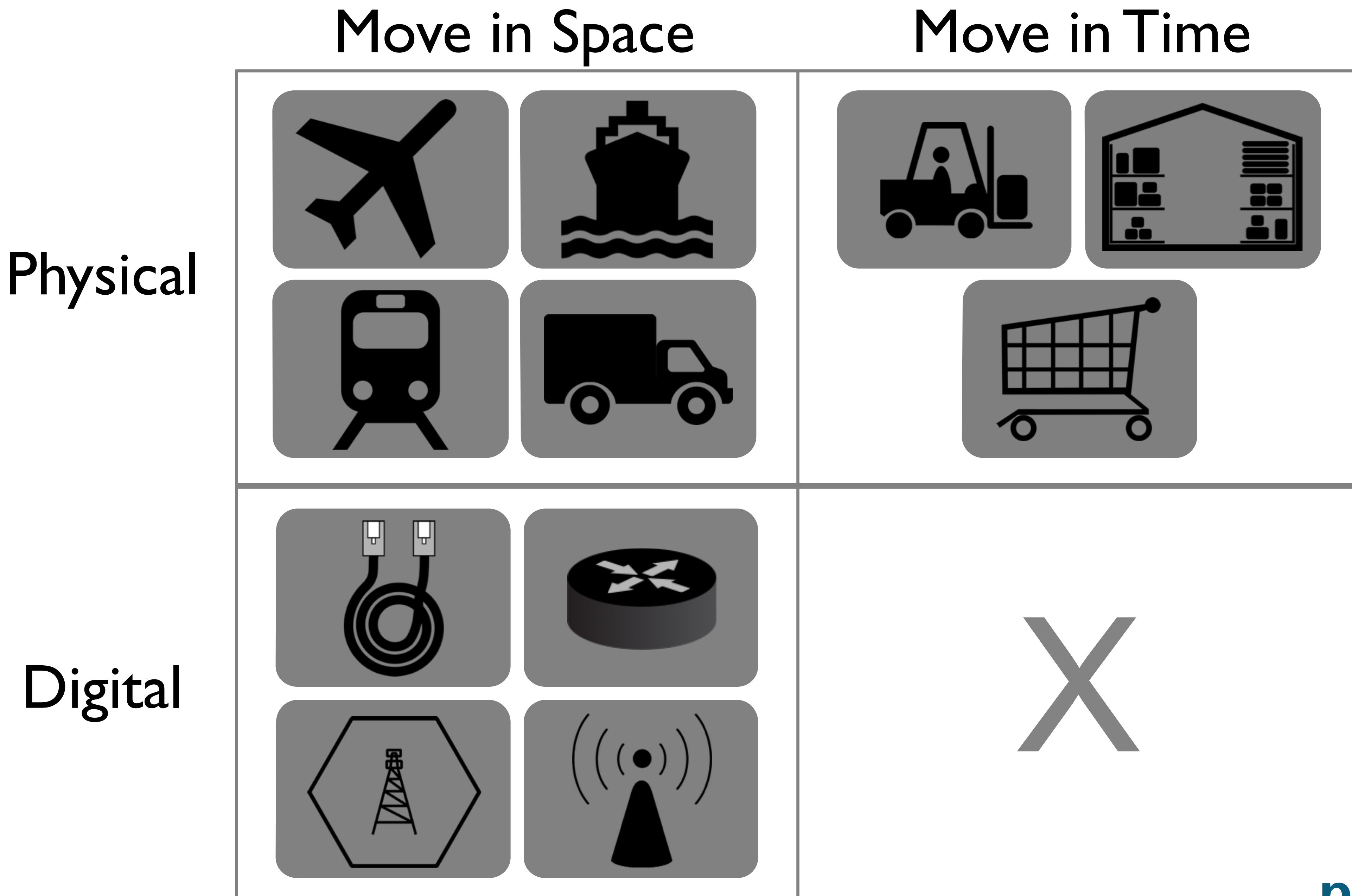
Distribution Networks

	Move in Space	
Physical		

Distribution Networks

	Move in Space	Move in Time
Physical		

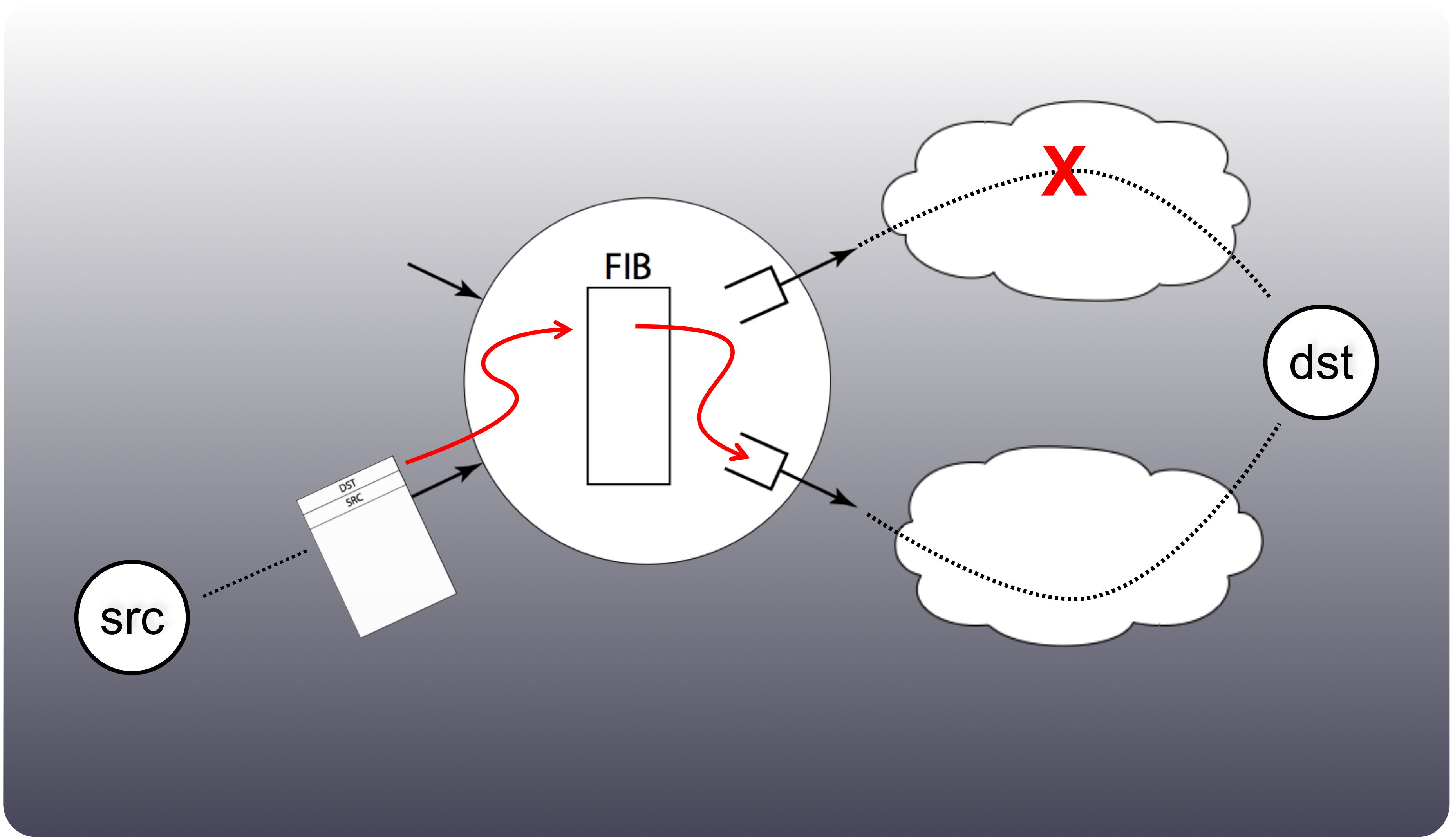
Distribution Networks



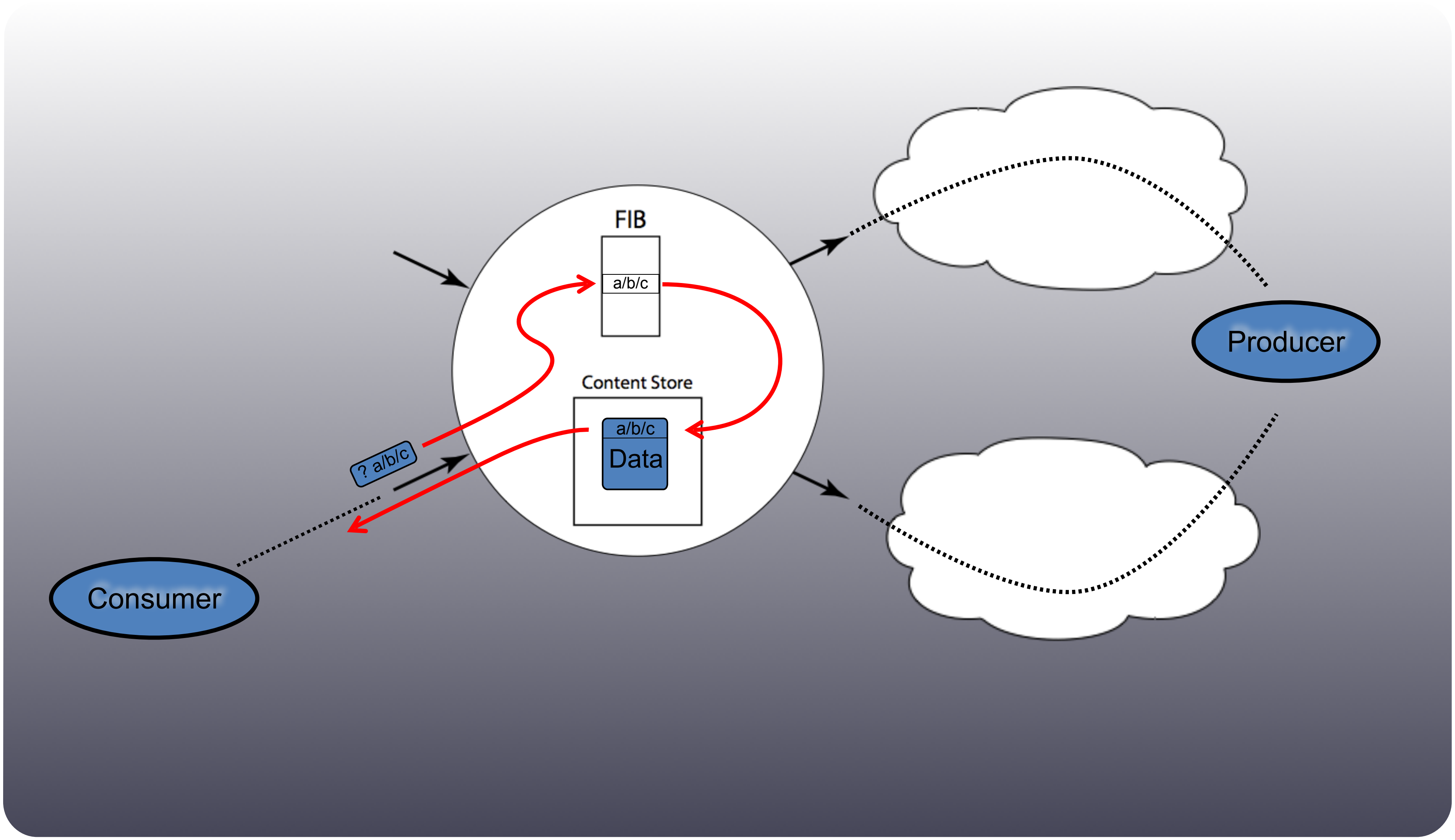
Agenda

- Motivation
- CCN Overview
- CCN Security/Privacy

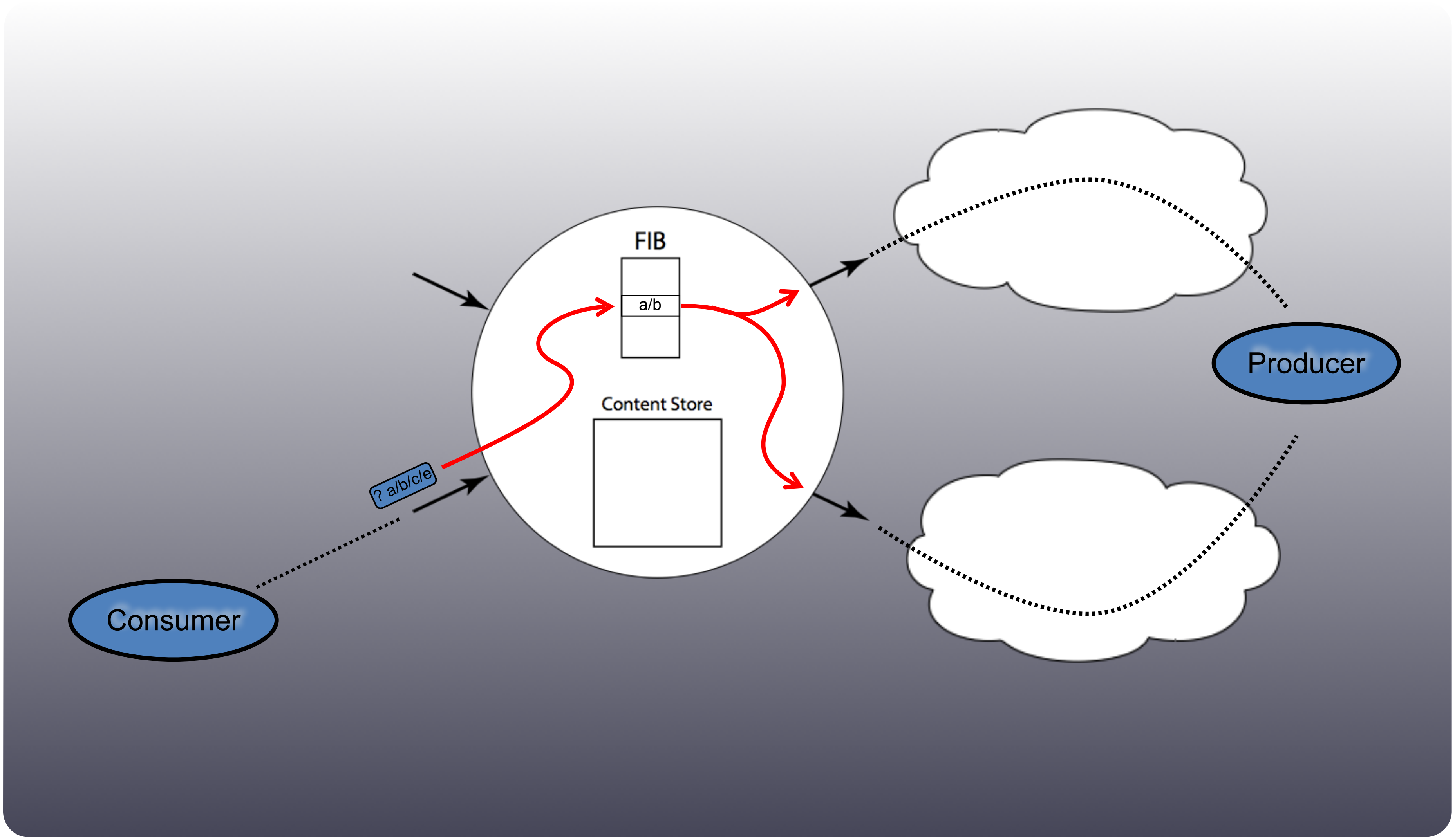
Today



CCN Approach



CCN Approach

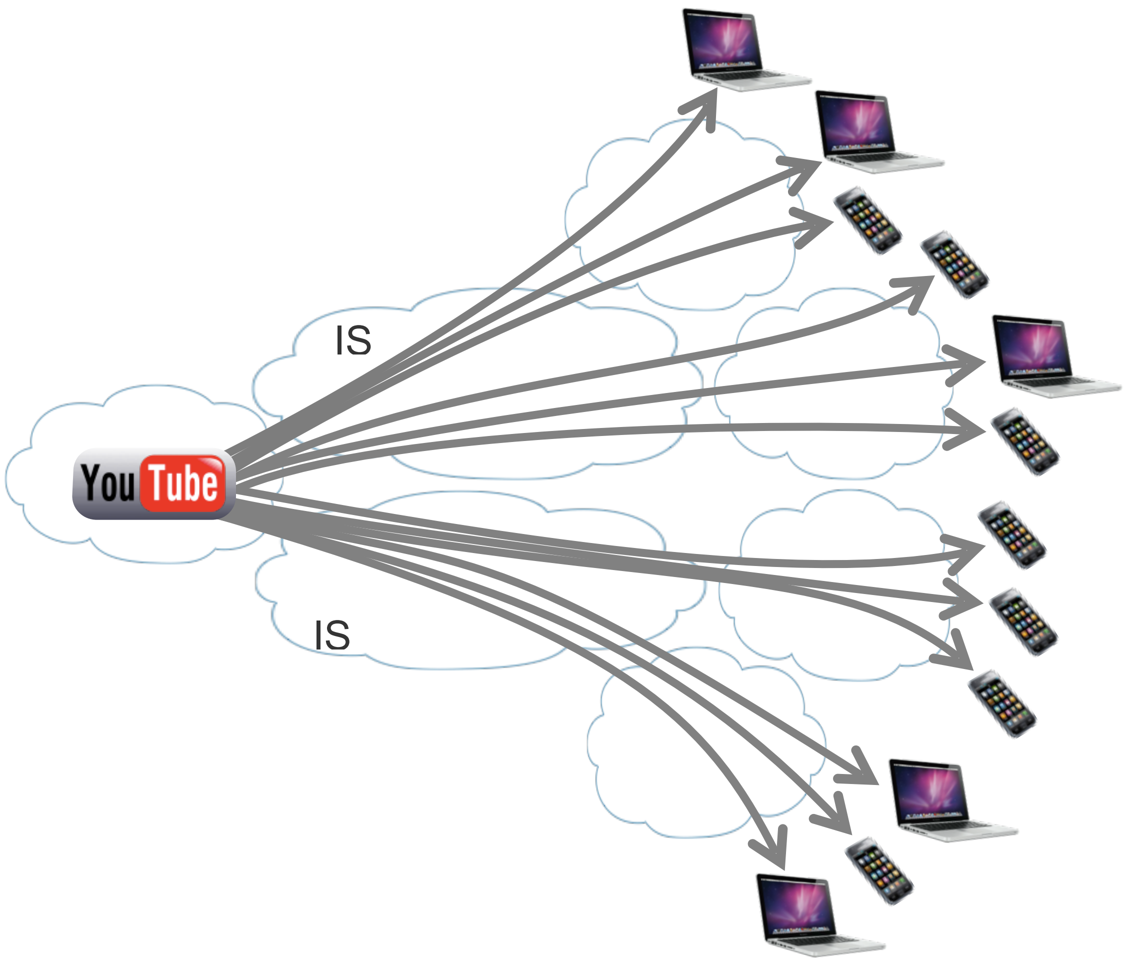


parc
A Xerox Company

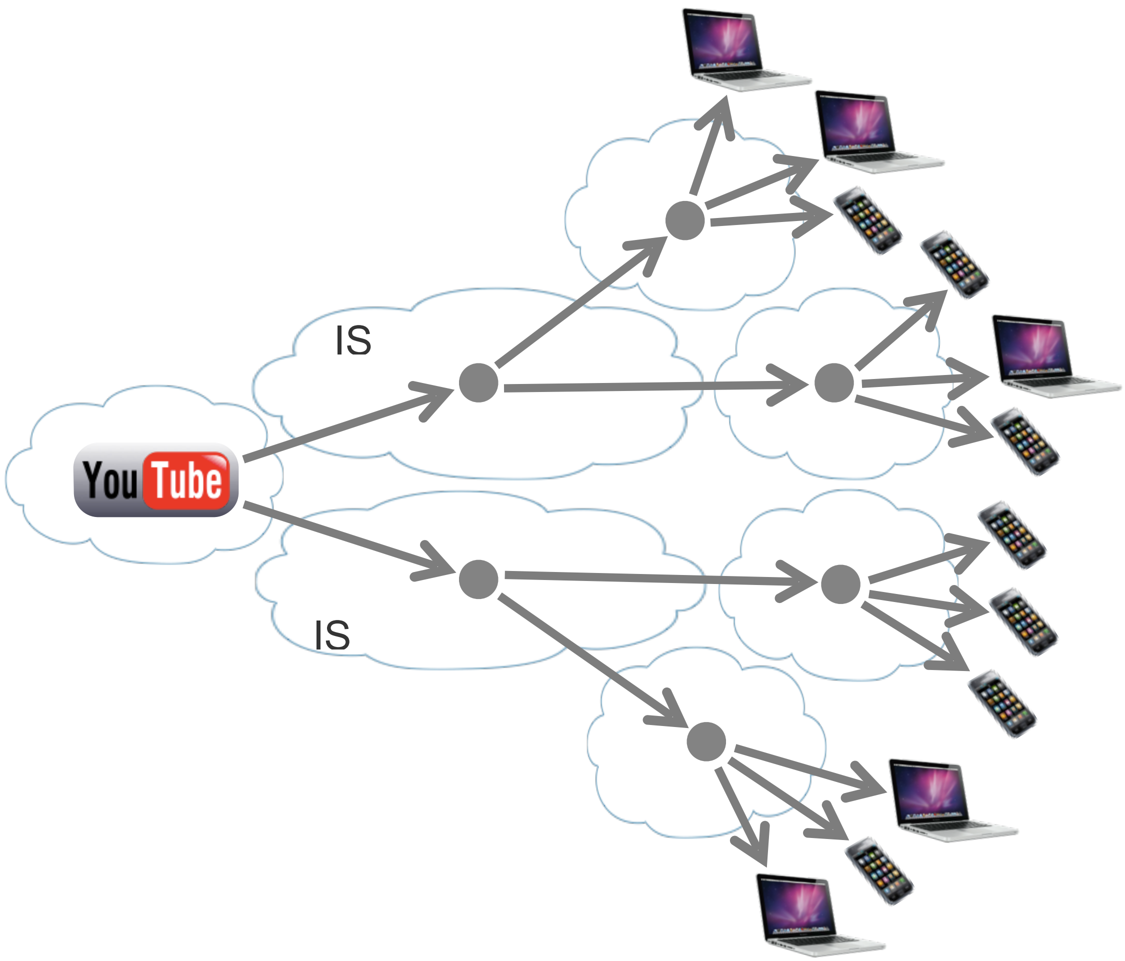
CCN Approach

- Packets say ‘what’ not ‘where’
  (i.e., no source or destination address)
- Forwarding decision is local
- Upstream performance is measurable

Envision replacing this:



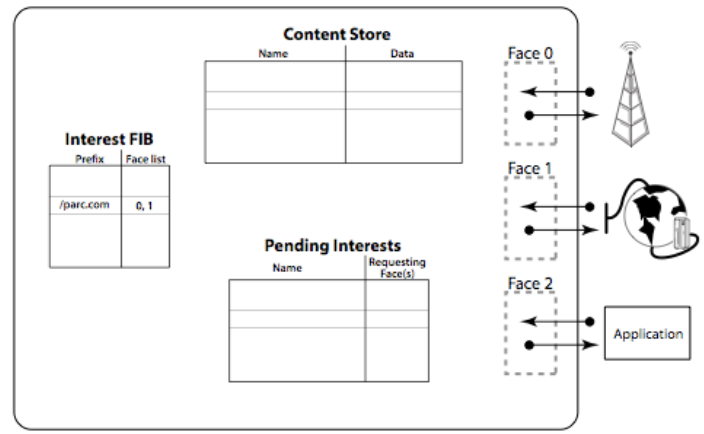
With THIS:

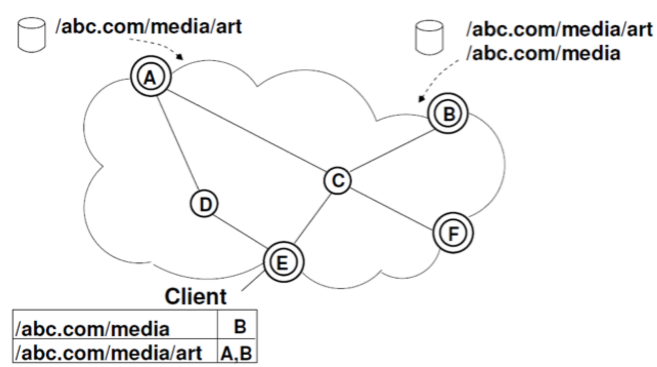


parc
A Xerox Company

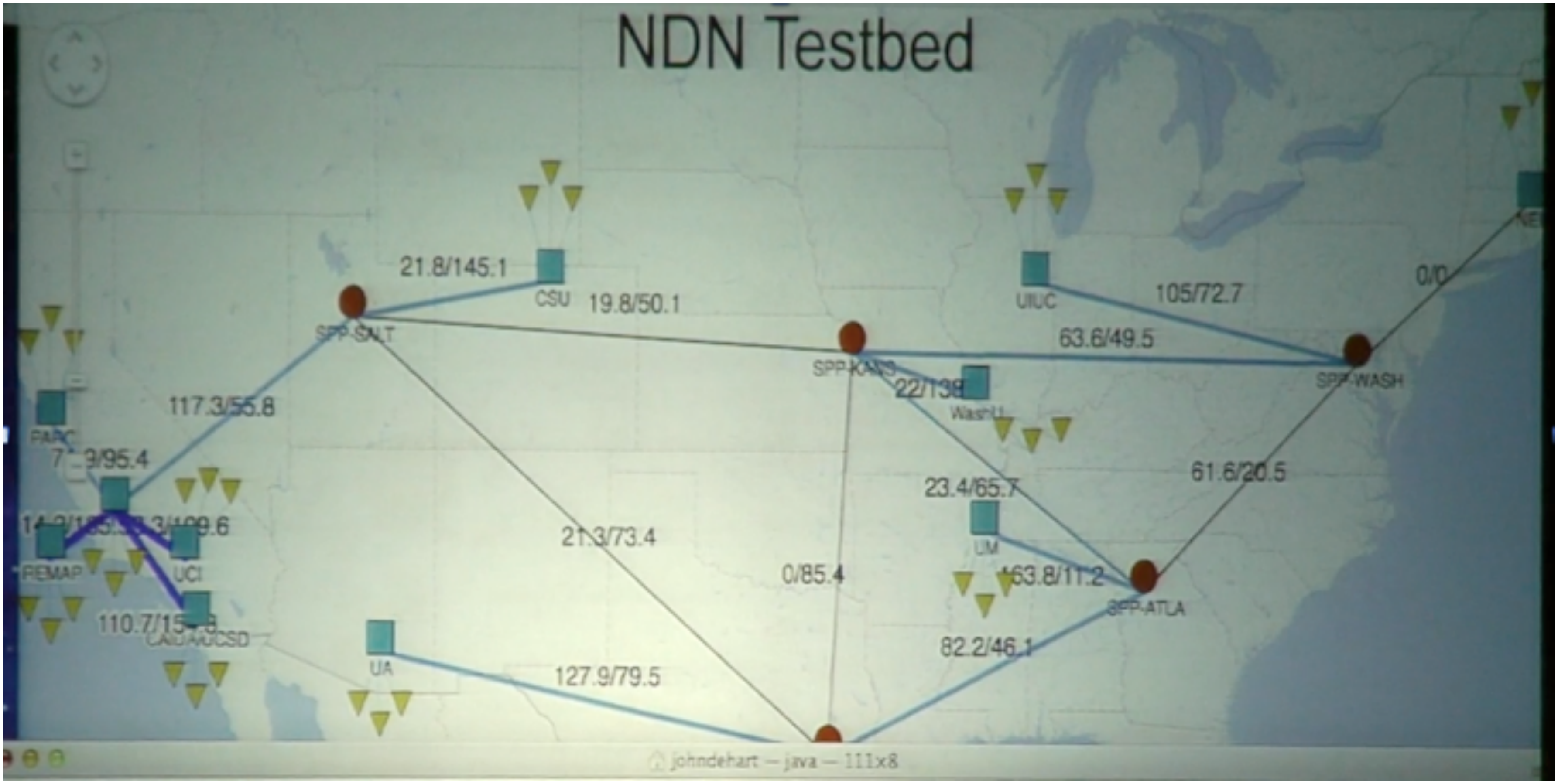
Forwarding and Routing

- **Forwarding**
  - Key operation is prefix-based longest match lookup, like IP
  - Interests forwarded according to routing table, but multipoint forwarding, broadcast, local flooding all ok
  - Data follows Interest path back
- **Routing**
  - Populating routing tables based on prefix reachability as in IP
  - Potential reuse of IP routing protocols like IS-IS, BGP





Large Scale Demos (Based on CCNx 0.7x codebase)



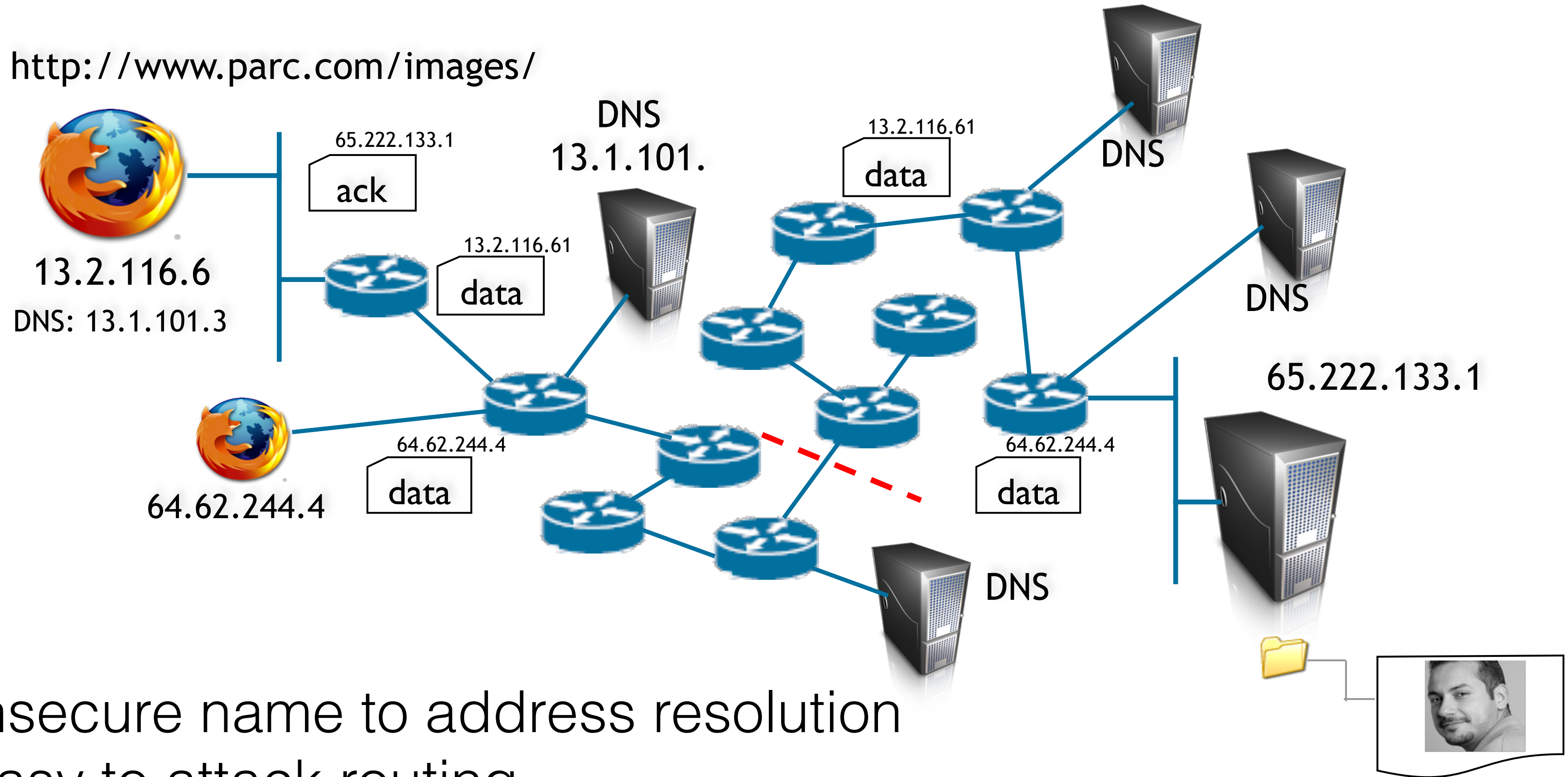
Video From 2012 GENI Engineering Conference:

www.arl.wustl.edu/~pcrowley/NDN_GEC13_demo.mp4

Agenda

- Motivation
- CCN Overview
- CCN Security/Privacy

Security Problems Today



- Insecure name to address resolution
- Easy to attack routing
- Localized content availability
- Arbitrary configuration bindings
- No intrinsic security in the network

High-level Security Goals

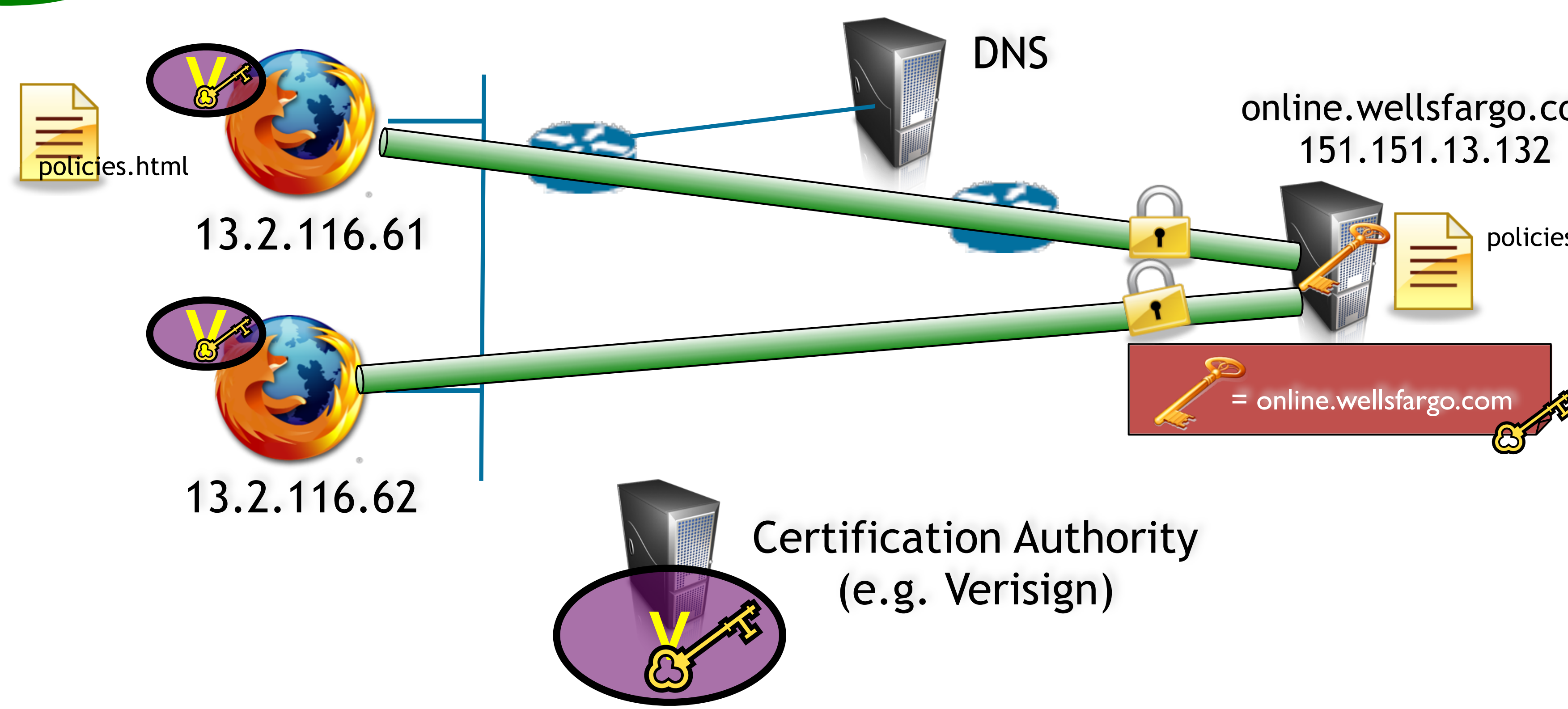
- Address some core problems of today's networks
  - Availability & Resilience
    - Make infrastructure harder to attack
    - Make individual hosts harder to attack
    - Make replication and failover easier
  - Authenticity & integrity
    - Confidentiality where necessary
- Improve application security/functionality
  - Make it easier to build secure network applications

Content-Based Security

Connection-Based Security

Today's internet secures *connections,* not *content:*

https://online.wellsfargo.com/policies.html

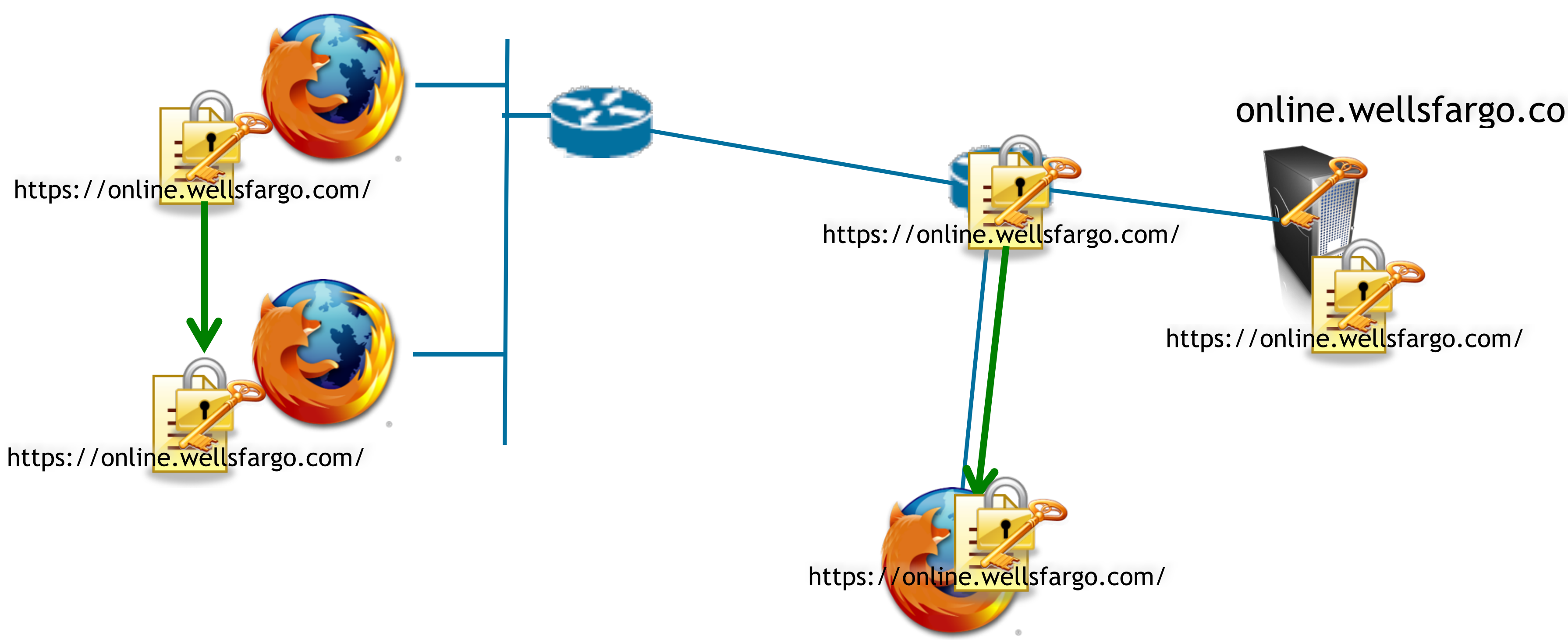


parc
A Xerox Company

Content-Based Security

Secure the *content*, wherever it travels…
…get it from anyone who has a copy.

https://online.wellsfargo.com/



Securing Content

Content Packet = 〈 *name*, *data*, *signature* 〉

Any consumer can ascertain:

- ***Integrity***: is data intact and complete?
- ***Origin***: who asserts this data is an answer?
- ***Correctness***: is this an answer to my question?

Advantages of Content-Based Security

- security travels with the content
  - secure caching: can get content from anyone with a copy, and still authenticate it
  - Confidentiality: encrypt content for access control
    - data protection travels with the content in transit and at rest
- move the security perimeter from the host to the application
  - content decrypted only inside the target application
  - effectively a networked encrypting file system
- talk about data, not about hosts
  - harder to mount an attack against a host if you can't easily address packets to it

Technical Challenges

- How do we provide high availability and assurance?
  - how do we ensure that available data is found?
  - how do we keep “real” data from being drowned in spam?
  - how do we provide better availability and resilience than today’s Internet?
  - challenge: *infrastructure protection*
- How do we actually authenticate content in practice?
  - how do you manage keys?
  - how do you decide which signers to trust? for what?
  - challenge: *user friendly key distribution/trust management*
- How do we protect promiscuously cached content?
  - how do you control access to content when requests may be fulfilled by arbitrary intermediaries?
  - challenge: *content protection and access control*

Infrastructure Protection

- CCN addresses many attacks we see today:
  - Can't address hosts directly = harder to target
  - No need for insecure indirection infrastructure(s) (e.g. DNS)
  - Content, and potentially interests are authenticated
  - infrastructure control messages are authenticated
    - CCN can use existing routing protocols (IS-IS, OSPF) unmodified but they will be better authenticated. Policy can easily associate authorized signers with namespaces they are allowed to update routing information for
- Content caching increases availability & mitigates DoS attacks
- Content not forwarded w/out interests (i.e., request) for it
- Multiple interests for same content are collapsed and one copy of content per "interested" interface is returned

parc A Xerox Company

Data plane resilience

- IP data delivery strictly follows FIB direction:
  - One-way data flow -- cannot detect failures
  - Has no effect on routing decisions
- CCN content delivery is a 2-step process:
  - Interest forwarding to set up state
  - Content traversal of interest path in reverse
- Interest forwarding state eliminates looping, allows exploitation of topological redundancies and multipath forwarding
- Content packets measure quality of selected (interest) paths ➔ lets forwarding plane incorporate congestion and fault mitigation into path decisions

New Security Challenges?

- **Content Poisoning**: Can’t fake data in CCN but what about drowning it out
  - Consumer can always verify that they have received data acceptable to them
  - Content consumers can specify desired content providers by specifying the provider’s public key
  - Content consumers can specify desired content by specifying the hash of the content
  - policy routing can drop unwanted data based on namespace

How to mitigate Content-poisoning?

1. Enforcing trust at the network layer
   - Expressive interests with enough information to enforce trust at the network layer
     - Interests identifying content hash or publisher's key
   - Minimizing the related overhead on routers
     - Provide the key in the content object
     - Make the trust related decisions (i.e., which key to trust?) on end-points
     - Use of manifests (a.k.a., secure catalogs) and self-certifying names might free most content traffic from signatures & related overheads
2. Securing the routing
   - Routing is another application on CCN. Security features in CCN makes it only easier to secure it.

For more details:
Uzun, E., *Elements of Trust in CCNx 1.0*, PARC Technical Report. 2014

parc
A Xerox Company

New Security Challenges?

- <u>**Interest Flooding Attacks**</u>: Exhaust resources in the network
  - Interests are unsolicited
  - Each non-collapsible interest consumes state (distinct PIT entry) in intervening routers
  - Interests requesting distinct data cannot be collapsed
  - Interests (usually) routed towards data producer(s)
- Unlike IP routers, CCN routers maintain rich state information that can be used to detect and react to interest flooding (and congestions)

Mitigating Interest Flooding

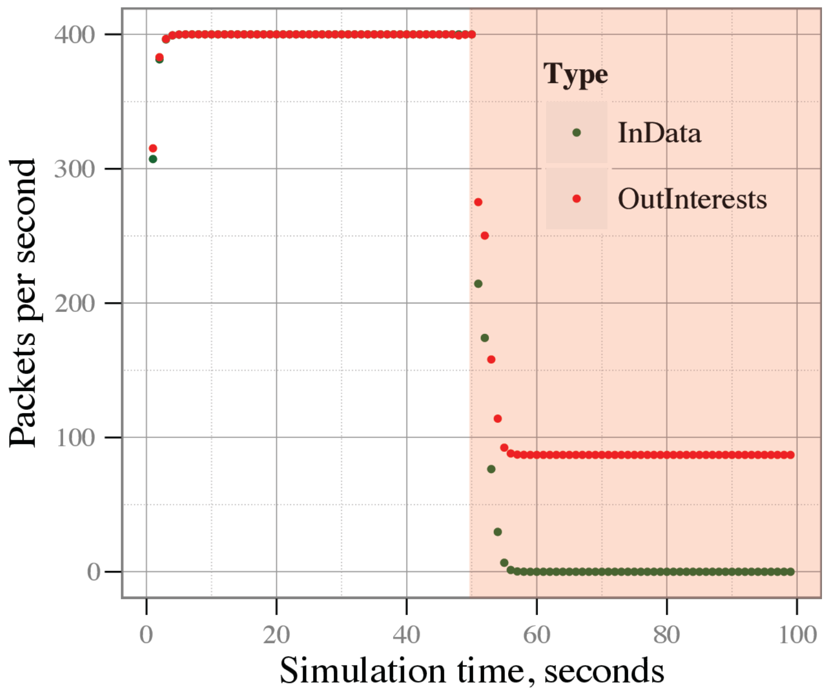
- The number of pending Interests to fully utilize a link can be estimated. E.g.,

$$\text{Interest limit} = \text{delay}(s) \cdot \frac{\text{bandwidth (Bytes/s)}}{\text{avg data packet size (Bytes)}} + \varepsilon$$

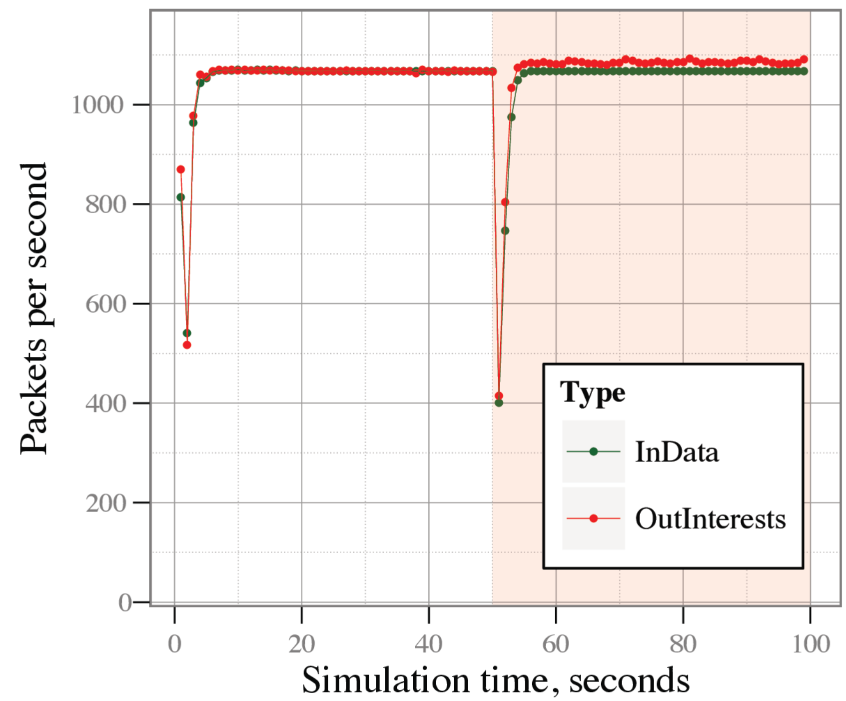
- Theoretically, CCN routers have the information needed to be able to differentiate good interests from bad ones.
    - Keep interest satisfaction statistics in routers
    - Use the statistics to differentiate/classify traffic.
    - Distribute available bandwidth per prefix (i.e., PIT space) to downstream routers based on observed recent behavior

Alexander Afanasyev, Priya Mahadevan, Ilya Moiseenko, Ersin Uzun, Lixia Zhang. "Interest flooding attack and countermeasures in Named Data Networking" IFIP/IEEE Networking 2013

Sample Results: Effectiveness of interest flooding mitigation



VS.



Graph of observed data traffic near victim.
Algorithm: Link-layer dynamic window advertisement based on observed statistics
Topology: 128-node tree topology with 50% uniformly distributed attacker population. No-caches for worst-case scenario

Alexander Afanasyev, Priya Mahadevan, Ilya Moiseenko, Ersin Uzun, Lixia Zhang. "Interest flooding attack and countermeasures in Named Data Networking" IFIP/IEEE Networking 2013

User Friendly

Key Distribution & Trust Management

- Proposing to sign every packet requires:
  - user-friendly mechanisms to manage public and private keys
  - easy to deploy mechanisms to determine trust in keys and content
- CCN itself makes this problem easier:
  - Key Distribution: one of the hardest parts is actually getting your hands on the (public) keys
    - CCN, together with a set of *naming conventions*, can make it easy to retrieve keys without pre-configuration
      - keys are just another form of data: /parc/users/euzun/key
    - We are also designing a highly scalable secure Key Resolution Service (think of secure DNS but for key resolution) over CCN that can be optionally queried for keys and revocation information.
  - Reuse of existing trust models: can easily represent any existing, deployed trust model directly in CCN
    - if there is a PKI, CCN can take advantage of it – and make it easier to manage and use
      - E.g., current Internet PKI can be used in CCN as it is.
    - if not, CCN can make it easier to build one

parc
A Xerox Company

Additional Trust Features

- CCN enables secure linkage
  - link to authenticated content
  - authenticated link to content
    - acts as a form of delegation
    - can be used to embed trust models (PKI, Web of Trust, SDSI) directly in CCN
- Can also embed these secure hyperlinks within content:
  - content can "certify" other content
- Content consumers can aggregate a securely interconnected "view" of the world, in the form of linked data
  - makes data forgery difficult – have to change too many things
  - limits the amount of work trust management has to do
    - most trust "contextual" – operating only in the context of specific data and data itself can help to authenticate keys and other content

parc
A Xerox Company

Content Protection and Access Control

- Access control by encryption
  - content encryption, key distribution transparent to CCN network layers
    - applications can tailor their use of encryption to their needs
  - common approach: a lightweight encrypting file system
    - permissions inheritance
      - associate permissions, keys with the content name hierarchy
    - group/role/attribute-based access control
      - a layer of indirection can decouple group membership from encryption
- Access control by policy routing
  - associate routing policies with content namespaces
    - policies distributed, managed using CCN itself
  - control where content itself can move
    - e.g. “content firewall” – only content in the namespace /parc/public can be sent outside the organization
  - control who can ask for content by namespace
    - Authenticate interests

Privacy Challenges in CCN

Lack of source addresses in CCN packets provide <u>better privacy</u> than IP

- There are some challenges ***if the attacker can monitor traffic close to consumers*** (e.g., in the same LAN):
  - ***Name Privacy:*** semantically related names
    - Interested in "/healthonline/STDs/.."
  - ***Content Privacy:*** unencrypted public content.
    - Retrieved content is an ".mp3" file
  - ***Signature Privacy:*** leaked signer(publisher) identity
    - Retrieved content is signed by "match.com"
  - ***Cache privacy:*** detectable cache hits/misses
    - Interests from this user usually misses caches – e.g., it is for Russian content. Or, somebody at PARC recently downloaded "hacking into your company guide".
- Most of the above challenges are can easily be solved by encrypting the sensitive part or use of a anonymizing proxy.
- For detailed overview of privacy problems and solutions in CCN, please see:
  - A.Chaabane, E. Cristofaro, M.A. Kafaar, E.Uzun. "Privacy in content-oriented networking: threats and countermeasures". ACM CCR July 2013
  - S. DiBenedetto, P. Gasti, G. Tsudik, E. Uzun. "ANDaNA: Anonymous Named Data Networking Application". NDSS'12

CCNx 1.0 vs. NDNx

NSF Named Data Networking (NDN) Project:

- Academic collaborative project that PARC was heavily involved and managed in its first phase (PARC is not in its 2^{nd} phase that started in 2014).
- NDN is based on previous generation CCNx design (v0.7x) --currently forked out as NDNx.
- From security point of view, it is yet to adapt the improvements of CCNx 1.0
  - NDN still uses selectors and exclusions (prone to content-poisoning in most cases)
  - Does prefix based content matching allowing easy cache snooping and content-poisoning attacks
  - Requires signatures on every packet with no concrete solution for trust enforcement in the network
    - Requires fetching of (potentially chain of) certificates by routers.
    - Yet to adapt a solution that could free majority of the traffic from the signature overhead without loss of security (such as manifests and secure catalogs in CCNx)
  - Handles mobility via insecure indirections that can be exploited for DoS attacks

parc
A Xerox Company