Named Data Networking and Internet decentralization: 
Steering New Application Developments 
Away from Centralized Realization

BEICHUAN ZHANG, LIXIA ZHANG
NDN COMMUNITY MEETING
MARCH 2, 2023
ACK: took inputs from two workshops & NDN retreat

- CoNEXT 2021 Interdisciplinary Workshop on (de)Centralization in the Internet (IWCI), https://conext-21-iwci.named-data.net/
  - Panelists: Geoff Huston, Henning Schulzrinne, Lixia Zhang, John Adler
  - Moderator: Alex Afanasyev
  - panel recording: https://www.youtube.com/watch?v=M-S2mj08onk
- NDN project retreat discussion, March 2022.
  - Beichuan, Lixia, Lan, Christos, Alex, Jeff, Kirk, Junxiao, Turan, Varun, and more.
- IETF DINRG Workshop on Centralization in the Internet, June 2021
  - Panelists: Jari Arkko, Trinh Viet Doan, Christian Huitema, Thomas Hardjono, Geoff Huston, Henning Schulzrinne
  - Moderators: Lixia Zhang and Kirk Kutscher
  - Workshop meeting materials: https://datatracker.ietf.org/meeting/interim-2021-dinrg-01/session/dinrg
  - Workshop recording: https://youtu.be/1kbsbvjb1zu
Where the Internet started

- Internet was originally designed as a decentralized system
  - End-to-end connections based on the always-on IP connectivity
  - Distributed routing decisions
  - Most parties running their own email, ftp servers
  - DNS as distributed name allocation system
    - ICANN *only* manages TLD allocation, each TLD domain, and all domains below, *independently* manage their own namespaces

- No central/global control, except
  - IANA manages address allocation to Regional Internet Registries
    - Also port number assignments
  - ICANN *only* handles the Top Level Domain name allocation
    Solely for the purpose of ensuring address/port/name uniqueness
How apps moved from decentralized to centralized

• In early days of Internet: organizations ran application servers to provide services for their own users
  • These are not revenue generating business

• With time, commercial app providers were born

• Once apps becoming revenue-generating business: economy of scale drives towards consolidation
  • Bigger sizes → afford more investment into better service
  • security threats increased over time: costly to mitigate failures/attacks
  → outsourcing apps/services become more attractive
  → more organizations outsource apps/services
Networking: the state of affairs

• Media streaming at scale: CDN overlays
• Conferencing at scale: supported by cloud
• IoT/smart homes: supported by cloud
• Augmented reality: supported by cloud

What cloud does not help:
• Can 2 laptops on the same table talk to each other directly?
• “What’s going on at front of the queue?”

Why not: no standard solution to identify/secure local communications
• Communication with cloud: user identities and authentication are controlled by the cloud
How we do networking today: picture from 3000 feet

1. IP: node-to-node *synchronous* communication

2. TCP: end-to-end connection for reliable delivery
   - Client to cloud server connectivity

3. TLS: authenticate cloud servers, securing the connection to them

Middle boxes (CDNs, firewalls of all sorts, MaaS, load balancers)
A popular Youtube talk, the title echoes many people’s view

Death of an End-to-End Internet
(and a way forward)
The wealth of today’s cyber giants is largely built on the foundation of aggregated individual user behaviour information → personal profile info → maximize advertisement revenue

Related factors:
- Data ownership?
- Company revenue versus user privacy protection?
- Specific regulations to safeguard basic user privacy?
As a side note:
“On Cyber Governance” by Geoff Huston

- It’s truly amazing that the sum of human knowledge is at my fingertips, instantly accessible from anywhere at any time. That's incredibly empowering.

- It’s truly frightening that all this information is only accessible through a single entity, who funds this service through an insidious economy based on surveillance capitalism.

https://www.potaroo.net/ispcol/2020-08/cgov.html
Some specifics (I): the focal point moving up

- Networking started from dominance of carriage
  - Then moved to dominance of platforms
  - Then the dominance by application services

☞ The locus of value and money shifted up the protocol stack
  - Where one can exploit centralization with minimized cost
  - Lower layer services became commodity services
Some specifics (II): surveillance economy $\iff$ free apps

- Companies investing into commercializing new apps
  - Search, email, social networking ...
  - More added over time

- They gained from a positive feedback loop:
  - More users $\implies$ more inputs for better services $\implies$ attract more users, get higher revenues

- Proliferation of free services by the cyber giants $\implies$ surveillance economy
  - The more the app providers know about specific users $\implies$ the better services
  - **AND** the more influence they have over users
    - blurring the line between service and implicit control

3/2/2023 @ NDNComm
Can Network Protocols Prevent Centralization?

• Protocols simply facilitate the movement of packets from one place to another
  • As carriers, protocols do not dictate where packets go
  • It is application deployments who make that decision.

• “protocols have not changed, but requirements changed. So we can design new protocols to prevent centralization”

Questions:

• What are those requirement changes?
• Can new protocol designs alone move the Internet towards decentralization?
  • Given they must operate within the existing architectural framework
    • communicating by pushing packets to numerical (semantic-free) address
Recall: how we do networking today

1. **IP**: node-to-node synchronous communication

2. **TCP**: end-to-end connection for reliable delivery

3. **TLS**: securing the end-to-end connection
   - patched on to TCP
   - The real security question (trust relation) outsources to 3rd parties (CAs)

Faceless entities
A sample set of cloud-independent apps (demoware)
DeftT Security in Action

Per-publication signing instead of session-based
Cert chains of every publication is validated
System trust policies are applied by the Trust Schema
Uses a shim to interface between app-specific code and DeftT

https://datatracker.ietf.org/doc/draft-nichols-iotops-defined-trust-transport
Hydra: SECURE, DISTRIBUTED Storage Framework

https://hydra-repo.io/
Developing a user-controlled smart home

- All entities possess structured, semantic names and keys
- All communication via pub-sub of named, secured data
- All data controlled by home owners
  - cloud may serve as backup storage for user named and secured data

Sovereign: Self-contained Smart Home with Data-centric Network and Security  
NpChat, a Multimedia Sharing Application over NDN

https://medium.com/@ritikk/npchat-604663a7047d

In the world dominated by big internet players like Google, Facebook, etc., most of our day to day internet traffic is routed to their servers. Virtually everything from E-commerce, Social Media, Web Streaming are increasingly controlled by some giant corporation. ...

Such a connected world requires a *decentralised end-to-end encrypted social multimedia app*. And when looking on it from Information-centric network perspective, NpChat seems quite promising.
Common features among the cloud-independent apps

Security is designed into the apps
- Instead of security patches applied to the existing unsecured systems

- User-owned identities

- User-managed security
  - authentication, authorization, policy management

- Empowering end users
  - utilize cloud services whenever feasible, with no reliance on it.

These apps adhere to, and extend, the end-to-end principle by enabling end-to-end security.
Take away

• To nudge Internet away from further centralization: enable distributed apps

• To enable distributed apps
  • User controlled (not cloud-owned) identities
  • User controlled security
    ➔ have security designed into the applications/systems
      • Without reliance on today’s “security patches” (they create communication obstacles)

• To design apps and system with intrinsic security: grow the NDN community