Decentralized and Secure Multimedia Sharing Application over Named Data Networking

Ashlesh Gawande, Jeremy Clark, Damian Coomes, Lan Wang
University of Memphis
September 25, 2019
ACM ICN 2019
Macau, China
Motivation

- Decentralized social media platform
- Blueprint for other developers
- Popular NDN apps
What’s Wrong with Centralization

- Rely on single entity
- What if it disappears?
- Single points of failure
- Censorship
- No idea how data is used
Design Requirements

- No central entity
- No single user directory
- No special infrastructure
- No single trust anchor
- User control of data
Naming

Application controlled namespace: simple to design, but needs central authority
Solution: User owned namespaces

Alice
/net/att/AliceDoe/npChat/alicedoe123

Bob
/edu/memphis/BobSmith/npChat/bobsmith321
Becoming Friends

Alice

Bob

Fetch content keys

Interests: CertA(KeyB)

Content keys:

CertA(KeyB)

CertB(KeyA)

A + B

A + B
Sharing Content

Alice

Bob

Pending sync interest
Updated sync number
File metadata
File interest
## File Transfer Time in Different Network Environments

<table>
<thead>
<tr>
<th>Data Transfer</th>
<th>Transfer Mode</th>
<th>No Pipelining</th>
<th>Pipelining</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File Size</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDN</td>
<td>IP Unicast via AP</td>
<td>10.0</td>
<td>2.5</td>
</tr>
<tr>
<td>Face</td>
<td>UDP Multicast via AP</td>
<td>24.1</td>
<td>4.8</td>
</tr>
<tr>
<td>Type</td>
<td>IP Unicast via WiFi Direct</td>
<td>70.9</td>
<td>10.8</td>
</tr>
<tr>
<td></td>
<td>UDP Multicast via AP</td>
<td>23.7</td>
<td>4.3</td>
</tr>
<tr>
<td></td>
<td>IP Unicast via WiFi Direct</td>
<td>69.9</td>
<td>10.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>113.6</td>
<td>5.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>205.5</td>
<td>14.9</td>
</tr>
</tbody>
</table>

Transfer time (seconds)

- **Notably faster over an AP**
- **Unicast and multicast perform similarly**
Local User Discovery

Bob

Carol

/edu/memphis/CarolRoe/npChat/carol1

Remembers Bob
Registers route to Bob

Remembers Carol
Registers route to Carol

Localhop Discovery interest
Reply data
Discovery Flowchart

Start discovery

- Discovered users on multicast? [Yes/No]
  - Yes: Discovered different users on DNS-SD? [Yes/No]
    - Yes: Use unicast faces for those users and multicast face for everyone else
    - No: Use multicast face for everyone
  - No: Discovered users on DNS-SD? [Yes/No]
    - Yes: Use unicast face for all discovered users
    - No: Use NDND if available
Friend Requests

Bob

Carol

Sign and fetch certificates and fetch keys as before
Friend Requests

- **Process is fast and finished in a few steps**
Sharing Friends List

Pending sync interest

Bob’s friends list

Sync update

Interest for friends list

New potential friend Alice!

New potential friend Carol!
Network Growth

- Large number of users discovered even if few people share friends
Friend Requests

Alice

Carol

Same as before, but using their certificates signed by Bob
Trust Model

Meeting in Person
Hierarchical/
Same Organization
Mutual Friends
Trust and Friendship

**Trust**  
acceptance of some key/data after verification

**Friendship**  
willingness of two users to connect

Friendship is built on trust, but trust does not require friendship.
Access Control

Pending sync interest
Updated sync data
Sync sequence no. interest
File metadata (filename, recipients, key hash)

New symmetric key
Interest for file
Interest for key
File data
Key data (file name, recipients, key hash)

For me! Fetch it!
Not for me!
Ignore it!
Encryption

<table>
<thead>
<tr>
<th></th>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MotoX</td>
<td>Nexus 5X</td>
</tr>
<tr>
<td>1.1MB</td>
<td>54</td>
<td>10</td>
</tr>
<tr>
<td>2.1MB</td>
<td>80</td>
<td>10</td>
</tr>
<tr>
<td>5.2MB</td>
<td>144</td>
<td>11</td>
</tr>
</tbody>
</table>

Access Control Cost: Data Encryption and Decryption Time (milliseconds) with Different Devices

- **Adds insignificant cost**
Content Store

Diagram showing the flow of data between a producer and two consumers, Consumer 1 (C1) and Consumer 2 (C2), over time. The diagram illustrates the synchronization of data (Sync data) and the serving of data (Serve data) between the devices. The time axis is marked in seconds (0.2 to 5).

Key actions:
- Sync data
- Fetch data
- Serve data

The diagram shows the connected and disconnected states of the devices and the flow of data between them.
Related Work: Fediverse

Federated Systems
- Relies on individual servers
- Some apps don’t encrypt server data
- Data pushed to servers; must always be online
- Step in the right direction
Related Work: NDN Apps

- Remove single point-of-failure
- Decentralization not the primary goal
  - Central application prefix
  - Single trust anchor
What We Learned

It’s feasible with right approach
Need the right design
What is Next?

- Better access control
- More complex trust models
- NDN testbed
- Better UI
- App store
Thanks!

Questions?

jrclark2@memphis.edu