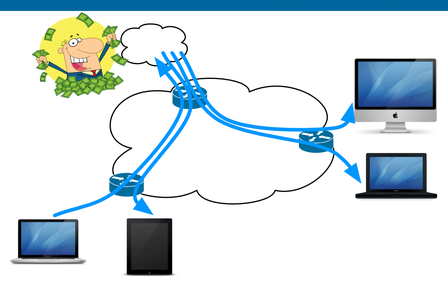
UCLA ENGINEERING
Henry Samueli School of Engineering and Applied Science
Birthplace of the Internet

ChronoChat: a Server-less Multi-User Instant Message Application Over NDN

Zhenkai Zhu, Alexander Afanasyev, Yingdi Yu, Lixia Zhang

Internet Research Laboratory

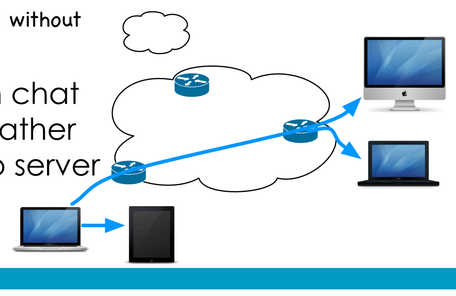
Introduction



Multi-user applications are commonly implemented using a centralized server

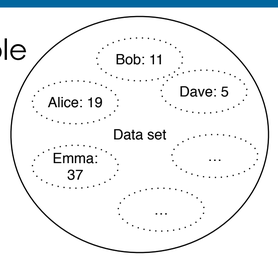
How to exchange chat messages without the centralized server?

- With NDN, we fetch chat messages directly rather than connecting to server

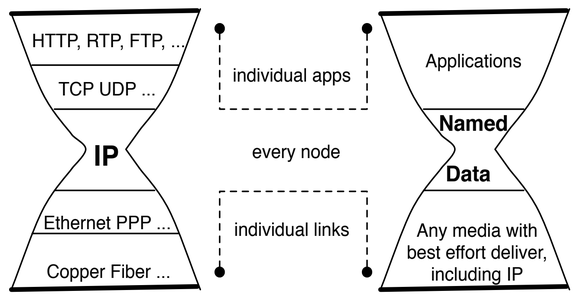


State of a data set

- A chatroom consists of multiple users
- A data set is the union of all chat messages produced by users
- By naming chat messages sequentially, a user's message subset can be represented as {name_prefix, max(seqNo)}
- The state, or knowledge, of the data set consists of such pairs.



NDN: a new Internet architecture

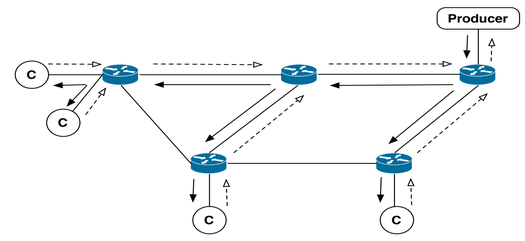


- Two packet types
  - Every piece of data has a name
  - Security is built into data

Interest
Name
Selectors
Nonce

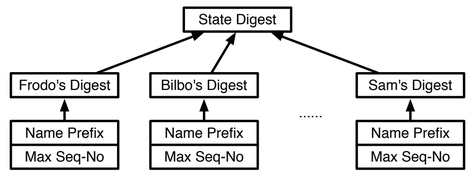
Data
Name
Content
Signed Info
Signature

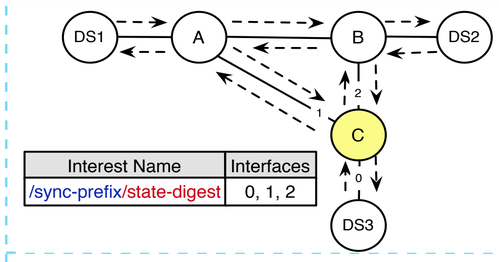
- Receiver-driven communications
  - Send Interest to retrieve Data
  - One Interest brings at most one Data packet
- Intelligent data plane
  - Router maintain "Pending Interest Table"
  - Aggregation of Interests by routers
  - Natural support for data multicast



ChronoSync: efficient state synchronization

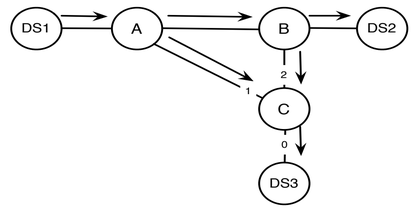
- Represent state as a digest tree
  - The root digest summarizes the state of the whole set
  - Each child node corresponds to a user's data subset





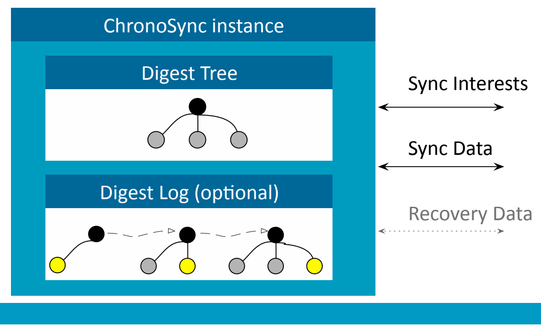
Interest Name	Interfaces
/sync-prefix/state-digest	0, 1, 2

- Users exchange root digests with broadcast Interests
  - All Interests are identical in steady state
- Whoever produces new data can reply the Interest
  - With his new {name prefix, SeqNo.} pair
  - Receivers update their hash tree and send out Interests with new root hash



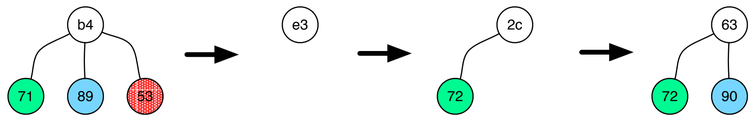
State reconcilation

- One may receive inconsistent states
  - Network delay/Packet loss
  - Simultaneous data generation
  - Network partition
- Reconcile state
  - keep a change log to identify old digest
    - send missing changes to reconcile
  - unrecognized digest
    - send current state to recover



Scalable maintenance

- Keep a scalable state & change log
  - remove inactive users
  - remove old change log
- Periodically reconstruct state & change log
  - initiated by reset interest
    - /<chatroomName>/reset
  - all users clean up state & change log
  - active users add themselves back again

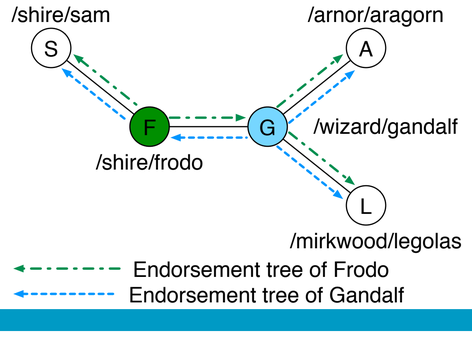


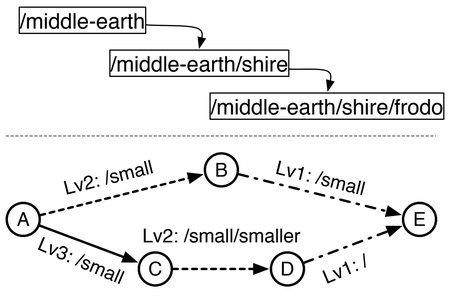
ChronoSync to ChronoChat

- Naming convention
  - **chatroom**: /ndn/multicast/ChronoChat/[chatroomName]
  - **sync interest**: /<chatroomName>/[digest]
  - **user prefix**: /<userNamespace>/ChronoChat/[chatroomName]
  - **chat msg**: /<userPrefix>/[sessionId]/[seqNo]
- Heartbeat message
  - a special chat message
  - automatically sent when user is idle
  - 1 heartbeat per minute
- Fetching strategy
  - always fetch each user's latest chat message

Security consideration

- Authenticate user membership
  - web-of-trust: through endorsements of existing users
  - new users join a chatroom by invitations





- Authenticate user identity
  - hierarchical: naming hierarchy
  - web-of-trust: 3 levels of endorsement
- Users are trusted for their own state updates and chat messages

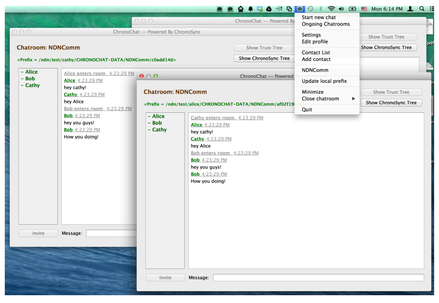
Name: /middle-earth/ChronoChat/SecretMeeting
Content:

Frodo's prefix	37	Frodo's sig
Sam's prefix	21	Sam's sig
Gandalf's prefix	96	Gandalf's sig

Signature

Name: /shire/Frodo/ChronoChat/SecretMeeting/12
Content: ....
Frodo's Signature

Implementations



- Open source native app in Mac OS X and Linux
  - https://github.com/named-data/ChronoChat
  - Binaries also available

This material is based upon work supported by the National Science Foundation under contract No. CNS-1040868.