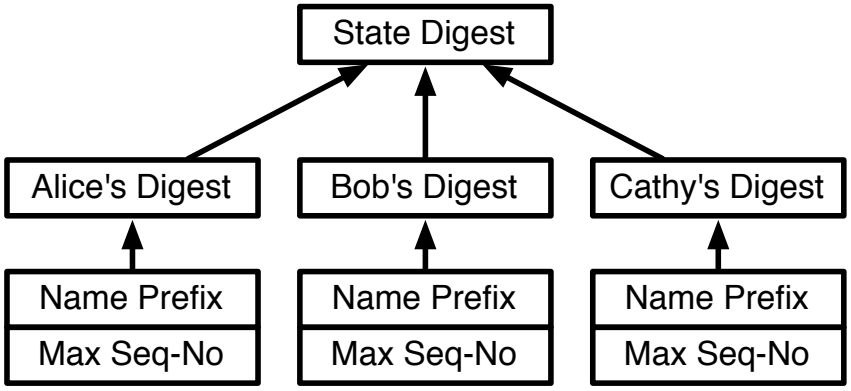
Secure Multicast Interest in ChronoSync

Yingdi
UCLA

ChronoSync

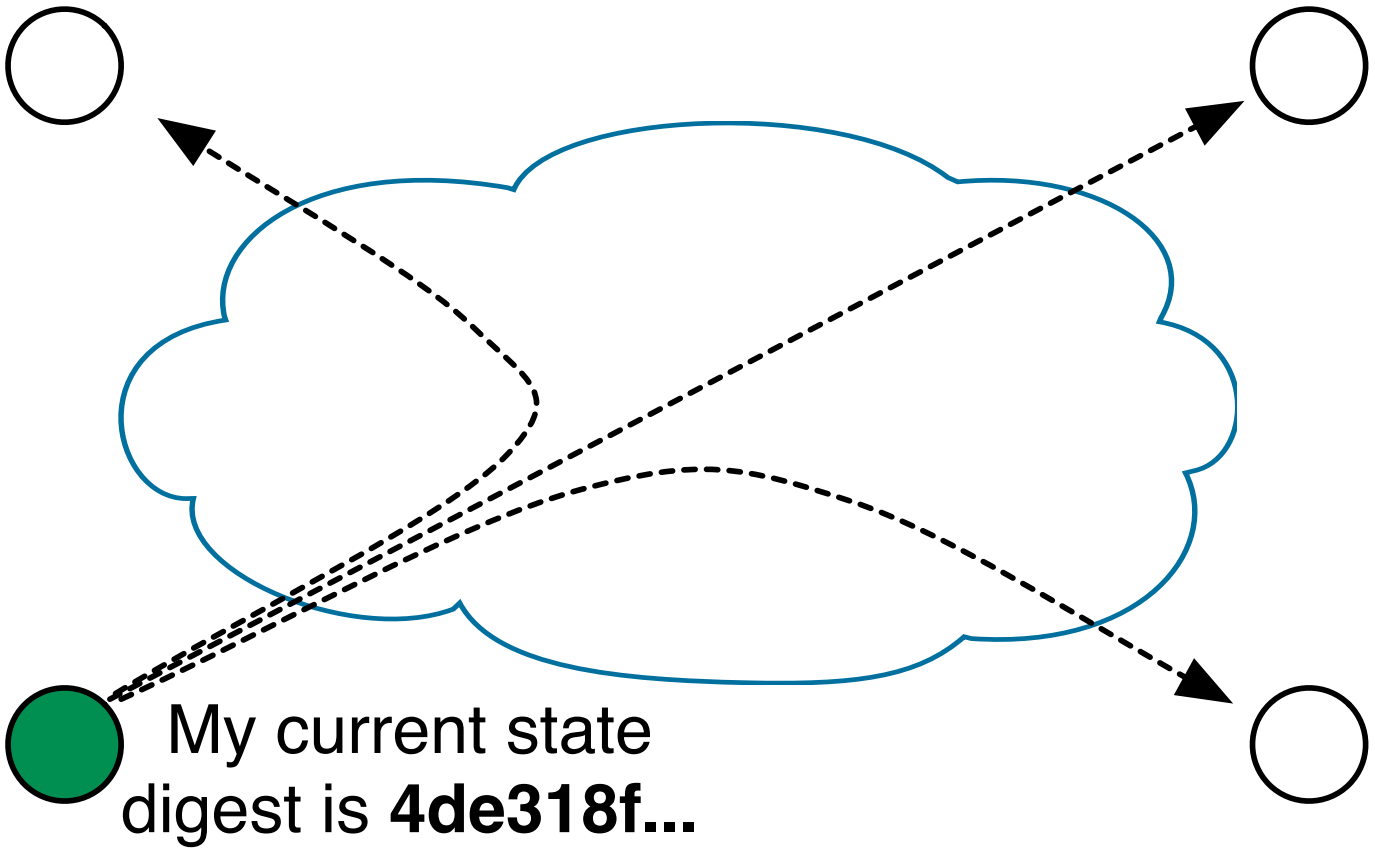
- State of a data set is expressed as a digest



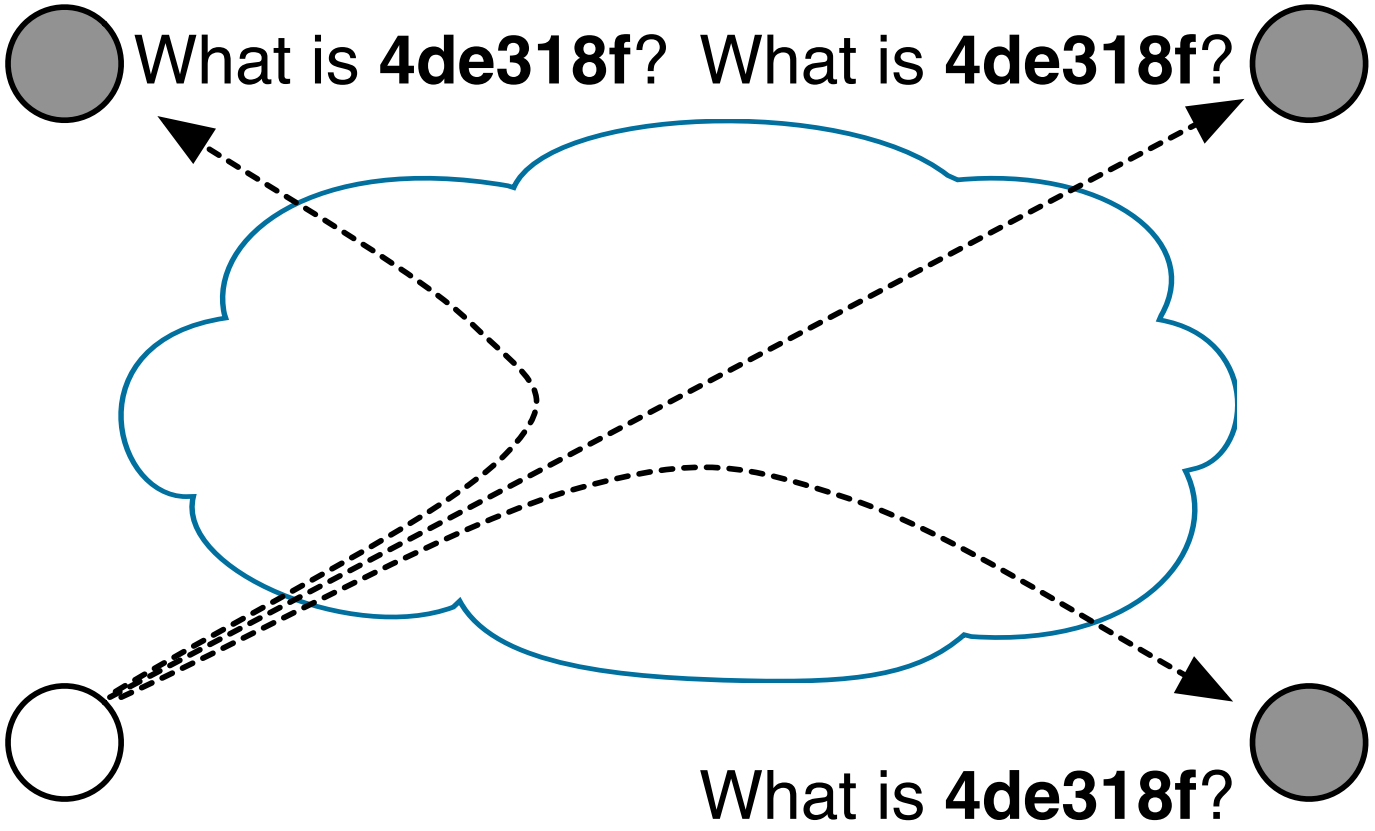
Digest	State tree modification
00a12...	<update **/ucla/alice** to SeqNo **4**>
3da49a	<update **/arizona/bob** to SeqNo **2**>
8f904d	<update **/arizona/bob** to SeqNo **1**>
c3412e	<update **/ucla/alice** to SeqNo **3**>
dd79f2	<update **/ucla/alice** to SeqNo **1**>

- Maintain a digest log to identify the state difference

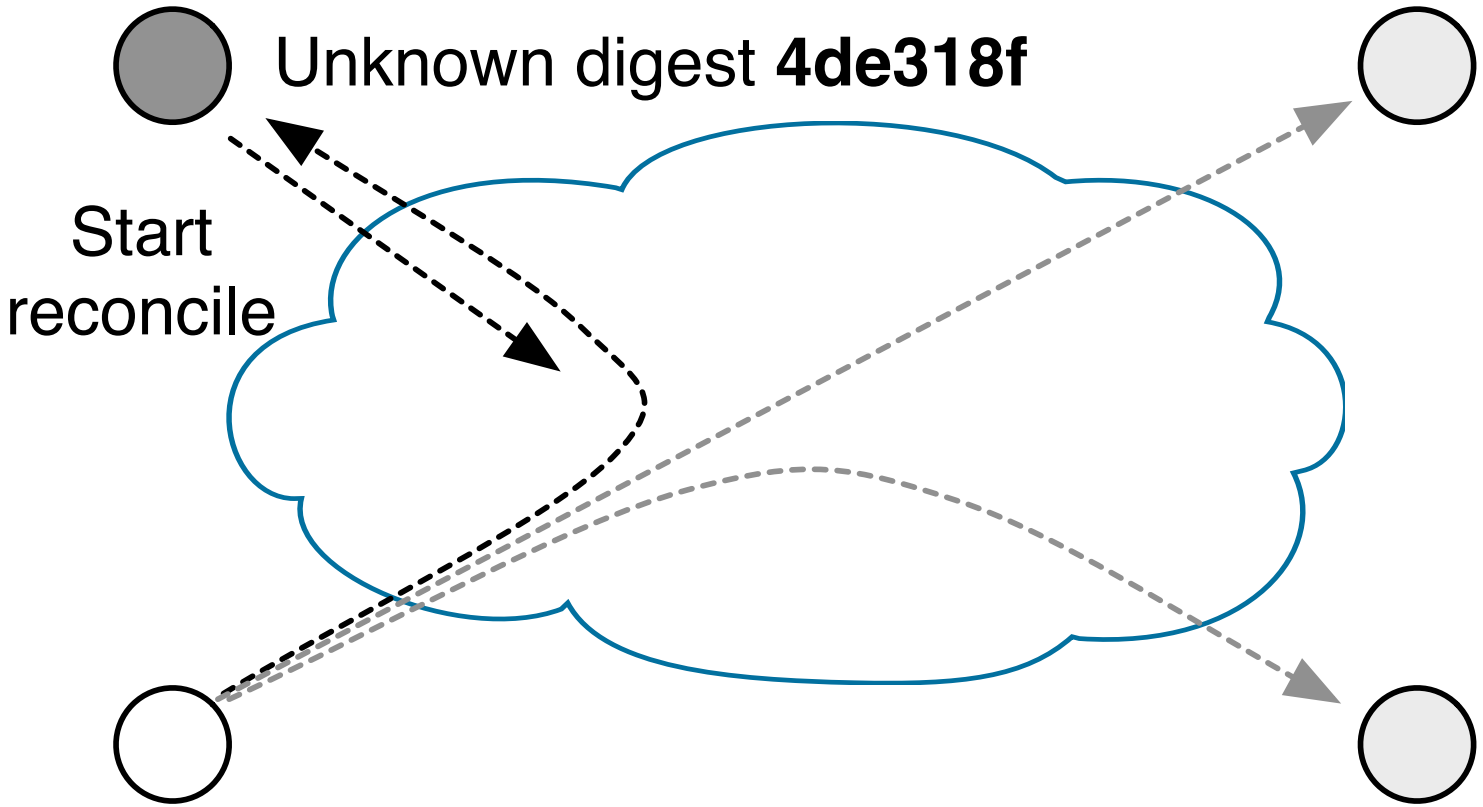
Sync interest multicast



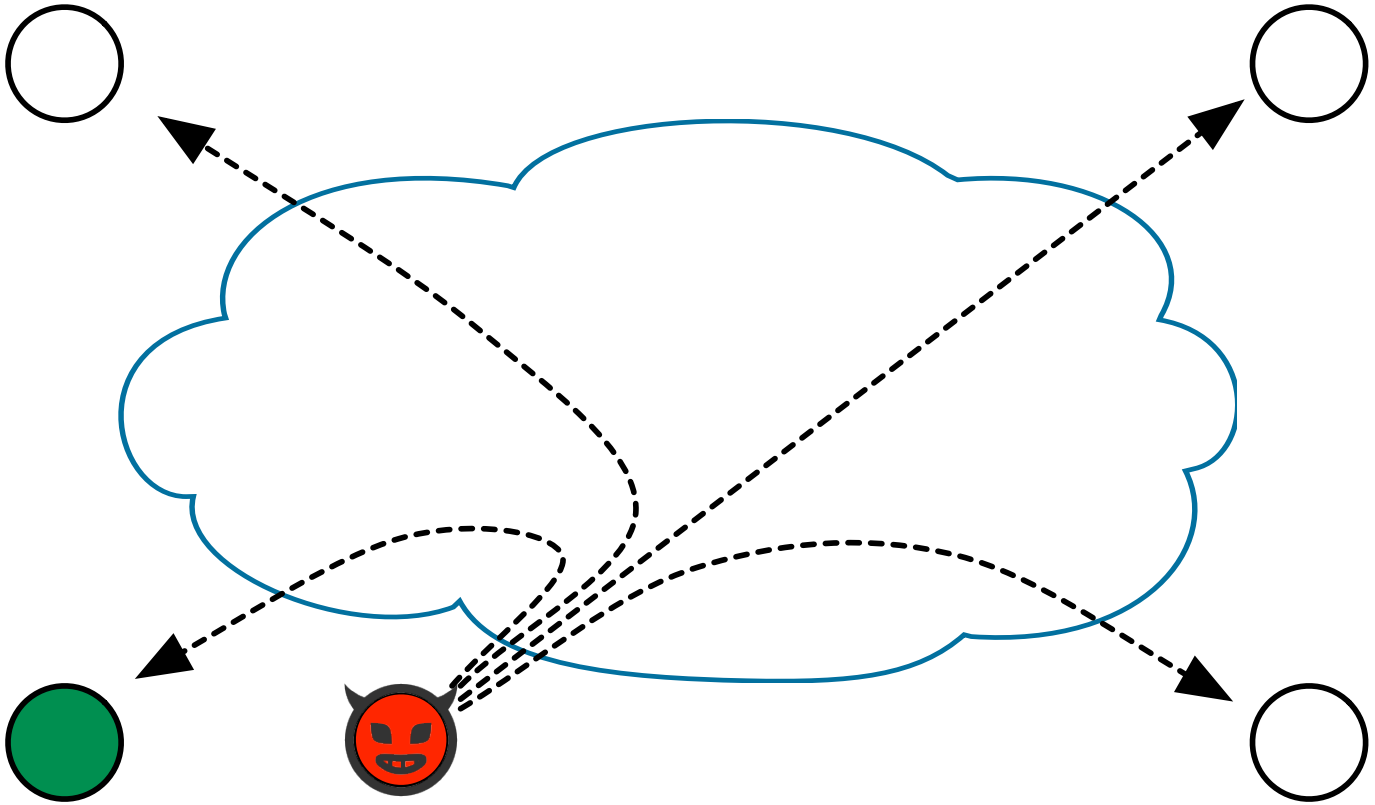
Identity state digest



Recover unknown digest



If anyone can send multicast interest…



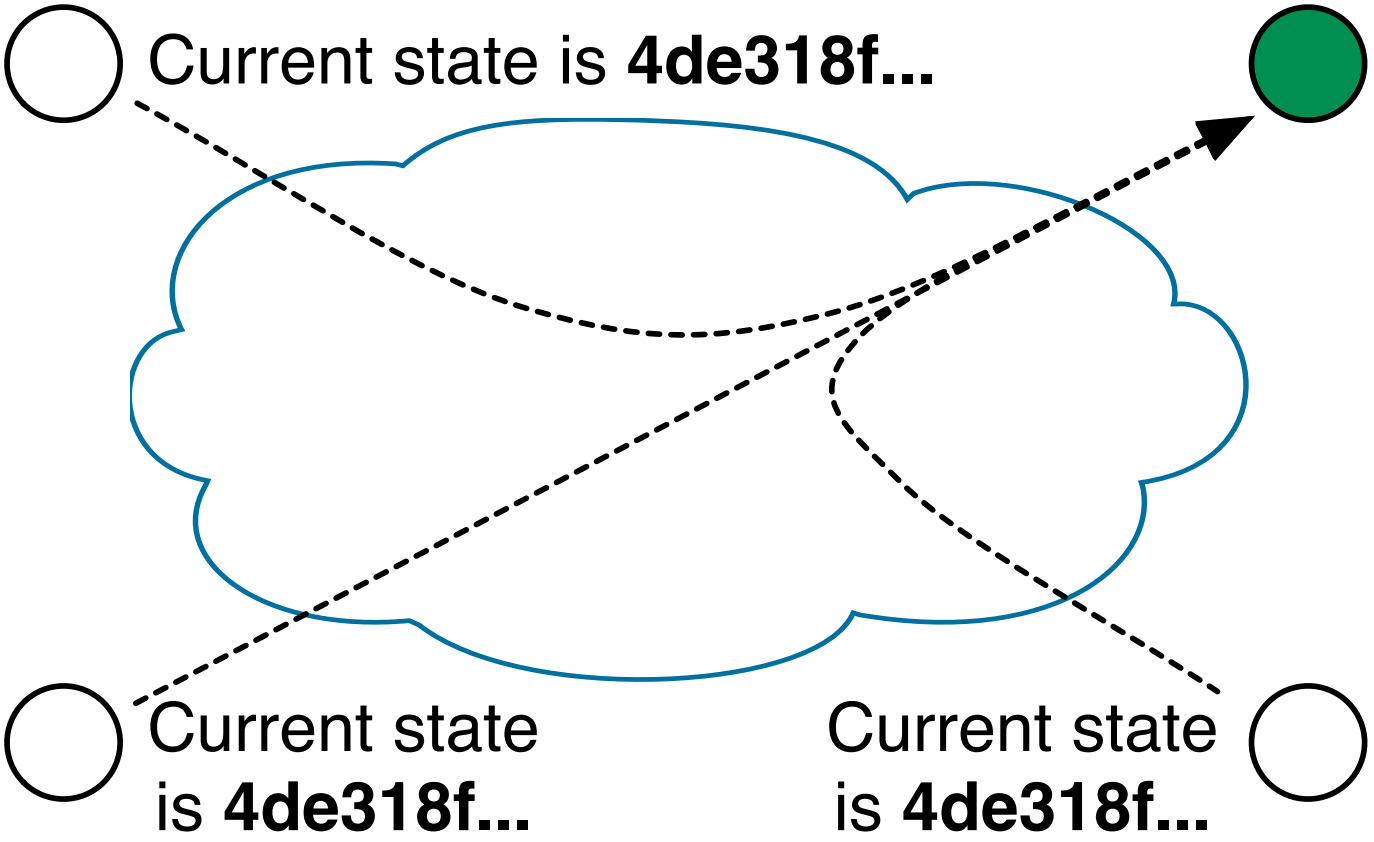
To launch attack

- Attacker needs to
  - get prefix of the sync group
  - generate a large number of sync interests with random digest
- All legitimate users will be forced to
  - do extra lookup
  - do unnecessary reconciliation
  - do extra signing
- No way to distinguish legitimate sync interests from malicious sync interests

Authenticate sync interest

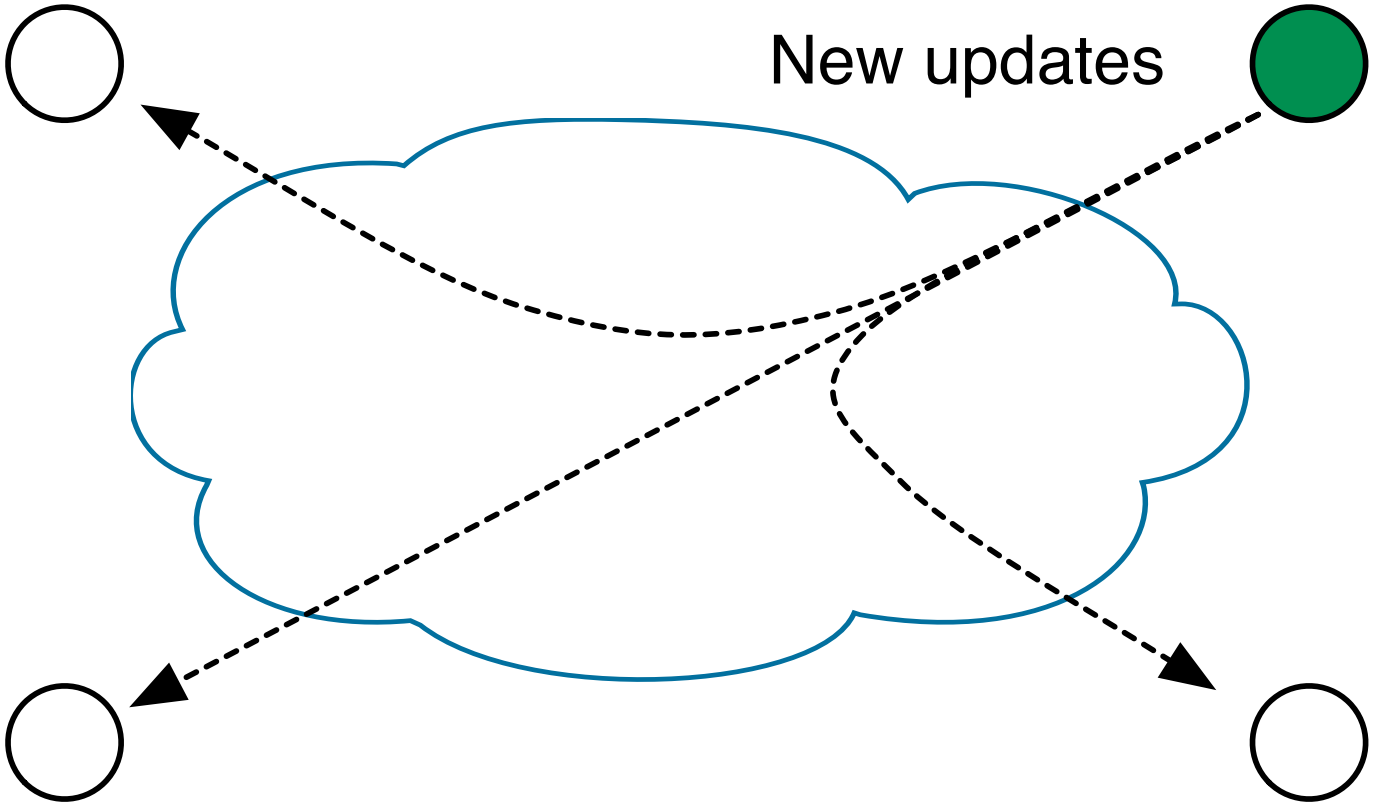
- Signed interest
- Should not prevent interests from being merged in the network

Interest merging



Interests representing the same state should be merged

Data multicast



Authenticate sync interest

- Signed interest
- Should not prevent interests from being merged in the network
  - asymmetric signatures do not work
- Symmetric signatures
  - **how to distribute the symmetric key?**

Symmetric Key Distribution

- Periodically generate a symmetric key
- Encrypt the symmetric key using the each user's public key
- Published as a single packet

- Who can generate the symmetric key?
  - designated user
    - single pointer failure
  - any user
    - resolve conflict when more than one user generate keys at the same time