Updates on HopAuth Draft - “Hop-by-Hop Authentication in Content-Centric Networking/Named Data Networking”

draft-li-icnrg-hopauth-01.txt

Ruidong Li, Hitoshi Asaeda

IETF 106 at Singapore

Contents

- Related ICNRG Draft (IETF 105)
  - draft-li-icnrg-hopauth-00: https://tools.ietf.org/html/draft-li-icnrg-hopauth-00 (The designs of HopAuth)

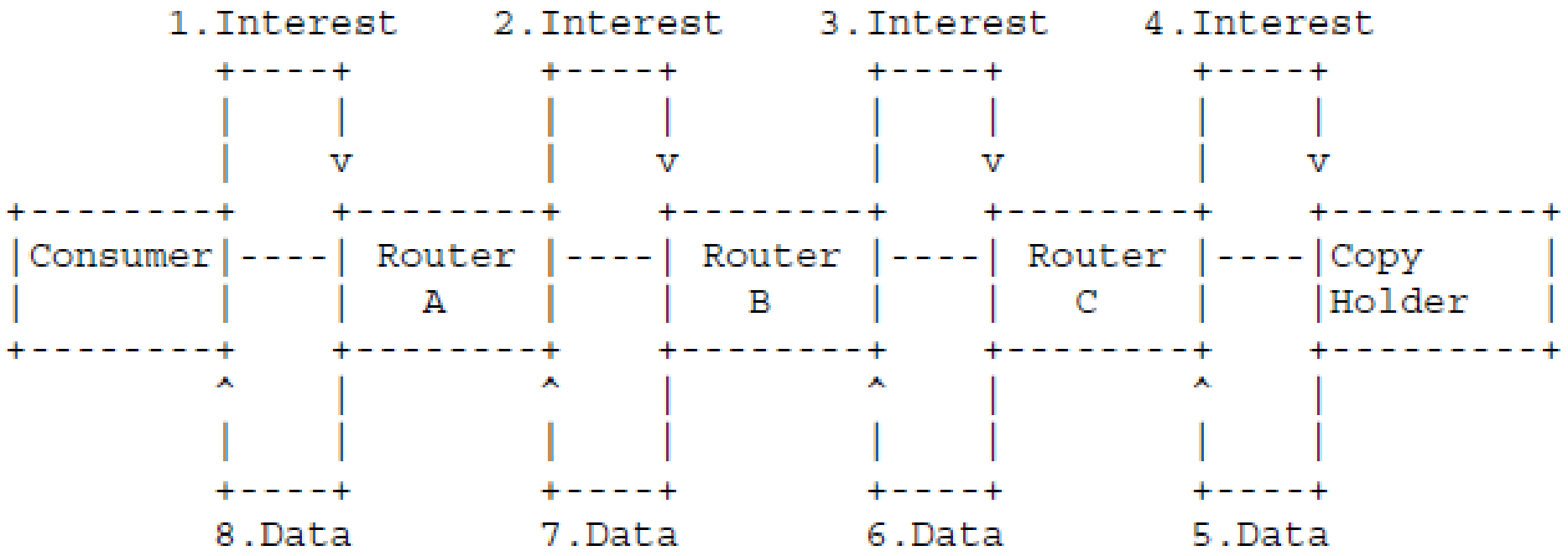
- The present ICNRG Draft (IETF 106)
  - draft-li-icnrg-hopauth-01: https://tools.ietf.org/html/draft-li-icnrg-hopauth-01 (The updates on the motivation and etc.)

Updates in v01

- Motivation clarification
- More descriptions on initial trust establishment

Content-Centric Network/Named Data Networking (CCN/NDN)

Packet Types: Interest/Data



Publisher: the entity that publishes data in network.

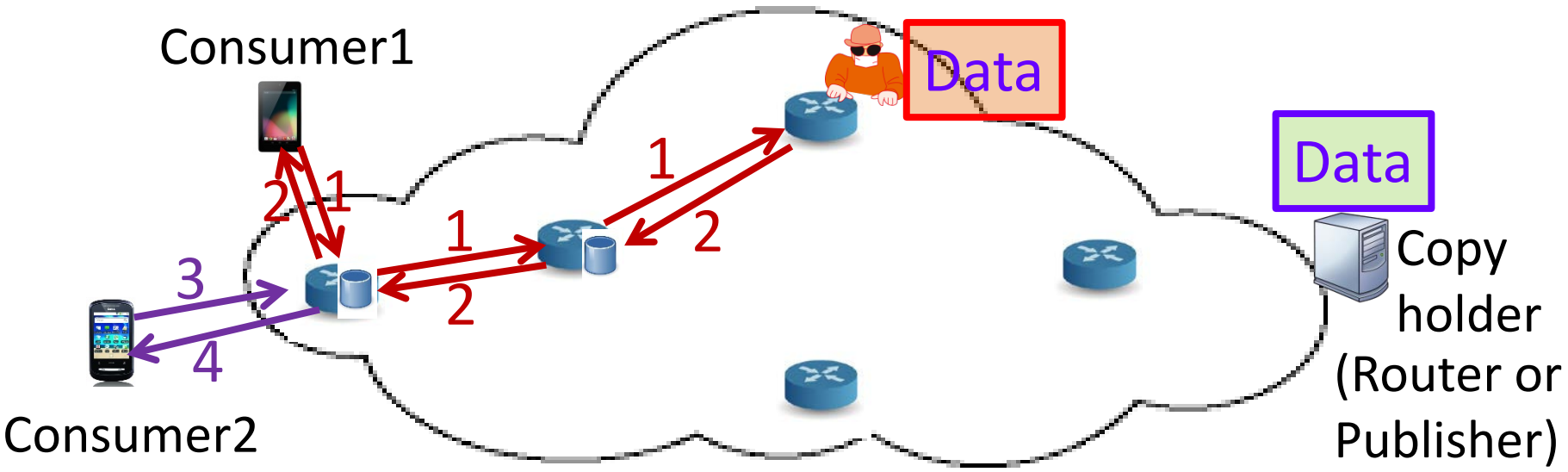
Consumer: the entity that retrieves data from network.

Copyholder: the entity that provides data to network. (Caching Router or Publisher)

Adversary Model

- A1 (Content Poisoning Attack): Impersonate a copy holder to provide fake data
  - Currently, the content is only signed with the key of the entity who publishes it.
  - Consumers may always retrieve the wrong/fake data because routers cannot detect the validity of the data
  - Necessary: all routers use the authentication service for all forwarded/cached data
- A2 (Interest Flooding Attack): Impersonate a Consumer to request data
  - Much existing work on restricting the Interest sending rate
  - Necessary: all the Copyholders (Router or Publisher) use the authentication service

Content Poisoning Attack

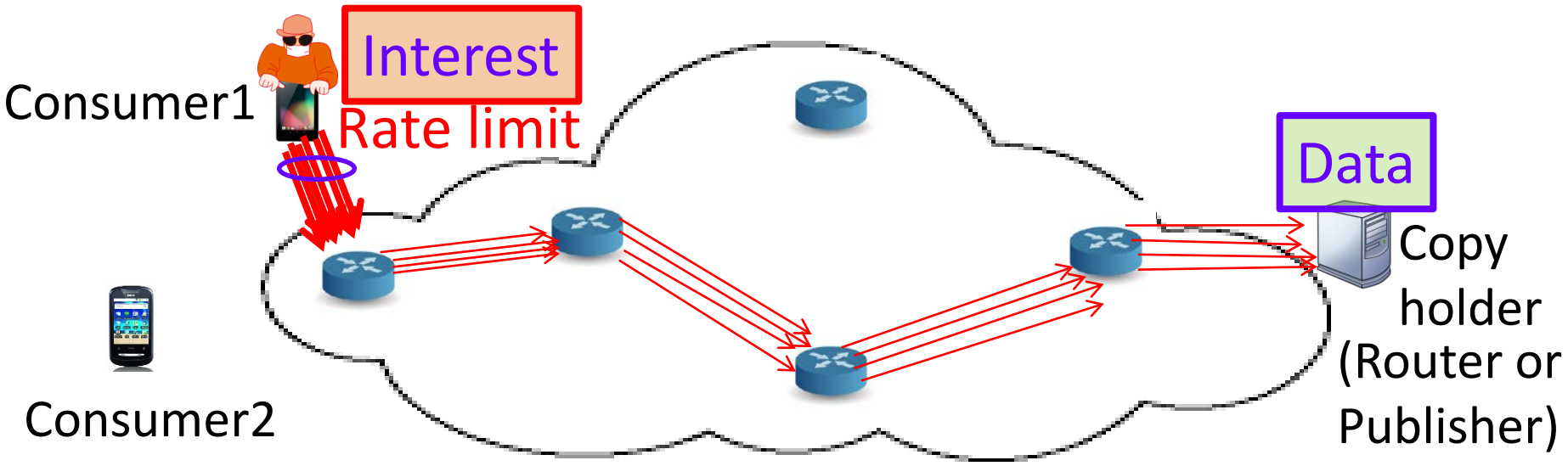


If fake/corrupted data are cached along the path,

Problem 1: Consumers always retrieve the wrong data, because the intermediate routers do not detect the cached data validity (as it's signed by attacker correctly)
Problem 2: Fake data are further cached, which pollute the routers as virus spreads.

Requirement 1: All routers along the path need to verify the data before caching. But we'd like to avoid heavy and complex tasks and central management systems.
Requirement 2: Consumers need to verify copyholder and path to identify the polluted entities besides data verifications.

Interest Flooding Attack



If malicious users flood Interests to the network to malfunction routers,

Problem1: The network may be broken.

Problem2: Even if malicious Interests can be reduced by rate limit, some malicious Interests still can reach the copyholder, and moreover it is not the ideal solution.

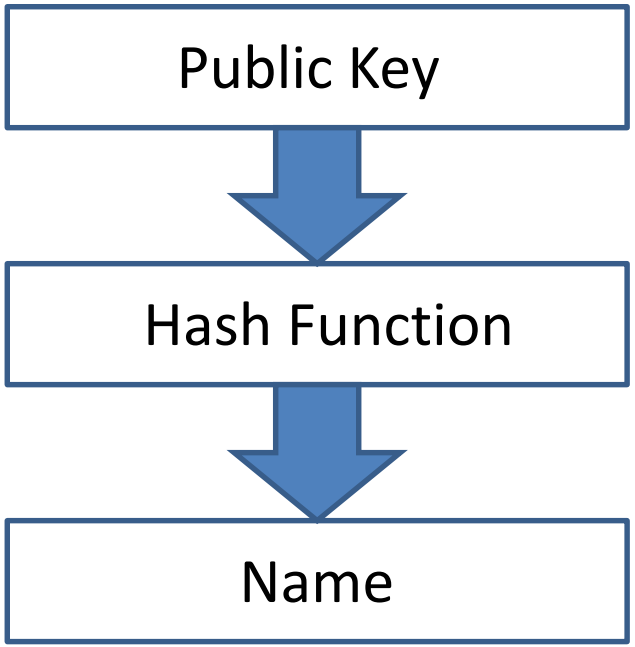
Requirement 1: The last hop routers need to eliminate the chance of Interest flooding attacks without heavy and complex tasks and central management systems.

Requirement 2: Copyholders need to verify the Interests before replying the data.

HopAuth in Summary

- Single mechanism
  - Enable the potential authentications from any consumer to data, copyholder (including publisher), and the data retrieval path
  - Enable routers to authenticate Interest
- Data-oriented mechanism
  - Does not necessarily rely on external server(s)
    - Do not exclude certificate authority (CA) as it contributes to Suspension Chain Model (later)

Self-Certifiable Naming for Initial Trust Establishment



Purpose: to prevent stealing and spoofing of the existing names.
Solution: Public key is embedded into the name to enable it to be self-certifiable. The name owner can use the corresponding private key to assert its ownership and to sign messages sent from the entity with that name.
Notice: an attacker can create a new name from an arbitrary public key. However, the attacker cannot impersonate somebody else's name.

Conclusions

- We update the HopAuth draft on motivations and initial trust establishment.

Thank you!