Requirements for Key Management Schemes in CCN/NDN

Ruidong Li, Hitoshi Asaeda

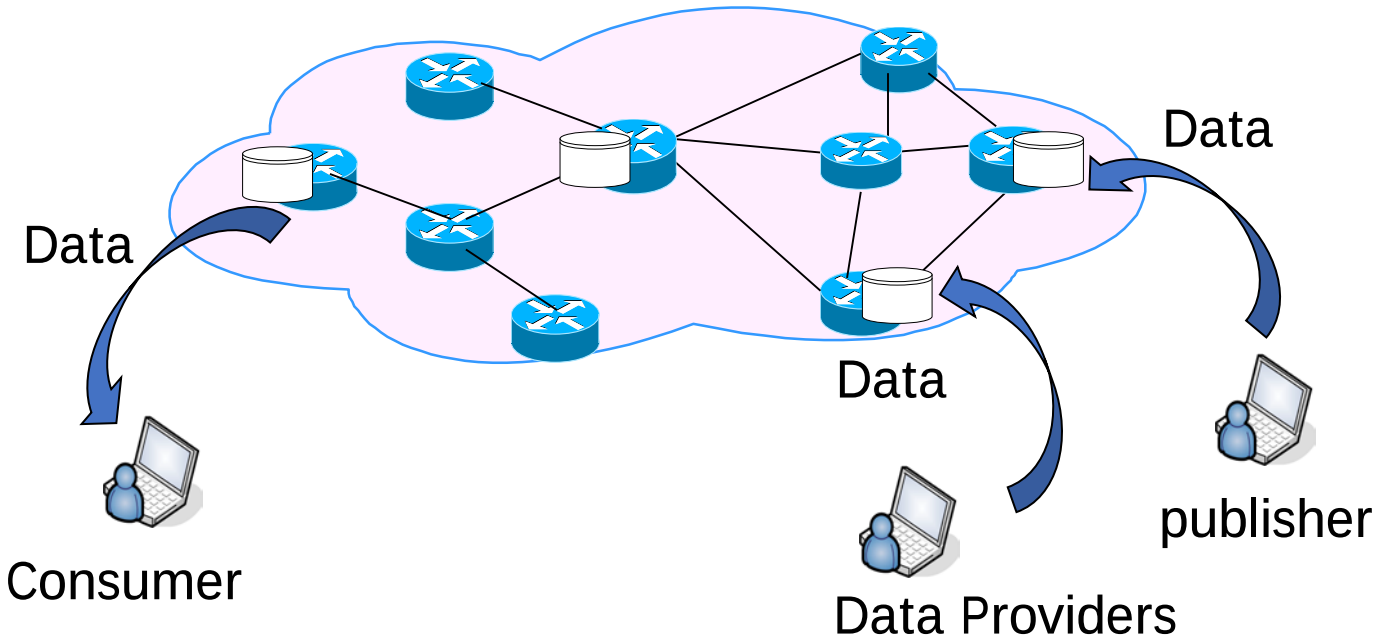
National Institute of Information and Communications Technology (NICT)

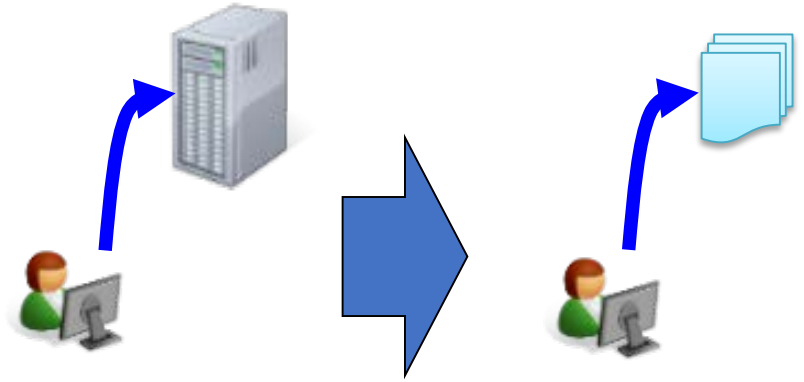
Outline

- Content-Centric Network/Named Data Network
- Key Management (KM) Scheme
- Related Work
- Network Operations and Use Scenarios
- KM Requirements for CCN/NDN
- Our Related Work

Content-Centric Network/Named Data Network

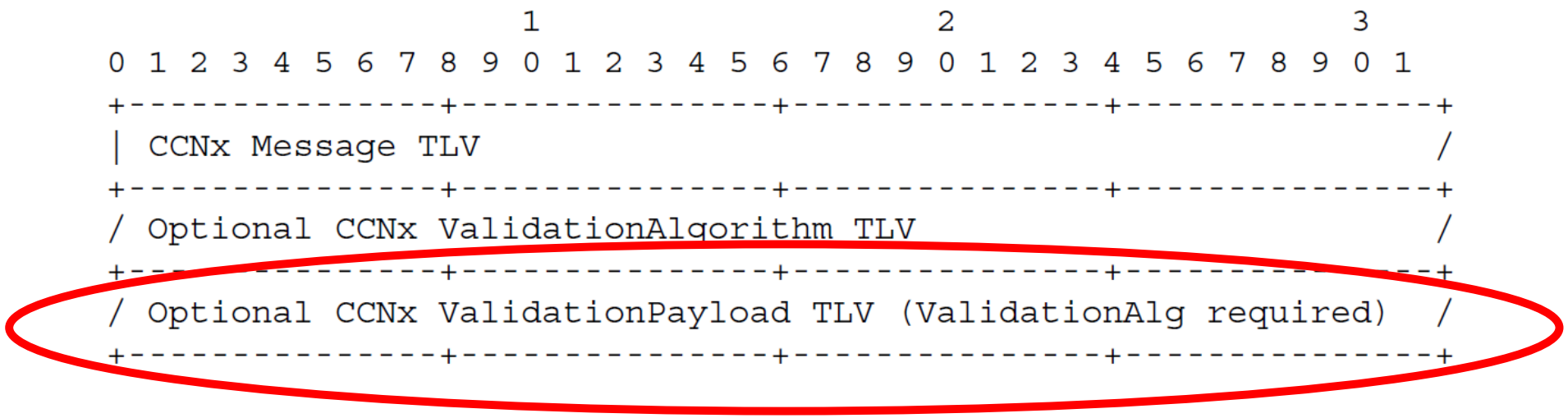
- Pulling based data retrieval
- Name-based interest/data forwarding





How to enable users to trust data?

Only Signature is not enough



- **How to get the trustable key for validation?**

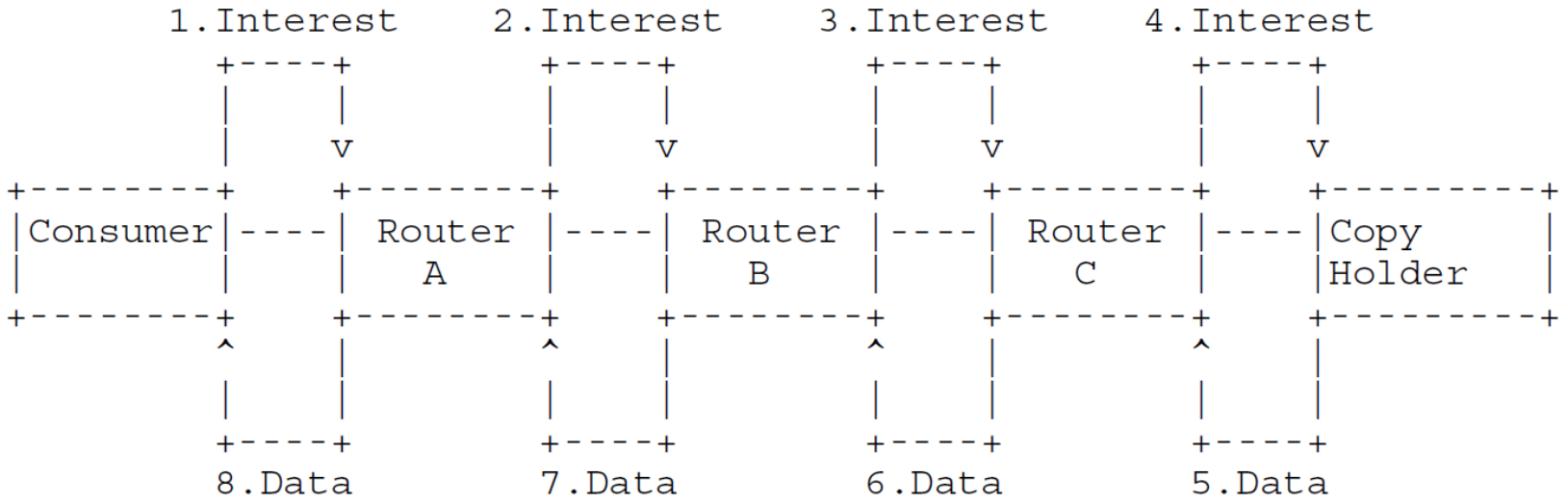
Key Management (KM) Scheme should be provided parallelly if signature or other cryptographic mechanism is used.

[1] CCNx Messages in TLV Format, draft-irtf-icnrg-ccnxmessages-06

Key Management Scheme

- **KM Scheme:** Manage the cryptographic keys throughout their lifecycles to establish and maintain the trust among entities for protecting system.
- It includes the procedures for the generation, delivery, storage, protection, update and revocation of cryptographic keys or certificates.
  - **P1 (Key Generation), P2 (Key Agreement), P3 (Key/Certificate Delivery), P4 (Key/Certificate Revocation), P5 (Key Storage), P6 (Key/Certificate Update), P7 (Key Backup), P8 (Compromise Recovery)**
- **The systems to be protected**
  - CCN/NDN infrastructure and network operations
  - Use Scenarios: US1: Disaster Networking, US2: Video Streaming, US3: Internet of Things (IoT)

CCN/NDN Operations (to be protected)



Request/Reply for data retrievals

Entities:
Consumer, Router,
Copy holder, Publisher

- **Violating trust of consumers** (Malicious data-request attacks): Impersonate consumers to create a flood of interests
- **Violating trust of copy holders** (data poisoning attacks): Impersonate copy holders (e.g., routers or publishers) to provide fake data.
- (**Severe**: Quickly pollute the router caches as the virus spreads, because routers cache the fake data, redistribute them, and other intermediate routers re-cache them.)

US1: Disaster Networking

- [2]: List the Emergency Support and Disaster Recovery as one of ICN Baseline Scenarios
- [3]: Outline the research directions for using ICN in disaster scenario.
- **Features**: Server down, in-network caching enabling movable data, fragmented networks
- **Violating trust of publisher or data provider**:
  - **For one fragmented network**: Deliberately disseminate or exchange the fake information to common users.
  - **For several fragmented networks**: Impersonate publisher/copy holder of other fragmented network to disseminate fake information for different fragmented networks

[2] Information-Centric Networking: Baseline Scenarios, RFC 7476
[3] Research Directions for Using ICN in Disaster Scenarios, draft-irtf-icnrg-disaster-03

US2: Video Streaming

- [2]: List real-time communication scenario including video transmission as one of ICN Baseline Scenarios
- [4]: Adaptive video streaming over ICN
- **Features**: Stricter requirements on QoE, low delay for the consumer, group communication, and in-network caching video data improving transmission performance
- **Violating trust of consumer**: Impersonate the consumers with right to retrieve data
- **Violating forward and backward trust**: The consumer can illegally get the previous data when she newly joins a video service. Also she can illegally continue to retrieve the data even her key has expired.

[2] Information-Centric Networking: Baseline Scenarios, RFC 7476
[4] Adaptive Video Streamingover Information-Centric Networking (ICN), RFC 7933

US3: Internet of Things

- [2]: List Internet of Things as one of ICN Baseline Scenarios
- [5]: Apply information-centric network to IoT
- **Features**: resource-constrained devices, heterogeneity on the underlay networks and operators, privacy, in-network caching helps fast data sharing
- **Violating trust of publisher, consumer, router**: impersonate sensor to publish data, impersonate routers to provide data, impersonate consumer to collect data

[2] Information-Centric Networking: Baseline Scenarios, RFC 7476
[5] Design Considerations for Applying ICN to IoT, draft-irtf-icnrg-icniot-01

Existing Key Management Schemes

- Kerberos – Symmetric key management relying on centralized server
- MSEC – Group key management relying on centralized server
- X.509 – Public key certificate management relying on centralized servers
- PGP – Public key certificate management relying on introduction and trust chain
- RPKI – Protect the DNS system
- **Problems**:
  - **Service mismatch**: Authenticate one specific entity based on end-to-end communication paradigm **vs.** Authenticate unpredictable entity with data based on data-centric communication paradigm
  - **Delay enlargement problem**: Need additional procedure(s) to request key/certificate for authentications

Requirements for protecting network operations

- **R1 (Data-centric design)**: Any router or consumer can easily authenticate the data, publisher, and copy holder, and any copy holder can easily authenticate consumers.
- **R2 (Secure registration)**: To guarantee the binding between name and real world identity.
- **R3 (Efficient revocation)**: To revoke the compromised or invalid key with low cost.
- **R4 (Efficient key update)**: To update key periodically without causing much overhead.
- **R5 (Key/certificate storage and caching)**: Improve the key/certificate distribution efficiency with in-network caching.
- **R6 (Routing Security)**: Enable the protection on the information exchanges among the routers.
- **R7 (Low bandwidth consumption)**: The KM scheme should have a negligible impact on bandwidth consumption.
- **R8 (Minimal additional delay)**: The KM scheme should only cause minimal (ideally zero) additional delays to data retrieval.

Requirements for protecting disaster networking with CCN/NDN

- **R9 (Availability)**: KM should be provided to make the authentications to data originator be possible, even the network is fragmented or disconnected. It also requires the KM service provision to enable cross-fragmentation authentications.
- **R10 (Energy efficiency)**: KM should not consume much energy of mobile devices for data exchange.
- **R11 (Robustness)**: KM should provide methods to bind a new name with a real-world identity, because there must be many newly assigned terminals for the refugees.
- **R12 (Revocation synchronization)**: The revocation for the identities should be synchronized for the fragmented networks.

Requirements for protecting video streaming over CCN/NDN

- **R13 (Backward and forward secrecy)**: KM should be provided to prevent a new consumer from decrypting the data published before it joined the streaming group and prevent a leaving consumer from accessing the further video data, even they are provided by the servers or in-network caches.
- **R14 (Light-weight)**: The KM should be light-weight for video data decryption.
- **R15 (Efficient key revocation)**: The revocation of keys should be efficient and prevent the further in-network cached data from being decrypted using the compromised or expired keys.
- **R16 (Scalability)**: The KM should enable thousands or millions of consumers, routers, and publishers. For example, the Olympic games or the football games attract a huge number of consumers simultaneously.

Requirements for protecting IoT using CCN/NDN

- **R17 (Low Energy Consumption)**: The KM should not consume much energy, especially when running on the constraint devices.
- **R18 (Heterogeneity)**: The KM should enable the sensor data to be provided to the devices over heterogeneous platforms managed by different operators .
- **R19 (Privacy preserving)**: The KM should protect the privacy of the sensor data, even they are cached in the network.

Conclusions

- Introduce the key management scheme
- Identify the potential risks for the network operations and use scenarios
- Identify the KM requirements for network operations and use scenarios

- **Next step**
  - **Case 1:** Maintain as is (i.e., **Requirement** draft)
  - **Case 2:** Include potential solutions and rewrite "**Requirements and solutions** for Key Management Schemes in CCN/NDN"

Comments welcome!

Our Related Work

1. R. Li, and H. Asaeda, "Secure In-Network Big Data Provision with Suspension Chain Model," *Proc. IEEE INFOCOM BigSecurity workshop*, Honolulu, Apr. 2018. (to be appeared)
2. R. Li, H. Asaeda, J. Li, and X. Fu, "A Verifiable and Flexible Data Sharing Mechanism for Information-Centric IoT," *Proc. IEEE ICC 2017*, Paris, May 2017.
3. R. Li, H. Asaeda, J. Li, and X. Fu, "A Distributed Authentication and Authorization Scheme for In-Network Big Data Sharing," *Elsevier Digital Communications and Networks*, vol. 3, issue 4, pp. 226-235, Nov. 2017.
4. R. Li, H. Asaeda, and J. Li, "A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT," *IEEE Internet of Things Journal*, vol. 4, issue 3, pp. 791-803, Jun. 2017.