Requirements for Name Resolution Service in ICN

ICNRG interim meeting, Berlin

Jungha Hong

ETRI

Updated Table of Contents

1. Introduction

   - Document goals and outline

2. Appropriateness of NRS in ICN

   - Why we need NRS

3. Architectural considerations

   - How NRS can fit into overall ICN architecture

4. Use cases in terms of mapping record types

   - Name to locator/another name/some other values/…

5. Requirements

   - Scalability/latency/locality/security/…

Document goals

- Provides motivation to consider NRS as a prominent challenge in designing an ICN architecture
    - Trying to get the consensus of ICNRG on appropriateness of NRS for ICN
- Provides requirements for NRS in ICN

Why we need NRS (1)

- ICN routing is to find a NDO based on its name
- Three steps of ICN routing

  1) Name resolution

  - Translates name of the requested NDO to its locator

  2) Discovery

  - Routes the request to the NDO

  3) Delivery

  - Routes the NDO to the requestor

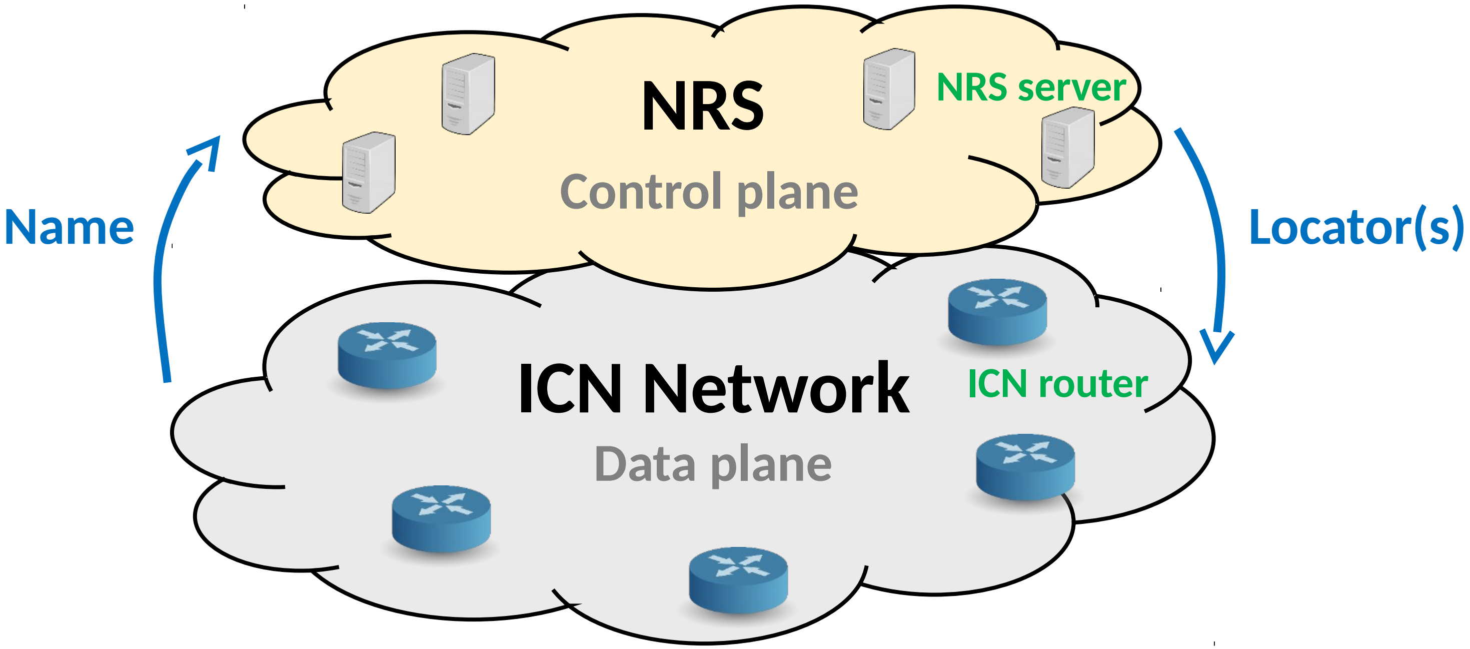
- ICN routing schemes according to the combination of the above steps
  - Route by name routing (RBNR) --> 2~3 steps
  - Lookup by name routing (LBNR) --> 1~3 steps
  - Hybrid routing (HR) --> RBNR + LBNR
- NRS is required unless RBNR itself is chosen in ICN
  - This is cited from draft of ICN research challenges

Why we need NRS (2)

- NRS is needed to efficiently support
  - Flat name(ID)
    - Self-certifying IDs, etc.
  - Mobility
    - Provider/host mobility
- References on NRS as architectural requirements
  - There are several ICN projects which has NRS as an impo rtant component in the architecture
    - NetInf, MobilityFirst, etc.
  - Name resolution is one of challenges in ICN for IoT

How to fit NRS into ICN architecture

- Distributed system as an infrastructure
- Control plane separated from data plane



Use case 1: Name to locator(s)

- Mapping name to locator(s) is a primary record type in NRS
  - Here, locator denotes routable information
  - Name can be hierarchical or flat
- A name can be mapped into multiple locators due to in-network caches
- Through the mapping, provider/host mobility can be supported efficiently and inherently

Use case 2: Name to name (alias)

- Even in RBNR scheme, if provider changes the name to another name which is designed for aggregation by provider, resolving the initial name to the aggregated name is required [quoted from ICN Challenges]
- Example: we name this contribution as “NRS motivation”, but the IRTF (provider) may change the name to “/ietf/irtf/ICN/NRS/motivation”

Use case 3: Name to IP address

- In terms of incremental deployment, even RBNR would need a mapping between name and IP address to access the current Internet (IP network) if necessary

Requirements (1)

- Scalability
  - Scalable to support a large number of NDOs as well as users/publishers
    - The number will increase more than the order of 10^{15} by the sensor data in IoT
- Low latency
  - Low latency for mapping information lookup
    - Processes multiple name resolution queries at the same time to browser one web-page which includes several data objects in it
- Fast update
  - Fast update in a highly dynamic environment
    - Supports frequently created/disappearing copies as well as moving NDOs
- Low maintenance cost
  - Some parts of the system may grow or shrink dynamically

Requirements (2)

- Locality
  - The system has to make use of any available copy and to keep r esolution and data retrieval local to improve network efficiency
- Deployability
  - Deployability is important for a real world system
- Resilience
  - If the resolution service fails, there is mostly no way for the use r to reach other end systems as the user knows only their IDs
- Fault isolation
  - The failure of a part of the distributed system should only have a local impact

Requirements (3)

- Security
  - Access control
    - A user may want to make a data copy known and accessible only within the local network
  - Authentication
    - Users/nodes that register themselves with NRS server require a uthentication to ensure who claims to be
    - The attacker can act as a fake NRS server which causes disruptio n or intercepts the data
  - Data confidentiality/integrity
  - Privacy
    - No privacy information in the system

Comments or questions?