Architectural Considerations of ICN using Name Resolution Service
draft-hong-icnrg-icnnrs-01

Abstract

This document discusses architectural considerations and implications of Information-Centric Networking (ICN) related to the usage of the Name Resolution Service (NRS). It describes how ICN architecture changes and what implications are in the routing system when NRS is utilized in ICN.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 3, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Regarding IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
Information-Centric Networking (ICN) is an approach to evolve the Internet infrastructure to directly access Named Data Objects (NDOs) by its name, i.e., the name of NDO is directly used to route the request to the data object. Such name based routing in ICN poses a number of issues, which are not solved yet in ICN. These issues includes global scalability of routing, producer mobility, off-path cache, etc. In order to address these issues, the name resolution function has been applied to several ICN projects and literature [Afanasyev][Zhang2][Ravindran][MF][Bayhan].

The requirements of Name Resolution Service (NRS) has been discussed in [NRS] which focus on designing NRS itself in terms of service, system and security aspects. As implementation of NRS, few NRS systems has been introduced in ICN. [BNRS] is an NRS system utilizing bloom filter to support a flat name based routing and [NRS_CCNx] is another NRS implemented on CCNx to support a scalable routing system for CCN. [NRS] has been well discussed on the considerations and requirements of NRS. However, it is necessary to discuss the ICN architectural issues considered when NRS system is implemented in ICN.

Thus, this document describes how ICN architecture changes and what implications are in the routing system when Name Resolution Service
(NRS) is utilized in ICN. It also discusses ICN architectural considerations for a NRS.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Background

The name based routing in ICN poses a number of issues, such as global scalability of routing, producer mobility, off-path cache, etc., which are not solved yet in ICN. In order to address these issues, the name resolution function as a Name Resolution Service (NRS) has been applied to several ICN projects and literature:

- **Routing scalability**: In ICN, application names identifying contents are used directly for packet delivery, so ICN routers run a name-based routing protocol to build namebased routing and forwarding tables. As same as scalability of IP routing, if non-aggregated name prefixes are injected to the Default Route Free Zone (DFZ) of ICN, then they would be driving the growth of the DFZ routing table size. Thus a NRS can be used as a solution to keep the routing table size under control, where the NRS resolves name prefixes which do not exist in the DFZ forwarding table into globally routable prefixes such as NDNS in [Afanasyev].

- **Producer mobility**: In ICN, if a producer moves into different authority domain or network location, then the request for a content produced by the moving producer with the origin name would be hardly forwarded to the moving producer. Especially in a hierarchical name scheme, producer mobility support is much harder than in a flat name scheme since the routing tables related in broad area should be updated according to the producer movement. Therefore, various ICN literatures such as MobilityFirst [MF] would adopt NRS to retrieve the producer’s location.

- **Off-path caching**: Caching in-network is considered to be a basic architectural component of an ICN architecture and caching approaches can be categorized into off-path caching and on-path caching based on the location of caches in relation to the forwarding path from a original server to a consumer. Off-path caching, also referred as content replication or content storing, aims to replicate content within a network in order to increase availability, regardless of the relationship of the location to the forwarding path. Thus, finding off-path cached objects is not trivial in name based routing of ICN. In order to support off-
path caches, replicas are usually advertised into a name-based routing system or into NRS such as in [Bayhan].

Thus, this document discusses architectural considerations and implications of ICN when NRS is needed and utilized in ICN to solve such issues due to the name based routing in ICN.

4. Implications of NRS in ICN

In general, NRS is not mandatory in an ICN architecture and the majority of ICN projects use the name based routing which omits the name resolution. Thus adopting a NRS would change the ICN architecture at least on procedures, latency, and security:

- **Procedure**: When NRS is adopted into an ICN architecture, the procedure of the name resolution has to be added into ICN overall procedures. On changing procedures, there are certain things that have to be decided such as who and how the resolution does.

- **Latency**: When NRS is adopted into an ICN architecture, the additional latency of the resolution obviously occurs. Although the latency of the resolution is added, the total latency could be minimized if the nearest copies or off-path caches can be found by NRS lookup. Also, there might be a trade-off between the resolution latency and inter-domain traffic reduction.

- **Security**: When NRS is adopted into an ICN architecture, security treats could be increased with the above additional procedures, which include authentication of NRS messages and name spaces, and protecting NRS entities such as mapping servers from Denial of Service or Distributed Denial of service attacks.

5. ICN Architectural Considerations for NRS

This section discusses what kinds of things have to be considered from the point of view of ICN architecture when it utilizes a NRS.

5.1. Resolution

When a NRS is applying to an ICN architecture, the followings have to be considered:

- **Who does the resolution?**

- **How does the resolution?**

The resolution can be done by consumer, routers, or both. Once it is decided where the resolution takes place, it has to be considered how
the resolution does. The name provided by consumer might be always
resolved to identifiers in a different namespace just like DNS
lookup. Conversely, a NRS is ever needed to map names to a different
namespace.

5.2. Protocols and Semantics

In order to develop NRS system whether in local ICN network domain or
global ICN networking system, new protocol and semantics should be
designed to manage and resolve in between different name spaces.
Basically NRS can be implemented by extension of basic ICN TLV format
and semantics enson of basic ICN TLV format and semantics
[CCNxMessages] [CCNxSemantics]. For instance, resolution and
response messages can be implemented by defining new type fields in
Interest and Content Object message format [CCNxNRS]. Then it allows
ICN architecture to minimize implication of ICN architectural
changes. But NRS system cannot support more flexible and scalable
designs cause to restrict basic ICN protocol and semantics.

On the other hand, NRS system can be implemented by using its own
protocol and semantics like as existing NRS systems, such as [Hong].
For instance, NRS protocol and messages can be implemented by using
RESTful API. Then NRS as application protocol can be operated
independently from basic ICN architecture. But ICN architecture
cannot get assist of routing protocol itself effectively.

5.3. Routing System

It has to be considered how to process the resolved information by
NRS lookup. The results of an NRS operation can be intended to be
used just to construct tunnels resulting in NRS identifying tunnel
endpoints.

Another way to process the resolved information by NRS lookup is to
use it as routing hints in request messages. In this case, request
message needs to be re-written by the resolved information including
the original name that was requested by consumer to check the data
integrity.

6. Security Considerations

When NRS is adopted in an ICN architecture, security threats shall be
increased in various aspects such as followings.
6.1. Name Space Separation

In order to deploy NRS on ICN architecture, ICN name spaces are separated into more than two name spaces. Thus these name spaces should be mapped and managed securely. According to the ICN research challenge [RFC7927], new name space can also provide an integrity verification function to authenticate its publishers. In addition to the verification, binding two different name spaces should be securely required.

6.2. NRS System

NRS enables deployment of new entities to build distributed and scalable NRS system. Thus, the entities, e.g., mapping server that can be a mapping database, could be a single point of failure cause to receive malicious requests from innumerable adversaries like as mount Denial of Service or Distributed Denial of service attacks. Additionally, in order to communicate with the entities to build NRS system, an initiator should rely on other NRS entities that are designed to distributed deploy mapping servers in each network domains. Because malicious entities should be involved in this communication to impersonate control functions. Thus, NRS entities should trust each other and communications with them should be protected securely.

6.3. NRS Protocols and Messages

Regarding NRS messages, such as lookup, update, and etc., if these messages are transported unauthenticated, an adversary can manipulate them and hijack the important communication to response or to store fake data. Thus, the adversary can generate malicious traffics to be redirected to victim hosts. Therefore, security requirements for NRS should be considered to protect ICN architecture as well as NRS.

7. Acknowledgements

[TBD]

8. References

8.1. Normative References

8.2. Informative References

[Afanasyev]


[Ravindran]

[MF] "NSF Mobility First project.", http://mobilityfirst.winlab.rutgers.edu/.


[CCNxSemantics]

[CCNxMessages]
Internet-Draft    Arch Considerations of ICN using NRS         July 2018


[Hong] Hong, J., Chun, W., and H. Jung, "Demonstrating a Scalable Name Resolution System for Information-Centric Networking", ACM ICN, September 2015.

Authors' Addresses

Jungha Hong
ETRI
218 Gajeong-ro, Yuseung-Gu
Daejeon 34129
Korea
Phone: +82 42 860 0926
Email: jhong@etri.re.kr

Tae-Wan You
ETRI
218 Gajeong-ro, Yuseung-Gu
Daejeon 34129
Korea
Phone: +82 42 860 0642
Email: twyou@etri.re.kr

Yong-Geun Hong
ETRI
218 Gajeong-ro, Yuseung-Gu
Daejeon 34129
Korea
Phone: +82 42 860 6557
Email: yghong@etri.re.kr