ICN Research Group
Internet-Draft
Intended status: Informational
Expires: January 9, 2020

J. Hong
T. You
Y-G. Hong
ETRI
L. Dong
C. Westphal
Huawei
B. Ohlman
Ericsson

July 08, 2019

Design Guidelines for Name Resolution Service in ICN
draft-irtf-icnrg-nrs-requirements-02

Abstract

This document discusses the motivation and design guidelines for Name Resolution Service (NRS) in ICN. The NRS in ICN is to translate an object name into some other information such as a locator and another name which is used for forwarding the object request.

Table of Contents

1. Introduction

The current Internet is a host-centric networking, where hosts are uniquely identified with IP addresses and communication is possible between any pair of hosts. Thus, information in the current Internet is identified by the name of host where the information is stored. In contrast to the host-centric networking, the primary communication objects in Information-centric networking (ICN) are the named data objects (NDOs) and they are uniquely identified by the location-independent names. Thus, ICN aiming to the efficient dissemination and retrieval of the NDOs in a global scale has been identified and acknowledged as a promising technology for the future Internet architecture to overcome the limitations of the current Internet such as scalability and mobility.[Ahlgren] [Xylomenos]. ICN also has been emerged as a candidate architecture for IoT environment since IoT focuses on data and information rather than end-to-end communications [Baccelli] [Amadeo] [Quevedo] [Amadeo2] [ID.Zhang2].

Since naming data independently from the current location where it is stored is a primary concept of ICN, how to find the NDO using the location-independent name is one of the most important design challenges in ICN. Such ICN routing may comprise three steps [RFC7927] :

- o Name resolution : matches/translates a content name to locators of content producers or sources that can provide the content.
- o Content discovery : routes the content request towards the content’s location either based on its name or locator.
- o Content delivery : transfers the content to the requester.

Among these three steps of ICN routing, this document focuses only on the name resolution step which translates a content name to the content locators. In addition, this document covers various possible types of name resolution in ICN such as one name to another name, name to manifest, name to locator, name to metadata, etc.

Thus, this document presents the overview of the Name Resolution Service (NRS) approaches in ICN and discusses the functionalities and the guidelines in designing the NRS for ICN.

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. Name Resolution Service in ICN

The Name Resolution Service (NRS) in ICN is defined as the service that provides the name resolution function for translating an object name into some other information such as a locator, another name, metadataetc. that is used for forwarding the object request. In other words, the NRS is the service that shall be provided by ICN infrastructure to help a consumer to reach a specific piece of content, service, or host. The consumer provides the NRS with a persistent name and the NRS returns a name or locator that represents a current instance of the requested object.

The name resolution is a necessary process in ICN routing although the name resolution either can be separated from the content discovery as an explicit process or can be integrated with the content discovery as an implicit process. The former is referred as explicit name resolution approach, the latter is referred as name-based routing approach in this document.

3.1. Explicit name resolution approach

The NRS could take the explicit name resolution approach to return the client with the locators of the content, which will be used by the underlying network as the identifier to route the client’s request to one of the producers. There are several ICN projects that use the explicit name resolution approach such as DONA[Koponen], PURSUIT [PURSUIT], NetInf [SAIL], MobilityFirst [MF], IDNet [Jung], etc.

3.2. Name-based routing approach

The NRS could take the name-based routing approach, which integrates the name resolution with the content request message routing as in NDN [NDN]/CCN [CCN].

In the case that the content request also specifies the reverse path, as in NDN/CCN, the name resolution mechanism also determines the routing path for the data. This adds a requirement on the name resolution service to propagate request in a way that is consistent with the subsequent data forwarding. Namely, the request must select a path for the data based upon the finding the copy of the content, but also properly delivering the data.

3.3. Hybrid approach

The NRS could also take hybrid approach which can perform the name-based routing approach from the beginning. When it fails at certain router, the router can go back to the explicit name resolution approach. The alternative hybrid NRS approach also works, which can perform explicit name resolution approach from the beginning to find locators of routers. And then it can carry out the name-based routing approach of the client's request.

A hybrid approach would combine name resolution as a subset of routers on the path with some tunneling in between (say, across an administrative domain) so that only a few of the nodes in the architecture perform name resolution in the name-based routing approach.

3.4. Comparisons of name resolution approaches

The following compares the explicit name resolution and the name-based routing approaches from different aspects:

- Update message overhead : The update message overhead is due to the change of content reachability, which may include content caching or expiration, content producer mobility etc. The name-based routing approach may require flooding parts of the network for update propagation. In the worst case, the name-based routing approach may flood the whole network (but mitigating techniques may be used to scope the flooding). However, the explicit name resolution approach only requires updating propagation in part of the name resolution overlay.

- Resolution capability : The explicit name resolution approach can guarantee the resolution of any content name in the network if it is registered to the name resolution overlay. In the name-based routing approach, content resolution depends on the flooding scope of the content names (i.e. content publishing message and the resulting name based routing tables). For example, when a content is cached, the router may only notify this information to its direct neighbors. Thus only those neighboring routers can build a named based entry for this cached content. But if the neighboring routers continue to propagate this information, the other nodes are able to direct to this cached copy as well.

- Node failure impact : Nodes involved in the explicit name resolution approach are the name resolution overlay servers (e.g. Resolution Handlers in DONA), while the nodes involved in the name-based routing approach are routers which route messages based on locally maintained name-based routing tables (e.g. NDN routers). Node failures in the explicit name resolution approach may cause some content discovery to fail even though the content is available. This problem does not exist in the name-based routing approach because other alternative paths can be discovered to bypass the failed ICN routers, given the assumption that the network is still connected.

o Maintained databases : The storage usage for the explicit name resolution approach is different from that of the name-based routing approach. The explicit name resolution approach typically needs to maintain two databases: name to locator mapping in the name resolution overlay and routing tables in the routers on the data forwarding plane. The name-based routing approach needs to maintain different databases: name routing table and optionally breadcrumbs for reverse routing of content back to the requester.

Additionally, some other intermediary step may be included in the name resolution, namely the mapping of one name to other names, in order to facilitate the retrieval of named content, by way of a manifest [Westphal] [Mosko]. The manifest is resolved using one of the two above approaches, and it may include further mapping of names to content and location. The steps for name resolution then become: first translate the manifest name into a location of a copy of the manifest; the manifest includes further names of the content components, and potentially locations for the content. The content is then retrieved by using these names and/or location, potentially resulting in additional name resolutions.

Thus, no matter which approach is taken by the NRS in ICN, the name resolution is the essential function that shall be provided by the ICN infrastructure.

4. Functionalities of NRS in ICN

This section presents the functionalities of NRS in ICN.

4.1. Support heterogeneous name types

In ICN, a name is used to identify data object and is bound to it [RFC7927]. ICN requires uniqueness and persistency of the name of data object to ensure the reachability of the object within a certain scope and with proper authentication and trust management. There are heterogeneous approaches to designing ICN naming schemes [Bari]. Ideally, a name can include any form of identifier, which can be flat, hierarchical, and human readable or non-readable.

Although there are diverse types of naming schemes proposed in literature, they all need to provide basic functions for identifying data object, supporting trust provenance, named data lookup and routing. The NRS may combine the good aspects of different schemes. Basically, the NRS should be able to support a generic naming schema so that it can resolve any type of content name, irrespective of whether it is flat or hierarchical.

In PURSUIT [PURSUIT], names are flat and the rendezvous functions are defined for NRS, which is implemented by a set of Rendezvous Nodes (RNs), the Rendezvous Network (RENE). Thus a name consisted of a sequence of scope IDs and a single rendezvous ID is routed by RNs in RENE. Thus, PURSUIT decouples name resolution and data routing, where NRS is performed by the RENE.

In MobilityFirst [MF], a name called a global unique Identifier (GUID) derived from a human-readable name via a global naming service is flat typed 160-bits strings with self-certifying function. Thus, MobilityFirst defines a global name resolution service (GNRS) which resolves GUIDs to network addresses and decouples name resolution and data routing as similar to PURSUIT.

In NetInf [Dannewitz], information objects are named using ni-naming [RFC6920], which consist of an authority part and digest part (content hash). The ni names can be flat as the authority part is optional. Thus, the NetInf architecture also includes a Name Resolution System (NRS) which can be used to resolve ni-names to addresses in an underlying routable network layer.

In NDN [NDN] and CCN [CCN], names are hierarchical and may be similar to URLs. Each name component can be anything, including a dotted human-readable string or a hash value. NDN/CCN adopts the name based routing approach. The NDN router forwards the request by doing the longest-match lookup in the Forwarding Information Base (FIB) based on the content name and the request is stored in the Pending Interest Table (PIT).

4.2. Support producer mobility

ICN natively supports mobility management. Especially, consumer or client mobility is handled by requesting the content again in case the mobility or handover occurred before receiving the corresponding content from the network. Since ICN can ensure that content reception continues without any disruption in ICN application, seamless mobility in consumer point of view can be easily supported.

However, producer or publisher mobility in ICN is complicated to support. If a producer moves into a different authority domain or network location, it would be difficult for the mobility management update RIB and FIB entries in ICN routers with the new forwarding path in a very short time. Therefore, various ICN architectures in literatures have proposed to adopt NRS to achieve the producer or publisher mobility, where NRS can be implemented in different ways such as at rendezvous points and overlay mapping systems.

In NDN [Zhang2], for producer mobility support, rendezvous mechanisms have been proposed to build interests rendezvous (RV) with data generated by a mobile producer (MP). There can be classified two approaches such as chase mobile producer and rendezvous data. Regarding MP chasing, rendezvous acts as a mapping service that provides the mapping from the name of the data produced by the MP to the MP's current point of attachment (PoA) name. Alternatively, the RV serves as a home agent like as IP mobility support, so the RV enables consumer's interest message to tunnel towards the MP at the PoA. Regarding rendezvous data, moving the data produced by the MP have been hosting at data depot instead of forwarding interest messages. Thus a consumer's interest message can be forwarded to stationary place as called data rendezvous, so it would either return the data or fetch it using another mapping solution. Therefore, RV or other mapping functions are in the role of NRS in NDN.

In [Ravindran], forwarding-label (FL) object is referred to enable identifier (ID) and locator (LID) namespaces to be split in ICN. Generally, IDs are managed by applications, while locators are managed by a network administrator, so that IDs are mapping to heterogeneous name schemes and LIDs are mapping to network domains or specific network elements. Thus the proposed FL object acts as a locator (LID) and provides the flexibility to forward Interest messages through mapping service between IDs and LIDs. Therefore, the mapping service in control plane infrastructure can be considered as NRS in this draft.

In MobilityFirst [MF], both consumer and publisher mobility can be primarily handled by the global name resolution service (GNRS) which resolves GUIDs to network addresses. Thus, the GNRS must be updated for mobility support when a network attached object changes its point of attachment, which differs from NDN/CCN.

In NetInf [Dannewitz], mobility is handled by the NRS in a very similar way as done in MobilityFirst.

Besides the consumer and producer mobility, ICN also has to face challenges to support the other dynamic features such as multi-homing, migration, and replication of named resources such as content, devices, and services. Therefore, NRS can help to support these dynamic features.

4.3. Support scalable routing system

In ICN, name of data objects is used for routing by either name resolution step or routing table lookup. Thus, routing information for each data object should be maintained in routing base, such as Routing Information Base (RIB) and Forwarding Information Base (FIB). Since the number of data objects would be very large, the size of information bases would be significantly large as well [RFC7927].

The hierarchical namespace used in CCN [CCN] and NDN [NDN] architectures reduces the size of these tables through name aggregation and improves scalability of routing system. In a flat naming scheme, on the other hand, it would aggravate the scalability problem in routing system. The non-aggregated name prefixes injected to the Default Route Free Zone (DFZ) of ICN would create more serious scalability problem similar to the scalability issue of IP routing system. Thus, NRS may play an important role in the reduction of the routing scalability problem regardless of the types of namespaces.

In [Afanasyev], in order to address the routing scalability problem in NDN’s DFZ, a well-known concept of Map-and-Encap is applied to provide a simple and secure namespace mapping solution. In the proposed map-and-encap design, data whose name prefixes do not exist in the DFZ forwarding table can be retrieved by a distributed mapping system called NDNS, which maintains and lookups the mapping information from a name to its globally routed prefixes, where NDNS is a kind of NRS.

4.4. Support off-path caching

Caching in-network is considered to be a basic architectural component of an ICN architecture. It may be used to provide a Quality-of-Service (QoS) experience to users, reduce the overall network traffic, prevent network congestion and Denial-of-Service (DoS) attacks and increase availability. 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.

In [Bayhan], a NRS used to find off-path copies in the network, which may not be accessible via content discovery mechanisms. Such capability is essential for an Autonomous System (AS) to avoid the costly inter-AS traffic for external content, to yield higher bandwidth efficiency for intra-AS traffic, and to decrease the data access latency for a pleasant user experience.

4.5. Support nameless object

In CCNx 1.0 [Mosko2], the concept of "Nameless Objects" that are a Content Object without a Name is introduced to provide a means to move Content between storage replicas without having to rename or re-sign the content objects for the new name. Nameless Objects can be addressed by the ContentObjectHash that is to restrict Content Object matching by using SHA-256 hash.

An Interest message would still carry a Name and a ContentObjectHash, where a Name is used for routing, while a ContentObjectHash is used for matching. However, on the reverse path, if the Content Object's name is missing, it is a "Nameless Object" and only matches against the ContentObjectHash. Therefore, a consumer needs to resolve proper name and hashes through an outside system, which can be considered as NRS.

4.6. Support manifest

In collection of data objects which were organized as large and file like contents [FLIC], the manifests are used as data structures to transport this information. Thus, the manifests may contain hash digests of signed content objects or other manifests, so that large content objects which represent large piece of application data can be collected by using the manifest.

In order to request content objects, a consumer needs to know a manifest root name to acquire the manifest. In case of FLIC, a manifest name can be represented by a nameless root manifest, so that outside system may be involved to give this information to the consumer. Therefore, NRS can be considered as a kind of mapping database system.

4.7. Support metadata

When resolving the name of a content object the NRS in addition to returning a locator could return a rich set of metadata. The metadata could include alternative object locations, supported object transfer protocol(s), caching policy, security parameters, data format, hash of object data, etc. The consumer could use this metadata for selection of object transfer protocol, security mechanism, egress interface, etc. An example of how metadata can be used in this way is provided by the NEO ICN architecture [NEO].

5. Design guidelines for NRS in ICN

This section presents the guidelines for designing NRS in ICN.

5.1. Resolution response time

The name resolution process should provide a response within a reasonable amount of time. The response should be either a proper mapping of the name to a copy of the content, or an error message stating that no such file exists. If the name resolution does not map to a location, the system may not issue any response, and the client should set a timer when sending a request, so as to consider the resolution incomplete when the timer expires.

The acceptable response delay should be of the order of a round trip time between the client issuing the request and the NRS servers that provides the response. While this RTT may be very greatly depending on the proximity between the two end points, some upper bound should be used.

The response time should be within the same order of magnitude for most pairs of a client issuing a request, and the NRS server responding to this request.

The response time should include all the steps of the resolution, including potentially a hop-by-hop resolution or a hierarchical forwarding of the resolution request.

5.2. Response accuracy

The NRS must provide an accurate response, namely a proper binding of the requested name (or prefix) with a location. The response can be either a (prefix, location) pair, or the actual forwarding of a request to a node holding the content, which is then transmitted in return.

The NRS must provide an up-to-date response, namely the NRS should be updated within a reasonable time when new copies of the content are being stored in the network. While every transient cache addition/eviction should not trigger an NRS update, some origin servers may move and require the NRS to be updated.

The NRS must provide mechanisms to update the mapping of the content with its location. Namely, the NRS must provide a mechanism for a content owner to add new content, revoke old/dated/obsolete content, and modify existing content. Any content update should then be propagated through the NRS system within reasonable delay.

Content that is highly mobile may require to specify some type of anchor that is kept at the NRS, instead of the content location.

5.3. Resolution guarantee

The NRS must ensure that the name resolution would be successful if the name matching content exists in the network, regardless of its popularity and number of cached copies existing in the network.

5.4. Resolution fairness

The NRS should provide this service for all content in a fair manner, independently of the specific content properties (content producer, content popularity, availability of copies, content format, etc.)

5.5. Scalability

The NRS system must scale up to support a very large user population (including human users as well as machine-to-machine communications). The system must be able to respond to a very large number of requests per unit of time. Message forwarding and processing, routing table building-up and name records propagation must be efficient and scalable.

The NRS system must scale up with the number of pieces of content (content names) and should be able to support a content catalog that is extremely large.

The NRS system must be able to scale up, namely to add NRS servers to the NRS system, in a way that is transparent to the users. Addition of a new server should have limited impact on the other NRS servers (or should have impact on only a small subset of the NRS servers).

The NRS system should support access from a heterogeneity of connection methods and devices. In particular, the NRS system should support access from constrained devices and interactions with the NRS system should not be too costly. An IoT node for instance should be able to access the NRS system as well as a more powerful node.

The NRS system should scale up in its responsiveness to the increased request rate that is expected from applications such as IoT or M2M, where data is being frequently generated and/or frequently requested.

5.6. Manageability

The NRS system must be manageable since some parts of the system may grow or shrink dynamically and an NRS system node may be added or deleted frequently.

The NRS may support an NRS management layer that allows for adding or subtracting NRS nodes. The management layer should be able to infer if the use of the NRS in some parts of the network is growing (or shrinking).

5.7. Deployed system

The NRS system must be deployable since deployability is important for a real world system. The NRS system must be deployable in network edges and cores so that the consumers as well as ICN routers can perform name resolution in a very low latency.

5.8. Fault tolerance

The NRS system must ensure resiliency in the event of NRS server failures. The failure of a small subset of nodes should not impact the NRS performance significantly.

After a NRS server fails, the NRS system must be able to recover and/ or restore the name records stored in the NRS server.

6. IANA Considerations

There are no IANA considerations related to this document.

7. Security Considerations

Accessibility, authentication, confidentiality and privacy protection are the concerns on security aspect of both the NRS server nodes and mapping records stored in the NRS system.

7.1. Accessibility

The name records must have assigned with proper access rights such that the information contained in the name mapping record would not be revealed to unauthorized users. In other words, the NRS system must be prevented from malicious users attempting to hijack or corrupt the name mapping records.

The NRS may support access control for certain name records, so that only users with the proper credential can access these record, and these records would not be shared to unauthorized users.

The NRS may support authentication of the content producers to determine that any location update/addition/removal that a content producer is requesting is indeed valid and that the content producer is authorized to modify this record.

The NRS should verify new mapping location that are being registered so that it cannot be polluted with falsified information or invalid records.

7.2. Authentication

The NRS must require authentication of new NRS nodes that register themselves in the NRS system to ensure they are who they claim to be. For example, it should detect an attacker attempting to act as a fake NRS server to disrupt the NRS service, or to intercept some users' data.

7.3. Data confidentiality

NRS must keep the data confidentiality to prevent a lot of sensitive data from reaching unauthorized data requestor such as in IoT environment.

NRS must keep meta-data confidential as well as usage to protect the privacy of the users. For instance, a specific user's NRS requests should not be shared outside the NRS system (with the exception of legal intercept).

7.4. Privacy protection

When a private name mapping record is registered in the system, the NRS system must support the privacy to avoid the information leaking. Otherwise, unauthorized entity may disclose the privacy.

7.5. Robustness/resiliency

The NRS system should be resilient to denial of service attacks and/ or other common attacks on the integrity of its system. The NRS system should be resilient if a few attacked nodes are unable to participate in the system.

7.6. Network privacy

The NRS node in a given subdomain should not leak information about this domain (say, topology, number of nodes, number of clients, number of requests) to nodes outside of this domain, except for sharing the content that it is allowed to advertise, or for the management protocols that it is supporting.

8. Acknowledgements

The authors would like to thank Ved Kafle for his valuable comments and suggestions on this document.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7927] Kutscher, D., Ed., Eum, S., Pentikousis, K., Psaras, I., Corujo, D., Saucez, D., Schmidt, T., and M. Waehlisch, "Information-Centric Networking (ICN) Research Challenges", RFC 7927, DOI 10.17487/RFC7927, July 2016, <https://www.rfc-editor.org/info/rfc7927>.

9.2. Informative References

[Ahlgren] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and B. Ohlman, "A Survey of Information-Centric Networking", IEEE Communications Magarzine Vol.50, Issue 7, 2012.

[Xylomenos] Xylomenos, G., Ververidis, C., Siris, V., Fotiou, N., Tsilopoulos, C., Vasilako, X., Katsaros, K., and G. Polyzos, "A Survey of Information-Centric Networking Research,Communications Surveys and Tutorials", IEEE Communications Surveys and Tutorials vol. 16, no. 2, 2014.

[Baccelli] Baccelli, E., Mehlis, C., Hahm, O., Schmidt, T., and M. Wahlisch, "Information Centric Networking in the IoT: Experiments with NDN in the Wild", ACM ICN 2014, 2014.

[Amadeo] Amadeo, M., Campolo, C., Iera, A., and A. Molinaro, "Named data networking for IoT: An architectural perspective", European Conference on Networks and Communications (EuCNC) , 2014.

[Quevedo] Quevedo, J., Corujo, D., and R. Aguiar, "A case for ICN usage in IoT environments", IEEE GLOBECOM , 2014.

[Amadeo2] Amadeo, M. et al., "Information-centric networking for the internet of things: challenges and opportunitiesve", IEEE Network vol. 30, no. 2, July 2016.

[ID.Zhang2] Zhang, Y., "Design Considerations for Applying ICN to IoT", draft-zhang-icnrg-icniot-01 , June 2017.

[Koponen] Koponen, T., Chawla, M., Chun, B., Ermolinskiy, A., Kim, K., Shenker, S., and I. Stoica, "A Data-Oriented (and Beyond) Network Architecture", ACM SIGCOMM 2007 pp. 181-192, 2007.

[PURSUIT] "FP7 PURSUIT project.", http://www.fp7-pursuit.eu/PursuitWeb/ .

[SAIL] "FP7 SAIL project.", http://www.sail-project.eu/ .

[NDN] "NSF Named Data Networking project.", http://www.named-data.net .

[CCN] "Content Centric Networking project.", https://wiki.fd.io/view/Cicn .

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

[Jung] Jung, H. et al., "IDNet: Beyond All-IP Network", ETRI Jouranl vol. 37, no. 5, October 2015.

[Jacobson] Jacobson, V., Smetters, D., Thornton, J., Plass, M., Briggs, N., and R. Braynard, "Networking Named Content", ACM CoNEXT , 2009.

[Baid] Baid, A., Vu, T., and D. Raychaudhuri, "Comparing Alternative Approaches for Networking of Named Objects in the Future Internet", IEEE Workshop on Emerging Design Choices in Name-Oriented Networking (NOMEN) , 2012.

[Bari] Bari, M., Chowdhury, S., Ahmed, R., Boutaba, R., and B. Mathieu, "A Survey of Naming and Routing in Information-Centric Networks", IEEE Communications Magazine Vol. 50, No. 12, P.44-53, 2012.

[Rajahalme]
Rajahalme, J., Sarela, M., Visala, K., and J. Riihijarvi, "On Name-based Inter-domain Routing", Computer Networks Vol. 55, No. 4, P. 975-986, March 2011.

[Katsaros]
Katsaros, K., Fotiou, N., Vasilakos, X., Ververidis, C., Tsilopoulos, C., Xylomenos, G., and G. Polyzos, "On Inter-Domain Name Resolution for Information-Centric Networks", Proc.IFIP-TC6 Networking Conference , 2012.

[ID.Wang] Wang, J., Li, S., and C. Wetphal, "Namespace Resolution in Future Internet Architectures", draft-wang-fia-namespace-01 , October 2015.

[ID.Zhang]
Zhang, X., Ravindran, R., Xie, H., and G. Wang, "PID: A Generic Naming Schema for Information-centric Network", draft-zhang-icnrg-pid-naming-scheme-03 , August 2013.

[D.Zhang] Zhang, D. and H. Liu, "Routing and Name Resolution in Information-Centric Networks", 22nd International Conference on Computer Communications and Networks (ICCCN) , 2013.

[Sevilla] Sevilla, S., Mahadevan, P., and J. Garcia-Luna-Aceves, "iDNS: Enabling Information Centric Networking Through The DNS", Name Oriented Mobility (workshop co-located with Infocom 2014) , 2014.

[RFC1498] Saltzer, J., "On the Naming and Binding of Network Destinations", RFC 1498, DOI 10.17487/RFC1498, August 1993, <https://www.rfc-editor.org/info/rfc1498>.

[oneM2M] "oneM2M Functional Architecture TS 0001.", http://www.onem2m.org/technical/published-documents. .

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[ID.Shelby]
Shelby, Z., "CoRE Resource Directory", draft-ietf-core-resource-directory-10 , March 2017.

[CoRE] "Constrained RESTful Environments, CoRE", https://datatracker.ietf.org/wg/core/charter/ , March 2013.

[Westphal] Westphal, C. and E. Demirors, "An IP-based Manifest Architecture for ICN", ACM ICN , 2015.

[Mosko] Mosko, M., Scott, G., Solis, I., and C. Wood, "CCNx Manifest Specification", draft-wood-icnrg-ccnxmanifests-00 , July 2015.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <https://www.rfc-editor.org/info/rfc6830>.

[RFC6833] Fuller, V. and D. Farinacci, "Locator/ID Separation Protocol (LISP) Map-Server Interface", RFC 6833, DOI 10.17487/RFC6833, January 2013, <https://www.rfc-editor.org/info/rfc6833>.

[RFC6920] Farrell , S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC6920, DOI 10.17487/RFC6920, https://rfc-editor.org/rfc/rfc6920.txt , Apr. 2013.

[Zhang] Zhang, L. et al., "Named data networking", ACM SIGCOMM Computer Communication Review vol. 44, no. 3, July 2014.

[Zhang2] Zhang, Y., "A Survey of Mobility Support in Named Data Networking", NAMED-ORIENTED MOBILITY: ARCHITECTURES, ALGORITHMS, AND APPLICATIONS(NOM) , 2016.

[Dannewitz] Dannewitz, C. et al., "Network of Information (NetInf)-An information centric networking architecture", Computer Communications vol. 36, no. 7, April 2013.

[Seskar] Seskar, I., Nagaraja, K., Nelson, S., and D. Raychaudhuri, "MobilityFirst Future Internet Architecture Project", 7th Asian Internet Engineering Conference , November 2011.

[Dannewitz2] Dannewitz, C., DAmbrosio, M., and V. Vercellone, "Hierarchical DHT-based name resolution for Information-Centric Networks", Computer Communications vol. 36, no. 7, April 2013.

[Vu] Vu, T. et al., "DMap: A Shared Hosting Scheme for Dynamic Identifier to Locator Mapping in the Global Internet", IEEE 32nd International Conference on Distributed Computing Systems , 2012.

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

[Ravindran] Ravindran, R. et al., "Forwarding-Label support in CCN Protocol", draft-ravi-icnrg-ccn-forwarding-label-01 , July 2017.

[Afanasyev] Afanasyev, A. et al., "SNAMP: Secure Namespace Mapping to Scale NDN Forwarding", IEEE Global Internet Symposium , April 2015.

[Mosko2] Mosko, M., "Nameless Objects", , July 2015.

[Bayhan] Bayhan, S. et al., "On Content Indexing for Off-Path Caching in Information-Centric Networks", ACM ICN , September 2016.

[FLIC] Tschudin, C. and C. Wood, "File-Like ICN Collection (FLIC)", draft-irtf-icnrg-flic-01, , June 2018.

[NEO] Eriksson, A. and A. M. Malik, "A DNS-based information-centric network architecture open to multiple protocols for transfer of data objects", 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), pp. 1-8, 2018.

Authors' Addresses

Jungha Hong
ETRI
218 Gajeong-ro, Yuseung-Gu
Daejeon 34129
Korea

Email: jhong@etri.re.kr

Tae-Wan You
ETRI
218 Gajeong-ro, Yuseung-Gu
Daejeon 34129
Korea

Email: twyou@etri.re.kr

Yong-Geun Hong
ETRI
218 Gajeong-ro, Yuseung-Gu
Daejeon 34129
Korea

Email: yghong@etri.re.kr

Lijun Dong
Huawei
10180 Telesis Court
San Diego, CA 92121
USA

Email: lijun.dong@huawei.com

Cedric Westphal
Huawei
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: cedric.westphal@huawei.com

Borje Ohlman
Ericsson Research
S-16480 Stockholm
Sweden

Email: Borje.Ohlman@ericsson.com