ï»¿

Internet Research Task Force (IRTF)
Request for Comments: 9138
Category: Informational
ISSN: 2070-1721

J. Hong
T. You
ETRI
L. Dong
C. Westphal
Futurewei Technologies Inc.
B. Ohlman
Ericsson

November 2021

Design Considerations for Name Resolution Service in Information-Centric Networking (ICN)

Abstract

This document provides the functionalities and design considerations for a Name Resolution Service (NRS) in Information-Centric Networking (ICN). The purpose of an NRS in ICN is to translate an object name into some other information such as a locator, another name, etc. in order to forward the object request. This document is a product of the Information-Centric Networking Research Group (ICNRG).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The current Internet is based upon a host-centric networking paradigm, where hosts are 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 the host (or server) where the information is stored. In contrast to host-centric networking, the primary communication objects in Information-Centric Networking (ICN) are the named data objects (NDOs), and they are uniquely identified by location-independent names. Thus, ICN aims for the efficient dissemination and retrieval of NDOs at a global scale and has been identified and acknowledged as a promising technology for a future Internet architecture to overcome the limitations of the current Internet, such as scalability and mobility [Ahlgren] [Xylomenos]. ICN also has emerged as a candidate architecture in the Internet of Things (IoT) environment since IoT focuses on data and information [Baccelli] [Amadeo] [Quevedo] [Amadeo2] [ID.Zhang2].

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

(1) Name resolution: matches/translates a content name to the locator of the content producer or source that can provide the content.

(2) Content request routing: routes the content request towards the content's location based either on its name or locator.

(3) Content delivery: transfers the content to the requester.

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

The focus of this document is a Name Resolution Service (NRS) itself as a service or a system in ICN, and it provides the functionalities and the design considerations for an NRS in ICN as well as the overview of the NRS approaches in ICN. On the other hand, its companion document [NRSarch] describes considerations from the perspective of the ICN architecture and routing system when using an

NRS in ICN.

This document represents the consensus of the Information-Centric Networking Research Group (ICNRG). It has been reviewed extensively by the Research Group (RG) members who are actively involved in the research and development of the technology covered by this document. It is not an IETF product and is not a standard.

2. Name Resolution Service in ICN

A 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, metadata, next-hop info, etc. that is used for forwarding the object request. In other words, an NRS is a service that can be provided by the ICN infrastructure to help a consumer reach a specific piece of information (or named data object). The consumer provides an NRS with a persistent name, and the NRS returns a name or locator (or potentially multiple names and locators) that can reach 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 request routing as an explicit process or can be integrated with the content request routing as an implicit process. The former is referred to as an "explicit name resolution approach", and the latter is referred to as a "name-based routing approach" in this document.

2.1. Explicit Name Resolution Approach

An NRS could take the explicit name resolution approach to return the locators of the content to the client, which will be used by the underlying network as the identifier to route the client’s request to one of the producers or to a copy of the content. There are several ICN projects that use the explicit name resolution approach, such as Data-Oriented Network Architecture (DONA) [Koponen], PURSUIT [PURSUIT], Network of Information (NetInf) [SAIL], MobilityFirst [MF], IDNet [Jung], etc. In addition, the explicit name resolution approach has been allowed for 5G control planes [SA2-5GLAN].

2.2. Name-Based Routing Approach

An NRS could take the name-based routing approach, which integrates name resolution with content request message routing as in Named Data Networking / Content-Centric Networking (NDN/CCNx) [NDN] [CCNx].

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

2.3. Hybrid Approach

An NRS could also take hybrid approach. For instance, it can attempt the name-based routing approach first. If this fails at a certain router, the router can go back to the explicit name resolution approach. The hybrid NRS approach also works the other way around: first by performing explicit name resolution to find the locators of routers, then by routing the client’s request using the name-based routing approach.

A hybrid approach would combine name resolution over 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 ICN network perform name resolution in the name-based routing approach.

2.4. Comparisons of Name Resolution Approaches

The following compares the explicit name resolution and the name-based routing approaches in several aspects:

* Overhead due to the maintenance of the content location: The content reachability is dynamic and includes new content being cached or content being expired from a cache, content producer mobility, etc. Maintaining a consistent view of the content location across the network requires some overhead that differs for the name resolution approaches. 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 system (which could be an overlay with a limited number of nodes).

* Resolution capability: The explicit name resolution approach, if designed and deployed with sufficient robustness, can offer at least weak guarantees that resolution will succeed for 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 content is cached, the router may only notify its direct neighbors of this information. Thus, only those neighboring routers can build a name-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 that route messages based on the name-based routing tables (e.g., NDN routers). Node failures in the explicit name resolution approach may cause some content request routing 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.

* 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 only the name-based routing tables.

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] [RFC8569]. 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 the following: first, translate the manifest name into a location of a copy of the manifest, which includes further names of the content components and potentially locations for the content, then retrieve the content by using these names and/or location, potentially resulting in additional name resolutions.

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

3. Functionalities of NRS in ICN

This section presents the functionalities of an NRS in ICN.

3.1. Support Heterogeneous Name Types

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

Although there are diverse types of naming schemes proposed in the literature, they all need to provide basic functions for identifying a data object, supporting named data lookup, and routing. An NRS may combine the better aspects of different schemes. Basically, an 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, hierarchical, attribute based, or anything else.

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

In MobilityFirst [MF], a name known as a "Global Unique Identifier (GUID)", derived from a human-readable name via a global naming service, is a flat typed 160-bit string with self-certifying properties. Thus, MobilityFirst defines a Global Name Resolution Service (GNRS), which resolves GUIDs to network addresses and decouples name resolution and data routing similarly to PURSUIT.

In NetInf [Dannewitz], information objects are named using Named Information (NI) names [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 CCNx [CCNx], names are hierarchical and may be similar to URLs. Each name component can be anything, including a human-readable string or a hash value. NDN/CCNx 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).

3.2. Support Producer Mobility

ICN inherently supports mobility by consumers. Namely, consumer or client mobility is handled by re-requesting the content in case the mobility event (say, handover) occurred before receiving the corresponding content from the network. Since ICN can ensure that content reception continues without any disruption in ICN applications, seamless mobility from the consumer's point of view can be easily supported.

However, producer mobility does not emerge naturally from the ICN forwarding model as does consumer mobility. If a producer moves into a different network location or a different name domain, which is assigned by another authoritative publisher, it would be difficult for the mobility management to update Routing Information Base (RIB) and FIB entries in ICN routers with the new forwarding path in a very short time. Therefore, various ICN architectures in the literature have proposed adopting an NRS to achieve the producer or publisher mobility, where the NRS can be implemented in different ways such as rendezvous points and/or overlay mapping systems.

In NDN [Zhang2], for producer mobility support, rendezvous mechanisms have been proposed to build interest rendezvous (RV) with data generated by a mobile producer (MP). This can be classified into two approaches: 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 name of the MP's current point of attachment (PoA). Alternatively, the RV serves as a home agent as in IP mobility support, so the RV enables the consumer's Interest message to tunnel towards the MP at the PoA. Regarding rendezvous data, the solution involves moving the data produced by the MP to a data depot instead of forwarding Interest messages. Thus, a consumer's Interest message can be forwarded to stationary place called a "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 an NRS in NDN.

In [Ravindran], the forwarding label (FL) object is used 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 mapped to heterogeneous name schemes and LIDs are mapped to the network domains or to specific network elements. Thus, the proposed FL object acts as a locator (LID) and provides the flexibility to forward Interest messages through a mapping service between IDs and LIDs. Therefore, the mapping service in control plane infrastructure can be considered as an 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/CCNx.

In NetInf [Dannewitz], mobility is handled by an NRS in a very similar way to MobilityFirst.

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

3.3. Support Scalable Routing System

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

The hierarchical namespace used in CCNx [CCNx] and NDN [NDN] architectures reduces the size of these tables through name aggregation and improves the scalability of the routing system. A flat naming scheme, on the other hand, would aggravate the scalability problem of the routing system. The non-aggregated name prefixes injected into the Default Route Free Zone (DFZ) of ICN would create a more serious scalability problem when compared to the scalability issues of the IP routing system. Thus, an 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 called "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 looks up the mapping information from a name to its globally routed prefixes, where NDNS is a kind of an NRS.

3.4. 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 level of quality-of-service (QoS) experience to users to reduce the overall network traffic, to prevent network congestion and denial-of-service (DoS) attacks, and to 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 the original server to the consumer. Off-path caching, also referred to 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 an NRS.

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

3.5. Support Nameless Object

In CCNx 1.0 [Mosko2], the concept of a "Nameless Object", which is 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, which is to restrict Content Object matching by using a 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 the proper name and hashes through an outside system, which can be considered as an NRS.

3.6. Support Manifest

For collections of data objects that are organized as large and file-like contents [FLIC], manifests are used as data structures to transport this information. Thus, manifests may contain hash digests of signed Content Objects or other manifests so that large Content Objects that represent a large piece of application data can be collected by using such a manifest.

In order to request Content Objects, a consumer needs to know a manifest root name to acquire the manifest. In the case of File-Like ICN Collections (FLIC), a manifest name can be represented by a nameless root manifest so that an outside system such as an NRS may be involved to give this information to the consumer.

3.7. Support Metadata

When resolving the name of a Content Object, NRS could return a rich set of metadata in addition to returning a locator. 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 the 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 Networked Object (NEO) ICN architecture [NEO].

4. Design Considerations for NRS in ICN

This section presents the design considerations for NRS in ICN.

4.1. 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 object 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 could be of the order of a round-trip time between the client issuing the request and the NRS servers that provide the response. While this RTT may vary greatly depending on the proximity between the two end points, some upper bound needs to be used. Especially in some delay-sensitive scenarios such as industrial Internet and telemedicine, the upper bound of the response delay must be guaranteed.

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

4.2. Response Accuracy

An 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.

An NRS must provide an up-to-date response -- namely, an 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.

An NRS must provide mechanisms to update the mapping of the content with its location. Namely, an NRS must provide a mechanism for a content provider 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 specifying some type of anchor that is kept at the NRS instead of the content location.

4.3. Resolution Guarantee

An NRS must ensure that the name resolution is successful with high probability if the name-matching content exists in the network, regardless of its popularity and the number of cached copies existing in the network. Per Section 4.1, some resolutions may not occur in a timely manner. However, the probability of such an event should be minimized. The NRS system may provide a probability (five 9s or five sigmas, for instance) that a resolution will be satisfied.

4.4. Resolution Fairness

An NRS could 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.). Fairness may be defined as a per-request delay to complete the NRS steps that is agnostic to the properties of the content itself. Fairness may be defined as well as the number of requests answered per unit of time.

However, it is notable that content (or their associated producer) may request a different level of QoS from the network (see [RFC9064], for instance), and this may include the NRS as well, in which case considerations of fairness may be restricted to content within the same class of service.

4.5. Scalability

The NRS system must scale up to support a very large user population (including human users as well as machine-to-machine communications). As an idea of the scale, it is expected that 50 billion devices will be connected in 2025 (per ITU projections). The system must be able to respond to a very large number of requests per unit of time. Message forwarding and processing, routing table buildup, and name record 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. Internet traffic is of the order of zettabytes per year (10^21 bytes). Since NRS is associated with actual traffic, the number of pieces of content should scale with the amount of traffic. Content size may vary from a few bytes to several GB, so the NRS should be expected scale up to a catalog of the size of 10^21 in the near future, and larger beyond.

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. The addition of a new server should have a limited negative impact on the other NRS servers (or should have a negative impact on only a small subset of the NRS servers). The impact of adding new servers may induce some overhead at the other servers to rebuild a hierarchy or to exchange messages to include the new server within the service. Further, data may be shared among the new servers for load balancing or tolerance to failure. These steps should not disrupt the service provided by the NRS and should improve the quality of the service in the long run.

The NRS system may support access from a heterogeneity of connection methods and devices. In particular, the NRS system may support access from constrained devices, and interactions with the NRS system would 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 machine-to-machine (M2M), where data is being frequently generated and/or requested.

4.6. 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 system may support an NRS management layer that allows for adding or subtracting NRS nodes. In order to infer the circumstance, the management layer can measure the network status.

4.7. 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.

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

4.9. Security and Privacy

On utilizing an NRS in ICN, there are some security considerations for the NRS servers/nodes and name mapping records stored in the NRS system. This subsection describes them.

4.9.1. Confidentiality

The name mapping records in the NRS system must be assigned with proper access rights such that the information contained in the name mapping records would not be revealed to unauthorized users.

The NRS system may support access control for certain name mapping records. Access control can be implemented with a reference monitor that uses client authentication, so only users with appropriate credentials can access these records, and they are not shared with unauthorized users. Access control can also be implemented by encryption-based techniques using control of keys to control the propagations of the mappings.

The NRS system may support obfuscation and/or encryption mechanisms so that the content of a resolution request may not be accessible by third parties outside of the NRS system.

The NRS system must keep confidentiality to prevent sensitive name mapping records from being reached by unauthorized data requesters. This is more required in IoT environments where a lot of sensitive data is produced.

The NRS system must also keep confidentiality of metadata as well as NRS 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).

4.9.2. Authentication

* NRS server authentication: Authentication of the new NRS servers/ nodes that want to be registered with the NRS system must be required so that only authenticated entities can store and update name mapping records. The NRS system should detect an attacker attempting to act as a fake NRS server to cause service disruption or manipulate name mapping records.

* Producer authentication: The NRS system must support authentication of the content producers to ensure that update/addition/removal of name mapping records requested by content producers are actually valid and that content producers are authorized to modify (or revoke) these records or add new records.

* Mapping record authentication: The NRS should verify new mapping records that are being registered so that it cannot be polluted with falsified information or invalid records.

4.9.3. Integrity

The NRS system must be protected from malicious users attempting to hijack or corrupt the name mapping records.

4.9.4. Resiliency and Availability

The NRS system should be resilient against denial-of-service attacks and other common attacks to isolate the impact of the attacks and prevent collateral damage to the entire system. Therefore, if a part of the NRS system fails, the failure should only affect a local domain. And fast recovery mechanisms need to be in place to bring the service back to normal.

5. Conclusion

ICN routing may comprise three steps: name resolution, content request routing, and content delivery. This document investigates the name resolution step, which is the first and most important to be achieved for ICN routing to be successful. A Name Resolution Service (NRS) in ICN is defined as the service that provides such a function of name resolution for translating an object name into some other information such as a locator, another name, metadata, next-hop info, etc. that is used for forwarding the object request.

This document classifies and analyzes the NRS approaches according to whether the name resolution step is separated from the content request routing as an explicit process or not. This document also explains the NRS functions used to support heterogeneous name types, producer mobility, scalable routing system, off-path caching, nameless object, manifest, and metadata. Finally, this document presents design considerations for NRS in ICN, which include resolution response time and accuracy, resolution guarantee, resolution fairness, scalability, manageability, deployed system, and fault tolerance.

6. IANA Considerations

This document has no IANA actions.

7. Security Considerations

A discussion of security guidelines is provided in Section 4.9.

8. References

8.1. Normative References

[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>.

8.2. Informative References

[Afanasyev] Afanasyev, A. et al., "SNAMP: Secure Namespace Mapping to Scale NDN Forwarding", 2015 IEEE Conference on Computer Communications Workshops, DOI 10.1109/INFCOMW.2015.7179398, April 2015, <https://doi.org/10.1109/INFCOMW.2015.7179398>.

[Ahlgren] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., and B. Ohlman, "A Survey of Information-Centric Networking", IEEE Communications Magazine, Vol. 50, Issue 7, DOI 10.1109/MCOM.2012.6231276, July 2012, <https://doi.org/10.1109/MCOM.2012.6231276>.

[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), DOI 10.1109/EuCNC.2014.6882665, June 2014, <https://doi.org/10.1109/EuCNC.2014.6882665>.

[Amadeo2] Amadeo, M. et al., "Information-centric networking for the internet of things: challenges and opportunities", IEEE Network, Vol. 30, No. 2, DOI 10.1109/MNET.2016.7437030, March 2016, <https://doi.org/10.1109/MNET.2016.7437030>.

[Baccelli] Baccelli, E., Mehlis, C., Hahm, O., Schmidt, T., and M. WÃ¤hlisch, "Information Centric Networking in the IoT: Experiments with NDN in the Wild", ACM-ICN 2014, DOI 10.1145/2660129.2660144, 2014, <https://doi.org/10.1145/2660129.2660144>.

[Bari] Bari, M.F., Chowdhury, S.R., Ahmed, R., Boutaba, R., and B. Mathieu, "A Survey of Naming and Routing in Information-Centric Networks", IEEE Communications Magazine, Vol. 50, No. 12, pp. 44-53, DOI 10.1109/MCOM.2012.6384450, December 2012, <https://doi.org/10.1109/MCOM.2012.6384450>.

[Bayhan] Bayhan, S. et al., "On Content Indexing for Off-Path Caching in Information-Centric Networks", ACM-ICN 2016, DOI 10.1145/2984356.2984372, September 2016, <https://doi.org/10.1145/2984356.2984372>.

[CCNx] "CICN", <https://wiki.fd.io/view/Cicn>.

[Dannewitz] Dannewitz, C. et al., "Network of Information (NetInf) - An information-centric networking architecture", Computer Communications, Vol. 36, Issue 7, DOI 10.1016/j.comcom.2013.01.009, April 2013, <https://doi.org/10.1016/j.comcom.2013.01.009>.

[FLIC] Tschudin, C., Wood, C. A., Mosko, M., and D. Oran, "File-Like ICN Collections (FLIC)", Work in Progress, Internet-Draft, draft-irtf-icnrg-flic-03, 7 November 2021, <https://datatracker.ietf.org/doc/html/draft-irtf-icnrg-flic-03>.

[ID.Zhang2] Ravindran, R., Zhang, Y., Grieco, L. A., Lindgren, A., Burke, J., Ahlgren, B., and A. Azgin, "Design Considerations for Applying ICN to IoT", Work in Progress, Internet-Draft, draft-irtf-icnrg-icniot-03, 2 May 2019, <https://datatracker.ietf.org/doc/html/draft-irtf-icnrg-icniot-03>.

[Jung] Jung, H. et al., "IDNet: Beyond All-IP Network", ETRI Journal, Vol. 37, Issue 5, DOI 10.4218/etrij.15.2415.0045, October 2015, <https://doi.org/10.4218/etrij.15.2415.0045>.

[Koponen] Koponen, T., Chawla, M., Chun, B., Ermolinskiy, A., Kim, K.H., Shenker, S., and I. Stoica, "A Data-Oriented (and Beyond) Network Architecture", ACM SIGCOMM 2007, pp. 181-192, DOI 10.1145/1282380.1282402, August 2007, <https://doi.org/10.1145/1282380.1282402>.

[MF] "MobilityFirst Future Internet Architecture Project Overview", <http://mobilityfirst.winlab.rutgers.edu>.

[Mosko2] Mosko, M., "Nameless Objects", IRTF ICNRG, January 2016, <https://datatracker.ietf.org/meeting/interim-2016-icnrg-01/materials/slides-interim-2016-icnrg-1-7.pdf>.

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

[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, DOI 10.1109/ICIN.2018.8401595, February 2018, <https://doi.org/10.1109/ICIN.2018.8401595>.

[NRSarch] Hong, J., You, T., and V. Kafle, "Architectural Considerations of ICN using Name Resolution Service", Work in Progress, Internet-Draft, draft-irtf-icnrg-nrsarch-considerations-06, 12 February 2021, <https://datatracker.ietf.org/doc/html/draft-irtf-icnrg-nrsarch-considerations-06>.

[PURSUIT] "FP7 PURSUIT", <https://www.fp7-pursuit.eu/>.

[Quevedo] Quevedo, J., Corujo, D., and R. Aguiar, "A case for ICN usage in IoT environments", IEEE GLOBECOM, DOI GLOCOM.2014.7037227, December 2014, <https://doi.org/GLOCOM.2014.7037227>.

[Ravindran]

Ravindran, R., Chakraborti, A., and A. Azgin, "Forwarding Label support in CCN Protocol", Work in Progress, Internet-Draft, draft-ravi-icnrg-ccn-forwarding-label-02, 5 March 2018, <https://datatracker.ietf.org/doc/html/draft-ravi-icnrg-ccn-forwarding-label-02>.

[RFC6920] Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Keranen, A., and P. Hallam-Baker, "Naming Things with Hashes", RFC 6920, DOI 10.17487/RFC6920, April 2013, <https://www.rfc-editor.org/info/rfc6920>.

[RFC8569] Mosko, M., Solis, I., and C. Wood, "Content-Centric Networking (CCNx) Semantics", RFC 8569, DOI 10.17487/RFC8569, July 2019, <https://www.rfc-editor.org/info/rfc8569>.

[RFC9064] Oran, D., "Considerations in the Development of a QoS Architecture for CCNx-Like Information-Centric Networking Protocols", RFC 9064, DOI 10.17487/RFC9064, June 2021, <https://www.rfc-editor.org/info/rfc9064>.

[SA2-5GLAN] 3GPP, "New WID: 5GS Enhanced support of Vertical and LAN Services", TSG SA Meeting #SP-82, December 2018, <http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_82/Docs/SP-181120.zip>.

[SAIL] "Scalable and Adaptive Internet Solutions (SAIL)", <http://www.sail-project.eu/>.

[Westphal] Westphal, C. and E. Demirors, "An IP-Based Manifest Architecture for ICN", ACM-ICN 2015, DOI 10.1145/2810156.2812614, September 2015, <https://doi.org/10.1145/2810156.2812614>.

[Xylomenos] Xylomenos, G., Ververidis, C., Siris, V., Fotiou, N., Tsilopoulos, C., Vasilakos, X., Katsaros, K., and G. Polyzos, "A Survey of Information-Centric Networking Research", IEEE Communications Surveys and Tutorials, Vol. 16, Issue 2, DOI 10.1109/SURV.2013.070813.00063, 2014, <https://doi.org/10.1109/SURV.2013.070813.00063>.

[Zhang2] Zhang, Y. et al., "A Survey of Mobility Support in Named Data Networking", IEEE Conference on Computer Communications Workshops, DOI 10.1109/INFCOMW.2016.7562050, April 2016, <https://doi.org/10.1109/INFCOMW.2016.7562050>.

Acknowledgements

The authors would like to thank Dave Oran, Dirk Kutscher, Ved Kafle, Vincent Roca, Marie-Jose Montpetit, Stephen Farrell, Mirja KÃ¼hlewind, and Colin Perkins for very useful reviews, comments, and improvements to the document.

Authors' Addresses

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

Email: jhong@etri.re.kr

Tae-Wan You
ETRI

Yuseung-Gu
218 Gajeong-ro
Daejeon
34129
Republic of Korea

Email: twyou@etri.re.kr

Lijun Dong
Futurewei Technologies Inc.
10180 Telesis Court
San Diego, CA 92121
United States of America

Email: lijun.dong@futurewei.com

Cedric Westphal
Futurewei Technologies Inc.
2330 Central Expressway
Santa Clara, CA 95050
United States of America

Email: cedric.westphal@futurewei.com

BÃ¶rje Ohlman
Ericsson Research
SE-16480 Stockholm
Sweden

Email: Borje.Ohlman@ericsson.com