Potential and Challenges of Information-Centric Networking

Hitoshi ASAEDA

Information- (or Content-) Centric Networking (ICN/CCN) uses "content name" as the communication identifier and enables users to obtain content from caching routers or nodes in the network. This future Internet technology provides content for users rapidly and effectively. ICN naturally supports mobility, broad/multicasting, and server-less communications. In this report, we present a great potential ICN gives and ICN research challenges we have been tackling.

1 Introduction

Today, the ever-increasing proliferation of high-performance mobile nodes (tablets, smart phones and others) and user-driven information-disseminating services such as SNS (social networking service) are stimulating further increase in Internet traffic, which is already quite busy handling rich contents such as music and video. To address these new waves of devices and services, conventional communication procedures that have been used for FTP (file transfer protocol) and sending/receiving mails are still in place—i.e. searching the server location (IP address) using the domain-name resolution system (DNS), followed by access to the server with the IP address for obtaining the desired content. Note, however, that the requirement placed on the user in this scheme—accessing a server that may be remotely located—is not essential to a communication if the objective of the communication is to fetch content. It would be more efficient if a communication unit (typically a router) near the user caches the desired content and provides the content to the user directly. It is considered that effective utilization of such units will pave the way for a new communication technology that will address further traffic increase in the future.

One of the new-generation networking technologies—called Information/Content-Centric Networking (ICN/CCN), hereafter referred to simply as ICN—has evolved from this concept. In an ICN system, a user fetches content by using its name, rather than by using an IP address. If a node (such as a router) located near the user contains the content or cache, the node transfers it directly to the user.

This scheme enables quicker information services independent of the conditions in which the servers are placed, leading to more effective utilization of server and network resources. Realization of the new communication architecture (ICN) still requires a variety of research and development efforts, because its non-reliance on the sender/receiver IP address scheme necessarily involves alternative communication technologies dissimilar to the current IP address-based technologies.

As a candidate new-generation networking technology, ICN has gained the spotlight both in Japan and overseas, on which a variety of studies are actively underway in the academic society in Japan[4]. In this report, the author outlines the possibilities that may be brought about by the introduction of ICN, some of the research challenges to be overcome for its realization[5], and the research themes to be tackled by the National Institute of Information and Communications Technology (NICT).

2 Content name and communication identifier

Unlike IP communication that uses an IP address as the destination identifier, ICN uses "interest" packets for communication, in which the content name is used as the destination identifier. Upon accepting an interest packet, the router returns the requested content to the originating host if it contains/caches it. If not, the router forwards the interest packet either to upstream routers on the routing path or to the neighbor routers that may have cached it. As a result, this scheme may lead to shorter response times as compared to conventional IP address based communication. Additional potential merits include upgraded efficiency of network usage (or reduction in communication traffic) and saving of server resources.

To perform content name-based communication, the content name must be uniquely identified by all the parties

involved: the receiver and the sender, or the network devices that transfer data. In other words, successful implementation of ICN requires a guarantee of uniqueness of the content name in the network. Successful completion of an IP-based communication is guaranteed by the global unique IP addresses on the Internet, which are managed by IANA (ICANN)[6] (or, by global uniqueness of the gateway's IP address that performs Network Address Translation (NAT)[7]). On the other hand, content names can be arbitrarily determined in the current Internet system. Therefore, to use the content name as a communication identifier, construction of a unified framework (or "naming" system) is required to specify unique and unambiguous content names. Against this backdrop, the discussions now underway in ICN research are grouped largely into the two approaches described next.

The first approach is to utilize current mainstream identifiers—e.g. URLs used to access websites, and other similar identifiers—as surrogates for content names. For example, content names proposed by CCN[1]/NDN[2] have a format such as "/example.com/news/today/video.mpg/_v<timestamp>/_segnum", in which case each router maintains routing path information corresponding to the prefix delimited by "/". This format enables the user to fetch the content from the caching routers on the path. This URL-style prefix-based name construction has a merit to facilitate ensuring uniqueness of the content, because it contains elements—typically domain names—used commonly in the current Internet practices. However, it also involves some problems. For example, a content owner in a mobile communication environment may alter his/her content name when he/she moves to a different domain network (i.e. source network of the content transmission), and then it is necessary for the receiver to re-send the data transmission request after changing the content name. Another problem lies in the difficulty of certifying the authenticity of the content name's portion below the domain name. Taking the content name, "/example.com/alice/sport/video.mpg," for example, it is impossible, only on the basis of this content name, to determine which Alice, among those who are named Alice, created this content, whether it is truly content created by Alice, or who actually created this content, or to guarantee the identification of the true creator of this content.

On the other hand, there has been ICN research, as shown in [3], that includes original naming technologies as a part of the communication architecture. In the study shown in Reference [3], a content name is constructed by first combining portions of meaningful names—e.g. "A company," "B division," "2015.10.1," and the file name "Conference_Document.pdf"—and then by connecting it with the hash of the content owner's public key, followed by signing the string with the content owner's secret key (this technique is called a "Self-signed certificate"). In this example, a different name ("Example corp. headquarter" instead of "Example corp.") and different order (e.g. "2015.10.1" comes before "Example division") generate a different content name.

A self-signed certificate (the content owner's signature given to the content name) provides the key to judge the authenticity of the content name. However, this naming convention has the problem of eliminating dependency between the content name (determined in flat namespace, instead of hierarchical structure as seen in URLs) and the routing or network topology. Therefore, a new mechanism must be implemented to configure/manage the network topology to which the content sender and receiver belong and connect the content name to the network topology. This mechanism—called "topology manager" in Reference [3]—must satisfy very complex functional requirements and can be a technological bottleneck. In addition, a content name is binary data, which is generated through the process of a "Self-signed certificate." It is difficult to recognize or trace the meaning of the content by users because the binary data is not human readable.

Regarding the naming technique in ICN research, many other studies have been conducted ([8], [9] and others). In our view, the range of networking and services within which the uniqueness of content names must be guaranteed—in other words, determination of the "scope" of communication objectives—plays a decisive role in the naming scheme in ICN. There are many cases in which the guarantee of uniqueness is required only within a certain scope—for example, within a network or application. Such instances include: sensor information inside a storehouse, video contents shared in a household, information/content relevant only in a localized network (dissimilar from, or separated from the Internet), and contents that serve only in specific applications and services. On the other hand, content on the Internet must have an identifier that guarantees its global uniqueness. For a naming system applicable to the countless number of contents on the Internet, it would be practical to make use of the URL-like hierarchical name construction, with additional mechanisms to resolve the problems described above.

Based on this standpoint, we designed an ICN

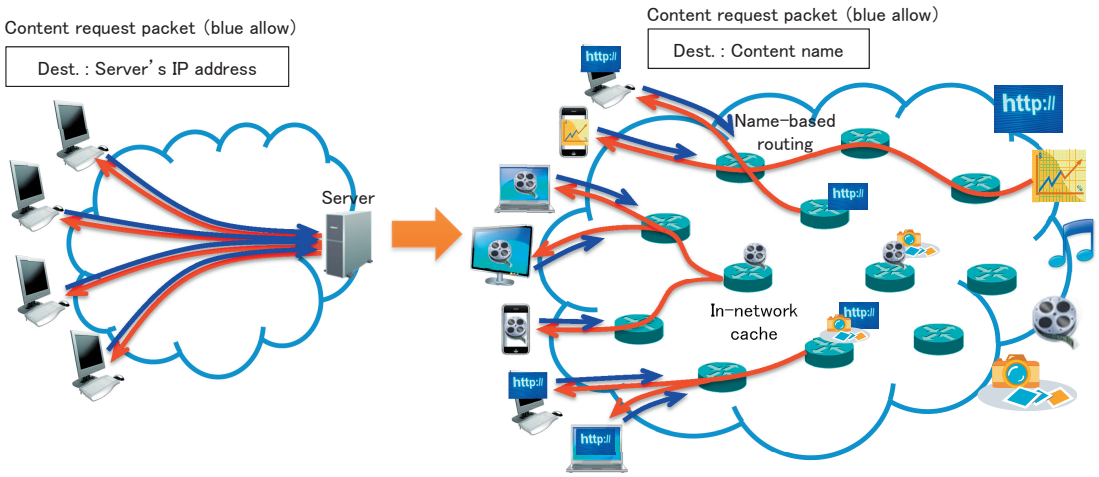

Fig. 1 Transition to Information-Centric Networking: from IP address-based to content name-based communication

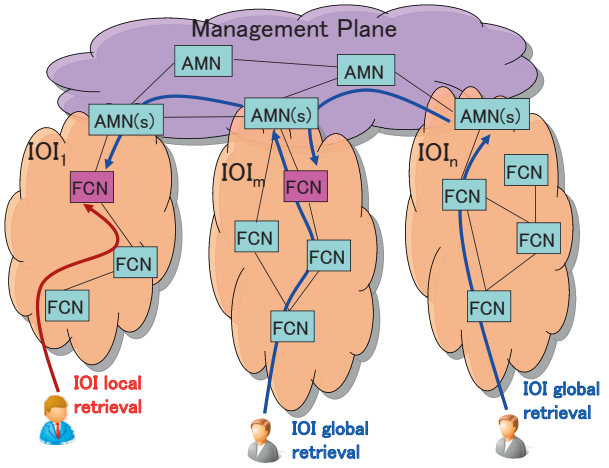

Fig. 2 Concept of Aggregatable Name-Based Routing (ANBR)

architecture—Aggregated Name-Based Routing (ANBR)[10] (see Fig. 2). In ANBR, the network that carries contents is divided into relatively small scopes, called Internet Islands (IOI), and the contents and routing are managed on a scope-by-scope basis. A router (Forwarding Cachable Node (FCN)) and a node (Aggregate Management Node (AMN)) are arranged in each IOI. All the contents within an IOI are registered to the AMN (guarantee of uniqueness of all the contents within an IOI), and this enables the FCN to control routings to reach to the contents within it. In addition, all of the AMNs are connected by means of an overlay network called the Management Plane. In wide area network communication that spans across IOIs, this overlay network enables the user to create a communication path by specifying the destination IOI name, allocated by ANBR, to the content name. A request for a content residing in another IOI is transferred to the destination IOI via the AMN in the source IOI.

In addition to the research described above, studies are also underway on the Name Resolution System (NRS) with special focus on the management of global content name information. NRS is an implementation similar to DNS (Domain Name System) on the Internet, and the NRS under study for implementation in the proposed ICN is designed based on the Distributed Hash Table (DHT) concept. We expect that the results obtained here can find their application in the implementation of the Management Plane in ANBR. See **6-2** for further information on NRS research.

3 In-network caching and name-based routing

One of the basic functions implemented in ICN is "in-network caching": each router in the network holds cache autonomously in distributed fashion, and transmits data upon content requests. This caching system requires a judgment mechanism, and its optimization, as to which router should cache which content, and how long the router should maintain the cache. As the routers in ICN obey "name-based routing," they must resolve the content name embedded in the interest packet and forward it to upstream routers accordingly.

During this process, the routers attempt to upgrade the efficiency of content transfer by, for example, searching for an appropriate neighbor cache router in coordination with the caching functions implemented in the network and steer the interest packet to it. Algorithms for this purpose are being studied actively.

In the ANBR system described above, contents are cached in FCNs (shown in red in Fig. 2) as appropriate, and the cache information is recorded in the corresponding

IOI. Based on this information, AMN steers content requests through the shortest possible route, contributing to upgrading network usage efficiency and reducing communication delay.

See **6-4** for further details on our research conducted so far on in-network caching and route guidance.

4 ICN testbed

In studies of communications architectures and protocols, simulators such as ns-3[11] and emulators such as Mini-CCNx[12] often provide a useful testing bench for evaluation of algorithm design and functionality. These evaluation tools, especially emulators, provide excellent services in early stages of protocol design and other research owing mainly to their easily configurable nature to realize a desirable evaluation environment. However, when applied to a communication environment (typically the Internet) in which resources are shared by an unspecified number of users, the performance results obtained in such simulator evaluations may often fail to materialize in the real-life environment because of competing traffic that occurs suddenly and unsteadily. Simulators and emulators also prove to be an insufficient evaluation tool when total performance of the system—including usage rate of computers—is under study. For this reason, construction of a "global testbed" (with workable prototypes implemented on it) is essential for research that aims at going into actual use. The global testbed deployed on the Internet then facilitates evaluating the implementation feasibility of the prototypes.

PlanetLab[13] is one representative case of such global testbeds deployed on the Internet. PlanetLab is a highly versatile testbed with a distributed arrangement of servers allocated in more than 1,000 sites, which allows the user to share those server resources for running and evaluating programs of their own development.

Several challenges must be overcome, however, before applying PlanetLab for the implementability validation of ICN. Construction of an experiment environment that includes a network layer represents one such challenge: this environment is required because ICN relies on name-based routing instead of IP address-based routing used in the current IP networks. As PlanetLab presupposes its use as a tool to evaluate the protocol performance in the higher layers of the IP network, e.g., the transport layer, construction of an environment is required using specialized tools and methods to accommodate evaluation of lower layers and routings, whereas it will take substantial cost for such evaluation. As many Planetlab users share common server resources simultaneously, a high-load experiment conducted by a specific user may affect other users' performance measurements and experiments. In addition, some ICN implementation (such as CCNx 0.8.2[14], which is the most popular ICN prototype implementation) uses memory as in-network cache, while larger cache capacity increases memory usage as server resource, leads to degraded system performance as a whole, and finally disables accurate verification of the implementation.

Viewing such issues in perspective, we developed a testbed specially designed for ICN using Linux Container (LXC) as the node virtualization technology[15]. The node configuration of the testbed is designed to operate on a virtual machine (VM) that runs on either VMware Hypervisor (ESXi), KVM, or VMware Player, and each LXC container defined on the VM is allocated to the user. The ICN testbed provides the following features: (1) the user can use each container as a virtually-independent server machine, (2) a unique local IP address is assigned to each container, and enables the user to access other containers in external testbed nodes via the Internet and to operate a dissimilar routing protocol independently, (3) the containers are installed with a common set of software and libraries used to evaluate ICN implementation as well as the Contrace evaluation tools[16] we originally developed (see further descriptions below), and (4) implementation of a resource management mechanism that allows setting the upper limit of CPU and memory resource usage, and is accessible from each container—this mechanism prevents any one user from exhausting the resources, but also allows any user to upgrade (on first-come basis) the limit imposed on him/her if there is enough leeway in the computer resources. In this ICN testbed, a cache area is secured for the CCNx users not in memory but in the filesystem. Cache data kept in the filesystem cache can be occupied by a single user or shared by more than one user. Active use of read-ahead and parallelized data transfer capabilities of the filesystem caching realize cache reading/writing performance that compares favorably with in-memory caching systems (see Reference [15] for detailed descriptions), and constitute an environment that allows a number of users to access the ICN testbed simultaneously.

In addition, we introduced a network tool of our own development called Contrace[16] to the ICN testbed, which contributes to verifying user-developed protocols and implementations. The testbed user can run the Contrace

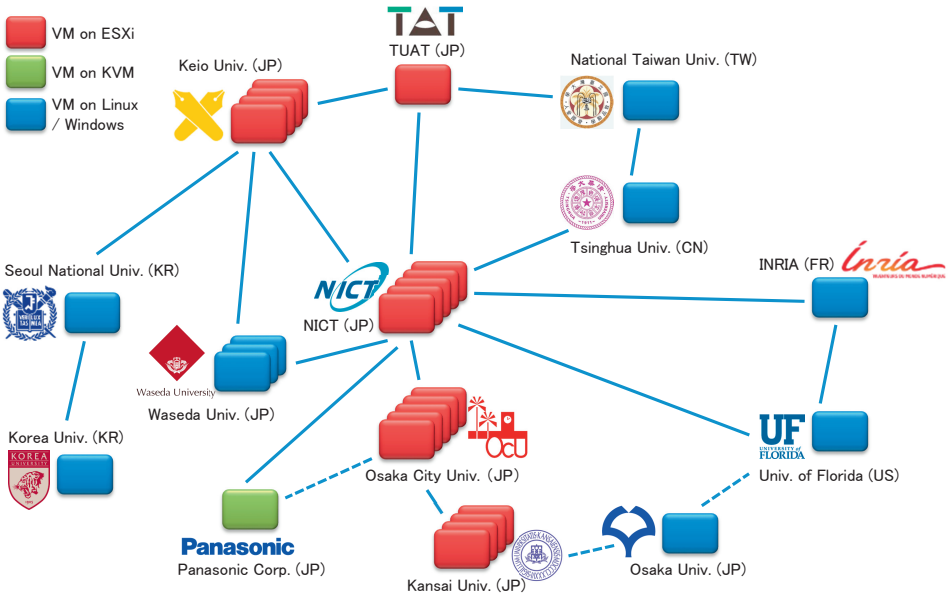

Fig. 3 An example of ICN testbed deployment (as of the 1st of June 2015) and ICN topology

command with a content name given as the argument, which invokes the Contrace daemon in the container. The daemon tracks/measures such variables as the cache routers along the routing path, transfer performance of the content (or cache), cache life time and hit ratio, and reports them to the user. By taking advantage of functions provided by Contrace, users can evaluate their ICN routing algorithms and implementations. It is also possible for users to compare their implementations with those developed by other researchers, and with the conventional IP network communication.

As shown in Fig. 3, this testbed site has been deployed in 14 organizations in and outside Japan (as of the 1st of June 2015). Further expansion of sites will be realized for enabling better ICN experiments in a wider area.

References

1 V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking Named Content," Proc. ACM CoNEXT 2009, pp.1–12, Dec. 2009.

2 "Named Data Networking," available at: http://named-data.net/.

3 D. Trossen, M. Sarela, and K. Sollins, "Arguments for an information-centric internetworking architecture," SIGCOMM Comput. Commun. Rev., Vol.40, No.2, pp.26–33, April 2010.

4 "Technical Committee on Information-Centric Networking (ICN)," The Institute of Electoronics, Information and Communication Engineers (IEICE), available at: http://www.ieice.org/~icn/ (Japanese only).

5 H. Asaeda, "Towards the Implementation of Information-Centric Networking (ICN)," IEICE Technical Report (Japanese edition), June 2015.

6 "IANA – Internet Assigned Numbers Authority", available at: http://www.iana.org/.

7 K. Egevang and P. Francis , "The IP Network Address Translator (NAT)," IETF RFC 1631, May 1994.

8 A. Ghodsi, T. Koponen, J. Rajahalme, S. Sarolahti, and S. Shenker, "Naming in Content-Oriented Architectures," Proc. ACM SIGCOMM ICN WS, Aug. 2011.

9 K. Sollins, "Pervasive Persistent Identification for Information Centric Networking," Proc. ACM SIGCOMM ICN Workshop, Aug. 2012.

10 R. Li, H. Harai, and H. Asaeda, "An Aggregatable Name-Based Routing for Energy-Efficient Data Sharing in Big Data Era," IEEE Access, Vol.3, 2015.

11 "Ns-3 network simulator," available at: https://www.nsnam.org/.

12 C. Cabral, C. E. Rothenberg, and M. Magalhaes, "Mini-CCNx Fast Proto-typing for Named Data Networking," Proc. ACM SIGCOMM ICN'13 Workshop, Hong Kong, Aug. 2013.

13 "PlanetLab," available at: http://www.planet-lab.org/.

14 "CCNx implementation," available at: http://www.ccnx.org/.

15 H. Asaeda, R. Li, and N. Choi, "Container-based Unified Testbed for Information-Centric Networking," IEEE Network, Vol.28, No.6, pp.60–66, Nov. 2014.

16 H. Asaeda, K. Matsuzono, and T. Turletti, "Contrace: A Tool for Measuring and Tracing Content-Centric Networks," IEEE Commun. Mag., Vol.53, No.3, pp.182–188, March 2015.

Hitoshi ASAEDA, Ph.D.

Planning Manager, New Generation Network Laboratory, Network Research Headquarters
Information Centric Networking