A Deployable and Scalable Information-Centric Network Architecture

Yuncheng Zhu
The University of Tokyo
qq109531@iii.u-tokyo.ac.jp

Akihiro Nakao
The University of Tokyo
nakao@iii.u-tokyo.ac.jp

Abstract—The misalignment between the host-centric architecture and the content-centric usage of the current Internet results in inefficient content and service access. Recent content-oriented network research fails to address the critical importance of an information-centric network architecture providing the availability of clients accessing services with user-generated content as well as accessing published content from the Internet services. This paper proposes a Deployable and Scalable Information-Centric Network Architecture (DSINA) that incorporates route-by-name system into the current Internet infrastructure. In this architecture, not only DSINA name information but also traditional host location is handled by network devices. With the register-access-result model, DSINA can handle not only content retrieval, but also other applications including user-generated content uploading and notification pushing.

Index Terms—information-centric networks, user-generated content, content delivery

I. INTRODUCTION

The current Internet architecture has remained relatively unchanged as end-to-end data communications since its turning point from the test-bed for interconnecting protocols to business and commercial use. Since the misalignment between the host-centric architecture and the content-centric usage of the current Internet results in inefficient content and service access, providers try to improve bandwidth utilization and reduce queuing delay by deploying content delivery networks (CDN) [1] and proxy caches [2]. Although caching facilities greatly improve content retrieve efficiency and thus are common nowadays, these intermediate elements are not integrated with routing and forwarding. As a result, they are criticized to be indirect, expensive and sometimes conflicting with the interest of network providers.

On the other hand, a number of researchers are aiming at redesigning the Internet from the content-oriented perspective. In their clean-slate designs [3], [4], [5], content delivery is directly central to the network architectures proposed. In these architectures, network devices forward the request of a specific piece of information to wherever the content is available, and carry the corresponding content towards the users requesting it. Therefore, the most critical information in routers is no longer what records the routes to networks and hosts, but the query and the result, that is, the information on the existence of the content.

However, all the content-oriented network architectures proposed today fail to address the critical importance of providing the availability of clients accessing services with user-generated content as well as accessing published content from Internet services. They can only handle the case that content is delivered from persistent servers (or caching hosts), but cannot deal with the situation where a client wants to push some data to a specified server or network service directly. In addition, some of such architectures have problems such as locating content storage only in forwarding nodes, not supporting name aggregation, or requiring additional rendezvous nodes.

In this paper, we propose a Deployable and Scalable Information-Centric Network Architecture (DSINA), which incorporates novel route-by-name system into the current Internet infrastructure. In the light of the host-to-host model in the traditional TCP/IP protocol suite, we posit that the most appropriate abstraction for a new architecture should be host-to-content or host-to-service. Therefore, not only content and service accessibility knowledge but also traditional host location information are critical information handled by network devices in DSINA. We propose register-access-result model to achieve content and client access, where data can be carried by both access and result messages. Compared to the existing proposals for future network architectures, DSINA can handle not only content retrieval as is done in content-oriented network architectures, but also user-generated content uploading, notification pushing and other applications. Moreover, persistent data storage and transient caches are separately used in DSINA and different strategies are employed to handle these two sorts of cache storage.

Besides providing unique information-centric functionalities, efforts have also been put to enhance the deployability and scalability of the architecture. Considering the deployability, DSINA is designed to operate over the current Internet infrastructure and allow incremental deployment of new functionalities. Regarding the scalability of inter-domain name propagation and resolution, DSINA adopts a hierarchical naming system, and uses distributed service to enable quick name resolution.

The remainder of the paper is organized as follows. In Section II, famous research efforts related to our work are discussed. In Section III and Section IV, we present design decisions in three aspects and the Deployable and Scalable Information-Centric Network Architecture (DSINA). In Section V, we discuss applications, transport protocol and security concerns of DSINA. And finally, we conclude our work in
II. RELATED WORK

The Content-Centric Networking (CCN) [3] proposes hop-by-hop content-centric routing based on hierarchical content names. In CCN, instead of host prefixes, content prefixes are stored in forwarding nodes. A forwarding node receives an “interest” packet sent from clients or other forwarding nodes, records the incoming interface and forwards the packet. A “data” packet responded by the server is forwarded exactly in the reverse direction to reach the client. However, the architecture has difficulty in supporting data uploading, while user-generated content is becoming popular nowadays [6], [7]. Since host locating information is eliminated from the architecture, the work-around suggests a client to send an “interest” packet including the publishing name for uploading data to trigger the server initiating another content retrieval process towards the client itself. This requires the client announce the name for its uploading data beforehand so that it is accessible from the server, while such behavior hampers the aggregation of names and the mobility of client hosts. DSINA borrows the hierarchical naming system from CCN, but extends it to both content and services so that clients can upload data directly to named services as they do today. Distributed name resolution service is also introduced to ensure fast access. Moreover, DSINA removes the limitation on locating content storage only in forwarding nodes.

In order to provide persistence, availability and authenticity in content access, the Data-Oriented Network Architecture (DONA) [4] adopts routing based on flat and self-certifying names rather than on hierarchical ones. In DONA, publishers “register” content and its locations to network devices, while clients send “find” packets to resolve the names and initiate the transport exchange. The packet exchanges that occur after a “find” packet reaching its target server are not handled by the proposed system but using standard IP routing and forwarding. Designed as a replacement to DNS naming resolution scheme, DONA is inadequate in taking into account the scalability problem. It is neither possible to store nor to resolve all unaggregated names for all the content available in the Internet for any network device in a tier-1 network. Aggregation for flat names [8] requires publishers to provide aggregation information, but it is hard to justify both incentives for such scheme and its effectiveness.

The Publish-Subscribe Internet Routing Paradigm (PSIRP) [5] focuses on providing layered information access control using rendezvous nodes. In this architecture, the metadata of published content is stored in the rendezvous nodes, and is accessible only by the members of the scope specified by the content. Users subscribe with specified identifier to the rendezvous node, which subsequently creates a forwarding path from the publishing server to the users using an MPLS-like label switching protocol and initiates the actual data transfer. However, this architecture does not specify how publish and subscribe messages are forwarded to the rendezvous node in charge, which is one of the critical challenges to information-centric networks. Besides, adopting label switching for content forwarding is impractical for the Internet, because the rendezvous node has to operate network devices of other network providers when the subscription comes from an external network, which is the very same problem that Multiprotocol Label Switching (MPLS) has been facing when it comes to wide-area routing.

DSINA incorporates several ideas from our past projects. In the Content-Oriented Network with Indexed Caching (CONIC) [9], we have proposed to exploit spare storage and bandwidth from end-system to eliminate redundant traffic and to enable efficient and fast access of content. The basic design of CONIC is to put cache storage onto end hosts while leaving the index on the network devices. In this way, the caching index can be distributed on several network devices without duplicating the cached content itself. To achieve efficient content-oriented network transport over the existing Internet infrastructure, we have also presented the Content-Oriented Transport Protocol (COL4) [10], a content-oriented and connection-less transport layer protocol enabling in-network processing, content-oriented security and transfer control.

III. DESIGN DECISIONS

According to the preceding analysis of the existing information-centric network architectures, it is obvious that there are three aspects to be improved in order to achieve efficient content and service access. In this section, we propose design decisions in the three aspects, functionality, deployability and scalability, that DSINA has to achieve.

A. Functionality

DSINA is designed to support a variety of content and service access, including but not limited to efficient content distribution. There are two unique novel functionalities employed in DSINA, user-generated content support and hierarchical caching scheme.

Upload of user-generated content, an emerging application of today’s Internet, is one of the features that must be supported by DSINA. As analyzed in the previous section, the interest-data model which is widely used in information-centric networks is not optimal for supporting content pushing. DSINA supports content pushing by enabling packets to carry payload data not only as responses but also as requests. Caching and authentication mechanisms for data uploading are also available as options provided by the architecture.

Content caching is one of the most important features of information-centric networks. In reality, caching facilities can be classified into two categories, persistent data storages, such as CDN, and transient caches, such as in-network caching and caching at client hosts. In DSINA, these two sorts of caching are distinguished in registration and propagation of content information, and different strategies are used correspondingly.

B. Deployability

Deployability is one of the distinctive features of DSINA compared to the existing information-centric networks. Different from clean-slate designs, the design of DSINA puts
a lot of effort into incremental deployment from the edge networks. Although the architecture is self-scaling, that is, the more servers and routers are enabled with DSINA, the better the efficiency of content and service access becomes, the architecture does not require routers in the core network to be upgraded to make the whole network benefit from the new architecture.

Moreover, the difficulty in supporting new functionalities is reduced by separation of cache storage and forwarding. Inheriting the idea of exploit spare storage and bandwidth from end-system [9], DSINA removes the limitation on locating content storage only in forwarding nodes. This enables the existing routers to be able to support the new architecture only by upgrading its software, without the cost to attach storage devices to all the network devices.

C. Scalability

Network routing scalability issues have been driving new network architecture designs, recently. Route-by-name, the new system adopted by information-centric networks, faces a scalability challenge which is much more critical than it is in the current Internet. The previous study [4] has revealed that the amount of registered names is in the order of 10^{10} or more, even under the optimistic expectation, extrapolated from the HTTP request rate in the Internet of today, i.e., about 10,000/Gb. This rate is unlikely to be resolved by a single network device and calls for a distributed solution.

DSINA employs a hierarchical and distributed route-by-name system, where globally available registration information is handled by an overlay system called Distributed Resolution Service (DRS). An individual DSINA router only stores all locally registered names and a fragment of foreign registered names, providing efficient resolution of frequently used names. If a DSINA message carries a name that is not resolvable in some DSINA router, it gets forwarded to the DRS. The names themselves are also hierarchical and therefore aggregatable, so that high hit rate for resolution can be achieved with a limited number of entries in DSINA routers.

IV. ARCHITECTURE

The purpose of DSINA is to achieve efficient content and service access by incorporating novel route-by-name system into the current Internet infrastructure. According to this objective and the design decisions stated in Section III, this section first introduces the overview of the architecture, followed by its naming system design, and then presents the register-access-result model.

A. Overview

As illustrated in Fig. 1, DSINA consists of three kinds of entities, client end-points, content/service end-points and DSINA routers. Communications in DSINA are abstracted as client-content/client-service asymmetric conversations. That is to say, in DSINA, a client end-point is located by its address as it is done in the current Internet, while a content end-point or a service end-point is located by a novel naming system.

Running above the existing Internet infrastructure, DSINA does not require all the routers to be migrated to benefit from the new architecture, especially the ones in the core networks (those not in the dotted frames in the figure) that can remain legacy ones. When a packet with DSINA name passes through a DSINA router, it gets forwarded by the name and has its network layer locator (i.e. IP address in the current Internet) modified correspondingly. While it passes through a legacy router, it is simply forwarded according to its network layer locator.

B. Naming system

DSINA adopts a human-readable, hierarchical naming system, which is similar to that used in CCN [3]. A DSINA name is composed of two parts, the publisher identifier and the publisher-dependent name. The former is a registered global-unique identifier that is similar to a domain name today and corresponds to a certificate issued by the registration organization so that content and services could be signed and verified, while the latter is a segmented name that is arbitrarily specified by the publisher to describe a specific piece of content or service provided by that publisher. To represent a group of content or services that share similar features, publishers can use an DSINA prefix which is composed by the publisher identifier and the prefix part of the publisher-dependent names. An example of DSINA names and prefixes is shown in Fig. 2.

For each name or prefix, there are two essential attributes, delegation and forwarding. The first attribute decides whether the content or services can be registered by a third-party without the certificate of the publisher. Names that allow delegation usually stand for the content that can be duplicated by anyone, while those that do not allow delegation usually designate services end-points that can only be deployed by the publisher and authorized partners. The second attribute, forwarding, specifies whether an access request to it should be forwarded to any end-point satisfying the request or all such end-points. An access message forwarded to all the end-points can be duplicated only at necessary network devices and saves bandwidth. The detailed usage of the attributes is described in the following parts.
C. Register

Any content or service end-point must be registered first to be accessed in DSINA. There are two kinds of registration, authoritative registration and delegated registration. The registration information and its propagation formulates the control plane of DSINA.

Authoritative registration is done by a publisher or its authorized partners, for example, Content-Distribution Networks (CDN). The registrant provides Authoritative Registration Information (ARI), which is composed by names, attributes and their locators with specific certificate of the publisher, to its upstream router. The DSINA router that handles ARI also submits it to the Distributed Resolution Service (DRS) of the local network, which is an overlay service realized by all the DSINA routers and other computing resources of the service provider, or can be shared by several service providers. An individual DSINA router stores three kinds of ARI records: all the locally registered ARI, a fragment of remote registered ARI that it is in charge of in the local DRS, and an ARI cache of frequently accessed remote registered ARI. The propagation of ARI among DRS is similar to that of today’s inter-domain routing, except that the object is not an address prefix but ARI. A DRS receives the ARI from its neighboring network, selects and aggregates appropriate candidates according to its policy for forwarding, and sends them to other neighboring networks.

If a name is declared to be delegable in its ARI, any third-party can carry out delegated registration of that name. The registrant provides Delegated Registration Information (DRI), which is a tuple of a delegable name and its locators, to its upstream router for the delegated registration. Different from authoritative registration, DRI is usually not submitted to DRS and thus is not disseminated globally. Its propagation depends on the policy of service provider. That is, the accessible scope of delegated registration is limited, which not only preserves the scalability of global registration table but also prevents malicious DRI polluting globally. This unique strategy with ARI and DRI in DSINA is analogous to the caching scheme with stable storage (CDN) and temporary caching (proxy) used in the current Internet.

D. Access

In DSINA, client end-points issue access messages to access desired content or service. An access message always includes a message header that carries an DSINA name specifying the content or service to be accessed as well as other information necessary for the message being forwarded in the network. It can also optionally contain access data which provides information to be processed at the content or service end-point. For example, to access private data on remote file server, the client should provide the authentication information of its account on the server in the access data.

One of the most distinctive differences between access messages in DSINA and requests in other network architectures is that access data can also be used to upload user-generated content to online services. For instance, a client can send an access message to a video publishing service, embracing the whole video clip as the access data in the message. This design avoids the additional round-trip communication to trigger a request from the service end-point to the client end-point in data uploading which is necessary in many other information-centric networks.
E. Result

Result messages are responses from content or service end-points to the access messages in DSINA. Similar to access messages, a result message includes a message header describing which access request it responds to, and optionally result data that provides additional information for the client end-points. Generally, if an access message requests for some piece of content, the result data provide the piece of content, and if the access message requests to execute some service operation, the result data provide the status of the executed operation.

Because result messages are delivered to client end-points, rather than names, locators of client end-points, i.e., IP addresses, are used in forwarding the messages. This saves the cost of route-by-name system from forwarding both access and result messages, and is expected to enhance the scalability of the architecture.

V. DISCUSSIONS

This section will briefly discuss applications, transport protocol and security concerns of DSINA.

A. Applications

We present several typical applications of information-centric networks. DSINA may implement all these applications with its naming system and register-access-result model.

1) Content distribution: Efficient content distribution is one of the most important functions of information-centric networks. DSINA achieves this through allowing delegated registration from clients that have finished downloading a piece of content. As shown in the left side of Fig. 1, when the DSINA router receives an access message from client end-point B, it forwards the message to content end-point J according to the corresponding ARI. J serves the requesting client using result messages. After B has received the content, it can register itself to its upstream router if ARI of the content is registered. Once the delegated registration is carried out successfully, B becomes another content end-point and can serve other requesting client end-point in the same edge network, i.e., A, in turn.

2) User-generated content upload: DSINA supports user-generated content upload to cloud services without additional round-trips. Cloud services provide computation, data and other resources without requiring end users to know the location of the infrastructure. A typical deployment of cloud service is usually composed by a series of server clusters located at different places on the Internet. In DSINA, as shown by the solid arrow in the middle of Fig. 1, client end-point D sends its data to the name registered by service end-point K using access messages directly, and routers forward such access messages according to ARI.

3) Notification push: Notification push is a typical application of publish-subscribe (pub/sub) system, where clients subscribe to interested information and publishers send messages without the knowledge of clients. As shown in the right of Fig. 1, in order to realize notification push, the publisher first performs an authoritative registration on a specific name. The name is specified as allowing delegated registration and forwarding to all in its ARI. Client end-points C and E that have interest in such information then perform delegated registration to their upstream routers to become subscribers. When there is a notification message to send, the service end-point L sends it in an access message. Routers receiving such a message duplicate and forward it to the corresponding ports according to the DRI it has received. Bandwidth is saved as the message is duplicated on routers when it is necessary.

B. Transport Protocol

DSINA adopts Improved Content-Oriented Transport Protocol (ICOL4), which is ameliorated to meet the requirements of DSINA from our previously developed Content-Oriented Transport Protocol (COL4) [10], as its transport protocol. Identical with COL4, ICOL4 is designed to be compatible with the current Internet Protocol (IP), with the ability to be incrementally implemented and deployed. All operations in this protocol are content-oriented and connection-less. Besides, the protocol includes the same congestion control mechanism as COL4 to be fair with the existing transport protocols and thus to enable traffic engineering. Due to the space limitation, we only focus on the partition handling of the protocol and leave the detail to the literature [10].

In the existing content-oriented designs, only content retrieval is supported so that it is fine to treat transport of content partition as independent procedures. However, because user-generated content is supported in DSINA, it is problematic if different partitions of the same piece of content forwarded to different service end-points. Therefore, the new challenge of supporting content partition in DSINA is that routers have to guarantee partitioned messages for the same access request be forwarded to the same content or service end-point, while at the same time retain the information-centric advantage that the forwarding be independent of addresses and automatically load-balanced. ICOL4 solves this problem using the access ID carried in access messages. A client end-point always send partitioned messages for the same access request with the same (name, access ID) tuple, and a router should always forward access messages with the same (name, access ID) tuple to the same destination. In this way, ICOL4 always transfer a series of partitioned access messages to the same content or service end-points.

C. Security Concerns

The basic concept of DSINA’s security follows that of the existing content-oriented design, where content security should be guaranteed by the content itself. That is to say, anyone in the network is able to verify the binding of name and data with the signature information transferred along with them, which is usually supposed to be implemented by the simple public key infrastructure (SPKI) [11]. However, the validation of signed data at network devices is not effective in DSINA because DSINA allows client end-point to send user-generated data with names registered by service providers. In this case,
there is a mismatch between the owner of the name (service provider) and the owner of the data (end user).

First, this may be considered a necessary trade-off for allowing user-generated content pushing in information-centric network. The security threats, such as denial-of-service attack, can be taken care of by other mechanisms. We also argue that such threats cannot be completely eliminated even without the content uploading functions.

Second, although there is problem using SPKI in DSINA, adopting certificate authorities (CA) approach of public-key infrastructure [12] resolves the validation problem without introducing much additional complexity. In brief, the service providers in DSINA play the role of CA, signing and publishing the public keys bound to users they provide services, so that DSINA routers can verify that an access message with data is sent by a valid user of the designated service name in the message header.

VI. Conclusion

In this article, we have proposed a Deployable and Scalable Information-Centric Network Architecture (DSINA), a novel architecture incorporating route-by-name system into the current Internet infrastructure. DSINA not only provides fresh information-centric functionalities, but also enhances the deployability and scalability of the architecture. In DSINA, both DSINA name information and traditional host location are handled by network devices. With the register-access-result model, DSINA can handle content retrieval as well as user-generated content uploading, notification pushing and other applications. The transport of DSINA messages is implemented by Improved Content-Oriented Transport Protocol (ICOL4), which is improved from its previous version in message header layout and fragmentation handling.

REFERENCES