Journal of Network and Computer Applications 52 (2015) 1–10

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Information centric network: Research challenges and opportunities

Athanasios V. Vasilakos [a,*], Zhe Li [b], Gwendal Simon [b], Wei You [c]

[a] Lulea University of Technology, Computer Science Department, Sweden
[b] Institut Mine Telecom – Telecom Bretagne, France
[c] Orange, France

ARTICLE INFO

Article history:
Received 15 March 2014
Received in revised form
9 December 2014
Accepted 17 February 2015
Available online 26 February 2015

Keywords:
Information centric networks
CDN

ABSTRACT

For more than a decade, the inherent drawbacks of current Internet have been calling for its revolutionary designs. The end-to-end model, which was designed for special data transmission in the early age of Internet, is causing troubles everywhere in nowadays content based web services. Consequently, Information Centric Network (ICN) is proposed to solve these problems. As the most permanent clean-slate approach for next generation Internet, ICN has attracted much attention from network researchers in the passed few years. This survey focuses on the current progress of the research work in ICN. It investigates various key aspects such as naming and routing schemes, in-network caching policies, *etc.*, and highlights the benefit of implementing ICN, open research issues and new interests in this domain.

Contents

* Corresponding author.
E-mail addresses: th.vasilakos@gmail.com (A.V. Vasilakos), zhe.li@telecom-bretagne.eu (Z. Li), gwendal.simon@telecom-bretagne.eu (G. Simon), wei.you@orange.com (W. You).

http://dx.doi.org/10.1016/j.jnca.2015.02.001
1084-8045/

1. Introduction

Since the Internet was designed in 60s–70s, it has played a more and more important role in people's life. From the beginning, the Internet runs on top of the protocol stack of TCP/IP with the intention of connection a few of machines. The Internet paradigm, which is deployed till now, is a host-host based model. All the Internet information exchanges are realized by establishing the communication channels. This host-centric Internet has perfectly matched the early Internet usage, which is not that complicated. Basically the Internet applications or protocols are all end-to-end communications like the web surfing, instance massage chat, sending e-mail or FTP file download, *etc*.

The science and technology never stop from evolving. For example, the networking link layer is no longer limited at the xDSL technologies. The Internet uses various technologies from WiFi, FTTH, Satellite, to mobile 3G and 4G for information exchanges. End-user terminals which support the Internet experience cover from the PC, laptop, to the smartphone, tablette, set-top box, *etc*. More importantly, the Internet usage is changing as well. It is switching from the host-centric to a content-oriented model. Peer-to-peer applications (P2P) (http://en.wikipedia.org/wiki/Peer-to-peer), Content-Delivery Networking (CDN) (Vakali and Pallis, 2003) are developed for improving the content delivery. HTTP video is already the major contribution of the networking traffic. Flickr, Instagram are more and more popular because people prefer more and more share their daily life on-line. And E-commerce, social-networks, Video-on-Demand, *etc*., all the things that people care about is no longer "where" it can get the information which they are interested in, but "what" the information actually are. In order to follow these evolutions, Internet becomes more and more complex. Security, NAT, DNS, multicast, multi-homing, mobility, CDN, security for multi-homing (Migault et al., 2012), security for mobility, *etc*., more and more patches or overlay are added on the current Internet protocol stack. From that the host-based TCP/IP Internet is becoming too heavy to offer the best performance to the end-users.

Facing these shortcomings, many research communities are motivated to develop an Information-Centric Networking paradigm (ICN). The ICN aims to shift the current complex Internet model to a simple and generic one. The basic networking unit is no longer the identified node (*servers, routers, terminals*). The ICN networking activities are all based on the named content objectives. ICN is receiver-driven networking model, where end-users only express their interests for a given content, the entire network is in charge of routing the requests based only on the content names towards the best content containers and delivering the contents through the reverse paths to the end-users. The ICN aims to build the features directly into the networking design. It natively includes the features as location-independent naming, name-based routing, in-networking caching, native multicast, self-secured content, *etc*.

Although ICN enters now into the main stream of networking research, it is still in its early stage. In the past few years many projects have been carried on in order to propose a concrete ICN solution to deploy it in reality. In this survey we intend to give a general presentation of different ICN features with the goal of raising an in-depth discussion of this novel Internet paradigm. Our study is arranged according to the common components in various ICN designs such as naming and routing schemes, in-network caching technique and security issues. These components are presented in Sections 2, 3 and 4 respectively. In the discussion for each component, we briefly introduce the design principles raised by various research projects, and address prospective opening issues. Then, we investigate in Section 5 other potential benefits brought by ICN in several aspects such as cloud computing environment and green IT. Finally, we summarize the study and research challenges in Section 6.

Different projects use distinct notations to indicate their design choices and features. For example, DONA uses *Data-Oriented* instead of information-centric, CCN is the abbreviation of *Content-Centric Network*. Therefore, in our presentation, the terms as information, content and data are used interchangeably.

- In CCN, the unit of transmitted content in the network is called *Data*, while in NetInf it is denoted as *Named Data Object*.
- Names for request routing devices are also diverse. PSIRP routing scheme consists of four key components: *RendzVous Nodes, Topology Nodes, Branching Nodes* and *Forwarding Nodes*. DONA leverages the *Resolution Handles* to discovery requested content. *Content Router* is implemented by CCN to realize their longest prefix matching routing scheme, and NetInf routing is achieved by a *multi-level DHT* mechanism.
- While the ubiquitous in-network caching is integrated as a function of Content Router in CCN, other projects usually depends on dedicated modules as *Storage Engine* in NetInf and RendezVous Nodes in PSIRP.

These distinct design patterns will be detailed in the following sections.

2. Naming and routing

The fundamental concept of the ICN is to switch the address based Internet architecture to a named-content based one. The naming and the named-based routing scheme is the core of all the concrete ICN projects. We will present firstly in this section the naming and routing issues of the ICN networking.

2.1. Overview

The content retrieving in ICN can be mainly divided into two parts: the content discovery and the content delivery. The content discovery is related to how a content is named, how it is published and how an ICN node addresses it. The content delivery defines the ICN routing protocol which is about how a content provider propagate its contents into the network, how an ICN router routes the end-users' interests to the best content sources and how an ICN router deliver the contents to the end-users. In this section we will globally present the ICN naming and routing aspect.

The content name is the only identifier of each content object, which permits either the end-user or the intermediate networking unit locates the best content holder. The content name usually is a globally unique identifier, but the unique named content can sojourn in different containers, for example the origin content servers, the CDN repositories or the on-path caches. In the following we will try to summarize the different naming issues of the ICN domain.

(a) *The properties of the ICN naming*: Of course the fundamental role of the unique name is to identify the different content, but it also include other properties:

- *Globally unique*: In ICN, each networking unit is identified by a content name. Thus the content name should be globally unique in order to arrive at a global level routing.
- *Location independent*: The IP address is highly related to the geography location. When the location is changed, the IP address is changed. The ICN name is independent from the physical location. A content is named when it is created, no matter where or from who. A named content can be re-published, replicated everywhere, but the name does not changed.
- *Security intergraded*: The security was not designed in the first version of IP network. As long as the Internet evolution, the security service is added into the IP prototype, *e.g. IPsec*. In ICN,

the security is directly guaranteed into the content name. The information objects are self-certificated by their names, which means each content name is signed by its legal publisher and it is binded with the related content. Only the authorized receivers can decrypt the content name and the content data.

- *Self-defined*: Unlike the IP addresses which are attributed by a centralized organization, the ICN name can be created by the content providers themselves, only follows the defined naming rules. However, the self-defined names will introduce a huge number of content identifiers in the network.

(b) *Hierarchical or flat name structure*: There exists mainly two categories of ICN naming structures: the hierarchical names and the flat names. Each naming structure has the advantages. The hierarchical structure is similar as the IP CIDR (Fuller et al., 1993). The IP addresses can be aggregated into the prefixes and perform the longest match or shortest match. The hierarchical names, for example the *CCN* naming (Jacobson et al., 2009), are structured for aggregation and extending. The names are uniqueness for routing but are human-readable for the end-users. The flat structure is not suitable for aggregation but it is easy to perform the DHT-like lookup methods (Stoica et al., 2001).

(c) *Metadatas*: Besides the unique names for identifying the content objects, ICN includes also the additional metadatas (Duval et al., 2002) in the names for describing the contents. For example a photo which is offered by *Flickr* can be named in a hierarchical structure as ccnx:/flickr.com/group_xxx/photo1/. It can also contain the tags as the metadata for example the author, the subject, the camera model or the place where the photo was taken. The metadata is important in ICN. First of all, the additional metadata can better describe the content. The content name is unique but sometimes the user may not know the exact name of each content. Thus the metadata is here for helping the user find out the right content for example by using the search engine with some keywords. The metadatas can also establish the association between similar content objects. For example a user who requests this photo may be also interested in the other photos that are token by the same camera model.

(d) *Named based routing or DNS-like resolution*: The ICN routing can be realized in two manners: the undirected naming resolution service and the direct name based routing. The naming resolution requires one or several centralized servers (*e.g. RendezVous points, register servers, trigger points, etc.*) in the networking topology. The content publications are collected in these servers, which have a global view of all the published content objects and the networking topology. When an ICN router wants to forward a request message, the routing path is calculated in the centralized server by implementing the IS-IS (Callon, 1990) or OSPF (Moy, 1998; Wang et al., 2012) like Shortest Path protocol. Contrarily, the name based routing is directly performed in the ICN routers. Each router has a local forwarding information base which is filled by the content publication messages. The request forwarding paths are thus calculated in the local routers followed their own forwarding strategies.

2.2. Existing solutions

The named content and content name-based routing are firstly introduced in TRIAD project (Cheriton and Gritter, 2000). After that more and more researchers show their interests into this new Internet paradigm and proposed several different ICN projects. In the following subsection we will give a brief view of some advanced ICN research project and their naming and routing solutions.

2.2.1. Content-centric networking (CCN)

The content-centric networking (Jacobson et al., 2009) and the Named Data Networking project (Zhang et al., 2010) are proposed by Palo Alto Research Center (PARC). It is one of the most attractive ICN research project. The ultimate objective of CCN is to replace the IP based Internet with a named content based model.

The content name in CCN is designed as a hierarchical structure (Fig. 1). The hierarchical name is organized as a *prefix-suffix* order. ccnx:/parc.org/video/widget1/version2/chunk2 is an example of a CCN content name. All the content provided by *parc* can share the same ccnx:/parc.org/ prefix. The tree-like structure can make the CCN name support the aggregations as the IP address aggregation. A same information object may have several different versions and a single content can be divided into multiple small segments (*chunks*) in order to adapt the transport layer. Thus each CCN name is ended by the version and chunk information which can simplify the content discovery. The entire name is signed with a SHA256 digital signature of the content provider. Thus only the authorized receivers can decrypt the digital data.

In CCN, the information exchange is realized with two types of packet: the *Interest* and *Data*. The Interests are used to express which content the end-users want to retrieve and the Datas are the response packets which contain the real binary contents. The Interest routing is based on the ContentName. Each CCN node has an element so-called Forwarding Information Base (FIB). The CCN FIB (Fig. 2) is similar as the IP FIB. It contains the Interest routing information. When a content provider has some contents to publish into the network, it spreads the advertisements into the network. These advertisements will fill the CCN FIB together with

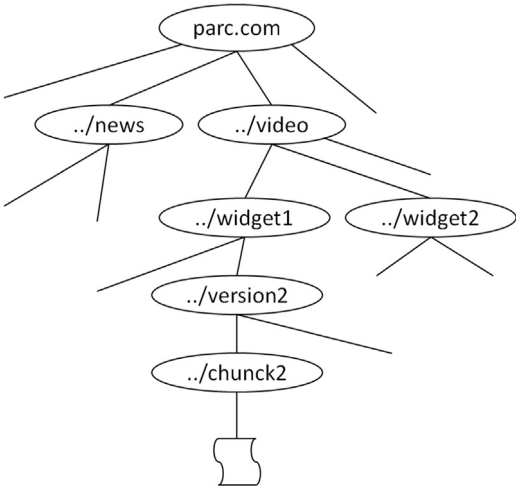

Fig. 1. The naming of content-centric network.

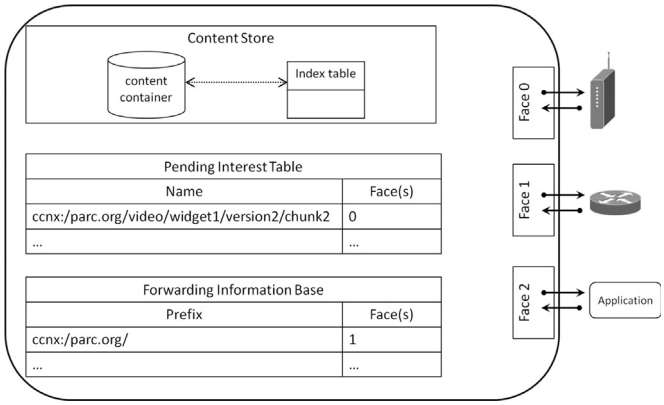

Fig. 2. The node structure of content-centric network.

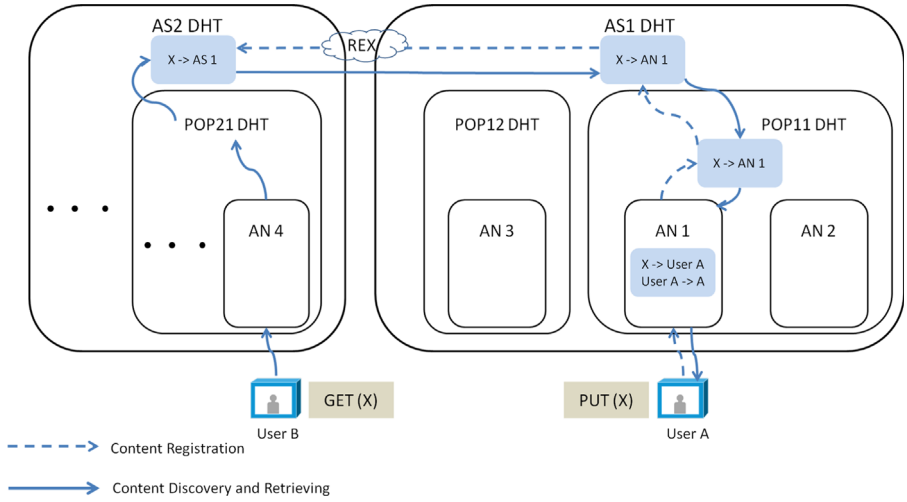

Fig. 3. The routing scheme of NetInf.

the incoming faces as the Interest outgoing faces. Each CCN node can aggregate the FIB entries on the prefix as the case might be. When the CCN node wants to route an Interest request, it will look the Interest ContentName up in the FIB table. And the Interest will be sent out through the faces of the longest match FIB entry. The CCN routing supports the multicast by default, which means that one FIB entry may contain more than one outgoing face. This is because one content can be provided by different providers, for example from the origin content providers, from a CDN repository or from a ISP border-cache.

In CCN, the Data packets are not routed. Each CCN node contains another component which is called Pending-Interest Table (Fig. 2). When a CCN node receives an Interest, if it locally does not have the right content, it should forward the Interest out according to its FIB. Meanwhile, it appends also the Interest name (the ContentName) in its PIT together with the incoming face identifier of the Interest like a "breadcrumb". After several forwarding hops, the Interest arrives at one content container which holds the required content. The container will reply the Data packet and the Data packet will follow the reverse path of the Interest forwarding until it is returned to the origin asker. The revers path forwarding is realized as every time the Data is back to a CCN node, the node will check the Data name in its PIT. If it finds a matched PIT entry, which means this node did received the Interest for this content, the Data will then sent out through the face(s) of the matched entry.

2.2.2. Named of information (NetInf)

NetInf (Dannewitz, 2009; Dannewitz et al., 2010a) is a part of the European FP7 project 4WARD (4WARD, 2010). The NetInf proposes an ICN networking architecture which is based on the content register scheme.

The NetInf applies the *Information Object (IO)* and *Bit-level Object (BO)* to differentiate the content identifiers and the real binary content in a *Named Data Object* (NDO). The naming of NetInf is included in the IOs. The NetInf IO contains three parts: the content-identifier, the metadata and the security attributes. The NetInf name uses a flat structure as *P:L*, which contains and separates the identifier of the content provider and the content self. The *P* is the content provider identifier that is usually the hash of the public key of the provider. The *L* is the label of the content chosen by the content provider, it is usually the hash of the content itself. The NetInf routing is a multi-level DHT (MDHT) based registration method which includes a name resolution service (Fig. 3). The MDHT structure is a three level topology: the Access Node level (AN), the Point of Presence level (POP) and the Autonomous System level (AS), from the lower to the upper. Each level applies its own DHT algorithm and any nodes at any levels can join in a cross-level DHT—the MDHT.

The routing in NetInf has two processes: the content registration and the content discovery. When a content provider wants to register a content, it will firstly map the content to an access node by the AN level DHT algorithm. The access node has two information bases. One is to tell which content can be found at which host, another one is to memorize the address or any other access information for reaching which host. After the AN level registration, the content will be registered in the MDHT, which means the content name and the attached access node are registered in both the local DHTs of the POP and the AS level. When an client want to retrieve a content, it will first try to get it in DHTs follows the order of AN, POP and then AS. If it cannot find the content even in the AS level, it will look the content name in a naming resolution service which is named REX (Resolution Exchange). The REX is an independent entity that runs at the AS level. The mappings generated by the REX are cached in the DHT of each AS.

2.2.3. Data oriented network architecture (DONA)

The DONA (Koponen et al., 2007) project aims to define a clean-slate ICN network. The core of the routing in DONA is a hierarchical naming resolution system with a flat content naming.

The naming issue in DONA is similar as the naming of NetInf. DONA uses also a flat *P:L* naming structure. The part *P* is the hash of the public key of the content owner (the Principle concept in DONA). And the *L* is the owner assigned content label. The content owners have the responsibility of ensuring the entire *P:L* name is globally unique.

However the routing in DONA is different from the NetInf routing. DONA applies a hierarchical content name resolution system (Fig. 4), the Resolution Handles (RHs). Each RH node has a information base which contains three tuples, the content name *P:L*, the *next hop* and the *distance*. The *next hop* is from where the node receive the content name advertisement. The DONA routing contains content *FIND* and contain *REGISTER* two processes. Both of the two processes are directly based on the flat content name. When a RH receive a *REGISTER* message, it will add the ⟨P:L, next hop, distance⟩ into its register table for a new arrival message, or update the next and distance for an existing entry if the new arrival message has a shorter distance. Then the RH will forward

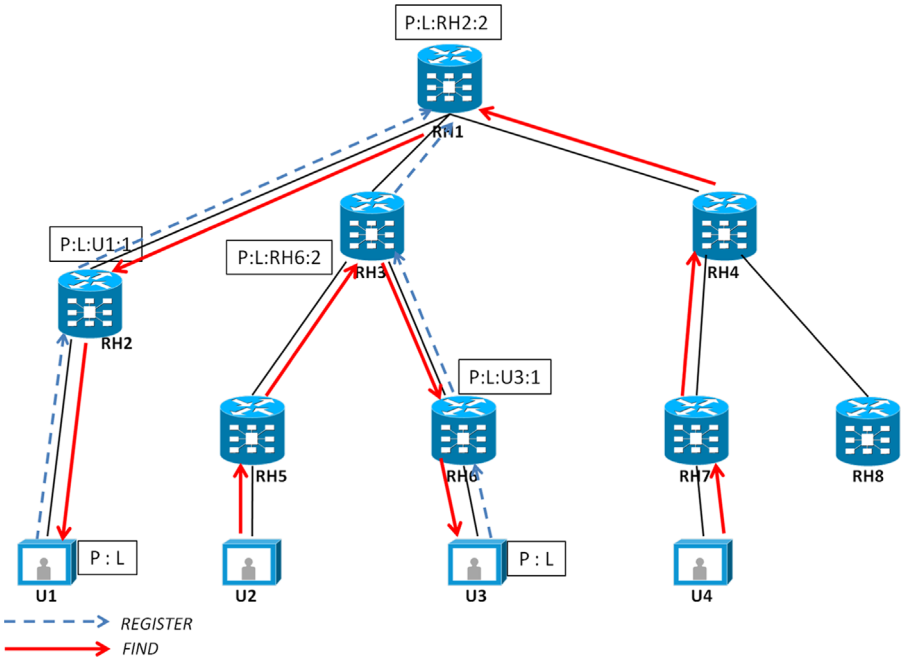

Fig. 4. The routing scheme of DONA.

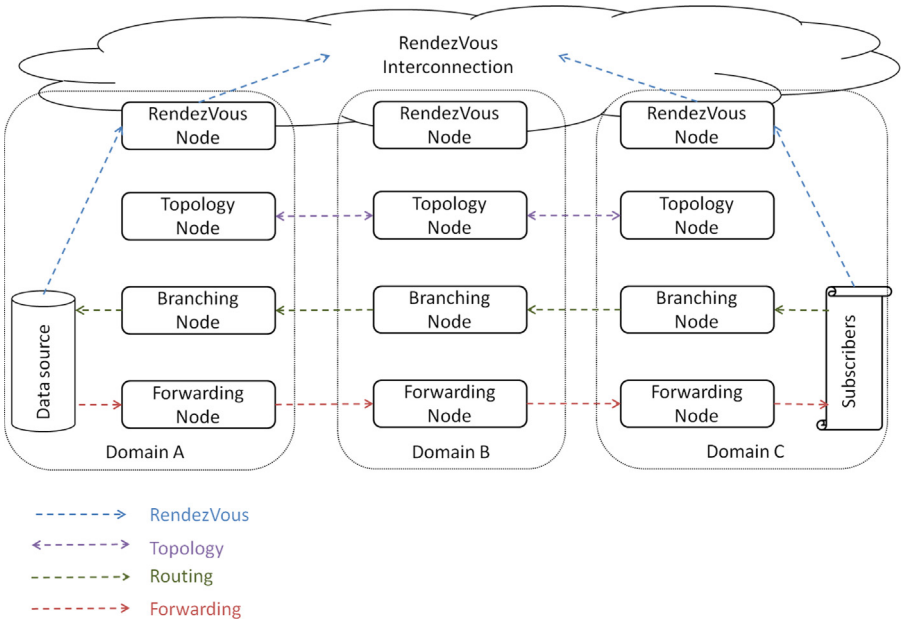

Fig. 5. The routing scheme of PSIRP.

this message to its parent RH(s). At last the content registration will end at the highest root RH(s). When a RH receives a *FIND* message, it will look the content name in its local register table. If it finds a matched entry, the *FIND* message will be forwarded through the *next hop* of the matched entry. Otherwise, the RH will transfer the *FIND* message to its parent RH(s). As the *FIND* message forwarding, each RH which is on the path appends the *FIND* locally, hence once the *FIND* arrives at the closest content container, the content object will be returned via the reverse path of the *FIND* forwarding.

2.2.4. Publish subscriber Internet routing paradigm (PSIRP)

PSIRP (Lagutin et al., 2012) is an European FP7 project which started in 2008 and ended at 2010. PSIRP proposed a clean slate ICN architecture which is based on a publisher-subscribe solution. PSIRP applied the same *P:L* naming structure as the DONA and NetInf. The content name is referred as *Resource Identifiers* (*RIds*). The PSIRP networking includes a basis concept which is named *Scopes*, which is identified with *Scope Identifiers* (*SIds*). The Scopes control the characteristics of a content, such as access right, authorizations, availability, reachability, replication, persistence and the upstream resources. Both of the content publication (*publish*) and the content request (*subscribe*) of a content are based on a pair of composition of ⟨SId, RId⟩.

The PSIRP routing scheme includes four important units: *RendezVous Nodes (RN)*, *Topology Nodes (TN)*, *Branching Nodes (BN)* and *Forwarding Nodes (FN)*. The entire PSIRP networking is divided into *Domains*, which is similar as the Autonomous System of the current Internet (Fig. 5). Each domain has one RN, one TN,

one BN and several FN. The RN of each domain is in charge of the matching between the content publishers and subscribers, the locating of the content publications and the scopes. Every individual RN can have its own name resolution system. All the RNs of every domain are interconnected with DHT into a global Rendez-Vous Interconnection (RI) which make the scopes of each domain are globally reachable. The TN is in charge of managing the intra-domain networking topology and load balancing. It also exchange the path vector information with the other inter-domain TNs. The BN builds up a routing map for routing the subscriber interests toward the inter-domain or intra-domain content containers by using the topology which is maintained by the TN. Finally the role of the FNs is to use a Bloom filter based forwarding implementation to realize the content forwarding from the content container to the subscribers. The Bloom filter which is named Forwarding Identifier (FId) is accumulated during the subscription delivery.

To summarize up, in PSIRP a subscriber expresses its subscription of a content to the local RN of its domain to get the content container location. The BN uses the networking topology which is obtained by the TN to forward the subscription to the content container. The subscription packet accumulates the return path into the Bloom filter and constructs the FId. At last the FNs use the FId to return the required content to the subscriber.

3. In-network caching

3.1. Motivations

One of the most remarkable characteristics that differs ICN from the current Internet is the in-network caching mechanism. While the research about content caching has flourished since the early age of web, the in-network caching mechanism further reduces the response delay by embedding cache storage deep into the network. Instead of leveraging the storage resource at the edge of network as P2P systems, or standalone web cache proxies, ICN enriches various network equipments (*e.g.*, routers, gateways) with caching capability. This widespread caching significantly improves the content searching efficiency and alleviates the traffic load on transit links between content provider and ISPs.

3.2. Existing solutions

Various ICN designs consider the in-network caching as an intrinsic and ubiquitous part of the network structure.

The in-network caching in NetInf is achieved by two different models that can coexist in the system: the *network-based storage model* and the *network-managed storage model*. The former model supposes that network operators have the total control of the storage resources since they integrate storage resources within network nodes, or deploy dedicated storage servers in the network considering certain criteria as resource dimensioning and performance targets. The latter one leverages the storage space at the user side. A user device contributes a portion of its storage capacity to the network when it is on-line. The network nodes that connect with on-line users manage the portions of donated storage and use them as the storage system under the operator's control. Accordingly, there are two approaches to retrieve those cached contents. Firstly, the required content can be found in the caching node on the path to the content source by cache-aware transport protocol. The content source could be the origin server of the content, or the location hosting a copy of the content. This location is registered in the *Storage Engine* used by NetInf to handle storage requests from user applications and manage the long term memory of the network. In the second approach, the cached object is retrieved directly by querying the *name resolution system* since either the location of the object is registered there, or it can be found by local search (*e.g.,* broadcast).

CCN protocol takes advantages of its URL alike hierarchical content name and an multi-cast routing mechanism to forward user's request to multiple sources of the content. The source could be the original provider of the content, or the users who are willing to share their local copies of it. Any network nodes along the path from the requester to the source holding the corresponding content can directly satisfy the end-user and consume the request. At the meantime, the node that does not cache it can decide to store the content passing through according to a certain policy. Since the copyright check and the authentication of the content are accomplished at the application level, network operator does not need to implement specific function to manage the storage space at user side and authorize the publication of the content from them. Because of the same reason, CCN protocol deals with the the cache storage offered by operator and contributed by user in the same manner. The CCN name-based routing is simple and efficient enough to retrieve the cached content.

In PSIRP, a multi-cast forwarding tree is established for data distribution(Katsaros et al., 2010). The in-network caching is limited to the scope of the RN point for the identifier associated with an content object. In other words, caches are located at the leaves of the multi-cast trees. Multiple locations close to the users are allowed to cache the same content. The multi-cast forwarding state established during the tree creation is used in the cache discovery process. Once caches are created, messages are sent by the leaf nodes towards the RN point to update the caching state. When a user requires content, the request will be treated by each intermediary node from the user to the RN point. Any node caches the content can send back the content directly. If one node finds the content in the caching state of its descenders, it will perform a DFS search for the content in the sub-tree of which the node is the root. If the content is not cached in the distribution tree, it will be fetched from the origin server in the scope. Each node refreshes its cache according to a certain replacement policy (*e.g.,* LRU, LRU).

3.3. Comparisons

In most of the ICN architectures, dedicated entities are necessary to manage the cache devices and trace the location of cached object. While the total control of the cache storage facilitates the optimization of caching efficiency, it complicates the redirection process of users' request. On the contrary, CCN Content Store (CS) that integrated into every network node and the hierarchical name structure allows network operator to get rid of specific devices for cache management. Due to the simplicity of CCN in-network caching and its high efficiency, it draws a great attention from research community.

3.4. Open questions and research directions

Although in-network caching has drastically improved the performance of ICN, most of the ICN designs provide only basic instructions on cache management, which opens a large research field. The contributions in this area mainly concentrate on two problems: the cache management and the resource discovery.

- Usually, cache management deals with the cache *decision* and *replacement* policies. The former decides which content should be cached when a new data object is received, and the latter selects the content should be evicted when the cache is full. Various studies have conducted advanced cache decision protocols (Borst et al., 2010; Dai et al., 2012; Li and Simon, 2011). While some papers argue that sophisticated cooperative cache may introduce only marginal benefit for serving web content

(Ghodsi et al., 2011), the booming video streaming service over current Internet may change the situation. For example, the authors in Borst et al. (2010) propose an optimal content placement policy for an IPTV system in a hierarchical tree-like topology. For the same IPTV service, Dai et al. (2012) realize the cache cooperation by jointly considering the content placement and dynamic request routing. In Li and Simon (2011), the authors design a cooperative in-network caching protocol for catch-up TV service in CCN. On the other side, multiple analytical tools are proposed to study the performance of cache replacement policies. The authors of Psaras et al. (2011) developed a mathematical model for a single content router (CR) based on continuous time Markov-chain. They showed that the performance of an entire multi-cache system can be approximated by their single cache model. Rosensweig et al. (2010) presented a model that approximates miss ratios for any multi-cache topology when the caching policy is basic LRU. In Li et al. (2012), the authors extend the work in Rosensweig et al. (2010), and develop an analytical model to predict the caching performance of various replacement policies in an in-network caching system. Based on the approximation, the authors of Li et al. (2012) further propose the multi-policy cache management where the replacement policy on each cache should be differentiated according to its location. Usually, these models analyze the caching network with different topologies, cache capacities, *etc.* However, the initial state of the system is often neglected. Opposite to the misunderstanding that the steady state of the caching system is independent of the initial state, authors of Rosensweig et al. (2013) demonstrate that distinct content placed initially at the caches will lead to different steady, long term behavior.

- Along the same time, the research work on cached resource discovery is also productive (Thaler and Ravishankar, 1998; Chiocchetti et al., 2012). In Thaler and Ravishankar (1998), the authors leverage a random hashing function to bind a content to one of the servers storing a replica, so that a request can be forwarded to the resource according to the name-based mapping. The authors of Chiocchetti et al. (2012) compare the exploitation and exploration approaches for request forwarding in intra-domain ICN. Their primary results reveal that the user delivery performance can benefit from the exploration approach since it enables the user to find close content replicas. Moreover, a chunk-level exploration is more effective than an object level request broadcast. In the same work, they also design a hybrid forwarding solution that mixed the exploitation and exploration. The hybrid strategy out performs the two primitive approaches in terms of reducing stored routing information and the efficiency of resource discovery.

Besides those two major directions in the optimization of ICN in-network caching performance, another piste of research is to examine its feasibility in real world ICN implementation. Following the study in Perino and Varvello (2011), CCN is realizable in an ISP network scope. How to upgrade the physical equipments so that ICN in-network caching can be achieved in the transit network is also an attractive research topic.

4. Security issues

4.1. Challenges

Unlike nowadays host-centric security (*e.g.,* transport layer security (TLS), authenticated server), ICN requires location independent security mechanism to enable ubiquitous in-network caching system. To this end, the next generation security model should provide an information oriented data integrity and authenticity check mechanism. Moreover, the model should get rid of the trusted third party (*e.g.,* software vendor) that compiles the trusted authorities in the current data integrity checking process. While ICN is intrinsically immune to the host-oriented attack because of the content based communication, solutions for denial-of- service (DoF) attack is worth to be addressed.

4.2. Existing solutions

In order to realize the content centric security model, ICN protocol usually integrates its proper security design as an inseparable part from its architecture. As it is in PSIRP, the system utilizes elliptic curve cryptography (ECC) (Miller, 1985) to guarantee the data availability and protect the network from DoF attacks. Concretely, a 160-bit ECC public key is involved into each packet so that the packet level authentication using per packet cryptographic signatures allows the integrity, authenticity and accountability on the network layer (Lagutin et al., 2012). As previously mentioned, host-oriented attacks are avoided inherently by zFilters (a scalable and fast forwarding mechanism proposed in PSIRP) since link identifiers are not globally known. The DoF attack can be further prevented by the zFormation (Rothenberg et al., 2009) mechanism. The scalable security mechanism is applied to various components of PSIRP such as the rendezvous system, routing of subscriptions, and the actual payload traffic so as to protect the whole network.

The common data format in NetInf is illustrated in Fig. 6. The NetInf name of a named data object (NDO) contains a hash algorithm and the corresponding hash value of the object's content body. The named information (ni) is registered in a URI architecture to foster application development and simplify migration. The functionality of this NetInf name is first to explicitly identify NDOs, then to enable name-data integrity and other advanced security features, and finally to perform as a key for name resolution and routing mechanisms. The integrity is ensured by verifying that the received data corresponds to the requested name, assuming that the correct name is obtained beforehand. Various accessories (*e.g.,* authority field, query string) can be added into the name with the aim of accessing the NDO for routing requests or assisting scalable name resolution service (NRS). Furthermore, the ni URL scheme can also provide the integrity check for dynamically changing data by means of including a hash of a public key in the ni URL rather than the hash of the NDO. The details about how NetInf supports additional security features as owner pseudonymity and owner identification are elucidated in Dannewitz et al. (2010b).

The CCN content-based security is achieved by authenticating *all* content with digital signatures, and encrypting private content (Jacobson et al., 2009). Each CCN data packet is validated by a self-

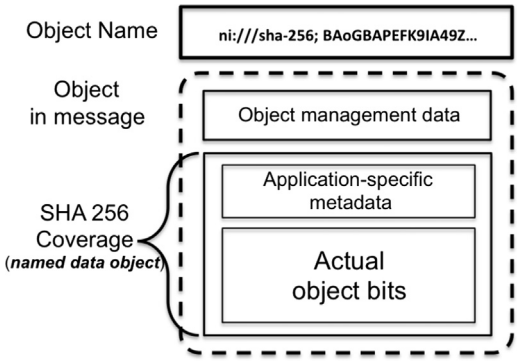

Fig. 6. Common format of NetInf message.

contained signature covering the name, the content, and a small amount of supporting data used to signature verification. Leveraging this per-packet signature scheme, CCN data becomes publicly authenticatable, which means not only the endpoints of the communication but also the nodes in the data forwarding path can verify that a name-content binding is signed by a particular key. The key can be obtained at a certain place indicated by a *key locator* included in the message. In terms of network security, the DoF attack is again the only focus of a malicious user. Two different ways to carry out the action are either hiding the legitimate content or preventing the delivery of the content by overwhelming it with massive spurious packets. To effectively defend the first case, users can put constraints on the publishers whose content can satisfy their requests. The second predicament is easily resolved by the *interest driven* communication scheme. No matter how many unsolicited data packets are produced, they will be eliminated immediately in the forwarding process.

4.3. Open questions and research directions

Although ICN is resistant to most of the traditional host-centric security problems, new architectures also yield concerns in several aspects as data privacy in caching network, security in mobile and virtual environment, *etc.* Various studies have been conducted center on the privacy issue in ICN (Lauinger et al., 2012a,b; Kim et al., 2012; Chaabane et al., 2013). In Lauinger et al. (2012a), the authors illustrate several attack scenarios where the malicious user takes advantage of in-network caching to investigate other users' behavior and launch attack. A simple example is that the attacker and the victim are the users of a same local cache device (*e.g.,* home gateway, DSLAM). The victim is supposed to be a unique user of a bank among his neighbors. By observing whether the pre-defined object of the bank's website is cached or not, the attacker can be aware of the time when the victim is operating his bank account. At the same time, the attacker may call the victim to tell him that the bank detected a security problem when the victim logged in, and let the victim reveal his password to fix the problem. In this way, the attacker can obtain the bank information of the victim. The solution to prevent this *request monitoring attack* is either to use one-time names for the content or to implement unpredictable caching policies. However, both of the two solutions could increase the complexity of data processing and degrade the network performance. Other caching related attack models as *object discovery attack and data flow cloning attack* are also depicted in Lauinger et al. (2012a). More detailed discussion about countermeasures approach against these cache monitoring attack can be found in Lauinger et al. (2012b).

The authors of Chaabane et al. (2013) extend the privacy issue generated by the in-network caching system to the overall design of the content message as content privacy, name privacy, signature privacy, anonymity, *etc.* For content privacy, more efficient encryption would be the de-facto solution. The problem of name privacy is usually provoked by the correlation between human-readable content name and the content itself. One of the potential solutions is to replace each component in the original hierarchical content name by the prefix generated by bloom filters. Signatures are powerful tools to ensure the integrity and authenticity. However, it is a double-blade sword since ordinary digital signatures may leak sensitive identity information about the signer. A couple of solutions, as ring signatures, group signatures and so on, is raised to enhance the security of signature.

While the privacy issue is a critical point in a relatively stable network environment, how to organize a virtual private network (VPN) in ICN is also a subject worth debating. Traditionally, the scope of a VPN includes the members of an enterprise's, institute or organization. But in the context of ICN, this scope can be expanded to a set of users sharing a social network or connecting to a dynamic ad hoc group. Although some primitive research works are presented in Ravindran et al. (2011), Kim et al. (2012) amd Lu et al. (2013), there is still large room to progress.

5. Other potential benefits

5.1. Motivations

As a panacea for content oriented Internet service, ICN offers potential solutions to various problems in the current location based Internet transmission. These fruits evolved by ICN can also benefit for *Cloud Computing* (a prominent technology that facilitates the business in IT resource sharing and the development of distributed applications) and *Green IT*.

5.2. ICN in cloud

Usually, the infrastructures of cloud computing provider are hosted by large data centers mainly due to the manage reasons. The management of data center networks based on the present end-to-end Internet requires a stable networking environment. However, ICN makes it possible to distributing cloud service objects across a mobile or a home networking environment. Moreover, ICN can ease many management related issues of today's cloud computing infrastructure such as permission control, load sharing, *etc.*

Since ICN can potentially reduce the complexity of cloud computing management, their conjunction has been conducted by several research works.

NetInf is coupled with cloud computing in the architecture proposed in Ohlman et al. (2009). In this architecture, NetInf is leveraged as a back-end of the upper layer cloud computing service. An API, which hides the dynamics of object locations and network topologies, runs as an interface between the cloud computing platform and under layer NetInf. One single name resolution and routing mechanism is used to reinforce the robustness of cloud computing service against object re-location or topology shifting of the underlying infrastructure network. Thus, NetInf successfully extends the cloud service into a dynamic networking environment. As the access control to information objects in NetInf is intrinsically achieved by cryptographic means, no virtualized storage and transport resources are needed to ensure the access rights. On the other side, virtualization of resource separation could be realized by using the advanced technique as Vnet (4WARD, 2010), which allows additionally the virtualization of wireless network resources. A novel object-to-object routing mechanism inspired by late locator construction is designed to adapt cloud computing service to a highly dynamic network topology.

A cloud computing platform is constructed above CCN in Tong et al. (2011). The Named Application Programming Interface (NAPI) is introduced to enable the interaction between CCN with the cloud computing platform. Various advantages yielded by combining CCN with cloud computing are addressed by the authors. For example, data availability is significantly improved since CCN uses universal unique data name, which allows the data flow across distinct cloud computing service providers. A bunch of malicious attacks to the data center network can be easily avoided thanks to the inherent security mechanism in CCN. Flexibility of the interface for developers can be enhanced by simply adding extra meaningful field in the named packet using NAPI. Due to the ubiquitous in-network caching in CCN and name based routing, the data recovery becomes extremely easy in the cloud over CCN. A novel universal sharing mechanism is proposed to expand the

sharing range of resources as storage, process capability, *etc*. This mechanism consists of two phases.

- In the *sharing announcement* stage, each client periodically announces its resources to the CR directly connects with it. The information is packed in a data packet with a name having special logical meaning, and then cached by the CR for further use.
- During the *capability sharing* phase, the cloud service provider send the interest packets to collect, and then process the resource information. Thereafter, the provider will disseminate the schedule of processing to the clients. The schedule includes the name of the resource so that the client will be able to retrieve the corresponding resource.

Since all the researches on using ICN to serve cloud computing are primary studies conducted from pure theoretically point of view, the most interesting future subject is to construct a real world cloud computing platform over an ICN infrastructure. Besides, the performance of ICN in supporting disparate cloud computing applications is also worth investigating.

5.3. Green ICN

Since ICN's in-network caching and content-oriented routing drastically diminish the data transmission distance, the transport energy consumption is reduced correspondingly. Various studies have addressed the energy benefit of ICN (Lee et al., 2011; Guan et al., 2011; Choi et al., 2012).

The authors of Lee et al. (2011) investigate the energy efficiency of several existing content dissemination architectures. They survey the energy consumption of various network devices used for content delivery and conduct a trace-based simulation. Their results reveal that the revolution from the host-oriented data transmission to the information-centric one can substantially improve energy efficiency of content dissemination. The benefit mainly comes from the reducing hop counts by serving content at in-network caching level.

In Guan et al. (2011), the authors focus on the benefit of CCN and dynamic optical bypass. For different implementation cases, energy consumption models are established based on the overhead of real network equipment and devices. The authors demonstrate that by optimizing the placement of content according to its popularity, CCN can yield a significant transport energy reduction. Comparing with dynamic optical bypass, their results indicate that CCN is more efficient in delivering popular content while the other performs better in serving less popular content.

As a following work of Guan et al. (2011), the authors argue in Choi et al. (2012) that the data transport consumption is not the only factor that impacts the overall energy efficiency in CCN. While the in-network caching saves the transport energy, the caching system itself may consume a considerable amount of energy. Therefore, more careful and in-depth estimation of CCN's energy efficiency is necessary. Inspired by this argument, the authors study the influence of various memory technologies on the overall energy efficiency. Moreover, they derive optimal cache locations in term of energy consumption via linear and non-linear programming models. Their numerical results indicate that sufficient caching capacity is a key point to realize green CCN.

All of those studies show that the in-network caching is the largest contributor in CCN's energy efficiency. Therefore, to design a caching protocol that can find the trade-off between energy consumption and service quality could be a long-term goal in the green CCN aspect. How to leverage the cooperative caching to achieve the energy efficiency could be a promising piste.

6. Conclusion

In this survey we have presented the new Information-Centric Networking paradigm that aims to switching the IP based Internet to a content information driven model. In the previous sections we presented the different aspects of the ICN properties and some existing solutions. As every new born element, the ICN cannot be successfully deployed all at once. Because many issues and challenges still remains to be addressed and tackled.

- Even the ICN is a hot research topic and there exist already many projects and short-term deployments, but those prototypes are all running as an overlay of the current IP Internet. How to deploy ICN in real word Internet is still a question. Should the deployment be restrained in the ISP, or could it be profitable if ICN is expanded to the network backbone? If the answer is positive, a clear business model that shows the incentive for each player in the game is necessary.
- In the real word implementation, the *Software-Defined Networking* (SDN) architecture is a potential approach to achieve ICN. By decoupling the physical network infrastructure and logical elements, SDN allows system administrators to quickly provision network configurations. Some preliminary studies have already addressed the feasibility of implementing ICN var SDN (Vahlenkamp et al., 2013; Salsano et al., 2013; Luo et al., 2014). The integration of SDN and ICN will enable the continuous evolution of ICN.
- In-network caching seems not to be appealing for some content providers since it may cause copyright problems or legal issues. For an ICN operator how to prevent the illegal propagation of certain content is not trivial. It is worth discussion if the combination of technical mechanism and new laws could help.
- As it is shown in the previous discussion, new data transmission mechanism in ICN invokes new security problems, especially in the aspect of users' privacy. Therefore, further investigation about privacy issues is necessary to nip an evil in the bud.
- Last but not least, facing to the exploring content in nowadays Internet, how to optimize various basic ICN architectures so as to guarantee their scalability and efficiency is not negligible.

But seeing the motivation and the advantages, we have confidence that one day the Internet will be constructed based on the ICN paradigm as a long-term deployment. That is also the reason that currently the ICN attracts much research attention from the ISP operators, Internet hardware vendors, Internet services providers and academical researchers.

References

4WARD, FP7-ICT-2007-1-216041-4WARD/D-4.5, 4WARD, Technical Report; June 2010.
Borst S, Gupta V, Walid A. Distributed caching algorithm for content distribution networks. In: IEEE INFOCOM; 2010.
Callon RW. Use of OSI IS-IS for routing in TCP/IP and dual environments, RFC Std. RFC1195; 1990.
Chaabane A, Cristofaro ED, Kafaar MA, Uzun E. Privacy in content-oriented networking: Threats and countermeasures. arxiv:1211.5183v2, 2013.
Cheriton DR, Gritter M. Triad: a scalable deployable nat-based internet architecture. Technical Report; January 2000.
Chiocchetti R, Rossi D, Rossini G, Carofiglio G, Perino D. Exploit the known or explore the unknown? Hamlet-like doubts in icn. In: ACM SIGCOMM workshop on information-centric networking; 2012.
Choi N, Guan K, Kilper DC, Atkinson G. In-network caching effect on optimal energy consumption in content-centric networking. In: IEEE ICC next generation networking symposium; 2012.
Dai J, Hu Z, Li B, Liu J, Li B. Collaborative hierarchical caching with dynamic request routing for massive content distribution. In: IEEE INFOCOM; 2012.
Dannewitz C. Netinf: an information-centric design for the future internet. In: Proceedings of the 3rd GI/ITG KuVS workshop on the future internet; 2009.

Dannewitz C, Kutscher D, Ohlman B, Farrell S, Ahlgren B, Karl H. Network of information (netinf) – an information-centric networking architecture. Comput Commun 2010a;36(7).
Dannewitz C, Golic J, Ohlman B, Ahlgren B. Secure naming for a network of information. In: IEEE INFOCOM; 2010.
Duval E, Hodgins W, Sutton S, Weibel SL. Metadata principles and practicalities. In: D-lib Magazine, vol. 8; 2002.
Fuller V, Li T, Yu J, Varadhan K. Classless inter-domain routing (CIDR): an address assignment and aggregation strategy, RFC Std. RFC1519 Obsoletes: 1338, BARRNet, cisco, MERIT, OARnet; 1993.
Ghodsi A, Koponen T, Raghavan B, Shenker S, Singla A, Wilcox J. Information-centric networking: Seeing the forest for the trees. In: ACM HotNets-X; 2011.
Guan K, Atkinson G, Kilper DC, Gulsen E. On the energy efficiency of content delivery architectures. In: IEEE ICC green communications workshop; 2011.
Available Online at: ⟨http://en.wikipedia.org/wiki/Peer-to-peer⟩.
Jacobson V, Smetters D, Thornton J, Plass M, Briggs N, Braynard R. Networking named content. In: ACM CoNEXT. ACM; 2009.
Katsaros K, Xylomenos G, Polyzos GC. A hybrid overlay multicast and caching scheme for information-centric networking. In: Proceedings of the global internet 2010 symposium; 2010.
Kim E, Kim D, Huh M, Lee B-J. Privacy protected content sharing in extended home environment over content-centric networking. In: IEEE International Conference on Consumer Electronics; 2012.
Koponen T, Chawla M, Chun B-G, Ermolinskiy A, Kim KH, Shenker S, et al. A data-oriented (and beyond) network architecture. SIGCOMM Comput Commun Rev 2007;37(August):181–92.
Lagutin D, Visala K, Tarkoma S. Publish/subscribe for internet: PSIRP perspective. IOS Press; 2012.
Lauinger T, Laoutaris N, Rodriguez P, Strufe T, Biersack E, Kirda E. Privacy implications of ubiquitous caching in named data networking architectures. Technical Report TR-iSecLab-0812-001. Northeastern University; 2012.
Lauinger T, Laoutaris N, Rodriguez P, Strufe T, Biersack E, Kirda E. Privacy risks in named data networking: what is the cost of performance. ACM SIGCOMM Comput Commun Rev 2012b;42(5).
Lee U, Rimac L, Kilper DC, Hilt V. Toward energy-efficient content dissemination. IEEE Netw 2011; 25.
Li Z, Simon G. Time-shifted tv in content centric networks: the case for cooperative in-network caching. In: IEEE ICC; 2011.
Li Z, Simon G, Gravey A. Caching policies for in-network caching. In: IEEE ICCCN; 2012.
Lu Y, Wang Z, Yu Y-T, Fan R. Social network based security scheme in mobile information centric network. In: IEEE ad hoc networking workshop; 2013.
Luo H, Chen Z, Cui J, Zhang H. Color: an information-centric internet architecture for innovations. IEEE Netw 2014;28(3).
Migault D, Palomares D, Herbert E, You W, Ganne G, Arfaoui G, et al. E2e: an optimized ipsec architecture for secure and fast offload. In: The seventh ARES; 2012.
Miller VS. Use of elliptic curves in cryptography. In: Proceedings of the CRYPTO' 85; 1985.
Moy J. OSPF version 2, IETF Std. IETF Obsoletes: 2323; 1998.
Ohlman B, Eriksson A, Rembarz R. What networking of information can do for cloud computing. In: IEEE international workshops on enabling technologies: infrastructures for collaborative enterprises; 2009.
Perino D, Varvello M. A reality check for content centric networking. In: ACM SIGCOMM workshop on information-centric networking; 2011.
Psaras I, Clegg RG, Landa R, Chai WK, Pavlou G. Modelling and evaluation of CCN-caching trees. In: IFIP Networking; 2011.
Ravindran R, Wang G, Zhang X. Towards secure mobile virtual group in information-centric network. In: IEEE international conference on advanced networks and telecommunication systems; 2011.
Rosensweig EJ, Kurose J, Towsley D. Approximate models for general cache networks. In: IEEE INFOCOM; 2010.
Rosensweig EJ, Menasche DS, Kurose J. On the steady-state of cache networks. In: IEEE INFOCOM; 2013.
Rothenberg CE, Jokela P, Nikander P, Sarela M, Ylitalo J. Self-routing denial-of-service resistant capabilities using in-packet bloom filters. In: Proceedings of the European conference on computer network defence; 2009.
Salsano S, Mellazzi NB, Detti A, Morabito G, Veltri L. Information centric networking over sdn and openflow: architectural aspects and experiments on the ofelia testbed. Comput Netw 2013;57(16).
Stoica I, Morris R, Karger D, Kaashoek MF, Balakrishnan H. Chord: a scalable peer-to-peer lookup service for internet applications. In: Proceedings of the 2001 conference on applications, technologies, architectures, and protocols for computer communications, ser. SIGCOMM '01; 2001.
Thaler D, Ravishankar C. Using name-based mapping to increase hit rates. IEEE/ACM Trans Netw 1998;6(1).
Tong J, Pi R, Xu K. Cloud computing infrastructure based on named content. In: IEEE pervasive computing and applications (ICPCA); 2011.
Vahlenkamp M, Schneider F, Kutscher D, Seedorf J. Enabling information centric networking in ip networks using sdn. In: IEEE SDN for future networks and services; 2013.
Vakali A, Pallis G. Content delivery networks: status and trends. IEEE Internet Comput 2003;7(6):68–74.
Wang L, Hoque MA, Yi C, Alyyan A, Zhang B. OSPFN: an OSPF based routing protocol for named data networking. Name data networking. Technical Report NDN-003; July 2012.
Zhang L, Estrin D, Burke J, Jacobson V, Thornton JD, Smetters DK, et al. Named data networking (ndn) project. Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC; 2010.