Chapter 1
Introduction

Syed Hassan Ahmed, Safdar Hussain Bouk and Dongkyun Kim

Abstract During the 19th century, ICT services and innovations have enabled humans and machines to interact in various ways. The very basic and most important invention was the "Internet," which actually connected and thus became the baseline for the rest of the upcoming discoveries in almost every scientific field of research. Today, the Internet is used by everyone regardless of their location, and people are depending on the Internet more than ever expected, even by its initial developers. In fact, it is not a difficult assumption to say that the rapid increase in the use of the Internet will bring several challenges to service providers. lasting past decades, we have seen the demands of end users increase faster than research and development efforts in the area of telecommunications. For example, today we want to FaceTime, YouTube, and Skype on the go rather than make a simple landline audio call with fixed wires. Similarly, much essential software and many systems require a significant amount of bandwidth. In short, we need to change the architecture of the Internet in the near future, and we expect that the new architecture will contribute to change the focal point of communications from host-centric to information-centric because today we are interested in services, rather than sources, providing content. In this introductory chapter, we will discuss the history of the Internet and why we require new developments such as content-distribution networks, peer-to-peer networks, and multi-cast communications. In addition, we enlighten our readers with the possible outcomes of the current research going on in the field of the future Internet.

Keywords Internet history · CDN · P2P · Future internet · Communication challenges

1.1 Introduction

Initially designed for secure yet limited use, such as e-mail exchange and file transfer, the **Internet** architecture has been transformed from the past decades. Later on, connected devices started sharing database registers, activating printers, and accessing files from online servers and so on. Therefore, we have witnessed

S.H. Ahmed et al., *Content-Centric Networks*, SpringerBriefs in Electrical and Computer Engineering, DOI 10.1007/978-981-10-0066-9_1

enormous research and development efforts being made for improving communication among hosts, clients, and end users. Hence, we believe the fact that the Internet emerged as an end-to-end communication network for sharing data and resources between devices [1].

With the passage of time and amazing growth during the technological era, the theme of communications has shifted from basic-level communication to content dissemination [2]. Here it is worth mentioning that the content can be a text file, an image, a short video, or larger data traffic. In contrast, new technological trends tend toward the need for increased bandwidth. No doubt increased bandwidth brought us a whole new set of applications including multimedia applications [3]. Moreover, in our daily life, the pervasive access of the Internet has presented a complete new set of businesses—such as online marketing, search engines, social networking, advertisements, and online commerce—that have been built on the aggregation and sharing of personal data. For instance, video-sharing websites (such as YouTube, Daily Motion, etc.) and peer-to-peer (P2P) networks are trending examples. Such applications strengthen our observations that content distribution over the Internet has grown from a textual toward a multimedia information system where services and applications focus on content [4].

This rapid growth in the volume or size of the data being exchanged over the Internet brings up several questions as follows:

- Is the current Internet going to be able to successfully handle content-centric communications?
- How can mobility be handled while having the same IP-based architecture?
- What security protocols will be sufficient to provide security for the massive amount of data?
- Will current infrastructure-based mobile networks be the only solution to handling mobility?

In short, there are many questions regarding the feasibility of the current Internet architecture, designed decades ago, to support our communications in future [5]. In history, we can see developments and advancements in the result of the enormous efforts initialized by researchers from both industry and academia. However, most of the advancements have been to improve IP-based networks and the discussion regarding how to address the contents instead of the end-to-end hosts remains very much alive.

1.1.1 History of the Internet

As mentioned previously, during the initial days Internet applications were mostly based on word-based information only. Similarly, users were expected to use the Internet for exchanging email messages and transferring files by way of file transfer protocol (FTP) and access remote servers. In contrast, today the Internet is a complex and heavily loaded multimedia/information system based on content

distribution [6]. For simplicity, we call documents, videos, audio, images, and web pages the "contents." Similarly, the metadata used to find, understand, and manage such contents is also included in the heading of "contents." Therefore, the new system must enable users to request and then receive the required content in an efficient manner [7].

For that purpose, first, content resolution is required, and thus it should be guaranteed by the system we design. "Resolution" here means that there should be a unique identifier of any content, and this can be achieved only when there is a state-of-the-art mechanism available to generate those identifiers. In addition, the lifetime of the content should also be considered as a parameter while setting the identifier. For example, let us consider the terms "chronological" and "perpetual." Data or content can be chronological if it has a shorter lifetime or validity such as a weather report, a road traffic condition, an emergency situation, any error in any system, and so on [8]. Perpetual or long-lasting valid data include location information on a fixed server of a building, a street, a data rate, the capacity of any system, and so on. Recently, it has been perceived that the advent of Web 2.0 has increased the number of content publishers. This means that users with no IT background and technical soundness can publish or upload the content of any size over the Internet. That content is most likely to be requested by users later. Hence, we can say that it is nearly impossible to assure a complete persistence of content while taking the current Internet architecture into account.

Second, it is expected that the new system must be scalable in such a fashion that the search and forwarding mechanisms of the contents are efficient regardless of the total number of users, their users' locations, and the content offered. Both the content users and providers must be able to operate at the Internet scale.

Finally, secure access to contents is key to providing authentication and further access-control mechanisms to the contents available. So far, there is no such solution or system that satisfies all the aforementioned requirements at the same time. However, the current literature is full of investigations being made to partially satisfy them. Figure 1.1 shows the revolutionary breakthroughs made so far in the IP-based Internet paradigm. It has been rationalized that the currently the communication focal point is content rather than the devices. Hereafter, this chapter will focus on the communication perspective on the current Internet and its limitations for future requirements.

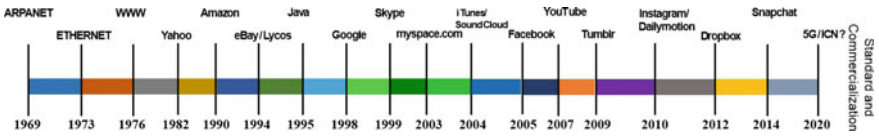

Fig. 1.1 Revolutionary advancements in Internet history

1.2 Communications in the Internet

In this section, we focus on the basics of Internet communications. Readers are provided with historical evolutions in Internet communications varying from end-to-end concepts to the latest applications of publish/subscribe systems.

1.2.1 End-to-End Communications

On a worldwide scale, the Internet is a packet-switched network where packet forwarding is based on the maximum best-effort service module possible by the Internet protocol (IP) [9]. During the process of packet forwarding, however, neither a resource nor any different predetermined service has been determined. As a result, contents are distributed without taking performance into account. Similarly, the current Internet architecture focuses on communication between hosts. This means that the name of the host as a source is included in the packet header in the form of an IP address, and the header also includes the IP header of the destination host. During the communication, the packets are traversed hop-by-hop, and this traversing is solely based on the destination IP address. Initially, this model was suitable for the Internet applications of that time where the main goal was to share resources remotely offered by a particular host, such as a printer server, a file server, and a Web server [10]. However, in the current era, it is difficult to satisfy the content distribution and its requirements due to various constraints such as the location information of the contents and the name under which the content is stored on the destination server. For this reason, content distribution in the current Internet is supported by patches, which consist of a set of mechanisms and protocols, thus partially satisfying the application requirements accordingly.

One known Internet protocol is the hypertext transfer protocol (HTTP), which redirects the content search, especially those with a nonpersistent nature [11]. Therefore, HTTP objects are usually requested using the resource locators and are referred to as "uniform resource locators" (URLs). The relevant URLs are included in the headers of the packets or messages being sent. Through this process, the HTTP forwards the events triggered by the server hosting the requested object or contents. In this case, an HTTP [12] redirect message is sent back to the client that contains the new URL in its header field. This process, however, must be aware of the content's location, and hence it is mandatory to have a complimentary mechanism assisting the persistent access to the required or requested contents irrespective of their location, characteristics, and other properties. Our example shows the working model of client server model. For instance, one point-to-point communication channel is built between one client and one server. Let's assume that several users simultaneously send a request message for a given content located at or hosted by the server where multiple point-to-point channels are established and single copy of content is to be sent over each channel. Hence, we conclude that the

most popular content results in less efficient distribution, specifically in terms of bandwidth. Despite the fact that it is not efficient, this model is being widely adapted by the current content distribution applications and architectures [13]. In short, the content distribution for applications on a large scale requires significant improvements in forwarding mechanisms to make them more scalable and different from the current client server model(s). In addition, the authentication and security of the content cannot be avoided; hence, it is expected that the applications for content distribution also provide security for the content during the Internet communication. However, in the current Internet system, security has been guaranteed for the channel being used between the source and destination host(s) while ignoring the security of the content(s).

Therefore, for the sake of security, a few additional processes and messages have been introduced, for example, Internet protocol security (IPSec) [14]. The IPSec causes overhead by introducing a patch that is used to ensure secure connection/communication. To be specific, IPSec enables users to maintain reliable and secure connections with the help of authentication headers (AHs); in addition, cryptography is applied to the data by encapsulated security payloads (ESPs) [15] and various key management mechanisms. Likewise, the content security still depends on the host and its relevant channel security levels. Hence, the scalability is still an open issue and requires appropriate attention from the research community [16]. Because the same content is not shared between users due to the unsecure channel between two or more hosts, an alternative method is to establish multiple secure connections among the content users and sources, which is of course going to increase the number of channels and security issues if the number of users increases. Therefore, we believe that some specific solutions for content distribution applications are still missing.

1.2.2 Multi-cast Communications

Here we discuss the multi-cast communication process, which is one of the initiatives for making effective content distribution possible over the Internet [17]. During development, the multi-cast is implemented by integrating an IP multi-cast on top of a medium-access control (MAC) layer. To be specific, in multi-cast communications, a single datagram of the content forwarded by a host may reach multiple destination hosts interested in the content. Basically, these destination hosts are accumulated in the form of group, which is originally identified by a single IP address. That's why the source host needs to send one datagram to that one IP address. All of the connected hosts to that one destination IP address receive the datagram/data accordingly. In this case, the network layer plays a vital role in forwarding and replicating the datagrams, sometimes, over the distribution tree, thus covering every host interested within that group. The main advantage of such approach is to avoid unnecessary copies of the same datagrams over the link during the communication process. However, we must know that IP multi-cast was

originally proposed in the 1990s and has not been adopted on the larger-scale Internet [18]. According to several researchers, one reason can be complexity of the system to configure, manage, and allocate the set of protocols required by the IP multi-cast. In short, a host is able to join and leave the group any time, and also it might be a member of more than one group at the same time. Moreover, it has also been reported that the sender is not required to be a member of the group. For instance, this approach leads us to the issues of authenticity and privacy.

1.2.3 Peer-to-Peer Systems

In the recent past, researchers from academia and industry developed a great idea of letting users share content with each other regardless of their location and other factors. Servers, instead of providers, started playing the role of the "bridge." However, the basic infrastructure is still IP based. The founders of that time named this new emerging technology "peer-to-peer" (P2P) systems [19]. Content sharing in P2P takes place in such a fashion that nodes with similar interests create an overlay network at the application layer and are known as "peers." These peers moderately share the bandwidth, the downloading process, and the storage capacity over the servers, thus resulting in efficient content retrieval. The basic idea is that the peer contributes to the given amount or the limit of its resources and uses the services made available by the overall P2P system [20]. As a result, additional peers in the systems contribute to the efficiency of the content available. The scalability of P2P system, however, still depends on the number of peers involved. Moreover, the P2P system is independent of any changes to be made in the network core compared with multi-cast IP systems [21].

In today's era, the user is interested in retrieving the required content regardless of the source. For example, in the current communication system, we can find in BitTorrent, where every new peer in the system chooses its partners or collaborator randomly and start collecting chunks of the required data. These partners were selected from the group of the peers already registered, or they have the same interests of the required content, and here we must clear that the location or identity of the peers involved is not mandatory or being used. The massive success of P2P networks for both file sharing and streaming applications has proven the fact that the Internet paradigm must be changed [22]. Here we argue that P2P is the baseline and runway for information-centric networks (ICNs) to take off.

It is expected that ICNs will be more scalable than P2P. Although P2P is providing good throughput and more efficient content retrieval [23], it suffers from security problems; in addition, there is a limited source of incentives for peers to share their resources. Moreover, P2P networks rely on peer collaboration to work properly [24]. Hence, whether or not the data forwarded by the other peers are trusted is a critical question to be answered by future networking paradigms such as ICNs. In addition, the robustness of the system is directly related to the number of peers joining or leaving the network. In the current Internet architecture, there is no

dedicated architecture or infrastructure to deal with (1) the management of those peers joining or leaving and (2) determining the remaining chunks out of the total chunks for any content.

1.2.4 Content-Distribution Networks (CDN)

Another attempt to increase the efficiency and scalability of the client server communication model has been made by proposing content-distribution networks (CDNs) [25]. No doubt CDNs are improving many applications for content distribution. Basically, CDNs consist of a group of distributed systems, and that group is interconnected by way of the Internet. Those systems cooperatively contribute in content distribution. To be specific, the contents are replicated on various servers, mostly by different Internet service providers (ISPs). This feature enables CDNs to increase the availability of any content. When a user requests any content, x, the request for x is forwarded and redirected to one of the servers close to the user. By this, CDNs try to minimize hops between the requester (user) and the provider (source server) and thus decrease the latency and increase the delivery rate due to the probability of less congestion [26]. CDNs are comprised of two main building blocks, i.e., the replication and distribution service and the request redirection service, where the content providers (servers) use the former service to find proper servers and to allocate storage capacity and so on. In contrast, the latter service is used as an interface between content consumers and providers.

Fundamentally, this service assists in receiving requests for the required content and later forwards each request to the most appropriate CDN server in order to satisfy it. Moreover, CDNs are typically composed of two types of servers: an origin server and a replica server. The origin server attributes the content identifier and is responsible for storing and announcing the contents. In contrast, the replica server forwards the content to the clients [27]. Generally, clients send request(s) to the origin server, which redirects these messages to the replica server closest to the client that stores the desired content. Figure 1.1 illustrates this process. In summary, redirection mechanisms severely affect a CDNs performance (Fig. 1.2).

1.2.5 Publish/Subscribe Systems

Here we give one example that shows that the current Internet architecture must be changed in the near future. That example is the recently proposed Publish/subscribe architecture, which is also known as pub/sub [28]. The pub/sub system also supports quite an identical mechanism to that of P2P for content retrieval. In pub/sub, the users are interested in receiving the content(s) only regardless of the identity of the sender. For that purpose, the contents are named “events,” and

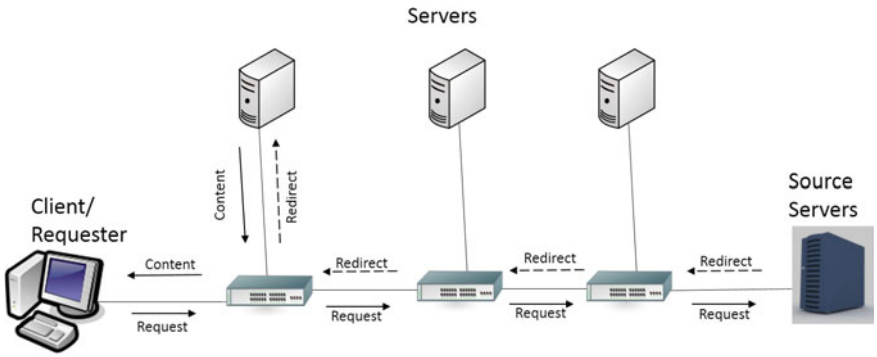

Fig. 1.2 Basic operations and scenario of CDN: A client sends a content request to the source server(s), which redirects this request to the server(s) closest to the client. Then the closest router sends the content to the client

their delivery is known as "notifications." The users basically subscribe for an event (i.e., content/data), and later on when the provider node or server finds that event in its repository, it replies back with the data, and that reply is supposed to be in the form of a notification. Here we describe the basic operations of pub/sub as follows:

Initially, the publisher node(s) create(s) event(s) and make a list of those events available to the subscriber(s). Later on, the subscriber nodes are able to initiate their interests in various events and patterns of events under the given preferences by the actual publisher, due to which subscribers are notified whenever is an event matching their interests is propagated by the publisher. There is a possibility that one publisher announced a list of events and got subscriptions; however, due to the factor of mobility (if applicable), the actual publisher moved away from the subscribers. In this case, other publisher for same events can be notified using some backbone networks. Here we must note that the subscribers and publishers are decoupled both in terms of time and space. As mentioned previously, publishers may announce their interest in any event, which is not yet published. In addition, the interest is not necessarily to be announced when the publisher of the associated event is online or in transmission range. Therefore, decoupling in this context somehow guarantees the scalability of the pub/sub system. In addition, it allows publishers and subscribers to work independently (readers can refer to Fig. 1.3).

The beauty of pub/sub is that it supports content distribution between a noticeably huge number of users because the publishers do not store information related to the interests of the subscribers, and similarly subscribers can receive content from any publisher regardless of whether the sender is known or not. The first pub/sub was proposed on the basis of a topics subscription. It allowed users to subscribe to a specific topic such as stock exchange information, weather reports for a specific area, and so on. Really simple syndication (RSS) feeds [29] are one of the successful milestones achieved, and they allow researchers to look into the topic later on. In topic-based pub/sub systems, users subscribe to events by using a topic

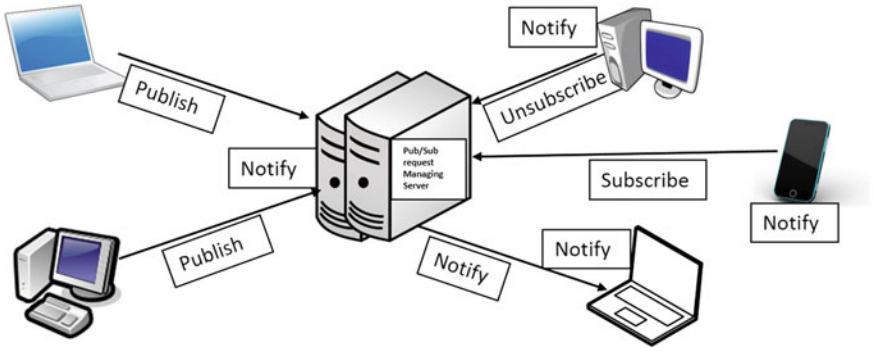

Fig. 1.3 Subscribe and event-notification functions in a simple pub/sub system

as a keyword, and whenever the publishers obtain fresh data on that event, the users are notified. Bloggers, Web sites, news channels, and any other applications have adopted RSS. The basic operations of pub/sub are quite similar to the concepts of IP multi-cast as described previously in this chapter. Each topic is a unique event, identified by the unique name, and must provide users with interfaces to use subscribe and publish functions.

Content-based systems are quite relevant and will be the next step in the evolution of pub/sub systems. In content-based systems, users subscribe to events based on the characteristics of the events themselves rather than on previously defined and static properties such as the identity of the topic. By this, the users are able to filter their subscriptions by using restrictions based on attribute value pairs (AVPs) and other basic logical operators, for example, <, >, =, and etc. Moreover, using Boolean operators and other looping techniques, the restrictions and conditions can be combined.

To be more precise, the various architectures of pub/sub systems are classified into centralized and distributed ones. The manner of subscription does not affect these classifications. Centralized pub/sub systems allow publishers to send messages to the central unit, e.g., a server, which stores all of those messages and redirects them to the subscribers when demanded. In contrast, the distributed architecture allows all system nodes to forward interests/notifications and process the requests because there is no central entity to take care of these various operations. Both strategies have their own merits and demerits. The authors here assume that the readers must have some preliminary knowledge of distributed and centralized architectures for different wireless and wired networks [30]. Generally, the distributed systems rely on multi-cast communications and are therefore prone to deliver the content more efficiently. Topic-based pub/sub systems offer benefits in terms of distributive properties. In contrast, content-based systems usually face many challenges if the distributed architecture is used due to the multi-cast communications. Multi-cast communication is influenced by the computational cost of filtering the subscriptions and forwarding the content.

1.3 Communications Challenges

No doubt, the Internet has changed our lifestyles in a positive manner. In addition, the contributions of the Internet to the growth of business cannot be downplayed. Moreover, the Internet has been playing a vital role in improving national defense and other important areas including hospitals, transportation systems, and economics. However, the fact is that most of the Internet architecture perspectives were designed and implemented almost 30 + years ago. In those 30 years, there has been extensive research and development about the networking and packet-switching modules. One question here arises: Is the current architecture appropriate way if we were given a chance to start the Internet today? In this chapter, we aim to answer this question, which has been raised by the National Science Foundation (NSF) while designing the next-generation Internet architecture known as the Global Environment for Network Innovation (GENI) [31]. More specifically, the next generation of the Internet is expected to be friendly for commercial use. For simplicity, we name the next generation of the Internet as "Internet 3.0." The reason behind this is to make sure that we are talking about the latest version compared with Web 2.0. Moreover, the NSF is looking forward to continuing this program of the next-generation Internet in line with the GENI initiative. According to the recent reports, the NSF plans to invest millions of dollars in this project, thud making it one of the largest projects the NSF has ever invested in. Hence, in the coming years, more research centers and academic giants will be attracted to and perform research for this project. Here we discuss the overview of the best available sources extracted from those existing works while putting them together in a coherent interoperable way.

Here it is worth stating that the Internet is a 40 -year-old technology because the first Internet RFC is dated approximately April 1969. So far, many steps have been taken to improve the Internet. In fact, we have witnessed the borrowing of ideas from current Internet-working research as well as from the other networking domains such as telephone, airlines, highways, railroads, postal services, and walkways. We came up with the solution that the next-generation Internet should be more secure compared with the existing version. In addition, it also should redefine the boundaries of the business as well as the policies inside those boundaries. The enormous use of Internet missionary governments sets further rules to protect citizens from cyber-crime in the same way that the government is responsible for protecting citizens from other hazards. Moreover, a new set of rules is required, and those rules should be flexible so that different governments can set various rules on top of the general ones. More precisely, the future Internet architecture should enable users to design mobile objects. For instance, we have new literature for software-defined networks (SDNs) that enables users to virtually set network functions according to their requirements [32]. However, those configurations require specific levels of training and infrastructure so that companies can handle them. We are expecting those complex operations to be turned into simple ones

for end users. This new architecture can be based on naming content and allow users to decide from where they would like to receive Internet traffic, control the privacy of their location, and so on.

1.4 Future Internet Technologies: A Solution?

From the previous discussions, we are convinced that we must move the current Internet architecture toward the emergence of new technologies collectively known as the "future Internet." In the future Internet, we have a rich literature available for ICNs [33]. The current Internet relies on purely point-to-point primitives, whereas according to the definitions of ICN projects, we are able to move the new Internet toward the data- or content- centric and -oriented networks. Almost a decade ago, a TRIAD paper proposed an architecture similar to ICN, and hence it should be given the credit to allow researchers to start working on future Internet architectures such as ICN. Later on, Baccala wrote an IETF draft in 2002, right after TRIAD, that also indicated that we should move forward from the primitive operation of displaying a Web content by way of end-to-end connection toward the delivery of a named set of data [34]. Moreover, few more researchers during those years claimed that they were ahead of the mentioned work. However, remarkably vatic, both of the designs still used the existing DNS-naming schemes, along with its inherent drawbacks, and only focused on basic content delivery with minor attention paid to other important issues including, but not limited to, security, streaming media, and faulty servers [35].

In this context, the data-oriented network architecture (DONA) was proposed almost 5 years after the former two identical works [36]. DONA was the first comprehensive and detailed clean-slate ICN design that supported the use of self-certified content names suggested by earlier works of its time. Different from the others, DONA also incorporated advanced cache functionalities to address the various ICN issues. Unfortunately, rapid follow-up on the work appeared later with reference to other ICN architectures, and this caused avoidance of the research topic to be pursued by the broader research community later.

Recently, content-centric networks (CCN) have been proposed with the ignition of interest in the ICN area, and the idea has spread widely [37]. The CCN inventor Van Jacobson took on this initiative while working for the Palo Alto Research Center (PARC). Several workshops have been devoted to CCN and ICN, and projects such as 4WARD, PSIRP/PURSUIT, SAIL, and COMET have been focusing on the given topic. Later on CCN became the preliminary architecture for the Named Data Networking (NDN) project [38], which was chosen as one of the four proposals in the Future Internet Architecture (FIA) program lead by the NSF. However, ICN research is still difficult to be adapted into real-time scenarios. There is little common terminology between these proposals, and because there is no common or standard framework yet, the focus is often on low-level mechanisms being performed in the recent research. Due to this early stage, many research

works emphasize the differences between design and others while leaving the readers to design/construct the "forest" of ICN out of these proposed tree-like structures. In contrast, the research community had taken it for granted so far, but the reality is that ICN deserves to be explored rapidly and widely. These current affairs led us to compile this book with the goal of providing a broader perspective on current ICN designs and their history to give readers a complete set of knowledge, and thus motivation toward research activities can be increased.

1.4.1 Fundamental Differences in Design

Now we will discuss several aspects of ICN that make it different from the current Internet. Mainly, ICN differs from the current Internet architecture in three important perspectives. Those include (1) naming the content, (2) interdomain routing, and (3) the location of the narrow waist with an ICN-based Internet. As discussed previously, in ICN each client or user looks up the content by its name while being unaware of its location. Similarly, it is expected that any content-oriented security model must hold the following properties:

(i) The consumer is expected to know the exact name of the content and the type it is looking for. That is, the consumer must be able to map between the real-world description of what they require (e.g., BBC headlines) and its corresponding ICN name resolved by the system.
(ii) The consumer should know the provider's public key for any content so that it can verify the attribution and integrity of the retrieved content.
(iii) The ICN system as a whole should be able to allow binding of an object's name to the public key of the content provider so that it can prevent attackers from registering false content(s). Avoiding this binding may result in favors of attackers who may use false content as a denial-of-service (DOS) attack.

In terms of naming, ICN consists of two main naming systems. The first one resembles today's DNS names and uses hierarchical human-readable names [39]. The human readability partially addresses the first requirement, and the hierarchical structure helps with scalability. There can be multiple ways or techniques that may allow the requester/consumer to know the public key (ranging from personal contacts to webs-of-trust to PKIs), but for the ICN system to be aware of this key requires a globally agreed-upon PKI to bind names to keys. In contrast, the second naming system takes self-certifying names into the account. In this case, the public key is bound to the name itself, so the ICN system does not depend on any PKI. However, these names are not human-readable, so requesters must use some other techniques (e.g., search engines, personal contacts, webs-of-trust) to determine the name of the required content.

For the satisfaction of interest packets being generated for any content, the ICN systems must route those requests or interest packets. To make this routing happen, there are many different approaches in the ICN literature for achieving name-based

routing within a given domain, but these differences are largely autonomous in nature and not of fundamental importance. Hence, the ICN proposals differ more fundamentally in terms of routing, i.e., how the routing is performed between domains. For example, a CCN leverages the current interdomain routing system and builds name-based routing on top of BGP. Here it is to be noted that CCN is one of the ICN architectures. Others (such as DONA) follow the BGP policy model, but they do their own name-based routing, and still others (such as PSIRP) develop their own interdomain routing paradigm.

Likewise, as we know, IP is the narrow waist of the current Internet architecture. This is frequently seen as a major difference between ICN designs, but we stand firm that this is actually a broader architectural debate that is mostly orthogonal to ICN design details. All of the ICN designs involve hop-by-hop communication between the ICN-layer elements (e.g., content routers in CCN, rendezvous nodes in PSIRP, resolution handlers in DONA, and content-aware routers in curling). Because this communication is merely between hops (and does not require global reachability), one could carry any of these designs over IP or as a substitute for the IP (running over some L2-like layer that offers local delivery). Nevertheless, whether one retains or replaces IP as the narrow waist obviously has implications for the overall Internet architecture as well as for the performance required in the ICN layer [40]. More detailed analysis and descriptions will be presented in Chap. 2 and 3 of this book.

1.4.2 Anticipated Changes in Future Internet Technologies

In this section, we list the top 10 features that would help remove some of the problems faced by current Internet users.

(i) Energy-efficient communication: Current Internet architecture requires both source and destination end-systems to be up and awake for the communication to take office. All packets received when the destination is down are dropped. By introducing wireless devices, this restriction is rendered tranquil by allowing base stations to store the packets while the subscriber device is sleeping. For energy-efficient communication, this should be generalized to wired devices as easily.

(ii) Separation of identity and address: In the current Internet, a system is identified by its IP address. As a result, when a system changes its point of attachment, the address changes. This makes reaching mobile systems more difficult. We agree with the fact that this is a well-known problem, and a number of attempts and proposals have been made in the past to solve such issues including mobile IP, internet indirection infrastructure, host-identity protocol, and others.

(iii) Location awareness: IP addresses are not linked to geographical position. This can be considered a strength of IP. However, a large share of

information-transfer applications, such as any other transport system, requires finding the nearest server. Likewise, mobile nodes must know their position. The next-generation Internet should have the receiver decide about location privacy.

(iv) Explicit support for client server traffic and distributed services: A large percentage of current Internet traffic is client server traffic. A Web user trying to reach Google is a model of client server traffic. These users tend to reach "Google," which is not a single system. In fact, it is a distributed service with hundreds of systems in hundreds of various locations. However, the user is interested in communicating with the nearest instance of this service for the quickest and most relevant response. In the current Internet, the name "Google" resolves to a single IP address, and so directing users to the right server is unnecessarily complex.

(v) Person-to-person communication: The Internet was originally designed for computer communications. However, the real target of communication is often a human being. In today's world, a human being may be reachable using a desktop computer, a laptop, a cell phone, or a landline (i.e., wired) phone. The main goal is to reach the person and not the desktop computer, the laptop, or the phones, respectively. Here, we recall in the section on IP addressing that the person does not have an IP address, and the user is forced to select one of these intermediate steps as the destination for person-to-person communication instead of the real destination, i.e., the person. If each person had an address, the network could decide the right intermediate device, or the person could dynamically change the device as appropriate in accordance with the requirement.

(vi) Privacy: Privacy and security issues of the current Internet are not concealed to any further extent. So far, we have many serious and proficient attempts and solutions available in the literature, but the truth is that we still receive lot of spam in our mailbox today. Moreover, every day, it is becoming necessary that the next generation of Internet must allow users the option of verification of content, its sources, and its destinations and intermediate systems. In addition, the privacy of data, location, and data integrity should be considered while designing new protocols and communications frameworks.

(vii) New framework integration: As far as the current Internet framework is concerned, data plane, control, and management plans are merging with one another. In today's Internet, the control messages (for example, TCP-connection setup messages) or management messages (such as SNMP messages) follow the same links as data messages. Moreover, control signals are also piggybacked on data packets. This results in high vulnerability and introduces significant security risk as demonstrated by all of the security attacks on the Internet. In contrast, the telephone network uses a separate control network and is generally considered more secure than Internet. For this problem, generalized multiprotocol label switching (GMPLS) is one attempt to separate control and data planes. One benefit of this parting is

that it allows data plane to be non packet-oriented such as wavelengths, SONET frames, or even power-transmission lines. This separation is expected to be an integral part of the next-generation Internet architecture.

(viii) Isolation requirements: For many, critical applications—such as military and various monitoring ones—users mostly demand isolation of the application (s) in a shared environment. "Isolation" here means that the performance of one application is not be affected by other application(s) sharing the same resources. Technically speaking, this is difficult to achieve; however, one substitution is to provide dedicated resources to such application(s). To bring this into reality, we have virtual private lines (T1/E1 lines) from telecommunications companies to create private networks. Similarly, it seems that the next-generation networks shall provide users with a programmable mix of isolation and sharing services for application(s).

(ix) Symmetric and asymmetric Internet protocols: Currently, although most Internet protocols are symmetric, they were designed for end-systems with similar competencies. Similarly, regarding wireless sensor and palm-device networks, one can argue that the end-system is significantly resource constrained compared with the others. Thus, in some instances it is reasonable to allow asymmetric protocols, and in the future we expect more sophisticated asymmetric protocols.

(x) Quality of service (QoS): As the name indicates, QoS belongs to a service that in one way or another is related to those packets that affect the services provided. We must know that the ultimate goal of any communication domain is to provide various services to users while using different wireless paradigms. Therefore, the main interest of the user is to receive guarantees about the delay and throughput of data-packet flows. However, IP-based networks make it difficult to guarantee QoS. In contrast, the future-generation Internet should allow a variety of QoS guarantees including total isolation if desired.

References

1. Gromov GR (2002) The roads and crossroads of internet history. NetValley [online]. [cit. 2015-05-22]. Dostupné z: http://www.netvalley.com/cgi-bin/intval/net_historypl (2002)
2. Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, Lynch DC, Postel J, Roberts LG, Wolff S (2009) A brief history of the Internet. ACM SIGCOMM Comput Commun Rev 39 (5):22–31
3. Russell AL (2012) Histories of Networking vs. the History of the Internet. In: SIGCIS Workshop
4. Cooper M (2014) The future of internet-enabled innovation: the long history and increasing importance of public-service principles for 21st century public digital communications networks. J on Telecomm & High Tech L 12:1–265
5. Handley M (2006) Why the Internet only just works. BT Technol J 24(3):119–129

6. Stuckmann P, Zimmermann R (2009) European research on future Internet design. Wirel Commun IEEE 16(5):14–22
7. Pan J, Paul S, Jain R (2011) A survey of the research on future internet architectures. Commun Mag, IEEE 49(7):26–36
8. Choi J, Han J, Cho E, Kwon TT, Choi Y (2011) A survey on content-oriented networking for efficient content delivery. Commun Mag, IEEE 49(3):121–127
9. Yu T, Zhang Y, Lin KJ (2007) Efficient algorithms for Web services selection with end-to-end QoS constraints. ACM Transa on Web (TWEB) 1(1):6
10. Floyd S, Fall K (1999) Promoting the use of end-to-end congestion control in the Internet. IEEE/ACM Trans on Netw (TON) 7(4):458–472
11. Fielding R, Gettys J, Mogul J, Frystyk H, Masinter L, Leach P, Berners-Lee T (1999) Hypertext transfer protocol–HTTP/1.1. No. RFC 2616
12. Padmanabhan VN, Mogul JC (1995) Improving HTTP latency. Comput Netw ISDN Syst 28 (1):25–35
13. Stoica I, Adkins D, Zhuang S, Shenker S, Surana S (2002) Internet indirection infrastructure. ACM SIGCOMM Comput Commun Rev 32(4):73–86. ACM
14. Thomasson JK, Neil RT, Davis MM, Mosbarger ML (2015) System and method for multicasting IPSEC protected communications. U.S. Patent 8,953,801. Issued 10 Feb 2015
15. Jokela P, Melen J, Moskowitz R (2015) Using the encapsulating security payload (ESP) transport format with the host identity protocol (HIP)
16. Hakiri A, Berthou P, Gokhale A, Schmidt DC, Thierry G (2014) Supporting SIP-based end-to-end data distribution service QoS in WANs. J Syst Softw 95:100–121
17. Moyer MJ, Rao JR, Rohatgi P (1999) A survey of security issues in multicast communications. Netw IEEE 13(6):12–23
18. Takase A, Tanabe S, Endo N, Takeyari R, Mishina Y, Oouchi T, Yanagi J (1997) Multicast communications method. U.S. Patent 5,612,959. Issued 18 Mar 1997
19. Rodrigues R, Druschel P (2010) Peer-to-peer systems. Commun ACM 53(10):72–82
20. Liben-Nowell D, Balakrishnan H, Karger D (2002) Analysis of the evolution of peer-to-peer systems. In: Proceedings of the twenty-first annual symposium on Principles of distributed computing, pp 233–242. ACM
21. Lua EK, Crowcroft J, Pias M, Sharma R, Sharon L (2005) A survey and comparison of peer-to-peer overlay network schemes. Commun Surv Tutorials, IEEE 7(2):72–93
22. Risson J, Moors T (2006) Survey of research towards robust peer-to-peer networks: search methods. Comput Netw 50(17):3485–3521
23. Detti A, Bruno R, Blefari-Melazzi N (2013) Peer-to-peer live adaptive video streaming for information centric cellular networks. In: 2013 IEEE 24th international symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp 3583–3588. IEEE
24. Peltotalo J, Jarmo H, Jantunen A, Saukko M, Vaatamoinen L, Curcio I, Bouazizi I, Hannuksela M (2008) Peer-to-peer streaming technology survey. In: Networking, 2008. ICN 2008. Seventh International Conference on, pp 342–350. IEEE
25. Mangili M, Fabio M, Antonio C (2013) A comparative study of content-centric and content-distribution networks: performance and bounds. In: Global Communications Conference (GLOBECOM), 2013 IEEE, pp 1403–1409. IEEE
26. Al-Kanj Lina, Dawy Zaher, Yaacoub Elias (2013) Energy-aware cooperative content distribution over wireless networks: design alternatives and implementation aspects. Commun Surv & Tutorials, IEEE 15(4):1736–1760
27. Xu C, Fallon E, Qiao Y, Zhong L, Muntean G-M (2011) Performance evaluation of multimedia content distribution over multi-homed wireless networks. Broadcast, IEEE Trans on 57(2):204–215
28. Katsaros D (2015) Cache control issues in pub–sub networks and wireless sensor networks. Coordination control of distributed systems. Springer, Berlin, pp 259–264
29. Travers N, Zeinab H, Nelly V, Du Mouza C, Christophides V, Scholl M (2014) RSS feeds behavior analysis, structure and vocabulary. Int J Web Inf Syst 10(3):291–320

30. Ma XingKong, Wang YiJie, Sun WeiDong (2014) Feverfew: a scalable coverage-based hybrid overlay for Internet-scale pub/sub networks. Sci China Inf Sci 57(5):1–14
31. Axelrod RS, VanDeveer SD (eds) (2014) The global environment: institutions, law, and policy. CQ Press
32. Sezer S, Scott-Hayward S, Chouhan P-K, Fraser B, Lake D, Finnegan J, Viljoen N, Miller M, Rao N (2013) Are we ready for SDN? Implementation challenges for software-defined networks. Commun Mag, IEEE 51(7):36–43
33. Brito GM, Velloso PB, Moraes IM (2013) Information-centric networks. Inf-Centric Netw 13–22
34. Ghodsi A, Shenker S, Koponen T, Singla A, Barath R, James W (2011) Information-centric networking: seeing the forest for the trees. In: Proceedings of the 10th ACM Workshop on Hot Topics in Networks, p 1. ACM
35. Loo J, Aiash M (2015) Challenges and solutions for secure information centric networks: a case study of the NetInf architecture. J Net Comput Appl 50:64–72
36. Abidi A, Gammar SM, Kamoun F, Dabbous W, Thierry T (2014) Towards a new internetworking architecture: a new deployment approach for information centric networks. In: Distributed Computing and Networking, pp 519–524. Springer, Berlin, Heidelberg
37. Kim D-H, Kim J-H, Kim Y-S, Yoon H-S, Yeom I (2015) End-to-end mobility support in content centric networks. Int J Commun Syst 28(6):1151–1167
38. Zhang L, Afanasyev A, Burke J, Jacobson V, Crowley P, Papadopoulos C, Wang L, Zhang B (2014) Named data networking. ACM SIGCOMM Comput Commun Rev 44(3):66–73
39. Pentikousis K, Ohlman B, Corujo D, Boggia G, Tyson G, Davies E, Molinaro A, Eum S (2015) Information-centric Networking: Baseline Scenarios. No. RFC 7476
40. Xu Y, Li Y, Lin T, Wang Z, Zhang G, Tang H, Ci S (2014) An adaptive per-application storage management scheme based on manifold learning in information centric networks. Future Gener Comput Syst 36:170–179