Architectures for Future Media Internet

María Alduán[1], Federico Álvarez[1], Theodore Zahariadis[2], N. Nikolakis[2], F. Chatzipapadopoulos[2], David Jiménez[1], José Manuel Menéndez[1]

[1]E.T.S.I. Telecomunicación, U.P.M, Avda Complutense s/n, 28040 Madrid, Spain
{mam, fag, djb, jmm}@gatv.ssr.upm.es

[2] Synelixis Solution, P. Stavrou 5, 34100, Chalkida, Greece
{zahariad, nikolakis}@synelixis.com

Abstract: Among the major reasons for the success of the Internet have been the simple networking architecture and the IP interoperation layer. However, the traffic model has recently changed. More and more applications (e.g. peer-to-peer, content delivery networks) target on the content that they deliver rather than on the addresses of the servers who (originally) published/hosted that content. This trend has motivated a number of content-oriented networking studies. In this paper we summarize some the most important approaches.

Keywords: Content Centric, Future Media Internet architecture

1 Introduction

Internet is today the most important information exchange mean and has become the core communication environment not only for business relations, but also for social and human interaction. Moreover, it is a common belief that the Internet is evolving towards providing richer and more immersive experiences. Advances in video capturing and creation will lead to massive creation of new multimedia content and internet applications, including 3D videos, immersive environments, network gaming, virtual worlds.

Among the major reasons for the success of the Internet have been the simple networking architecture and the IP interoperation layer, which is so flexible as to support a wide spectrum of applications. However, the original Internet architecture is designed based on a client-server communication model. Every packet should have the addresses of the endpoints (source and destination) to support host-to-host applications like remote login and file transfer. However, the recent traffic measurements reveal that more and more applications (e.g. peer-to-peer, content delivery networks) target on the content that they deliver rather than the addresses of the servers who (originally) published/hosted that content. This trend has motivated content-oriented networking studies (e.g. DONA, CCNx).

In this paper we try to summarize some of the most important approaches in Content Centric Internet, towards a Future Media Internet architecture model.

2 Future Media Internet Architecture proposals

Before we analyze the various Future Media Internet proposals, let's review the relation between naming and routing. The current Internet focuses on the endpoints, thus, hosts are assigned (domain) names. Subsequently, content hosted in a server is characterized by the URL, which is the concatenation of the retrieval protocol, the host name and the path name. In order to fetch the content, the host (domain) name included in the URL has to be resolved to an IP address. So, the client application first retrieves the locator of the requested content (or more precisely, its holder) from a host name by looking up a database, DNS. Then the holding server is contacted to receive the content. Even though there is an additional layer of indirection (i.e. DNS lookup process), this lookup-by-name method has well served the Internet users with host-centric naming. Note that what is resolved it is not the individual contents, but the content holders.

In contrast, content-oriented networking designs hardly take hosts into account. Instead, content naming is used in routing directly, following the route-by name paradigm. In this paradigm, the content name is specified, the closest copy is located and dynamic routing is used to avoid the link/server failure. In terms of delivery efficiency, the route-by-name approach is more attractive since it can avoid the DNS lookup delay and will less likely waste time for servers out of service. However, the number of content files is orders of magnitude larger than the number of hosts. What is worse, it is difficult to aggregate the content names, while the locators (or addresses) of hosts are ready to be abstracted by a single identifier (i.e. a network prefix).

In the following we group different approaches towards the Future Media Internet architectures in those focused on the evolution of the current network architecture and those centered on its redesign. Both approaches aim to migrate "from the *where* to the *what"*.

2.1 Content-Centric Network

One of the major candidates in content-centric networks is the CCNx approach proposed by Van Jacobson's *et. al.* [1]. This architecture targets the "*always available*" instead of the "*always on*" paradigm and the "*multiparty-to-multiparty information dissemination*" rather than traditional "*point-to-point conversations*". CCN is a purely content centric approach, based on named content/content chunks instead of named hosts.

CCN decouples content routing/forwarding, localization, security and content access, departing from IP in the critical way (Figure 1). CCN considers two packet types: Interest packets and Data packets. Content consumers request data by broadcasting their interests; interests are received by other nodes that, if they can satisfy them, respond with a Data packet. If not, they forward the interest packet via another network interface. As packets identify content, multiple nodes interested in the same information can share transmissions within the same medium by means of standard multicast suppression techniques [2].

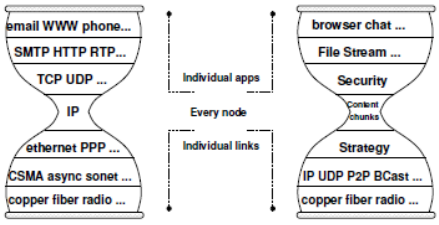

Figure 1: CNN moves the universal component of the network stack from IP to chunks of named content [1].

Moreover, CCN architecture introduces three main data structures:

- FIB (*Forwarding Information Base*): used to forward interests towards potential sources of matching data.
- *Content Store*: the same as a buffer memory of an IP router but with a different replacement policy. IP packets belong to a point-to-point Communications so that once forwarded they are not useful anymore. On the other hand, all CCN packets are potentially useful for more than one consumer due to their idempotent nature. Unlike IP FIFO model, CCN allows data caching in intermediate network points
- PIT (*Pending Interest Table*): keep track of interests forwarded upstream towards content sources. These structures allow Data packets to return get to their requesters (it can be seen as a breadcrumb system

Similar to a URL path name, CNN naming follows a hierarchical structure (Figure 2) Each individual name in composed as a number of components that can be encrypted for privacy. The nature of this naming system allows different levels of granularity.

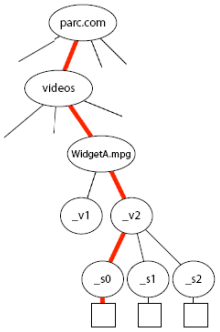

Figure 2: Hierarchical Naming: Named Tree traversal

CCN architecture, includes evolutions of different mechanisms also present in IP networking such as: flow and congestion control, intra-domain and inter-domain routing, etc. Another feature of CCN is that the security resides in the data itself, not in the network channel as in today's Internet. Instead of focusing the security in the hosts and in communication links, it focuses security on encrypting the content itself.

The network only concerns how to distribute the data and the publishers control the security of the data. As a consequence, it foresees the Future Internet network as a huge storage of authenticated data [1].

2.2 Data Oriented Network Architecture (DONA)

Instead of a hierarchical naming system that inherits from current IP model, DONA (Data Oriented Network Architecture) **[**4] is focused in naming and name resolution using flat names. DONA proposes a strict separation between naming and name resolution so that persistence, availability and authenticity problems can be solved. Persistence and authenticity problems are solved by the use of flat self-certifying names [4][5][6]. Availability problem is solved by the name resolution technique applied.

This resolution technique is based on the route-by-name paradigm so that a new entity called Resolution Handler (RH) appears. RHs, by interpreting the basic primitives FIND and REGISTER, are able to route content requests and responses. To support these two primitives, DONA introduces resolution handlers, which forward content to the users in an overlay manner. DONA names are flat, long and user unfriendly; so users will not have to remember these names directly, they will have their private human-readable name spaces [8] and rely on reliable external mechanisms such as search engines, recommender services, etc. for name resolution.

These flat self-certifying names are not new in the scientific community, it can also be found in TRIAD [6], HIP [7] and SFS [5]. The role this naming system can take in generic network architectures has been discussed in [9][10][11], which, as DONA, are focused in both, naming and name resolution.

2.3 Publish/Subscribe for Internet Perspective (PSIRP)

PSIRP (Publish/Subscribe for Internet Perspective) [13], [14] advocates for a new redesign of the network by means of a pub/sub approach. Just like DONA, PSIRP approach can be considered as semantically similar to a publish/subscribe (pub/sub) interface. PSIRP however aims to prevent SPAM or DoF attacks by living the control of the Communications to the information receivers.

PSIRP considers 4 identifiers in order to refer data chunks [12]: Application Identifiers (AId), Rendezvous Identifiers (RId), Scope Identifiers (SId) and Forwarding Identifiers (FId). RIds and SIds are self-certified names, so that, the same as in DONA, authenticity and integrity is guaranteed.

PSIRP architecture consists of autonomous systems called domains. These domains have at least three kind of nodes:

- ***Topology Nodes (TN)***: in charge of the intra-domain topology, load balance between BNs and routing vector interchange among different domains (in a similar way as BGP)
- ***Branching Nodes (BN)***: responsible of subscription messages routing and popular content caching

- ***Forwarding Nodes (FN)***: implement a simple, cheap and fast forwarding algorithm by using a Bloom filter [15]
- ***Rendezvous Points*** are used to locate Publications within the network; these entities form rendezvous points Networks globally connected by hierarchical DHTs [16]. This aggregation enlarges system scalability.

For security purposes, PSIRP uses elliptic curve cryptography [17] and packet level authentication [18].

Similar to PSIRP, Scalable Internet Event Notification Architectures (Siena) [12] features a generic scalable publish/subscribe event-notification service. Siena formulates a general model of content-based addressing and routing to maximize both expressiveness and scalability.

2.5 Evolutionary FI Architecture (EFIA)

Assuming a progressive, rather than aggressive evolution towards Future Internet, the Future Content Networks (FCN) [19] group has proposed the EFIA architecture that consists of different virtual hierarchies of nodes (overlays, clouds or virtual groups of nodes), with different functionality (Figure 3). This model may be easily scaled to multiple levels of hierarchy (even mesh instantiations, where nodes may belong in more than one layers) and multiple variations, based on the available level of information and service delivery requirements and constrains.

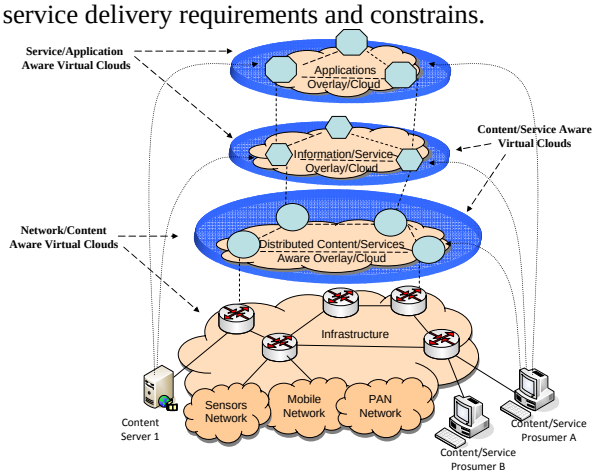

Figure 3: Logical Future Content-Centric Internet Architecture

At the lower layer, it is the *Service/Network Provider Infrastructure*. Users are connected to the infrastructure as content producers and consumers (Prosumers). Content will be routed, assuming basic quality requirements and if possible cached to some degree in this layer. Progressively this overlay will be reduced or even eliminated.

The Infrastructure should, on the one hand, hide all unnecessary complexity (e.g. physical network topology, mobile terminal handover) and on the other hand provide all the necessary information, so that more intelligent nodes will take all necessary

decisions in order to support the required functionality (including guaranteeing the QoS).

The medium layer is the *Distributed Content/Services Aware Overlay.* Content-Aware Network Nodes (e.g. core routers, edge routers, home gateways, terminal devices) will be located at this overlay. These nodes will have the intelligence to filter the content and Web services that flow through them (e.g. via Deep Packet Inspection, DPI) or identify streaming sessions and traffic (e.g. via signalling analysis). Alternatively, the content may be considered formulating *information objects* as first order elements in the network, thus be directly identifiable by the network nodes. In either case, the Nodes of this group will recognise and qualify the content. Part of this information may be stored locally and/or reported to the higher layer of hierarchy (Information Overlay).

Content/Services Aware Overlay may be dynamically constructed at the layers between the content and the information overlays. We may consider overlays for content caching, content classification (even content indexing in the future), network monitoring, content adaptation, optimal delivery/streaming. With respect to content delivery, nodes at this layer may operate as hybrid client-server, peer-to-peer or cloud networks, according to the delivery requirements.

At a higher layer, it is the *Information Overlay*. It will consist of intelligent nodes or servers that have a distributed knowledge of both the content/web-service location/ caching and the (mobile) network instantiation/conditions. Based on the actual network deployment and instantiation, the service scenario, the service requirements and the service quality agreements, these nodes may vary from unreliable peers in a next-P2P topology to secure corporate routers or even data centers in distributed carrier-grade cloud networks. The content may be stored/ cached at the *Information Overlay* or at lower hierarchy layers, though the *Information Overlay* will be always aware of the content/services location/caching and the network information. Based on this information, it may decide on the way that content will be optimally retrieved and delivered to the subscribers or inquiring users or services.

Finally, at the highest layer the *Application's layer* is located. Applications will use efficiently the services, the information and the media/content provided by the content-centric architecture and offer novel media experiences to the users.

2.6 Autonomic Layer-Less Object Architecture (ALLOA)

Moving from an evolutionary to a more clean-slate approach, FCN and [20] introduce the concept of ALLOA (Autonomous Layer-Less Object Architecture) based on the "Content Objects". A Content Object (or simply object) is a polymorphic/holistic container, which may consist of media, rules, behaviour, relations and characteristics or any combination of the above.

- ***Media: anything that a human can perceive/experience with his/her senses***
- ***Characteristics:*** meaningfully description of the object.
- ***Rules:*** can refer to the way an object is treated and manipulated by other objects or the environment (discovered, retrieved, casted, adapted, delivered, transformed, presented)

- ***Behaviour:*** can refer to the way the object affects other objects or the environment
- ***Relations:*** between an object with other objects can refer to time, space, synchronization issues

Objects can be hierarchically organized, like the constituting instrument channels of a music band, and can trigger the generation of new objects. An object can be divided/ spit into new objects or multiple objects can be combined/merged and finally create new objects, and these operations may happen while travelling over the network. Also an object can be cloned. The clone keeps the characteristics of its "parent" object but knows that it is a clone.

The autonomous objects will travel over the network, split and combined to generate the new service or virtual world object. The Future Content Centric Internet will support the content objects in order to meet their relations.

More specifically, transfer and integration of objects for the purpose of the creation of an orchestrated "Media" experience clearly demands intelligence that combines application ("Service/Media") and "Content" information. The intelligence could be embedded in the objects themselves, retrieving information from the network and providing instructions for routing and transformation, or the intelligence could be hosted in network nodes that attempt to satisfy the requests of the objects as they are described in the "Rules", "Behaviours" and "Relationships" (which take input from the "Information/Adaptation", "Content" and "Infrastructure" layers) . Finally, the "Characteristics" that meaningfully describe an object take, mainly, input from the "Information/Adaptation" layer.

3 Conclusions

Among the major reasons for the success of the Internet have been the simple networking architecture and the IP interoperation layer, which is so flexible as to support a wide spectrum of applications. However, the recent traffic measurements reveal that more and more applications target on the content that they deliver rather than the addresses of the servers who (originally) published/hosted that content.

In this paper we summarized some of the most important approaches towards a Future Media Internet architecture model. As this is a very hot-topic world-wide, this can't be an extensive list. However, it is obvious that there are many new ideas that have to be tested /evaluated towards efficiency, scalability, backwards compatibility and security before we can safely and realistically remove IP from Internet.

Acknowledge

This paper is partially based on the EC funded projects nextMedia (ICT-249065) and COAST (ICT-248036) and the work that has taken place at the European Commission Future Content Networks Group (FCN), and the Future Media Internet Architecture Think Tank (FMIA-TT), supported by the project nextMEDIA.

References

1. Jacobson V., Smetters D., Thornton J., Plass M., Briggs N., Braynard R (2009), "Networking Named Content," Proceeding of ACM CoNEXT 2009. Rome, Italy, December 2009.
2. Palo Alto Research Center, Content-centric network, http://www.ccnx.com/
3. B.Adamson, C. Bormann, M. Handley, and J. Macker. "Multicast Negative-Acknowledgement (NACK) Building Blocks". IETF, November 2008. RFC 5401.
4. T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica. A Data-Oriented (and Beyond) Network Architecture. In SIGCOMM, 2007.
5. D. Mazi`eres, M. Kaminsky, M. F. Kaashoek, and E. Witchel, "Separating Key Management from File System Security" In Proc. of SOSP '99, pages 124–139, Charleston, SC, USA, Dec. 1999.
6. M. Gritter, D. R. Cheriton "TRIAD: A New Next-Generation Internet Architecture," http://www-dsg.stanford.edu/triad, July 2000.
7. R. Moskowitz and P. Nikander, "Host Identity Protocol Architecture", RFC 4423, IETF, May 2006.
8. B. Ford, J. Strauss, C. Lesniewski-Laas, S. Rhea, F. Kaashoek, and R. Morris, "Persistent Personal Names for Globally Connected Mobile Devices" In Proc. of OSDI 2006, pages 233–248, Seattle, WA, USA, Nov. 2006.
9. H. Balakrishnan, K. Lakshminarayanan, S. Ratnasamy, S. Shenker, I. Stoica, and M. Walfish. A Layered Naming Architecture for the Internet. In Proc. of ACM SIGCOMM '04, pages 343–352, Portland, OR, USA, Aug. 2004.
10. M. Walfish, H. Balakrishnan, and S. Shenker. Untangling the Web from DNS. In Proc. of NSDI '04, pages 225–238, San Francisco, CA, USA, Mar. 2004.
11. M. Walfish, J. Stribling, M. Krohn, H. Balakrishnan, R. Morris, and S. Shenker. Middleboxes No Longer Considered Harmful. In Proc. of OSDI 2004, pages 215–230, San Francisco, CA, USA, Dec. 2004.
12. Siena (Content-based Network) http://wwwserl.cs.colorado.edu/ carzanig/siena/
13. Dmitrij Lagutin, Kari Visala, Sasu Tarkoma. "Publish/Subscribe for Internet: PSIRP Perspective. In Towards the Future Internet -- A European Research Perspective", G. Tselentis et al., Eds., IOS Press, 2010, pp. 75-85.
14. Tarkoma et al. "The Publish/Subscribe Internet Routing Paradigm (PSIRP): Designing the Future Internet Architecture. In Towards the Future Internet -- A European Research Perspective," G. Tselentis et al., Eds., IOS Press, 2009, pp. 102-11.
15. P. Jokela, A. Zahemszky, C. Esteve, S. Arianfar, and P. Nikander. "LIPSIN: Line Speed Publish/Subscribe Inter-Networking," Proceeding of SIGCOMM 2009, Barcelona, Spain, August 2009.
16. P. Ganesan, K. Gummadi, H. Garcia-Molina. "Canon in G Major: Designing DHTs with Hierarchical Structure" in ICDCS'04, 2004, pp.263-272, 2004.
17. Miller, V. S., "Use of elliptic curves in cryptography", Proceedings of CRYPTO '85: The Advances in Cryptology, August 1985.
18. D. Lagutin. "Redesigning Internet – The packet level authentication architecture." Licentiate's thesis, Helsinki University of Technology, Finland, June 2008.
19. FCN, "Why do we need a Content-Centric Future Internet? Proposals towards Content-Centric Internet Architectures," Prague, May 2009
20. Theodore Zahariadis, Petros Daras, Jan Bouwen, Norbert Niebert, David Griffin, Federico Álvarez, Gonzalo Camarillo. "Towards a Content-Centric Internet." In Towards the Future Internet -- A European Research Perspective, G. Tselentis et al., Eds., IOS Press, 2010, pp. 227-236.