Elaboration of Information and Content Centric Networking

Izzet Fatih Cetinkaya, Markus Sosnowski*
*Chair of Network Architectures and Services, Department of Informatics
Technical University of Munich, Germany
Email: izzetfatih.cetinkaya@tum.de, sosnowski@net.in.tum.de

***Abstract*—Information-centric networking (ICN) and Content-centric networking (CCN) are new architectures that aim to replace or initially support current internet protocols (IPs). Consumers no longer need to wait for a response from hosts to access information with the usage of internet protocols. ICN, speciall through CCN, resolves this waiting time by allowing the data exchange within the naming content.Based on the naming content CCN additionally offers safer architecture for consumers by using cryptography in searched content.In this paper we aim to explain the backstory and the primary working structure of ICN/CCN. Furthermore, we give a small example of an existing tool based on CCN working principles which also aims to explain how CCN can operate and compare CCN and IP in three categories.**

***Index Terms*—content-centric networking, information-centric networking, forwarding,internet protocols.**

1. Introduction

The current internet protocols (IPs) ,due to security reasons and slowleness caused by host to host information exchange, are no longer sufficient enough to meet today's demand to reach information faster. Therefore we needed new protocols which could replace IPs or change the way they are operating. In classical IPs, information location and how it is distributed to consumers are the key elements of data distribution. Hence, we need to rely on pipelines and local hosts more than the content we are looking for. However, at the beginning of 2009, researchers in Pao Alto, United States, created another networking architecture that can answer the need for fast and secure information more efficiently [1]. The new architecture is called information-centric networking (ICN). The difference between IPs and ICNs is heavily based on the concept of their working mechanism. While IPs are relying on the host information and *how* they are shared with consumers, in contrast, ICNs are based on the name of the content and *what* is delivered to consumers [1]. Thus, ICN allows reaching information much faster and more secure than IPs thanks to avoidance of host data, which can contain malicisous threads, and caching information to reuse later [2] [1]. This new information-based architecture consists of different sub-structures and sub-architectures. The most used among the new ICN is content-centric networking (CCN). The reason CCN is a more common approach than others is that CCN has an effective way of data exchange. In other words, CCN enables the information exchange between users only on the content that they are looking for. Hence, information flow does not depend heavily on the layer protocols. In this paper, we are going to explain the back story of ICN and CCN in Section 1 briefly, and then we are going to elaborate on the current working structures of CCN with detailed information in section 2. Furthermore, we are going to give an example of a tool that aims to explain how CCN works and in the last section, we are going to compare IPs and CCN in three different categories, where CCN is offering consumers better usage.

2. Background of ICN and CCN

ICN was created to accelerate current internet protocols more efficiently and securely. Hence ICN offers a shift from "Host Centric Network" to "Information-Centric Network." [3]. What does this shift mean? The classical approach of internet protocols (IPs) is based on the host data, which is essential to know where the data storage, that was restricted into four layers; Application Layer (HTTP), Transport Layer (TCP), Network Layer (ISO 7498/4) and Link Layer (Ethernet). However, in ICN, Host-data plays an insignificant role in determining requested information. In contrast, the ICN approach is more in which data has been requested from the consumers. Therefore we can eliminate the long wait time, which IPs are based on, with the help of information-centric networking.ICN has several approaches like Named Data Networking (NDN) [4] or Data-Oriented Networking Architecture (DONA) [5]. NDN is Content-Centric Network (CCN) based architecture. What we mean by based architecture? When NDN is first used, the working priciples and structure were build upon the CCN's working structure [4]. For example, NDN also uses interest and data packets for information exchange,for a more detailed explanation of interest packets (section 3). DONA is, on the other hand, created to accelarete existing application and try to improve security. DONA's working principles aim to change domain name system (DNS) names with flat names, self-certified names (section 3), and DNS name resolution with name-based anycast primitive that lays above IP layer [5]. DONA also improves data retrieval by providing more coherent support for persistence, authentication, and availability [5]. But, CCN is still one of the most common approaches of ICN architecture. While the conception of data request switched to content based rather than the host location, CCN has significant advantages in compare to DONA, to answering the need for ICN by replacing IP Layers.The reason is CCN is the key and common approach of ICN that CCN is more adaptable to

doi: 10.2313/NET-2023-06-1_01

new environments and being able to provide better caching and naming in multicast traffic in compare to DONA and NDN [2]. Thus, CCN has the upper hand in comparison to other approaches like Named Data Networking (NDN) [4] or Data-Oriented Networking Architecture (DONA) [5]. Additionally, in some cases, CCN has been considered that is not precisely replacing layer 3 (ISO 7498/4) but plays an additional role in speeding up the resulting process [1].

3. Basic Concept of CCN

As we briefly explained in section 2, ICN based architecture CCN can be more efficient approach to exchange information between providers and consumers. In this section, we elaborate on this efficient approach, which can create switch from IP to CCN with a clear concept of CCN. In order to point out the working mechanism and structure of CCN, the main part of our illustration of structure is based on the new working principles of CCN, which is information exchange within packets or, in other words, faces. CCN data exchange consists of two main bodies, and these are *interest packets* and *data packets.* The interest packet consists of three main layers, which are *content name selector,* and *nonce* [1]. The data packet, however, consists of four layers, those are *content name, signature, signed info* and *data* [1] [2]. As we can clearly identify, the key indicator for both packets is the content's name. Even though both packages contain the same content name as the vital unifier for packets, their core roles are not overlapping but rather complete each other. In other words, the interest packet's name contains the requested information by consumers or CCN nodes, and data packets have the corresponding information from servers or hosts [2].

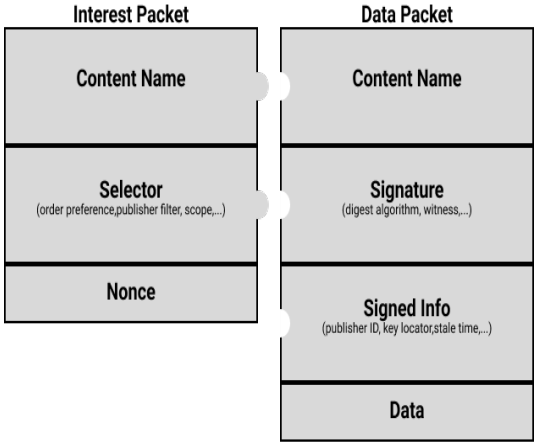

Figure 1: CCN Package Layers [1]

In figure 1 and figure 2 are visualising the interest and data packets.After visualisation of the packets, we can touch the content of the each layer. The content name layer contains a sequence of name components [4].The signature is defined in two different parts; firt one is signature-info, which indicates digitial signature algorithm and relavent information in local certificate.Second one is signature-value that hold the bits of the signature [4]. Last but not least Nonce is used to carry randomly generated long byte-stting [4]. Additionally, figure 2 shows IP layer

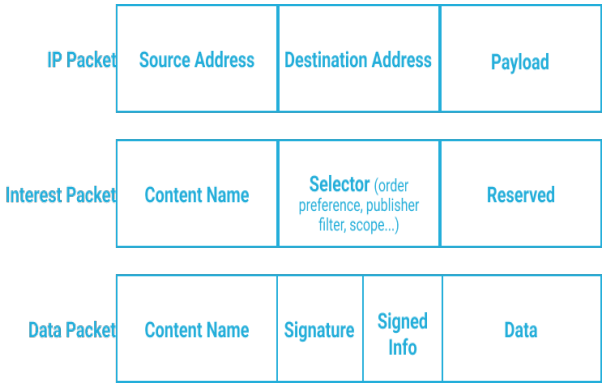

Figure 2: CCN and IP Package Layers Comparison [2]

distribution compared to CCN, which helps us see how content-centric networking differs from current internet protocols.

After we explained the two central bodies of the CCNs, we also want to point out how this mechanism works and how those main strategies support Content Centric Networking.

The main working mechanism that CCN is built upon is the following strategies:

3.1. *Forwarding*

The forwarding strategy is one of the key elements of CCN to transfer data from sender to receiver or receiver to sender. Forwarding has three essential sub-structures:

- Pending Interest Table (PIT)
- Forwarding Information Base (FIB)
- Content Store (CS)

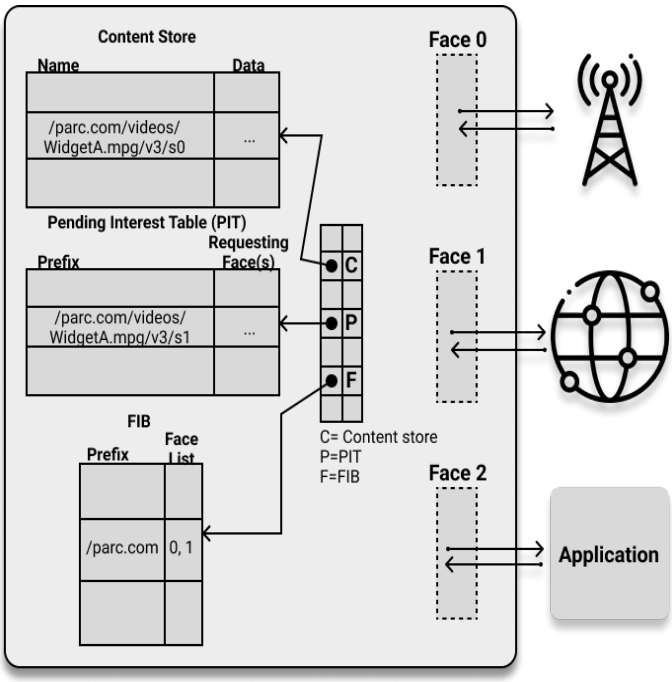

Figure 3: Forwarding structure [1]

In figure 3 it can be seen that each of the three sub-structures works alone or with other structures. In the

doi: 10.2313/NET-2023-06-1_01

first step of cooperation work, requests are created by the receivers as following interest packets sent to corresponding faces (PIT). In the second step, FIB transfers the information to potential matching data, which will collect the related data and send it back to the receiver, and in the mean time, CS stores founding data in its storage in order to create a faster response in the future. In [1] the whole process and detailed explanation of each step can be seen better.

3.2. *Naming*

The main concept of Content-Centric architecture is naming the content directly. “Then, publishers place it in the network where it is replicated in caches” [2]. Thanks to the naming strategy, it allows publishers and receivers to have a more secure, more flexible, and more scaleable CCN. In [6] Ghodsi et al. explained how the CCN Naming works. In our structural explanation, we want to also point out two main approaches to Naming. These are hierarchical naming and flat naming. Although they are both responding to the naming process of CCN, they have slight differences. While Hierarchical naming ensures that the content name can be human readable, Flat naming provides self-certified naming. In figure 4 the main differences can be identified better, in order to understand which of the naming approaches are used where. Additionally, figure 5 shows how the structural concept of the two naming approaches works.

Scheme	Advantages and Limitations
Hierarchical Naming(Human readable)	+While the crytofraphic algorithms evolve it remains unchanged, more backwards compatible and more usable +Hierarchical names ensure scalability -Provides low intrinsic binding -Provides an imperfect binding between names and publishers. -Reduces the flexibility of trus mechanisms
Flat Names(Self-certified)	+The intrinsic binding between names and key is crytographically tight, clean and algorithmic that is understandable by the network +Can deal with service deny -Impossible to have an aggregation that provides scalability -Requires another translation service between human names and self-certified names, which reduces security

Figure 4: Naming Comparison [2]

3.3. *Caching*

Caching is also one of the conspicuous structures of CCN. Caching structure is heavily correlated with Forwarding due to the nature of Caching. Caching’s working principle is transferring data from buffer memory, which is holding information temporarily, to cache space memory, where it can be stored for a longer time. This is also to process of Content Store (CS) (see Section A). Thanks to caching, in event of a data request from a consumer, FIB does not require to go to different servers to find

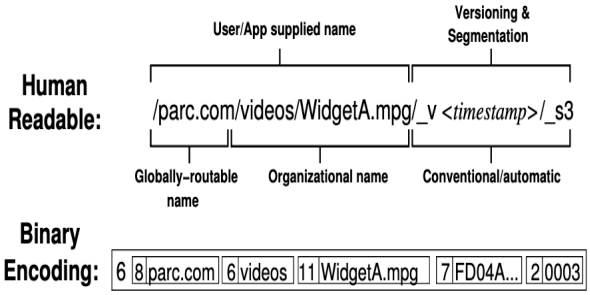

Figure 5: Naming data structure [1]

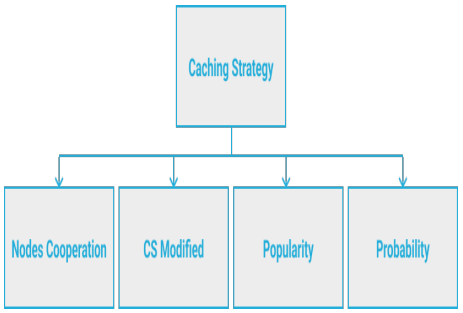

Figure 6: Caching Strategy Layers [2]

information. Instead, it can use the stored data in caching to respond to requests.

In figure 6 various different caching strategies can be seen, which are segmented into four main layers and sublayers.In Nodes cooperation caching, information that currently cached will be shared with neighbour cache [2]. Following cache strategy (CS) suggest that proactive mechanism can be used as an additional modul [2]. In the third CS data packet processing is focused [2]. And in the last one higher cache hit is the key indicator [2].

3.4. *Security Mechanism*

Security structure is based on four main components; those are confidentiality, provenance, integrability, and availability [2]. Thanks to these components, CCN eliminates malicious threads, one of the IP’s main security threats. "In CCN, all content is authenticated with digital signatures, and private content is protected with encryption. This is a critical enabler for CCN’s dynamic content-caching capabilities. If you are to retrieve content from the closest available copy, you must be able to validate the content you get" [1].Hence, CCN enables secure and trustable internet to consumers.

In [1] content-based security more details are explained with experiment. Which helps to elaborate, how CCN can be safer than IPs.

3.5. *Monitoring*

While CCN allows consumers to request data simultaneously, Monitoring needs arise with these simultaneous actions. The main task of Monitoring is enhancing the data that has been transferred to protect CCN from attacks

doi: 10.2313/NET-2023-06-1_01

[2]. The enhancing mechanism works as following; Monitoring captures and analyses the information concerning content distribution flows [2]. In papers [7], [8] different tools have been provided to us for Monitoring.

4. An Existing Tool for CCN

In this section, we want to give a small example of CCN based tool [3], which helps us to understand how CCN works. CONET: A Content-Centric Inter Networking Architecture aims to provide consumers with named data rather than host data [3]. By doing so, CONET either replaces existing IPs with additional noted IPs that make them content aware, or creates new CCN-based networking that can conduct data requests with content-name-based architecture.

In figures 7 and 8, CONET's architecture and primary working packet system can be seen.

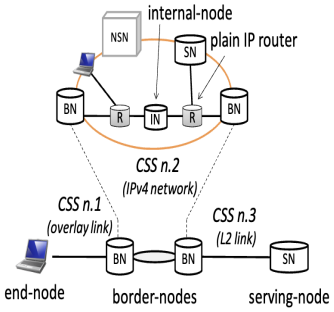

Figure 7: CONET Architecture [3]

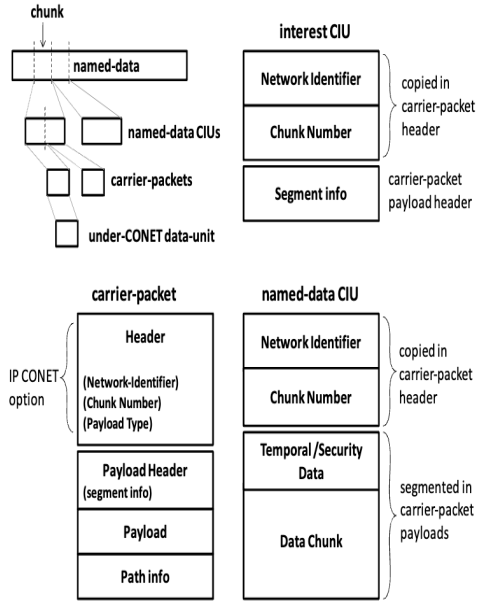

Figure 8: CONET Information Unit [3]

5. Comparison and Discussion

In our last section, we aim to point out three categories where CCN has the upper hand compared to IPs.These are Availability, which we also mentioned (see section D), Security, and Location dependence. We want to start with the one we think, where CCN resolves so many issues compare to IP and this is Security.

- CCN's core structure relies on the data transfer on the content name. Therefore transferred data is no longer a property of pipelines that move data from one another without caring about the content itself but focusing on the data holders. " In CCN, all content is authenticated with digital signatures, and private content is protected with encryption" [1]. Thus, CCN provides a more robust security system for malicious attacks on data transactions. Another defining characteristic of CCN's security is "Key Handling" (Trusting Key). In [1] it is explained under three sub-categories, which are keys directly addressed to the problem, second publishing only one key, and third CCN is not empowering one key for all sizes but it creates trust between publishers (senders) and consumers (receivers).
- The second category that we want to compare CCN with IP is Location dependence. While ICN and CCN are not relying on the host locations and connections between hosts. This independence allows CCN to operate easily without being restricted by internet protocols. Thus, CCN-requested data engages with the consumers faster, and the information is more reliable.
- Last but not least, Availability. CCN's availability is greatly based on the CCN's flexibility. More like location dependency, requested data is not bonded to any host location. Hence, in the case of data requests, contented data can be transferred flexibly to one another. Availability allows CCN to provide more reliable data to consumers.

6. Related work

Content-centric networking is still growing in architecture that is not fully established yet. Therefore there are many ongoing surveys, experiments, and collaborations with other tools. For example, Ahlgren et al. [9] tackle the design choices of ICN and, respectively CCN. In another example, Nakamura et al. [10] focus on how ICN will cooperate in the event of network failure. Even though ICN is offering more sustainable data exchange, it does not entirely eliminate the risk factor of failure, but it decreased significantly. The findings of the [10] indicate thanks to ICN topology, in case of network failure, ICN still operates more efficiently than old internet protocols due to selective node removal. Ghali et al. [11] handle the possible problems with the high usage of CCN. While security is among the key aspects of CCN, this paper should be mentioned in our writing to underline CCN security.

doi: 10.2313/NET-2023-06-1_01

7. Conclusion

In conclusion, we tried to elaborate why ICN and CCN are replacing or accelerating current Internet Protocols. Additionally, we elaborate on the current state of CCN and how CCN is structured. By doing so, we briefly mentioned five critical structures of the CCN. So we could understand the CCN process better. Furthermore, we give an example of a tool that operates under CCN protocols and underline three aspects where CCN works better than IP. As a result, we can say that CCN has significant advantages in security, flexibility, and mobility, which can make CCN more reliable and more demanded in the near future.

References

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, ser. CoNEXT '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 1–12. [Online]. Available: https://doi.org/10.1145/1658939.1658941

[2] R. Jmal and L. Chaari Fourati, "Content-centric networking management based on software defined networks: Survey," *IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1128–1142, 2017.

[3] A. Detti, N. Blefari Melazzi, S. Salsano, and M. Pomposini, "Conet: A content centric inter-networking architecture," in *Proceedings of the ACM SIGCOMM Workshop on Information-Centric Networking*, ser. ICN '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 50–55. [Online]. Available: https://doi.org/10.1145/2018584.2018598

[4] L. Zhang, "Named Data Networking (NDN) Project," *NDN-0001 October 31, 2010*, vol. 25, no. 26, pp. 1–18, 2010.

[5] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," vol. 37, no. 4, 2007. [Online]. Available: https://doi.org/10.1145/1282427.1282402

[6] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker, "Naming in content-oriented architectures," in *Proceedings of the ACM SIGCOMM Workshop on Information-Centric Networking*, ser. ICN '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 1–6. [Online]. Available: https://doi.org/10.1145/2018584.2018586

[7] W. Kang, B. Sim, J. Kim, E. Paik, and Y. Lee, "A network monitoring tool for ccn," in *2012 World Telecommunications Congress*, 2012, pp. 1–3.

[8] D. Goergen, T. Cholez, J. François, and T. Engel, "Security monitoring for content-centric networking," in *Data Privacy Management and Autonomous Spontaneous Security*, R. Di Pietro, J. Herranz, E. Damiani, and R. State, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 274–286.

[9] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, 2012.

[10] R. Nakamura and N. Kamiyama, "Analysis of content availability at network failure in information-centric networking," in *2020 16th International Conference on Network and Service Management (CNSM)*, 2020, pp. 1–7.

[11] C. Ghali, G. Tsudik, and E. Uzun, "In content we trust: Network-layer trust in content-centric networking," *IEEE/ACM Transactions on Networking*, vol. 27, no. 5, pp. 1787–1800, 2019.