Recent Advances in Information-Centric Networking

Qihang Huang (A paper written under the guidance of Prof. Raj Jain)

Abstract

After so many years of development of Internet architecture, people are paying more and more attention to the function and security of Internet architecture. Today, the Internet architecture we are most familiar with can no longer meet our needs. Therefore, the architects proposed information-centric network architecture and introduced it into the network field. The information-centric network is a new network architecture that realizes the identification of each piece of information through the name of the information. Through ICN, the content will be independent of physical location, and any node in ICN can act as a producer to generate content. In recent years, many ideas about ICN have been put forward. Still, the goal of ICN is unified and straightforward, that is, to provide a more efficient network architecture to promote content distribution to users, improve network security, and solve large-scale network scalability and Simplify distributed applications. This article will discuss the advanced technologies recently built in the ICN architecture, including discovering content and network information in Content-Centric Networks, LoWPAN network.

Keywords

Information-Centric Networking, ICN, Content-Centric Networking, CCN, CCNinfo, Future network architecture, LoWPAN Networks, ICN security

Table of Content

1. Introduction

More and more people use today's Internet architecture, and architects have discovered that it contains a lot of problems. Like our society, the Internet also needs improvement and development. The current Internet architecture is a point-to-point connection communication based on data packets between each terminal. Therefore, if there is no host, people cannot directly obtain information. With the massive increase in communication services such as voice calls and real-time video, the capabilities of the Internet have been challenged due to the inherent architecture of TCP/IP.

The TCP/IP network architecture makes it complicated to obtain information, a large amount of information is redundant, and resources are wasted. In the TCP/IP network architecture, information must pass through the host and convert to IP using DNS. The system has gone from simple to complex, which also proves its high complexity. In addition, security is a crucial issue. The security in TCP is not as high as we thought [Jaikumar]. The host is the content owner, and it is essential as the part responsible for transmitting the content in the TCP/IP network. Therefore, if hackers compromise the host as a single point of failure, our information will be stolen or lost. Thus, security has not yet reached a complete guarantee. This problem led to the birth of the ICN network architecture, which separates content from terminals and provides storage and multi-party communication through a publish/subscribe paradigm.

In 2012, the Internet Research Task Force (IRTF) established an ICN Research Group (ICNRG) dedicated to using ICN concepts to cooperate to solve Internet problems[Keping19]. Many ongoing ICN research projects have received support from academia and industry organizations around the world. Each research project has adopted a different method to develop the framework of the network architecture using the ICN concept. Either way, its purpose is to break the traditional host-centric network architecture. The end-to-end connection based on the content distribution architecture and uniquely named data replaces the conventional method, building a more secure, scalable, and flexible network. At the same time, it complies with and supports the connection of location transparency, mobility, and indirectness. These further improvements help users get closer to the content, and everything is information, complete information interconnection.

After several years of development, many related studies on ICN have been put forward. We will learn about various ICN projects and standards recently proposed, including discovery content and network information (CCNinfo), ICN Adaptation to LoWPAN Networks.

2. Content-Centric Networking (CCN)

Packet switching has been proposed for nearly 50 years, and it is also because this idea gave birth to our current network architecture. But on today's Internet, we communicate with each other through information and content. From a content-centric point of view, the people who

send the message, the people who receive the message, and where the sender and receiver are far less important than the information. People care about the content and don't care where the information storage server is. Therefore, a new batch of network applications was born. But they are scattered in the application layer rather than changing the network architecture. Thus, a new ICN network architecture arises with demand.

CCN, as a kind of ICN, the communication model is no longer based on the location of the network node, but the content name, and the content is implemented in a layered scheme. The primary use demand of the Internet now is the acquisition and distribution of content. Although the application has undergone significant changes, the Internet's architecture is still the Host-to-Host communication mode. The Host-to-Host communication mode has obvious shortcomings for the Internet that mainly publishes and obtains informationA [Haque13]. The primary demand of the Internet now is that users are more concerned about getting data faster, more accurately, and more efficiently. In this section, we will introduce the CCN networking architecture.

2.1 General concept of CCN

The content-centric network is also called the information-centric network. It all uses the information object as the basis for constructing the network, separating the information's location information and content identification, and obtaining data through the content name instead of the host IP address. Use a built-in network cache to improve transmission efficiency, regardless of data storage location. Request data through the publish/subscribe model to decouple the supplier and the consumer in space and time. This new network architecture focuses on information objects, attributes, and user interests and adopts the "information sharing communication model" to achieve efficient and reliable information distribution.

The naming method adopted in the CCN network architecture is hierarchical nomenclature. Similar to the expression of URL, which is string sequence, it is helpful for users to understand and remember. However, because the binding of RWI-name (Real-World Identity) is very fragile, binding the public key and name is necessary through an external trusted mechanism [Cesar16]. This method may lead to security breaches. CCN also uses unstructured routing to make it compatible with IP. Unstructured routing is similar to IP routing, and its routing announcements are mainly carried out through flooding. This routing method allows an inheritance relationship between CCN and IP to achieve easy deployment on the IP network. It uses content identifiers instead of network prefix names. Therefore, there is no need to modify too many IP routing protocols.

2.2 CCN working mechanism

Although CCN and TCP/IP are different network architectures, their architectures are very similar. As shown in Figure 1, they all have an hourglass-like architecture [Van]. However, in the CCN architecture, the network is not reached through IP packets but uses another information content name as a routing identifier. The CCN structure also contains a strategy layer and a security layer to provide strategies and provide security functions. The CCN structure no longer has the demand of the transport layer.

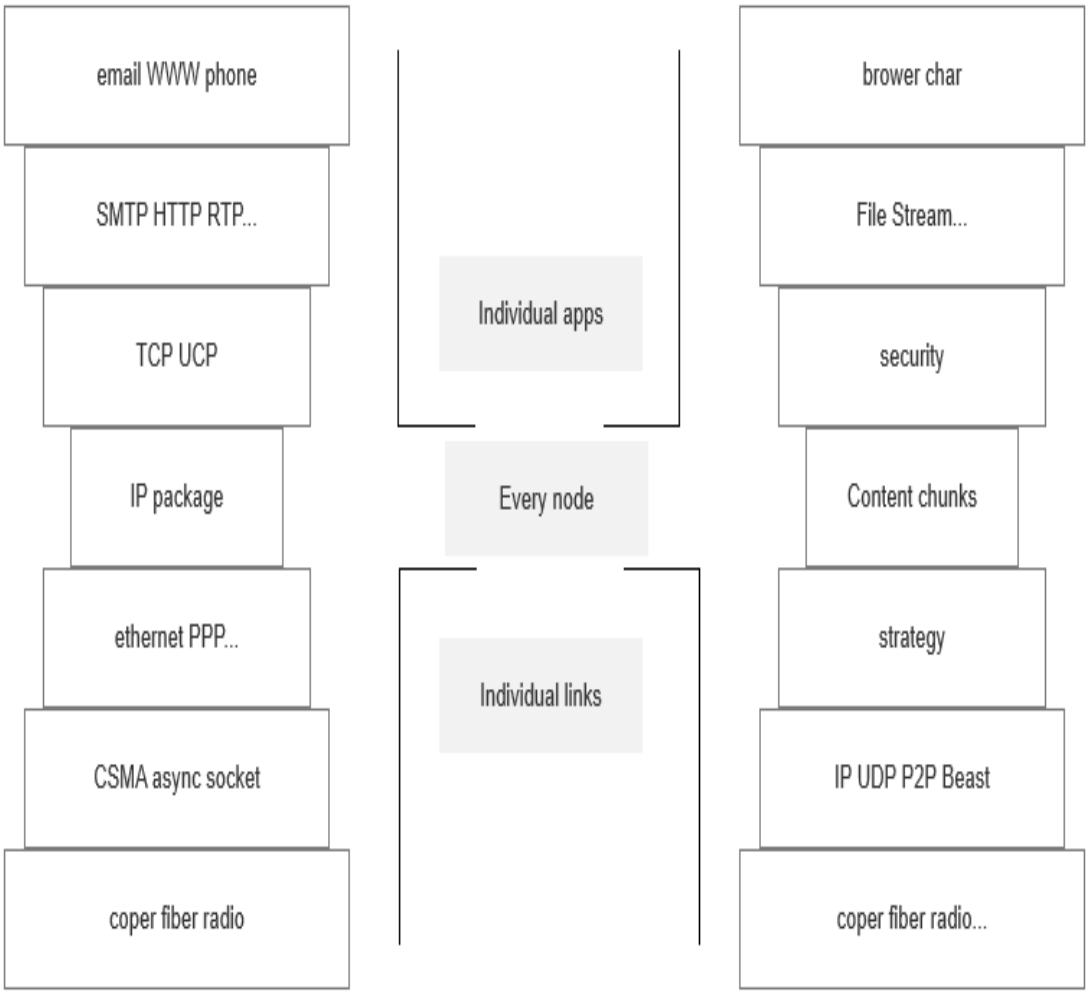

Figure 1. CCN Architecture[Fabian13]

There are only two data types in the CCN network: data packets and interest packets. The data package consists of the content name, data payload, digital signature of the content issuer, and corresponding authentication information (content issuer ID, public key, etc.). The content name is the content named in the data package. The digital signature and authentication information are used to provide authenticity authentication, integrity protection, and identity authentication of the content publisher to the content requester. The interest package is composed of content name, user options, and random numbers. User options represent the particular needs of the requester. The random number is to judge whether the received interest package has been received repeatedly. Each router has content transmission, forwarding, and caching functions to ensure the transmission of information [Fabian13].

In CCN communication, consumers reach the operation of requesting content by broadcasting interesting packages. The three data structures of Forwarding Information Basei1/4^FIBi1/4 ,

Content Storei1/4^CSi1/4 , and Pending Interest Tablei1/4^PITi1/4 are used to complete the information forwarding [Fabian13]. The router responds to the requested data by looking up the content cache. Either find the data directly in the cache or obtain the location of the data through the PIT entry and forward the request. If neither exists, jump to FIB to find the content request. In FIB, if the CCN router cannot find the information that meets the conditions, the router will terminate the request. The router also processes data packets. But in the data packet, the router does not need to look for the data in the FIB. If there is no required data in the PIT, it terminates the request and discards the data packet.

2.3 CCN security

Security is an inevitable part of any network architecture. In the CCN architecture, there are two types of privacy protection. One is cache privacy, and the other is content privacy. Cache privacy refers to privacy issues related to the router cache function in the CCN network [Cesar16a]. For example, hackers use content response time to obtain the privacy of neighboring routers. Another type of content privacy is that users themselves send requests through content, but hackers can obtain relevant sensitive information by monitoring such requests. In the face of this type of privacy attack, the CCN architecture pays more attention to protecting a single information packet than the traditional architecture. The data packet is protected by encryption, and if you encounter an unauthorized user, you will not be able to obtain the content without the decryption key. Therefore, we need to understand the way of data packet encryption to protect our information security.

The main encryption methods in the CCN network are symmetric encryption, broadcast encryption, and proxy re-encryption. The concept of symmetric encryption is to encrypt content through a user-generated key and the public key of the content publisher [Chaabane13]. When the publisher receives the information, it performs the same encryption operation and returns it to the requester. However, this encryption causes the caching mechanism in the CCN network to be disabled. This problem causes birth to broadcast encryption. Broadcast encryption uses the publisher's public key to encrypt the content and then forwards it to other router nodes. Other router nodes can store the content, but you must pass the private key owner if you need to decrypt the content [Misra13]. In this way, the number of the key is too large and affects communication. The last encryption method perfectly solves the previous problem. The proxy re-encryption requires the user's identity to be encrypted first, and then the ciphertext is re-encrypted by the proxy [Wood14]. This method only needs to store two private keys before they can be spread on the network. In addition, digital signatures provide additional security for information packets. Verify the digital signature to determine whether the owner's information has been obtained. Guarantee authenticity.

In the CCN architecture, although the safety performance has been greatly improved. It is difficult for an attacker to use existing attack methods to cause a network breakdown through many requests because abnormal requests become very obvious in CCN. The CCN network architecture is highly robust due to its multicast function and content distribution. However, the CCN network framework still has shortcomings. For example, interest packet flooding attacks, network congestion. In the CCN network, an attacker can use CCN's unique CS and PIT features to carry out a new type of DoS attack, thereby depleting the resources of the CCN router or

content publisher [Cesar16]. In addition, due to the limited resources of storage nodes, many data packets in the network may also cause network congestion and affect the network. Although the CCN network architecture characteristics have reduced information redundancy, there are still such possible problems. All in all, the security of CCN network architecture is still slowly developing and progressing under the development of researchers.

3. CCNinfo: Discover content and Network information

CCNinfo is a network tool implemented based on CCN (a type of ICN) network architecture and provides a large amount of information from CCN transponders. It can accumulate a lot of experience from the CCN network to analyze and improve the future Internet architecture. In this section, we will discuss CCNinfo type, router behavior, and security specifications.

3.1 General Concept of CCNinfo

CCNinfo, as a networking tool, is used to discover the path and content caching information in CCN. Contrace is the guardian of external processes in TCP/IP to implement such investigations, similar to the ping protocol and traceroute protocol in IP. As lightweight operation tools, Contrace can reduce the load of network operators' forwarders and protect information. In other words, the administrator can hide his information without stopping the information forwarding. Compared with TCP/IP, user safety is guaranteed under certain circumstances.

Developers of CCNinfo can quickly check information, such as the size, quantity, number of accesses, and lifetime and usage time of the cached content in the network through its feature that can identify the status of the cache. This information is within the tracking scope of CCNinfo. In addition, CCNinfo will also track the routing path information of real-time text between the content forwarder and the user and each name prefix. These information-based features reduce complexity and additional overhead. At the same time, a lot of experience was given to prepare for the improvement of CCNinfo [Hitoshi21].

3.2 Request type and Reply type

CCNinfo defines two message types. 1) Request type. 2) Reply type. In CCNinfo, both request and reply types are encoded in CCN x TLV format. Secondly, there are only two types of fixed headers: PT_CCNINFO_REQUEST and PT_CCNINFO_REPLY [Hitoshi21]. Determine whether it is the request type, or the reply type is based on the fixed header. When the request type passes through the content forwarder, you only need to change the PT_CCNINFO_REQUEST in the header to PT_CCNINFO_REPLY to convert it to the reply type and forward it again.

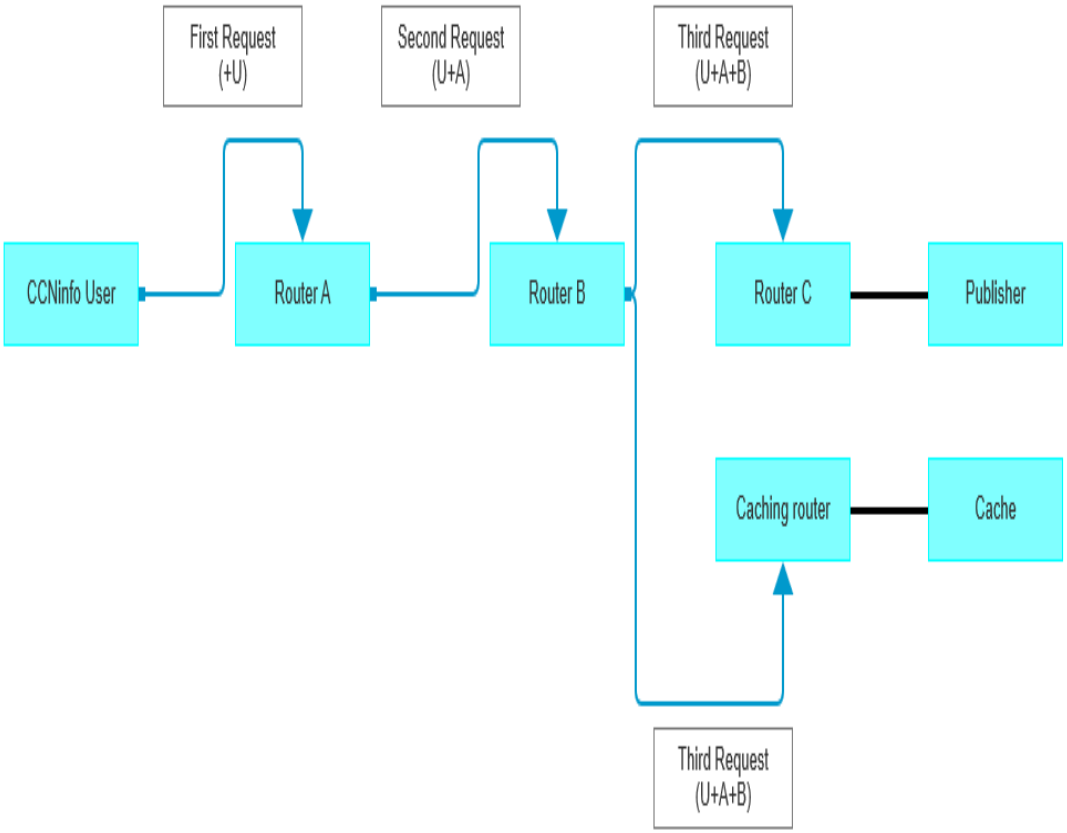

Figure 2. request message forwarded between the user and router.[Hitoshi21]

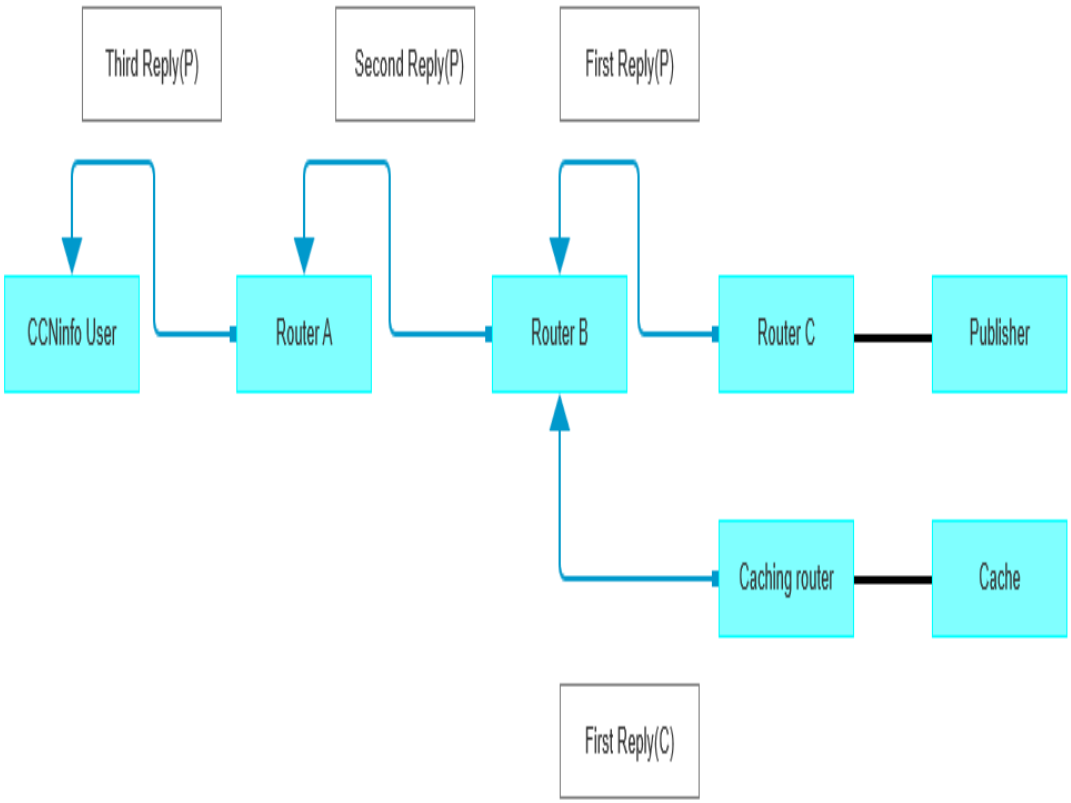

Figure 3. Reply message forwarded between the user and router (Default behavior)[Hitoshi21]

Figure 2 shows the forwarding process of the request message between the user and the router. Each forwarding will add its report block to the publisher or caching router. Secondly, modify the fixed header and return information to the user through them, as shown in Figure 3. However, when returning, the information produced by the caching router will be thrown away by router B if router B has returned the publisher's content.

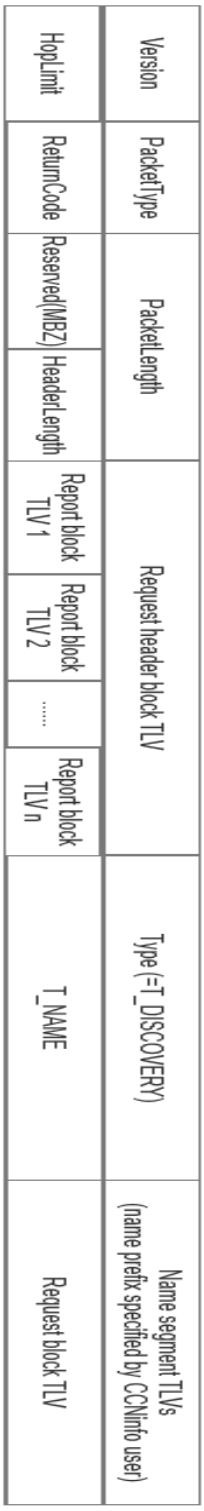

Figure 4. Request message composition[Hitoshi21]

In CCNinfo, the fixed header, request block TLV, report block TLV, and name TLV form a request message, as shown in Figure 4. When a CCNinfo user requests via the CCNinfo command, a fixed header with PT_CCNINFO_REQUEST will be generated. In this request message, HopLimit (on the lower left of table) will determine how far our request message can be forwarded. It occupies 8bit in this request message. Every time a request is delivered, HopLimit will be reduced. The upstream router that is the furthest away will stop tracking and modify the information into a reply message and send it back to the original user.

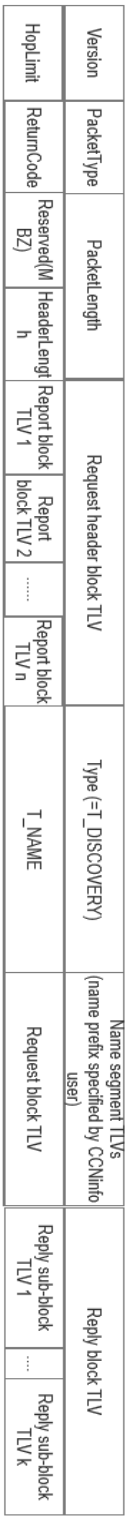

Figure 5. Reply message composition[Hitoshi21]

Compared with the request message, the reply message adds a reply block, as shown in Figure 5 (right part of the figure). After receiving the request from the neighboring router, modify it. As mentioned before, change the fixed header to PT_CCNINFO_REPLY to identify the router. After the modification, the router that owns the content inserts its unique reply block and returns to the CCNinfo user step by step. At the same time, after the user receives the reply, it needs to match the request ID and the node identifier. Otherwise, it will drop the response received this time.

3.3 Router Behavior

As the main transmission node, the router needs to filter many requests and forward them. CCNinfo follows the forwarding request of neighboring nodes. Therefore, when a request from a neighboring node is invalid, the router needs to remain silent and ignore the request or reply. This way guarantees the flexibility of the router to the greatest extent. In addition, the router follows the HopLimit rule and does not forward when its value is 0. Therefore, the router always needs to check its HopLimit and SkipHop values. When the value of SkipHop is greater than the value of Hoplimit, the router will terminate the request and cause a timeout instead of returning.

Flag	Value	Description
C	0	Path discovery(i.e., no cache information retrieved)
C	1	Cache information retrieval
O	0	Request to any content forwarder
O	1	Publisher discovery(i.e., only FHR can reply)
F	0	Request based on FIB's strategy(default)
F	1	Full discovery request. Request to possible multiple upstream routers specified in FIB simultaneously
V	0	No reply validation(default)
V	1	Reply sender validates Reply message

Figure 6. Flag field with codes and type specified[Hitoshi21]

In CCNinfo, the router distinguishes the requested information based on the Flag field in the request block, as shown in Figure 6. C and O represent cache information discovery and publisher discovery, respectively. The remaining characters represent the routing path information discovery. Figure 7 shows the judgments made by routers in different Flag fields.

There are two main situations. Checking FIB and CS or checking First-hop router (FHR) depends on the Flag field. Information uses routing to determine whether to return or forward. Routing has a flexible mechanism to determine the requested information.

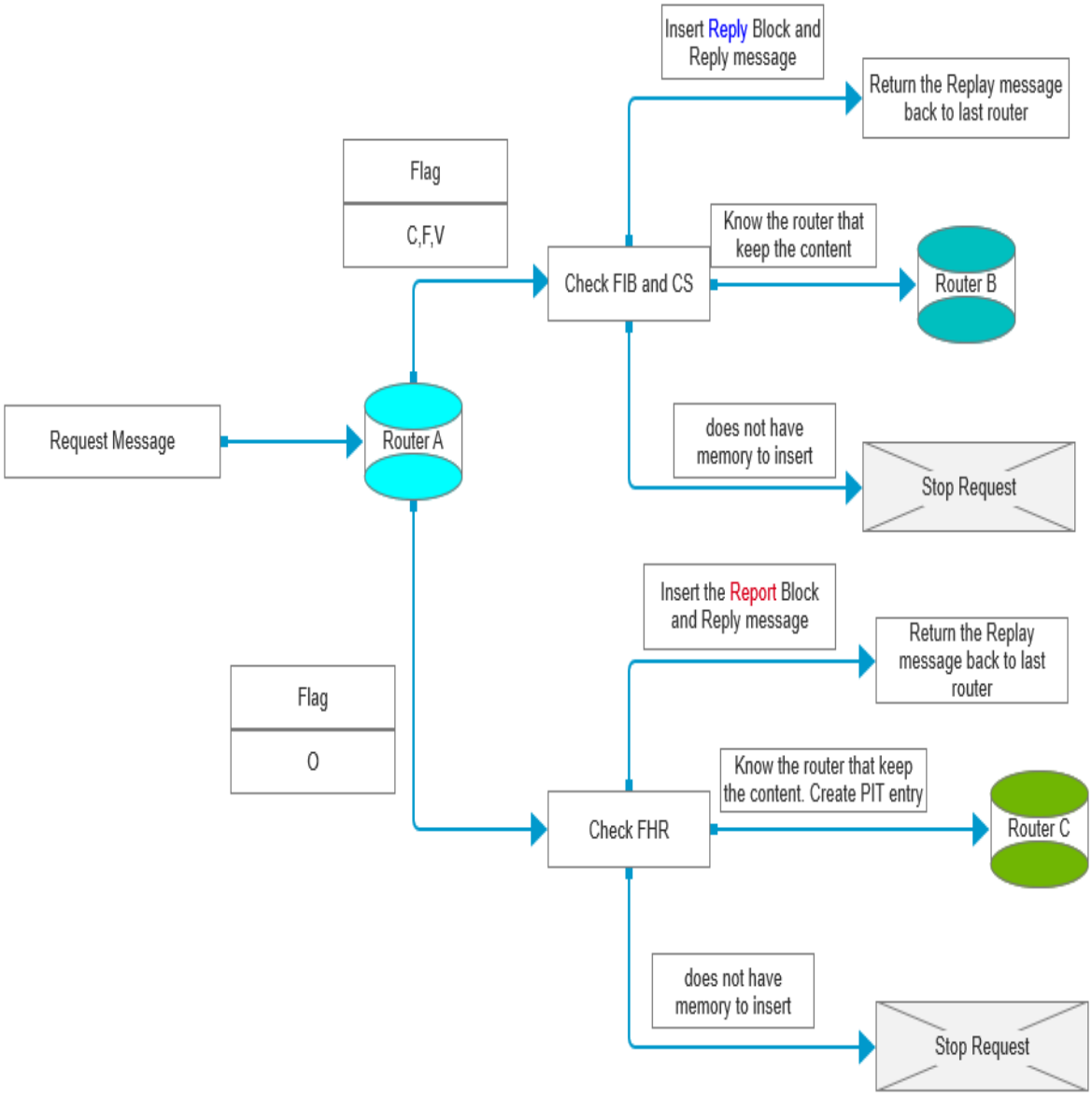

Figure 7. the path of different flag field

In the first case, when checking FIB and CS, the router will check whether it has the requested content. If it has the content, it will insert its reply block and return the reply message. It will terminate the request if it cannot insert its reply block or reply message (no space). If the router

does not contain this information but knows where it is stored, it will insert its report block and forward the request to the target router. If both conditions do not satisfy, the router will terminate the request.

In the second case, the router will check whether it is the FHR requesting the content. If it is an FHR with content, it will insert its report block and reply message. Suppose the router is not the FHR that contains the requested content, but it knows the target router. It will create a PIT entry, insert it into its report block and forward it to the target router. Similarly, if the router cannot insert its report block, it will terminate the request as before.

All in all, the CCNinfo tool can ensure the correct forwarding of information through the Flag field. It also completes the self-checking of routing. At the same time, this judgment method can also provide a reasonable allocation of routing resources to avoid congestion or other security problems.

3.4 Security specifications

Although CCNinfo improves security based on ICN, there may still be security vulnerabilities in the application layer. Therefore, CCNinfo provides an excellent diagnostic analysis method: 1.) Number of Hops and RTT 2.) Caching Router Identification 3.) TTL or Hop Limit 4.) Time Delay 5.) Path Stretch 7.) Cache Hit Probability [Hitoshi21].

Security issues are not completely manifested between the request and the reply. Some administrators do not want to display network information, so CCNinfo also gives administrators the power to create a strategy for each router to forward response information. The administrator can let the router check the signature to determine whether to return specific information or refuse to reply to the detailed information through the return code with ADMIN_PROHIB.

CCNinfo can also identify the importance of information through content characteristics, and at the same time, treat it as the return code of ADMIN_PROHIB to limit the request. At the same time, to protect the content transponder, CCNinfo allows the content transponder to hide some calculated values to ensure that the content transponder will not take on heavy tasks.

4. ICN Adaptation to LoWPAN Networks

Due to the huge difference between IoT devices and devices running on the traditional Internet, IoT applications' technical issues and challenges require in-depth research. Compared with the conventional Internet communication technology, the ICN network has more advantages in infrastructure-free access, flexible forwarding, and data replication. The introduction of a lossy radio link in the low-power Internet of Things increases its transmission cost. Appropriate LoWPAN can bring great help to solve the problem of exchanging messages through low-power wireless links under lossy conditions. As a link layer, LoWPAN improves the actual performance of the ICN network. It introduces the definition framework to realize the combination of communication technology and wireless network and solves the problem of essential adaptation.

4.1 Header Compression

Interest and data messages in CCN are composed of Type-Length-Value (TLV) fields. However, in a restricted network environment, the standard header is cumbersome and unsuitable for this type of network environment. Therefore, LoWPAN proposes two compression schemes to achieve header adaptability. One is stateless header compression, and the other is stateful header compression [Cenk18]. In the stateless header compression scheme, LoWPAN can delete the TLV structure and re-encode the header. As shown in Figure 8, the example uses a compact bit method to compress the header. In the variable-Length TLV, part of the Type is deleted. The second is Fixed-Length TLV, so the Type and Length fields are also removed. The third representative is the part of Boolean TLV, where this part is completely deleted to compress the header.

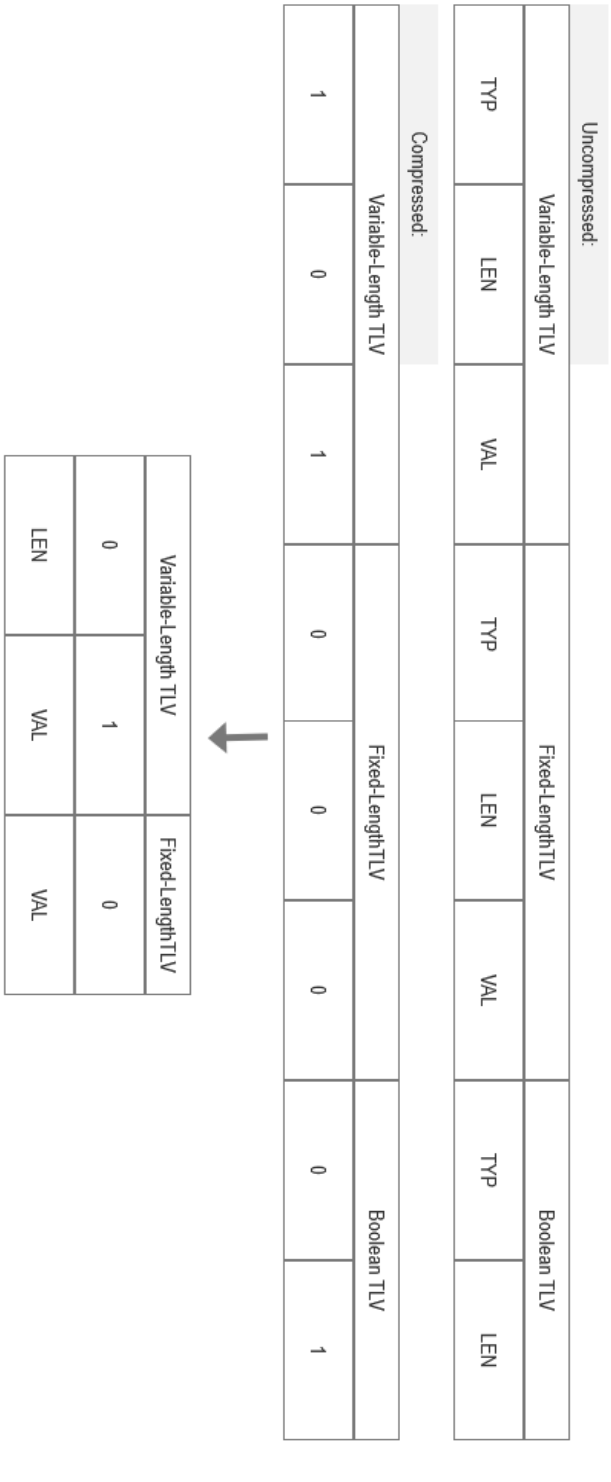

Figure 8. Compression using a compact bit field[Cenk21]

The other is stateful header compression, as shown in Figure 9, which uses context identifiers to replace duplicate information or common information-for example, the prefix and suffix in the header. The context identifier is shared by the sender and receiver and occupies 7 bits. If there is a most significant bit, it must be followed by a context identifier. Because the context identifier is in a shared state, the sender will delete it before sending it and reinsert it after the receiver receives the information. Stateful header compression can also reduce redundant storage by converting the link-local HopID to the original name header. Obtain the HopID as needed until all ID bits in the header are converted to 0. The HopID can be invalidated. But at the same time, to ensure the validity of HopID, HopID is recorded as HIDi and HIDo in PIT. Hopi is used to replace HopID, and Hopo is used to verify correctness [Cenk21].

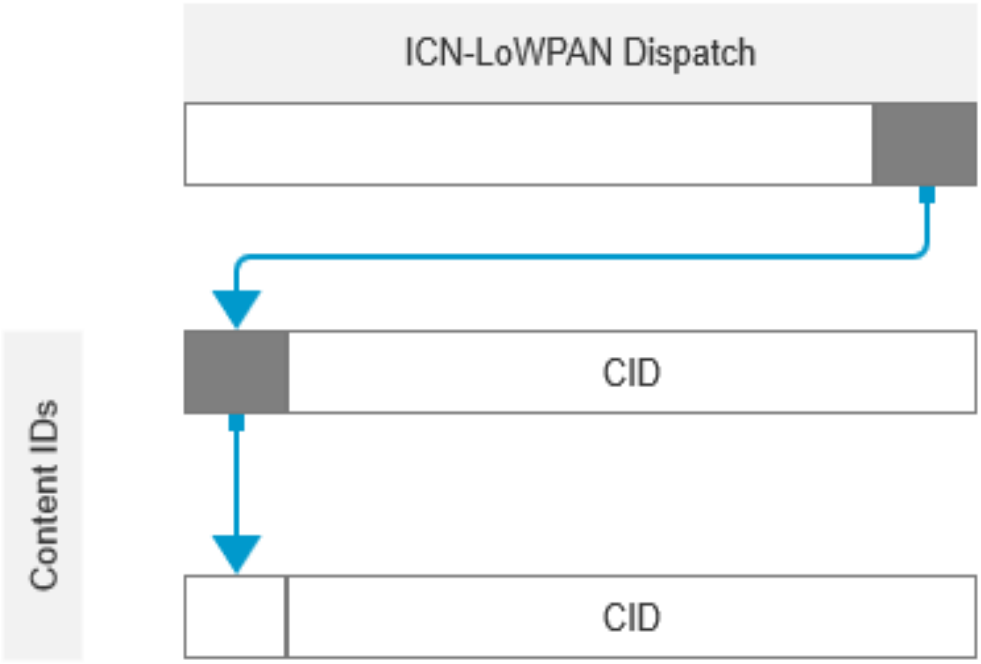

Figure 9. Header compression using LoWPAN-local state

4.2 Security Consideration

The most scarce resource in a constrained network is storage. In LoWPAN, data fragments need to wait for all received before they can be reorganized or deleted. If the buffer is already saturated, the remaining recipients cannot accept the remaining data fragments together. This problem will cause the loss of essential data and may lead to uncorrectable errors. Therefore, for safety reasons, users need to consider the replacement of the buffer to prevent saturation of the buffer and ensure that the data can be obtained entirely. In addition, users also need to consider appropriate access protection mechanisms deployed at the link layer. This method can prevent the problem of forged fragments or Interest initiations. If this factor is not considered, it may

cause HopID to be abused and exhausted, causing the recipient to refuse to accept subsequent data content. For example, IEEE 802.15.4 provides protection frames and restricts them to the function of a point-to-point link or a group of devices.

5. Summary

After the traditional Internet has been used for so long, people are paying more and more attention to the problems that arise. The ICN network architecture is slowly maturing as the most likely future network architecture. Although the ICN network architecture has not yet been built on our Internet, its technology is now slowly catching up and no longer stops theoretical ideas. New research projects such as CCN network, CCNinfo tools, and LoWPAN will all be on the cusp of the Internet over time.

As CCN technology matures, it is now also used in many private architectures. For example, audio conference tools and so on [Zhenkai11]. In addition, the security technology in CCN has become a research hotspot in the field of future networks. Under the impetus of the researchers, the three aspects of privacy protection, DoS attacks, and congestion control in CCN have some analysis and discussion results. However, there are still shortcomings in the existing research results, so many critical issues still need to be further studied in-depth and in detail.

The goal of the CCN framework is also to build on our Internet, so various application-level technologies are indispensable. Application tools like CCNinfo also help to collect more experience with CCN framework data. Researchers unanimously recognize the practicality of CCNinfo technology. The investigation of caches and paths by such tools is an indispensable part of the research network. The maturity of these application tools has laid the foundation for building the ICN framework.

Consider the Internet of Things as the most popular field nowadays. Among them, the problems of the restricted frame and the high transmission cost have benefited from developing the ICN framework. ICN is a framework designed as fixed network infrastructure. The design of LoWPAN gives the possibility to build the ICN framework on the Internet of Things. Although it is still in a state of research, as R&D personnel has a deeper understanding of the ICN network, the remaining obstacles will be overcome over time. In the end, these Internet technologies will benefit the entire human society.

6. Reference

[Bastiaan20]	Bastiaan Wissingh, Christopher Wood, Alex Afanasyev, Lixia Zhang, David Oran, Christian Tschudin, "Information-Centric Networking (ICN): Content-Centric Networking (CCNx) and Named Data Networking (NDN) Terminology", IETF, June 17, 2020 , https://datatracker.ietf.org/doc/rfc8793/
[Cenk18]	Cenk GundoAYan, Peter Kietzmann, Thomas C. Schmidt, Matthias Wahlisch, "ICN-LoWPAN: Header Compression for the Constrained IoT", 2018, https://conferences.sigcomm.org/acm-icn/2018/proceedings/icn18posterdemo-final1.pdf

[Cenk21]	Cenk GundoAYan, Thomas Schmidt, Matthias Wahlisch, Christopher Scherb, Claudio Marxer, Christian Tschudin, "ICN Adaptation to LoWPAN Networks (ICN LoWPAN)", September 29, 2021, https://datatracker.ietf.org/doc/draft-irtf-icnrg-icnlowpan/
[Cesar16]	Cesar Ghali, Gene Tsudik, Christopher A. Wood, "Network Names in Content-Centric Networking", 2016, https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2013-02-1/NET-2013-02-1_06.pdf
[Cesar16a]	Cesar Ghali, "Security and Privacy Issues in Content-Centric Networking", 2016, https://escholarship.org/uc/item/68q6z2w6
[Chaabane13]	Chaabane A, de Cristofaro E, Kaafar M A, et al. Privacy in Content-oriented Networking[J]. ACM SIGCOMM Computer Communication Review, 2013, 43(3): 25-33.i1/4OE http://www.sigcomm.org/sites/default/files/ccr/papers/2013/July/2500098-2500102.pdf
[Fabian13]	Fabian Oehlmann, "Content-Centric Networking", 2013, https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2013-02-1/NET-2013-02-1_06.pdf
[Haque13]	M. Ul Haque, A. Willig, K. Pawlikowski and L. Bischofs, "Name-based routing for information centric future internet architectures,"A 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN), 2013, pp. 517-522. https://ieeexplore.ieee.org/document/6614874
[Hitoshi21]	Hitoshi Asaeda, Atsushi Ooka, Xun Shao, "CCNinfo: Discovering Content and Network Information in Content-Centric Networks", IETF, July 27, 2021, https://datatracker.ietf.org/doc/draft-irtf-icnrg-ccninfo/
[Jaikumar]	Jaikumar Vijayan, "TCP security hole may be more dangerous than first thought",https://www.computerworld.com/article/2591808/tcp-security-hole-may-be-more-dangerous-than-first-thought.html
[Keping19]	Keping Yu, Suyong Eum, Toshihiko Kurita, Qiaozhi Hua, Takuro Sato, Hidenori Nakazato, Tohru Asami, Ved P. Kafle, "Information-Centric Networking: Research and Standardization Status" , IEEE, 2019,https://www.researchgate.net/publication/335513098_Information-Centric_Networking_Research_and_Standardization_Status
[Marc19]	Marc Mosko, Ignacio Solis, Christopher Wood, "Content-Centric Networking (CCNx) Messages in TLV Format", IETF, July 09, 2019, https://datatracker.ietf.org/doc/rfc8609/
[Misra13]	Misra S, Tourani R, Majd N E. Secure Content Delivery in Information-centric Networks: Design, Implementation, and Analyses[C]. the 3rd ACM SIGCOMM workshop on Information-centric networking, 2013: 73-78. , https://conferences.sigcomm.org/sigcomm/2013/papers/icn/p73.pdf
[Van]	Van Jacobson, Diana K. Smetters, James D. Thornton, Michael Plass, Nick Briggs, Rebecca Braynard, "Networking Named Content", http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0BB6375A98CFFACBCD693CCC0876E083?doi=10.1.1.642.2386&rep=rep1&type=pdf

[Wood14]	C A. Wood, E. Uzun. Flexible end-to-end content security in CCN[C]. Consumer Communications and NETWORKING Conference. IEEE, 2014:858-865. , https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.708.6919&rep=rep1&type=pdf
[Zhenkai11]	Zhenkai Zhu, S. Wang, X. Yang, V. Jacobson, and L. Zhang. Act: An audio conference tool over named data networking[C].ACM Sigcomm workshop ICN'11, August 2011i1/4OE https://conferences.sigcomm.org/sigcomm/2011/papers/icn/p68.pdf

7. List of Acronyms

CS	Content Store
CCN	Content-Centric Networking
CCNx	Content-Centric Networking Architecture
FHR	First-hop router
FIBs	Forwarding Information Bases
ICN	Information-Centric Networking
ICN LoWPAN	Information-Centric Networking Architecture over Low-power Wireless Personal Area Network
IOT	Internet of Things
IP	Internet Protocol
LHR	Last-hop router
LLN	Low-Power and Lossy Network
PIT	Round-Trip Time
RTT	Pending Interest Table
RWI	Real-World Identity
TCP	Transmission Control Protocol
TLV	Type-Length-Value

Last modified on December 15, 2021
This and other papers on recent advances in networking are available online at
http://www.cse.wustl.edu/~jain/cse570-21/index.html
Back to Raj Jain's Home Page