The Group Data Access Control Method in Content Centric Network

Shouhei NAGAI, Takahiro KAIDA, Osamu MIZUNO
Graduate School of Electrical Engineering and Electronics
Kogakuin University
Tokyo, Japan

Abstract **Usage of the Internet for content delivery is increasing. Content Delivery Network is proposed for efficient content delivery in an IP network. However, there are some issues, including over load to content servers, and so on. Content Centric Network attracts attention as a new generation network, which can solve these issues. However, in Content Centric Network anyone who knows the content ID would get the contents, therefore, it is difficult to deliver content only to permitted person. To solve this problem, we propose the group data access control method. The proposed method is evaluated confidentiality, integrity and availability, and performance. The proposed method is also evaluated its action by emulation program.**

Keywords—component; Content-Centric-Network, Security, Access Control Scheme, Next Generation Network

I. INTRODUCTION

Due to spread of high-performance mobile devices, video data occupies about 53 percent of mobile traffic at the end of 2013[1]. It has increased 3 percent compared to 2012. It is indicated that content delivery, including videos and images are increasing. Content Delivery Network is known as an effective content delivery system in the IP network. It has the load distribution function to avoid access concentration to the specified node. However, there are problems about the overhead of frequent query to the DNS and intensive load to content servers.

Content Centric Network (CCN) [2] attracts attention as a next generation network to solve these problems. In Content Centric Network anyone who knows the content ID would get the contents, therefore, it is difficult to deliver content only to permitted person.

This research object is to deliver content to person having access rights in CCN. We proposed access control based on group management.

In Section 2, we mention overview of CCN and access authentication methods. Problems using existing security measure are also discussed. Then, we show analysis of user authentication issues. Also, to solve this problem, we propose the group data access control method in Section 3. Evaluations of the proposed method are in Section 4. Section 5 is the conclusion of this paper.

II. CCN ACCESS AUTHENTICATION

A. Overview of Content Centric Network

In CCN, ID called the content ID is assigned to a data generated by a content creator (called a publisher). A publisher put his content data to a node called a content storage node. Content ID is advertised by flooding at fixed interval. When a user (called a subscriber) requests to get a content data, he sends the content ID to the network. Routing for getting content data is executed on the network. Then, a node which has the content data is discovered. The content data corresponds to the content ID is replied as a response from the discovered node (Fig 1). Also, when the content data are transferred among relay nodes the data is cached in the relay nodes. In case of getting requests with the content ID, the content data is replied from a relay node which cached it (Fig.2).

As existing security measures of CCN, for example, the content data manipulation detection and authentication, hash value and public key cryptography are used.

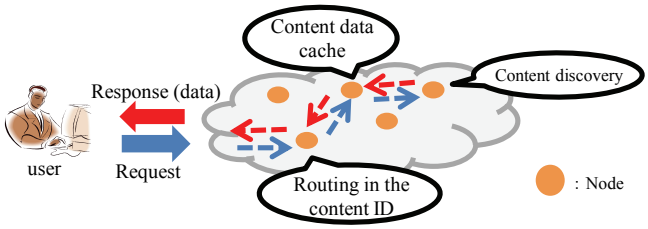

Figure 1 Overview of the CCN (Normal)

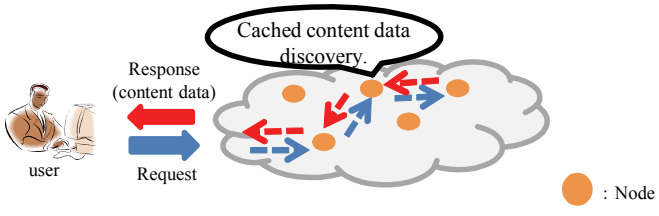

Figure 2 Overview of the CCN (When the cache is used)

B. Access Authentication

The current IP network uses some authentication methods for access control, for example, ID/password and Kerberos.

In general, public key cryptography and hash value used as CCN security measures. First of all, a publisher calculates hash value using the hash functions. Next, the hash value is encrypted with a secret key, to generate the digital signature. Generated signature is replied to the subscriber with content data. A subscriber decrypts the digital signature using with a public key and he determines the risk of tampering or spoofing.

C. CCN Access Authentication Issues

Using existing security measures, a subscriber can confirm whether received content data is corresponds to the requested content ID. He also can detect confirms received content data is not manipulated and so on. These are for integrity of receiving content data. However, they are not for subscriber authentication.

III. Proposed Method

A. Analysis of the Issues

We discuss a new access authentication method to solve above problems. As shown in Chapter II, in CCN, content data are distributed at many nodes to reduce traffic, and a subscriber needs not know where content data is. It is difficult to provide user authentication functions in specific node, because content data will not always be replied from the specific node. It is preferable to reduce load which caused from added authentication method.

B. Grouping Access Authentication Method

A publisher assigns user group who permitted to access his content data. The member of the user group is called a group member. The publisher distributes element for user authentication to group members, in order to restrict content access. We assume that all of relay nodes are trusted.

Referred to authentication methods in IP network [3-4], we nominate two access authentication methods by the grouping access authentication. One is based on one-time password authentication and the other is based on digital signature.

1) CCN-OTP: To synchronize time between a content storage node and relay nodes, time data is added to advertise data. A subscriber generates onetime password using the common group formula with time-seed. Each group member and nodes have the formula. He sends authentication element, which is composed of generating one-time password, the group ID and the group password, with content ID. Routing is executed by the content ID only. After the content data is discovered, authentication is performed using the authentication element at the node that stores content data. If authentication is valid, the content data are delivered to the user. Relay nodes cache the group authentication elements correspond to the content data (Fig.3). If required content data is found in cached node, authentication would execute using cached group authentication elements (Fig.4).

2) User Challenge Method: The digital signature of a subscriber is created using the content ID. It encrypts with the private key that only group members have. The subscriber sends the content ID with encrypted digital signature, group ID and group password to network. Routing is executed using the content ID only. When the content data corresponds the content ID is discovered, content storage node creates a digital signature from content ID. Content storage node verifys the encrypted signature, group ID and group password decrypted with the public key. Authorization is executed to compare created digital signature and decrypted digital signauter. If it is authorized, the corresponding content data delivery to the subscriber. Relay nodes cache a set of the content ID, content data, the group ID, group password and public key. If the public key is cached in relay nodes, it would be used for authentication. This method may use the common key system as an option.

C. Comparison of the Methods

Table 1 shows evaluation results about the feasibility of confidentiality, integrity and availability of the two methods shown above. Table 2 is evaluation results from performance points of view. CCN-OTP is better from those analyses.

TABLE I. Information Security Evaluation Results

	CCN-OTP	***User Challenge Method***
Confidentiality	Confidentiality is achieved by authentication element.	Confidentiality is achieved by authentication element.
Integrity	Integrity is achieved by using security of CCN.	Integrity is achieved by using security of CCN.
Availability	Availability is achieved by cached data.	Availability is achieved by cached data.

[a.] Node is confirmation whether it is possible to actualize information security.

TABLE II. Performance Evaluation Results

	CCN-OTP	***User Challenge Method***
Number of operationsr to reqest-get	No change	No change
Whether cache use	Available	Available
Traffic	Little increase	Traffic transform by data size of content ID
Data size of content ID	It is increased by authentication element.	It is increased by authentication element.
Load increased amount in node	It is calculation of one-time password and the user authentication process.	It is the decryption of digital signature, creation of digital signature and the user authentication process.
Operation at time of user increased	Action increase	Action increase
Operation at time of data incerased	Action increase	Action increase

[b.] Comparison with CCN-OTP and User challenge method.

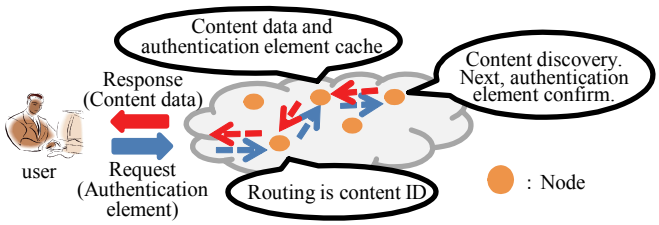

Figure 3 CCN-OTP

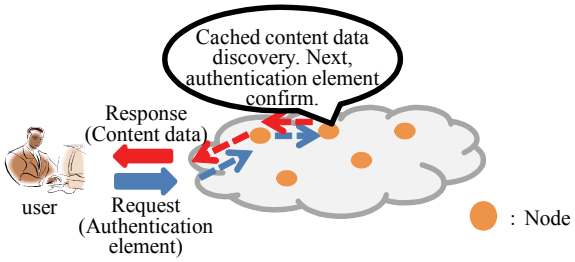

Figure 4 CCN-OTP (When the cache is used)

IV. VERIFICATION

A. Overview of Validation

Feasibility of proposed method confirmed in emulation. We design detail procedure of the method and confirm authentication process. Emulation program is written in Java. Figure 3 shows execution results.

```
No.0 Subscriber
otp=459
Please enter content ID 'a' or 'b'
a
Please enter to send requirement node '1-4'
1
Please enter group ID
kou
Please enter group password
gaku
Please enter one-time password
459

No.1Node
Intrest coincidence
Node send No.3Node

No.3Node
Intrest coincidence
Node send No.4Node

No.4Node
Intrest coincidence
Here is content storage node
Group ID and Group password coincidence
one-time password coincidence
Node reply reponce. Node send No.3Node

No.3Node
To Refer PIT
Responce send No.1Node

No.1Node
To Refer PIT
Responce send Subscriber

No.0 Subscriber
get responce
Subscriber got content data 'Hello world'
```

Figure 3 Emulation results

B. Discussion of Results

Figure 3 shows that subscribers enter the content ID ‘a’ and authentication element as a request message. Node 1 receives the request. Node 1 determines distention by content ID ‘a’, and transfers it to Node 3. The request would transfer to the content storage node in the same way. In this example, Node 4 has corresponding content data. Node 4 replies the content data after authentication process. Relay node ‘Node 3’ and ‘Node 1’ deliver data to the subscriber. He might exist in the direction where the request has come.

The propose method cause a little increase of traffic. Because, number of signals are same as that of ordinary method, and size of authentication element data will be smaller than content data itself. Increased load to the node is a little, because authentication process is simple.

V. CONCLUSION

CCN attracts attention for efficient content data delivery. To deliver content data in permitted person in CCN, we proposed the group data access control method. We also confirmed the feasibility of the method with emulation.

In this paper, we assume that relay nodes are trusted and the authentication element can deliver to group member safety. Existing untrusted nodes and how to deliver the authentication element safety are future studies.

REFERENCES

[1] Cisco Visual Networking Index, ”Cisco Visual Networking Index: Forecast and Methodology, 2013-2018”
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html
(confirmed Dec., 19, 2014)

[2] V. Jacobson et al, “Networking named content,” Proc. of the 5th international conference on Emerging networking experiments and technologies, ACM, pp.1-12 2009.

[3] Kaori.Isi et al. Author “Jouhou sekyurithi no kiso” Kyouritu shuppan, Tokyo, 2011.

[4] Charlie Kaufman, Mike Speciner, Radia Parlman Author, Keiichirou et al Translation, “Network Security”, Pearson Education, Tokyo, 1997.

[5] Kazuaki Ueda et al, “Novel scheme of route aggregation for contents centric networking”, IEICE Technical Report, NS2012-58, vol.122, No.208, pp.41-46, Sept, 2012

[6] Bari, MdFaizul, et al. "A survey of naming and routing in information-centric networks." Communications Magazine, Vol.50, No. 12 pp44-53, Dec., 2012.