http://dx.doi.org/10.14400/JDC.2016.14.6.405

미래 인터넷 기술의 Privacy 보호 기술 동향 및 개선

김대엽
수원대학교 정보보호학과

Trend and Improvement for Privacy Protection of Future Internet

DaeYoub Kim
Dept. of Information Security, Suwon Univ.

요 약 인터넷의 여러 문제들을 해결하고, 데이터 전송 성능을 개선하기 위하여 제안된 다양한 미래 인터넷 아키텍처들은 네트워크 노드나 프락시 서버에 캐싱된 데이터를 활용하고 있다. 미래 인터넷 기술 중 하나인 데이터 이름 기반 네트워킹 (NDN)은 네트워크 노드에 데이터 캐싱 기능을 구현하고, 네트워크 노드가 데이터 요청 메시지에 응답함으로써 인터넷의 성능을 개선한다. 그러나 네트워크 노드에 데이터가 캐싱 된 이후에는 해당 데이터의 소유자가 데이터 배포 및 사용에 관여할 수 없기 때문에 사용자 프라이버시에 심각한 위협이 될 수 있다. 이를 해결하기 위해, NDN은 데이터 암호화 및 그룹 기반 키 관리 기술을 사용하여 데이터 접근 제어 기능을 제안하고 있다. 그러나 제안된 기술은 접근 통제 리스트와 복호화 키를 획득하기 위하여 추가적인 메시지 교환이 필요하기 때문에 성능 저하 요인이 될 수 있다. 본 논문은 NDN의 접근 통제 기능을 살펴보고, 성능 향상을 위한 개선된 방안을 제안한다.

주제어 : 미래인터넷, 데이터 이름 기반 네트워킹, 프라이버시, 인증, 접근제어

Abstract To solve various problems of the Internet as well as to enhance network performance, various future Internet architectures utilize cached data in network nodes or in proxy servers. Named-data networking (NDN), one of future Internet architectures, implements in-network data caching functionality, and then responds itself to request messages. However, it can cause users' privacy invasion that the publisher of data can not engage in the sharing/using process of the data anymore after the data was cached in-network. So NDN implements both encryption-based access control and group access control. But, since such access control schemes need to exchange additional messages in order to search for a proper access control list and keys, it causes inefficiency. This paper surveys the access control schemes of NDN, and then proposes an improved scheme.

Key Words : Future Internet, NDN/CCN, Privacy, Authorization, Access Control

1. 서론

초기 인터넷 개발자의 주된 목적은 원거리에 위치한 호스트들 사이에 안전한 네트워크 연결을 제공하는 것이었다[1]. 그러므로 현재와 같이 다양한 서비스에 인터넷이 활용됨에 따라 발생하는 여러 문제들과 이에 대한 대응 방안들은 고려되지 않았다. 이로 인하여 네트워크 병목현상으로 인한 비효율성 증가 및 여러 취약점으로 인

* 본 논문은 2015년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2013R1A1A2008389)
Received 20 April 2016, Revised 25 May 2016
Accepted 20 June 2016, Published 28 June 2016
Corresponding Author: DaeYoub Kim(Suwon Univ.)
Email: daeyoub69@suwon.ac.kr

ISSN: 1738-1916

한 인터넷 사고 증가와 같은 문제점들이 발생하고 있다. 그러나 사물인터넷, 차량 간 통신과 같은 인터넷 기반의 서비스들이 지속적으로 개발/보급됨에 따라 인터넷이 갖고 있는 이러한 문제들은 서비스 적용 및 보급에 큰 장애 요소가 되고 있다.

인터넷을 이용한 다양한 서비스가 보급되고, 서비스 이용자가 폭발적으로 증가함에 따라 사용자의 개인 정보 유출에 대한 우려가 높아지고 있다. 그러므로 서비스 개발과 보급에 있어 사용자의 개인정보를 보호하기 위한 추가적인 기술 개발이 지속적으로 요구되고 있다 [2,3,4,5,6,7,8].

미래 인터넷 아키텍처로 제안되고 있는 다양한 기술들은 인터넷의 태생적인 문제들을 해결하고, 향후 개발/보급될 서비스를 보다 효과적이고 안전하게 제공하기 위한 다양한 방안들을 제안하고 있다[7]. 미래 인터넷 아키텍처 중에서 기존의 물리적 호스트에 접속하던 인터넷의 기능을 원천적으로 개선하여 사용자가 원하는 데이터에 직접 접속하는 기능을 제공하는 정보 기반 네트워킹 (ICN, Information Centric Networking) 기술들이 제안되었다[10]. ICN은 프락시 서버나 네트워크 노드에 데이터 임시저장(Data Caching) 기능을 구현하고, 사용자가 요청한 데이터를 가장 효율적으로 제공할 수 있는 서버/노드로부터 해당 데이터를 제공 받도록 설계되었다. 이와 같은 전송 기법은 기존의 CDN (Content Delivery Network)이나 P2P (Peer-to-Peer Network)에서도 사용하고 있으나, CDN/P2P는 응용/서비스 계층에서 이러한 기능을 제공하는 반면에, ICN은 네트워크 계층에서 동일한 기능을 제공함으로써 원천적으로 기능을 개선하려고 시도하고 있다.

ICN 기술 중 하나인 데이터 이름 기반의 네트워킹 (NDN, Named Data Networking) 기술은 전송되는 데이터의 전송 구간에 위치한 네트워크 노드들에 데이터 캐싱 기능을 구현하고, 해당 노드들이 캐싱하고 있는 데이터에 대한 요청 메시지를 수신하면, 수신된 요청 메시지를 더 이상 포워딩하지 않고 캐싱된 데이터를 이용하여 직접 응답하도록 설계 되었다[9]. 또한, 이와 같은 중간 노드에서의 요청 메시지 처리를 보다 효율적으로 수행하기 위하여 데이터의 유일한 식별자 (Data Name)를 기반으로 요청 및 응답 메시지를 포워딩하도록 설계 되었다. 그러나 중간 노드에 의한 요청 메시지 처리는 위/변조된 데이터의 제공이 가능하며, 데이터 사용 권한이 없는 사용자의 데이터 사용을 제어할 수 없기 때문에 사용자의 프라이버시를 침해할 수 있다.

이러한 문제들을 해결하기 위하여, NDN은 데이터에 해당 데이터의 원생성자의 전자 서명을 첨부하도록 강제하고 있으며, 암호화를 이용한 접근 제어 기술을 구현하여 데이터의 부적절한 사용을 제어할 수 있도록 하였다. 그러나 이와 같은 보안 기능을 구현하기 위하여 추가적은 절차가 필요하며, 이러한 절차는 NDN의 성능을 저해하는 주요 요인이 될 수 있다.

본 논문은 NDN의 보안 기능 중에서 접근 통제 기능을 살펴보고, NDN의 접근 통제 기능을 개선하기 위한 방안을 제안한다.

2. Named Data Networking (NDN)

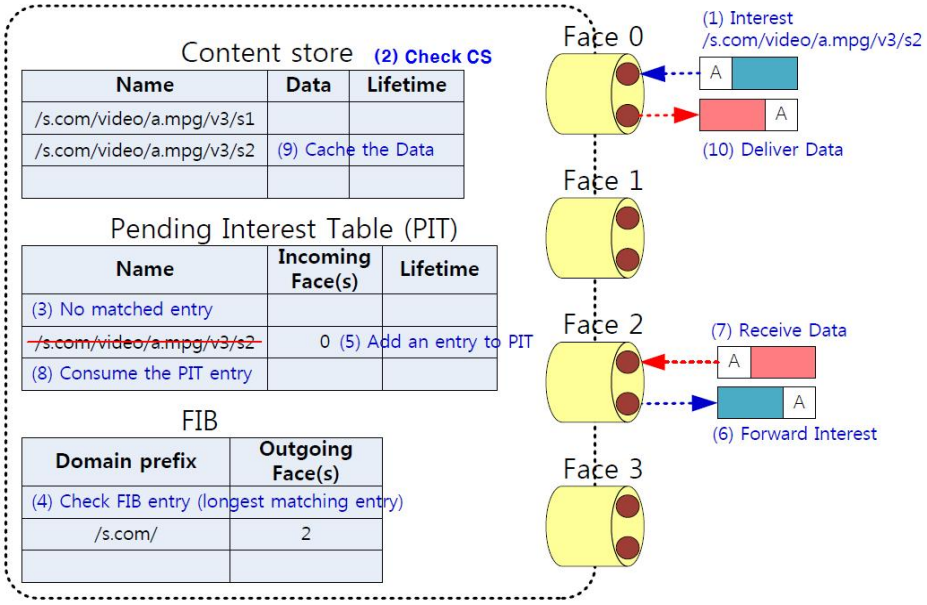
NDN의 특징은 다음과 같이 세 가지로 요약될 수 있다:

(1) 데이터 이름 기반의 요청 메시지 (Interest)/ 응답 메시지(Data) 포워딩
(2) 중간 네트워크 노드에서의 데이터 캐싱 및 포워딩
(3) 전자 서명 기반의 데이터 인증

이와 같은 특징을 구현하기 위하여 NDN은 다음과 같은 요소들이 필요하다:

(1) FIB (Forwarding Information Base) 테이블: Interest에 포함되어 있는 데이터 이름을 기반으로 해당 Interest를 포워딩할 전송 인터페이스 (Face)를 결정하기 위한 정보를 제공한다. FIB 테이블의 정보는 일반 IP 라우터의 라우팅 프로토콜과 유사한 방법으로 정보를 공유하여 관리할 수 있다.
(2) PIT (Pending Interest Table): 요청한 Data를 수신했을 때, 해당 Data를 사용자들에게 전송하기 위하여, 수신된 Interest와 incoming Face 정보를 기록/관리하기 위해 사용한다.
(3) 네트워크 캐쉬 (CS, Content Store): 네트워크 노드가 수신한 Data를 임시로 저장하는 내부 저장 공간으로 사용한다.

[Fig. 1]은 NDN의 Interest/Data 처리 절차를 설명한다.



[Fig. 1] NDN Interest/Data Forwarding Process

(1) 노드의 인터페이스 (Face 0)로 Interest를 수신한다.
(2) Interest에 해당하는 데이터를 CS에 저장하고 있는지 확인한다. 만약 저장하고 있다면, Face 0로 해당 데이터를 전송한 후, Interest 처리를 종료한다.
(3) Interest에 해당하는 entry가 PIT에 존재하는지 확인하다. 만약 기록이 존재한다면, 해당 entry에 Face 0을 추가한 후, Interest 처리를 종료한다.
(4) FIB 테이블을 참조하여, Interest를 포워딩할 Face (예를 들어, Face 2)를 선택한다.
(5) PIT에 Interest를 위한 entry를 새로 추가한다.
(6) 4단계에서 선택된 Face 2로 Interest를 전송한 후, Interest 처리 절차를 종료한다.
(7) 이 후, 노드의 인터페이스 (Face 2)로 Data를 수신한다.
(8) 수신 된 Data에 해당하는 entry가 PIT에 존재하는지 확인한다. 만약 해당 entry가 PIT에 기록되어 있지 않다면, Data를 폐기한 후, 처리 절차를 종료한다.
(9) Data를 CS에 저장한다.
(10) 단계 8에서 검색된 entry에 기록되어 있는 Face들 (예를 들어, Face 0)로 Data를 전송한 후, 해당 entry를 PIT에서 삭제한다.

3. NDN 데이터 접근 통제

NDN은 캐싱된 데이터의 접근 통제를 위하여 암호화 기반 접근 통제 (EAC, Encryption-based Access Control)와 그룹 멤버쉽 기반 접근 통제 (GAC, Group-based Access Control)를 구현하고 있다 [12]. 이를 보다 효율적으로 적용하기 위하여 Manifest-based Access Control (MaAC) 기법이 최근에 새로 제안되었다[13,14,15,16].

3.1 암호 기반 접근 통제

네트워크를 통해 전송/공유되는 데이터의 무단 이용 및 배포를 제어하기 위하여, NDN은 데이터 생성자 (Publisher)가 해당 데이터를 암호화해서 배포할 수 있도록 암호화를 통한 접근제어 기능(Encryption-based Access Control, EAC)을 제공하고 있다. 전송되는 데이터는 데이터 키(DK, Data Key)를 이용하여 암호화 되며, 특별히 대용량 데이터의 경우 단편화를 통해 일정 크기의 Segment로 분할 처리된 후, 각각의 Segment를 독립적인 Data Object로 처리한다. 이 때, 각각의 Data Object를 암호화 하는 실제 암호화 키(KO)를 DK를 이용하여 다음과 같이 생성한다.

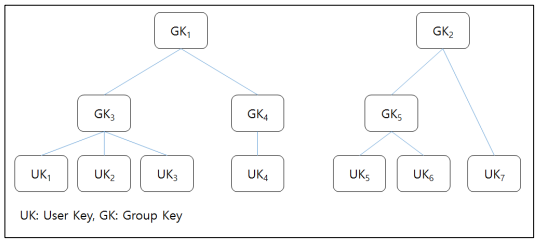
$$KO||IVO=KDF(Label,\ DK,\ DataO,\ h) \quad (1)$$

여기서, IVO는 암호화에 사용되는 초기 값을 의미하며, Label은 생성된 키의 사용용도 구분자를 의미한다. DataO는 Data Object의 보조 데이터, h는 KO||IVO의 길이를 각각 의미한다.

DK의 배포/공유를 위해, NDN은 DK를 하나의 Data Object로 간주하여 처리한다. 사용자가 암호화된 데이터를 이용하려고 할 때, 해당 데이터의 복호화에 필요한 DK를 NDN을 통해 획득할 수 있도록 다음과 같이 미리 정해진 데이터 이름을 사용 한다:

$$<N>/\_access\_/DK \quad (2)$$

여기서 <N>은 해당 데이터의 계층적 이름에서 Segment 번호를 제외한 부분적 계층이름을 나타낸다.



[Fig. 2] User/Group Key Structure Example

3.2 그룹 기반 접근 제어

NDN은 데이터의 접근 제어를 구현하기 위해서는 DK의 암호화 및 그룹 기반 접근제어(Group-based Access Control, GAC)를 추가로 구현 한다. 이를 위하여 NDN은 노드 키(NK, Node Key)와 접근 제어 리스트(ACL, Access Control List)를 이용한다. ACL은 데이터에 접근할 수 있는 개인 및 그룹에 대한 정보를 포함하고 있으며, 각각의 개인/그룹 은 각각 고유의 공개키 및 비밀키 쌍을 갖고 있다고 가정한다. DK와 마찬가지로 NDN은 NK, ACL, 공개키/비밀키를 각각 Data Object로 간주하여 처리함으로써 네트워크를 통해 NK/ACL을 획득할 수 있도록 구현하고 있다.

DK는 NK로 암호화 되어 있으며, NK는 ACL에 명시된 개인/그룹의 공개키로 암호화 된다. 또한, 개인/그룹 키의 효율적인 관리를 위해 [Fig. 2]와 같은 계층화된 키 체계를 적용한다. 예를 들어, 그룹 3에 속한 사용자 1, 2, 3이 그룹 3의 비밀키를 안전하게 공유하기 위하여, 그룹 3의 비밀키는 사용자 1, 2, 3의 비밀키로 각각 암호화되어 배포된다.

DK의 암/복호화에 사용되는 NK를 효과적으로 관리하기 위하여, NDN은 계층화된 데이터 이름 구조의 각 계층 노드마다 NK를 생성/운영할 수 있도록 제안하고 있다. 또한, DK의 암/복호화에 필요한 NK를 획득할 수 있도록 NDN은 다음과 같이 미리 정해진 데이터 이름을 사용 한다:

$$<N>/access/NK/<version\ marker>/ \quad (3)$$

DK와 달리, NK는 키 관리 정책에 따라 키 갱신이 이뤄질 수 있기 때문에, <version marker>를 사용하여 갱신된 키를 구분한다. 또한, <version marker>는 DK 생성 및 암호화 시점에 유효한 NK를 구분하기 위해서도 사용된다.

ACL은 NK에 접근할 수 있는 권한을 명시하고 있으므로, NK와 함께 운영/관리된다. ACL은 다음과 같은 데이터 이름을 사용 한다:

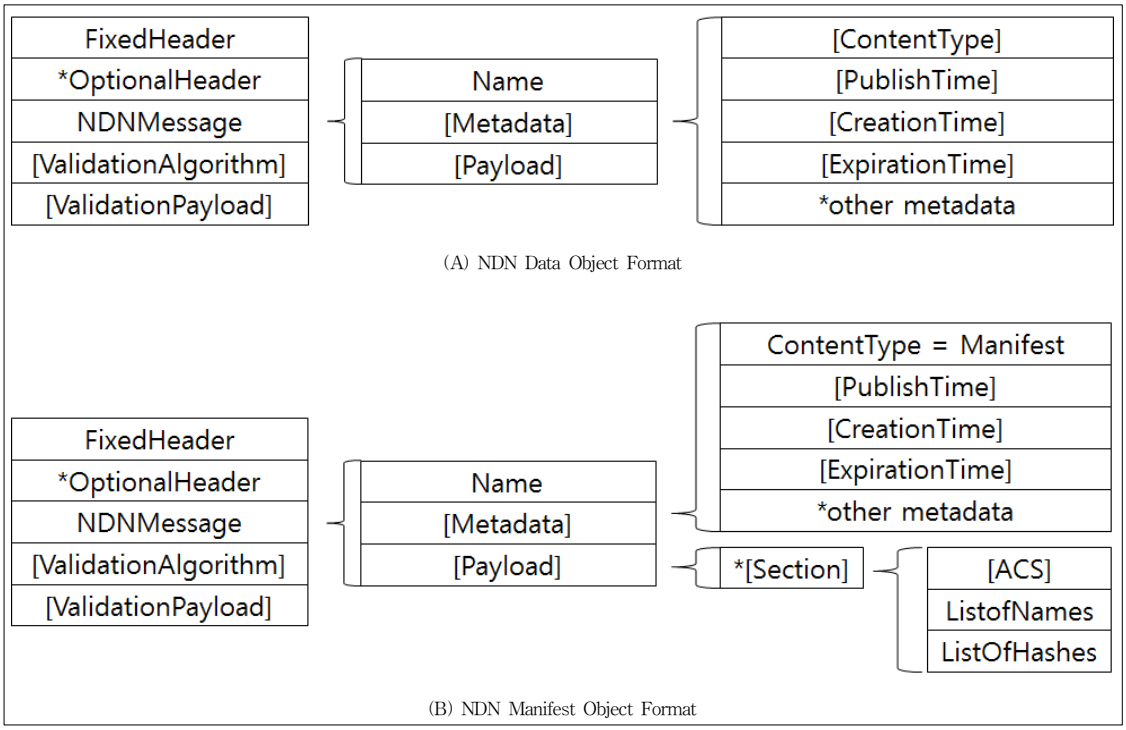
$$<N>/\ access\ /ACL/<version\ marker> \quad (4)$$

NK와 ACL을 효과적으로 운영하기 위하여 NDN은 개선된 계층적 접근 통제 (Hierarchical Access Control, HAC)를 사용한다. 즉, 계층적 이름 구조에 포함된 노드에 NK와 ACL이 정의 되어 있지 않다면, 상위 계층 노드에 정의된 ACL이 적용되며, 해당 상위 계층에 정의된 NK를 이용한다. 그러나 전통적인 HAC와 달리 NDN은 필요 시 하위 노드에 ACL과 NK를 정의할 수 있도록 허용한다. 또한, 하위 노드에 정의된 ACL과 NK가 적용 시 우선권을 갖는다.

EAC/GAC를 이용한 데이터 접근제어가 구현될 때 사용자의 데이터 이용 절차는 다음과 같다:

(1) 사용자는 이용하려고 하는 데이터의 단편화된 Data Object를 단편화 순서에 따라 NDN을 통해 수신한다. 이 때, 해당 Data Object의 type이 ENCR로 설정되어 있음을 확인한다.

(2) 수신된 Data Object의 데이터 이름을 확인한 후,



[Fig. 3] NDN Message Format

NDN AccessControlManager (ACM)에게 해당 데이터 이름을 전달한다.

(3) ACM은 입력된 데이터 이름을 기반으로 암호화된 DK를 획득을 위한 Data Object의 이름을 생성한 후, NDN을 통해 DK를 획득한다.

(4) 암호화된 DK를 복호화하기 위하여 해당 데이터 이름에 정의된 ACL과 NK를 획득한다. 이 때, 데이터 이름에 대응되는 노드에 DK를 복호화할 ACL/NK가 정의 되어 있지 않으면, 점진적으로 상위 이름 계층 노드를 탐색하여, 필요한 ACL/NK를 획득한다.

(5) ACL에 정의된 권한을 바탕으로 NK의 복호화에 필요한 키를 획득한 후, NK와 DK를 순차적으로 복호화 한다.

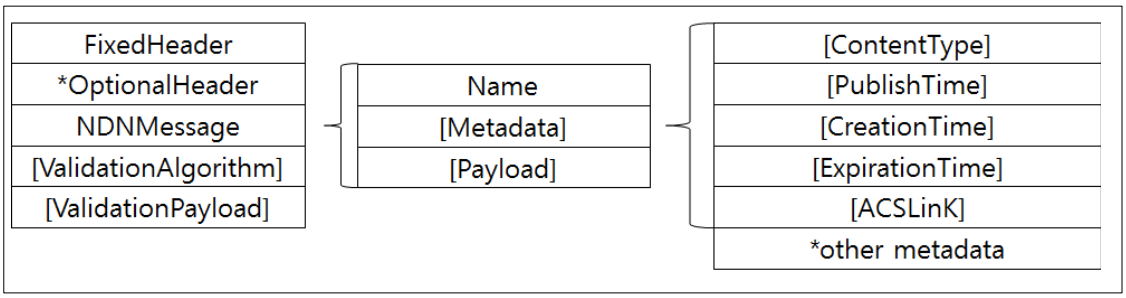
(6) Data Object를 인증한 후, 사용한다.

3.3 메니페스트 기반 접근통제

NDN은 대용량 데이터의 전송 및 관리를 보다 효과적으로 하기 위하여, 데이터를 일정 크기의 Segment로 단편화 한 후, 단편화된 Segment를 Data Object로 간주하여 처리한다. 또한, 단편화를 효율적으로 구현하기 위하여 Manifest Data를 이용한 데이터 획득 방안이 새롭게 제안되었다[13].

Manifest Data를 전송하는 Data Object를 Manifest Object라고 할 때, Manifest Object는 전송하려는 데이터를 단편화한 세그먼트 집합에 대한 정보를 제공하기 위하여 사용된다. [Fig. 3]은 일반적인 Data Object와 Manifest Object를 설명한다. Manifest Object의 ContentType은 'Manifest'로 지정되며, Payload 필드를 이용하여 접근제어 정보(Access Control Specification, ACS)와 세그먼트 정보(ListofNames, ListofHashes)를 전달한다. 각각의 필드는 다음과 같이 구성 된다:

- ACS: Data Object의 암호화에 사용된 Nonce Key의 Name Prefix를 저장한다.
- ListOfNames: Manifest Object에 의해 처리되는 Data Object의 Name Prefix를 저장하는 MediaName 서브필드와 해당 Data Object들의 시작 Segment 번호 전달을 위한 StartChunk 서브



[Fig. 4] Improved Data Message Format

필드로 구성된다.

- ListOfHashes: Manifest Object에 의해 처리되는 Data Object 들의 해쉬 값을 순차적으로 저장한다.

기존의 Data Object를 인증하기 위하여, NDN은 머클 해쉬 트리(MHT, Merkel-Hash Tree) 를 기반으로 개별 Data Object를 인증하도록 구현되었다[12,17]. Manifest는 ListofNames와 ListOfHashes를 이용하여 데이터의 단편화 결과를 수신자가 미리 알게 함으로써, 다중 Interest 생성/전송 등을 보다 효율적으로 구현할 수 있도록 했으며, ListOfHashes를 이용하여 Data Object를 순차적으로 보다 효율적으로 검증할 수 있도록 설계 되었다. 또한, 기존의 NDN은 고정된 형식 DK 데이터 이름을 사용한 반면에, ACS는 사용자가 다양한 구조/형식으로 DK의 이름을 구현할 수 있도록 허용하고 있다.

4. Improved Access Control Procedure

이 절에서는 GAC와 MaAC의 특징을 분석하고, 개선 방안을 제안한 후, 그 성능을 비교 분석한다.

4.1 GAC와 MaAC의 특성 분석

기존의 NDN과 GAC는 데이터 마다 오직 하나의 DK만을 정의해서 사용한다. 즉, 데이터를 구성하는 Data Object의 수에 관계없이 하나의 DK만 적용된다. 그러나 대용량 데이터의 경우 일반적으로 DK를 주기적으로 갱신하여 적용한다. 그러므로 이와 같은 서비스의 경우에는 기존의 GAC를 그대로 적용하기 어렵다.

또한, DK를 복호화하기 위해서는 지정된 데이터 이름 계층의 하위 계층 노드부터 시작하여 순차적으로 상위 계층 노드를 탐색하여 필요한 NK를 검색한다. 이와 같은 NK 검색을 위해서 사용자는 데이터 이름을 분석하여 각각의 상위 계층 노드에 대응하는 Name Prefix를 생성한 후, 해당 노드에 정의된 NK를 획득하기 위한 Interest를 생성/전송하는 절차를 반복적으로 수행한다. 특히, NK의 경우 키 갱신으로 인하여 다양한 버전의 NK가 해당 노드에 정의되어 있을 수 있으며, 이 경우, 해당 노드에 NK가 정의되어 있다 하더라도, 다시 적당한 버전을 검색해서 회득하기 위하여 버전을 변경하여 재요청하는 작업을 수행해야 한다. 이는 Interest를 전송량을 증가시키는 원인이 되며, 특히 NK 획득 시간을 지연시켜 전체적인 서비스 지연을 초래할 수 있다.

MaAC는 Data Object를 암호화 할 때 사용된 키를 Manifest Object에 명시하고 있기 때문에, 암호화된 DK를 복호화하기 위해 필요한 NK를 순차적으로 탐지할 필요가 없다. 그러므로 반복적으로 NK를 요청하는 GAC의 비효율성을 개선할 수 있다. 또한, 이론적으로 ACS 필드를 이용하여 다양한 이름의 DK를 적용할 수 있다. 그러나 [13]에서 제안하고 있는 NDN의 구현 절차는 데이터 요청할 때, 첫 번째 Data Object가 Manifest Object로 설정되어 있기 때문에, 중간에 DK가 갱신 적용되는 상황을 고려하여 구현되어 있지 않다. 즉, 하나의 데이터를 암호화할 때 복수 개의 DK를 사용할 수 없도록 구현되어 있다.

또한, Manifest Object의 Payload 부분은 암호화하면 안 되기 때문에, Data Object 처리 절차를 일반 Data Object 처리와 Manifest Object 처리로 구분해서 구현해야 한다.

특히 대부분의 멀티미디어 콘텐츠 서비스의 경우 데이터 생성자와 배포자(서비스 업자)가 서로 다르다. 이와

<Table 1> Characteristics Comparison

Scheme	Additional Implement			Possibility		
	NK search	AC Object	Authen.	Multiple keys	Multiple ACL	Cached Key Reuse
GAC	Need	Needless	Needless	Impossible	Impossible	Impossible
MaAC	Needless	Need	Need	Impossible	Impossible	Possible
MeAC	Needless	Needless	Needless	Possible	Possible	Possible

경우, 데이터 암호화 및 데이터 인증 정보 생성은 데이터 배포를 담당하는 데이터 서비스 업자에 의해 수행된다. 그러므로 Manifest Object를 적용할 경우, 데이터의 Manifest Object는 데이터 서비스 업자가 생성해야 한다. 그러나 NDN은 모든 Data Object마다 생성자의 전자서명을 첨부하도록 강제규정하고 있기 때문에, 서비스 업자는 생성한 Manifest Object를 데이터 생성자에게 다시 인증 받아야 한다. 이 경우, MHT를 사용하고 있다면, 전체 인증 정보를 다시 생성해야 된다. 만약 하나의 데이터가 여러 서비스 업자에 의해 배포되고 있다면, 상이한 인증 정보가 생성/배포될 위험이 존재한다. 뿐만 아니라, 전체적인 서비스 흐름을 매우 복잡하게 만들 수 있다.

4.2 개선 방안

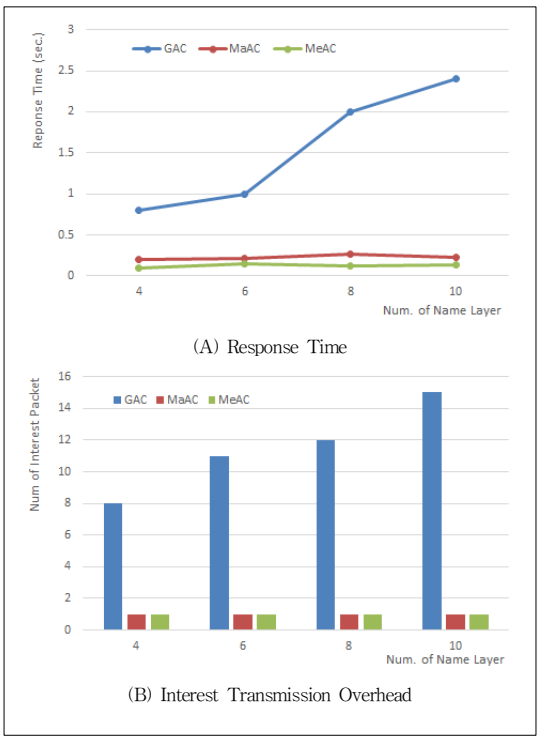
[13]에서 설명한 것처럼, Manifest Object를 이용할 때 다중 데이터 요청 프로세스를 보다 효과적으로 운영할 수 있으며, MHT를 이용할 때보다 인증을 위한 전송 및 계산 오버헤드를 개선할 수 있다. 그러나 Manifest Object를 이용할 경우, 앞서 언급한 것처럼 여러 문제점들이 발견된다. [Fig. 4]는 GAC와 MaAC의 단점을 보완하기 위해 본 논문에서 제안하는 Data Object의 구조를 나타낸다. 개선된 구조는 다음가 같은 두 개의 서브 필드를 기본 Metadata 필드에 추가 한다:

- ACSLink: Data Object가 암호화 되어 있으면, 복호화에 필요한 키의 데이터 이름을 저장한다. 다음과 같은 3개의 서브 필드로 구성된다.
  - KN (Key Name): 복호화에 사용될 키의 계층적 데이터 이름
  - KI (Key Identity): 복호화에 사용될 키의 계층적 데이터 이름의 해쉬 값
  - ACLN (Access Control List Name): Data Object에 접근이 허용된 개인/그룹 리스트의 데이터 이름
- FragmentNum: 데이터가 단편화 되었다면, 해당 데이터로부터 단편화된 전체 Segment의 수 저장한다.

표 1은 GAC, MaAC, 그리고 본 논문에서 제안한 MeAC의 특성을 비교 분석한 결과이다. 개선된 Data Object의 장점은 다음과 같이 요약 된다:

- 암호화에 사용된 키의 데이터 이름 및 구분자를 직접 명시하여, NK 획득을 위하여 반복적으로 검색/요청하는 절차가 필요 없다.
- Metadata 필드에 ACSLink 정보를 삽입함으로써, 별도의 Manifest Object를 추가적으로 운영하지 않고도 적용 가능하다.
- Data Object 생성 시, 암호화 및 인증에 대한 정보가 모두 결정되어 적용되므로, MaAC와 같이 추가적인 인증 절차의 필요로 인한 재인증과 같은 비효율성을 개선할 수 있다.
- 각각의 Data Object 마다 ACSLink 정보를 별도로 운영하기 때문에, 각각의 Data Object를 암호화할 때 서로 다른 키를 이용하여 암호화 할 수 있으며, 별도의 추가 절차 없이 암호화에 사용된 키를 구분/획득할 수 있다.
- 각각의 Data Object 마다 ACLLink 정보에 포함되어 있는 ACLN을 이용하여 서로 다른 ACL을 적용할 수 있다. 이는 특정 데이터의 미리보기 서비스 제공 기능 등의 구현을 용이하게 만든다.
- 또한, 앞서 사용된 복호화 키와 동일한 키를 사용하는 경우, KI를 이용하여 이와 같은 상황을 쉽게 구분할 수 있다. 이 경우, 키를 캐쉬에 임시 저장한 후 재사용할 수 있다.

[Fig. 5]는 NK 획득에 필요한 전송량 증가 및 응답시간을 시뮬레이션을 통해 분석한 결과이다. GAC에 비해 MaAC/MeAC는 응답시간 및 전송량을 모두 개선하였다.



[Fig. 5] Performance Comparison

5. 결론

네트워크 캐쉬를 이용하는 NDN에서 공유 데이터의 접근 통제는 필수 요소 기술 중 하나이다. 이러한 기술을 구현하기 위하여, 초기 NDN은 데이터 암호화와 그룹 접근 통제 기술을 접목하여 구현하였다. 그러나 이와 같은 기술들은 암호 키의 획득을 위해 반복적인 검색과 요청으로 인한 서비스 지연이 발생하는 문제점을 갖고 있다. 이를 개선하기 위해 제안된 Manifest 기반의 접근통제는 서비스 지연 문제는 해결하였으나, 실제 구현 시 추가 인증을 필요로 하는 요인이 발견되었으며, 다양한 데이터 서비스에서 요구되는 기능들을 구현하기에 부적절한 요소들일 갖고 있다.

본 논문에서 제안된 개선된 NDN 데이터 구조를 적용하면, GAC의 문제점으로 제기된 반복적인 키 검색과 요구로 인한 서비스 지연 문제를 해결하고, 동시에 MaAC가 갖고 있는 서비스 구현 한계를 해결하여 다양한 서비스에 적용할 수 있다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2013R1A1A2008389).

REFERENCES

[1] D. Clark, “The design philosophy of the DARPA Internet protocol,” ACM Sigcomm Comp. Comm. Review, vol. 18, no. 1, pp. 106-114, Aug. 1988.

[2] C. Park and J. Kim, “An Empirical Research on Information Privacy Concern in the IoT Era,” Journal of Digital Convergence, vol.14, no.2, pp.65-72, 2016. 02.

[3] S. Nam and C. Seo, “Privacy Preserving Source Based Deduplication Method,” Journal of Digital Convergence, vol.14, no.2, pp.175-181, 2016. 02.

[4] C. Park and J. Kim, “An Empirical Research on Information Privacy and Trust Model in the Convergence Era,” Journal of Digital Convergence, vol.13, no.4, pp.219-225, 2015. 04.

[5] S. Kim and S. Yeo, “A Study on Secure Data Access Control in Mobile Cloud Environment,” Journal of Digital Convergence, vol.11, no.2, pp.317-322, 2013. 02.

[6] Y. Jeong, K. Han, and S. Lee, “Access Control Protocol for Privacy Guarantee of Patient in Emergency Environment,” Journal of Digital Convergence, vol.12, no.7, pp.279-284, 2014. 07.

[7] Keun-Ho Lee, “A Method of Defense and Security Threats in U-Healthcare Service”, Journal of the Korea Convergence Society, Vol. 3, No. 4, pp. 1-5, 2012.

[8] Sik-Wan Cho, Won-Jun Jang, Hyung-Woo Lee, Development of User Oriented Vulnerability Analysis Application on Smart Phone”, Journal of the Korea Convergence Society, Vol. 3, No. 2, pp. 7-12, 2012.

[9] J. Pan, S. Paul and R. Jain, “A Survey of the Research on Future Internet Architectures,” IEEE communication magazine, vol 49, no. 7, pp 26-36, July 2011.

[10] B. Ahlgren, C. Dannewitz, C. Imbrenda, and D. Kutscher, “A survey of information-centric networking,” IEEE Communications Magazine, vol. 50, no. 7, pp 26-36, July 2012.

[11] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking named content,” ACM CoNext, pp. 1-12, Dec. 2009.

[12] PACR, “CCNx Access Control Specifications,” July 30, 2010.

[13] J. Kurihara, E. Uzen, and C. Wood, “An Encryption-based Access Control Framework for Content-Centric Networking,” IFIP Networking Conference (IFIP Networking), pp. 1-9, May 2015.

[14] C. Wood and E. Uzun, “Flexible end-to-end content security in CCN,” 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), pp. 858-865, Jan. 2014.

[15] C. Ghali, M. Schlosberg, G. Tsudik, and Christopher Wood, “Interest-based Access Control for Content-Centirc Networks,” arXiv preprint, arXiv:1505.06258, 2015.

[16] R. Touriani, T. Mick, S. Misra, and G. Panwar, “Security, Privacy, and Access Control in Information-Centric Networking: A Survey,” arXiv preprint, arXiv:1603.03409, Mar. 2016.

[17] R. Merkle, “Protocols for public key cryptosystems,” In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 122 - 134, Apr. 1980.

김 대 엽(Kim, Dae Youb)

- 1994년 2월 : 고려대학교 수학과(이학사)
- 1997년 2월 : 고려대학교 수학과(이학석사)
- 2000년 2월 : 고려대학교 수학과(이학박사)
- 2000년 2월 ~ 2001년 2월 : 텔리맨 정보보호연구소
- 2001년 3월 ~ 2002년 8월 : 삼성 시큐아이 정보보호연구소
- 2002년 9월 ~ 2012년 2월 : 삼성전자 종합기술원
- 2012년 3월 ~ 현재 : 수원대학교 정보보호학과 교수
- 관심분야 : 콘텐츠 보안, 미래 인터넷 보안, 스마트카 보안
- E-Mail : daeyoub69@suwon.ac.kr