ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 19-02-21
130

j.inst.Korean.electr.electron.eng.Vol.23,No.2,479~486,June 2019
http://dx.doi.org/10.7471/ikeee.2019.23.2.479

CCN 콘텐츠 인증을 위한 MHT 개선에 따른 오류 발생 및 영향 분석 연구

The Error Occurrence and Its Impact Analysis of Improved MHT Operation for CCN Content Authentication

김 대 엽*★

Dae-Youb Kim*★

Abstract

CCN utilizes MHT-based content authentication scheme. Some schemes propose improved MHT scheme to solve the inefficiency of the MHT-based content authentication scheme which is caused by repetitive hash value computation and witness transmission. For using MHT, it is essentially needed to minimize the possibility of error-occurrence as well as to improve the efficiency of the authentication scheme. This paper describes the improved MHT scheme is error-prone. Also, it analyzes the effect of a segment authentication error, especially, the degree of error propagation.

요 약

CCN은 MHT에 기반한 콘텐츠 인증 기술을 사용한다. MHT의 중복 해시 계산 및 인증정보 중복 전송으로 인한 비효율성을 개선하기 위한 연구가 발표되었다. 그러나 MHT를 이용하기 위해서는 효율성 향상뿐만 아니라 오류 발생 가능성도 최소화해야 한다. 이 논문에서는 개선된 MHT의 오류 발생 가능성을 설명하고, 오류 발생 시 그 파급효과에 관하여 분석한다.

Key words : P2P, CDN, CCN, Data Authentication, Data Integrity, MHT

Ⅰ. 서론

미래 인터넷 기술들은 인터넷의 내재된 기술적 문제들을 해결하고, 데이터 및 정보를 효율적이고 안전하게 제공하는 인터넷 기반의 다양한 서비스를 구현하기 위하여 제안되었다[1]-[3]. 정보중심 네트워킹 아키텍처(ICN, Information Centric Networking Architecture)는 미래 인터넷 아키텍처 기술들 중에서 가장 주목 받고 있는 기술이다. ICN은 콘텐츠를 생성/배포하는 콘텐츠 생성/배포 주체(CP, Content Publisher/Provider)에게 네트워크를 통해 전달되는 사용자들의 콘텐츠 요청 패킷들을 네트워크 내에서 콘텐츠 프락시 서버(CPS, Content Proxy Server) 또는 네트워크 노드

* Dept. of Information Security, Suwon University
★ Corresponding author
E-mail : daeyoub69@suwon.ac.kr, Tel : +82-31-229-8284
※ Acknowledgment: This work was supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education under Grant NRF-2017R1D1A1B03034215.
Manuscript received Jun. 6, 2019; revised Jun. 17, 2019; accepted Jun. 17, 2019.

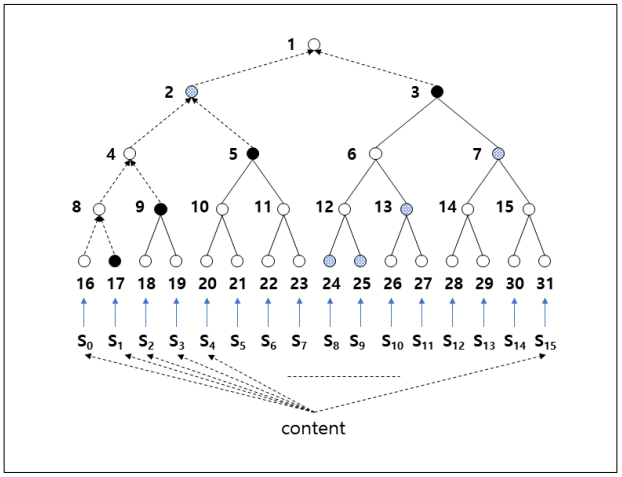

Fig. 1. MHT-based Content Authentication.
그림 1. MHT에 기반한 콘텐츠 인증 기법

(Network Node)로 분산시킨 후, CP를 대신하여 CPS 또는 네트워크 노드가 콘텐츠 요청 패킷에 직접 응답 패킷을 전송하도록 설계 되었다.

콘텐츠 중심 네트워크 아키텍처(CCN, Content Centric Networking Architecture)는 네트워크 노드에 콘텐츠 임시 저장 기능 (Caching)을 구현하고, 콘텐츠 요청 패킷의 전송 경로 상에 위치한 중간 네트워크 노드들이 수신된 콘텐츠 요청 패킷에 직접 응답할 수 있도록 하기 위하여 제안된 ICN 기술이다[2]-[5]. P2P (Peer-to-peer) 네트워킹이나 CDN(Content Distribution Networking)처럼 CCN은 사용자가 불특정 다수의 노드들로부터 콘텐츠를 제공 받을 수 있다. 네트워크 노드에 저장 되어 있는 콘텐츠 캐시를 보다 효율적으로 활용하기 위하여 CCN은 콘텐츠 식별자 정보(Content Name)를 활용한 패킷 라우팅을 제안한다. 호스트 중심의 인터넷 기술은 IP 주소와 같은 호스트의 고유 식별자 정보를 네트워크 패킷에 포함시켜 패킷 라우팅 및 인증에 활용하는 반면에, CCN은 목적지 IP 주소와 같은 특정 호스트 식별 정보가 아닌 콘텐츠 식별자 정보(Content Name)를 네트워크 패킷 헤더에 포함시켜 라우팅과 캐싱에 모두 활용되도록 제안되었다.

그러나 CCN 패킷의 호스트 식별자 정보 부재로 인하여 사용자가 CCN 콘텐츠를 수신했을 때, 수신된 패킷의 전송자를 식별/인증할 수 없다. CCN의 이와 같은 특성이 공격자에 의하여 악의적으로 이용될 경우, 콘텐츠를 위/변조하는 공격뿐만 아니라 위/변조된 콘텐츠를 이용한 다양한 추가 공격이 가능할 수 있다. 그러므로 CCN을 콘텐츠 서비스에 안전하게 적용하기 위해서는 네트워크를 통해 전송되는 콘텐츠와 해당 콘텐츠의 CP를 식별하고 인증하는 기술이 필수적으로 요구된다.

콘텐츠 인증을 위하여 CCN은 콘텐츠 패킷(Data)에 해당 콘텐츠의 CP 전자 서명 값을 첨부하도록 규정하고 있다. CCN을 통해 Data를 수신한 사용자는 해당 Data에 첨부된 CP의 전자 서명 값을 검증함으로써 수신된 콘텐츠의 위/변조 여부를 판별할 수 있다. Data는 개별 콘텐츠를 일정 크기 이하로 단편화한 세그먼트 패킷을 의미한다. 그러므로 Data 인증은 개별 콘텐츠가 아닌 콘텐츠의 단편화된 세그먼트 단위로 수행된다. 사용자가 대용량 콘텐츠를 이용하기 위하여 CCN을 통해 해당 콘텐츠를 수신한 경우, 콘텐츠를 구성하는 전체 세그먼트들을 각각 인증하기 때문에 콘텐츠 인증에 많은 시간이 소요되며, 이로 인하여 서비스 지연이 발생할 수 있다.

이와 같은 비효율성을 개선하기 위하여 CCN은 MHT(Merkle Hash Tree)에 기반을 둔 인증 기술을 활용하여 콘텐츠 CP 인증, 콘텐츠 인증 및 콘텐츠의 개별 세그먼트 인증을 동시에 수행 한다 [6], [7]. 그러나 [8]-[11]은 MHT 기반의 콘텐츠 인증을 수행할 경우 과도한 중복 연산 및 중복 전송이 발생될 수 있음을 지적하였고, 이와 같은 MHT에 기반을 둔 콘텐츠 인증 기술의 비효율성을 개선하고 성능을 최적화하기 위한 방안이 [12]에서 제안되었다.

[12]에서 제안된 MHT 기반의 콘텐츠 인증 기술을 위한 성능 최적화 기법은 콘텐츠의 세그먼트를 순차적으로 인증할 때, 세그먼트 인증을 위하여 해당 세그먼트 보다 앞서 인증 완료된 이전 순번 세그먼트의 인증 정보를 저장 후 재사용 한다. 그러므로 이와 같은 성능 최적화 기법을 적용하기 위해서는 콘텐츠의 세그먼트들이 반드시 순차적으로 모두 수신되어야만 한다.

본 논문에서는 [12]에서 제안된 MHT에 기반을 둔 인증 기술에 대한 성능 최적화 기법을 설명하고, 제안된 성능 최적화 기술의 인증 오류 발생 가능성을 살펴본다. 또한, 특정 세그먼트에 대하여 인증 오류가 발생한 경우, 발생된 인증 오류로 인하여 추가적인 인증 오류 발생 여부를 분석하고 그 개선 방안을 제안한다.

II. MHT 기반 CCN Data 인증

1. MHT 기반 Data 인증

CCN은 MHT를 이용하여 콘텐츠의 개별 세그먼트에 대한 무결성 검증 및 CP 인증을 수행하고, 동시에 해당 세그먼트가 콘텐츠의 정상적인 세그먼트임도 검증한다[1]-[5]. Fig. 1은 MHT 기반의 CCN 콘텐츠 인증 절차를 설명한다.

가. 세그먼트 인증 정보 생성

CCN은 네트워크를 통하여 콘텐츠를 전송하기 위해 콘텐츠를 N ($\leq 2^n$) 개의 세그먼트들로 단편화 한다. Fig. 1은 $N=16=2^4$ 인 경우를 가정한 것이다. CP는 콘텐츠의 개별 세그먼트를 전송하기 위하여 다음과 같이 Data를 생성한다.

(1) 2^n개의 최하위 계층 노드(Leaf Node)로 구성된 이진트리(Binary Tree)를 생성한다. 생성된 이진트리는 $n+1$개의 계층(Level)으로 구성되며, 최하위 계층 노드는 0 계층 노드, 최상위 계층 노드(Root Node)는 n 계층 노드라 한다. 이진트리를 구성하는 모든 노드에는 상위 계층 노드부터 하위 계층 노드 순으로, 좌측 노드에서부터 우측 노드 순으로 유일한 노드 번호가 순차적으로 부여된다. 이진트리의 i번째 노드 N_i에 할당된 노드 값을 V_i라 한다.

(2) 콘텐츠를 구성하는 세그먼트는 단편화된 순서에 따라 생성된 이진트리의 최하위 계층 노드에 좌측 노드부터 순차적으로 할당 된다. Fig. 1에서 i번째 세그먼트(S_i)는 최하위 계층 노드 N_{i+N} ($=N_{i+16}$)에 할당 된다.

(3) 세그먼트 S_i의 해시 값 $H(S_i)$를 계산 한 후, 계산된 해시 값을 S_i에 할당된 최하위 계층 노드 N_{i+N}의 노드 값 V_{i+N}으로 부여한다. 여기서, $H()$는 단방향 해시 함수를 의미한다.

(4) 중간 및 최상위 계층 노드 N_i ($1 \leq i \leq 2^n-1$)의 두 자식 노드들(Child Nodes)을 N_{2i}와 N_{2i+1}이라 할 때, N_i의 노드 값 V_i는 $H(V_{2i}, V_{2i+1})$와 같이 계산된다. 예를 들어, Fig. 1에서 $V_4=H(V_8, V_9)$으로 계산된다. 이와 같은 방법으로 하위 계층 노드들부터 최상위 계층 노드까지 순차적으로 모든 노드 값들을 계산한다.

(5) 콘텐츠를 생성한 CP의 전자서명 키($priK$)를 이용하여 최상위 계층 노드 N_1의 노드 값 V_1에 대한 전자서명 값을 계산 한다: $E_{priK}(V_1)$.

(6) 개별 세그먼트 S_i 마다 할당된 최하위 노드 N_{i+N}의 노드 값 $V_{i+N}=H(S_i)$으로부터 V_1을 계산하기 위해 필요한 중간 계층 노드들의 노드 값들을 계산한다. 이 중간 계층 노드들의 노드 값들을 세그먼트 S_i의 인증정보(Witness)라고 한다. 인증정보는 해당 세그먼트에 대응하는 최하위 계층 노드부터 최상위 계층 노드까지를 연결한 인증경로(Path)에 포함된 노드의 형제 노드(Sibling Node)의 노드 값으로 구성된다. 예를 들어, Fig. 1에서 S_0의 인증경로는 N_{16}, N_8, N_4, N_2, N_1이고, 이 때 S_0의 인증정보는 N_{16}, N_8, N_4, N_2의 형제노드의 노드 값인 V_{17}, V_9, V_5, V_3이다.

(7) S_i, 인증정보, 그리고 $E_{priK}(V_1)$으로 구성된 Data를 생성하고 CCN을 통해 사용자에게 Data를 전송한다.

나. 세그먼트 인증 정보 검증

사용자가 요청한 S_i를 포함한 Data가 수신되면, 사용자는 다음과 같이 S_i를 검증한다.

(1) Data에 포함된 S_i와 인증정보를 이용하여 S_i에 할당된 최하위 계층 노드 N_{i+N}부터 최상위 계층 노드 N_1까지 연결한 인증경로 상에 있는 노드의 노드 값을 하위 계층 노드부터 차례로 계산하여 V_1을 획득한다. 예를 들어, Fig. 1에서 S_8이 포함된 Data는 인증정보 V_{25}, V_{13}, V_7, V_2를 포함한다. 사용자는 S_8과 인증정보를 이용하여 V_1을 다음과 같이 계산 한다.

$$V_1=H(H(H(H(S_8), V_{25}), V_{13}), V_7), V_2) \quad (1)$$

(2) 이렇게 계산된 V_1과 CP의 공개키를 이용하여 수신한 Data에 포함되어 있는 $E_{priK}(V_1)$을 검증한다.

(3) 콘텐츠 인증을 보다 효율적으로 수행하기 위하여 첫 번째 세그먼트(S_0) 검증 과정에서 수신된 Data의 $E_{priK}(V_1)$이 유효하면, 사용자는 S_0 검증 시, 계산된 V_1을 저장한다. 이 후, 해당 콘텐츠의 다른 세그먼트 S_i ($i>0$)를 검증 시, S_i의 인증정

보를 이용하여 계산한 V_1과 S_0 검증 과정에서 저장했던 V_1을 비교하여 두 값이 같으면, 전자서명 값을 검증하지 않아도 S_i가 인증된 것으로 간주한다.

2. MHT의 해시 값 계산 및 전송 중복도

MHT에 기반을 둔 콘텐츠 인증을 위해서는 각각의 세그먼트마다 서로 다른 인증정보 집합을 전송해야 한다. 그러나 콘텐츠 인증을 위해서 전송되는 모든 세그먼트들의 인증정보 집합들을 고려할 때, 같은 노드 값들이 인증정보 값으로 중복해서 전송되고, 상위 노드 값 계산을 위한 해시 값 역시 중복해서 계산된다. [10, 11]은 이와 같은 중복 전송 및 중복 계산으로 인한 비효율성을 각각 분석하였다.

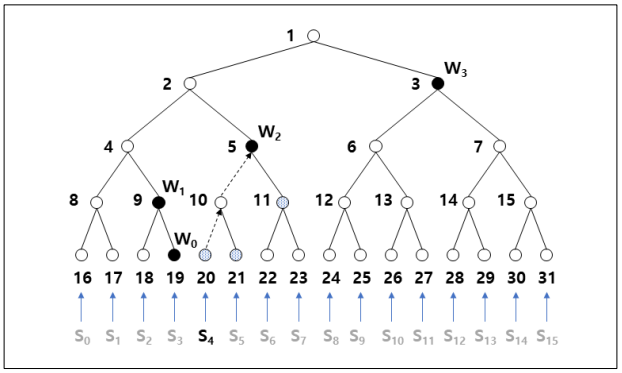

Fig. 2. MHT Transmission and Computation Optimization.
그림 2. MHT에 기반한 콘테츠 인증 기법의 최적화 방법

3. MHT의 중복 비효율성 개선

[12]는 인증정보 중복 전송과 해시 값 중복 계산의 비효율성을 개선하기 위한 최적화된 MHT 운영 방안을 제안하였다. [12]에 제안된 인증 방안은 수신된 인증정보의 노드 값들을 캐시(W_i)에 계층별로 각각 저장한 후, 이 값들을 다음 세그먼트 인증 과정에서 재활용 한다. Fig. 2는 [12]에서 제안된 인증정보 전송량과 노드 값 계산량을 최적화한 개선안을 설명한다. S_0을 포함하는 Data는 기존 CCN Data와 동일하게 모든 인증정보 V_{17}, V_9, V_5, V_3을 포함하며, 세그먼트 인증절차 또한 동일하다. S_0 인증이 완료되면, 수신된 인증정보는 $\{W_i\}$에 계층별로 저장된다. 이 후, 세그먼트 S_i $(i > 0)$의 인증은 다음과 같이 처리된다.

(1) i가 홀수이면, $H(S_i)$와 W_0의 값을 비교한 후, 두 값이 같으면 S_i가 인증된 것으로 간주한다.

(2) i가 짝수이면, 캐시에 저장된 인증정보에 대응하는 노드와 S_i의 인증경로 상의 노드가 최초로 교차하는 노드의 노드 값까지만 계산한다. 이와 같이 계산된 노드 값과 교차된 노드에 해당하는 캐시 값을 비교하여 두 값이 같으면 S_i가 인증된 것으로 간주하고, S_i와 함께 전송된 인증정보를 $\{W_i\}$에 계층별로 저장한다. Fig. 2에서 S_4를 인증할 때, 노드 N_5가 교차 노드이므로, V_5 값을 계산한 후, V_5 값과 W_2 값을 비교하여 두 값이 같으면 S_4가 인증된 것으로 간주한다. 인증이 정상적으로 완료되면, V_5 계산에 사용된 V_{21}과 V_{11}을 각각 W_0와 W_1에 저장한다.

일반적으로 MHT를 이용하여 콘텐츠를 인증하기 위해서는 $n \times 2^n$개의 인증정보 전송과 $n \times 2^n$번의 해시 값 계산이 필요하다. [12]에서 제안된 최적화된 MHT 운영 기법을 적용할 경우, $2^n - 1$개의 인증정보 전송과 $2^n - 1$번의 해시 값 계산이면 충분하다. 단, n개의 캐시를 운영하기 때문에 메모리 효율성이 다소 낮아 질 수 있다.

III. MHT 개선안의 오류 정도 분석

MHT를 이용한 세그먼트 인증 기법에서 하나의 세그먼트에 대한 검증을 완료하면, 해당 세그먼트 뿐만 아니라 함께 전송된 인증정보도 동시에 검증된 것이라 할 수 있다. 이와 같은 특성을 이용하여, [12]는 기본적으로 인증이 완료된 세그먼트의 인증정보를 $\{W_i\}$에 저장한다. 이 후, 다음 순번의 세그먼트들을 인증할 때 $\{W_i\}$에 저장된 인증정보를 재활용한다. 또한, 패킷 전송량을 줄이기 위하여 $\{W_i\}$에 저장된 인증정보는 중복해서 전송하지 않는다.

이와 같은 MHT 운영을 위해서는 콘텐츠를 구성하는 모든 세그먼트들이 순차적으로 손실 없이 수신되어야만 한다. 그러나 콘텐츠 서비스의 경우 일반적으로 TCP 보다는 UDP로 구현되는 경우가 많으며, CCN은 콘텐츠 (또는, 세그먼트)가 불특정 네트워크 노드들로부터 전송되고, 네트워크 성능을 향상하기 위하여 복수개의 세그먼트를 동시에 요청하는 기법도 제안되었다 [13]. 이와 같은 경우, 콘텐츠의 모든 세그먼트가 순차적으로 수신된다고 보장할 수 없다.

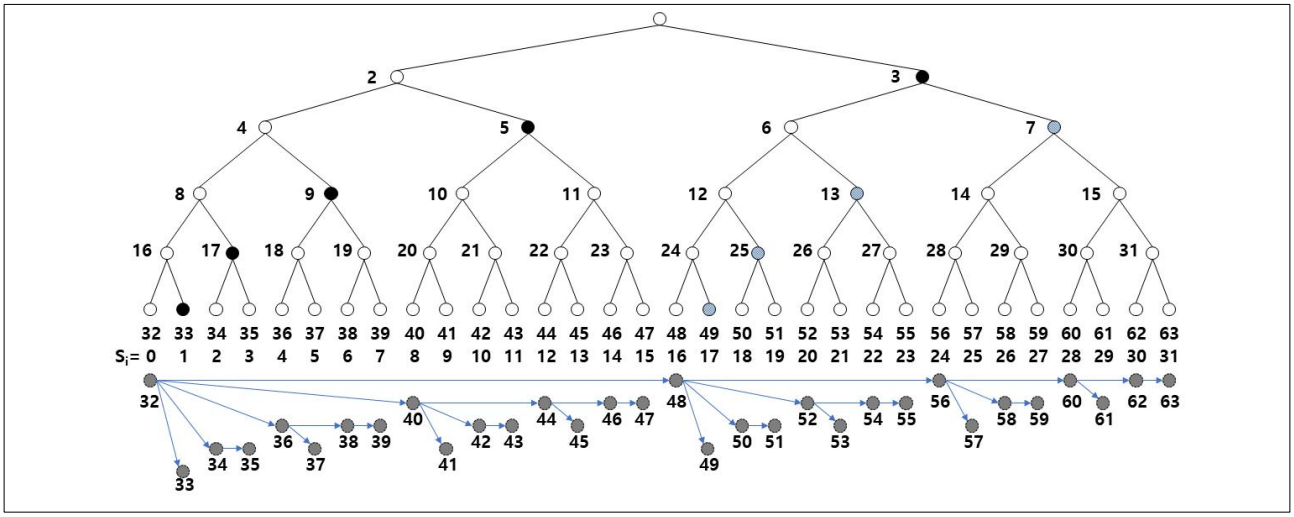

Fig. 3. The Description of Error Propagation of improved MHT.
그림 3. MHT에 기반한 콘텐츠 인증 기법의 개선에 따른 오류 발생 및 그 영향력

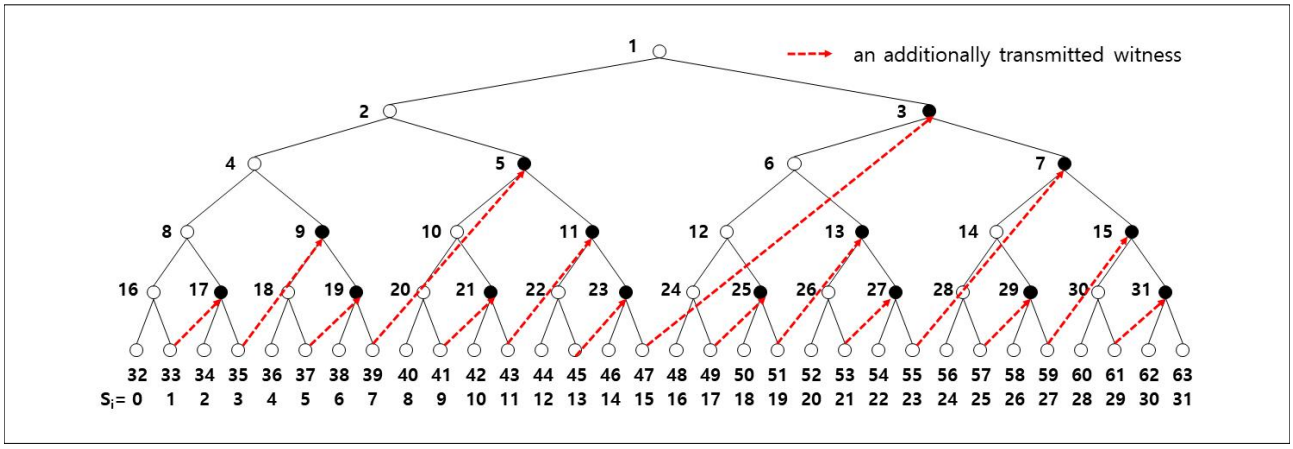

Fig. 4. Countermeasure for Authentication Error Propagation.
그림 4. MHT 기반한 콘텐츠 인증 개선안의 오류 제한 기법

만약 콘텐츠의 세그먼트가 순차적으로 전송되지 않거나 일부 세그먼트가 손실된다면, [12]의 인증 절차는 오류가 발생할 수 있다. Fig. 3은 이와 같은 오류 발생 가능성 및 발생된 오류의 영향력을 설명한다. 예를 들어 Fig. 3에서 N_{32}에 대응되는 콘텐츠 세그먼트 S_0이 정상적으로 수신되지 않은 상태에서 N_{48}에 대응하는 세그먼트 S_{16}이 먼저 수신되어, S_{16}을 인증하려고 한다면, S_{16} 인증을 위해 필요한 V_3가 W_4에 정상적으로 저장되어 있지 않기 때문에 S_{16}의 인증을 정상적으로 수행할 수 없다. 특히, 사용자가 S_0 인증을 정상적으로 완료하지 못했음을 인지하지 못한 상태에서 S_{16} 인증을 수행할 경우, 사용자가 W_4에 저장된 값을 그대로 사용한다면, S_{16}이 위/변조 되었다고 간주할 수 있다.

또한 이렇게 발생한 인증 오류는 하나의 세그먼트 인증에만 영향을 미치지 않고, 또 다른 세그먼트들의 인증도 정상적으로 수행되지 못하게 한다. 앞서 설명한 예에서 세그먼트 S_{16}을 인증할 수 없다면, 함께 전송된 인증정보 V_{49}, V_{25}, V_{13}, V_7의 유효성도 검증되지 않기 때문에 이 값들을 캐시에 저장할 수 없다. 이 경우, V_{49}, V_{25}, V_{13}, V_7을 교차 노드 값으로 이용하는 N_{49}, N_{50}, N_{52}, N_{56}에 대응하는 세그먼트 S_{17}, S_{18}, S_{20}, S_{24}를 정상적으로 인증할 수 없다. 또한, 이 세그먼트들이 인증되지 않았을 때 다음 순번의 세그먼트들도 인증할 수 없는 상황이 발생할 수 있다.

Table 1. Authentication Error Propagation.
표 1. 콘텐츠 인증 기술의 오류 전파 정도 분석

S_i	N_j	Error Propagation Degree						(x, y)
		1st	2en	3rd	4th	5th	Total Error	
0	32	5	10	10	5	1	31	(5, 0)
2	34	1	0	0	0	0	1	(1, 7)
4	36	2	1	0	0	0	3	(2, 3)
6	38	1	0	0	0	0	1	(1, 6)
8	40	3	3	1	0	0	7	(3, 1)
10	42	1	0	0	0	0	1	(1, 5)
12	44	2	1	0	0	0	3	(2, 2)
14	46	1	0	0	0	0	1	(1, 4)
16	48	4	6	4	1	0	15	(4, 0)
18	50	1	0	0	0	0	1	(1, 3)
20	52	2	1	0	0	0	3	(2, 1)
22	54	1	0	0	0	0	1	(1, 2)
24	56	3	3	1	0	0	7	(3, 0)
26	58	1	0	0	0	0	1	(1, 1)
28	60	2	1	0	0	0	3	(2, 0)
30	62	1	0	0	0	0	1	(1, 0)

Table 1은 Fig. 3과 같이 32개의 세그먼트로 구성된 콘텐츠의 세그먼트 S_i $(0 \leq i \leq 31)$가 정상적으로 인증되지 않았을 때, 해당 오류로 인하여 추가적으로 발생되는 세그먼트 S_j $(i < j)$ 인증 실패 경우의 수를 나타낸다. Table 1에서 i차 오류전파 정도 (Error Propagation Degree)는 $i-1$차 오류로 인하여 발생되는 오류의 개수를 의미한다. 예를 들어 세그먼트 S_0가 인증 실패된 경우, S_0의 인증정보 검증 실패로 인하여 5개의 세그먼트 S_1, S_2, S_4, S_8, S_{16}을 인증할 수 없다. 이를 S_0에 의한 1차 오류라고 한다. 1차 오류로 인하여 S_1, S_2, S_4, S_8, S_{16}과 함께 전송된 인증정보를 검증할 수 없고, 이 인증정보를 사용하여 세그먼트 인증을 수행하는 10개의 세그먼트 S_3, S_5, S_6, S_9, S_{10}, S_{12}, S_{17}, S_{18}, S_{20}, S_{24}를 인증할 수 없다. 이를 S_0에 의한 2차 오류라고 한다. 마찬가지로 2차 오류로 인한 인증정보 검증 실패로 인하여, 이 인증정보를 세그먼트 인증에 사용하는 10개의 세그먼트를 인증할 수 없다. 이를 S_0에 의한 3차 오류라고 한다. 이와 같이 S_0의 인증 실패로 인하여 연속적으로 인증되지 않는 세그먼트의 전체 수는 31개이다.

이와 같은 인증 오류전파정도는 다음과 같이 예측될 수 있다. $N=2^n$ 개의 세그먼트로 구성된 콘텐츠를 인증하기 위해 MHT를 사용할 때, 홀수 순번의 세그먼트 인증에 오류가 발생한 경우, 이러한 세그먼트 인증 오류로 인한 추가적인 세그먼트 인증 오류는 발생하지 않는다. 그러므로 짝수 순번의 세그먼트 S_k $(k=2r,\ 0 \leq r < 2^{n-1})$ 인증 오류만 고려하면 된다. 세그먼트 S_k의 인증 오류로 인하여 발생할 수 있는 추가 인증 오류의 개수는 다음과 같이 두 가지 방법으로 계산할 수 있다.

(1) 추가 인증 오류 수 예측-1

(a) $k = f(x,y) = 2^n - 2^x(1+2y)$를 만족하는 음이 아닌 정수 쌍 (x,y)를 찾는다. 이 때, $1 \leq x \leq n$, $y \geq 0$ 을 만족한다.

(b) 세그먼트 S_k의 인증 오류로 인하여 발생하는 추가 인증 오류의 수는 $2^x - 1$개이다.

Table 1의 $(x,\ y)$는 각각의 $k=S_i$에 대하여 $k=f(x,y)$ 의 해를 의미한다.

(2) 추가 인증 오류 수 예측-2

세그먼트 인증 오류 발생 시, 추가적인 세그먼트 인증 오류를 발생시키는 세그먼트에 대응하는 최하위 계층 노드는 항상 MHT의 부분트리에 포함된 첫 번째 최하위 계층 노드라는 특징이 있다. 이 때, 해당 부분트리의 최하위 계층 노드의 수를 2^k라고 하면, 첫 번째 최하위 노드에 대응하는 세그먼트의 인증 오류로 인하여 발생되는 추가 오류의 수는 $2^k - 1$개이다.

Ⅳ. 인증정보 전송 이중화

본 논문에서는 세그먼트 인증 오류 발생 시, 추가적으로 발생하는 인증 오류를 개선하기 위하여 중요한 인증정보를 이중으로 전송하는 방안을 제안한다.

[12]에서는 콘텐츠의 세그먼트 중 홀수 색인(Index)에 해당하는 세그먼트 전송 시, Data에 인증정보를 포함하지 않고 전송하도록 제안하였다. 본 논문에서는 이와 같은 홀수 색인의 세그먼트 S_i 전송 시, 다음 세그먼트 S_{i+1} 인증의 교차 노드 값을 전송하는 방안을 제안한다. 예를 들어 S_{15}를 전송할 때,

인증정보 V_3을 Data에 포함시켜 전송한다. 세그먼트들이 정상적으로 전송되어졌고, 전송된 세그먼트들이 정상적으로 인증되었다면 인증정보 V_3은 세그먼트 S_0가 전송될 때 사용자에게 전송되었을 것이다. 그러므로 V_3가 인증정보로 활용되기 전에 사용자는 두 번에 걸쳐 V_3 값을 전송받는다. 즉, 사용자는 S_{16}을 수신하기 전에 S_0 또는 S_{15} 중 적어도 하나의 세그먼트를 수신하여 성공적으로 세그먼트를 인증했다면, S_{16}을 정상적으로 인증할 수 있다.

Table 2는 이와 같이 인증정보 전송 이중화를 구현한 경우, 그 성능을 분석한 결과이다. 전송 오버헤드는 일부 증가하지만, 계산 및 저장 오버헤드는 [12]와 동일하게 유지할 수 있음을 알 수 있다.

Table 2. Performance Evaluation.
표 2. 콘텐츠 인증 기술의 성능 비교 분석

	Transmission Overheads	Computation Overheads	Storage Overheads
MHT	$n\times 2^n$	$n\times 2^n$	0
[12]	$2^{n+1}-2$	$2^{n+1}-2$ $(2^n+2^{n-1}-2)$	0 (n)
[13]	$2^n+2^{n-1}-2$	$3\times 2^n-2$	$2\times n$
[14]	2^n-1	2^n-1	n
Proposal	$2^n+2^{n-1}-2$	2^n-1	n

이 성능분석은 인증 오류발생에 따른 서비스 지연을 고려하지 않고 정상적인 상황을 가정하여 분석한 결과이므로, 향후 실제 네트워크 환경에서 오류 발생 가능성을 고려하여 서비스 지연 정도에 대한 정밀한 성능 분석이 요구된다.

Ⅴ. 결론

네트워크 성능 개선 및 서비스 효율성 개선을 위하여 CCN은 패킷 전송 경로 상의 네트워크 노드에 전송 데이터를 캐싱하고, 이를 활용하여 사용자의 콘텐츠 요청 메시지를 처리하도록 제안되었다. 중간 네트워크 노드에 의한 콘텐츠 요청 메시지 응답 처리를 통하여 CCN은 CP에게 집중되는 콘텐츠 요청 메시지를 효율적으로 분산 처리할 수 있다. 그러나 이와 같은 중간 네트워크 노드에 의한 콘텐츠 요청 메시지 응답 처리 시, 사용자는 자신이 수신한 콘텐츠의 실제 전송 노드를 식별할 수 없다는 문제점을 갖고 있다. 이와 같은 취약점으로 인하여 데이터의 위/변조를 통한 다양한 악의적인 공격이 가능하다. CCN은 이러한 취약점을 해결하기 위하여 MHT를 사용한 콘텐츠 인증 기법을 사용하고 있다. 그러나 MHT에 기반을 둔 콘텐츠 인증은 계산 및 전송 중복으로 인하여 비효율성이 발생할 수 있다. 이와 같은 비효율성을 개선하기 위하여 개선된 MHT 운영 방법들이 제안되었다.

본 논문에서는 개선된 MHT 운영 방법들을 적용할 경우, 하나의 세그먼트 인증 오류로 인하여 추가적으로 발생할 수 있는 세그먼트 인증 오류의 정도를 분석하고, 이와 같은 오류 전파를 방지하기 위한 방안을 제안한다. 제안된 기법은 세그먼트 인증에 필요한 최소의 인증정보를 추가적으로 전송하여 하나의 세그먼트 인증 오류로 인한 추가적인 인증 오류 발생 가능성에 대처하도록 설계되었다. 이로 인하여 제안된 기법은 인증정보 전송량은 다소 증가할 수 있지만 계산 및 저장 성능에는 차이가 없음을 성능 분석을 통하여 증명하였다.

References

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher and B. Ohlmann, “A Survey of Information-Centric Networking,” *IEEE Communications Magazine,* Vol.50, No.7, pp.26-36, 2012. DOI: 10.1109/MCOM.2012.6231276

[2] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs and R. Braynard, “Networking Named Content,” *5th International Conference on Emerging Networking Experiments and Technologies,* pp.1-12, 2009. DOI: 10.1145/1658939.1658941

[3] D. Kim, “Content Centric Networking Naming Scheme for Efficient Data Sharing,” *Journal of Korea Multimedia Society,* Vol.15, No.9, pp. 1126-1132, 2012. DOI: 10.9717/kmms.2012.15.9.1126

[4] “Trend and Improvement for Privacy Protection of Future Internet,” *Journal of Digital Convergence,* Vol.14, No.6, pp.405-413, 2016.
DOI: 10.14400/JDC.2016.14.6.405

[5] “A Comparison Study on Data Caching Policies of CCN,” *Journal of Digital Convergence,*

Vol.15, No.1, pp.327-334, 2017.
DOI: 10.14400/JDC.2017.15.2.327
[6] R. Merkle, "Protocol for public key cryptosystems," *IEEE Sympo. Research in Security and Privacy,* 1980. DOI: 10.1109/SP.1980.10006
[7] B. Georg "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis," *Ruhr-Universität Bochum. Retrieved.* 2013. DOI: 10.1.1.392.7879
[8] D. Y. Kim and J. S. Park, "Efficient Contents Verification Scheme for Contents-Centric-Networking," T*he Journal of Korean Institute of Comm. and Inform Sciences,* Vol.39, No.4, pp.234-241, 2014. DOI: 10.7840/kics.2014.39B.4.234
[9] D. Kim, "A Efficient Content Verification Scheme for Distributed Networking/Data Store," *Journal of The Korea Institue of Information Security & Cryptology*, Vol.25, No.4, 2015. DOI: 10.13089/JKIISC.2015.25.4.839
[10] D. Y. Kim, "Improvement of the Data Authentication of CCN," *Journal of Digital Convergence,* Vol.15, No.8, pp.341-349, 2017. DOI: 10.14400/JDC.2017.15.8.341
[11] D. Kim, "Network Overhead Improvement for MHT-based Content Authentication Scheme," *Journal of Digital Convergence,* Vol.16, No.1, pp.271-279, 2018. DOI: 10.14400/JDC.2018.16.1.271
[12] D. Kim, "The Shortest Authentication Path for Performance Improvement of MHT Contents Authentication Method in Distributed Network Environment," *KIPS Trans. Comp. and Comm. Sys.*, Vol.7, No.9, pp.235-242, 2018. DOI: 10.3745/KTCCS.2018.7.9.235
[13] D. Kim, "Group-Interest-based Verifiable CCN," Mobile Information System, Vol.2016 Article ID 9202151. 2016. DOI: 10.1155/2016/9202151

BIOGRAPHY

Dae-Youb Kim (Member)

1994 : BS degree in Math., Korea University.
1997 : MS degree in Math., Korea University.
2000 : PhD degree in Math., Korea University.

2000~2002 : Senior Engineer, SECUI .
2002~2012 : Senior Researcher and Project Manager, Samsung Electronics.
2012~ : Professor, Dept. of Information Security, Suwon University.