https://doi.org/10.14400/JDC.2017.15.8.341

CCN 데이터 인증 기술의 성능 개선 연구

김대엽
수원대학교 정보보호학과

Improvement of the Data Authentication of CCN

KIM DAEYOUB
Dept. of Information Security, Suwon Univ.

요 약 CCN은 네트워크 성능을 개선하기 위하여 데이터 전송 구간 위에 위치한 네트워크 중간 노드들이 전송 중인 데이터를 임시 저장한 후, 이 노드들이 해당 데이터에 대한 요청 메시지를 수신하면 임시 저장된 데이터를 이용하여 요청 메시지에 직접 응답할 수 있도록 설계되었다. CCN은 네트워크 중간 노드들에 의해서 요청 메시지가 응답될 수 있기 때문에, 호스트 중신 네트워킹 기술보다 빠른 응답 시간 구현과 데이터 전송량 감소를 실현할 수 있다. 그러나 중간 노드를 활용하는 네트워킹은 데이터 수신자가 데이터 제공자를 확인할 수 없기 때문에 데이터 위조를 이용한 공격에 쉽게 노출될 수 있다. 그러므로 안전한 CCN 구현을 위해서는 수신된 데이터를 인증해야 한다. 그러나 데이터 인증은 CCN 기반의 서비스 지연을 발생시키는 주요 원인 중 하나가 되고 있다. 본 논문은 CCN 데이터 인증의 문제점을 분석하고, 효율적인 CCN 인증 구현을 위하여 개선된 인증 절차를 제안하고, 그 성능을 평가한다.

주제어 : ICN, CCN, 콘텐츠 캐시, 데이터 인증, 머클 해쉬 트리

Abstract CCN proposes that intermediate network nodes on a network path for a transmitted data-packet cache the data-packet. If the nodes receive request packets for the cached data, the nodes can directly respond to the request-packets using the cached data. Since a request-packet can be responded by one of the intermediate nodes on a path of the request-packet, both faster response time and decreased data transmission amount are expected comparing to the existing host centric networking. However, CCN is vulnerable against forgery attacks because data-packet receivers cannot identify a data provider. Hence, a data authentication scheme is essentially needed to make CCN more secure. But such a data authentication process is one of the main causes of CCN-based service delays. This paper first analyzes the problems of a CCN data authentication scheme, then proposes an improved authentication operation scheme for efficiently authenticating data, and finally evaluates its performance.

Key Words : ICN, CCN, Content Cache, Data Authentication, MHT

* 이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 2017R1D1A1B03034215)과 수원대 교내 연구비 지원 사업(No. 2017-0016)의 결과임.
Received 18 May 2017, Revised 19 June 2017
Accepted 20 August 2017, Published 28 August 2017
Corresponding Author: Kim DaeYoub (Suwon Univ.)
Email: daeyoub69@suwon.ac.kr

ISSN: 1738-1916

1. 서론

네트워크를 이용하여 실시간 데이터 및 대용량 콘텐츠를 전송/공유하는 다양한 서비스가 증가하고, 특히 클라우드 기반의 다양한 IT 서비스가 광범위하게 보급/이용됨에 따라 네트워크 전송 용량의 폭발적이고 지속적인 증가가 예상되고 있다. 그러나 이와 같은 데이터 용량 증가를 처리하기 위하여 통신 선로를 전체적으로 확장시키는 것은 매우 많은 비용이 요구되며, 물리적인 통신 선로 확장 속도에 비하여 데이터 전송량 증가 속도가 더 빠른 추세이기 때문에 물리적 해결책 외에 네트워크 효율성을 개선할 수 있는 기술적 대안이 필요하다 [1, 2]. 이러한 대안 중 하나가 CDN (Content Delivery Network) 서비스와 P2P (Peer-to-Peer) 네트워킹 기술이라 할 수 있다. CDN/P2P는 사용자가 요청하는 콘텐츠를 원배포자 (Content Provider, CP) 뿐만 아니라 Proxy Server나 콘텐츠를 이전에 다운로드 받은 사용자들과 같이 다양한 경로를 통하여 요청된 콘텐츠를 제공할 수 있도록 설계되어, CP로 집중되는 요청을 효과적으로 분산 처리함으로써 네트워크 효율성을 개선할 수 있었다 [3, 4].

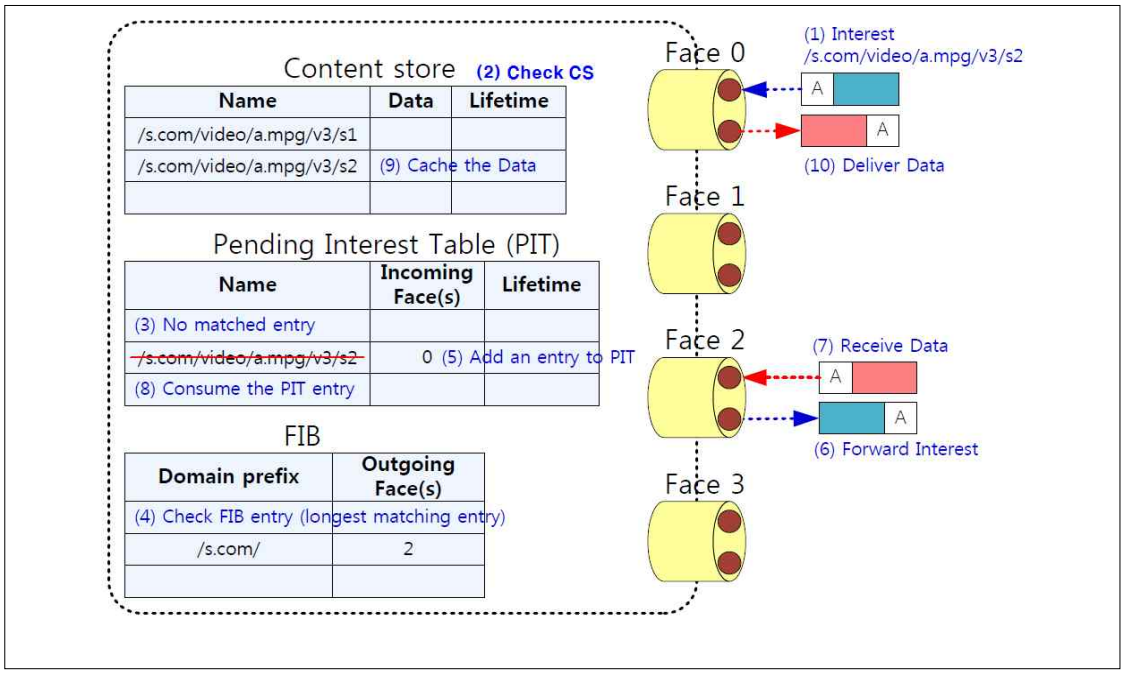
원격 호스트들 사이의 안전한 네트워크 연결을 구현하기 위하여 개발된 인터넷은 현재와 같이 다양한 서비스 적용과 대용량 데이터의 효율적인 전송 같은 변화에 효과적으로 대응할 수 있게 설계되지 않았다. 이로 인하여 데이터 전송량 증가로 인한 네트워크 병목현상, 인증 구조 부재와 같은 취약한 보안 구조로 인한 심각한 침해사고, 디바이스의 빈번한 이동으로 인한 비효율성 발생과 같은 다양한 문제점들이 발생하고 있다 [5]. 특히 다양한 IT 융복합 서비스의 증가는 이와 같은 인터넷의 문제점들을 더욱 심화시킬 것으로 예상되며, 인터넷이 갖고 있는 기본적인 취약점들은 IT 융복합 서비스의 저변확대를 방해하는 주요 요인이 될 것으로 우려되고 있다. 따라서 이러한 인터넷의 문제들을 해결하고, 인터넷을 통하여 다양한 데이터 및 정보를 보다 효과적으로 지원하기 위한 미래 인터넷 기술 연구가 다양하게 진행되고 있다 [6, 7, 8].

미래 인터넷 기술 중 하나인 정보 중심의 네트워킹 기술(Information Centric Networking)은 데이터 제공자 (CP)에게 집중되는 데이터 요청 메시지를 효율적으로 분산 처리하기 위하여 멀티미디어 프락시 서버(Multimedia Proxy Server)나 라우터와 같은 네트워크 노드 (Network Node)에 데이터를 임시 저장한 후, CP를 대신하여 이들 기기들이 데이터 요청 메시지를 직접 처리할 수 있도록 하는 기술을 제공하고 있다. ICN 기술 중 하나인 콘텐츠 중심 네트워킹 (Content-Centric Networking, CCN)은 데이터의 계층화된 고유 이름에 기반한 패킷 라우팅 기술과 네트워크 노드의 콘텐츠 임시 저장 (Caching) 기능을 이용하여 콘텐츠 요청 메시지를 네트워크 노드들이 직접 응답할 수 있도록 설계되었다 [7, 8, 9, 10, 11]. 그러나 CCN은 네트워크 전송 효율성을 높이기 위하여 네트워크 노드에 캐싱 되어 있는 데이터를 이용하므로, 기존 호스트 중심 네트워킹과는 달리 실제 데이터를 제공하는 호스트를 사용자가 식별할 수 없다. 이와 같은 취약점을 악의적으로 이용하여 CCN을 활용하는 서비스를 공격할 경우, 데이터 위/변조로 인한 해킹 가능성이 매우 높다. 그러므로 CCN은 네트워크를 통해 전송되는 모든 데이터에 최초 생성자의 전자 서명을 포함시키도록 요구하여 이러한 공격 가능성에 대응하고 있다. 특히, CCN은 대용량 콘텐츠 전송을 지원하기 위해 콘텐츠를 단편화하여 일정 크기 이하의 세그먼트들로 나눈 후, 각각의 세그먼트를 모두 인증한다. 그러나 이와 같은 세그먼트 단위의 인증 정책은 콘텐츠 수신에 소요되는 시간에 비해 콘텐츠의 전체 세그먼트들을 인증하는데 소요되는 시간이 매우 길기 때문에 서비스 지연의 주요 원인이 된다.

본 논문에서는 CCN의 데이터 인증 기술을 분석하고, 그 성능을 평가한다. 또한 CCN 성능 개선을 위해 보다 효율적으로 인증 기술을 운용할 수 있는 개선안을 제안하고 그 성능을 평가한다. 제안된 기법은 인증에 소요되는 시간뿐만 아니라 인증을 위해 필요한 데이터의 전송량도 기존 CCN 인증 기술에 비해 개선할 수 있다.

2. 콘텐츠 중심 네트워킹

CCN은 인터넷의 문제점들을 해결하고 네트워크 효율성을 개선하기 위하여 데이터 고유 이름 기반의 패킷 라우팅 기능, 중간 네트워크 노드에서의 데이터 캐싱 및 포워딩 기능, 그리고 전자 서명 기반의 데이터 인증 기능을 제공 한다 [7]. CCN은 콘텐츠 세그먼트 요청 메시지 (Interest) 전송에 의하여 네트워킹 프로세스가 진행되며,



[Fig. 1] CCN Packet Forwarding Process

Interest에 대응되는 응답 메시지(Data)는 Interest가 전송된 경로의 역경로를 따라서 사용자에게 전송된다. 이와 같은 특징을 효과적으로 구현하기 위하여 CCN은 IP 주소와 같은 호스트 식별자 (Host Identity) 대신에 콘텐츠 식별자인 콘텐츠 이름(Content Name)을 기반으로 Interest/Data의 라우팅을 결정한다. 특정 원격 호스트들 사이의 네트워크 연결을 주된 목적으로 개발된 호스트 식별자 기반의 네트워킹 기술과 달리 CCN은 콘텐츠의 효과적인 전송/배포를 목적으로 다양한 중간 노드들로부터 콘텐츠를 수신할 있기 때문에 호스트 식별자가 네트워킹에서 큰 의미를 갖지 못한다. 그 대신에 CCN을 구현하기 위해서는 Interest 전송 경로 상의 네트워크 노드들이 네트워크 계층 정보만으로 요청된 콘텐츠의 캐싱 여부를 확인할 수 있어야 한다. 그러므로 네트워크 계층 정보에 콘텐츠 식별자 정보가 반드시 포함 되어야 한다. 또한, 콘텐츠 이름만을 이용하여 Interest를 라우팅하기 위하여 콘텐츠 이름은 계층적으로 구성한다. 계층적으로 구성된 콘텐츠 이름은 네트워크 상에서 해당 콘텐츠를 유일하게 식별할 수 있어야 하고, 동시에 Interest를 해당 콘텐츠의 생성자에게 전송할 수 있도록 구성해야 한다. 또한, 데이터의 위/변조 여부를 사용자가 검증 할 수 있도록 전송되는 Data는 원생성자(Publisher)의 전자 서명을 포함하고 있으며, 사용자는 이 전자 서명 값을 이용하여 Publisher 확인과 데이터 위/변조 여부를 검증한다. 또한, 호스트 중심 네트워킹과 달리 네트워크 노드는 콘텐츠 요청 정보 테이블(Pending Interest Table, PIT)과 네트워크 캐시(Content Store, CS)를 자체적으로 운영한다. PIT는 수신된 Interest와 해당 Interest가 유입된 경로(Incoming Face) 정보를 기록/관리한다. Data 수신 시, 해당 Data에 대응하는 Interest의 정보를 PIT에서 획득한 후, Data를 기록된 Face를 통하여 전송한다. 또한, 네트워크 노드들은 전송 중인 Data를 노드의 CS에 캐싱 한다. CS에 캐싱 된 Data에 대한 요청을 수신하면, 저장된 Data를 사용하여 해당 Interest에 즉시 직접 응답하고, Interest 처리 절차를 종료한다.

[Fig. 1]은 CCN의 Interest와 Data 처리 절차를 설명한다:

(1) 노드의 인터페이스 (Face 0)로 Interest를 수신한다.

(2) Interest에 대응되는 데이터가 CS에 저장되어 있는지 여부를 확인한다. 만약 해당 데이터가 저장

되어 있다면, 저장되어 있는 데이터를 Interest가 수신된 Face 0을 통하여 요청자에게 전송한 후, 수신한 Interest 처리를 완료한다.

(3) 수신한 Interest와 같은 콘텐츠 이름을 갖는 기록이 PIT에 존재하는지 확인하다. 만약 대응되는 기록이 PIT 내에 존재한다면, 해당 기록에 Face 0을 추가한 후, 수신한 Interest 처리를 완료한다.

(4) PIT에 대응되는 기록이 없다면, 포워딩 정보(Forwarding Information Base, FIB) 테이블을 참조해서 Interest를 포워딩할 Face (예를 들어, Face 2)를 선택한다. FIB 테이블은 Interest에 포함되어 있는 콘텐츠 이름을 기반으로 해당 Interest를 포워딩할 물리적/논리적 전송 Face를 결정할 때 필요한 정보를 제공한다. CCN에서는 Interest의 콘텐츠 이름과 FIB 테이블 정보를 비교한 후 Longest Prefix Matching 원칙에 따라 Interest를 포워딩할 Face를 결정한다.

(5) PIT에 수신한 Interest를 위한 새로운 기록을 추가한다.

(6) 단계 4에서 선택된 Face 2로 수신한 Interest를 전송한 후, 해당 Interest 처리 절차를 완료한다.

(7) 이 후, 해당 노드의 인터페이스 (Face 2)로 Data가 수신된다.

(8) 수신된 Data에 대응하는 기록이 PIT에 존재하는지 확인한다. 만약 대응되는 기록이 PIT에 존재하지 않는다면, 수신한 Data를 폐기한 후 Data 처리 절차를 종료한다.

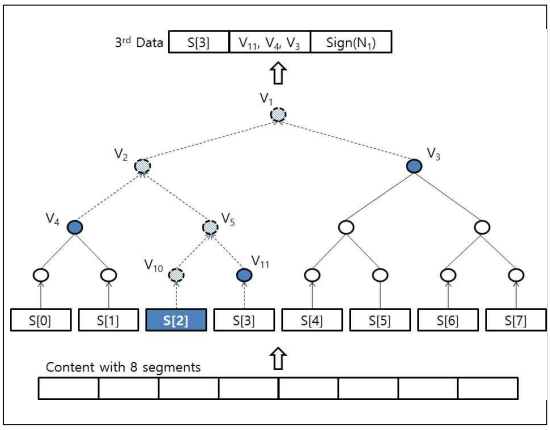
(9) 수신된 Data를 노드의 CS에 저장한다.

(10) 단계 8에서 검색된 PIT 기록에 있는 Face들 (예를 들어, Face 0)로 Data를 전송한 후, PIT에서 해당 기록을 삭제한다.

3. CCN 데이터 인증

3.1 머클 해쉬 트리 기반 데이터 인증

CCN은 콘텐츠를 일정 크기의 세그먼트로 단편화한 후, 각각의 세그먼트를 독립된 Data로 간주해서 처리한다. 그러므로 안전한 콘텐츠 전송을 위하여 CCN은 콘텐츠 생성자 인증뿐만 아니라 세그먼트 인증이 필요하다.



[Fig. 2] CCN MHT-based Authentication Process

콘텐츠 생성자 인증은 수신된 콘텐츠의 최초 생성자의 신원을 식별하고 인증하는 것을 의미한다. 이러한 인증을 통해서 수신된 콘텐츠의 신뢰성을 일차적으로 검증할 수 있다. 콘텐츠 생성자 인증 외에도 만약 수신된 세그먼트가 요청한 콘텐츠의 세그먼트가 아니면, 콘텐츠 전체를 수신 한 후에도 해당 콘텐츠를 정상적으로 이용하지 못할 수도 있다. 그러므로 수신된 세그먼트가 사용자가 요청한 콘텐츠의 단편화된 세그먼트임을 검증하는 세그먼트 인증이 추가로 필요하다. 이와 같은 인증 요구사항을 만족시키기 위하여 CCN은 머클 해쉬 트리(Merkle Hash Tree, MHT) 기반의 데이터 인증 기법을 제안하였다 [11, 12, 13, 14, 15]. [Fig. 2]는 MHT 기반의 콘텐츠 인증 절차를 예를 들어 설명한 것이다. 콘텐츠 생성자는 다음과 같은 과정을 수행한다:

(1) 콘텐츠를 일정 크기로 단편화하여 N ($\leq 2^n$) 개의 세그먼트들을 생성 한 후, 2^n개의 리프 노드(Leaf Node)로 구성된 이진 트리(Binary Tree)를 구성한다. 각각의 세그먼트들은 콘텐츠 구성 순서에 따라 생성된 이진 트리의 리프 노드에 할당된다. [Fig. 2]는 $N=8$ 인 경우를 가정한다.

(2) 세그먼트의 해쉬 함수 값을 각각 계산 한 후, 세그먼트에 대응된 리프 노드의 노드 값으로 할당한다. [Fig. 2]에서 i번째 세그먼트에 할당된 리프노드의 노드 값은 $V_{N+i-1} = H(S[i])$이다.

(3) 리프 노드들을 제외한 k번째 노드의 노드 값 V_k를 다음과 같이 계산 한다:

$$V_k = H(V_{2k} || V_{2k+1}). \quad (1)$$

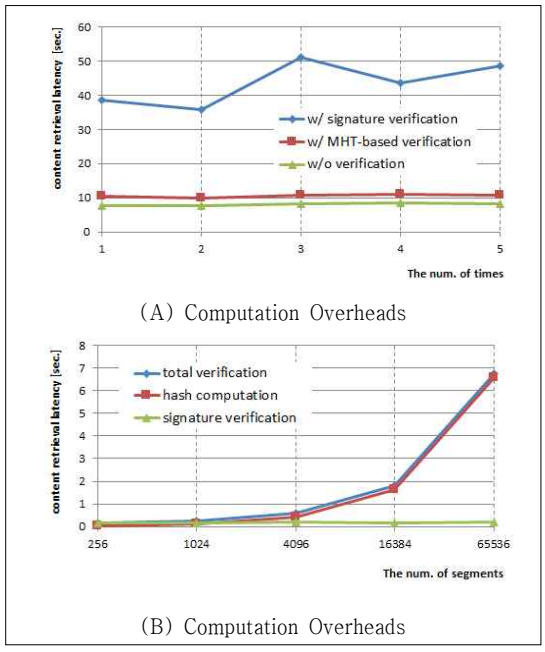
여기서 V_{2k}와 V_{2k+1}은 k번째 노드의 두 자식 노드들(child nodes)의 노드 값들을 의미한다. 이와 같은 방법을 반복적으로 수행하여 하위 노드들부터 루트 노드까지 각각의 노드 값들을 순차적으로 계산하여 각각의 노드에 할당 한다.

(4) 콘텐츠 생성자의 전자 서명 키를 이용하여 루트 노드 값 V_1에 서명하여 $sign = Sign(V_1)$을 생성한 후, 콘텐츠의 세그먼트와 $sign$을 함께 패키징하여 Data를 생성한다.

(5) i번째 세그먼트 전송을 위한 Data가 수신되었을 때, 사용자가 Data와 함께 수신된 $sign$을 검증하기 위해서는 V_1을 계산할 수 있어야 한다. 이를 위하여 각각의 세그먼트 마다 $sign$ 검증에 필요한 중간 노드들의 노드 값들($witness$)을 계산한 후, $witness$를 Data에 추가로 패키징한다. 즉, 해당 세그먼트에 대응하는 리프 노드부터 루트 노드까지의 경로(Path)에 포함된 노드들의 형제 노드(Sibling Node)의 노드 값을 세그먼트와 함께 전송하여 사용자가 $sign$을 검증할 수 있도록 한다.

(6) 콘텐츠 사용자가 요청한 콘텐츠에 대응하는 Data를 수신하면, Data에 포함된 세그먼트와 $witness$를 이용하여 리프 노드부터 루트 노드까지의 노드 값들을 차례로 계산하여 V_1을 획득한 후, $sign$을 검증한다.

데이터 인증을 보다 효율적으로 수행하기 위하여, CCN은 첫 번째 세그먼트 검증 단계에서 수신된 $sign$이 유효하다면, 사용자는 이 때 계산된 V_1을 임시 저장한다. 이 후, 다음 Data를 검증할 때에는, 해당 Data로 부터 계산된 V_1과 앞서 저장된 V_1을 비교하는 것으로 세그먼트 검증을 대신한다. 각각의 세그먼트 검증 시, 매번 $sign$을 검증할 필요가 없으므로 세그먼트 검증에 소요되는 시간을 효과적으로 줄일 수 있다. 그러나 MHT를 대용량 콘텐츠 배포에 적용할 경우, 각각의 세그먼트 마다 $witness$ 전송해야만 하고, V_1 계산을 위하여 하위 노드 값들을 반복적으로 계산해야만 한다. 이러한 전송 및 계산 오버헤드는 여전히 전체 서비스 지연의 한 원인이 될 수 있다. [Fig. 3]은 안드로이드폰 사용자가 CCN을 통해 배포된 콘텐츠를 이용할 때, 콘텐츠 인증으로 인한 서비스 지연 정도를 분석한 결과이다. [Fig. 3]-(A)는 256개의 세그먼트로 구성된 콘텐츠를 요청할 때 세그먼트 인증을 위하여 서명을 각각 검증하는 경우, MHT를 이용하여 세그먼트를 검증하는 경우, 그리고 세그먼트 검증 절차를 생략한 경우를 가정하고 콘텐츠를 요청하여 이용하는데 까지 소요된 시간을 5회 측정한 결과의 평균치이다. [Fig. 3]-(B)는 앞선 실험 결과를 바탕으로 세그먼트의 수가 증가하는 경우를 가정하여 소요 시간을 계산한 결과로, 세그먼트 수가 증가할수록 해쉬 계산에 소요되는 시간이 전체 인증 시간의 대부분을 차지함을 알 수 있다. 특히 CCN은 세그먼트의 크기를 규정하고, 콘텐츠를 규정된 세그먼트 크기 이하로 단편화하도록 요구하고 있기 때문에, 콘텐츠 세그먼트의 크기/수와 전송되는 인증 정보의 양은



[Fig. 3] CCN MHT-based Authentication Overheads

$$cs = \sum_{i=1}^{2^n} (fs + (n \times hs)) \quad (2)$$

으로 계산된다. 여기서, cs, fs, hs는 각각 content size, fragment size, hash value size를 의미한다. 그러므로 각

각의 세그먼트에 포함되는 $witness$의 개수가 많을수록 콘텐츠를 더 작은 크기로 단편화해야 된다. 그러므로 전송되는 인증 정보의 양을 줄임으로써 세그먼트를 보다 효율적으로 구성할 수 있다.

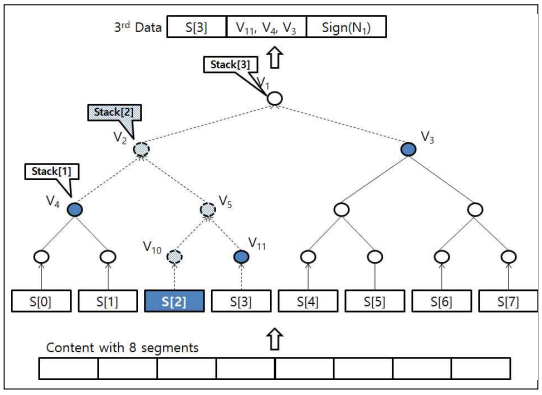
<Table 1> The degree of duplicated calculation of node values

	$N=2^8$	$N=2^{10}$	$N=2^{12}$	$N=2^{14}$	$N=2^{16}$
V_1	256	1024	4096	16384	65536
V_2	128	512	2048	8192	32768
V_4	64	256	1024	4096	16384
V_8	32	128	513	2048	8192
V_{16}	16	64	256	1024	4096
V_{32}	8	32	128	512	2048

3.2 MHT 운영 개선

MHT를 기반한 콘텐츠 인증의 비효율성은 노드 값 계산의 중복성 때문에 발생한다. <Table 1>은 콘텐츠를 구성하는 세그먼트의 개수에 따라 발생하는 중복계산 회수를 나타낸다. 이와 같은 중복 계산은 동일 계층 노드의 경우 동일한 회수의 중복이 발생한다. 또한 k 번째 계층의 노드 값을 한번 계산하기 위해서는 k번의 해쉬 값 계산이 필요하다. 그러므로 $N=2^{16}$ 인 경우, 콘텐츠 인증을 위해 모든 세그먼트들에서 V_1 값 계산을 위해 1,048,576회의 해쉬 값 계산이 필요하다. 일반적으로 해쉬 함수가 고속 연산이 가능하다고 하더라도 대용량 콘텐츠의 경우 이와 같이 중복된 해쉬 값 계산은 전체 서비스 지연의 주요 요인이 될 수 있다.

중복 계산에 따른 비효율성 문제를 해결하기 위하여 일반적으로 동적 프로그래밍 기법을 적용한 개선된 알고리즘을 적용한다[16]. 동적 프로그래밍 기법은 중복 계산이 발생하는 알고리즘을 효과적으로 구현하기 위하여 계산된 결과 값을 일부 저장한 후, 이 값을 이용하는 방식으로 비효율성을 해결한다. [Fig. 4]는 본 논문에서 제안하는 동적 프로그래밍 기법을 이용한 MHT 운용 방안을 예를 들어 설명한다. 세그먼트 S[1] 인증 시, 인증 경로 상의 노드 값들을 노드의 계층에 따라 스택에 저장된다. 다음 세그먼트인 S[2]를 수신한 사용자는 S[2]를 인증하기 위해 계산해야 되는 인증 경로 상의 노드들과 이전 인



[Fig. 4] Improved MHT-based Authentication Process

증 단계에서 스택에 저장된 노드들을 하위 계층부터 계층 별로 비교하여 동일 노드를 탐색한다. 탐색된 노드 중 최하 계층의 노드를 선택한다. [Fig. 4]에서는 노드 N_2가 선택된다. 이 경우, 세그먼트 S[2]를 인증하기 위해서 사용자는 루트 노드 N_1의 노드 값까지 계산하지 않고 노드 N_2의 노드 값까지만 계산 한 후, 스택에 저장된 값과 비교하면 충분하다. 제안하는 콘텐츠 인증 절차를 일반화한 방법은 다음과 같다: 콘텐츠를 구성하는 세그먼트의 수를 $N=2^n$개라고 가정하고, 이와 같은 콘텐츠를 처리하기 위한 MHT의 크기(Level)를 n이라 하자. 각각의 세그먼트에는 구성 순서에 따라 세그먼트 번호 ($sn=\{0,1,2,...,N-1\}$)가 할당되며, 세그먼트의 인증을 위해 전송되는 $witness$를 구성하는 노드의 레벨을 i라 할 때, 해당 노드의 값을 $w[i]$라 하자. 한 개의 리프 노드부터 루트 노드까지의 경로를 인증 경로(Authentication Path)라고 하자. 이 인증 경로 위의 노드들의 노드 값을 각 레벨마다 저장한 값을 $stack[i]$라고 하자.

(1) 첫 번째 세그먼트를 수신한 사용자는 첫 번째 리프 노드부터 루트 노드까지의 인증 경로에 있는 노드 값들을 계산한 후, 루트 노드의 서명 값을 검증한다. 검증에 성공하면 첫 번째 세그먼트가 인증된 것으로 간주하고, 인증 경로 상의 노드 값들을 대응하는 $stack[i]$에 각각 저장한다.

(2) 다음 세그먼트를 수신한다. 수신된 세그먼트에 할당된 리프 노드부터 루트 노드까지의 인증 경로를 계산한다. 계산된 인증 경로 상의 노드들과 $\{stack[i]\}$에 저장된 노드들을 하위 계층부터 비

교하여 같은 노드가 있는지 확인한다. i번째 세그먼트의 경우, $k=0$부터 순차적으로 증가 시키면서 i가 2^k의 배수인지 확인한다. 만약 i가 2^k의 배수이면, 인증 경로 상의 $k+1$번째 계층의 노드와 $stack[k+1]$에 저장된 노드가 동일한 노드이다. 이 노드를 인증 노드라고 부르고, i번째 세그먼트의 인증 노드를 $N_{a[i]}$라고 표시하자.

(3) 이 경우, 사용자는 인증 경로 상의 노드들 중에서 리프 노드부터 $k+1$ 계층 노드까지의 노드 값들을 순차적으로 계산한다.

(4) 계산된 $k+1$ 계층 노드 값 ($V_{a[i]}$)과 $stack[k+1]$의 값을 비교하여 두 값이 같은지 확인한다. 만약 두 값이 같다면 수신한 세그먼트가 인증된 것으로 간주한다.

(5) 리프노드부터 k 계층 노드까지 계산된 값들로 $\{stack[0],...,stack[k]\}$의 값들을 갱신한다.

(6) 마지막 세그먼트를 인증할 때까지 (2)~(5) 단계를 반복 수행한다.

<Table 2>는 개선된 MHT 운영 방법을 이용하여 콘텐츠를 인증하는 유사 코드(pseudo code)를 나타낸다. 본 논문에서 제안하는 MHT 운영 방법은 콘텐츠 요청자의 인증 절차만을 수정하여 적용할 수 있다. 이 경우, 사용자 측면에서 콘텐츠 인증 절차를 수행하는데 소요되는 시간은 단축되나 불필요하게 전송되는 인증 정보로 인한 전송량 개선은 이뤄지지 않는다. 그러므로 제안하는 개선안을 적용할 경우, 불필요한 인증 정보를 제외한 세그먼트를 생성하여 전체 전송량을 개선하는 방안을 제안한다. 전송된 세그먼트 $S[k]$의 인증 과정을 분석할 때 스택에 저장된 노드들과의 비교를 통해서 이전 세그먼트 $S[k-1]$의 인증 경로와 동일한 노드의 계층을 r이라 하면, $S[k]$인증에 필요한 인증 정보 중에서 $w[r-1]$은 스택에 저장되어 있음을 알 수 있다. 그러므로 $S[k]$의 인증을 위해서 필요한 인증 정보는 $\{w[0],...,w[r-1]\}$이면 충분하다. 이 경우, 세그먼트의 번호가 홀수인 세그먼트는 $r=1$이므로 필요한 인증 정보가 $w[0]$ 뿐이고, 이 값은 이미 스택에 저장되어 있기 때문에 인증 정보를 전송할 필요가 없다. 이와 같은 방법으로 세그먼트를 구성하는 절차는 <Table 3>과 같다.

<Table 2> Segments Authentication Pseudo Code

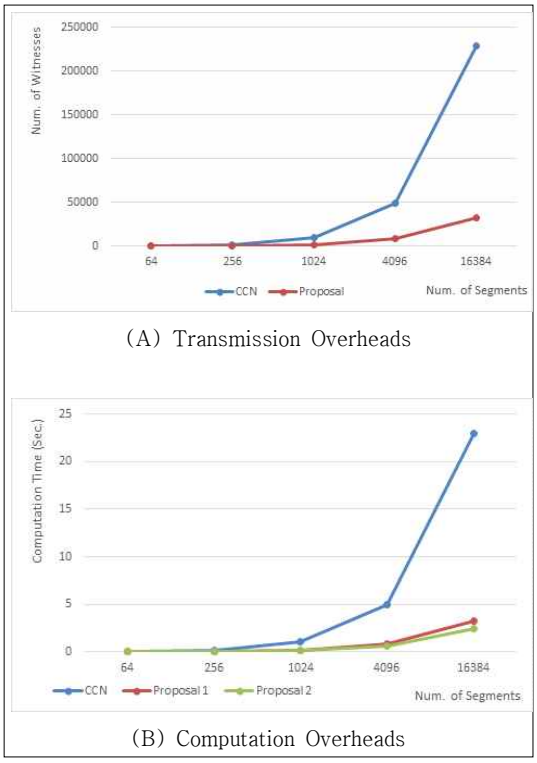
```
FOR segment number i = 0 to 2^n − 1 :
  RECEIVE i-th segment (sn[i])
  SET mask := 1;
  FOR level = 0 to n − 1 :
    IF (i & mask) is not zero THEN
       STOP this routine
    ELSE
       SET mask := mask << 1
    ELDIF
  ENDFOR
  FOR j = 0 to level :
    RECEIVE j-th witness (w[j])
    CALCULATE a hash, h = H(w[j], stack[j])
    IF j < level THEN
      SET stack[j+1] := h
    ELSE
      IF stack[j+1] ≠ h THEN
        REPORT an error
      ENDIF
    ENDIF
  ENDFOR
ENDFOR
```

<Table 3> Segments Generation Pseudo Code

```
FOR segment number i = 0 to 2^n − 1 :
  READ the i-th fragment (cf[i]) of content
  SET mask := 1;
  FOR level = 0 to n − 1 :
      IF (i & mask) is not zero THEN
          STOP this routine
      ELSE
          SET mask := mask << 1
      ELDIF
  ENDFOR
  FOR j = 0 to level − 2 :
      GENERATE j-th witness (w[j])
  ENDFOR
  GENERATE S[i]
          using cf[i] and {w[j]}_{j=0,...,level−2}
ENDFOR
```

3.3 성능 분석

제안된 운영 방안의 성능을 분석하기 위하여 세그먼트 인증 시 필요한 $witness$의 전송량과 해쉬 계산량을 각각 분석한다. 콘텐츠를 구성하는 세그먼트의 수를 $N=2^n$이라 하면, CCN에 구현된 MHT의 기본적인 운영 방법을 적용할 때, 각각의 세그먼트는 n개의 인증 정보를 포함한다. 그러므로 콘텐츠를 구성하는 전체 세그먼트들을 고려할 때 $n \times 2^n$개의 인증 정보가 전송되어야



(A) Transmission Overheads

(B) Computation Overheads

[Fig. 5] Improved MHT-based Authentication Overheads

한다. 그러나 개선 안의 경우 $\sum_{i=1}^{n} 2^i = 2(2^n - 1) = 2 \times 2^n - 2$ 개의 인증 정보 전송이 필요하다. [Fig. 5]-(A)는 인증 정보 전송량을 비교한 것이다. [CCN]은 MHT의 기본적인 운영 방법을 구현한 경우이며, [Proposal]은 개선된 운영 방법을 구현한 결과이다. 세그먼트의 수가 많은 수록 개선안의 전송량 개선 효과가 두드러짐을 알 수 있다. 세그먼트의 수가 1만개 이상인 경우, 기존 대비 전송량을 15% 이하로 줄일 수 있다. 또한, 현재 CCN은 기본 4K 바이트로 세그먼트를 구성하도록 기본 설정되어 있다. 이 경우, n이 4보다 크면 세그먼트를 구성하는 인증 정보가 콘텐츠보다 더 큰 용량을 차지하게 되어 매우 비효율적일 수 있다.

콘텐츠의 세그먼트들을 수신한 사용자가 CCN의 기본 구현에 따라서 수신된 세그먼트를 모두 인증하기 위해서는 $n \times 2^n$번의 해쉬 값 계산이 요구된다. 개선 안을 적용할 경우, 루트 노드부터 리프 노드의 부모 노드들까지 모든 내부 노드들의 노드 값들이 두 번씩 계산된다. 그러므로 전체 해쉬 값계산 회수는 $2 \times \sum_{i=0}^{n-1} 2^i = \sum_{i=1}^{n} 2^i = 2(2^n - 1) = 2 \times 2^n - 2$번이다. 만약 이전 세그먼트의 인증 시, 인증 정보로 전송되는 다음 세그먼트의 해쉬 값 정보를 저장한다면, 콘텐츠 인증에 필요한 해쉬 계산 회수는 $2 \times \sum_{i=0}^{n-2} 2^i + 2^{n-1} = 2^n + 2^{n-1} - 2$이 된다.

[Fig. 5]-(B)는 인증 정보를 활용하여 세그먼트들을 인증할 때 계산량을 시간으로 비교한 것이다. [CCN]은 MHT의 기본적인 운영 방법을 구현한 경우이며, [Proposal 1]은 개선된 운영 방법을, [Proposal 2]는 인증 정보의 일부를 저장/이용하는 기능을 추가로 적용한 방법을 구현한 결과이다.

4. 결론

CCN은 네트워크 노드에 캐싱 된 데이터를 활용하여 네트워크의 효율성을 높이기 위해 제안되었다. 이와 같은 목적을 달성하기 위하여 CCN은 콘텐츠 생성자에게 집중되는 요청 메시지를 효과적으로 분산 처리할 수 있게 네트워크 노드에 캐싱 기능을 구현하고, 캐싱되어 있는 콘텐츠에 대한 요청 메시지를 수신한 네트워크 노드가 콘텐츠 생성자를 대신하여 해당 요청 메시지에 응답할 수 있게 설계되었다. 그러나 이와 같은 중간 노드에 의한 응답 처리는 사용자가 실제 콘텐츠를 전송한 노드를 식별할 수 없기 때문에 호스트 인증 기반의 보안 체계를 적용할 수 없다는 문제점과 함께 데이터의 위/변조가 가능하다는 취약점을 갖고 있다. 이러한 문제를 해결하기 위해 CCN은 MHT를 사용한 콘텐츠 인증 기법을 제안하고 있다. 그러나 MHT를 이용한 콘텐츠 인증은 해쉬 값을 중복해서 계산해야하기 때문에 대용량 콘텐츠 전송 및 인증 시 서비스 지연 요인이 될 수 있다. 본 논문에서는 이러한 문제점을 개선하기 위하여 앞서 계산된 세그먼트의 인증 정보를 저장한 후, 다음 세그먼트에서 활용하는 동적 알고리즘 기법을 적용하여 해쉬 값의 중복 계산 문제를 개선함으로써 CCN의 인증 비효율성을 개선하였다. 본 논문에서 제안된 기법을 적용할 경우, 대용량 콘텐츠 인증 시간을 60~85%까지 개선할 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 (2017R1D1A1B03034215) and by Suwon Univ. Research Grant (2017-0061).

REFERENCE

[1] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015 – 2020," Cisco Public, February 3, 2016

[2] "Cisco Visual Networking Index: Forecast and Methodology, 2015 – 2020," Cisco Public, February 3, 2016

[3] A. K. Pathan, and R. Buyya, "A Taxonomy and Survey of Content Delivery Networks," Tech Report, Univ. of Melbourne, 2007.

[4] E. Meshkova, J. Riihijarvi, M. Petrova, and P. Mahonen, "A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks," Computer Networks J., Vol. 52, No. 11, pp. 2097 – 2128, 2008.

[5] D. Clark, "The Design Philosophy of the DARPA Internet Protocols," ACM Sigcomm Comp. Comm. Review, Vol. 18, No. 1, pp. 106- 114, Aug. 1988.

[6] 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, July 2012.

[7] 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.

[8] D. Kim, "Content Centric Networking Naming Scheme for Efficient Data Sharing," Journal of Korea Multimedia Society, Vol. 15, No. 9, pp. 1126-1132, 2012.

[9] "Trend and Improvement for Privacy Protection of Future Internet," Journal of Digital Convergence v. 14, n. 6, pp. 405-413, Jun. 2016

[10] D. Kim, "A Comparison Study on Data Caching Policies of CCN," Journal of Digital Convergence v.15, n.1, pp. 327-334, Feb, 2017

[11] R. Merkle, "Protocol for public key cryptosystems," IEEE Sympo. Research in Security and Privacy, Apr.1980.

[12] D. Y. Kim and J. S. Park, "Efficient Contents Verification Scheme for Contents-Centric-Networking," The Journal of Korean Institute of Comm. and Inform. Sciences, Vol. 39, No. 4, pp. 234-241, April, 2014.

[13] 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, Aug. 2015.

[14] D. Kim, "Group-Interest-based Verifiable CCN," Mobile Information Systems, Volume 2016, Article ID 9202151

[15] B. Georg "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis,". Ruhr-Universität Bochum. Retrieved 2013-11-20.

[16] T. Cormen,"Introduction to Algorithm," The MIT Press, pp. 301-328, 1992

김 대 엽(Kim, Dae Youb)

- 1994년 2월 : 고려대학교 수학과(이학사)
- 1997년 2월 : 고려대학교 수학과(이학석사)
- 2000년 2월 : 고려대학교 수학과(이학박사)
- 2000년 2월 ~ 2002년 8월 : 시큐아이 정보보호연구소 차장
- 2002년 9월 ~ 2012년 2월 : 삼정전자 종합기술원 수석연구원
- 2012년 3월 ~ 현재 : 수원대학교 IT 대학 정보통신학부 학부장, 정보보호학과 조교수
- 관심분야 : 악성 코드 분석, 웹 보안, 콘텐츠 보안, 미래 인터넷 보안
- E-Mail : daeyoub69@suwon.ac.kr