Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.975

블록체인 기반 CCN 콘텐츠 인증 기술*

김 대 엽†‡
수원대학교

A Blockchain-Based Content Authentication Scheme for CCN*

DaeYoub Kim†‡
Suwon University

요 약

미래 인터넷 기술 중 하나인 ICN은 콘텐츠 소스에게 집중되는 콘텐츠 요청을 다수의 노드들이 분산 처리함으로써, 콘텐츠 소스의 주변 네트워크에서 발생하는 네트워크 병목 현상을 해결하고, 서비스 시스템이나 네트워크의 운영 상태와 상관없이 지속적으로 콘텐츠를 배포할 수 있다는 장점을 갖고 있다. 특히, CCN은 네트워크 노드에 콘텐츠 임시 저장 기능을 구현하고, 콘텐츠 요청 패킷의 전송 경로 상에 있는 중간 네트워크 노드가 직접 콘텐츠 요청에 응답할 수 있도록 제안되었다. 그러나 이와 같이 분산된 불특정 노드로부터 콘텐츠가 전송될 경우, 사용자가 실제 콘텐츠 제공 노드를 인증할 수 없기 때문에 공격자의 불법적인 서비스 개입 및 악의적인 콘텐츠 변경을 통한 다양한 해킹 공격에 취약할 수 있다. 이러한 문제점을 해결하기 위하여 CCN은 콘텐츠 인증 기능을 제안하고 있다. 본 논문에서는 CCN의 콘텐츠 인증 기술의 문제점을 분석하고 블록체인을 이용하여 이를 개선할 수 있는 방안을 제안한다. 또한, 기존 기술과의 성능 비교 분석을 통하여 개선안의 성능을 평가한다.

ABSTRACT

ICN architecture, one of future Internet technologies, proposes that content request packets toward a content source can be responded by several distributed nodes. So, ICN can solve network congestion which is happened around content sources and provide a seamless content distribution service regardless of the network and system statuses of content sources. Especially, CCN implements content caching functionality in network nodes so that such intermediated network nodes can themselves respond to content requests. However, when receiving content from distributed nodes, users receiving content cannot authenticate the nodes providing the content. So CCN is vulnerable to various attacks such as an impersonation attack, a data pollution attack, and so on. This paper first describes CCN content authentication and its weakness. Then it proposes an improved content authentication scheme based on a blockchain and evaluates the performance of the proposed scheme.

Keywords: ICN, CCN/NDN, Data Authentication, PKI, Blockchain

I. 서 론

콘텐츠 배포/공유 시, 콘텐츠 전송 성능을 향상시키기 위한 방법으로 여러 노드에 이미 분산 저장되어 있는 콘텐츠의 캐시들을 활용하는 다양한 기술들이 개발되었다. P2P 네트워킹 기술과 CDN 서비스가 그 대표적인 예라 할 수 있다. 미래 인터넷 기술 중 하나인 콘텐츠 중심 네트워킹 아키텍처 (Content-

Received(07. 06. 2018), Modified(08. 07. 2018), Accepted(08. 07. 2018)
* 본 연구는 수원대학교 교내 연구과제(No. 2018-0023) 지원으로 수행하였습니다.
† 주저자, daeyoub69@suwon.ac.kr
‡ 교신저자, daeyoub69@suwon.ac.kr(Corresponding Author)

centric Networking Architecture, CCN)는 네트워크 장비(노드)에 전송되는 콘텐츠를 임시 저장할 수 있는 캐싱 기능(In-network Caching)을 구현하고, 캐싱 된 콘텐츠에 대한 요청 메시지를 네트워크 노드가 수신하면, 해당 네트워크 노드가 직접 콘텐츠를 전송한 후, 응답처리를 완료하도록 설계되었다[1][2]. 사용자로부터 콘텐츠 공급자(Publisher)까지 콘텐츠 요청 메시지가 전송되는 네트워크 전송 경로 상에 위치한 네트워크 노드가 사용자의 콘텐츠 요청 메시지에 직접 응답할 수 있기 때문에 사용자에게 콘텐츠를 보다 신속하게 전송할 수 있을 뿐만 아니라, 콘텐츠 공급자에게 집중되는 콘텐츠 요청 메시지들을 네트워크 내에서 분산 처리함으로써 콘텐츠 공급자의 주변 네트워크에서 발생하기 쉬운 네트워크 병목 현상을 방지할 수도 있다. 또한 콘텐츠 캐시를 활용한 네트워킹 기술은 콘텐츠 공급자의 서비스 시스템 및 네트워크 상태에 상관없이 지속적으로 콘텐츠 서비스를 제공할 수 있다는 장점도 갖고 있다.

기존 호스트 기반 일대일 네트워킹 기술의 경우, IP 주소와 같은 호스트 식별자를 활용하여 사용자와 콘텐츠 공급자가 상호 식별 및 인증을 할 수 있다. 그러나 분산된 노드들의 캐시들을 활용한 네트워킹 기술은 불특정 다수의 노드들로부터 콘텐츠가 사용자에게 전송되기 때문에 콘텐츠를 제공한 실제 노드들을 사용자가 식별하기 어렵다. 이와 같은 특징 때문에 콘텐츠 캐시를 활용한 네트워킹 기술을 콘텐츠 서비스에 적용할 경우, 콘텐츠 위/변조 및 다양한 공격에 취약할 수 있다. CCN은 이러한 문제를 해결하기 위하여 사용자가 콘텐츠 및 콘텐츠 공급자를 모두 인증할 수 있도록 공급자의 전자 서명과 머클 해시 트리(Merkle Hash Tree, MHT) 기반의 인증 기술을 제안하고 있다[3][4]. 콘텐츠 공급자의 전자 서명을 검증하기 위해서는 공급자의 서명키를 인증할 수 있는 PKI(Public Key Infrastructure)와 같은 신뢰 체계의 구축 및 운영이 필수적으로 요구된다. 그러나 CCN은 네트워크 계층의 기반 기술이기 때문에, 네트워크를 이용하는 모든 노드/사용자들이 공급자가 될 수 있다. 이 경우, 콘텐츠 인증을 지원하기 위해서는 대규모 인증 시스템 운영이 요구된다. 또한, CCN이 네트워크 계층의 기술임에도 불구하고, 콘텐츠 인증은 네트워크 계층의 노드가 아닌 최종 사용자(End User)에 의해서만 운영된다. 즉, 모든 개인 사용자가 네트워크 패킷의 인증 주체가 될 수 있다. 그러나 이와 같이 모든 개인 사용자를 포함하는 인증 체계를 구축하는 것은 매우 어려운 작업이다.

블록체인(Blockchain) 기술은 탈중앙화를 지향하는 분산 데이터 인증 기술로, 별도의 중앙 인증 시스템의 도움 없이 분산된 서비스 환경 아래에서 서비스 참여자들의 상호 합의를 통하여 데이터를 인증하는 기술이다. 블록체인 기술은 탈중앙화 애플리케이션이나 서비스의 데이터를 인증하는 수단으로 주목받고 있다. 특히, 데이터 인증을 위하여 별도의 신뢰기관에 인증을 위탁할 필요가 없기 때문에 저비용 인증 서비스를 구현할 수 있으며, 시간 및 지역의 차이에 상관없이 서비스를 이용할 수 있다는 장점이 있다. 이와 같은 블록체인 기술은 암호 화폐를 포함하여 향후 다양한 분야에서 활용될 것으로 예상되고 있다[5][6].

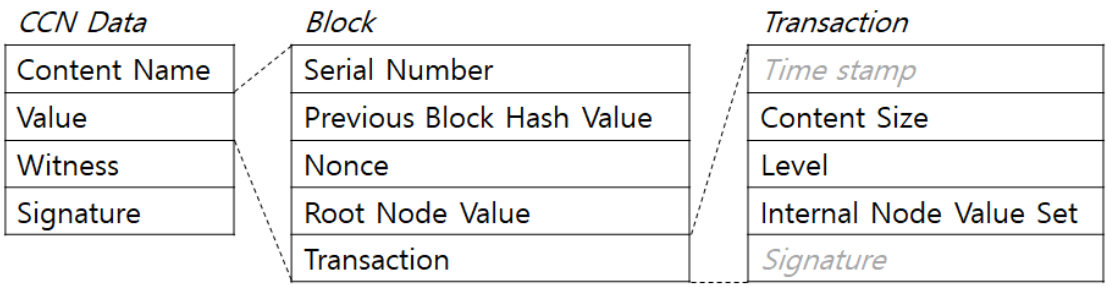
본 논문에서는 CCN 콘텐츠 인증 구현의 문제점을 분석하고, 블록체인 기술을 활용하여 보다 효율적으로 콘텐츠를 인증할 수 있도록 인증 구조 및 CCN 데이터 구조를 제안한다. 또한 제안하는 블록체인 기반 콘텐츠 인증 기술의 성능을 분석한다.

II. CCN 콘텐츠 인증

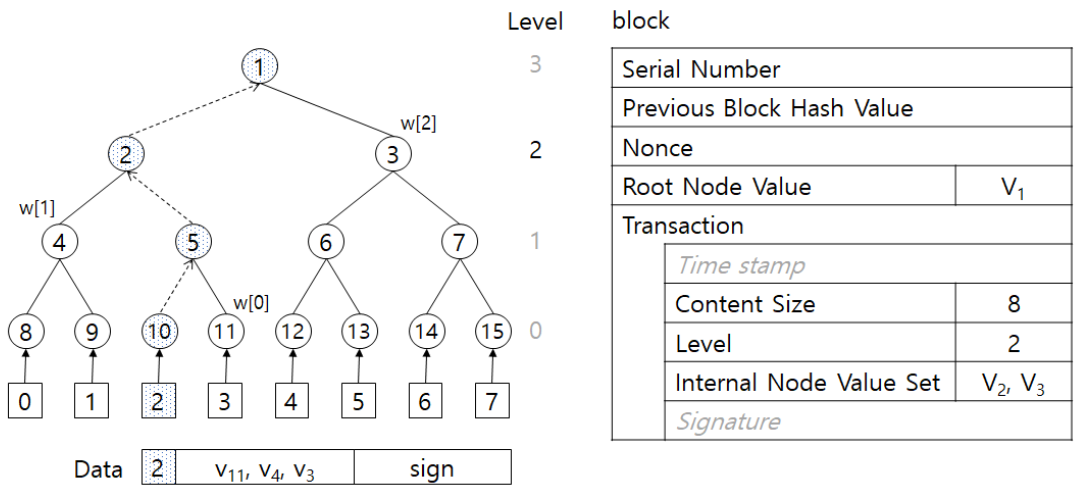
대용량 콘텐츠의 효율적인 전송을 위하여 CCN은 콘텐츠를 일정 크기 이하의 세그먼트 (Segment)들로 단편화하여 처리한다. 이 때, CCN은 콘텐츠의 단편화된 개별 세그먼트를 각각 독립적인 CCN 전송 패킷(Data)으로 간주하고, 콘텐츠 인증 또한 각각의 Data에 대하여 독립적으로 수행한다. 즉, 콘텐츠 공급자는 콘텐츠의 모든 Data에 공급자의 전자서명을 첨부해야 한다. 그러나 단편화된 세그먼트의 수가 많은 대용량 콘텐츠의 경우, 콘텐츠의 모든 Data의 전자 서명을 생성/검증하는 것은 서비스 지연 요인이 될 수 있다. 또한, 안전한 콘텐츠 이용을 보장하기 위해서는 수신된 개별 Data의 무결성 검증 및 공급자 인증뿐만 아니라, 해당 Data가 사용자가 요청한 콘텐츠의 정상적인 세그먼트가 맞는지 여부도 검증해야 한다. 그러나 개별 Data에 첨부된 전자 서명을 검증하는 것만으로는 이와 같은 세그먼트 적합성 여부를 판단할 수 없다.

이와 같은 문제를 해결하기 위하여 CCN은 Fig.1.의 (B)처럼 MHT 기반의 콘텐츠 인증 기술을 제안했다.

Fig.1.의 (B)는 콘텐츠가 8개의 세그먼트로 단편화된 경우를 가정한다. 단편화된 8개의 세그먼트를



(A) CCN Data, Block, and Transaction Structure



(B) MHT and Block Example

Fig. 1. The structure of Block and Transaction for CCN Content Authentication

순서에 따라 $S[0],...,S[7]$이라 하자. 콘텐츠 공급자는 세그먼트 수($N=2^n$)만큼의 리프 노드(Leaf Node)를 갖는 이진트리를 생성한 후, 각각의 세그먼트를 순서에 따라 이진트리의 리프 노드에 할당한다. 이때, 세그먼트의 해시 값은 할당된 리프 노드의 노드 값으로 사용된다. 즉, k번째 노드(n_k)의 노드 값을 v_k라고 할 때, i번째 세그먼트에 대응하는 리프 노드의 노드 값은 다음과 같다:

$$v_{N+i} = H(S[i]) \quad (1)$$

이진트리의 리프 노드를 제외한 나머지 노드의 노드 값은 해당 노드의 두 자식 노드(Child Node)들의 노드 값들에 대한 해시 값으로 계산된다. 즉, n_i의 두 자식 노드를 각각 n_{2i}와 n_{2i+1}라고 할 때, n_i의 노드 값은 다음과 같이 계산된다.

$$v_i = H(v_{2i} \| v_{2i+1}) \quad (2)$$

이와 같은 방법으로 이진트리의 노드 값은 하위 노드부터 루트 노드(Root Node)까지 차례로 계산된다.

루트 노드의 노드 값(v_1)이 계산되면 콘텐츠 공급자는 자신의 전자 서명키를 이용하여 v_1에 대한 전자서명 값을 계산한 후, 콘텐츠의 모든 Data에 계산된 전자 서명 값을 첨부한다.

i번째 세그먼트 전송을 위한 Data를 수신한 사용자가 Data에 첨부된 v_1에 대한 전자서명 값을 검증하기 위해서는, v_1을 계산할 수 있어야 한다. 이를 위하여 공급자는 v_1 값 계산에 필요한 추가 인증정보(Witness)를 Data에 함께 첨부한다. 이러한 인증정보는 i번째 세그먼트에 할당된 리프 노드(n_{N+i})부터 루트 노드(n_1)까지의 노드 경로(Path) 위에

있는 노드들의 형제 노드(Sibling Node)의 노드 값들로 구성된다. 즉, Fig. 1.의 (B)에서 $S[2]$ 인증 시, v_1 값을 계산하기 위해서는 v_{11}, v_4, v_3가 추가적으로 필요하므로, 이 값들을 인증정보로 Data에 첨부한다. 그러므로 $S[i]$를 전송하기 위한 Data는 다음과 같이 구성된다.

$$Data[i] = \{S[i], \{W_i[k]\}, sg(v_1)\} \quad (3)$$

여기서, $\{W_i[k]\}$는 $S[i]$의 인증정보를 의미하고, $sg(v_1)$은 이진트리의 v_1 값에 대한 콘텐츠 공급자의 전자 서명 값을 의미한다.

Data를 수신한 사용자는 첨부된 인증정보와 세그먼트를 이용하여 v_1을 계산하고, 콘텐츠 공급자의 공개키를 이용하여 전자서명을 검증한다.

이와 같은 Data 인증을 통하여 사용자는 수신된 Data가 콘텐츠 공급자에 의해서 배포된 콘텐츠의 세그먼트이고, 중간에 위/변조 되지 않았음을 검증할 수 있다. 그러나 CCN 콘텐츠 인증 기술은 다음과 같은 몇 가지 문제점을 갖고 있다.

(1) 콘텐츠를 구성하는 세그먼트의 수에 비례하여 해시 값 계산 횟수가 증가한다. 그러므로 대용량 콘텐츠의 경우 콘텐츠 인증에 소요되는 시간으로 인하여 서비스 지연이 발생할 수 있다. Fig. 2.는 콘텐츠의 용량에 따른 처리 시간 분석 결과이다. MHT를 콘텐츠 인증에 적용할 때, 반복적인 해시 값 계산으로 인한 서비스 지연이 발생한다[7][8].

(2) 콘텐츠 공급자의 전자서명을 검증하기 위해서는 공급자의 서명키를 검증할 수 있는 PKI와 같은 신뢰 체계의 구축 및 운영이 요구된다. 그러나 CCN은 네트워크 계층의 기반기술이므로, 일반 사용자를 포함하여 네트워크를 이용하는 모든 사용자가 콘텐츠 공급자가 될 수 있다. 이 경우, 전 세계적으로 공용되거나 적어도 상호 인증되는 대규모의 서명키 인증 체계 구축이 필요하다.

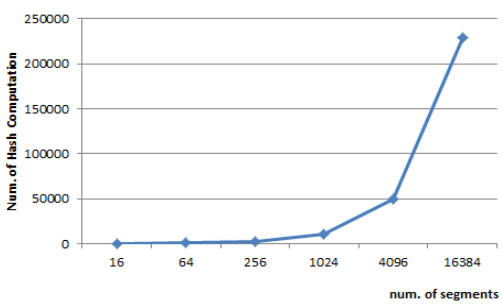


Fig. 2. CCN Authentication Computation Overheads

III. 블록체인

기존의 중앙 집중화된 데이터 인증 체계에서는 애플리케이션이나 서비스에서 생성되고, 교환되는 데이터를 인증하기 위해서 별도의 신뢰/인증 시스템을 운영 및 관리해야 된다. 전자서명 기반의 인증 서비스를 구축할 때 필요한 PKI의 CA(Certificate Authority) 운영이 대표적인 예라 할 수 있다. 그러나 이와 같은 신뢰 기관을 운영하기 위해서는 별도의 운영비용이 필요하고, 전 세계적으로 상호 신뢰할 수 있는 인증 체계를 구축하기 위해서는 추가적인 비용뿐만 아니라 상호 신뢰 구축을 위한 별도의 노력이 요구된다. 특히, 중앙 집중화된 인증 서비스를 이용하여 콘텐츠 서비스를 구축할 때, 인증 서비스 시스템이 주요 공격 목표가 되는 경우, 애플리케이션이나 서비스가 공격을 받지 않았더라도 인증 서비스 시스템에 대한 공격의 영향을 받게 된다.

블록체인 기술은 탈중앙화 애플리케이션이나 서비스의 데이터를 인증하는 수단으로 주목 받고 있다. 특히, 데이터 인증 위하여 별도의 신뢰 기관에 인증을 위탁할 필요가 없기 때문에 저비용 인증 서비스를 구현할 수 있으며, 시간 및 지역의 차이에 상관없이 서비스를 이용할 수 있다는 장점이 있다.

블록체인 기술은 유효한 블록체인, 즉 가장 긴 블록체인에 연결되어 있는 블록에 포함된 데이터(Transaction)는 참여자(채굴자, Miner)들의 합의에 의해 인증된 것으로 간주한다. 채굴자는 데이터 풀(Transaction Pool)에 저장되어 있는 사용자들의 데이터를 검증한 후, 해당 데이터를 포함하는 새로운 블록을 생성한다. 이렇게 생성한 블록을 유효한 블록체인에 연결되어 있는 가장 최신 블록에 연결시킨다. 이를 위하여, 유효한 블록체인에 연결되어 있는 가장 최신 블록의 블록 헤더 해시 값을 계산하고, 계산된 해시 값을 새로 생성한 블록에 기록한 후, 다른 채굴자들에게 생성한 블록을 전파한다. 유효한 블록체인에 새롭게 연결된 블록을 수신한 채굴자들은 해당 블록 및 블록에 포함된 데이터를 검증한 후, 해당 블록 및 데이터가 유효하면, 해당 블록을 유효한 블록체인에 연결된 최신 블록으로 간주하고 향후 다른 데이터의 인증이 필요할 때, 블록을 생성하여 이

최신 블록에 연결한다. 이와 같은 과정을 참여자 합의 과정(Consensus)이라 부르며, 합의 과정을 통하여 유효한 블록체인에 연결된 블록은 채굴자들에 의하여 인증된 것으로 간주된다. 그러므로 가장 긴 길이의 블록체인에 연결된 블록은 많은 채굴자들의 합의에 의하여 인증된 것으로 간주되며, 이와 같은 유효한 블록체인에 포함된 블록은 이전 블록의 블록 헤더의 해시 값을 포함하므로 유효한 블록체인에 포함된 블록의 내용을 변경하기 위해서는 해당 블록 이후에 블록체인에 연결된 블록들을 모두 수정해야만 된다. 그러므로 인증 완료된 블록의 내용을 위/변조하는 것은 매우 어렵다.

IV. 블록체인기반 CCN 인증

효율적인 CCN Data 인증을 구현하기 위하여 본 절에서는 콘텐츠 이름 기반의 인증 체계를 구축하고, 블록체인을 기반으로 콘텐츠 공급자와 세그먼트들을 인증하는 새로운 방안을 다음과 같이 제안한다.

첫째, 본 논문에서는 기존의 CCN 콘텐츠 인증 기법과 함께 블록체인을 이용한 인증 기법을 추가로 사용할 수 있도록 제안한다. 즉, 콘텐츠 인증 결과를 인증 데이터(Transaction)으로 구성하고, 블록체인을 이용하여 인증 데이터를 인증함으로써, 사용자가 선택적으로 콘텐츠를 직접 인증하지 않고 블록체인을 활용하여 인증 데이터에 대응되는 콘텐츠를 인증할 수 있도록 제안한다.

둘째, 일반적인 블록체인의 경우, 최신 블록을 생성한 채굴자는 유효한 블록체인에 해당 블록을 연결한 후, 다른 채굴자들에게 최신 블록을 전파하여, 많은 채굴자들이 새로 생성된 블록을 유효한 블록으로 인정하도록 유도한다. 이러한 절차는 모든 채굴자가 블록체인의 모든 블록을 공유하도록 유도함을 의미한다. 그러나 블록체인 기술을 CCN 콘텐츠 인증에 적용할 경우, 채굴자들이 전 세계 사용자들이 생성한 모든 콘텐츠의 인증 정보를 포함하는 블록들을 공유하게 하는 것은 매우 비효율적이며, 네트워크를 이용하여 배포되는 콘텐츠의 수를 고려할 때 현실적으로 구현하기 어렵다. 이러한 문제를 해결하기 위하여, 본 논문에서는 계층화된 CCN 네트워크 도메인에 대표 채굴자 시스템을 설치/운영하는 방안을 제안한다.

4.1 시스템 구성 요소

CCN은 콘텐츠를 생성하고 사용하는 사용자 노드와 콘텐츠 전송을 담당하는 네트워크 노드로 구성된다. 네트워크 노드는 전송되는 Data의 인증 검증 과정에 관여하지 않기 때문에, 본 논문의 설명에서는 제외한다. 사용자 노드의 경우, 콘텐츠를 생성/배포하는 콘텐츠 공급자와 콘텐츠를 요청하는 사용자는 Data 인증과 관련하여 각각 서로 다른 역할을 수행하기 때문에 구분하여 설명한다. 또한, 본 논문에서는 블록체인을 이용하여 콘텐츠의 인증을 대행하는 콘텐츠 인증 노드 (Content Authentication Node, CAN)를 추가한다. 각각의 시스템 구성 요소들의 역할은 다음과 같다.

(1) 콘텐츠 인증 노드(CAN): 콘텐츠 공급자는 콘텐츠를 배포하기 위한 CCN Data를 생성한 후, CAN에게 생성한 Data (실제로는 Data Set)의 인증을 요청한다. CAN은 Data를 기존 CCN 인증 절차에 따라 인증한 후, 그 결과를 블록체인을 이용하여 일반 사용자가 콘텐츠 인증 결과를 확인할 수 있도록 제공한다. 즉, CAN은 블록체인의 채굴자 역할을 수행한다. 이를 위하여 다음과 같은 네트워크 및 시스템 환경을 가정 한다:

- 가정 1: CCN의 계층화된 콘텐츠 이름 구조는 네트워크의 토폴로지 계층 구조를 반영한다. 즉, 동일한 네트워크 도메인에 포함되어 있는 서브 네트워크들은 상위 네트워크 도메인의 네트워크 이름을 네트워크 이름 접두어(Prefix)로 사용한다. 즉, 상위 네트워크 도메인의 네트워크 식별자를 '/kr/ac/sw'라고 할 때, 해당 네트워크 도메인의 서브 네트워크 도메인들의 네트워크 식별자는 '/kr/ac/sw/it' 또는 '/kr/ac/sw/edu'와 같이 상위 도메인의 이름을 접두어로 사용한다.
- 가정 2: 계층화된 네트워크 도메인에는 적어도 하나 이상의 CAN이 운영된다. 즉, 사용자 기기는 자신이 포함된 계층화된 네트워크 도메인들 중 적어도 하나의 계층에서 운영되는 CAN을 이용할 수 있다. 이 때, CAN의 CCN 기본 이름은 '/miner'라 하자. 즉, 네트워크 도메인 '/kr/ac/sw' 아래에서 운영되는 CAN의 기본 식별자는 '/kr/ac/sw/miner'이다. 특히, [9]에서 제시한 custodian-based routing protocol을 CCN에 적용한다면, custodian node가 CAN의 역할을 수행할 수도 있다.

(2) 콘텐츠 공급자: 콘텐츠 공급자는 콘텐츠의 CCN Data를 생성한 후, CCN을 이용하여 Data를 배포한다. 또한, 일반 사용자가 콘텐츠 인증을 보다 효율적으로 수행할 수 있도록, 생성된 콘텐츠가 블록체인을 통하여 인증되도록 CAN에게 요청한다.

(3) 콘텐츠 사용자: 콘텐츠 사용자는 CCN을 이용하여 콘텐츠를 요청하고, 수신된 콘텐츠의 세그먼트들을 인증한 후, 콘텐츠를 이용한다. 전송된 콘텐츠를 효율적으로 인증하기 위하여 블록체인을 활용하여 해당 콘텐츠를 인증할 수도 있다.

4.2 블록체인을 위한 CCN Data 구성

CCN 오픈 소스 코드의 수정을 최소화하기 위하여 본 논문은 CAN에 의해 생성/배포되는 블록을 CCN 데이터로 간주하여 처리한다. CCN은 데이터 요청과 전송을 위해 Interest 패킷과 Data 패킷의 구조와 전송/처리 방법을 규정하고 있다[2]. 일반 콘텐츠의 요청 및 응답을 위한 Interest/Data의 구성은 기존 CCN의 Interest와 Data의 구조와 동일하기 때문에 본 절에서는 CAN이 생성한 블록을 위한 Data 구조만을 추가로 정의한다.

또한, CCN을 기반으로 블록체인 시스템을 할 때, 유효한 블록체인에 연결된 블록을 검색/요청/수신하기 위해서는 블록의 CCN 콘텐츠 이름이 필요하다. 본 절에서는 사용자가 특정 블록의 이름을 확인할 수 있도록 블록 데이터의 이름을 지정해 주는 두 종류의 블록 이름 데이터를 정의한다.

4.2.1 CCN 블록 데이터 (Block-Data)

본 절에서는 콘텐츠 인증 결과를 전송하기 위하여 CAN에 의해서 생성되는 Block-Data의 구조를 제안한다. Fig.1.의 (A)는 Block-Data의 구조를 나타낸다. Block-Data는 기존 CCN Data 구조와 동일하며, Data의 Value에 블록을 저장하도록 제안한다.

(1) Content Name: Block-Data의 콘텐츠 이름은 CCN 콘텐츠 이름 규약을 기본적으로 준수한다. 단, 효과적인 구현을 위하여 기존 CCN 이름의 구조를 일부 수정한다. 즉, 기존 CCN 콘텐츠 이름 구조(/name_ prefix/file_name/seg_no/ver)에 따르면 세그먼트 버전 정보(ver)가 세그먼트 번호(seg_no) 이후에 기록되도록 구성되어 있다. 그러나 사용자가 세그먼트 단위로 콘텐츠를 관리하는 것이 아니라 콘텐츠 자체를 하나의 오브젝트로 관리하기 때문에, 버전 정보는 세그먼트 단위가 아니라 콘텐츠 단위로 관리하는 것이 보다 합리적이다. 그러므로 CCN 콘텐츠 이름 구조에서 ver 필드와 seg_no 필드의 순서를 서로 바꾸도록 한다. 즉, '/name_prefix/file_name/ver/seg_no'로 수정한다. 수정된 CCN 콘텐츠 이름 구조에 따라서 Block-Data에 사용되는 콘텐츠 이름 구조는 다음과 같다: '/[NP]/miner/[H]/ver/seg_no'. 여기서 [NP]는 CAN이 속한 네트워크의 식별자를 의미하고, [H]는 블록 데이터를 통하여 인증되는 콘텐츠의 이름에 대한 해시 값을 의미한다. 여기서 해시 값 계산에 사용되는 콘텐츠 이름은 세그먼트 번호를 제외한 이름을 사용한다.

(2) Serial Number: 블록체인에 연결된 블록의 순번을 의미한다. 최초 생성 블록(Genesis Block)의 일련번호는 0이며, 이 후 블록체인에 연결된 블록은 연결 순서에 따라 1씩 증가된 값을 갖는다.

(3) Previous Block Hash Value: 유효한 블록체인에 블록을 연결할 때, 블록체인에서 해당 블록이 연결된 블록의 블록 헤더에 대한 해시 값을 의미한다.

(4) Nonce: 블록 생성을 위해 CAN이 해결한 Puzzle의 솔루션 값을 의미한다.

(5) Root Node Value: 블록에 포함되어 있는 Transaction 들로 구성된 MHT의 루트 노드의 노드 값을 의미한다.

(6) Transaction: 콘텐츠 공급자의 요청에 따라 CAN은 해당 콘텐츠를 인증한 후, 인증 결과를 Transaction에 저장한다. 콘텐츠 인증 정보는 다음과 같은 요소들로 구성된다.

- Time stamp: Transaction 생성 시각 정보를 의미한다. 단, CCN Name의 Version 정보와 중복될 경우, 선택적으로 적용할 수 있다.
- Content Size: 인증하려는 콘텐츠의 전체 세그먼트 수를 의미한다.
- Level: 콘텐츠를 CCN의 기본 인증 기술을 이용하여 인증하기 위해 구성한 MHT의 계층 값 중 하나의 계층 값을 나타낸다. 특히, 인증 계층 값은 INVS(Internal Node Value Set)에 포함된 노드들의 계층 값을 의미한다.
- Internal Node Value Set: 콘텐츠의 MHT를 구성하는 노드 중에서 Level에 해당하는 노

드들의 노드 값들을 의미한다.

- Signature: MHT의 루트 노드 값에 대한 CAN의 전자 서명 값을 의미한다. 단, CCN Data의 Signature와 기능이 중복되므로 선택적으로 적용할 수 있다.

4.2.2 CCN 최신 블록 이름 데이터(LBN-Data)

블록체인을 운영하기 위해서는 블록체인에 연결된 최신 블록을 검색/요청할 수 있는 기능이 필요하다. 최신 블록 이름 데이터(Latest Block Name Data, LBN-Data)는 블록체인에 연결된 가장 최신의 블록 데이터에 대한 콘텐츠 이름 정보를 제공하는 Data이다. 이와 같은 CCN Content Name Resolution Service를 제공하기 위하여 해당 데이터의 콘텐츠 이름 및 데이터(Name Resolution Data)는 다음과 같다:

- Content Name: LBN-Data의 CCN 콘텐츠 이름은 '/[NP]/ver/seg_no'와 같이 구성된다. 여기서 [NP]은 블록체인의 고유 식별 이름을 의미한다. ver은 블록체인의 최신 블록의 일련번호(i)를 의미한다.
- Time stamp: LBN-Data 생성 시각 정보를 의미한다. 두 CAN이 생성한 동일 버전의 블록이 중복된 이름으로 존재할 경우, 시각 정보를 바탕으로 먼저 생성된 LBN-Data를 유효한 것으로 간주한다.
- Name Resolution: 블록체인에 연결된 i번째 블록의 블록 데이터 이름을 의미한다.

4.2.3 CCN 이전 블록 이름 데이터 (PBN-Data)

블록체인에 속한 블록을 인증하기 위해서는 블록체인의 최신 블록부터 역순으로 연결된 블록을 추적할 수 있어야 한다. PBN-Data (Previous Block Name Data)는 블록체인에서 특정 블록이 연결된 바로 이전 블록의 이름을 제공하는 Data이다. 이와 같은 Name Resolution Service를 제공하기 위하여 PBN-Data의 콘텐츠 이름 및 데이터는 다음과 같이 구성된다.

- Content Name: PBN-Data의 CCN 콘텐츠 이름은 '/[NP]/miner/[H]/ver/seg_no'와 같이 구성된다. 여기서 [NP]은 블록체인에 새롭게 추가되는 블록의 Name Prefix를 의미하고, [H]는 블록체인에서 해당 블록이 연결되는 이전 블록의 블록 헤더에 대한 해시 값을 의미한다.
- Name Resolution Data: 해당 블록이 연결된 이전 블록 데이터의 Content Name을 의미한다.

4.3 블록체인 기반 CCN 인증 절차

4.3.1 Block-Data 생성

Fig.3.은 콘텐츠에 대한 Block-Data 생성 절차를 나타낸다. 콘텐츠 공급자는 콘텐츠의 CCN Data를 생성한 후, 다음과 같은 절차에 따라 CAN에게 콘텐츠의 Block-Data를 요청한다.

(1) 콘텐츠 공급자는 콘텐츠의 CCN Data를 생성한다.

(2) 사용자가 콘텐츠 인증을 보다 효율적으로 수행할 수 있도록, 콘텐츠 공급자는 자신이 속한 도메인의 CAN에게 생성한 CCN Data 들을 전송하고, 블록체인을 활용한 콘텐츠 인증을 요청한다. 일반적인 블록체인 시스템을 적용할 경우, CAN이 접근할 수 있는 Transaction Pool에 Data를 저장시켜 두는 것으로 충분하다.

(3) CAN은 기존 일반 사용자들처럼 수신된 Data들을 CCN 콘텐츠 인증 방법을 사용하여 검증한다. 이 때, 콘텐츠 공급자는 CAN이 속한 도메인에 소속된 사용자이므로, 일반성을 잃지 않고 CAN이 콘텐츠 공급자의 서명키를 획득/검증할 수 있다고 가정할 수 있다. 즉, 서명키 인증을 위한 신뢰/인증

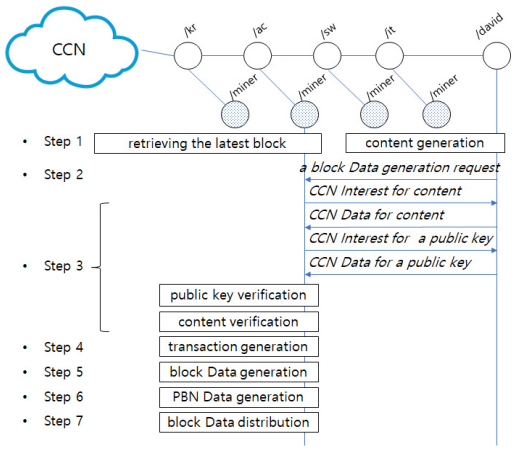


Fig. 3. Block-Data Generation

체계를 네트워크 도메인 단위로 독립적으로 운영하면 충분하다.

(4) CAN은 인증된 콘텐츠의 인증 결과를 바탕으로 인증 데이터를 생성한다. 특히, 블록 데이터의 크기와 인증 효율성을 고려하여 Level 값을 결정한 후, MHT에서 Level에 대응되는 노드들의 노드 값들을 계산하여 INVS를 구성한다. 또한, 콘텐츠의 MHT의 루트 노드 값에 대한 전자 서명 값을 계산한다.

(5) CAN은 콘텐츠 인증 결과를 공지하기 위한 Block-Data를 생성한다.

(5-1) 블록 생성을 위해 필요한 Puzzle의 솔루션 값(Nonce)을 계산한다.

(5-2) 콘텐츠의 콘텐츠 이름에 대한 해시 값을 계산하여 Block-Data의 Content Name을 구성한다.

(5-3) LBN-Data를 이용하여 블록체인의 최신 블록을 획득하고, 최신 블록의 블록 헤더에 대한 해시 값을 계산 한다. 최신 블록의 정보를 이용하여 블록 데이터의 Serial Number와 Previous Block Hash Value를 구성한다.

(6) CAN은 콘텐츠 이름과 블록체인의 최신 블록의 이름을 이용하여 PBN-Data을 생성한다.

(7) CAN은 생성한 Block-Data를 다른 CAN들에게 전파하여 향후 해당 Block-Data가 다른 CAN들에 의해서 유효한 블록체인의 최신 블록으로 활용될 수 있게 한다. 이 때, CAN은 계층화된 네트워크/서비스 도메인의 구성원이므로, 일반성을 잃지 않고 CAN들 사이에는 상호 신뢰 관계가 형성되어 있다고 가정할 수 있다. 즉, Block-Data를 생성한 CAN의 공개키를 다른 CAN들이 획득/인증할 수 있다.

4.3.2 콘텐츠 인증

사용자가 요청한 콘텐츠가 수신되면, 사용자는 다음 두 가지 콘텐츠 인증 방법 중 하나를 선택하여 수신된 콘텐츠를 인증한다.

4.3.2.1 CCN 콘텐츠 인증

사용자는 CCN에서 제공하는 기본적인 콘텐츠 인증을 수행한다. 이를 위하여 사용자는 콘텐츠 공급자의 공개키를 획득하고 이를 검증한다. MHT의 루트 노드 값을 계산한 후, 콘텐츠 공급자의 저자 서명 값을 검증한다. CAN의 경우, 이와 같은 방법으로 사용자의 콘텐츠를 인증한다.

4.3.2.2 블록체인을 이용한 콘텐츠 인증

Fig.4.는 블록체인을 활용한 콘텐츠 인증 절차를 설명한다. 블록체인 기술을 이용한 콘텐츠 인증을 위해서 콘텐츠를 수신한 사용자는 다음과 같은 절차를 수행한다.

(1) 사용자는 수신한 콘텐츠의 이름을 기반으로 Block-Data를 요청한다. CAN은 콘텐츠 공급자의 네트워크 도메인 계층에 위치하고 있기 때문에, 사용자는 콘텐츠의 계층화된 이름을 기반으로 CAN의 이름을 추정하여 요청한다. 예를 들어, 콘텐츠의 이름을 '/kr/ac/sw/it/david/a.txt'라고 하고, 콘텐츠의 이름에 대한 해시 값을 '0x9486'이라면, 사용자는 다음과 같은 콘텐츠 이름들을 이용하여 CCN을 통해 Block-Data를 요청하는 Interest를 전송한다.

- /kr/miner/0x9486/v.1/s.1
- /kr/ac/miner/0x9486/v.1/s.1
- /kr/ac/sw/miner/0x9486/v.1/s.1
- /kr/ac/sw/it/miner/0x9486/v.1/s.1

이와 같이 사용자가 전송한 4개의 Interest 중 하나는 반드시 응답되고, 사용자는 Block-Data을 수신하게 된다. 이 때, 해당 블록의 최신 버전이 필요할 경우, 버전 정보를 수정하여 재요청할 수도 있다.

(2) 사용자는 수신된 Block-Data를 인증한다.

(2-1) Block-Data의 INVS 값을 이용하여 콘텐츠의 MHT의 루트 노드 값을 계산한다.

(2-2) 블록 인증은 다음과 같은 두 가지 방법 중 하나를 택하여 수행 한다:

(2-2-1) 블록이 유효한 블록체인에 포함되어 있는지 확인한다. 블록 인증은 일반적인 블록체인 기법의 인증 과정과 동일하다. 이 때, LBN-Data와 PBN-Data를 활용하여 블록체인의 블록들을 CCN을 통하여 전송 받을 수 있다.

(2-2-2) MHT의 루트 노드 값에 대한 CAN의 전자 서명을 검증한다. CAN은 네트워크 도메인 계층에서 운영되는 신뢰 기관으로 가정하기 때문에, CAN의 서명 검증을 위한 공개키는 획득/검증된다고 가정한다.

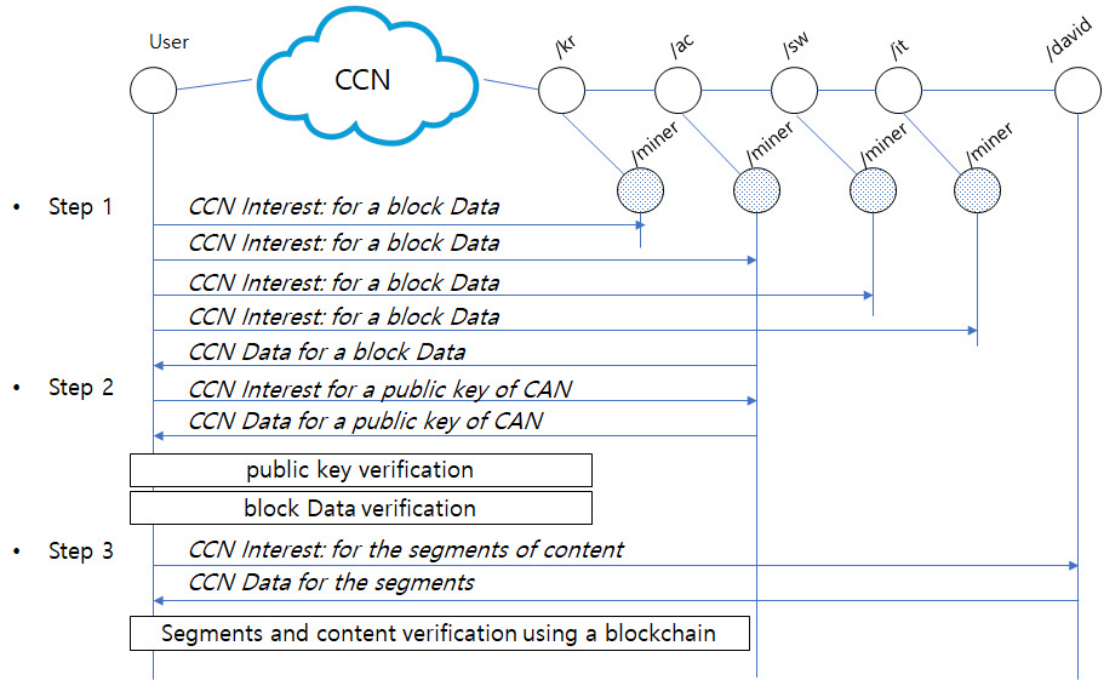


Fig. 4. CCN Content Authentication using a blockchain

(3) 수신된 세그먼트와 인증 정보를 이용하여 MHT의 노드 값들을 계산한다. 이 때, MHT의 인증 경로 중에서 블록 데이터의 Level에 대응되는 노드의 노드 값까지만 계산하면 충분하다. 계산된 노드의 값과 INVS에 저장되어 있는 값을 비교하여, 두 값이 동일한 경우 해당 Data의 세그먼트가 인증된 것으로 간주한다.

V. 성능 분석

CCN의 MHT 기반 CCN 콘텐츠 인증 기술과 블록체인을 이용한 콘텐츠 인증의 성능을 비교 분석하기 위하여 다음과 같은 시험 환경을 가정한다.

(1) 사용자는 인증기관(CA)으로부터 공개키 인증서를 발급 받으며, 인증기관은 최상위 인증기관(Root CA)으로부터 인증서를 발급 받는다. 블록체인 적용 시, 각각의 CAN은 일종의 인증기관으로 간주하여 최상위 인증기관으로부터 공개키 인증서를 발급 받는다. 또한 일반적인 공개키 인증서의 크기는 3K 바이트 이하이므로, 한 개의 세그먼트로 구성이 가능 하다.

(2) 블록체인의 적용 가능성 및 효율성에 대한 직접적인 분석은 본 논문의 연구 범위를 넘어가는 것으로, 본 논문에서는 블록체인의 블록의 전파/공유는 분석하지 않는다. 즉, 사용자는 콘텐츠 인증 시, 유효한 블록체인에 속한 블록을 확보하였다고 가정한다.

Fig.5.와 Fig.6.은 콘텐츠 인증에 필요한 해시 값 계산 횟수에 대한 분석 결과이다. Fig.5.는 콘텐츠의 세그먼트의 개수가 $\{2^n | n = 12, 14, 16, 18\}$인 경우를 고려할 때, 블록의 인증 Level에 따른 해시 값 계산 횟수를 나타낸다. 실제로 1G 바이트의 콘텐츠를 CCN을 이용하여 배포하는 경우 4K 바이트의

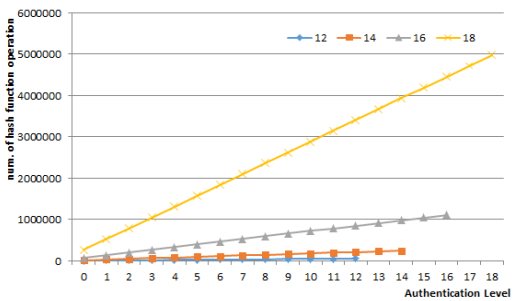


Fig. 5. Computation Overheads for CCN Authentication

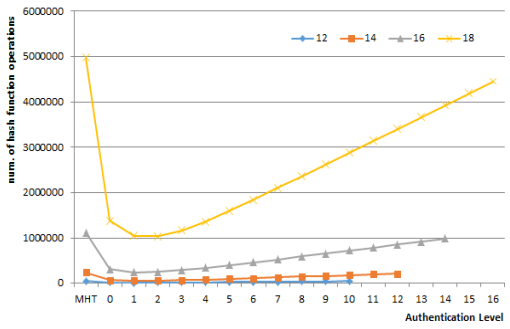


Fig. 6. Computation Overhead for a blockchain-based CCN Authentication

세그먼트 262,144개가 필요하다. 또한, 이를 인증하기 이해서는 2^{18}개의 리프 노드로 구성된 MHT를 구성하고 처리해야 한다. 이 경우, MHT를 이용하여 콘텐츠를 인증할 경우, SHA-512 해시 값 계산에만 500초 이상의 계산 시간이 소요된다. 이는 실제 서비스에 적용하기 어려운 성능이라 할 수 있다.

그러나 블록체인을 이용하여 CCN 콘텐츠를 인증할 경우, CCN의 세그먼트의 크기가 4K 바이트 이하이므로, 블록에는 4개의 512 바이트 해시 값이 포함될 수 있다. 그러므로 블록의 Level에 따라서 블록은 여러 개의 CCN 세그먼트로 구성될 수 있다. 예를 들어 2^n개의 세그먼트로 구성된 콘텐츠의 인증을 위하여 Level의 값이 0인 블록을 구성할 경우, 2^n개의 해시 값이 INVS에 저장된다. 이 경우, 블록은 2^{n-2}개의 세그먼트로 구성된다. 비슷한 논리 전개에 의하여 Level이 1인 경우에는 블록을 구성하기 위하여 2^{n-3}개의 세그먼트가 필요하다. 콘텐츠를 인증하기 위해서는 대응하는 블록을 함께 인증해야 한다. 이 때, 전체 해시 계산 회수는 다음과 같다:

$$((n-k-1)+(k\times 2^{k+2}))\times 2^{n-2-k} \quad (4)$$

여기서 k는 Level을 의미하며, 콘텐츠의 세그먼트의 수는 2^n개라 가정한다.

Fig.6.은 콘텐츠의 세그먼트 수가 각각 $\{2^n | n=12,14,16,18\}$인 경우, 인증 Level에 따라 블록을 구성할 경우, 해시 값 계산 회수를 나타낸다. x축의 MHT는 CCN의 기본 인증 기능을 구현한 경우 해시 값 계산 회수를 나타내며, $\{0,1,\cdots,16\}$은 블록체인을 적용할 경우 인증 Level을 의미한다. 특히, Fig.6.에서 알 수 있듯이, 블록체인을 적용할 경우, 콘텐츠의 크기와 인증 Level에 따라 최소 10%에서 최대 80% 까지 성능 개선 효과가 다름을 알 수 있다. 이와 같은 결과를 바탕으로, 블록 전송량과 계산의 효율성을 고려할 때, Level을 2로 설정하는 것이 가장 효율적임을 알 수 있다.

VI. 결 론

본 논문에서는 블록체인을 활용하여 CCN 콘텐츠 인증의 효율성을 개선하는 방안을 제안하였다. 제안하는 인증 기법은 다음과 같은 개선 효과가 있다.

첫째, 사용자는 기존의 전자 서명 기반의 콘텐츠 인증과 블록체인 기반의 콘텐츠 인증 중에서 선택하여 사용할 수 있다. 사용자가 콘텐츠 공급자의 전자 서명을 검증할 수 없을 때, 사용자는 블록체인의 블록을 확인함으로써 콘텐츠를 인증하도록 제안한다. 이를 위하여, 본 논문은 네트워크 도메인 단위의 독립된 신뢰 체계 구축을 제안하며, 이와 같은 독립된 신뢰 체계는 기존의 custodian-based CCN routing과 같이 CCN 라우팅을 위한 네트워크 도메인의 대표 관리자를 활용하여 구축할 수 있다. 특히, 이와 같은 대표 관리자는 일반 사용자에 비해 그 수가 적으므로, 대표 관리자의 서명키 인증을 위한 신뢰 체계는 소규모로 운영이 가능하다. 그러므로 CCN 사용자를 모두 포함하는 대규모 신뢰 체계 구축 없이도 CCN을 안전하게 이용할 수 있다.

둘째, 블록체인을 이용하여 콘텐츠를 인증할 수 있도록 블록의 Data 구조와 생성 방법을 제안하였다. 본 논문은 기존 CCN의 Data 구조와 전송 방식을 변경하지 않고 적용할 수 있으며, 제안된 인증 방법은 사용자의 애플리케이션 계층의 수정만을 요구한다.

셋째, 블록체인을 활용한 콘텐츠 인증 시, 인증 데이터(Transaction)를 활용하여 MHT의 인증 계층을 설정하게 하도록 제안하였다. 그러므로 MHT의 루트 노드의 노드 값을 계산하기 위해 반복적으로 수행되던 해시 값 계산 횟수를 대폭 줄임으로써 서비스 지연을 개선하였다.

References

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlmanet, "A Survey of Information-Centric Networking," IEEE Communications Maga-

zine, vol. 50, no. 7, pp. 26-36, Jul. 2012
〔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
〔3〕 R. Merkle, "Protocol for public key cryptosystems," IEEE Sympo. Research in Security and Privacy, Apr. 1980
〔4〕 B. Georg, "Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis,". Ruhr-Universität Bochum. Retrieved 20 Nov. 2013
〔5〕 D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," Draft NISTIR 8202, NIST, Feb. 2018
〔6〕 S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cahs System," https://bitcoin.org/bitcoin.pdf, Retrieved 12 Nov. 2011
〔7〕 DaeYoub Kim, "Improvement of the Data Authentication of CCN," Journal of Digital Convergence, 15(8), pp. 341-349, Aug. 2017
〔8〕 DaeYoub Kim, "Network Overhead Improvement for MHT-based Content Authentication Scheme," Journal of Digital Convergence, 16(1), pp. 271-279, Jen. 2018
〔9〕 V. Jacobson, and et. al, "Custodian-based information sharing," IEEE Communications Magazine, vol. 50, no. 7, pp. 38-43, Jul. 2012

〈저자소개〉

김 대 엽 (DaeYoub Kim) 종신회원
2000년 2월: 고려대학교 수학과 (이학박사)
1997년 9월~2000년 2월: Teleman, CAS 연구원
2000년 3월~2002년 8월: 시큐아이, 정보보호연구소 차장
2002년 9월~2012년 2월: 삼정전자 종합기술원 수석연구원
2012년 3월~현재: 수원대학교 정보보호학과 조교수
〈관심분야〉 콘텐츠 보호 기술, 블록체인, 미래 인터넷 보안