http://dx.doi.org/10.7840/kics.2015.40.4.692

효과적인 XaaS 구현을 위한 NDN 데이터 인증 기술

김 대 엽◆°

NDN Contents Verification Scheme for Efficient XaaS Implementation

DaeYoub Kim◆°

요 약

서비스형 IT 요소 배포 기술(XaaS)는 소프트웨어, 프랫폼, 인프라와 같은 IT 요소의 기능 중 사용자가 필요로 하는 기능만을 서비스로 배포해 이용하도록 한 IT 서비스 형태를 말한다. XaaS와 같은 서비스를 안전하고 효과적으로 제공하기 위해서는 네트워크 병목현상, 취약한 보안 문제와 같은 인터넷의 문제들을 해결해야만 한다. 미래 인터넷 기술은 이와 같은 인터넷이 갖고 있는 다양한 문제들을 해결하기 위하여 제안되었다. 특히, 데이터 이름 기반 네트워킹 기술 (NDN)은 네트워크 노드 또는 멀티미디어 프락시 서버 등에 데이터를 임시 저장한 후, 해당 데이터에 대한 요청이 다시 수신되면 앞서 저장된 데이터를 사용자에게 전송함으로써 데이터 배포자에게 집중되는 과다한 요청 메시지를 효과적으로 분산 처리하도록 설계되었다. 그러나 NDN은 수신된 데이터의 실제 배포자가 원배포자와 다르고, 실제 배포자를 확인할 수 없기 때문에 수신된 데이터를 신뢰할 수 없다는 문제점을 내포하고 있다. 그러므로 수신된 데이터를 이용하기 전에 반드시 해당 데이터를 검증해야 한다. 이와 같은 검증 프로세스는 XaaS의 서비스 운영 지연을 초래할 수 있다. 본 논문에서는 데이터 인증에 따른 문제점을 살펴보고, 효율적인 데이터 인증을 위한 개선된 운영 방안을 제안한다.

Key Words : XaaS, Futur Internet, NDN, Content Verification, MHT

ABSTRACT

Evarything as a Service (XaaS) is a software, platform, infra distribution method which provide users with necessary modules, not entire modules, as a service. To efficiently and securely operate services such as XaaS, it is needed to solve various Internet problems like network congestion, weak security and so on. Future Internet technologies are provided to solve such problems. Specially, named data networking architecture (NDN) proposes that network nodes cache transmitted data, and then they send the cached data if receiving request messages for the cached data. So NDN can efficiently diffuse excessive request messages transmitted toward original contents providers. However, when receiving contents through NDN, receivers can not confirm the practical providers because the practical providers can be different from original contents providers. Hence, it is requested for receivers to verify the received contents and such a verification process can cause service delay of XaaS. In this paper, we improve a content verification scheme of NDN to enhance the performance of services such as XaaS.

※ 본 연구는 한국연구재단 기초연구사업과제(NRF-2013R1A1A2008389) 지원으로 수행되었습니다.
◆° First and Corresponding Author : Suwon University Department of Information Security, daeyoub69@suwon.ac.kr, 정회원
논문번호 : KICS2015-03-062, Received March 23, 2015; Revised April 17, 2015; Accepted April 17, 2015

Ⅰ. 서 론

서비스형 IT 요소 배포 기술 (Everything as a Service, XaaS)는 소프트웨어, 플랫폼, 인프라와 같은 IT 요소의 기능 중 사용자가 필요로 하는 모듈만을 서비스 형태로 배포하고, 사용자는 자신이 필요할 때, 필요한 기능만을 전송 받아 이용한 후, 이용한 기능만큼만 요금을 지불하는 서비스 형태이다. XaaS는 필요한 기능을 사용자가 다운로드하여 자신의 단말기에 설치하는 형태와 서버 상에서 작동하는 기능을 네트워크를 통해 온라인으로 이용하는 형태가 있다. 최근에는 무선 인터넷 보급과 모바일 디바이스의 성능 진화가 지속되면서 기업과 개인 컴퓨터, 모바일 영역까지 다양한 형태의 XaaS 모델이 제안되고 있다. 이와 같은 XaaS를 구현하기 위해서는 네트워크의 효율성과 안전성 확보가 필수적으로 요구 된다[1-3].

초기 인터넷 개발자의 주된 관심은 네트워크에 연결된 호스트들 사이에 안전한 연결을 제공해 주는 것이다. 그러므로 현재와 같은 다양한 환경과 서비스에 인터넷이 활용되는 상황은 고려하지 못했다. 그 결과, 네트워크 병목 현상, 다양한 보안 위협, 기기들의 이동에 따른 비효율성과 같은 다양한 문제들이 발생하고 있다. 이와 같은 인터넷의 문제들을 해결하고, 인터넷을 통해 고용량 멀티미디어 데이터를 빠르게 전송하고, 다양한 서비스를 효과적으로 구현하기 위해 미래 인터넷 기술에 대한 연구가 활발하게 진행되고 있다[4-13]. 특히, 데이터 제작자(Publisher)에게 집중되는 데이터/서비스 요청 메시지들로 인해 발생되는 네트워크 병목 현상을 해결하기 위하여 주요 미래 인터넷 기술들은 중간 네트워크 노드들 또는 프락시 서버에 데이터를 임시 저장한 후, 저장된 데이터에 대한 요청 메시지를 네트워크 노드 또는 프락시 서버가 수신하면, 제작자를 대신하여 해당 노드 또는 서버가 저장된 데이터를 사용자에게 전송하는 방안을 고려하고 있다.

기존의 P2P (Peer-to-Peer) 네트워킹 기술과 CDN (Content Delivery Network) 기술도 이와 같은 측면에서 네트워크의 효율성을 연구한 기술들이라 할 수 있다. 그러나 P2P/CDN 등이 네트워킹 계층 위에 overlay로 구현된 기술인 반면, 데이터 이름 기반 네트워킹 (Named Data Networking, NDN)과 정보 중심의 네트워킹 (Inform. Centric Networking, ICN) 같은 미래 인터넷 기술들은 네트워킹 계층에서 이와 같은 기능을 구현하고 있다[7,8].

NDN은 네트워크 중간 노드들이 수신된 데이터를 다른 노드 또는 사용자에게 중개할 때, 해당 노드의 저장 매체(Content Store, CS)에 데이터를 임시 저장(Caching)하도록 제안한다. 네트워크 노드에 임시 저장된 데이터에 대한 요청 메시지 (Interest)를 해당 네트워크 노드가 다시 수신하면, 네트워크 노드는 저장된 데이터를 사용자에게 응답 메시지 (Data)로 직접 전송하고, 수신된 Interest의 중계를 중단한다. 이와 같이 사용자와 데이터 Publisher 사이에 위치한 중간 네트워크 노드들에 의해서 Interest가 분산 처리되기 때문에 Interest가 Publisher에게 집중되어 발생하는 네트워크 병목 현상을 효과적으로 처리할 수 있다.

그러나 NDN은 사용자가 요청한 데이터를 불특정 다수의 노드들로부터 전송 받을 수 있고, 데이터를 실제 전송한 노드를 확인할 수 없기 때문에 악성 코드 배포 등에 악용될 수 있다. 그러므로 사용자가 수신된 데이터를 이용하기 전에, 해당 데이터를 인증하는 절차를 반드시 수행할 것을 권고한다. 그러나 이와 같은 수신 데이터의 반복적인 인증 절차는 서비스 지연의 주된 원인이 되고 있어, 이에 대한 개선이 요구된다.

본 논문에서는 NDN을 이용한 데이터 전송 서비스의 효율성을 높이기 위하여 NDN 데이터 인증 절차의 개선 방안을 제안한다.

Ⅱ. Named Data Networking (NDN)

그림 1은 NDN의 네트워크 노드가 Interest 및 Data를 처리하는 과정을 설명 한다. (A~F)는 Interest 처리 절차이고, (G~J)는 Data 처리 절차이다.

(A) 네트워크 노드의 네트워크 인터페이스 (Face 1)을 통하여 Interest가 수신된다.

(B) 수신된 Interest에 대응되는 Data가 CS에 저장되어 있는지를 우선 확인한다. 만약 요청된 Data가 CS에 저장되어 있다면, 해당 Data를 Face 1을 통해 전송한 후, Interest 처리 절차를 종료한다.

(C) 수신된 Interest에 대응되는 Data가 CS에 저장되어 있지 않다면, 수신된 Interest 정보가 PIT (Pending Interest Table)에 기록되어 있는지 확인한다. 만약 PIT에 해당 기록이 있다면, 해당 정보의 incoming Face 필드에 Face 1을 추가한 후, Interest 처리 절차를 종료한다.

(D) 수신된 Interest 정보가 PIT에 기록되어 있지 않다면, FIB (Forwarding Information based) 테이블을 참조해서, 수신된 Interest를 전송할 네트워크 인터페이스 (Face 3)를 선택한다.

(E) PIT에 수신된 Interest와 Face 1을 기록한다.

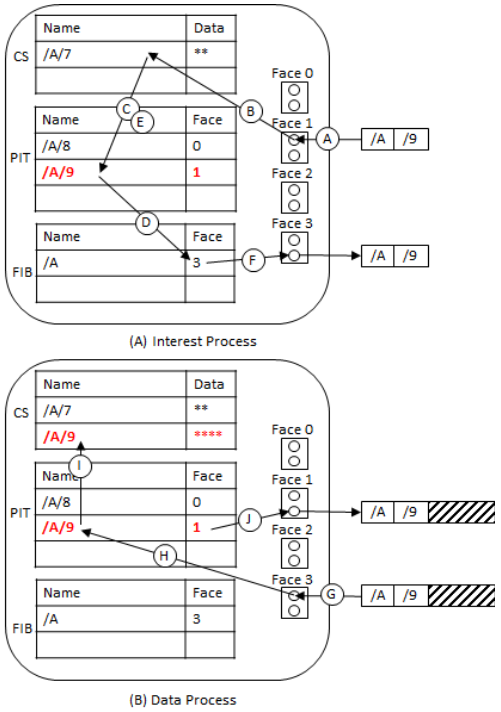

그림 1. NDN Interest 패킷과 Data 패킷 처리 절차
Fig. 1. NDN Interest and Data Packet Process

(F) FIB에서 선택한 Face 3를 통하여 수신된 Interest를 전송한다.

(G) Face 3를 통하여 Data가 수신된다.

(H) 수신된 Data에 대응되는 Interest 정보가 PIT에 있는지 확인한다. 만약 없으면, 해당 Data는 폐기 된다.

(I) 수신된 Data에 대응하는 Interest 정보가 PIT에 존재하면, CS에 Data를 저장한다.

(J) PIT에서 확인된 Interest 정보의 incoming Face들을 통해서 Data를 전송한다.

그러나 이와 같은 중간 네트워크 노드에 의한 데이터 전송 기법은 데이터가 Publisher가 아닌 불특정 다수의 노드로부터 전송될 수 있기 때문에 데이터 수신자가 데이터 송신자를 정확하게 확인할 수 없다. 그러므로 수신된 데이터가 인증되지 않은 노드로부터 전송된 악성 데이터일 가능성이 있다. 일반적으로 비연결지향 (connectionless) 통신에서는 데이터의 출처를 인증 (data origin authentication)한다. 그러므로 이와 같은 인증 문제를 해결하기 위하여, NDN도 사용자가 수신된 데이터를 이용하기 전에 반드시 데이터의 Publisher를 인증할 것을 요구한다.

또한, 대용량 데이터의 효과적인 배포를 위하여 NDN은 데이터를 단편화(fragmentation)하여 세그먼트(segment) 단위로 관리/전송하며, 데이터 인증 역시 세그먼트 단위로 수행한다. 그러므로 대용량 데이터 배포 시, 모든 세그먼트 마다 반복적으로 수행되는 인증 절차는 서비스 지연을 발생시키는 주요 원인이 된다. 그러므로 NDN을 실제 서비스에 응용하기 위해서는 효율적으로 데이터 인증 기술에 대한 연구가 반드시 필요하다.

Ⅲ. NDN 데이터 인증

3.1 MHT 기반 NDN 데이터 인증 기술

효과적인 데이터 인증을 위해 NDN은 기본적으로 Merkel Hash Tree 기반의 데이터 인증 기술 (MHT)을 사용 한다[7,14-18]. MHT는 계층화된 해쉬 값 전송 및 처리가 필요하기 때문에, NDN을 통해 대용량 데이터를 전송할 경우, MHT 기반 인증의 계산 및 전송 오버헤드의 개선이 요구된다. 그림 2는 NDN에서 제안된 MHT 기반 세그먼트 인증 방법을 설명한다[7,8]. 데이터 Publisher는 다음과 같은 절차를 따라 NDN 세그먼트들을 생성 한다:

(A) Publisher는 데이터를 N ($N \le 2^n$) 개의 세그먼트, $\{S_1,\cdots,S_N\}$으로 단편화 한다. 각각의 세그먼트는 NDN에서 1개의 Data 패킷으로 전송 가능한 최대 용량으로 구성한다.

(B) 생성된 S_i들을 인증하기 위하여 2^n개의 최하위 노드(Leaf Node)들로 구성된 이진트리 (Binary Tree)를 생성한다. 이진트리의 최상위 노드 (Root Node)를 N_1이라 하자. 각각의 S_i는 인덱스 순서에 따라 이진트리의 최하위 노드 N_{2^n+i-1}에 할당 된다.

(C) S_i의 해쉬 값을 계산하여 N_{2^n+i-1}의 노드 값 (V_{2^n+i-1})으로 사용 한다:

$$V_{2^n+i-1} = H(S_i). \quad (1)$$

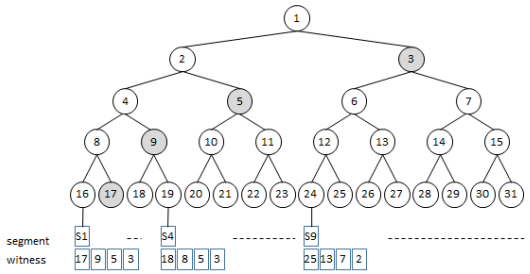

그림 2. MHT 기반 데이터 인증
Fig. 2. MHT-based Data Verification Scheme

여기서, $H()$는 단방향 해쉬 함수를 의미한다.

(D) 최하위 노드를 제외한 모든 상위 노드 N_k $(1 \leq k \leq 2^n - 1)$의 노드 값 V_k를 다음과 같이 계산한다:

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

여기서, V_{2k}와 V_{2k+1}은 각각 N_k의 왼쪽/오른쪽 자식 노드 (Left/Right Child Node)의 노드 값을 의미한다. 이와 같은 노드 값 계산 과정을 하위 노드부터 상위 노드 방향으로 반복 수행하여 최상위 노드 N_1의 노드 값 V_1 까지 계산한다.

(E) Publisher는 자신의 전자 서명 키 (SK)를 이용하여 V_1에 대한 전자서명 값을 계산 한다:

$$St = Sign_{SK}(V_1). \quad (3)$$

(F) S_i 검증에 필요한 witness W_i를 생성 한다. W_i는 S_i에 대응하는 최하위 노드 N_{2^n+i-1} 부터 최상위 노드 N_1 까지의 경로(Path)에 포함된 모든 노드들의 형제 노드 (Sibling Node)들의 노드 값들로 구성된다. 예를 들어, 그림 2에서와 같이 16개의 최하위 노드로 구성된 이진트리에서 S_1에 대응하는 최하위 노드 N_{16}부터 최상위 노드 N_1 까지 이르는 경로에 포함된 노드들의 형제 노드들은 N_{17}, N_9, N_5, N_3이다. 그러므로 W_1는 $\{V_{17}, V_9, V_5, V_3\}$으로 구성된다.

(G) S_i 전송을 위한 Data (D_i)를 다음과 같이 구성하여 배포 한다:

$$D_i = \{S_i, (St, W_i)\}. \quad (4)$$

수신된 데이터가 실제 Publisher에 의해 생성된 유효 데이터인지를 검증하기 위하여 사용자는 다음과 같이 수신된 데이터를 검증한다.

(A) 사용자는 데이터의 D_1을 요청하기 위한 Interest를 생성/전송한다. 사용자가 D_1을 수신하면, D_1에 포함되어 있는 S_1과 W_1을 이용하여 V_1을 계산한다. 계산된 V_1을 이용하여 D_1에 첨부 된 St를 검증한다. 만약 St가 유효하면, D_1이 유효한 것으로 간주한 후, V_1을 임시 저장한 한다.

(B) D_i $(i > 1)$를 요청하기 위한 Interest를 차례로 생성/전송한다. D_i를 수신하면, 수신된 D_i에 포함된 S_i와 W_i를 이용하여 V_1을 계산한다. 계산된 V_1과 앞서 임시 저장한 V_1을 비교한다. 만약 두 값이 같으면, 사용자는 D_i가 유효한 것으로 간주한다.

(C) 데이터의 모든 D_i들이 유효하면, 해당 데이터를 유효하다고 간주하고, 수신된 S_i들을 조합하여 데이터를 재구성한다.

D_1 인증에서 V_1을 저장 한 후, D_i $(i > 1)$ 인증을 위하여 전자 서명 값을 직접 확인하지 않고, 단순히 V_1 값만 비교하면 충분하기 때문에 데이터 인증 소요 시간을 보다 효과적으로 줄일 수 있다. 그러나 MHT를 대용량 데이터 인증에 적용할 경우, 각각의 S_i 마다 W_i를 추가로 전송해야 하고, V_1을 계산하기 위하여 해쉬 값을 반복적으로 계산해야 한다. 이와 같은 인증 방법은 여전히 전체 서비스를 지연시키는 원인이 될 수 있다.

그림 3은 데이터를 안드로이드 폰과 NDN을 통해 전송할 때 데이터 인증 절차로 인한 서비스 지연 정도를 측정한 결과를 나타낸다. 실험 결과에서 보이듯이 MHT 기반 데이터 인증 기술이 적용된 경우, 데이터 처리 시간이 평균 20% 이상 지연되는 것을 알 수 있다.

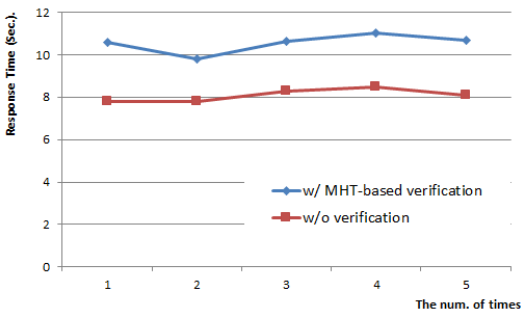

그림 3. 데이터 인증에 따른 서비스 응답 시간 분석
Fig. 3. Service Response Time Evaluation for Verification

3.2 개선된 MHT기반 NDN Data 인증

Witness 전송으로 인하여 발생하는 전송량 증가 (Transmission Overhead)를 개선하고, 각각의 세그먼트 마다 반복적인 해쉬 값 계산으로 인한 서비스 지연 (Computation Overhead)을 개선하기 위하여 MHT 운영 방안을 다음과 같이 개선한다.

3.2.1 Witness 중복 전송 방지 기법

NDN은 기본적으로 세그먼트의 순서에 따라 순차적으로 요청/처리된다. 이 때, 각각의 세그먼트는 인증

을 위해 witness를 포함한다. 그러나 2^n개의 세그먼트로 구성된 데이터를 이용하기 위해서 2^n개의 세그먼트를 수신/처리한다고 할 때, 중복되어 전송되는 witness가 매우 많다. 실제로 최하위 노드의 level을 $n-1$ 이라 하고, 최상위 노드의 level을 1이라고 할 때, level이 $n-1$인 노드에 대응되는 노드 값 (해쉬 값)은 witness로 1번씩만 전송되지만, level이 $n-2$인 노드에 대응되는 노드 값은 witness로 2번씩, level이 $n-3$인 노드에 대응되는 노드 값은 4번씩 전송된다. 즉, level이 $n-k$인 노드에 대응되는 노드 값은 witness로 2^k-1번씩 중복되어 전송된다.

이와 같이 중복해서 전송되는 witness를 효과적으로 처리하기 위해, 본 논문에서는 앞서 전송된 witness를 임시 저장한 후, 다시 사용하는 기법을 제안한다. 그림 4는 개선된 세그먼트 인증 방법의 예이다. 기본 MHT 기반 인증과 같이 데이터 인증을 위해 해당 데이터의 Publisher는 배포하려고 하는 데이터를 N ($N \leq 2^n$) 개의 세그먼트, $\{S_1,\cdots,S_N\}$으로 단편화한 후, 이진트리를 구성하여 노드 값을 계산한다. Publisher는 세그먼트에 할당된 최하위 노드의 순서에 따라 witness를 다음과 같이 구성 한다: 세그먼트 S_i에 할당된 최하위 노드(N_α)가 N_{2^n} 또는 $N_{2^n+2^{n-1}}$인 경우, N_α는 이진트리를 구성하는 2개의 최대 서브 트리 중 하나의 가장 왼쪽에 위치한 최하위 노드이다. 그림 4에서는 N_{16}과 N_{24}가 이에 해당된다. N_α에 할당된 S_i를 전송하기 위한 witness는 기본 MHT에서 제안된 것처럼 해당 노드의 경로 위에 있는 노드들의 형제 노드 값들로 구성된다. N_α를 제외한 나머지 최하위 노드 N_β에 할당된 S_i는 다음과 같이 witness를 구성한다.

(A) $2^\gamma \leq \beta-\alpha < 2^{\gamma+1}$을 만족하는 γ 값을 계산한다.

(B) 기본 MHT에서 제안된 것처럼 N_β에서부터 N_1에까지의 경로 위에 있는 노드들의 형제 노드들의 노드 값들 중에서 하위 level에 대응되는 2^γ개의 노드 값만을 선택하여 witness로 구성한다.

이와 같이 구성된 W_i를 포함한 D_i를 수신한 사용자는 D_i에 대응되는 최하위 노드의 위치를 확인한다. 해당 최하위 노드가 N_{2^n} 또는 $N_{2^n+2^{n-1}}$인 경우, D_i에 포함된 W_i를 이용하여 세그먼트 S_i를 검증한다. 검증 결과 S_i가 유효한 세그먼트로 판단되면, D_i에 포함되어 있는 W_i를 인덱스의 순서에 따라 차례로 임시 저장한다. 이 후, 같은 서브 트리에 속한 최하위 노드에 대응되는 D_j를 순차적으로 수신하면, 각각의 D_j에 저장된 W_j와 사용자가 임시 저장한 W_i를 비교하여, 부족한 witness는 임시 저장한 W_i의 원소로 대체한 후, 세그먼트 S_j를 검증한다. 그림 4에서 D_9는 N_{24}에 대응되기 때문에, S_9와 witness $\{V_{25}, V_{13}, V_7, V_2\}$로 구성된다. 사용자는 witness를 이용하여 V_1을 계산 한 후, 검증 결과 V_1이 유효 하다면, V_1과 $\{V_{25}, V_{13}, V_7, V_2\}$를 저장한다. D_{13}이 수신되면 D_{13}의 witness $\{V_{29}, V_{15}, V_6\}$를 확인한 후, 저장된 $\{V_{25}, V_{13}, V_7, V_2\}$와 개수를 비교한 후, 부족한 V_2를 읽어 와서 witness $\{V_{29}, V_{15}, V_6, V_2\}$를 구성한 후 S_{13}을 검증한다.

3.2.2 부분 트리 기반 계층화된 MHT 운영

그림 5는 부분 트리 기반 계층화된 MHT의 예이다. 데이터 인증을 위해 Publisher는 배포하려고 하는 데이터를 N ($N \leq 2^n$) 개의 세그먼트, $\{S_1,\cdots,S_N\}$으로 단편화한다. MHT에서 설명한 것처럼 이진트리를 구

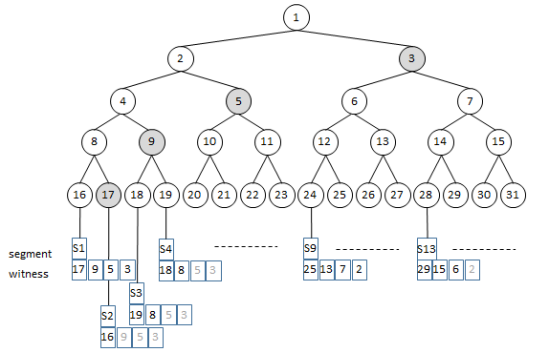

그림 4. MHT의 중복 전송 방지 기법
Fig. 4. MHT Duplication Prevention Scheme

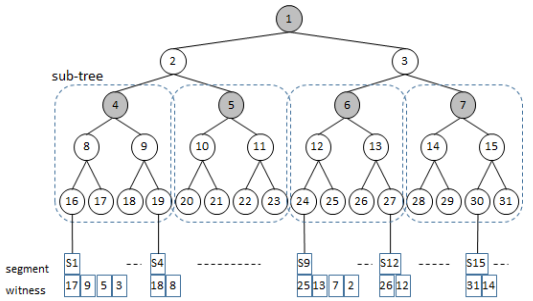

그림 5. 서브 트리 기반 MHT 운영 기법
Fig. 5. Sub-Tree based MHT operation Scheme

성한 후, 노드 값을 계산하여 할당 한다. Publisher는 세그먼트에 할당된 최하위 노드의 인덱스 순서에 따라 witness를 다음과 같이 구성 한다.

(A) 생성한 이진트리에서 같은 크기의 2^k개의 부분 트리를 구성한다.

(B) 각각의 부분 트리의 최하위 노드 중에서 가장 왼쪽 노드 (N_α)에 할당된 S_i를 인증하기 위해 필요한 witness는 기본 MHT에서 제안된 것처럼 전체 이진트리에서 해당 노드의 경로 위에 있는 노드들의 형제 노드 값들로 구성된다. 예를 들어 N_{16}에 대응되는 S_1을 전송하기 위한 witness는 V_1 계산에 필요한 $\{V_{17}, V_9, V_5, V_3\}$ 이다.

(C) 각각의 부분 트리의 최하위 노드들 중에서, 가장 왼쪽 최하위 노드인 N_α를 제외한 나머지 최하위 노드 N_β에 할당된 S_j를 인증하기 위해 필요한 witness는 해당 부분 트리에서 N_β의 경로 위에 있는 노드들의 형제 노드 값들로 구성된다. 예를 들어 N_{19}에 대응되는 S_4을 전송하기 위한 witness는 V_4 계산에 필요한 $\{V_{18}, V_8\}$ 이다.

이와 같이 구성된 W_i를 포함한 D_i를 수신한 사용자는 D_i에 대응되는 최하위 노드의 위치를 확인한다. S_i에 대응된 최하위 노드를 N_α라고 하자.

(A) $\alpha = 2^n$ 이거나 적당한 양의 정수 r에 대하여 $\alpha = 2^n + (r \times 2^{n-k})$이면, D_i에 첨부된 W_i를 이용하여 V_1을 계산한 후, 첨부된 서명을 검증한다. 만약 V_1이 유효한 노드 값이면, S_i도 유효하다고 간주하고, N_α를 포함한 부분 트리의 최상위 노드 N_β의 노드 값 V_β을 V_1와 함께 임시 저장한다.

(B) α가 그 외의 경우라면, D_i에 첨부된 W_i를 이용하여 V_β를 계산한 후, 임시 저장되어 있는 V_β 값과 비교한다. 두 값이 같으면, S_i를 유효하다고 간주한다.

Ⅳ. 성능 분석

그림 6은 기본 MHT 기반의 데이터 인증 기법과 제안된 2가지 인증 기법을 적용했을 때, 필요한 witness의 총 수를 나타낸다. 성능 평가를 위해 데이터가 64, 128, 256, 512, 1024, 2048개의 세그먼트로 단편화된 경우를 가정하였다. 그림 6-(A)는 witness 중복 전송 방지 기법을 MHT에 적용한 결과이다 (MHT+1). 기본 MHT와 비교하 할 때, witness 전송량은 세그먼트의 수가 늘어남에 따라 급속히 줄어들

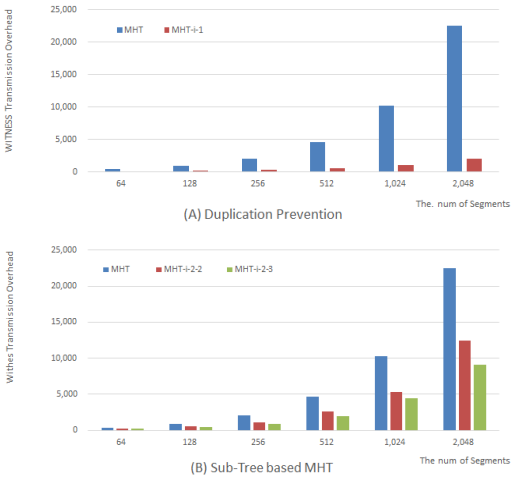

그림 6. 성능 분석 (전송량)
Fig. 6. Transmission Overhead Performance Evaluation

어 1,024개의 세그먼트로 구성된 데이터의 경우 기본 MHT 대비 10% 정도의 witness 만을 필요로 한다. 그러나 기본 MHT가 V_1 만을 저장하는 반면, MHT+1은 이진트리의 depth 수만큼의 V_i를 저장 한다. 또한, 전송되지 않은 witness를 판단하고, V_1을 계산하기 위해 추가적인 작업이 필요하지만 평가 결과 그 성능 차이는 거의 변화가 없다.

그림 6-(B)는 부분 트리 기반 계층화된 MHT 운영 기법이 적용된 결과이다 (MHT+2). MHT+2는 적용한 부분 트리의 크기에 따라 성능에 차이를 보인다. 전체 이진트리의 depth를 n이라고 할 때, MHT+2-2는 부분 트리의 depth을 $n/2$로 설정하고 평가한 결과를 나타낸다. MHT+2-3은 이 값을 $n/3$으로 설정하고 평가한 결과를 나타낸다. 이는 부분 트리의 크기가 작을수록 전체 성능은 개선됨을 알 수 있다. 그러나 부분 트리의 depth를 2로 설정하면, 전체 witness의 수가 다시 증가하는 것으로 관찰되었다.

MHT-i-1은 전송되는 witness의 양은 기본 MHT에 비해 많이 감소했지만, V_1을 계산하기 위해 필요한 해쉬 값 계산양은 MHT와 동일하다. 그러나 그림 7에서와 같이 MHT-i-2는 데이터 검증에 필요한 해쉬 값 계산 횟수도 개선되었다.

Ⅴ. 결 론

XaaS는 서비스로서의 소프트웨어(SaaS), 서비스로서의 플랫폼(PaaS), 서비스로서의 개발(DaaS), 서비스로서의 인프라(IaaS) 등 서비스 형태로 제공될 수 있

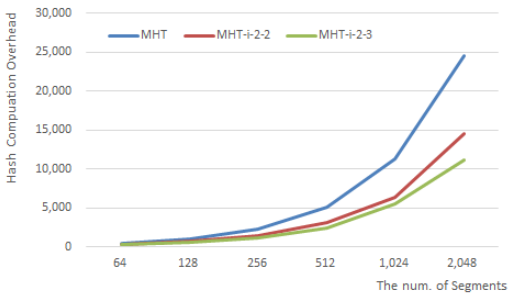

그림 7. 성능 분석 (계산량)
Fig. 7. Computation Overhead Performance Evaluation

는 모든 IT 요소를 말한다. 본래 XaaS의 출발점은 SaaS였으나 서비스 대상이 다양화되고, 의미가 더욱 확장되고 있다. 필요한 만큼 쓰고 사용한 만큼 지불하는 유틸리티 컴퓨팅이 확산되면서 소프트웨어의 범위를 넘어 플랫폼, 하드웨어, 데이터베이스 등 다양한 서비스 모델들이 속속 등장하고 있다. 최근에는 무선 인터넷 환경과 모바일 디바이스의 성능 진화가 지속되면서 기업과 개인 컴퓨터 환경, 모바일 영역까지 확대되고 있다.

이러한 서비스 형태를 구현하기 위해서는 네트워크 성능 향상이 필수적으로 요구된다. 그러나 네트워크 인프라 교체를 통한 성능 향상은 고비용이라는 단점이 있다. 또한, 인터넷의 많은 문제점들 또한 해결해야 될 과제이다. 본 논문에서는 이러한 문제들을 해결하기 위해 제안된 미래 인터넷 기술을 살펴보고 제안된 미래 인터넷 기술이 보안성 향상 방안을 제안하였다. 제안된 기법은 전송 패킷의 인증에 필요한 추가 정보의 중복 전송을 방지하여 네트워크의 성능이 향상 되도록 설계 되었으며, 부분 트리를 이용한 인증 기법은 인증 정보의 전송량 감소뿐만 아니라 인증 프로세스를 개선할 수 있게 제안되었다.

제안된 기법은 미래 인터넷 기술의 패킷 인증을 위해 요구되는 Transmission/Computation Overhead를 개선하여 SaaS와 같이 네트워크를 이용한 다양한 형태의 서비스의 성능을 개선할 수 있을 것으로 기대된다.

References

[1] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "Key challenges in cloud computing: Enabling the future internet of services," *IEEE Internet Computing,* vol. 17, no. 4, pp. 18-25, 2013.

[2] B. P. Rimal, C. Eunmi, and I. Lumb, "A taxonomy and survey of cloud computing systems," *Int. Joint Conf. INC, IMS and IDC*, pp. 44-51, Seoul, Aug. 2009.

[3] M. Jensen, J. Schwenk, N. Gruschka, and L. Iacon, "On technical security issues in cloud computing," in *Proc. IEEE Int. Conf. Cloud Computing (CLOUD-II)*, pp. 109-116, India, 2009.

[4] T. Koponen, M. Chawla, B. Chun, A. Ermolinskiy, K. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," *ACM SIGCOMM'07*, pp. 181-192, Oct. 2007.

[5] B. Ahlgren, et al., *Second NetInf architecture description*, 4WARD EU FP7 Project, Deliverable D-6.2 v2.0, Apr. 2010.

[6] J. Pan, S. Paul, and R. Jain, "A survey of the research on future internet architectures," *IEEE Commun. Mag.*, pp. 26-36, Jul. 2011.

[7] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," *ACMCoNext*, pp. 1-6, Dec. 2009.

[8] L. Zhang, et al., "Named data networking (NDN) Project," *NDN-0001*, Oct. 2010.

[9] J. H. Kim and S. K. Kim, "Recent trend on the semantic web and future internet services," *KICS Summer Conf.*, pp. 316-317, Korea, Jun. 2011.

[10] Y. J. Kim, J. S. Park, and B. M. Chin, "Standardization on future internet," *KICS Spring Conf.*, pp. 342-343, Korea, Feb. 2011.

[11] M. K. Park, S. H. Min, B. C. Kim, J. Y. Lee, and D. Y. Kim, "Implementation of a future internet testbed using software based MAC in IP capsulator," *KICS Fall Conf.*, pp. 240-241, Korea, Feb. 2011.

[12] J. Y. Lee and J. H. Lee, "Secure routing scheme in CCN-based mobile ad-hoc networking environments," *J. KICS*, vol. 39B, no. 5, 2014.

[13] J. Shin, J. Lee, and J. Lee, "Secure routing scheme in CCN-based mobile ad-hoc networking environments," *J. KICS*, vol. 39B,

no. 12, 2015.

[14] R. Merkle, “Protocol for public key cryptosystems,” *IEEE Symp. Research in Security and Privacy*, Apr. 1980.

[15] G. Zion and D. Kavitha, “Remote sensing data as a service in hybrid clouds: Security challenges and trusted third party auditing mechanisms,” *Int. J. Advanced Research in Computer and Commun. Eng.*, vol. 1, no. 7, pp 481-486, Sept. 2012.

[16] K. Grover and A. Lim, “A survey of broadcast authentication schemes for wireless networks,” *Ad Hoc Networks*, vol. 24, part A, pp. 288-316, Jan. 2015.

[17] S. Hyun, P. Ning, A. Liu, and W. Du, “Seluge: Secure and DoS-resistant code dissemination in wireless sensor network,” *Int. Conf. Inf. Process. in Sensor Netw.*, 2008.

[18] D. Y. Kim and J. S. Park, “Efficient contents verification scheme for contents-centric networking,” *J. KICS*, vol. 39B, no. 4, 2014.

김 대 엽 (DaeYoub Kim)

2000년 2월 : 고려대학교 수학과 박사

2000년 2월~2002년 8월 : 시큐아이 정보보호연구소 차장

2002년 9월~2012년 2월 : 삼성전자 종합기술원 전문연구원

2012년 3월~현재 : 수원대학교 정보보호학과 조교수

<관심분야> 콘텐츠 보안, 미래 인터넷 보안, 난독화, 포렌직