Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.4, Aug. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.4.831

콘텐츠 중심 네트워크를 위한 안전한 패킷 단편화 기술*

현 상 원†‡
성균관대학교

Secure Fragmentation Technique for Content-Centric Networking*

Sangwon Hyun†‡
Sungkyunkwan University

요 약

본 논문에서는 콘텐츠 중심 네트워크(CCN, Content-Centric Networking)를 위한 안전한 패킷 단편화(fragmentation) 기술을 제안한다. 제안하는 기술은 패킷조각(fragment)들에 대한 불법적인 위변조 가능성을 차단하고, 패킷조각 수신 시 높은 확률로 즉각적인 신뢰성 검증을 제공함으로써 검증 지연을 악용한 DoS 공격으로부터 높은 안전성을 제공한다. 본 논문의 성능 분석 결과는 약간의 부하 증가만으로 제안하는 기술이 기존 기술보다 훨씬 더 높은 안전성을 제공함을 보여준다.

ABSTRACT

This paper presents a secure and DoS-resistant fragment authentication technique for Content-Centric Networking (CCN). Our approach not only guarantees the authenticity of each fragment, but also provides a high resistance to DoS attacks through the immediate verification of fragment authenticity at interim nodes on the routing path. Our experimental results demonstrate that the proposed approach provides much stronger security than the existing approach, without imposing a significant overhead.

Keywords: Content-Centric Networking, Fragmentation, Fragment Authentication, DoS Attacks

I. 서 론

콘텐츠 중심 네트워크(CCN, Content-Centric Networking)[1]은 콘텐츠 이름 기반 라우팅(name-based routing) 및 중간 라우터에서 콘텐츠 캐싱(in-network caching) 기능을 기반으로 효율적이고 확장성 있는 콘텐츠 서비스 제공이 가능하며, 이에 인터넷 트래픽의 폭발적 증가에 효과적으로 대처하기 위한 미래 인터넷 기술로써 활발한 연구가 진행 중이다(https://named-data.net/). 한편 CCN에서 각 콘텐츠 패킷은 물리적인 네트워크 전송 경로 상에 MTU(Maximum Transmission Unit) 값에 따라 단편화(fragmentation)를 통해 작은 패킷조각(fragment)들로 나누어져서 전송된다. 이러한 패킷 단편화에 대한 악의적인 공격(예: DoS 공격)들로부터 CCN 네트워크를 보호하기 위해서는 불법 위변조된 패킷조각들을 효과적으로 찾아내서 제거할 수 있는 인증 방안이 반드시 필요하다[2].

CCN에서는 사용자가 특정 서버를 지정해서 콘텐츠를 요청할 수 없기 때문에 요청한 콘텐츠를 수신했을 때 그것이 신뢰할 수 있는 호스트/서버로부터 온 것인지를 확인하는 것이 불가능하다. 이런 이유 때문에 CCN에서는 콘텐츠를 수신한 사용자가 그 신뢰성(무결성 및 출처 확인)을 확인할 수 있도록 각 콘텐츠 패킷에 생성자의 전자서명이 반드시 첨부된다

Received(07. 10. 2017), Modified(08. 07. 2017), Accepted(08. 11. 2017)
* 이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2016R1A6A3A11930593)
† 주저자, swhyun77@skku.edu
‡ 교신저자, swhyun77@skku.edu(Corresponding author)

[1].

한편 CCN에서 콘텐츠 패킷이 단편화를 통해 여러 작은 패킷조각들로 나누어져서 전송되는 상황에서 전자서명을 이용해서 수신된 패킷조각을 검증하려면 우선 동일한 콘텐츠 패킷을 구성하는 나머지 모든 패킷조각들이 수신될 때까지 기다렸다가 패킷조각들 재조합을 통해 원래 콘텐츠 패킷을 복원해야 한다. 그러고 나서 복원된 패킷에 첨부된 전자서명 검증을 통해 결과적으로 수신했던 모든 패킷조각들의 신뢰성 검증이 이루어진다. 다시 말해서 수신된 패킷조각을 검증하기 위해서는 나머지 모든 패킷조각들이 도착하기를 기다려야 하며, 그렇게 검증을 마친 후에야 전송 경로 상에 다음 네트워크 노드로 전달함으로써 불법 위변조된 패킷조각들이 네트워크로 전파되어 자원이 낭비되는 것을 방지할 수 있다.

하지만 이러한 방식은 필연적으로 전송 지연을 증가시키기 때문에 비효율적이며, 더욱이 전송 경로 상에 각 노드를 거칠 때마다 이러한 전송 지연이 누적되므로 문제는 더욱 심각해진다[2]. 이러한 비효율 문제를 해결하기 위해서는 각각의 패킷조각 단위 인증(fragment-based authentication)이 반드시 필요하다. 패킷조각 단위 인증을 통해 검증을 통과한 패킷조각은 나머지 패킷조각들이 도착할 때까지 기다릴 필요 없이 다음 노드로 전달이 가능하며, 이를 통해 최종 사용자에게까지 전송 지연이 크게 개선된다.

최근에 발표된 논문 [2]에서 저자들은 일방향 해시체인(one-way hash chain) 기술과 전자서명을 결합한 CCN 환경에서 패킷조각 단위 인증을 제공하기 위한 기술인 FIGOA를 제안했다. 하지만 FIGOA는 일방향 해시체인을 사용하기 때문에 해시체인 상에 특정 패킷조각이 손실될 경우 그 이후 모든 패킷조각들은 수신되더라도 즉각 검증이 불가능하다. 그리고 이러한 패킷조각 손실로 인한 검증 지연이 전송 지연으로 이어지는 것을 피하기 위해 FIGOA에서는 수신된 패킷조각의 진위 여부가 아직 확인되지 않았더라고 우선은 다음 노드로 전파하는 전략을 취하는데, 이럴 경우 검증 과정을 거치지 않은 불법 위변조된 패킷조각들이 네트워크로 전파된다. 따라서 공격자가 의도적으로 즉각 검증이 불가능한 위변조된 패킷조각들을 대량으로 네트워크에 유입시킬 경우 이 패킷조각들이 빠르게 네트워크로 전파되어 라우터들의 버퍼를 점유함으로써 정상적인 서비스에 지장을 초래하는 DoS(Denial of Service) 공격이 가능하다. 더욱이 이 같은 공격이 발생할 경우 위변조된 패킷조각들이 최초 공격자로부터 시작해서 여러 라우터들을 거쳐서 빠르게 전파되기 때문에 최초 공격의 진원지를 규명하는 것 또한 어렵다.

본 논문에서는 CCN 환경에서 패킷조각들에 대한 불법적인 위변조를 방지하고, 더불어서 검증 지연을 악용한 DoS 공격으로부터 높은 안전성을 제공하는 패킷조각 단위 인증 기술을 제안한다. 제안하는 핵심 기술은 순방향 오류정정(forward error correction) 기술 중 하나인 Rabin의 정보 분산 알고리즘(IDA, Information Dispersal Algorithm)[3]을 통합 적용한 새로운 해시트리 구조이며, 제안된 해시트리를 통해 생성된 패킷조각들은 수신 시 높은 확률로 즉각적인 신뢰성 검증이 가능하기 때문에 검증 지연을 악용한 DoS 공격으로부터 안전하다. 본 논문에서는 제안기법과 FIGOA의 성능에 대한 비교 분석을 수행하였으며, 그 결과 제안 기법은 평균적으로 14%의 패킷조각 수 증가를 통해 FIGOA보다 평균 52% 더 높은 즉각 검증 가능 확률을 제공한다. 더불어서 제안 기법은 모든 실험 케이스들에 대해 98.2% 이상의 높은 즉각 검증 가능 확률을 제공한다.

DoS 공격에 대한 추가적인 보호 방안으로써 본 논문에서는 즉각적인 신뢰성 검증이 불가능한 패킷조각 수신 시 현재 네트워크 상황을 고려하여 추가 전파 여부를 유연하게 조정하는 방안을 제안한다. 제안 기법에서는 최근에 수신된 나머지 패킷조각들의 정상/비정상 비율을 기반으로 현재 수신된 즉각 검증 불가능한 패킷조각을 다음 네트워크 노드로 추가 전파할 확률을 가변적으로 조정한다. 이를 통해 DoS 공격이 진행 중인 네트워크 환경에서는 불법 패킷조각들을 효과적으로 필터링하여 추가 전파를 막고, 반대로 정상적인 네트워크 환경에서는 불필요한 성능 저하를 피하면서 패킷조각들이 신속하게 전파되도록 한다.

본 논문의 구성은 다음과 같다. 먼저 2절에서 관련 연구를 서술한 후, 3절에서 제안 기법을 설명한다. 4절에서는 효율성과 안전성 측면에서 제안 기법과 FIGOA의 성능을 비교 분석한 결과를 설명한다. 마지막으로, 5절에서 결론을 맺는다.

II. 관련 연구

2.1 CCN 개요

CCN[1]의 가장 핵심적인 특징은 콘텐츠 이름 기반의 요청 및 라우팅이며, 이를 위해 모든 패킷에는 기존 인터넷의 호스트 IP 주소 대신에 콘텐츠 이름

이 포함된다. CCN에서 특정 콘텐츠를 다운로드 받고자 하는 사용자는 자신이 원하는 콘텐츠 이름이 명시된 관심(interest) 패킷을 생성 및 전송함으로써 콘텐츠를 요청한다. 이 관심 패킷은 콘텐츠 이름 기반의 라우팅을 통해 콘텐츠 제공자/서버에게까지 전달되며, 콘텐츠 제공자는 수신한 관심 패킷에 명시된 콘텐츠 이름과 매칭되는 콘텐츠 패킷을 전송한다. 이때 콘텐츠 패킷에도 콘텐츠 이름이 포함되며, 콘텐츠 이름 기반의 라우팅을 통해 사용자의 관심 패킷이 전달된 라우팅 경로의 역방향을 따라 콘텐츠 패킷이 사용자에게까지 전달된다. 한편 콘텐츠 패킷은 네트워크 전송 경로 상에 가용한 MTU 값에 따라 단편화를 통해 작은 패킷조각들로 나누어져서 전송된다.

또한 데이터 전송의 효율성을 높이기 위해서 CCN 라우터는 콘텐츠 캐시를 운영하며, 관심 패킷 수신 시 요청된 콘텐츠가 자신의 캐시에 저장되어 있을 경우 굳이 콘텐츠 서버에게까지 요청할 필요 없이 캐시된 콘텐츠를 사용자에게 전달한다. 마지막으로 콘텐츠 패킷을 수신한 사용자가 데이터의 출처 및 무결성을 확인할 수 있도록 모든 콘텐츠 패킷에는 콘텐츠 생성자의 전자서명이 첨부된다.

2.2 해시트리

본 절에서는 제안기법의 기반이 되는 해시트리[4]에 관해 설명한다. Fig.1.은 $V_{0,0}$부터 $V_{0,7}$까지 8개의 조각들로 구성된 주어진 데이터(Data Chunk)를 인증하기 위한 해시트리의 예를 보여준다. Fig.1.에서 보는 바와 같이 인증하고자 하는 각각의 데이터 조각이 해시트리의 리프 노드(leaf node)가 된다. 해시트리의 내부 노드에는 그 자식 노드들 각각에 대해서 암호 해시 함수(예로, SHA-256)를 적용한 결과 해시 값들이 저장된다. 루트 노드에는 1개의 해시 값과 더불어서 그 해시 값에 대한 전자서명(RSA, DSA 또는 ECDSA signature)이 포함된다. Fig.1.에 해시트리의 경우 각 내부 노드(루트 노드 포함)는 최대 4개의 해시 값 또는 1개의 해시 값과 그것에 대한 전자서명 값을 포함할 수 있다. 해시트리에 각 노드를 검증하기 위해서는 그 노드로부터 루트 노드까지의 경로 상에 모든 노드들이 주어져야 하며, 이 경로를 *인증경로*라고 부른다. 예를 들어, Fig.1.에서 노드 $V_{0,1}$의 인증경로는 $V_{0,1}$, $V_{1,0}$, $V_{2,0}$, $V_{3,0}$으로 구성된다.

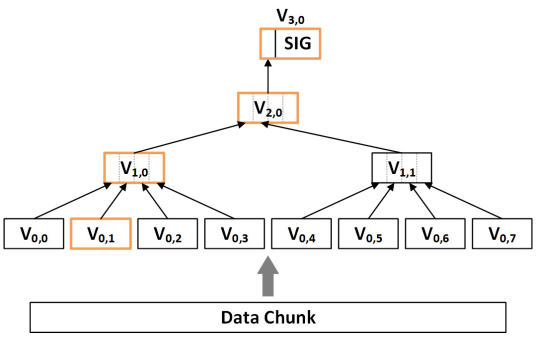

Fig. 1. Basic hash tree to authenticate eight pieces of data denoted as V0,0~V0,7

어떤 인증경로에 모든 노드가 주어졌을 때 검증 과정은 다음과 같다. 우선 루트 노드에 포함된 해시 값을 전자서명 검증을 통해 확인한다. 그리고 인증경로에 나머지 노드들 각각에 대해서는 그 노드의 해시 값을 계산하고 계산된 해시 값과 이미 신뢰성이 확인된 부모 노드에 저장된 해시 값을 비교함으로써 검증이 이루어진다. 이러한 구조의 해시트리에서 임의의 리프 노드에 저장된 값이 변경되면, 루트 노드를 포함한 모든 부모 노드들에 저장된 해시 값들이 변경된다. 더욱이 암호 해시 함수의 충돌 저항성(collision-resistance) 때문에 올바른 전자서명 키를 모르는 공격자가 해시트리에 포함된 임의의 데이터를 변경하는 것은 불가능하다. 결과적으로 해시트리에 모든 데이터 조각들은 루트 노드에 저장된 단일 서명 값(SIG)을 통해 인증되는 것이다.

2.3 정보 분산 알고리즘

본 논문의 제안기법은 해시 값들이 저장된 해시트리의 내부 노드가 손실되었을 때 효율적인 복원을 위해 Rabin의 정보 분산 알고리즘(IDA, Information Dispersal Algorithm)[3]을 이용한다. IDA는 Dispersal()과 Recovery() 2개의 연산들로 구성된다. 주어진 데이터 F에 대해 Dispersal(F, m, n)은 n개의 인코딩 된 조각들 $EB_i(0 \le i < n,\ n \ge m)$를 생성한다. 이때 인코딩 된 각 조각의 크기는 |F|/m과 같다(|F|는 데이터 F의 바이트 단위 크기를 나타냄). n개의 인코딩 된 조각들 중 임의의 m개가 주어지면, $Recovery\left(\left\{EB_{i_j} | 0 \le i_j < n, 0 \le j < m\right\}, m, n\right)$은 원본 데이터 F를 복원한다. 즉, IDA를 이용하면 최대 (n-m)개 조각들이 손실되더라도 원본 데이터의

복원이 가능하다. 본 논문에서는 (n-m)/n을 IDA의 *중복률*이라고 부르며, 이 비율은 IDA를 통해 복원 가능한 손실률을 의미한다.

III. 제안기법

본 절에서는 CCN 환경에서 안전한 콘텐츠 전송을 위해 제안하는 패킷조각 단위 인증 기술을 설명한다. 본 논문의 3절과 4절에서는 다음 표기법들을 사용한다. |M|은 데이터 M의 바이트 단위 크기를 나타낸다. M||M′은 데이터 M과 M′을 연결한 것을 나타낸다. f는 제안기법 해시트리에 각 패킷조각의 크기를 나타내며, h와 d는 각각 해시트리 전체의 높이와 각 내부 노드의 자식 노드들의 수를 나타낸다. $Frg_{i,j}$는 제안기법 해시트리의 높이 i에 j번째 패킷조각을 나타낸다. r은 IDA의 중복률을 나타내며, F()는 SHA-256 같은 암호 해시 함수를 나타낸다.

3.1 콘텐츠 패킷 단편화 및 인증

제안기법에서 전송하고자 하는 콘텐츠 패킷은 패킷조각 단위 인증을 위해 동일한 크기 f의 패킷조각들로 나누어진다. 각 패킷조각의 크기 f로는 콘텐츠 패킷이 전송될 네트워크 경로의 MTU 값이나, 또는 네트워크 표준에 명시된 최소 MTU 값을 사용할 수 있다. 콘텐츠 패킷이 전송될 네트워크 경로의 MTU 값은 [2]에 기술된 방법을 통해 얻을 수 있다. 크기 f로 나누어진 패킷조각들에 대해서 2.2 절에 설명된 방법으로 해시트리를 구성한다. 제안기법에서 해시트리에 각각의 노드는 하나의 패킷조각에 해당하므로 본 논문에서는 문맥에 따라 "노드"와 "*패킷조각*" 2개의 용어를 같은 의미로 번갈아 사용한다. Fig.1.에 묘사된 해시트리는 $V_{0,0}$~$V_{0,7}$ 8개의 패킷조각들로 구성된 콘텐츠 패킷을 인증하기 위한 해시트리이며, 각 내부 노드는 최대 4개의 해시 값들을 저장할 수 있다(d=4).

그런데 Fig.1.의 해시트리 구조에서 만약 어떤 내부 노드에 대응되는 패킷조각이 전송 중에 손실될 경우 그 노드의 모든 자식 노드들로부터 루트 노드까지의 인증경로가 끊어지게 된다. 즉, 어떤 자식 노드에 대응되는 패킷조각을 수신하더라도 루트 노드까지의 인증경로를 구성하지 못하기 때문에 그 신뢰성을 즉시 검증하는 것이 불가능하다. 그리고 이러한 검증 지연은 DoS 공격에 악용될 수 있다[5]. 따라서 Fig.1.에 해시트리 구조에서는 내부 노드들의 손실에 효과적으로 대처하는 것이 중요하다. 이를 위해 제안기법에서는 해시트리 생성 시 트리의 같은 높이에 위치한 내부 노드들에 대해서 Rabin의 IDA를 적용하여 일부 노드가 손실되더라도 재전송 없이 즉각적인 복원이 가능하도록 한다.

IDA 개선: IDA를 이용할 경우 정해진 수 이상의 인코딩 조각들이 주어지기 전까지는 원본 데이터를 부분적으로라도 얻는 것이 불가능하다. 뿐만 아니라 정해진 수 이상의 인코딩 조각들로부터 원본 데이터를 복원하기 위해서는 반드시 Recovery() 연산을 수행해야 한다. 제안기법에서는 Vandermonde 행렬[6]을 이용하여 IDA의 이런 점들을 개선한다.

행렬 V를 크기가 n×m(n≥m)인 Vandermonde 행렬이라고 하면, V는 다음 두 가지 속성을 만족한다.

(1) 행렬 V를 구성하는 n개 행들 중 임의의 m개 행들을 선택하여 m×m 부분 행렬을 구성할 경우 그 부분 행렬의 역행렬이 반드시 존재한다.

(2) 행렬 V에 첫 m개 행들로 구성된 m×m 부분 행렬이 항등 행렬(identity matrix)인 경우에도 위 속성 (1)을 만족한다.

제안기법에서는 IDA의 Dispersal() 연산 내부에서 사용되는 인코딩 행렬로써 이러한 Vandermonde 행렬을 사용하며, 그 결과 Dispersal() 연산을 통해 생성된 n개 인코딩 조각들 중 첫 m개는 원본 데이터 조각들과 동일하다. 따라서 첫 m개 조각들 중 일부만 주어지더라도 그 만큼의 원본 데이터를 얻게 되며, 또한 첫 m개 조각들 모두 손실 없이 전달될 경우 Recovery() 연산 수행 없이 원본 데이터를 얻게 된다. 이를 통해 결과적으로 제안기법의 데이터 복구 프로세스의 효율성이 향상된다. 본 논문의 이후 부분에서 IDA는 이러한 개선된 IDA를 의미하며, 개선된 IDA의 두 연산을 각각 Dispersal′()와 Recovery′()로 표기한다. 아울러 설명의 편의를 위해 Dispersal′() 결과 생성된 n개 조각들 중 첫 m개는 *원본 조각*이라고 명명하고, 나머지 n-m개는 *추가 중복 조각*이라고 명명한다.

지금부터는 2.2 절에 기술된 기본 해시트리에 개선된 IDA를 적용한 제안기법의 해시트리 형성 과정을 설명한다. Fig.2.는 제안기법을 통해 생성된 해시트리의 예와 그 생성 과정을 보여준다.

제안기법을 통해 생성된 해시트리에 리프 패킷조

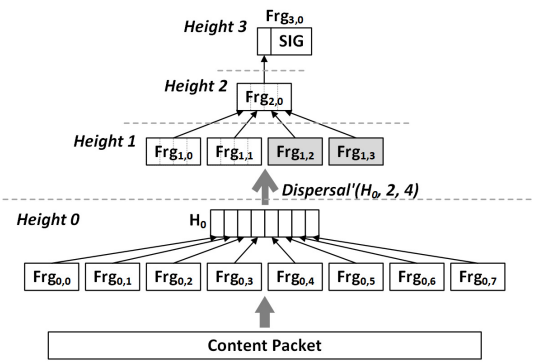

Fig. 2. Proposed hash tree to authenticate eight content fragments

각들을 높이 0, 그리고 루트 패킷조각을 높이 h라고 하면, 높이 1부터 h-2까지 각 높이에 위치한 패킷조각들에 대해서 IDA가 적용된다. n_i는 해시트리의 높이 i에 위치한 모든 패킷조각들의 수를 나타내고, m_i는 그 중 원본 패킷조각들만의 수를 나타낸다고 하자. 우선 높이 0에 리프 패킷조각들에 대해서는 IDA가 적용되지 않으며, 따라서 $m_0=n_0$ 이다. 해시트리의 높이 i에 위치한 n_i개 패킷조각 각각에 대해 암호 해시 함수를 적용하여 해시 값을 계산한다. 계산 결과 n_i개 해시 값들은 모두 함께 결합되며, 그것을 H_i라고 표기한다 (즉, $H_i = F(Frg_{i,0}) \| ... \| F(Frg_{i,n_i-1})$). 이렇게 생성된 H_i는 그 자체가 그대로 높이 i+1에 m_{i+1}개 원본 패킷조각들이 된다($m_{i+1} = \lceil |H_i|/f \rceil$). 다음 단계로 m_{i+1}개 원본 패킷조각들에 대해 Dispersal′(H_i, m_{i+1}, n_{i+1}) 연산을 수행하여 $n_{i+1}-m_{i+1}$개 추가 중복 패킷조각들 $Frg_{i+1,m_{i+1}} \sim Frg_{i+1,n_{i+1}-1}$을 생성함으로써 높이 i+1에 대한 생성 과정을 완료한다. 이때 $n_{i+1} = \min(\lceil m_{i+1}/(1-r) \rceil, d(m_{i+1}-1))$ 이며, n_{i+1} 값을 결정하기 위해 추가적으로 $d(m_{i+1}-1)$을 고려하는 이유는 해시트리가 높이 h-1에서 궁극적으로 하나의 노드로 수렴하도록 하기 위함이다.

예를 들면, Fig.2.에 해시트리에서 $H_0=F(Frg_{0,0})||...||F(Frg_{0,7})$ 이며, H_0 자체가 높이 1에 원본 패킷조각들인 $Frg_{1,0}$와 $Frg_{1,1}$이 된다. 그리고 Dispersal′(H_0, $2(=m_1)$, $4(=n_1)$) 연산을 통해 높이 1에 추가 중복 패킷조각 $Frg_{1,2}$와 $Frg_{1,3}$을 생성한다. 높이 1에 원본 패킷조각들 $Frg_{1,0}$과 $Frg_{1,1}$ 중 손실이 발생하더라고 $Frg_{1,0} \sim Frg_{1,3}$ 중 임의의 2개가 주어진다면 Recovery′()를 통해 손실된 원본 패킷조각을 복원할 수 있다. 즉, 최대 2개 패킷조각 손실까지는 재전송 없이 복원이 가능하다.

해시트리에 높이 0부터 높이 h-2까지 각각의 높이에 대해서 위에 기술된 과정을 반복 수행함으로써 패킷조각들을 생성하며, 결과적으로 해시트리는 높이 h-1에 하나의 패킷조각 $Frg_{h-1,0}$으로 수렴한다. 마지막으로 $Frg_{h-1,0}$의 해시 값 $F(Frg_{h-1,0})$와 그 해시 값에 대한 전자서명 SIG를 포함하는 루트 노드 $Frg_{h,0}$을 생성함으로써 전체 해시트리 생성 과정이 완료된다.

3.2 패킷조각 전송 및 신뢰성 검증

앞서 1절에서 논의한 바와 같이 DoS 공격에 대한 안전성을 위해서는 수신된 패킷조각의 검증 지연 상황을 최소화 하는 것이 중요하다. 제안기법에서 수신된 패킷조각에 대한 즉각적인 검증이 가능하려면, 수신된 패킷조각의 인증경로 상에 모든 조상 노드들(수신된 패킷조각보다 상위 높이에 위치한 노드들)에 대응되는 패킷조각들이 이미 수신된 상태여야 한다. 즉, 해시트리의 높이 i의 부모 노드가 높이 i-1의 자식 노드보다 항상 먼저 수신되어야 한다.

한편 CCN에서 동일한 콘텐츠 패킷을 구성하는 모든 패킷조각들은 같은 콘텐츠 이름을 달고 전송되며, 따라서 같은 라우팅 경로를 통해 전송된다[7]. 이처럼 같은 라우팅 경로를 통해 전송된다는 것은 이러한 패킷조각들이 전송된 순서와 같은 순서로 도착할 가능성을 높이게 된다. 이 같은 CCN의 특성을 고려하여 제안기법에서는 해시트리의 높이 i에 패킷조각들을 높이 i-1에 패킷조각들보다 먼저 전송하며, 동일한 높이 i에 패킷조각들에 대해서는 $Frg_{i,0}$부터 $Frg_{i,ni-1}$ 순서로 순차적으로 전송한다. 이러한 패킷조각 전송 방식은 CCN의 콘텐츠 이름 기반 라우팅 방식과 결합되어 수신된 패킷조각의 즉각 검증 가능 확률을 높인다. 이와 더불어서, 제안기법에서는 IDA를 적용함으로써 일부 패킷조각들이 전송 중 손실되더라도 수신된 패킷조각들의 즉각 검증 가능 확률을 높인다.

Fig.2.에 묘사된 바와 같이 제안기법의 해시트리의 높이 h에 루트 패킷조각과 높이 h-1에 그 자식 패킷조각 중 어느 하나라도 손실되면, 그 해시트리에 나머지 모든 패킷조각들은 수신되더라도 즉각적인 신

뢰성 검증이 불가능하다. 이러한 문제점을 개선하기 위해 제안기법에서는 이 두 패킷조각들 각각에 대해서는 $(\lceil 1/(1-r) \rceil - 1)$개의 패킷조각 사본을 추가로 전송한다. 이러한 추가적인 사본 전송을 통해 패킷조각 손실률 r까지는 재전송 없이 복구가 가능하다.

지금부터는 수신된 패킷조각을 검증하고, 그 검증 결과에 따라 네트워크 전송 경로 상에 다음 노드로 전달하는 절차를 설명한다. 본 설명을 위해서 다음 표기법을 사용한다. B는 수신된 패킷조각들을 저장하는 버퍼를 나타낸다. V는 B에 저장된 패킷조각들 중 신뢰성 검증을 통과한 정상 패킷조각들의 집합을 나타낸다($V \subseteq B$). V_i는 집합 V에 포함된 패킷조각들 중 해시트리의 높이 i에 속하는 패킷조각들만의 부분 집합을 나타낸다($V_i \subseteq V$). 마지막으로 W는 B에 저장된 패킷조각들 중 즉각 검증이 불가능하여 그 신뢰성이 아직 확인되지 않은 패킷조각들의 집합을 나타낸다($W \subseteq B$).

제안기법에서 패킷조각 $Frg_{i,j}$ 수신 시 우선 전자서명이 포함된 루트 패킷조각인지를 확인한다. 만약 루트 패킷조각인 경우 서명 검증을 통해 신뢰성을 확인하고, 검증이 통과된 경우에는 $Frg_{i,j}$를 집합 V에 추가하고 전송 경로 상에 다음 네트워크 노드로 전달한다. $Frg_{i,j}$가 루트 패킷조각이 아닌 경우에는 해시트리에 그 부모 패킷조각인 $Frg_{i+1,\lceil j/d \rceil}$이 이미 집합 V에 존재하는지를 확인한다. 만약 그렇다면 $Frg_{i,j}$의 해시 값을 계산하고, 계산된 해시 값과 이미 검증 통과된 부모 패킷조각에 포함된 해시 값을 비교한다($F'(Frg_{i,j}) = Frg_{i+1,\lceil j/d \rceil}$에 포함된 $F(Frg_{i,j})$ 인지를 확인). 만약 두 해시 값이 같다면 $Frg_{i,j}$가 검증 통과된 것이고, 따라서 $Frg_{i,j}$를 V에 추가하고 다음 네트워크 노드로 추가 전파한다. 그렇지 않고 두 해시 값이 다르다면, $Frg_{i,j}$ 검증이 실패한 것이고, 이럴 경우 $Frg_{i,j}$를 버퍼에 추가하거나 다음 네트워크 노드로 전달하지 않고 폐기한다.

만약 높이 i에 원본 패킷조각들인 $Frg_{i,0} \sim Frg_{i,m_i-1}$ 중 일부 패킷조각들이 손실된 상황에서 $|V_i| \geq m_i$ 이면, 손실된 원본 패킷조각을 복원하기 위해 $Recovery'\left(\left\{Frg_{i,j_k} | 0 \leq j_k < n_i, 0 \leq k < m_i\right\}, m_i, n_i\right)$를 수행한다. Recovery′()을 통해 복원된 패킷조각들은 집합 V에 추가된다. 추가 중복 패킷조각들 $Frg_{i,m_i} \sim Frg_{i,n_i-1}$ 중 손실된 패킷조각이 있을 경우에도 다음 네트워크 노드로 추가 전달을 위해 $Dispersal'(Frg_{i,0} \| ... \| Frg_{i,m_i-1}, m_i, n_i)$을 통해 재생성 한다.

Fig.2.에 해시트리 예를 가지고 위에 기술된 과정을 정리하면, 해시트리에 패킷조각들 중 $Frg_{2,0} \in V$인 상황에서 $Frg_{1,0}$이 수신되었다고 하자. 그러면 $Frg_{1,0}$의 해시 값을 계산하여 부모 노드인 $Frg_{2,0}$에 포함된 해시 값과 비교함으로써 수신된 $Frg_{1,0}$에 대한 즉각적인 검증이 가능하다. 뿐만 아니라 $Frg_{1,0}$과 $Frg_{1,2}$만 V_1에 포함되어 있고 $Frg_{1,1}$은 손실된 상황이라면 $Recovery'(\{Frg_{1,0}, Frg_{1,2}\}, 2, 4)$ 연산을 통해 $Frg_{1,1}$을 복원한다. 이렇게 되면 결과적으로 $Frg_{0,0} \sim Frg_{0,7}$ 패킷조각 수신 시 즉각적인 검증이 가능하다.

제안기법이 패킷조각 수신 시 높은 확률로 즉각 검증 가능하도록 하기 위한 다양한 방안들을 포함하고 있음에도 불구하고 일부 패킷조각들에 대해서는 수신 즉시 검증이 불가능한 경우가 발생할 수 있다. 이러한 즉각 검증 불가능한 패킷조각 수신 시 만약 FIGOA에서처럼 무조건 다음 네트워크 노드로 전파시킬 경우 공격자가 이를 악용하여 의도적으로 수신 즉시 검증이 불가능한 패킷조각들을 유입시켜 네트워크로 전파되도록 함으로써 불법적으로 네트워크 자원을 점유하여 정상적인 서비스에 지장을 초래할 수 있다. 반대로 즉각 검증 불가능한 패킷조각 수신 시 추가 전파 없이 무조건 버릴 경우 정상적인 패킷조각이 의도치 않게 버려져서 불필요한 재전송과 그로 인한 지연을 유발하게 된다.

따라서 즉각 검증 불가능한 패킷조각 수신 시 추가 전파 여부를 주어진 네트워크 상황에 맞게 유연하게 조정할 수 있는 방안이 필요하다. 예를 들어 수신된 전체 패킷조각들 중 검증 과정을 통과하지 못한 패킷조각들의 비율이 높은 상황이라면 현재 수신된 즉각 검증 불가능한 패킷조각을 악의적인 것으로 간주하고 추가 전파를 막는다. 반대로 수신된 대부분의 패킷조각들이 정상인 상황이라면 현재 수신된 즉각 검증 불가능한 것 또한 정상으로 간주하여 추가 전파되도록 하는 것이 합리적이다.

이를 위해 제안기법에서는 즉각 검증 불가능한 패킷조각 수신 시 최근에 수신되었던 다른 패킷조각들의 진위 여부에 대한 통계를 기반으로 상황에 맞는 유연한 결정을 내린다. 각 네트워크 노드는 일정 시

간 주기 동안 수신된 모든 패킷조각들을 그 진위 면에서 *정상*, *비정상*, 또는 *즉각 검증 불가* 세 가지 범주 중 하나로 분류하고 개수를 집계한다. 본 논문에서는 현재 시간 주기 동안 수신된 정상, 비정상, 즉각 검증 불가 패킷조각들의 개수 각각을 x, y, z로 표기한다.

네트워크 노드가 즉각 검증이 불가능한 패킷조각을 수신하면 x/(x+y+z) 확률로는 수신된 패킷조각을 정상으로 가정하고, 버퍼링을 통해 집합 W에 패킷조각을 추가하고 다음 네트워크 노드로 추가 전파한다(옵션1). 반대로 y/(x+y+z) 확률로는 수신된 패킷조각을 비정상으로 가정하고, 버퍼에 추가하거나 추가 전달 없이 폐기한다(옵션2). 마지막으로 z/(x+y+z) 확률로는 비정상 패킷조각이 네트워크로 전파되는 잠재적인 위험을 피하기 위해 다음 네트워크 노드로 추가 전달은 하지 않고, 버퍼에 추가할지 여부는 랜덤하게 결정한다(옵션3). 만약 x, y, z 값이 모두 0인 초기 상황에서는 위 세 가지 옵션 중 하나를 랜덤하게 취하여 수신된 패킷조각을 처리한다. 이러한 방식을 통해 대부분의 패킷조각들이 정상인 네트워크 환경에서는 즉각 검증 불가능한 패킷조각일지라도 폐기하기 보다는 다음 네트워크 노드로 전달함으로써 빠른 전파를 가능하게 한다. 반대로 대부분의 패킷조각들이 비정상인 악의적인 공격 상황에서는 즉각 검증 불가능한 패킷조각 또한 추가 전파 없이 폐기함으로써 공격을 효과적으로 억제한다.

제안기법에서는 집합 W에 포함된 패킷조각들이 궁극적으로 검증되도록 하기 위해 새로운 패킷조각이 집합 V에 추가될 때마다 그 자식 패킷조각이 집합 W에 존재하는지를 확인한다. 만약 존재할 경우에는 그 자식 패킷조각에 대한 검증 과정을 수행하며, 검증 성공일 경우 그 패킷조각은 집합 V로 옮겨지고, 그렇지 않은 경우에는 폐기된다. 뿐만 아니라 검증 결과에 맞춰 z 값은 1만큼 감소시키고, x 또는 y 값은 1만큼 증가시킨다.

3.3 패킷조각 크기의 가변적 조정

CCN에서는 효율적인 콘텐츠 전송을 위해서 라우터들이 콘텐츠 캐싱(caching) 기능을 수행한다. 그리고 이러한 특징 때문에 콘텐츠 생성자에 의한 해시트리 구성 및 전자서명을 통해 인증된 패킷조각들이 중간 라우터에 캐싱 되었다가 다양한 전송 경로를 통해 전송될 수 있다. 이때 만약 전송하고자 하는 새로운 라우팅 경로의 MTU 값에 맞는 새로운 패킷조각의 크기(f_{new})가 콘텐츠 생성자에서 해시트리 구성 당시 설정된 패킷조각의 크기(f_{orig})보다 더 작을 경우 f_{new} 크기의 더 작은 패킷조각들로 나누어져서 전송되어야 한다. 하지만 중간 라우터의 경우 콘텐츠 생성자의 서명키를 모르기 때문에 새로운 패킷조각 크기에 맞게 해시트리를 재구성하고 그 결과 루트 노드를 재서명 하는 것이 불가능하다. 이러한 요구사항들을 만족시키기 위해 제안기법에서는 기존 해시트리에 패킷조각을 f_{new} 크기의 여러 개의 더 작은 패킷조각들로 나누고, 그들 간을 FIGOA에서처럼 암호 해시 함수의 내부 상태 값들을 이용해서 일방향 해시 체인으로 연결한다[2]. 이를 통해 결과적으로 해시트리의 재구성 및 재서명 절차 없이 f_{orig} 크기의 기존 패킷조각을 f_{new} 크기의 여러 개의 더 작은 패킷조각들로 나눌 수 있으면서 동시에 패킷조각 단위 인증 속성이 유지된다.

IV. 성능 분석

본 절에서는 효율성과 안전성 측면에서 제안기법을 분석하고, FIGOA에 대한 분석 결과와 비교한다. 본 절의 설명을 위해 3절에서 사용된 동일한 표기법들을 사용한다.

첫 번째로, 아래 정리 1에서는 주어진 콘텐츠 패킷에 대해 제안기법의 해시트리를 통해 생성되는 패킷조각들의 총 수를 분석한다.

정리 1. 주어진 콘텐츠 패킷 CP에 대한 제안기법의 해시트리에 포함된 패킷조각들의 총 수 N은

$$\left\lceil \frac{|CP|}{f} \right\rceil + \sum_{i=1}^{h-2} \min\left(\left\lceil \frac{m_i}{1-r} \right\rceil, d(m_i-1) \right) + \left\lceil \frac{2}{1-r} \right\rceil$$

이다.

증명. 제안기법 해시트리의 높이 0에 대해 $m_0 = n_0 = \lceil |CP|/f \rceil$ 이다. 다음으로 해시트리의 높이 1부터 (h-2)까지 각 높이 i에 대해서 $m_i = \lceil (n_i - 1)/d \rceil$ 이고 $n_i = \min(\lceil m_i/(1-r) \rceil, d(m_i-1))$ 이다. 마지막으로, 해시트리의 높이 (h-1)과 h에 대해서, $m_h = m_{h-1} = 1$ 이고 $n_h = n_{h-1} = \lceil 1/(1-r) \rceil$

이다. 결과적으로, 제안기법 해시트리의 높이 0부터 h까지 모든 패킷조각들의 수를 합하면

$$\sum_{i=0}^{h} n_i = \left\lceil \frac{|CP|}{f} \right\rceil + \left\lceil \frac{2}{1-r} \right\rceil + \sum_{i=1}^{h-2} \min\left(\left\lceil \frac{m_i}{1-r} \right\rceil, d(m_i-1) \right)$$

이다. □

제안기법에서 해시트리와 IDA 사용으로 인해 FIGOA 대비 어느 정도의 추가적인 패킷조각들이 필요한지를 보기 위해 아래 정리 2에서는 동일한 콘텐츠 패킷에 대해서 제안기법과 FIGOA 각각에 의해 생성되는 패킷조각들의 총 개수 간 차이를 분석한다.

정리 2. 주어진 콘텐츠 패킷 *CP*에 대해서 FIGOA 대비 제안기법에서 추가적으로 필요한 패킷조각들의 수는

$$\left\lceil \frac{|CP|}{f} \right\rceil + \sum_{i=1}^{h-2} \min\left(\left\lceil \frac{m_i}{1-r} \right\rceil, d(m_i-1) \right) + \left\lceil \frac{2}{1-r} \right\rceil - \left\lceil \frac{\lceil |CP|/\beta \rceil}{\lfloor (f-|F()|)/\beta \rfloor} \right\rceil - 1$$

이다. (β는 암호 해시 함수에서 기본 데이터 처리 단위인 블록(block)의 크기(바이트)를 나타낸다.)

증명. FIGOA에서 각 패킷조각에는 주어진 *CP*의 데이터가 블록 단위로 포함된다. 여기서 블록은 암호 해시 함수에서 주어진 데이터에 대한 해시 값 계산 시 처리의 기본 단위가 되는 데이터 조각을 의미하며, SHA-256의 경우 32 바이트 블록 단위로 주어진 데이터를 처리한다. 여기서 β는 블록의 크기를 나타낸다고 하자. 주어진 *CP*를 블록 단위로 나누었을 때 총 블록 수는 $\lceil |CP|/\beta \rceil$ 이다. FIGOA에서는 패킷조각들 간에 해시체인을 형성하기 위해 각 패킷조각에 기본적으로 한 개의 해시 값이 포함된다. 따라서 각 패킷조각에 저장 가능한 블록의 수는 $\lfloor (f-|F()|)/\beta \rfloor$ 이다. 그리고 FIGOA에서는 해시체인 상의 마지막 해시 값과 그것의 전자서명을 포함하는 패킷조각이 추가로 한 개 생성된다. 따라서 FIGOA에서 주어진 *CP*에 대해 생성되는 패킷조각들의 총 수는 $\left\lceil \frac{\lceil |CP|/\beta \rceil}{\lfloor (f-|F()|)/\beta \rfloor} \right\rceil + 1$ 이다. 결과적으로 주어진 *CP*에 대해서 FIGOA 대비 제안기법에서 추가적으로 필요한 패킷조각들의 수는

$$\left\lceil \frac{|CP|}{f} \right\rceil + \sum_{i=1}^{h-2} \min\left(\left\lceil \frac{m_i}{1-r} \right\rceil, d(m_i-1) \right) + \left\lceil \frac{2}{1-r} \right\rceil - \left\lceil \frac{\lceil |CP|/\beta \rceil}{\lfloor (f-|F()|)/\beta \rfloor} \right\rceil - 1$$

이다. □

앞서 언급한데로 수신된 패킷조각의 즉각 검증 가능 여부는 DoS 공격에 대한 안전성을 위해 중요하다. 이에 아래 정리 3에서는 정상적인 전송 상황에서 제안기법 해시트리에 각 패킷조각에 대해 수신 즉시 검증 가능할 확률을 분석한다. 아래 분석에서 각 패킷조각이 에러나 손실 없이 정상적으로 수신될 확률은 (1-p)라고 가정한다.

정리 3. 제안기법 해시트리에 임의의 패킷조각 $Frg_{i,j}$ 수신 시 수신자가 그 패킷조각을 즉각 검증 가능할 확률 f(i)는 $0 \le i < h$ 일 때 $\prod_{u=i+1}^{h} \left\{ 1 - p \sum_{v=0}^{m_u-1} \binom{n_u-1}{v} (1-p)^v p^{n_u-1-v} \right\}$ 이고, f(h)=1 이다.

증명. 수신된 $Frg_{i,j}$가 즉각 검증 가능하려면 $Frg_{i,j}$의 인증경로 상에 각 높이 $u((i+1) \le u < h)$에 대해서 다음 두 가지 조건들 중 적어도 하나가 만족되어야 한다.

- $Frg_{i,j}$의 인증경로 상에 높이 u에 위치한 패킷조각이 정상적으로 수신되었다.
- 위 첫 번째 조건이 만족되지 않은 상황에서 높이 u에 나머지 n_u-1개 패킷조각들 중 m_u개 이상의 패킷조각들이 정상적으로 수신되었다.

높이 u에 대해서 위 두 가지 조건들 중 적어도 하나가 만족될 확률은 $1 - p \sum_{v=0}^{m_u-1} \binom{n_u-1}{v} (1-p)^v p^{n_u-1-v}$ 이다. 따라서 $Frg_{i,j}$가 수신 즉시 검증 가능할 확률 f(i)는

$$\begin{cases} \prod_{u=i+1}^{h} \left\{ 1 - p \sum_{v=0}^{m_u-1} \binom{n_u-1}{v} (1-p)^v p^{n_u-1-v} \right\}, & 0 \le i < h \\ 1, & i = h \end{cases}$$

이다. □

정리 4. 제안기법의 해시트리에 포함된 모든 패킷조각들에 대한 즉각 검증 가능 확률의 기대 값은 $\sum_{i=0}^{h} f(i)\frac{n_i}{N}$ 이다($N=\sum_{u=0}^{h} n_u$).

증명. X는 제안기법 해시트리에 각 패킷조각이 수신 즉시 검증 가능할 확률을 나타내는 확률 변수(random variable)를 나타낸다고 하자. 그러면 확률 변수 X가 가질 수 있는 모든 가능한 값들의 집합은 $\{f(i)|0 \le i \le h\}$이다. 그리고 변수 X의 값이 f(i)일 확률 Pr(X=f(i))은 n_i/N 이다($N=\sum_{u=0}^{h} n_u$). 따라서 해시트리에 모든 패킷조각들에 대한 즉각 검증 가능 확률의 기대 값은 $\sum_{i=0}^{h} f(i)\frac{n_i}{N}$ 이다. □

본 절의 분석 결과 유도된 식들을 기반으로 동일한 콘텐츠 패킷에 대해 제안 기법과 FIGOA의 성능을 비교하기 위한 실험을 수행했다. Fig.3.과 Fig.4.는 다양한 크기의 콘텐츠 패킷들에 대해 제안 기법과 FIGOA에서 필요한 패킷조각 수와 즉각 검증 가능 확률을 비교한다. 두 그래프의 x 축은 콘텐츠 패킷 크기를 나타내며, Fig.3.의 y 축은 필요한 패킷조각 수를, Fig.4.의 y 축은 해시트리에 각 패킷조각에 대해 기대되는 즉각 검증 가능 확률을 나타낸다.

다음으로 Fig.5.와 Fig.6.은 다양한 패킷조각 크기에 대해 제안 기법과 FIGOA의 패킷조각 수와 즉각

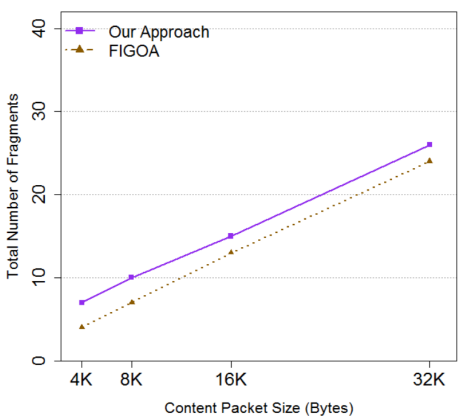

Fig. 3. Total number of fragments in our approach and FIGOA for different sizes of content packets (fragment size fixed to 1500 bytes)

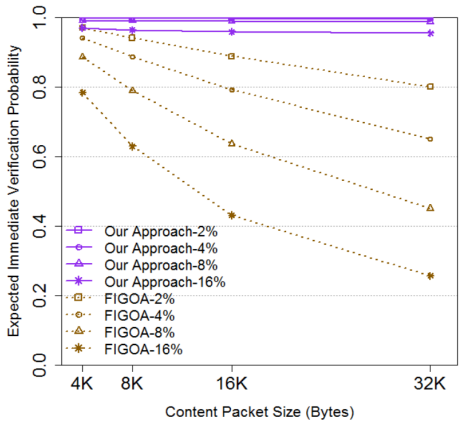

Fig. 4. Expected immediate verification probability in our approach and FIGOA for different sizes of content packets (fragment size fixed to 1500 bytes)

검증 가능 확률을 보여준다. 또한 패킷조각 에러/손실 확률 p가 즉각 검증 가능 확률에 미치는 영향을 보기 위해 다음 4가지 손실 확률에 대해서 실험을 수행했다: p=0.02(2%),0.04(4%),0.08(8%),0.16(16%). 해시 값의 크기는 32 바이트로 가정하였으며, IDA의 중복률은 0.2로 설정했다. 실험 결과를 요약하면, 제안 기법은 모든 실험 케이스들에 대해서 98.2% 이상의 높은 즉각 검증 가능 확률을 보였다. 그리고 제안기법이 FIGOA 보다 평균적으로 52% 더 높은 즉각 검증 가능 확률을 보였으며, 필요한 패킷조각 수 면에서는 평균 14% 증가를 보였다.

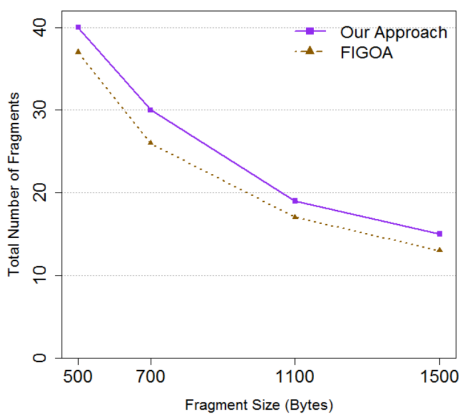

Fig. 5. Total number of fragments in our approach and FIGOA for different fragment sizes (content packet size fixed to 16K bytes)

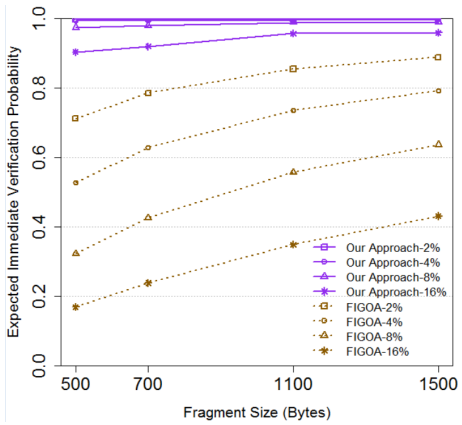

Fig. 6. Expected immediate verification probability in our approach and FIGOA for different fragment sizes (content packet size fixed to 16K bytes)

Fig.7.과 Fig.8.은 정리 2의 분석 결과에 대한 그래프를 보여준다. Fig.7.에서 보는 바와 같이 제안기법은 다양한 콘텐츠 패킷 크기와 IDA 중복률 값(r=0.1~0.5)에 대해서 FIGOA 대비 2~3개의 패킷조각 수 증가를 보인다. Fig.8.에 다양한 패킷 조각 크기에 대해서는 r≤0.3 일 때는 제안기법이 2~4개의 패킷조각 수 증가를 보이며, r=0.5 일 때 2~5개의 패킷조각 수 증가를 보인다.(다양한 파라미터 값들 하에서 제안기법과 FIGOA에 의해 생성

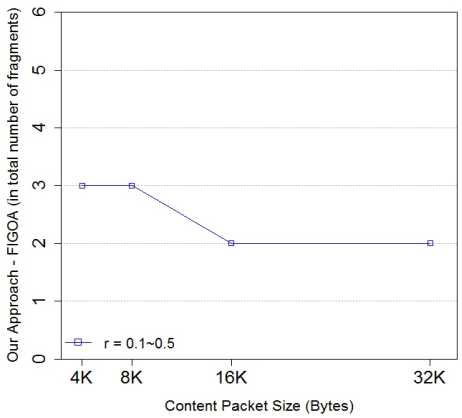

Fig. 7. Difference in the total number of fragments between our approach and FIGOA for different content packet sizes and IDA redundancy rates (fragment size fixed to 1500 bytes)

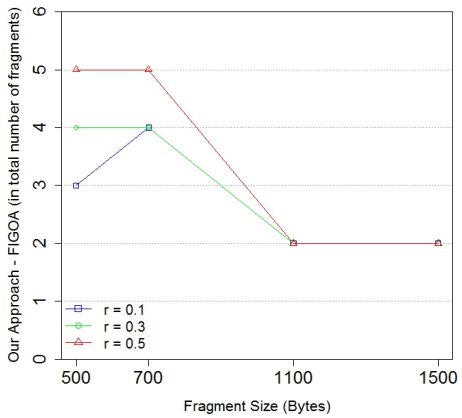

Fig. 8. Difference in the total number of packets between our approach and FIGOA for different fragment sizes and IDA redundancy rates (content packet size fixed to 16K bytes)

되는 총 패킷조각 수에 관해서는 Fig.3.과 Fig.5.를 참고하기 바란다.)

V. 결 론

본 논문에서는 CCN 환경에서 안전한 콘텐츠 전송을 위한 패킷조각 단위 인증 기술을 제안했다. 제안기법은 패킷조각들에 대한 불법적인 위변조를 방지하고, 패킷조각 수신 시 높은 즉각 검증 가능 확률을 제공함으로써 검증 지연을 악용한 DoS 공격을 방지한다. 뿐만 아니라 제안 기법에서는 아직 신뢰성이 확인되지 않은 패킷조각들의 추가 전파 확률을 가변적으로 조정함으로써 주어진 네트워크 상황에 맞는 유연한 대처가 가능하다. 본 논문의 성능 분석 결과는 제안 기법이 약간의 부하 증가만으로 기존 기술보다 훨씬 더 높은 안전성을 제공함을 보여준다.

References

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," Proceedings of ACM International Conference on Emerging Networking Experiments and Technologies, pp. 1-12, Dec. 2009.

[2] C. Ghali, A. Narayanan, D. Oran, G.

Tsudik, and C. A. Wood, "Secure fragmentation for content-centric networks," Proceedings of IEEE International Symposium on Network Computing and Applications, pp. 47-56, Sept. 2015.
〔3〕 Michael O. Rabin, "Efficient dispersal of information for security, load balancing and fault tolerance," Journal of the Association for Computing Machinery, vol. 36, no. 2, pp. 335-348, Apr. 1989.
〔4〕 J. Deng, R. Han, and S. Mishra, "Secure code distribution in dynamically programmable wireless sensor networks," Proceedings of International Conference on Information Processing in Sensor Networks, pp. 292-300, Apr. 2006.
〔5〕 A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient and secure source authentication for multicast," Network and Distributed System Security Symposium, pp. 35-46, Feb. 2001.
〔6〕 L. Rizzo, "Effective erasure codes for reliable computer communication protocols," ACM SIGCOMM Computer Communication Review, vol. 27, no. 2, pp. 24 - 36, Apr. 1997.
〔7〕 L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, KC Claffy, D. Krioukov, D. Massey, C. Papadopoulos, T. Abdelzaher, L. Wang, P. Crowley, and E. Yeh, "Named data networking (NDN) project," NDN-0001, Xerox Palo Alto Research Center, Oct. 2010.

〈저자소개〉

현 상 원 (Sangwon Hyun) 정회원
2002년 2월: 성균대학교 전기전자컴퓨터공학부 졸업
2004년 2월: 서울대학교 컴퓨터공학과 석사
2011년 12월: 노스캐롤라이나주립대학교 전산학과 박사
2016년 3월~현재: 성균관대학교 소프트웨어대학
〈관심분야〉 네트워크 및 시스템 보안