정 보 보 호 학 회 지
제26권 제6호, 2016. 12

ICN Naming 기법에 대한 연구 동향

윤 덕 상*, 김 대 엽**

요 약

기존 인터넷이 원격지 호스트들 사이의 안정적인 연결에 중점을 두고 개발되었기 때문에 대용량 콘텐츠 전송을 포함해서 다양한 종류의 서비스의 요구사항을 충족시키지 못하고 있다. 이와 같은 문제를 해결하기 위하여 미래 인터넷 아키텍처 및 기술이 제안되었다. 미래 인터넷 아키텍처 중 하나인 ICN은 네트워크를 통해 전송되는 콘텐츠의 캐시를 탐색하고 효율적으로 전송하는 기술에 중점을 두어 개발된 새로운 패킷 전송 모델이다. 특히, ICN은 전송 효율을 높이기 위한 방법으로 콘텐츠 배포지의 다변화를 추구하여, 멀티미디어 프락시 시스템 또는 네트워크 노드에 콘텐츠를 임시 저장한다. 이와 같이 임시 저장된 콘텐츠 캐시를 이용하여 사용자의 요청 메시지를 콘텐츠 공급자 외에도 다양한 호스트/노드들이 응답할 수 있도록 개발되었다. 이와 같은 패킷 전송 모델을 구현하기 위하여 호스트 식별자를 패킷 라우팅 정보로 활용하던 기존 인터넷 주소 체계와는 다른 콘텐츠 식별 정보를 정의하고, 이 식별 정보를 라우팅 정보로 활용한다. 본 논문에서는 ICN의 콘텐츠 식별 정보 체계와 이를 활용한 라우팅 방안들을 살펴보고 그 특징들을 비교 분석한다.

Ⅰ. 서 론

인터넷 아키텍처는 원격 호스트들 간의 안전한 연결을 주목적으로 1960년대 말에 처음 제안되기 시작한 후, HTTP, FTP와 같은 클라이언트-서버 기반의 다양한 서비스 및 어플리케이션에 매우 적합한 통신 아키텍처로 평가되어져 왔다[1]. 그러나 인터넷의 호스트 중심의 전송 모델은 이동 기기를 이용 및 대용량 콘텐츠 전송을 중심으로 빠르게 변화되고 있는 현대의 다양한 서비스들의 요구사항들을 충분히 충족시키지 못하고 있다. 특히, 네트워크 병목현상으로 인한 성능 저하, 취약한 보안 구조로 인한 사고 증가, 기기의 이동성으로 인한 비효율성 증가와 같은 다양한 문제들에 대한 해결책을 적절히 제공하지 못함으로 말미암아 IoT와 같은 다양한 서비스 개발 및 보급에 걸림돌이 되는 현상까지 발생하고 있다. 이와 같은 문제들을 해결하고 서비스들을 보다 효율적으로 구현하기 위하여 호스트 중심의 통신 모델은 지난 몇 년간 점차 콘텐츠 중심의 통신 모델로 변화하고 있다[2,3].

P2P(Peer-to-Peer Network Application)와 CDN (Content Distribution Network)은 콘텐츠 중심의 통신 모델의 대표적인 서비스 예라 할 수 있다. P2P의 경우, 콘텐츠를 제공할 수 있는 콘텐츠 배포지(Content Source)를 다변화함으로써 콘텐츠 공급자(Original Content Source/Provider)로 집중되는 콘텐츠 요청에 대한 분산 처리가 가능케 했으며, 특히 콘텐츠 공급자의 네트워크 연결 상태와 상관없이 해당 콘텐츠를 획득할 수 있다는 추가적인 장점도 갖고 있다. CDN은 콘텐츠의 복사본을 저장/배포하는 대표적인 서비스이다. 호스트 중심의 통신 모델인 인터넷은 콘텐츠의 복사본의 위치 정보를 사용자에게 직접 제공할 수 없다. DNS (Domain Name System)와 같은 Name Resolution System을 이용해도 콘텐츠의 복사본이 저장된 호스트의 위치 정보를 사용자가 획득할 수 없다. CDN에서는 이와 같은 문제의 해결 방안을 제공하고, 사용자의 콘텐츠 요청 패킷을 관련 복사본이 저장되어 있는 프락시 서버로 포워딩되도록 구현했다. 그러나 P2P/CDN은 기본적으로 IP 오버레이 기술을 기반으로 구현된 서비스/어플리케이션 기술이기 때문에 기반 네트워크의 위상에 대한 정보를 활용하여 성능을 최적화시킬 수 없다는 한계를 갖고 있다. 또한, CDN의 경우는 관련 서비스를 제공하는 서비스 업자와 통신 업자의 협업이 필요하기 때문에 일반 사용자들이

본 연구는 한국연구재단 기초연구사업과제(NRF-2013R1A1A2008389) 지원으로 수행되었습니다.
* KT DS (yoondark@naver.com)
** 수원대학교 정보보호학과 (daeyoub69@suwon.ac.kr)

직접 해당 서비스를 구현할 수 없다.

ICN (Information Centric Networking)은 콘텐츠 중심의 통신 모델을 기반 네트워크 계층에서 구현하는 새로운 네트워크 아키텍처라 할 수 있다. 콘텐츠 중심 통신 모델을 구현하기 위하여 ICN은 호스트 위치 정보와 무관하게 운영/관리되는 새로운 네트워크 주소 체계(Naming)와 이 네트워크 주소 체계를 이용한 패킷 전송 기술을 제안하고 있으며, 네트워크 효율성을 높이기 위한 네트워크 캐시 운영 기술과 콘텐츠 인증 기능 등을 함께 제안하고 있다 [4-6]. ICN 이외에도 FP7을 중심으로 다양한 미래 인터넷 프로젝트들이 진행되었다 [7-12].

본 논문에서는 ICN 기술들의 Naming 기법들과 패킷 포워딩을 위한 라우팅 기술들 소개하고, 그 특징들을 분석한다.

Ⅱ. ICN Project

표 1은 본 논문에서 분석하려고 하는 주요 ICN 프로젝트들을 나타낸다.

〔표 1〕 미래 인터넷 프로젝트

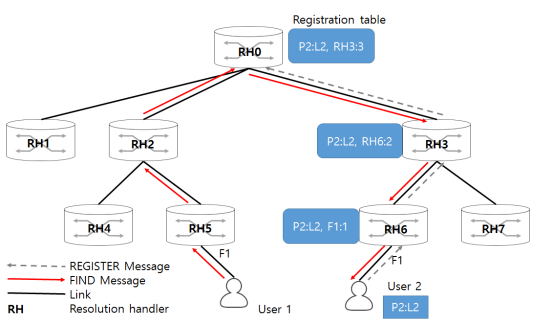
Project	Year
Data Oriented Network Architecture (DONA)	2007
Network of Information (NetInf)	2009
Named Data Networking (NDN)	2009
Publish Subscribe Internet Technology (PUSRSUIT)	2010

2.1. Data Oriented Network Architecture

2007년에 발표된 Data Oriented Network Architecture (DONA)는 인터넷의 네트워크 주소 체계를 완전히 새롭게 제안하고 있다 [13]. DONA에서 제안하는 네트워크 주소체계의 특징은 비계층적 콘텐츠 식별 정보 구조 (Flat Naming)와 콘텐츠 식별 정보를 이용한 콘텐츠 자가 인증 구조(Self-certifying)로 요약할 수 있다. DONA의 네트워크 주소체계의 구조는 P:L 형태를 취한다. 여기서 P는 콘텐츠 공급자의 공개키의 해쉬값을 의미하며, L은 해당 공급자에게 할당된 Label 정보를 의미한다. 콘텐츠 공급자는 L을 생성할 때, 다른 공급자와 명확히 구분될 수 있도록 유일성을 확보/유지해야 한다. 즉, L의 값은 연결된 네트워크 도메인들 사이에서 유일한 값으로 유지되어야 한다. 또한, 콘텐츠의 meta-data는 해당 콘텐츠 공급자의 공개키와 함께 전자서명 값을 포함한다. 이와 같은 정보들을 이용하여 사용자는 자신이 수신한 콘텐츠의 공급자와 콘텐츠의 무결성을 검증할 수 있다.

DONA의 Naming 구조는 네트워크 캐시 구현에 매우 유용한 기능을 제공한다. 이론적으로 네트워크에 연결된 호스트들 중에서 검증된 콘텐츠를 갖고 있는 호스트들은 콘텐츠의 검증된 콘텐츠 배포자로 간주될 수 있다. 그러나 기존 인터넷에서는 콘텐츠 공급자 이외에 해당 콘텐츠를 제공하는 호스트의 신뢰성을 검증하기 어렵다. CDN의 경우는 신뢰성이 검증된 서비스 제공자에 의해 운영/관리되는 프락시 시스템들을 이용해서 이러한 문제들을 해결하고 있다. 그러나 DONA는 콘텐츠 자가 인증이 가능한 Naming 기법을 사용하기 때문에 원출처가 오프라인 상태라 할지라도 수신된 콘텐츠의 무결성과 원출처의 인증이 가능하다. 그러므로 콘텐츠 캐시를 활용할 때 보다 안전하게 구현할 수 있다.

DONA의 Naming 기법을 활용하여 콘텐츠 요청 패킷을 포워딩하기 위해서는 계층적 네트워크 도메인마다 Resolution Handler (RH)를 관리/운영해야 한다. DONA는 FIND(P:L)과 REGISTER(P:L)의 두 종류 패킷을 정의하여, RH의 정보를 갱신/관리한다. FIND(P:L)은 P:L을 식별 정보로 갖는 콘텐츠의 호스트 위치를 계층적으로 구성된 RH들에서 찾기 위해 사용되고, REGISTER(P:L)은 FIND(P:L)을 계층적으로 구성된 RH들 사이에서 효율적으로 라우팅하기 위해 RH들의 정보를 설정/갱신하기 위해 사용된다. 그림 1은 계층적인 RH 기반으로 콘텐



〔그림 1〕 DONA RH 계층 구조 운영 절차

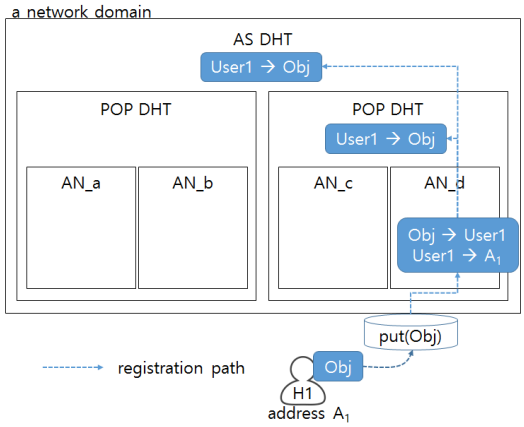
츠 (P2:L2)을 등록하고, 해당 콘텐츠를 찾기 위해 FIND(P2:L2)와 REGISTER(P2:L2)을 활용한 패킷 포워딩 방식을 설명한다. RH의 라우팅 테이블은 <P:L, next hop RH, distance>로 구성된 정보를 운영한다. 각각의 RH는 수신된 REGISTER(P:L)에 대한 정보를 기존에 갖고 있지 않았거나 이전 정보보다 distance가 더 가까운 경우에 상위 계층 RH로 포워딩한다. REGISTER(P2:L2)은 User2 → RH6 → RH3 → RH0 순으로 포워딩 된다. 각각의 RH는 수신된 REGISTER(P2:L2)을 기반으로 자신의 라우팅 테이블을 갱신한다. User1이 콘텐츠(P2:L2)을 찾기 위해 FIND(P2:L2)을 생성/전송하면, 해당 FIND (P2:L2)에 부합되는 정보가 라우팅 테이블 있을 경우, 해당 정보에 따라 FIND(P2:L2)을 포워딩하고, 부합하는 정보가 없는 경우에는 상위 RH로 포워딩한다.

User2가 FIND(P2:L2)을 수신하면, 콘텐츠(P2:L2)는 기존의 호스트 중심 네트워킹 기술을 이용하여 User1에게 전송된다.

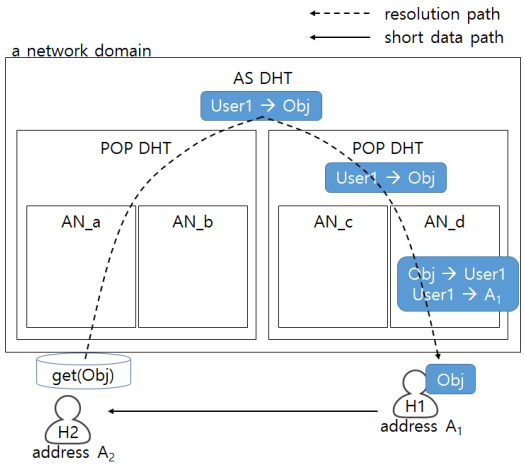
2.2. Network Of Information

Network of Information (NetInf)는 EU FP7 프로젝트인 4WARD/SAIL에서 제안되었다 [14]. NetInf 역시 DONA와 유사하게 P:L 형태의 비계층적 콘텐츠 식별 정보 구조를 이용하며, 콘텐츠 자가 인증이 가능하다. 단, P는 콘텐츠 공급자가 생성한 공개키의 해쉬값이고, L은 콘텐츠 공급자에 의해 생성된 콘텐츠의 Label이다. 특히, L은 콘텐츠 자체를 해쉬한 값을 정적으로 사용할 수도 있고, 고정된 ID 값을 사용할 수도 있다. 후자의 경우에는 콘텐츠의 무결성 검증을 위하여 콘텐츠의 meta-data에 전자서명을 포함시킬 것을 권고한다. NetInf는 콘텐츠 마다 공개키/서명키 쌍을 생성/운영한다. 그러므로 콘텐츠 공급자는 복수 개의 공개키/서명키 쌍을 생성/관리할 수 있다. 이 경우, 콘텐츠 공급자의 식별 및 인증을 위해서 meta-data에 공개키 체인 정보를 포함시키도록 권고한다. 이와 같은 권고 사항은 원출처의 익명성을 보장할 수 있다는 추가적인 장점이 있다.

콘텐츠 요청 메시지를 포워딩하기 위해서 다중 DHT-based Name Resolution Service (MDHT)를 활용한다. 그림 2에서 설명하는 것과 같이 계층적으로 Access Node (AN), Point of Presence (POP) 그리고 Autonomous System (AS)에서 독자적으로 DHT를 운



(a) Content Registration Process



(b) Data Retrieve Process

〔그림 2〕 NetInf DHT 계층 구조 운영 절차

영한다. 콘텐츠 (Obj)를 등록하는 절차는 다음과 같다: 호스트 H1이 콘텐츠 Obj를 3개의 계층 AN, POP, AS에 등록한다. 이 때, AS에는 2개의 정보가 등록된다. 첫 번째 정보는 Obj가 호스트 H1에 의해 생성/배포 된다는 정보이고, 두 번째 정보는 호스트 H1의 식별자/위치 정보를 제공한다. 상위 계층인 POP와 AN의 DHT에는 콘텐츠 Obj가 호스트 H1에 의해 생성/배포 된다는 정보만 기록/관리된다.

호스트 H2가 콘텐츠 Obj를 찾기 위해서 우선 로컬 AS와 POP에 순차적으로 요청하고, 부합되는 정보를 찾지 못하는 경우에 로컬 AN에 요청한다. 로컬 AN에서도 정보를 찾지 못하면 Resolution Exchange System

(REX)에 정보를 요청한다. REX는 AN들의 정보를 글로벌하게 관리/운영하는 최상위 계층 시스템이다.

호스트 H1이 H2의 콘텐츠 요청 패킷을 수신하면, 콘텐츠(Obj)는 기존의 호스트 중심 네트워킹 기술을 이용하여 H2에게 전송된다.

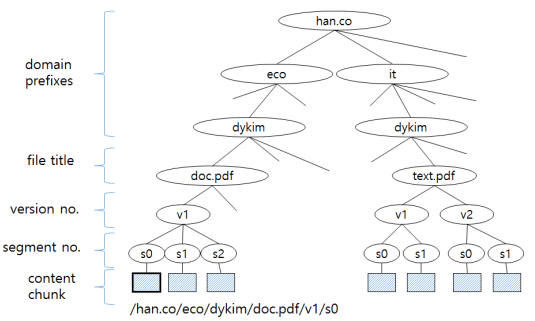
2.3. Named Data Networking

Named Data Networking (NDN)은 NSF FIA 프로젝트일 일환으로 제안되었다. NDN은 Parc에서 제안된 콘텐츠 중심 네트워킹 아키텍처 (Content Centric Networking Architecture)를 기반으로 제안되었으며 계층적이고 가독성을 갖는 이름 구조를 채택하고 있다 [15-17].

그림 3은 NDN은 계층적인 이름 구조를 나타낸다. 각각의 계층을 구성하는 이름 요소들의 길이와 내용은 제한이 없으며, NDN은 계층화된 구조만을 제안함으로써 다양한 서비스/어플리케이션에서 독자적으로 이름을 구성할 수 있도록 하였다. 단, NDN은 콘텐츠를 단편화한 후, 각각의 단편화된 콘텐츠 Segment를 개별 콘텐츠 오브젝트로 간주하고 처리한다. 이렇게 단편화된 콘텐츠 Segment를 구분하기 위하여 계층화된 이름 구조에 세그먼트 번호를 포함시키고, 콘텐츠 수정등과 같은 경우를 고려하여 버전 정보를 포함시키고 있다. 그림 3의 예와 같이, 콘텐츠 식별정보는 콘텐츠 공급자에 대한 식별 정보인 계층적 구조의 Domain Prefixes와 콘텐츠 식별 정보인 File Title, Version No., Segment No. 등으로 구성된다. 이와 같이 구성된 콘텐츠 식별정보는 네트워크 내에서 유일하게 정의되어야 한다.

NDN의 특징은 계층화된 콘텐츠 식별 정보를 기반으로 패킷을 포워딩하기 때문에 별도의 Resolution System을 도입할 필요가 없다. 그림 4는 NDN의 패킷 포워딩 절차를 나타낸다. NDN의 전송 패킷은 요청 메시지 (Interest) 전송 및 이에 대한 응답 메시지 (Data)로 구분된다. Interest를 요청하는 콘텐츠의 계층적 이름을 포함하며, 중간 노드들은 이와 같은 계층적 이름을 참조하여 Interest를 포워딩한다. 호스트 식별자를 사용하지 않기 때문에 Data는 Interest가 전송된 경로를 역으로 따라서 사용자에게 전송된다. 이와 같은 특징을 구현하기 위하여 NDN은 다음과 같은 몇 가지 추가적인 요소들을 사용 한다:

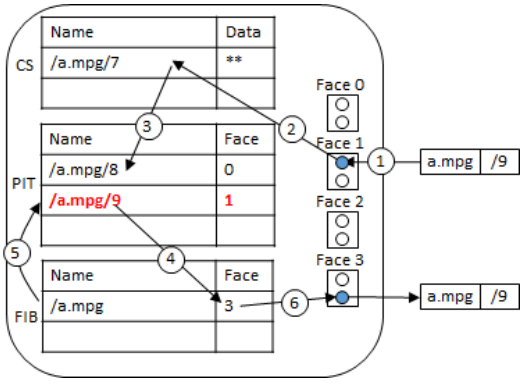
- 포워딩 (Fowarding Information Base, FIB) 테이블: 데이터 요청 메시지(Interest)에 포함되어 있는 데이터 이름을 기반으로 해당 Interest를 포워딩할 전송 인터페이스 (Face)를 결정에 필요한 정보를 제공한다.
- 요청 정보 테이블 (Pending Interest Table, PIT): 응답 메시지(Data) 수신 시, 해당 Data를 사용자들에게 전송하기 위하여, 수신된 Interest와 incoming Face 정보를 기록/관리한다.
- 네트워크 캐시 (Content Store, CS): 네트워크 노드들은 전송 중인 Data를 노드의 CS에 임시 저장한다.



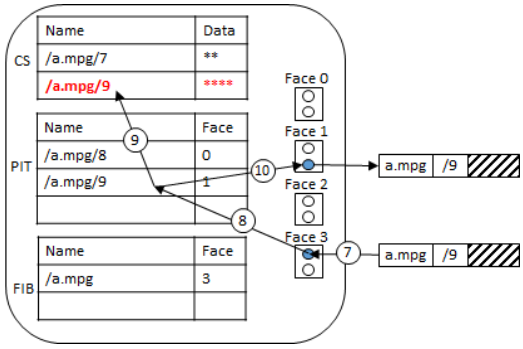
〔그림 3〕 NDN Name 계층 구조

그림 4-(a)의 NDN Interest 처리 절차는 다음과 같다: (1)네트워크 노드의 인터페이스 (Face 1)로 Interest를 수신되면, (2) Interest에 부합하는 데이터가 CS에 저장되어 있는지 여부를 확인한다. 만약 해당 데이터가 저장되어 있다면, 해당 데이터를 Interest를 수신한 인터페이스를 통하여 요청자에게 전송한 후, 수신한 Interest 처리를 완료한다. (3) 부합하는 데이터가 CS에 존재하지 않으면, 수신한 Interest에 해당하는 기록(entry)이 PIT에 존재하는지 확인하다. 만약 대응되는 기록이 PIT 내에 존재한다면, 해당 기록에 Interest가 수신된 인터페이스 정보를 추가한 후, 수신한 Interest 처리를 완료한다. 그러나 PIT에 대응되는 기록이 없다면, (4) FIB 테이블을 참조해서 Interest를 포워딩할 인터페이스 (예를 들어, Face 3)를 선택한 후, (5) PIT에 수신한 Interest를 위한 새로운 entry를 추가하고, (6) Interest를 선택한 인터페이스를 통하여 전송한다.

그림 4-(b)의 NDN Data 처리 절차는 다음과 같다: (7) 노드의 인터페이스 (예를 들어, Face 3)로 Data가 수신되면, (8) 수신 된 Data에 대응하는 entry가 PIT에



(a) Interest Process



(b) Data Process

〔그림 4〕 NDN Interest/Data 운영 절차

존재하는지 확인한다. 만약 대응되는 entry가 PIT에 존재하지 않다면, 수신한 Data를 폐기한 후, Data 처리 절차를 종료한다. (9) 수신 된 Data를 노드의 CS에 저장한다. (10) PIT에서 Data에 부합되는 entry에 기록되어 있는 인터페이스들 (예를 들어, Face 0)로 Data를 전송한 후, PIT에서 대응되는 entry를 삭제한다.

NDN에서 사용되는 Naming 기법은 콘텐츠 자가 인증 기능을 제공하지 못한다. 그러나 콘텐츠 배포자를 인증할 수 없기 때문에, 콘텐츠의 무결성 및 인증 기능을 제공하기 위하여 배포되는 Data에 콘텐츠 공급자의 전자서명을 반드시 첨부하도록 강제하고 있다. 또한, 단편화된 Segment들의 효율적인 인증을 위해 머클 해쉬 트리를 이용한 콘텐츠 인증 방안의 사용을 권고한다.

2.4. ICN 프로젝트 콘텐츠 식별 정보 특성 분석

표 2는 ICN 프로젝트의 콘텐츠 식별 정보의 특성을 비교 분석한다.

〔표 2〕 콘텐츠 식별 정보 특성 비교

Project	Name Structure	Privacy	Resolution	Self-Certifying
DONA	flat	O	O	O
NetInf	flat	O	O	O
NDN	hierarchy	X	X	X

2.4.1. 구조적 특성

ICN의 Naming 기법은 크게 계층적 구조와 비계층적 구조로 구분될 수 있다. 비계층적 식별 정보 구조는 콘텐츠의 해쉬 값을 식별 정보로 사용한다. 그러므로 식별 정보만으론 콘텐츠 요청 패킷을 콘텐츠 공급자/배포자에게 라우팅할 수 없다. 이와 같은 문제를 해결하기 위하여 Name Resolution System의 운영이 필요하다. 또한, 콘텐츠를 배포하기 위해서는 콘텐츠 공급자/배포자가 해당 콘텐츠 정보 및 호스트 정보를 Name Resolution System에 선등록 해야 한다. 그러나 네트워크를 통해 배포되는 모든 콘텐츠를 Name Resolution System이 등록/관리하는 경우, 그 정보의 양이 매우 많기 때문에, 정보를 저장하기 위한 저장 공간과 정보의 관리/탐색을 위한 오버헤드에 대한 처리 방안이 필요하다. 무엇보다도 Name Resolution System이 정상적으로 동작하지 않거나, 접속이 원활하지 못할 경우, 네트워크 패킷 전송이 중단될 수 있다. 즉, Name Resolution System이 서비스 거부 공격과 같은 공격의 원점이 될 수 있으며, DNS 스프핑과 같은 공격에도 취약할 수 있다.

계층적 식별 정보 구조는 Name Resolution System을 이용하지 않고 네트워크 노드가 해당 식별 정보만을 분석하여 요청 메시지를 전송할 경로를 결정하기 때문에 Name Resolution System 사용 시 발생하는 문제점들을 해결할 수 있다. 그러나 네트워크 노드가 콘텐츠 식별 정보를 분석하기 위해서는 네트워크 노드들 사이에 Domain Prefixes 정보들을 교환하는 라우팅 프로토콜이 필요하다. 또한 콘텐츠 식별 정보의 길이를 제한하

지 않기 때문에 PIT를 관리/운영할 때 데이터 오버플로우 및 서비스 거부 공격에 취약할 수 있다 [18,19].

2.4.2. 콘텐츠 인증

ICN의 Naming 기법은 콘텐츠 자가 인증 기술과 전자 서명 기반 인증 기술로 구분된다. 콘텐츠 자가 인증 기술은 콘텐츠의 해쉬 값을 콘텐츠 식별 정보로 사용하기 때문에 별도의 인증 시스템을 이용하지 않고 콘텐츠의 무결성을 검증할 수 있다. 그러나 콘텐츠 공급자를 인증할 수 없다는 단점과 함께 해쉬 값 교체를 통하여 검증 절차를 쉽게 우회할 수 있다.

전자 서명 기반 인증 기술은 콘텐츠 공급자의 서명을 콘텐츠에 추가하여 배포한다. 콘텐츠의 무결성 검증뿐만 아니라 공급자 인증 기능도 제공한다. 그러나 전자 서명을 운영하기 위해서는 글로벌 인증 체계와 시스템 운영이 요구된다.

2.4.3. 콘텐츠 익명성

ICN의 Naming 기법의 계층적 구조는 콘텐츠의 해쉬 값을 콘텐츠 식별 정보로 사용하기 때문에, 식별 정보만으로 교환되는 콘텐츠의 정확한 이름을 분간할 수 없다. 그러나 비계층적 구조의 콘텐츠 식별정보는 가독성이 높고, 콘텐츠 공급자의 네트워크 및 조직 구성, 콘텐츠 이름등의 정보를 분석할 수 있기 때문에 사용자의 프라이버시 침해 문제에 대한 해결이 필요하다 [20,21].

Ⅲ. 결 론

미래 인터넷은 전송 효율성을 높이기 위하여 기본적으로 콘텐츠 캐시를 이용해 복수 개의 콘텐츠 배포자를 운영한다. 그러나 호스트 식별 정보를 네트워크 주소로 사용할 경우, 캐시 탐색을 위해서는 상위 계층의 정보를 분석해야 한다. 그러므로 콘텐츠 식별 정보를 네트워크 주소의 일부 또는 전부로 사용하는 방안이 요구된다. 미래 인터넷 기술은 이와 같이 콘텐츠 식별 저보를 네트워크 주소로 사용하기 위한 식별 정보 구조와 함께 운영 절차를 제안한다.

본 논문에서는 미래 인터넷의 ICN 프로젝트들이 정의한 콘텐츠 식별 정보 구조와 운영 방안을 비교 분석하고, 각각의 장단점을 분석하였다.

참 고 문 헌

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

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

[3] E. Meshkova, J. Riihijarvi, M. Petrova, and P. Mahonen, “A survey on resource discovery mechanisms, peer-to-peer and service discovery frameworks,” Computer Networks Journal., vol. 52, no. 11, pp. 2097–2128, 2008.

[2] 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.

[3] 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.

[4] G. Xylomenos, C. N. Ververidis, and V. A. Siris, “A Survey of Information-Centric Networking Research,” IEEE Communications Surveys & Tutorials, Volume: 16, Issue: 2, 2014

[5] R. Tourani, T. Mick, S. Misra, and G. Panwar, “Security, Privacy, and Access Control in Information-Centric Networking: A Survey,” http://arxiv.org/abs/1603.03409, Sep 2016.

[6] N. Sastry, R. Cuevas, I. Rimac and A. Mauthe, “Where is in a Name ? A Survey of Mobility in Information-Centric Networks,” In Communications of the ACM (CACM), Vol. 56, No. 12, 2013

[7] FP7 PURSUIT project. Available: http://www.fp7-pursuit.eu/PursuitWeb

[8] FP7 PSIRP project. Available: http://www.psirp.org
[9] FP7 SAIL project. Available: http://www.sail-project.eu
[10] FP7 4WARD project. Available: http://www.4ward-project.eu
[11] FP7 COMET project. Available: http://www.comet-project.org
[12] FP7 CONVERGENCE project. Available: http://www.ict-convergence.eu
[13] T. Koponen, M. Chawal, B. Chun, A. Eromolinsky, K. H. Kim, S. Shenker, and I. Stoica, “A Data-oriented (and beyond) network architecture,” in ACM SIGCOMM, 2007, pp. 181-192. 2007.
[14] C. Dannewitz et al., “Secure Naming for a Network of Information,” INFOCOM IEEE Conf. Comp. Commun. Workshop, pp. 1-6, Mar., 2010.
[15] V. Jacobson, D. K. Smetters, J. D. Thornoton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking Named Content,” in ACM CoNEXT, 2009.
[16] Content Centric Networking project. Available: http://www.ccnx.org
[17] NSF Named Data Networking project. Available: http://www.named-data.net
[18] D. Kim, “How to make content centric network (CCN) more robust against DoS/DDoS attack,” IEICE Transactions on Communications E.96, pp. 313-316, January 2013
[19] P. Gasti and G. Tsudik, “DoS & DDoS in Named Data Networking,” Computer Communications and Networks (ICCCN), 2013
[20] C. A. Wood, E. Uzun, “Flexible end-to-end content security in CCN,” Proc. IEEE CCNC 2014, Jan. 2014.
[21] D. Kim, “Content Centric Networking Naming Scheme for Efficient Data Sharing,” Journal of Korea Multimedia Society, Vol. 15, No. 9, pp. 1126-1132, 2012.

〈저자소개〉

윤 덕 상 (Duck Sang Yoon)
정회원

1989년 2월 : 고려대학교 자연과학대 수학과 졸업
2005년 2월 : 고려대학교 정보보호대학원 석사
1999년 8월 : 삼성 SDS
2005년 7월 : 시큐아이 부장
2014년 6월 : 롯데정보통신 부문장
2014년 7월~현재 : kt ds 정보보안센터장
관심분야 : 정보보호정책, 위험관리, 개인정보보호, 보안관제

김 대 엽 (Kim DaeYoub)
종신회원

2000년 2월 : 고려대학교 대학원 수학과 박사
2002년 2월 : 시큐아이닷컴 정보보호연구소 차장
2012년 2월 : 삼성전자 종합기술원 수석연구원
2012년 3월~현재 : 수원대학교 정보보호학과 조교수
관심분야 : 미래 인터넷 보안, Connected Vehicle 보안, 콘텐츠 보안