JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 4, pp. 87-95, April 2020
https://doi.org/10.9708/jksci.2020.25.04.087

A Study of Advanced Internet Strategy for Future Industry

Jae-Kyung Park*, Hyung-Su Lee*, Young-Ja Kim*

*Professor, Dept. of Information Security, Korea Polytechnics, Seoul, Korea
*Professor, Dept. of Information Security, Korea Polytechnics, Seoul, Korea
*Professor, Dept. of Information Security, Korea Polytechnics, Seoul, Korea

[Abstract]

In this paper, we examine the problems of the current Internet due to the development of network services and the expansion of network bandwidth. The current Internet has been used for a long time because it is composed of TCP / IP, but fundamental problems such as bandwidth, transmission rate, and security have not been solved. Therefore, the future network must be prepared through continuous investment and maintenance. In order to overcome this problem, we will propose a way to overcome the above problems and upgrade by converting the current Internet Protocol into the next generation network. Currently, many researches on next-generation networks have been conducted, but there are not many studies in Korea, and research on next-generation networks will be a very important task for the future development of the Internet service industry at the national level. In this paper, we propose an advanced internet environment through the advantages of various next generation protocols.

▸ **Key words**: Internet, Content Delivery Network, Software Defined Network, Content Centric Network, Information Centric Network, Future Generation Technology Integrated Network

[요 약]

본 논문에서는 향후 네트워크 서비스의 발전 및 네트워크 대역폭 확대에 따른 현재의 인터넷이 가지고 있는 문제점을 살펴보고 이를 고도화할 수 있는 방안에 대해 제안한다. 현재의 인터넷은 TCP/IP로 구성되어 오랜 시간 사용되어 왔으나 대역폭, 전송량, 보안 등의 근본적인 문제가 해결되지 않아 지속적인 투자 및 유지보수를 통해 미래 네트워크를 대비하여야 한다. 이를 극복하기 위해 현재의 인터넷 프로토콜을 차세대 네트워크로 변환하여 이러한 문제를 극복하고 고도화할 수 있는 방안을 제시하고자 한다. 현재 차세대 네트워크에 대한 많은 연구가 이루어지고 있으나 국내에는 이러한 연구가 많이 이루어지지 않고 있으며 국가적인 차원에서 미래의 인터넷 서비스 산업 발전을 위해 차세대 네트워크에 대한 연구는 매우 중요한 과제일 것이다. 본 논문에서는 다양한 차세대 프로토콜을 통한 장점을 통해 고도화된 인터넷 환경을 제안하고자 한다.

▸ **주제어**: 인터넷, 콘텐트 전송 네트워크, 소프트웨어 정의 네트워크, 콘텐트 중심 네트워크, 정보 중심 네트워크, 차세대 네트워크

• First Author: Jae-Kyung Park, Corresponding Author: Hyung-Su Lee
*Jae-Kyung Park (jakypark@kopo.ac.kr), Dept. of Information Security, Korea Polytechnics
*Hyung-Su Lee (hslee01@kopo.ac.kr), Dept. of Information Security, Korea Polytechnics
*Young-Ja Kim (tiny89@kopo.ac.kr), Dept. of Information Security, Korea Polytechnics
• Received: 2020. 03. 05, Revised: 2020. 04. 01, Accepted: 2020. 04. 01.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

4차산업혁명 활성화 전략에 따라 새로운 형태의 서비스 및 산업 활성화 방안에 대한 투자 및 연구가 활발하게 논의되고 있으며 특히, 차세대 네트워크 서비스에 대한 도입 및 개발이 박차를 가하고 있으며 이를 원활하게 지원할 네트워크의 필요성도 함께 증가되고 있는 실정이다. 모바일 통신 사업자들이 이미 5G를 세계 최초로 상용화하였고 이를 바탕으로 콘텐트, 게임, 사물인터넷 등의 서비스가 날로 증가하고 있는 추세이다. 최근 10 여년 간 네트워크의 콘텐트가 텍스트나 이미지 중심에서 동영상 중심으로 이동하고 있다는 것은 누구나 실감하고 있는 상황이다. 가장 큰 변화는 유튜브(YouTube)의 성장으로 대부분의 콘텐트를 유튜브를 통해 활용하고 있다고 해도 과언이 아닐 정도로 네트워크에서 차지하는 비중은 상당하다고 판단하다.

앞으로의 네트워크 서비스는 더 빠르게 변화하여 향후 몇 년 안에 이러한 비디오 중심의 서비스가 전체 인터넷의 80~90% 이상을 차지할 것으로 전망하고 있다. 이러한 변화의 중심에 새로운 네트워크에 대한 연구와 관심은 근 시일 내에 국내에도 적용되어야 하는 상황이라고 볼 수 있다. 특히 콘텐트 기반의 네트워크를 통해 국내 일부 연구기관에서 차세대 네트워크에 대한 실효성 여부를 연구하고 있다. 하지만 이러한 연구가 단지 논문 수준이 아닌 실제 개발로 이어지고 SW 정책적으로 설계되어야 할 것이다. 또한 최근 정보통신기술의 발전은 클라우드 및 사물인터넷 등의 다양한 센서들과와 이러한 센서 간의 통신기술을 이용하여 일상생활을 보다 편리하게 해주는 기술의 발전을 이끌어 냈다. 하지만 이러한 기술의 발전은 생활의 편의성을 증가시킨 반면, 정보의 유출, 데이터의 위변조, 이를 이용한 해킹 사고 등 새로운 서비스를 악용한 다양한 위협에 노출되어 있다.

이러한 보안 위협이 증가하는 이유는 정보통신 활용기술의 발전과 취약점을 방어할 수 있는 보안기술의 적용이 가능한가의 문제이다. 즉, 네트워크 장비의 특징에 따라 현재 컴퓨터 환경에서 사용되는 인증기술이나 보안 기능 등을 바로 적용하기에는 한계가 많은 것이 사실이다. 기존의 많은 연구 결과 차세대 네트워크가 추구하는 바는 저용량, 초경량을 추구하지만 현재 환경에서 활용되는 보안 관련 기술은 고성능을 요구하므로 이러한 기술 자체를 그대로 적용할 수는 없는 상황이다. 이러한 원인으로 보안 인증 기술을 우회하여 불법적으로 허용되지 않는 접근을 통해 주요 정보와 기타 개인정보를 탈취하거나 내부망의 서버로 침투가 가능해져 더욱 큰 위협을 초래할 수 있다.

최근 전반적인 환경의 변화는 기존 IP 트래픽을 지속적 확장을 통해 통신망 및 정보보안 등 모든 인터넷 관련 업체가 무시할 수 없는 문제로 데이터의 송수신량이 평균 23%씩 증가하고 있으며 이러한 추세는 계속 이어질 전망이다. 이러한 다양한 장비의 특성을 맞추고 특화된 데이터나 대량의 트래픽을 효과적으로 처리하기 위한 방안이 강구되어야하며 단순히 기기의 성능만을 증가시키는 방식은 그 효과가 매우 미흡하다고 할 수 있다. 또한 이러한 서비스에 필요한 데이터를 처리 및 가공하는데 있어 보안의 요소를 고려하는 것은 그 무엇보다도 중요한 것으로 반드시 함께 고려되어야 한다.

본 논문에서는 이러한 차세대 네트워크가 갖추어야 할 중요한 요소를 중심으로 향후 미래 인터넷으로 활용 가능한 네트워크를 정책적으로 제안하고자 한다. 대용량을 데이터를 보다 빠르고 안전하게 처리하고 보안적인 문제도 해결할 수 있는 형태의 네트워크를 통해 현재의 인터네 환경을 보다 고도화하여 다가오는 미래를 준비하고자 함이 본 논문의 목적이다. 다음 2장에서는 차세대 네트워크의 국내외 동향에 대해 살펴보고 3장에서는 콘텐트 기반의 네트워크를 통한 네트워크를 제안하고자 한다. 4장에서는 기존의 네트워크와 제안된 네트워크를 비교하여 장단점을 살펴보고 5장에서 결론을 제안하도록 한다.

II. Preliminaries

1. Related works

1.1 CDN(Content Delivery Network)

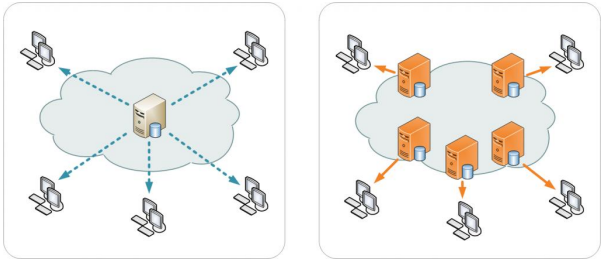

Fig. 1. CDN System Architecture

CDN(Contents Delivery Network)은 지리적 물리적으로 떨어져 있는 사용자에게 콘텐트 제공자의 콘텐트를 더 빠르게 제공할 수 있는 기술을 말한다. 기본적으로 사용자가 원격지에 있는 서버(Origin Server)로 부터 콘텐트(Content)(예. Web Object, Video, Music, Image, Document 등)를 다운로드 받을 때 가까이 있는 서버에서

받는 것보다 시간이 오래 걸리므로, 사용자와 가까운 곳에 위치한 Cache Server에 해당 Content를 저장(캐싱)하고 Content 요청 시에 Cache Server가 응답을 주는 기술이다.

CDN을 사용하지 않으면 콘텐트를 담고 있는 오리진 서버들은 모든 엔드유저의 요청에 일일이 응답해야 한다. 이는 오리진과 오리진에 막대한 트래픽을 유발하고 이후에도 엄청난 부하를 유발하여 트래픽이 과도하게 증가하거나 부하가 끊임없이 들어오는 경우 오리진에서 장애가 발생할 확률을 높인다. CDN은 오리진을 대신하여 엔드유저와 가까운 물리적 위치 및 네트워크에서 엔드유저 요청에 응답함으로써 콘텐트 서버의 트래픽 부하를 줄이고 엔드유저의 웹 경험을 개선하여 콘텐트 제공업체와 엔드유저 모두에게 막대한 이점을 제공한다.

따라서 사용자는 가까운 곳에 있는 서버(Cache Server)로 부터 Content를 수신하게 되므로 원격지 서버에서 받는 것보다 빠르게 페이지나 콘텐트를 이용할 수 있다. CDN은 웹, 애플리케이션, 스트리밍 미디어를 비롯한 콘텐트를 전송하도록 최적화된 전 세계적으로 촘촘히 분산된 서버로 이루어진 플랫폼으로 이 서버 네트워크는 수많은 물리적 위치와 네트워크 위치에 분산되어 있어 웹 콘텐트에 대한 엔드유저의 요청에 직접적으로 응답하고 빠르고 안전한 미디어 전송을 보장한다.

기본적으로 인터넷은 오늘날 사용자들이 기대하는 막대한 양의 데이터에 대한 수요, 라이브 고화질 동영상, 플래시 광고, 대용량 다운로드를 처리할 수 있도록 설계되지 않았다. 반면 CDN은 인터넷이 보다 효율적으로 작동하고, 규모에 맞게 미디어를 전송하고, 상상할 수 있는 모든 온라인 경험을 제공할 목적으로 설계되었다. 따라서 현재는 CDN이 온라인 비즈니스를 성공적으로 수행하기 위한 필수 도구가 되었다고도 할 수 있다. 콘텐트 전송 네트워크는 여러 기업들이 미디어 전송의 다양한 문제들을 극복하도록 지원할 수 있도록 고유의 역량을 보유하고 있으며 CDN은 20년이 넘는 세월 동안 유통, 금융, 헬스케어를 비롯한 여러 업종이 전 세계 엔드유저에게 빠르고 규모에 맞게 온라인 콘텐트를 제공할 수 있도록 지원해 오면서 인터넷의 보이지 않는 백본 역할을 수행해 왔다. 따라서 사용자가 온라인으로 어떤 작업을 행한 적이 있다면, 실제로 인식했든 인식하지 않았든, 이미 CDN의 이점을 누린 경험이 있으며 앞으로도 CDN의 활용은 당분간 이어질 전망이다.

하지만 CDN의 가장 큰 단점은 콘텐트 전송 네트워크 추가 비용이 많이 든다는 것이다. 또한 웹 사이트 및 배포 절차가 복잡해진다. 고객에게 일부 콘텐트 전송 네트워크를 차단하고 콘텐트가 로드되지 않도록 하는 네트워크 필터가 있을 수 있으며 지리적 위치는 목표 고객과 가까울 수 있다. 실제로 자신의 웹 사이트를 직접 운영하면서 얻는 혜택보다 더 많은 혜택을 잃을 수 있다는 점 등이 단점으로 꼽힌다.

추가적으로 갈수록 많은 기업들이 온라인에서 사업을 영위하고 갈수록 많은 사용자들이 인터넷에서 쇼핑과 공유를 즐기고 있다. 따라서 콘텐트 제공업체는 다양한 콘텐트의 전송, 서로 다른 디바이스 유형에 맞춘 콘텐트 조정(디바이스 인식), 데이터 및 엔드유저의 온라인 정보 보안이라는 일련의 도전 과제에 직면하고 있다.

1.2 SDN(Software Defined Network)

소프트웨어 앱을 사용하여 네트워크를 지능화 하고 중앙에서 제어하거나 프로그래밍 할 수 있는 네트워크 아키텍처 접근법이다. 사업자는 기본 네트워크 기술에 상관없이 전체 네트워크를 일관적으로 전체적으로 관리할 수 있다. 물리적인 네트워크를 소프트웨어 기술을 이용하여 제어하는 네트워크 기술이다. SDN은 네트워크의 제어 플레인을 네트워크 트래픽을 전달하는 데이터 플레인과 분리한다는 개념이다. 이런 분리의 목적은 중앙에서 관리하고 프로그래밍이 가능한 네트워크를 만드는 것이다. 일부 SDN 구현 솔루션은 범용 네트워크 하드웨어를 통제하는 소프트웨어 기반 관리 플랫폼을 사용한다. 또 다른 접근법은 통합된 소프트웨어와 하드웨어를 사용하기도 한다.

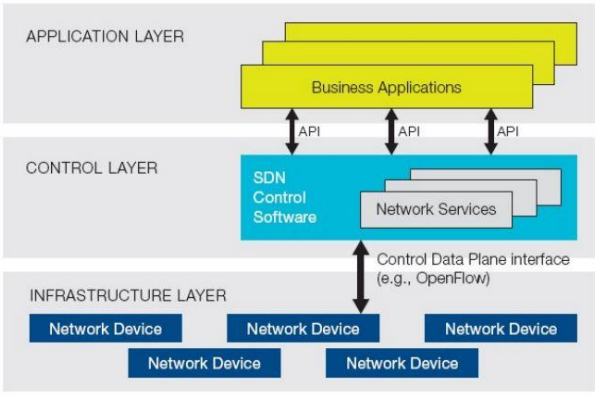

Fig. 2. SDN System Architecture

SDN은 주로 대기업 데이터센터에서 사용하는데, 전통적인 네트워킹 아키텍처와 비교해 비즈니스의 요구에 좀 더 쉽게 대응할 수 있는 네트워크를 필요로 하는 환경이다. SDN을 주목하는 이유는 네트워크 관리 측면에서의 효율성과 향상과 새로운 비즈니스 생태계 구축을 통해 현재 침체되어 있는 네트워크 시장을 활성화 시킬 수 있을 것이라는 기대감 때문이다.

하지만 이러한 SDN에도 여러 가지 단점이 존재한다. SDN는 컨트롤러를 통해 네트워크의 흐름을 제어할 수 있

고 이를 통해 네트워크를 단순화 할 수 있다. 하지만 컨트롤러로 인해 발생 가능한 보안 문제점도 있다.

첫 번째로 컨트롤러가 악성코드에 감염됐을 때로 컨트롤러가 악성코드에 감염된다면 공격자는 프로그램을 재설치 하여 네트워크 상에 있는 데이터 스니핑 또는 드랍핑 할 수 있다.

두 번째로 관리자가 악의적인 의도를 가졌을 때이다. 컨트롤러의 룰을 작성하는 관리자나 아키텍쳐가 악의적 의도로 컨트롤러의 룰을 변경하면 네트워크가 정지될 수 있고 정보유출까지 가능하다.

마지막으로 컨트롤 플레인과 데이터 플레인 사이의 디도스 공격이다. 이 공격은 컨트롤러가 정상적으로 데이터 계층에 지시를 내리지 못하게 되어 정상 작동을 방해 받는다. 그 밖에 OpenFlow의 취약점을 이용하여 다양한 형태의 공격이 이루어질 수 있는 문제들이 해결되어야 할 것으로 판단한다.

1.3 ICN(Information Centric Network)

CCN 기술을 바탕으로 CISCO에서 새롭게 개발하고 있는 차세대 네트워크로 통신을 원하는 개체가 통신 대상 호스트(host)의 주소에 기반한 통신이 아니라 정보 식별자를 기반으로 하는 통신 방법이다. 이는 정보 자체를 식별하도록 Name을 정의하고 Name을 기반으로 라우팅과 포워딩을 지원하며, 캐싱 기능을 통해 인터넷의 코어에 부담 없이 효과적이며 빠른 형태의 전송 서비스 및 정보의 무결성을 지원해 주는 암호화 기법을 제공한다.

ICN에서는 중간 어느 노드에서도 정보를 획득할 수 있으므로 획득한 정보가 인증된 게시자로부터 생성된 것인지에 대한 암호 정보를 기본으로 탑재하고 사용자는 자신이 원하는 정보의 이름과 함께 유효한 게시자 정보 공개(공개키)를 이용하여 정보의 무결성을 체크할 수 있다. 즉,

1) 기존 인터넷 주소는 인터넷 인프라를 구성하는 전달망 요소들을 식별하는 용도로만 사용하고, 정보의 유통 문제는 주소 대신 식별자를 사용해 해결하는 방식

2) 기존 인터넷이 통신의 목적보다는 절차에 집중한 반면, ICN은 절차보다는 목적에 집중하는 형태의 네트워킹 기술

3) 현재 인터넷의 단대단(end to end) 통신기법을 중심으로 한 호스트 기반 네트워킹과는 달리, 실제 전달하고자 하는 정보를 가장 효과적으로 제공하기 위한 네트워킹 기술을 포함하고 있으며, 전달된 정보 자체의 무결성을 위한 신뢰 기법

4) 현재 인터넷과는 달리, ICN에선 정보 자체를 식별하도록 Name을 정의했고, 이는 모든 네트워크 상에서 정보를 찾는 것뿐 아니라 기존의 라우팅과 포워딩에도 사용하게 된다. 이는 자연스럽게 단대단 통신 세션을 유지하지 않고 한 홉을 건너 갈 때마다 정보를 찾고 다시 포워딩 하는 절차를 수행하는 형태로 통신 형태가 바뀌게 되는 구조이다.

5) 실시간 대용량 미디어 서비스를 위해 P2P · CDN(Content Delivery Networking) 등과 같은 OTT(Over The Top) 기반의 캐시 서버를 별도로 구축하는 것(응용 서비스 차원의 분산된 미디어 서비스를 제공하는 형태를 탈피해 전송장비 자체에 네트워크상의 정보를 직접 캐싱할 수 있는 기능을 탑재한 것)으로 네트워크상의 캐싱 기능은 네트워크 상의 미디어 정보들이 자연스럽게 사용자 주변 장비에 저장되도록 하며, 결과적으로 부담이 없이 효과적이며 빠른 형태의 전송 서비스를 제공할 수 있게 개발하고 있다.

위에서 살펴본 CDN, SDN, ICN 등의 네트워크는 현재의 인터넷을 보완하기 위해 개발된 고도화된 네트워크이다. 하지만 이러한 네트워크들도 각기 장단점이 존재하며 보완해야할 필요성이 존재한다. 따라서 본 논문에서는 이러한 고도화된 네트워크의 기능을 복합적으로 설계하여 보다 고도화된 차세대 네트워크를 제안하고자 한다.

III. The Proposed Scheme

1. Analysis Problems

차세대 네트워크가 적용될 수 있는 분야로 가장 많이 회자되는 것이 사물인터넷 분야와 동영상 서비스 분야이다. 사물인터넷은 그동안 개별 네트워크(silo)로 존재하던 서로 다른 사물네트워크들이 인터넷으로 서로 연결되어 미래사회를 위한 창조적인 서비스 창출을 가능하게 하는 기반 인프라 기술이었다.

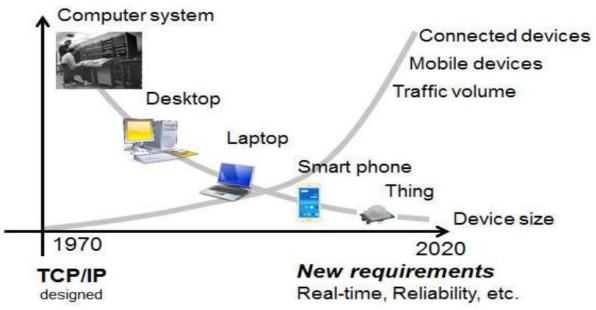

Fig. 3. New Requirement for Internet

이는 네트워크 기술 관점에서는 초기 대형 컴퓨터 간 연결에서 데스크탑, 랩탑, 스마트폰으로 그 영역을 점점 확대해가던 인터넷이 센서나 RFID와 같은 제한된 능력을 가지는 사물

까지 그 연결성을 확장한 개념으로 이러한 환경 변화에 따라 기존과는 다른 새로운 도전적 기술 이슈를 동반하고 있다.

사물인터넷 기술은 차세대 ICT 인프라 핵심기술로 세계적으로도 가장 중요한 R&D 이슈로 간주되고 있으며 이를 보다 효율적으로 이용하기 위해 차세대 네트워크와의 연결이 많이 연구되고 있다. 하지만 현재 다양한 사물 네트워크 간 간 통신을 위해서는 기존 IP 네트워킹 기술이 유력하게 고려되고 있으나 현 IP 네트워킹 기술은 기존 네트워크와 현저히 차별화된 특성을 가지는 사물 네트워크 지원에 구조적 비효율성을 가지고 있다는 것이 가장 큰 걸림돌이다.

인터넷 표준화 기관인 IETF에서는 많은 주소공간을 가지는 IPv6를 기반으로 기존 TCP/IP 기술을 경량화하여 사물인터넷에 적용하는 방향으로 표준화를 진행 중이나 이 또한 현재 IP 기반 네트워킹 기술로 기본 설계 개념상 사물네트워크 적용에 구조적 한계를 가진다는 것을 부인할 수는 없을 것이다. 아래의 이러한 기술적인 사유로 차세대 네트워크의 콘텐트 기반의 네트워크를 통한 사물인터넷이 주목 받고 있는 것이다.

- 종단 호스트에 대부분의 기능을 구현하는 종단간 설계 원칙으로 인해 메모리, 전원, 프로세싱에 제한성을 가지는 사물 디바이스에 비효율적인 구조임
- 주소 기반의 정보 전달로 높은 이동성을 가지는 수 백억개 이상의 사물에 대한 라우팅/포워딩이 비효율적인 구조임
- 위변조가 용이한 IP 주소 기반의 통신으로 사물인터넷에서 요구하는 높은 수준의 보안성 제공에 비효율적인 구조임

이에 따라 기존 IP 네트워킹 기술이 아닌 새로운 차세대 네트워킹 기술을 기반으로 사물인터넷에서 궁극적으로 추구하는 비전을 실현하고자 하는 연구가 전 세계적으로 최근 시작되고 있는 것이다.

그렇다면 이러한 당면한 문제를 해결하기 위한 차세대 네트워크는 어떠한 형태를 가져야 하는가에 대한 해결책을 제시해야 한다. 첫 번째로 가장 중요한 문제는 현재의 네트워크를 물리적으로 계속 확대하지 않고 대역폭을 늘려 대용량의 데이터를 빠르게 전송할 수 있는 네트워크가 필요할 것이다. 또한 전송되는 데이터가 신뢰를 바탕으로 서비스되어 데이터에 대한 보안이 지원되어야 할 것이다. 이러한 특징을 본 논문에서는 '대용량', '초고속', '고신뢰'의 세 가지 문제로 분류하여 고도화할 수 있는 네트워크를 제안하고자 한다.

2. FG-TIN (Future Generation Technology Integrated Network)

앞 절에서 살펴본 내용에 따라 본 논문에서는 새로운 네트워크 형태인 FG-TIN(Future Generation Technology Integrated Network)을 제안한다. 제안하고자 하는 네트워크는 기존의 차세대 네트워크의 장점을 파악하여 새롭게 구성한 네트워크이다.

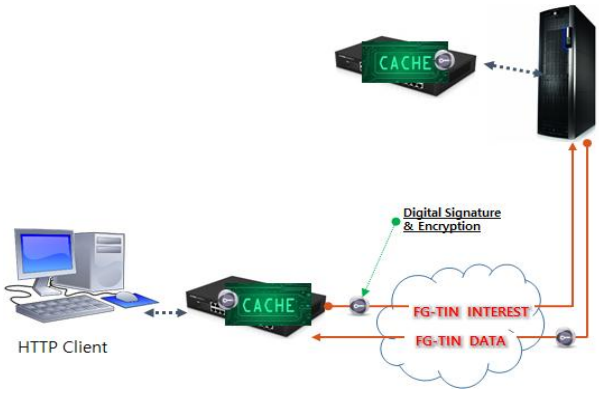

Fig. 4. FG-TIN System Architecture

Fig. 4에서와 같이 기존의 시스템과 네트워크 인프라는 인터넷을 동일하게 사용한다. 다만 변경된 내용은 클라이언트 단에서 나오는 패킷을 인터넷으로 내보내기 전에 게이트웨이 형태의 장비를 통해서 기존의 TCP/IP를 FG-TIN으로 변경한 후 이를 UDP로 서버에 전달하고 서버 앞단에는 FG-TIN을 해석할 수 있는 네트워크 장비를 설치하여 FG-TIN을 해석한 후 원본 데이터를 서버로 전송하는 역할을 수행한다.

이때 FG-TIN의 데이터는 요청 및 수신 데이터에 각 디바이스의 전자서명을 붙여 데이터가 무결성을 유지하도록 한다. 이는 기존 연구에서 설명한 ICN의 프로토콜과 마찬가지로 무결성이 유지되며 Interest 패킷과 Data패킷의 단순한 프로토콜을 사용한다. 또한 데이터는 전자서명이 되어 있으므로 캐싱을 하더라도 위변조의 위험이 없으므로 재사용이 가능하다. 그리고 FG-TIN을 통한 데이터들은 TCP가 아닌 UDP를 사용하여 세션이 없이 데이터를 주고받으므로 기존의 네트워크의 보안성을 크게 강화할 수 있는 방안이라고 할 수 있다. 다음 절에서 이러한 FG-TIN을 이용한 기능별 장점에 대해 설명하기로 한다.

3. Advanced Bandwidth

현재의 인터넷을 구성하는 서버, 클라이언트, 라우터 등의 네트워크 디바이스는 서비스를 제공하기 위해 대부분 TCP/IP를 사용하고 있다. 하지만 전송되는 데이터를 재사용

하지 못하고 요청이 들어오면 다시 동일한 데이터를 동일한 방식에 의해 송수신한다. 이를 보완하기 위해 적용된 CDN과 같이 각 네트워크 장비에 Fig. 5와 같이 캐싱을 적용할 경우 동일한 대역폭에서 더 많은 데이터를 전송할 수 있다. CDN의 경우는 서버를 서비스가 많이 요청되는 지역에 서버를 캐싱하는 기능을 제공하지만 제안 시스템은 각 디바이스에 캐싱 기능을 추가하므로 인해 지역적 캐싱을 탈피하고 보다 효율적인 대역폭 관리를 할 수 있다는 장점을 지닌다.

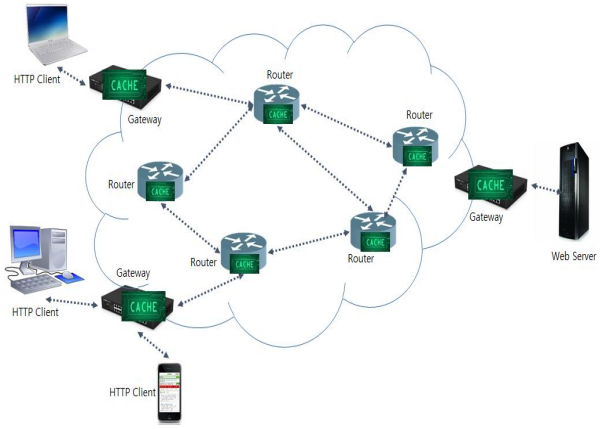

Fig. 5. Install Cache Function of N/W Device

다만, 실제 환경에서 모든 서비스를 캐싱으로 활용하기 위해서는 각 디바이스의 캐싱 크기나 데이터 내용을 판단할 수 있는 기능들도 추가되어야만 원활하게 활용이 가능하다는 점도 추가적인 고려사항이 되어야할 것이다. 따라서 캐싱되는 데이터는 콘텐트 기반의 데이터로 서비스되어야만 하며 요청되는 서비스의 저장 단위 또한 콘텐트 기반이어야만 한다. 이러한 사유로 인해 본 논문에서는 콘텐트를 HTTP로 한정하여 설계하였다.

4. Advanced Performance

위에서 설계한 캐싱을 각 네트워크 디바이스에 적용할 경우 현재의 물리적인 대역폭을 보다 효율적으로 활용할 수 있는 장점이 있었다. 또한 추가적으로 캐싱이 되어 있는 가장 근접한 디바이스에서 전송이 이루어지므로 매우 빠른 반응 속도를 나타낸다. 또한 추가적인 성능 개선점은 다음의 그림과 같이 기존의 방식과 같이 TCP를 사용하는 것이 아니라 UDP를 통해 데이터를 주고받을 경우 훨씬 더 빠른 전송 속도를 얻어낼 수 있다. TCP의 경우 데이터 수신에 대한 신뢰성이 있는 반면에 세션을 유지해야하는 부담이 있으며 또한 보안성 측면에서 보완해야 할 점이 많다는 것이다. 본 논문에서는 다음 Fig. 6과 같이 데이터 자체에 전자서명을 포함하여 데이터 원본을 만들고 이를 캐싱한 후 데이터 요청이 들어오면 UDP로 데이터를 빠르게 전송하는 메커니즘을 사용한다.

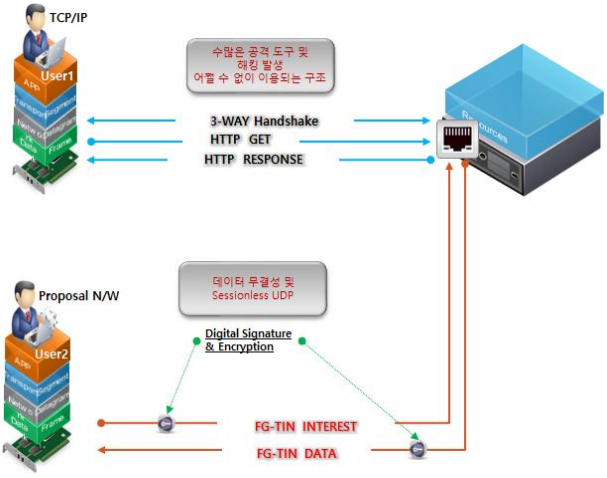

Fig. 6. FG-TIN Transaction

다만 기존의 TCP의 경우 데이터를 상대방이 수신했는지에 대한 확인이 가능한 반면 UDP의 경우는 수신 여부를 확인할 수 없으므로 별도의 재전송 메커니즘을 적용하여 단점을 보완해야 한다. 이 부분은 향후 추가적인 설계를 통해 보완하기로 하며 본 논문에서는 데이터의 수신이 명확하게 이루어진다고 가정하도록 한다.

5. Advanced Security

FG-TIN을 활용할 경우 다음과 같은 보안적인 특면의 장점을 얻을 수 있으며 이는 콘텐트 기반의 네트워크에서 제시한 장점을 그대로 활용할 수 있으므로 기존 네트워크에서 발생한 많은 문제점들을 보완할 수 있는 방안이라고 판단할 수 있다.

- 클라이언트 요청 후 응답 데이터를 응용 레벨로 암호화 및 전자서명 함으로써 인해 데이터 비밀성, 무결성 확보
- 중간 네트워크 장비에 포함된 키값을 통해 복호화 및 서명 검증이 가능함으로 강력한 보안 및 인증 가능
- 중간 네트워크 장비를 H/W뿐만이 아닌 S/W로도 구현 가능하여 PC나 모바일 단에 에이전트로 설치 가능한 확장성 지원
- 기존 인프라 환경 변화 없이 구성 가능하므로 현재 인터넷 환경에 바로 적용 가능
- 다만, 응용에 대한 다양성으로 인해 부하가 가중될 가능성 및 콘텐트의 다양성에 대한 추가 연구 필요

위에서 언급한 보안성 강화 방안 이외에도 DDoS 공격용 Flood 패킷들이 유입되어 네트워크 대역폭을 잠식하는 공격에 대해 보다 효율적인 방어가 가능하다. 즉 중간 네

트워크 장비는 모든 종류의 TCP/IP기반 Flood 패킷들을 전부 Garbage 및 Junk 패킷으로 분류/인식하여 해석하지 않고 즉각 차단이 가능하므로 DDoS 공격에도 매우 효과적이라고 할 수 있다.

IV. Simulation

1. Test System Architecture

본 논문에서 제안한 시스템인 FG-TIN을 시뮬레이션하기 위해 다름 Fig. 7과 같이 시스템을 구성하였다. PC단에는 중간 네트워크 장비 역할을 위해 라즈베리파이를 활용하여 리눅스 시스템을 설치한 후 FG-TIN 모듈을 탑재하여 TCP/IP통신과 FG-TIN통신을 연결하는 역할을 개발하였다. 또한 인터넷 대신 무선 AP를 이용하여 UDP통신을 통해 인터넷을 대신하도록 구성하였다. 마지막으로 서버 앞단에는 게이트웨이 장비에 FG-TIN을 개발하여 탑재하여 인터넷 구간에는 기존의 TCP/IP 대신 FG-TIN을 통해 통신이 이루어질 수 있도록 설계하였다.

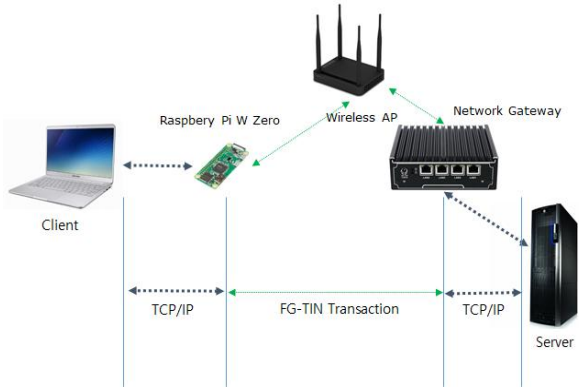

Fig. 7. FG-TIN Test System

이러한 구성을 통하여 본 논문에서는 HTTP 서비스와 SSH 서비스를 테스트하였으며 정상적으로 통신이 이루어짐을 확인하였다. Fig. 8은 PC에서 서버로의 ping을 통해 통신이 이루어지는 결과를 나태내고 있다.

본 논문에서 제시한 FG-TIN에는 콘텐트 기반의 캐싱 기능을 탑재하여 성능적인 측면에서 Table 1과 같이 FTP 프로토콜을 통해 데이터 전송을 측정한 결과 약 200%의 성능 개선을 확인할 수 있었다. 가각의 프로토콜에서 100Mb의 데이터를 10번 반목하여 전송하였고 이를 평균한 값을 구해서 측정하였다. FG-TIN의 경우 처음에는 TCP/IP와 비슷한 성능을 나타내었지만 두 번째 부터는 캐쉬된 내용을 처리하여 성능이 많이 개선된 것을 확인할 수 있었다. 하지만 이는 라즈베리파이의 하드웨어적인 성능 문제와 최적화되지 않은 모듈을 사용하여 성능 개선이 예상한 것 보다는 낮게 나왔다. 이처럼 캐싱을 활용할 경우 기존 전송 방식에 비해 더 높은 대역폭 활용 및 성능 개선을 기대할 수 있을 것으로 판단한다.

Table 1. Compare performance TCP/IP with FG-TIN

Protocol	Data	Iteration	Time(avg)
TCP/IP	100Mb	10	6.73sec
FG-TIN	100Mb	10	3.44sec

Table 2. TCP/IP vs FG-TIN

Items	TCP/IP	FG-TIN	Rem
Connection	each	Session-less	F*
Bandwidth	Normal	High	F
Caching	NA	Available	F
DDoS	NA	Protection	F
Data Security	NA	Supporting	F
Integrity	NA	Digital Signature	F
Vulnerability	Many	NA	F
Implement	Easy	Hard	T**
Performance	Normal	High	F

*FG-TIN, **TCP/IP

본 논문에서 비교한 항목으로는 Table 1의 각 항목에 표현한 바와 같이 세부적으로는 다음과 같으며 프로토콜을 평가하는 지표로 활용한다.

- Connection : 통신 대상간의 연결 방법
- Bandwidth : 대역폭의 활용도로 응용 프로그램을 통한 성능 지표 활용
- Caching : 데이터의 캐쉬 사용 여부
- Data Security : 데이터 원본에 대한 암호화 여부
- Integrity : 데이터 보존에 대한 무결성 적용 여부
- Vulnerability : 프로토콜에 대한 취약성 포함 여부
- Implement : 프로토콜 활용 및 구현 여부
- Performance : 프로토콜을 활용한 응용 성능 지표

또한 HTTP 프로토콜을 활용하여 임의의 파일에 전자서명을 넣어 데이터를 송수신하였으며 중간 네트워크 장비 자체가 전자서명을 직접 수행하지는 못했다. 이는 다음 연구에서 개발하여 추가할 예정이다. 하지만 콘텐트 자체의 전자서명을 통해 비밀성 및 무결성을 콘텐트 자체가 제공할 수 있다는 것을 확인할 수 있었다. 이러한 FG-TIN의 특징 및 장점을 Table 2와 같이 정리할 수 있으며 이는 TCP/IP의 기존 네트워크와 비교할 때 매우 우수한 차세대 네트워크라고 판단할 수 있다.

V. Conclusions

현재의 인터넷은 수 십 년간 현재의 인터넷을 이끌어 왔고 수많은 혜택을 제공했다고 해도 과언이 아니다. 하지만 나날이 발전하는 서비스와 사용자 증가 및 단말의 변화는 현재의 인터넷에 대한 새로운 요구를 하고 있다.

앞으로의 네트워크 서비스는 기존의 텍스트 및 이미지 중심에서 벗어나 비디오로 빠르게 변화하고 있고 향후 몇 년 안에 이러한 비디오 중심의 서비스는 전체 인터넷의 80~90% 이상을 차지할 것으로 전망하고 있다. 이러한 변화의 중심에 콘텐트 기반의 네트워크가 연구되고 있고 국내에서도 일부 연구 기관을 통해 연구되고 있다. 하지만 이러한 연구가 단지 논문 수준이 아닌 실제 개발로 이어지고 SW 정책적으로 설계되어야 할 것이다. 본 논문에서는 이러한 점을 부각하고자 콘텐트 기반의 네트워크에 대해 분석하고 이를 시뮬레이션 하였다.

현재까지 사용된 TCP/IP 기반으로는 수많은 보안 제품에도 불구하고 해커의 공격을 완전 차단할 수 없는 구조적 문제점을 가지고 있다. 더욱이 해킹 이후에 보완을 위해 단순 기능을 패치하는 보안체계로는 더 이상 안전하지 않고 오히려 추가적인 비용만 늘어나는 실정이다. 이를 극복하기 위해 새로운 패러다임의 적용으로 인해 기존 문제를 해결할 수 있는 가장 효율적인 방안이라고 판단한다. 보안에 대한 면역체계를 갖추어 해킹을 완전히 무력화할 수 있으며 대용량 트래픽의 성능적인 측면에서도 효과적이고 또한 비용절감을 가지고 올 수 있다고 판단한다.

이처럼 차세대 네트워크를 통한 새로운 서비스의 제공은 필수적인 요소로 국내에서도 차세대 네트워크에 대한 더 깊은 연구와 개발이 필요할 것으로 판단된다. 특히 SW 분야에 있어 네트워크 프로토콜 및 서비스와 결합된 정책이 선행되어야 할 것이며 이는 4차산업혁명 시대를 맞이하는 측면에서 무시해서는 안 될 중요한 요소라고 할 수 있으며 본 논문에서 제안한 FG-TIN이 이러한 국내의 차세대 네트워크의 연구에 일조할 수 있기를 바란다.

REFERENCES

[1] Van Jacobson, D. K. Smetters, James D. Thornton, Michael Plass, Nick Briggs, and Rebecca Braynard. Networking Named Content. In CoNext, 2009.

[2] Michael Meisel, Vasileios Pappas, and Lixia Zhang. Ad hoc networking via named data. In MobiArch'10. ACM, 2010. DOI: 10.1016/j.adhoc.2018.08.008

[3] Van Jacobson, D. K. Smetters, Nick Briggs, Michael Plass, Paul Stewart, James D. Thornton, and Rebecca Braynard. VoCCN: Voice-over Content-Centric Networks. In ReArch, 2009. DOI: 10.1145/1658978.1658980

[4] James Roberts. What QoS for the future internet? In The proceedings of FISS09, July 22, 2009.

[5] http://en.wikipedia.org/wiki/Named_data_networking

[6] Jae-Kyung Park, Strengthening Authentication Through Content Centric Networking, KSCI, Mar 24 2018.

[7] Jae-Kyung Park, A Network Translate System Using Next Generation Content Centric Networking Technology, KSCI, Mar 24 2018.

[8] Jae-Kyung Park, A Design of client BBS systems for Secure HVA, KSCI, Sep 21 2018.

[9] Michael Meisel, Vasileios Pappas, and Lixia Zhang. Ad hoc networking via named data. In MobiArch'10. ACM, 2010. DOI: 10.1145/1859983.1859986

[10] G. Loukas and G. Öke, "Protection against denial of service attacks: a survey," The Computer Journal, vol. 53, pp. 1020-1037, 2010. DOI: 10.1093/comjnl/bxp078

[13] M. Li, J. Li, and W. Zhao, "Simulation study of flood attacking of DDOS," in Proc of International Conference on Internet Computing in Science and Engineering 2008, pp. 286-293. DOI: 10.1109/icicse.2008.14

[14] W. Liu, "Research on DoS attack and detection programming," in Proc. of Third International Symposium on Intelligent Information Technology Application 2009, pp. 207-210. DOI: 10.1109/iita.2009.165

[15] J. Nazario, "DDoS attack evolution," Network Security, vol. 2008, pp. 7-10, 2008. DOI: 10.1016/s1353-4858(08)70086-2

[16] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, "Detecting DNS amplification attacks," in Critical Information Infrastructures Security, ed: Springer, 2008, pp. 185-196. DOI: 10.1007/978-3-540-89173-4_16

[17] M.-J. Chen, K.-P. Chien, C.-Y. Huang, B.-C. Cheng, and Y.-S. Chu, "An ASIC for SMTP Intrusion Prevention System," in Proc. of IEEE International Symposium on Circuits and Systems 2009, pp. 1847-1850. DOI: 10.1109/iscas.2009.5118138

[18] F. Huici, S. Niccolini, and N. d'Heureuse, "Protecting SIP against very large flooding DoS attacks," in Proc. of Global Telecommunications Conference 2009, pp. 1-6. DOI: 10.1109/glocom.2009.5425524

[19] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Communications, vol. 31, pp. 4212-4219, 2008. DOI: 10.1016/j.comcom.2008.09.018

[20] Van J., et al, "Networking Named Content", SIGCOMM Conference, 2009

[21] Hyung-Su Lee, Jae-Pyo Park, Jae-Kyung Park, "A Network Transport System Using Next Generation CCN Technology," Journal of The Korea Society of Computer and Information, Vol. 22, No. 10, pp. 93-100, Oct. 2017.

[22] Jae-Kyung Park, Won Joo Lee, Kang-Ho Lee, "A Study on the Isolated Cloud Security Using Next Generation Network" Journal of The Korea Society of Computer and Information Vol. 22 No. 11, pp. 41-48, November 2017.

[23] Sung-Jin Kim, Jae-Kyung Park, "Strengthening Authentication Through Content Centric Networking" Journal of The Korea Society of Computer and Information Vol. 22 No. 4, pp. 75-82, April 2017.

[24] Hyung-Su Lee, Jae-Pyo Park, Jae-Kyung Park, "A Network Transport System Using Next Generation CCN Technology" Journal of The Korea Society of Computer and Information Vol. 22 No. 10, pp. 93-100, October 2017.

Authors

Jae-Kyung Park 1993: BS, Department of Computer Engineering, Dongguk University 1996: MS, Department of Computer Science, Hongik University 2002: PhD, Department of Computer Science, Hongik University.

Dr. Park joined the faculty Department of Information Security at Korea Polytechnics, Seoul, Korea, In 2015. He is currently a Professor in Department of Information Security at Korea Polytechnics, Seoul, Korea. He is interested in Network security, cyber security.

Hyung-Su Lee: 1991: BS, Electronic Engineering, SungKyunKwan University 2011: MS, Department of Computer Engineering, SoongSil University 2014: Doctorate, Department of Computer Engineering.

Dr. Lee joined the faculty Department of Information Security at Korea Polytechnics, Seoul, Korea, In 2016. He is currently a Professor in Department of Information Security at Korea Polytechnics, Seoul, Korea. He is interested in Network security, cyber security and information communication.

Young-Ja Kim 1993: BS, Department of Computer Engineering, Kunsan National University 1998: MS, Department of Computer Education, Sunchon National University 2007: PhD, Department of Computer Engineering, Kunsan National. Dr. Kim joined the faculty Department of Data Analysis at Korea Polytechnics, Seoul, Korea, In 2002. He is currently a Professor in Department of Information Security at Korea Polytechnics, Seoul, Korea. She is interested in Network security, cyber security and information communication.