Journal of The Korea Society of Computer and Information
Vol. 22 No. 10, pp. 93-100, October 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.10.093

A Network Transport System Using Next Generation CCN Technology

Hyung-Su Lee*, Jae-Pyo Park**, Jae-Kyung Park***

Abstract

Current internet has evolved from the sharing and efficiency aspects of information, it is still vulnerable to the fact that the Internet is not secure in terms of security and is not safe to secure of security mechanism. Repeating patches on continuous hacking are continuously demanding additional resources for network or system equipment, and consequently the costs continue to increase. Businesses and individuals alike are speeding up the damage caused by crime like of ransomware, not jusy simple attacks, and businesses and individuals need to respond to cyber security. In addition, the ongoing introduce of security device, and separate of networks for secure transmission of contents in the existing TCP/IP system, but it is still lacking in security. To complement the security implications of this existing TCP/IP Internet Protocol, we intend to propose a Secure Contents Transport System (SCTS) on the network using the CCN concept.

▸Keyword: Network Transport, CCN, network security, contents, next-generation network

I. Introduction

현재인터넷은 단순히 정보의 공유 및 효율적인 측면에서 진화해왔지만, 현재 사용하고 있는 인터넷 표준 프로토콜이 보안 측면에서 그 자체로 안전하지 못하여 별도의 보안 메커니즘들을 적용하고 있지만, 그럼에도 불구하고 인터넷은 여전히 취약한 것이 사실이다. 지속되는 해킹에 따라 반복되는 패치작업과 새로이 발견되는 위협들에 대한 추가 보안 메커니즘들을 적용하는 체계는 부수적인 네트워크나 시스템 장비를 과다하게 요구하고 있으며 이에 따른 비용도 지속적으로 증가 있다. 최근들어 단순한 공격방식이 아닌 랜섬웨어와 같은 범죄로 인한 피해가 가속화되고 있어 기업뿐만 아니라 개인에게도 사이버 보안에 대한 대응 방안들을 마련하여야 하는 상황이다.

또한, 스마트폰과 IoT기기들의 폭발적인 증가에 따라 요구되어 지는 콘텐츠들에 대한 관리의 필요성이 점차 증가해가고 있다. 현재의 인터넷에서 콘텐츠를 전송 방법은 데이터가 무엇이든 상관없이 송수신 호스트의 IP 주소를 이용하여 서비스를 제공하므로 콘텐츠를 보유하고 있는 시스템의 위치가 인터넷상에 노출되어 있어서 항상 외부로부터의 위협을 받고 있다고 할 수 있다. 이에 따라 콘텐츠를 제공해야하는 시스템 및 서비스들은 인터넷의 위협으로부터 보다 안전한 환경을 구현하여 전송되는 콘텐츠에 대한 신뢰성을 확보하기 위한 많은 노력을 기울이고 있다. 이를 위해 기존의 복잡한 구조와 사이버 공격 및 해킹에 쉽게 노출되는 TCP/IP 체계의 현재 인터넷 체계에서는 네트워크 장비 및 콘텐츠 제공 서버들의 확충과 더불어, 현재 지속적으로 진행되고 있는 보안의 문제를 해결하기 위한 방편으로 보안장비 도입, 망 분리 등의 대책을 마련하여 보완하고 있지만 여전히 보안 측면에서는 미흡한 것이 현실이다. 이러한 기존 인터넷 체계의 문제점들을 보완하고 근본적인 대안을 제시하기 위해 CCN개념을 활용한 안전한 콘텐츠 전송 시스템(SCTS : Secure Contents Transport System)을 제안하고자 한다. 이러한 SCTS를 이용할 경우 보안뿐만 아니라 CCN의 특

• First Author: Hyung-Su Lee, Corresponding Author: Jae-Kyung Park
*Hyung-Su Lee (hyungsu.lee@gmail.com), Department of Computer, Graduate School, SoongSil University
**Jae-Pyo Park (pjerry@ssu.ac.kr), Graduate School of Information Science, SoongSil University
***Jae-Kyung Park (jakypark@kopo.ac.kr), Dept. of Information Security, SeoulGangseoCampus, Korea Polytechnics
• Received: 2017. 09. 04, Revised: 2017. 09. 25, Accepted: 2017. 10. 19.

징인 데이터의 캐쉬 기능을 최대한 활용함에 따라 서버의 증설 효과를 가져올 수 있다. 즉, 서버의 데이터를 SCTS에 캐쉬함으로 인해 대역폭을 늘리거나 서버를 증설하지 않고도 기존의 서비스를 훨씬 더 빠르게 수행할 수 있다. 이는 CCN의 기본 기능을 최대한 활용하면서 보안 개념을 추가하여 안정적이면서도 빠른 서비스를 제공할 수 있음을 의미한다.

본 논문에서는 기존 TCP/IP 체계의 문제점을 극복하고자 고안된 여러 차세대 네트워크들 중에서 CCN (Content Centric Networking)기술을 이용하여 현재 인터넷의 근본적 보안 취약점인 호스트 중심에서 벗어나 콘텐츠를 기반으로 하는 새로운 차세대 네트워킹 아키텍처를 활용하고자 한다. 즉, 인터넷에 접속되는 기기들끼리 상호 연결하는 데이터 채널을 제공하고, 해당 채널을 보호하는 최근 40여 년간의 인터넷 프로토콜 방식 대신에 네트워크 단에서 콘텐츠를 사용자에게 안전하고 빠르게 제공하고자 하는 기술로, 콘텐츠를 보유하고 있는 서버의 IP 노출에 따른 인터넷으로 부터의 위협을 방지하고, 보안이 적용된 안전한 채널을 통해 사용자에게 원하는 콘텐츠를 전달해 줄 수 있는 신뢰성 있는 시스템을 구현하고자 한다. 이를 위해 2장에서는 관련된 연구를 살펴보고, 3장에서는 CCN을 적용한 SCTS 모델을 제시하며, 4장에서는 프로토타입에 대한 검증을 실시하고 5장에서 결론을 제시한다.

II. Literature Review

1. Security Issues of TCP/IP

1.1 Scalability problem

1969년 미국의 국방성 주도 하에 이루어진 네트워크 시험 ARPANET은 단지 4개로 컴퓨터를 연결한 것이었으나 현재는 거의 모든 전 세계의 서버를 비롯한 호스트 컴퓨터가 연결되어 있는 상황이며 그 사용자의 수가 20억 명을 넘고 하루 평균 수천만 명 이상이 인터넷에 접속하고 있는 것으로 예측될 정도로 급속도로 확산되고 있다[1][2][3]. 이로 인해 트래픽 엔지니어링, 멀티호밍 등으로 라우팅 테이블의 크기가 상상이상의 기하급수적으로 증가하고 있다. 앞으로도 인터넷 대역폭은 100배 이상 증가하고 사물인터넷의 도입 및 활용에 따라 센서와 같은 작은 엔티티의 폭발적인 증가의 이유 때문으로 네트워크 자체의 복잡도가 커질 것으로 예상되어 현 네트워크의 확장성 부족은 인터넷이 갖고 있는 가장 큰 문제점[4]이며 보안도 매우 취약한 것으로 나타나고 있다.

1.2 Mobility problem

몇 대의 컴퓨터를 서로 연결하여 케이블 형태로 이용하기 시작한 인터넷은 점점 그 활용이 확대 보급되면서 수많은 컴퓨터 및 서버들이 다양한 케이블들로 서로 연결되었고 무선을 포함하여 복잡한 구조를 띄게 되었다[5][6]. 이러한 환경에서는 네트워크 환경에서 단말이 이동하거나 하는 일이 발생하지 않기 때문에 단말의 위치를 반영하는 IP 주소 체계를 통해 효율적인 서비스 전달을 구현할 수 있었다[7]. 하지만 스마트폰, 패드, 노트북 등 이동성을 지닌 휴대 단말 기기들이 등장하고 이러한 기기들을 통한 인터넷 서비스가 시작되면서 이동 단말들은 메시지를 받고 있는 중에도 물리적인 위치를 변경하는 경우가 빈번히 발생하게 되었다[5]. 현재의 IP 주소 체계에서는 이러한 단말이 통신 중에 다른 위치로 이동을 할 경우, 인터넷은 단말의 IP 체계상의 이동을 실시간으로 확인할 수 없기 때문에 더 이상 IP 통신이 불가능해진다. 이와 같이 단말의 물리적인 이동으로 인해 발생하는 메시지 전달의 불연속성을 근본적으로 해결하고자 인터넷의 단말에 대한 이동성에 대한 연구가 시작되었다[6]. 이와 같은 인터넷에서의 단말의 이동성은 이동단말의 위치 관리 및 위치변경 중에도 네트워크 서비스의 연속성 보장을 위한 통신 메커니즘 전부를 포함한다.

1.3 Diversity problem

인터넷은 지난 40여 년간 유선망을 기반으로 하여 네트워크를 효율적으로 전달할 수 있도록 수정 및 추가 개발되어 왔다. 통신 서비스의 목적지까지 최적의 네트워크 경로를 찾는 방법 즉, 라우팅은 신뢰성 있는 통신을 위한 전달 방법, 링크 사용의 효율성을 고려한 알고리즘 등의 모든 인터넷 기술들이 유선망의 특징을 바탕으로 설계되고 개발되었으며 이를 보안에 대한 근본적인 대책이 없이 사용되어 왔다. 최근 들어 다양한 무선기기들 및 특히 스마트폰 등이 무선망 기술들을 전체 유선 인터넷으로 통합시키는 노력이 진행되면서 기존의 IP환경의 인터넷 기술들에 대한 근본적인 고찰이 필요하게 되었다[8]. 인터넷을 구성하던 단말들이 기존의 PC, 서버 및 라우터 등에서 보다 이동성 및 활용성이 뛰어난 휴대용 기기들로 확장되고, 초고속으로 서비스 데이터(LTE, 5G 등)를 전송할 수 있으며 전송 서비스 중 데이터 손실이 적은 유선망에서 상대적으로 저속으로 데이터를 전송하고 전송 서비스 중 데이터 손실률이 높으며 전송거리가 제한적인 여러 무선망들로 확장되면서, 기존의 인터넷 기술들 역시 이와 같은 이종 기기 및 네트워크들의 특성을 보다 다양하게 고려할 수 있도록 하는 연구 및 보안에 대한 해결 연구가 반드시 필요하게 되었다.

1.4 Security problem

보안성은 모든 종류의 통신에 있어서 중요시되고 있는 문제이다. 인터넷 역시 개발된 이래로 많은 보안 공격을 경험하였고, 이에 대한 해결책을 제시하여 왔다[9][10]. 다른 사용자들의 통신을 도청하거나 단말들에 불법적인 접근을 하여 정보를 조작하는 무결성 위반이나, 특히 특정 단말이나 망이 제대로 동작하지 못하도록 만드는 서비스거부공격 등의 공격들이 인터넷 기술상의 취약점을 활용한 허점을 이용하여 이루어져 왔다. 이러한 취약성 공격이 있을 때마다 기존 인터넷은 보안을 고려한 새로운 기본 기술을 제시하기 보단 현재의 기본 기술은 그대로 두고 때

우기 식의 보안을 위한 메커니즘을 계속 추가하는 방향으로 보안 문제를 해결하여 왔다. 이와 같은 방법은 취약성에 대한 보안성을 얻는 대신 전송 효율성 측면을 악화시켰고, 이는 개발된 보안 기술들의 적용에 있어 막대한 유지보수 비용을 양산하는 걸림돌이 되어 왔다. 전송 효율성 문제는 제한적인 자원의 특정 무선기기 및 네트워크들이 인터넷에 통합되면서부터 더욱 부각되고 있다[11]. 또한 무선기기 및 네트워크의 제한된 특성은 취약성 보안 공격을 더욱 쉽게 만든 반면 기전의 유선망에서 사용해 왔던 보안 대책들을 적용시키기 어렵도록 하였다. 따라서 무선으로의 인터넷 영역의 확장은 기존의 인터넷 보안성을 강화하는 측면에서 더욱 근본적인 접근을 요구하고 있다.

2. CCN(Contents Centric Network)

1990년 초 웹 서비스의 등장과 글로벌 시대를 이끈 인터넷의 세계적인 확산으로 네트워크에 대한 새로운 시대의 요구가 되었다. 그러나 지금의 인터넷은 시대적 요구를 수용하기에는 보안적인 측면에서 근본 구조에 문제가 제기되고 있어, 새로운 개념의 혁신적 접근의 차세대 미래인터넷에 대한 연구가 진행되고 있으며 국내에서도 이에 대한 연구가 필요하다. 본 장에서는 이러한 차세대 미래인터넷 연구 기술의 하나인 콘텐츠 중심의 네트워킹 기술에 대해 살펴보도록 한다[12].

콘텐츠 중심의 네트워크는 현재 대용량의 대역폭을 사용하는 데이터 서비스에 대해 IP 주소체계의 단점을 극복하여 보다 콘텐츠 중심의 전송 방식을 제공함으로써 더 빠르고 안전한 서비스를 제공하고자 하는 기술로[1][12][13], 기존 위치 중심인 IP 체계를 콘텐츠 중심의 네트워크 체계로 구현하여 안전한 콘텐츠 전송능력을 향상시키고 보다 강화된 보안체계를 제공하여 서비스 및 보안을 획기적으로 개선한 새로운 개념의 차세대 네트워크이다. CCN은 특정한 인증 이름 규칙을 콘텐츠에 부여하여 IP가 없이도 콘텐츠의 내용으로 데이터를 처리할 수 있는 메커니즘으로[12] [Fig. 1]과 같이 구성이 된다.

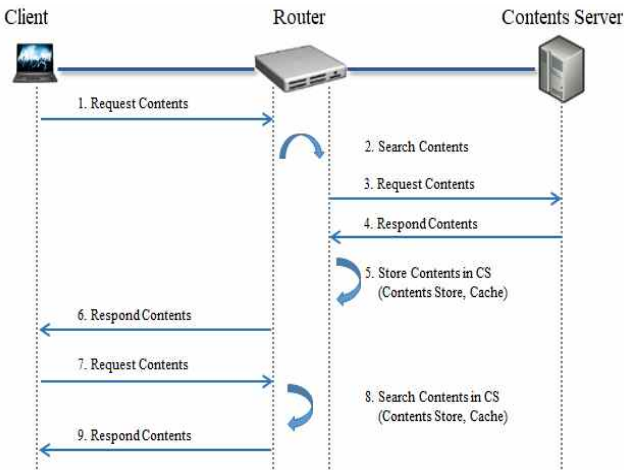

Fig. 1. CCN's Connection process

CCN을 이용할 경우 서비스 요청자 또는 악의적인 공격자는 콘텐츠 서버에 접근자체가 불가하여 서버의 운영체제, 웹 서비스, 응용 서비스 등을 전혀 알 수 없다. 공격자가 요청을 통해 콘텐츠를 받을 수는 있으나 이는 콘텐츠 저장소에 저장된 캐시 내용을 받는 것이며 이러한 데이터 서비스 또한 정상적인 인증을 해결해야만 받을 수 있는 개념이다[12][14][15].

CCN은 기존 TCP/IP의 질의 & 응답 메시지를 사용하지 않고, 별도의 요청(Interest) 메시지와 응답(Data) 메시지를 정의하고 있다. 요청 메세지은 사용자가 원하는 콘텐츠의 정보를 나타내며 응답 메세지은 Interest에서 요청한 콘텐츠와 인증과 관련된 정보들이 포함되어 있다. [Fig. 2]는 CCN에서 사용하는 메시지들의 구조이다.[12]

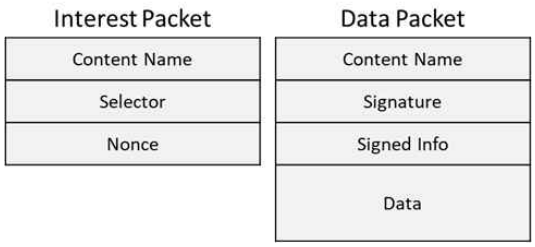

Fig. 2. CCN's Interest & Data Packet

현재 인터넷 데이터 서비스의 규모는 매우 빠르게 증가하고 있다. IDC가 예측하는 인터넷 사용 인구와 데이터는 계속 증가하는 추세이다[16][17][18]. 또한, 데이터 서비스의 양은 2006년 161 Exabytes에서 2010년 988 Exabytes로 전체 약 6배 증가함을 알 수 있다. 현재 인터넷 서비스는 웹 서비스와 같이 대량의 사용자가 동일하게 요구하고 처리되는 서비스의 데이터라는 특징을 가진다. 이에 비해, 데이터 전송 방법은 데이터가 무엇이든 송수신 호스트의 IP를 이용하여 서비스를 제공하므로 동일한 데이터들이 네트워크상에 사용자 수만큼 전송되는 방식으로 매우 비효율적으로 운영되는 방식이다. 이러한 데이터 전송의 비효율성을 피하여 콘텐츠 중심 기술은 데이터 배포의 개념을 도입하여 사용한다. 즉, 인터넷의 IP 주소를 전혀 사용하지 않고 대신, 데이터의 이름을 활용하여 네트워크에서 데이터 전달을 수행한다. 또한, 데이터 전송 채널과 데이터 저장소를 보안하는 종래의 보안 방식에서 벗어나, 데이터 자체를 보안하는 새로운 방식으로 설계되었다.

III. Main Subject

본 논문에서 제안하는 SCTS는 다양한 위험요소들을 근본적으로 해결하기 위한 새로운 방식의 접근으로 네트워크 패러다임 자체를 미래 지향적 차세대 인터넷 패러다임인 CCN을 활용한 새로운 콘텐츠 전송 시스템이다. 현재뿐만 아니라 향후에도 콘텐츠와 서비스는 인터넷의 핵심으로 보안은 반드시 적용해야

할 필수 요소이다. 본 논문에서는 기존의 TCP/IP의 단점으로 나타난 보안의 문제를 어떻게 근본적으로 해결할 것인가에 대한 대안으로 차세대 네트워크인 CCN을 활용하여 TCP/IP의 단점을 극복하고자 한다.

CCN은 TCP/IP의 문제점들을 해결하기 위해 진행되고 있는 차세대 인터넷 연구들 중에 콘텐츠 자체의 이름을 이용하여(named data) 네트워크 단에서의 라우팅(route by name)과 네트워크 스위치에서의 캐싱(in-network caching)을 가능하게 함으로써 많은 사용자가 원하는 콘텐츠를 가장 가까운 곳에서 안전하고 빠르게 가져오도록 하는 정의 된 프로토콜로, 많은 경우 그 수요가 가변적이며 예측이 불가능한 고용량 콘텐츠에 대한 요청이 하나의 서버에 집중되는 것을 효과적으로 분산시켜서, 가용한 네트워크의 획기적인 용량 증대와 사용자의 콘텐츠 접근시간 (content download 혹은 access delay)에 대한 단축 효과를 얻을 수 있다.

이러한 CCN 프로토콜을 활용하여 새로운 콘텐츠 전송시스템을 제안하고, 프로토타입으로 구현하여 실험으로 증명하고자 한다. SCTS는 내부적으로 CCN 프로토콜을 사용하므로 TCP/IP 공격 자체가 무의미하도록 서로 다른 통신을 사용함으로 TCP/IP의 문제를 근본적으로 해결하고자 한다. 또한 TCP/IP와의 호환성을 지원하도록 하여, 기존의 TCP/IP 네트워크상에서 안전적인 콘텐츠 전송이 이루어 질 수 있도록 하였다.

1. System Concept

본 논문에서 제안하는 안전한 콘텐츠 전송 시스템의 개념으로 [Fig. 3]과 같이 제안하며, TCP/IP 호환 CCN 통신, 사용자 인증, 콘텐츠 요청 및 전달 등의 TCP/IP 네트워크 상에서 안전한 콘텐츠를 전달하기 위한 시스템 설계를 목표로 한다.

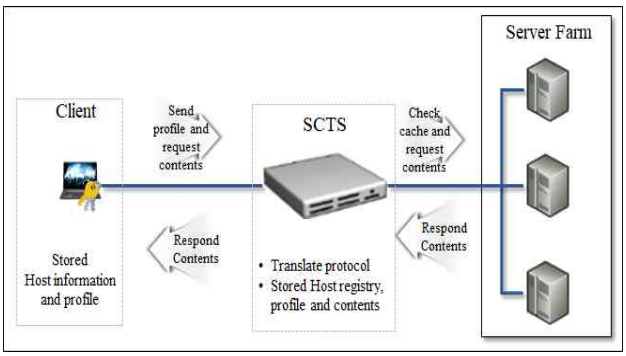

Fig. 3. Target System of SCTS

안전한 콘텐츠 전달을 위해 클라이언트에 SCTS와 통신을 위한 전용 프로그램이 설치되어 SCTS와의 정보교환 및 CCN이 적용된 암호화 통신을 수행하도록 한다. 클라이언트에서 SCTS에 콘텐츠를 요청할 경우 사용자의 프로파일과 필요로 하는 콘텐츠의 정보를 생성하여 SCTS에 전달하도록 한다. SCTS에서는 사용자의 프로파일을 확인하여 요청하는 콘텐츠에 대한 권한에 따라 콘텐츠의 전달 또는 거부를 확인할 수 있도록 각 사용자별 프로파일을 관리하도록 한다. 또한, SCTS 내부의 캐쉬 공간에 사용자가 요청한 콘텐츠가 존재하지 않는 경우 내부 서버팜에서 해당되는 콘텐츠를 요청하여 캐쉬 공간에 저장하고 클라이언트에 전달하도록 한다. 이때, 클라이언트에서 요청하는 패킷은 SCTS에 의해서 요청 내용을 분석만 하며 내부 서버팜에 직접적인 패킷의 전달은 허용하지 않는다. 즉, SCTS의 콘텐츠 관리 메카니즘에 의해 캐쉬와 서버팜의 통신만 가능하며, 클라이언트와의 통신은 캐쉬 공간의 내용에 대해서만 서비스가 되도록 한다.

2. System Structure

[Fig. 4]는 본 논문에서 제안한 SCTS의 시스템 구성을 나타내고 있다. 기존의 통신 방법인 TCP/IP와 내부망을 연결하기 위해 아웃바운드에서는 TCP/IP를 그대로 받아서 처리하는 호환 메커니즘을 제공한다. 아웃바운드에서 수신한 패킷은 SCTS 내부에서 프로토콜 변환모듈을 통해 CCN 프로토콜로 변환하도록 한다. 또한, SCTS에서 보호하고 있는 콘텐츠에 대한 권한을 각 사용자들에 대한 프로파일에 설정하여 클라이언트 사용자의 권한에 따라 요청하는 콘텐츠의 전달여부를 결정하게 된다.

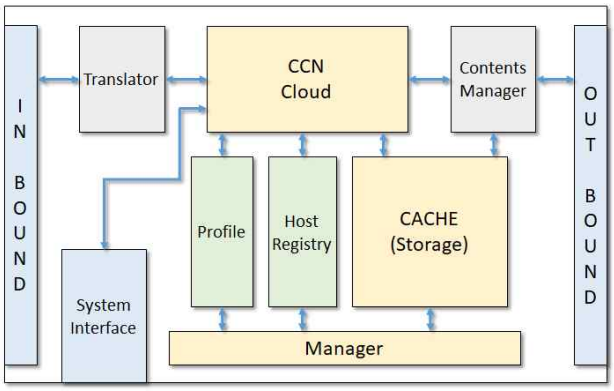

Fig. 4. System Diagram

호스트 레지스트리는 콘텐츠를 보유하고 있는 서버들에 대한 정보를 보유하고 있으며, 클라이언트에서 요청한 콘텐츠에 대한 정보에서 서버의 정보를 분리하여 호스트 레지스트리의 정보를 비교하도록 한다. 콘텐츠에 대한 사용자의 권한을 관리하는 프로파일에는 내부 서버 및 콘텐츠에 대한 생성과 관련된 권한을 보유하고 있는 특정 사용자를 관리하도록 하며, 일반 사용들의 경우 내부 서버로의 직접적인 접근은 원천적으로 불가하며, 캐쉬공간에 존재하는 콘텐츠에 대해 읽기 권한만 허용한다. 캐쉬공간에 대한 관리는 CCN의 메커니즘을 그대로 적용한다. 다만, 콘텐츠를 생성할 수 있는 권한을 갖는 사용자에 의해 내부 서버로 전달되는 콘텐츠에 대한 안정성을 확보하기 위하여 악성코드 분석 시스템과 연동할 수 있도록 추가적인 인터페이스를 제공한다.

SCTS 구조 및 내부 핵심은 일반적으로 알려진 것이 아니다. 예를 들면 기존 인터넷과 호환하기 위해 제공되는 IP 주소, IP

프로토콜, IP 포트 등에 대해서도 외부에는 공개되지 않으며 다만 외부와 호환을 위해서 TCP/IP 대표 IP만 공개되며, 내부 데이터 전송은 강력한 데이터 암호화 및 보안이 사용된다.

SCTS의 동작은 [Fig. 5]과 같이 이루어진다. 클라이언트에 SCTS와 통신하기 위한 추가적인 프로그램이 설치되고, 프로그램 실행을 위해 사용자 정보를 입력하도록 한다. 일반 사용자의 경우 공유되는 게스트 계정을 사용하도록 하며 이 경우 별도의 사용자에 대한 정보를 입력하지 않는다. 컨텐츠를 생성할 수 있는 권한을 갖는 사용자의 경우 자신의 정보를 입력하여 SCTS의 프로파일 모듈로부터 승인을 받고 특정권한들이 부여된 프로파일을 받아 향후 SCTS와의 통신 시 권한과 관련된 프로파일 전송에 사용하도록 한다.

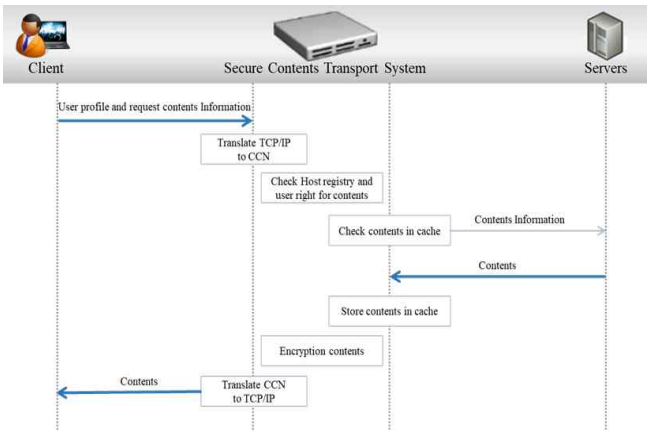

Fig. 5. Operating Flow

클라이언트에서 콘텐츠가 필요로 하는 경우 사용자의 프로파일과 필요로 하는 콘텐츠의 정보를 SCTS에게 전달한다. 이때 SCTS에 전달하는 패킷을 클라이언트 모듈에 의해 CCN 프로콜 변환 및 암호화 되며, 암호화된 내용은 UDP 프로토콜로 캡슐화되어 전달한다. SCTS에서는 수신된 패킷을 CCN 프로토콜로 변환하여 클라이언트가 요청한 내용을 복호화하여 사용자의 프로파일, 서버정보, 요청하는 콘텐츠 정보로 분리한다. 클라이언트가 요청한 콘텐츠를 보유하고 있는 서버가 내부에 존재하는지를 체크하기 위해 호스트 레지스트리 정보를 검색하여 클라이언트에서 전달된 서버정보가 존재하는지 체크한다. 서버정보가 정상적인 경우 사용자가 요청하는 콘텐츠가 캐쉬공간에 보유하고 있는지 확인하게 된다. 캐쉬공간에 콘텐츠가 있는 경우 사용자의 프로파일에 대한 권한을 확인하여 콘텐츠에 대한 접근 권한을 보유한 경우 콘텐츠를 암호화 하여 UDP 프로토콜로 캡슐화 하여 클라이언트에게 전달하도록 한다.

클라이언트가 요청한 콘텐츠가 캐쉬공간에 존재하지 않는 경우 SCTS는 CCN프로토콜을 이용하여 내부 서버에 콘텐츠를 요청하는 패킷을 보내게 된다. 콘텐츠를 보유하고 있는 내부 서버에서 전달받은 콘텐츠는 캐쉬공간에 저장 후 클라이언트에 전송하는 절차를 따르게 된다.

3. SCTS vs. TCP/IP

3.1 System efficiency aspects

기존 TCP/IP 방식의 네트워크는 콘텐츠를 전송하는데 있어 Host-to-Host 방식으로 지원이 되므로 많은 대역폭 및 비효율적인 구조를 가지고 있다. 하지만, [Fig. 3]와 같이 SCTS의 경우 CCN 매커니즘을 이용하여 콘텐츠를 캐쉬하여 서버에 부하를 최소화할 수 있는 구조이다.

동일한 콘텐츠에 대해서 또 다른 클라이언트가 요청하는 경우 SCTS는 내부 서버에 접근하지 않고, 캐쉬된 콘텐츠를 클라이언트에게 바로 전달할 수 있으며 반응시간도 최소화할 수 있는 장점을 가진다. 또한 이를 통해 응용 서버 및 DB 서버의 스토리지를 대폭 절감할 수 있으며 이는 대규모의 투자비 절약을 이끌 어 낼 수 있다.

또한, SCTS 내부는 IP와 같은 내부서버에 대한 정보를 외부에 노출하지 않으며, 외부에서 내부서버에 직접적인 접근이 불가하여 TCP/IP 상에서 진행되는 기존의 공격방식은 전혀 통하지 않는 면역지역을 만들 수 있다.

3.2 Functional comparison

[Table 1]에서 보는 바와 같이 기존 TCP/IP의 단점을 SCTS를 통해 많은 부분을 극복할 수 있다. 특히 보안 측면에서는 CCN의 특성상 콘텐츠가 없으면 서비스를 하지 않는 특성을 이용하여 DDoS와 같은 공격은 전면적으로 차단이 가능한 큰 장점을 가질 수 있다.

Table 1. Comparison TCP/IP vs. SCTS

Subject	TCP/IP	SCTS(CCN)	note
Connection	Session	None	SCTS
Cache	None	Use	SCTS
DDoS Attack	Defensibility	Unable to connect	SCTS
Security	3rd party	Encryption	SCTS
Integrity	3rd party	PKI support	SCTS
Vulnerability	Majority presence	No IP, no existing vulnerability	SCTS
Implementation	Easy	Difficulty	TCP/IP
Performance	Normal	High (cache)	SCTS

IV. Test and verification

본 논문에서 제안하고자 하는 SCTS는 기존의 TCP/IP 문제

점을 개선하기 위해 새로운 네트워크인 CCN을 활용하여 기존 보안 문제를 해결할 수 있음을 제안하였고 프로토타입을 통해 공격을 차단하는 것을 검증하고자 한다. 기존 및 신규 종류의 DDoS 공격 등이 CCN 기반의 SCTS에서 무력해 지는 실험을 진행하였으며, 테스트 환경은 [Fig. 6]와 같이 구성하였다.

Fig. 6. Test configure

SCTS의 내부에 CCNx 프로토콜을 설치한 리눅스 서버로 구축하고 웹 서비스와 텔넷 서비스를 사용할 수 있도록 하였다. 클라이언트는 윈도우 10을 사용하였으며, 공격을 위해 칼리 리눅스 가상머신을 추가로 사용하였다.

테스트는 클라이언트에서 내부 서버로 웹 통신 및 콘텐츠 요청이 정상적으로 수행되는지를 확인하고 DDoS 공격에 대한 대응이 정상적으로 이루어지고 있는지 테스트를 진행 한 이후에 정상적인 콘텐츠 요청 및 DDoS 공격을 동시에 수행하여 SCTS에서 패킷의 처리 상태를 확인하였다.

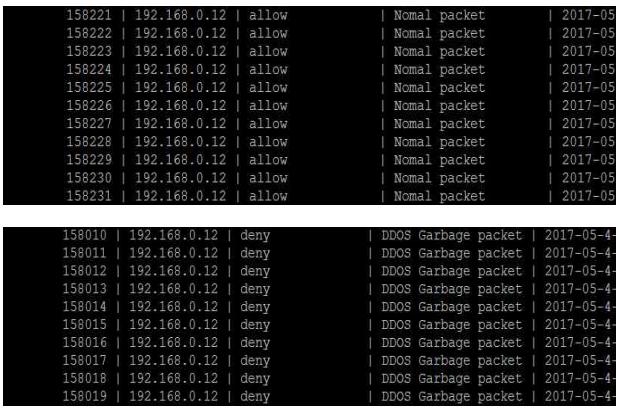

Fig. 7. Normal and DDoS attack test

[Fig. 7]에서 보는 바와 같이 SCTS에서 클라이언트의 요청에 따른 정상적인 콘텐츠 요청과 비정상적인 DDoS 공격에 대한 정상적인 대응을 하고 있는 것을 알 수 있다.

다음의 [Fig. 8]은 공격자가 지속적으로 DDoS 공격을 수행하는 중에 클라이언트에서 정상적인 콘텐츠 요청을 하는 경우 SCTS에서 패킷의 종류에 따라 어떻게 동작하는지를 확인할 수 있다. DDoS 공격의 경우 결과 확인을 위해 초당 10만 패킷을 생성하도록 제한하여 진행하였다.

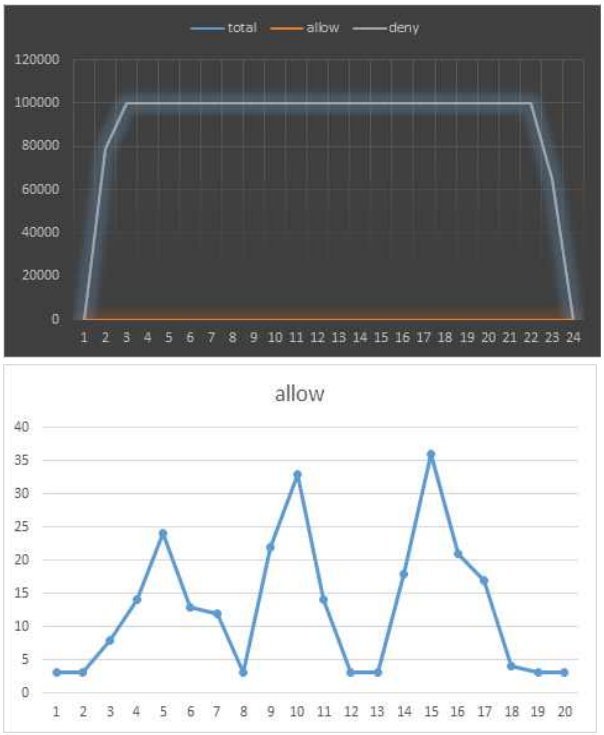

Fig. 8. Packet status

[Fig. 8]에서 보는것과 같이 클라이언트와 내부서버와의 정상적인 콘텐츠 요청에 대한 패킷들은 SCTS에 의해 정상적으로 처리가 되어 서비스를 받고 있지만, DDoS 공격의 경우 프로토콜 확인, 사용자 프로파일, 호스트 레지스트리 확인 등을 통해 비정상적인 패킷으로 구분하여 모두 거부되고 있는 것을 확인할 수 있었다.

V. Conclusions

본 논문에서는 TCP/IP의 보안상 문제점을 파악하고 이를 근본적으로 해결하기 위한 SCTS 시스템을 제안하였다. SCTS는 내부적으로 CCN 프로토콜을 사용하므로 기존의 TCP/IP의 보안상 취약점이 전혀 통용되지 않는 별도의 프로토콜을 사용한다. 또한 이러한 SCTS를 현재의 인터넷 환경과 연결하기 위하여 TCP/IP 호환이 가능한 기능을 지원하였다. 추가적으로 현재 인터넷의 보안상 중요한 부분인 DDoS 공격, 미라이공격 등을 막기 위해 내부적으로 콘텐츠를 처리할 수 있는 엔진을 설계하여 실험하였다. 이러한 SCTS를 통해 현재의 인터넷에 즉, TCP/IP 환경에서 발생할 수 있는 보안의 문제를 근본적인 입장에서 해결 가능하다는 점을 실험을 통해 증명하였다.

하지만, 본 논문에서 제안한 SCTS는 내부 네트워크가 반드시 CCN으로 연결되어야 하며, Client에 별도의 솔루션이 설치되어야 한다는 단점이 있다. 이는 SCTS를 활용하기 위해서는

기존의 TCP/IP 환경을 CCN으로 변경하여야 하므로 사이트에 바로 적용할 수 없다는 문제점이 있다. 따라서 향후 추가적인 연구에서는 현재 TCP/IP 환경에서 바로 적용이 가능하도록 프로토콜 전환 및 추가적인 보안 방안에 대한 연구를 통해 기존 네트워크 환경에 대한 변환 없이 안전한 콘텐츠를 전송할 수 있도록 하는 연구가 진행되어야 한다.

현재 인터넷 세계 최고 수준을 자랑하는 인프라를 갖는 한국의 입자에서는 북한 및 중국의 해킹 위협에서 절대 자유롭지 못한 상황이다. 이러한 시점에 기존의 방식으로는 해킹이 불가능한 새로운 메커니즘에 대한 연구 및 투자가 반드시 필요하며 본 논문에서 제시한 SCTS를 통해 보다 적극적인 기술 도입이 필요할 것으로 보인다.

REFERENCES

[1] Parc Homepage, http://www.parc.com/

[2] 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.

[3] ENC (Emerging Network Consortium), http://www.parc.com/services/focus-area/emerging-networksconsortium/

[4] Swarun Kumar, etal, “CarSpeak: A ContentCentric Network for Autonomous Driving,” ACM Sig Comm’12, Helsinki, August 2012

[5] Michael Meisel, Vasileios Pappas, and Lixia Zhang. Ad hoc networking via named data. In MobiArch’10. ACM, 2010.

[6] Publish-Subscribe Internet Routing Paradigm (PSIRP): http://www.psirp.org/

[7] Mark Gritter and David Cheriton,“An architecture for content routing support in the Internet,” 3rd USENIX symposium on Internet technologies and systems, 2001

[8] David Cheriton and Mark Gritter, “TRIAD: a Scalable Deployable NAT-based Internet Architecture,” Technical Report, http://www-dsg.stanford.edu/triad/#papers, January 2000

[9] Van Jacobson, et al,“Networking Named Content,” ACM CoNEXT 2009

[10] IRTF ICNRG (Information-Centric Networking Research Group), http://trac.tools.ietf.org/group/ irtf/trac/wiki/icnrg

[11] BongYong Kwon, ChoongSeon Hong "Popularity-based Caching Scheme for Content Centric Networking" proc. of the KCC 2014, 1053p, June 27, 2014 (in Korean)

[12] CCN & CCNx Homepage, http://www.ccnx.org/

[13] Jaehoon Kim, et al, “Content Centric Network-based Virtual Private Community,” IEEE ICCE, Las Vegas, January 2011

[14] Named Data Networking project web site: http://www.named-data.org/

[15] FP7 4WARD Project - Networking of Information (NetInf): http://www.4ward-project.eu/

[16] Van Jacobson, et al,“Networking Named Content,” ACM CoNEXT 2009

[17] Van Jacobson, et al, “Custodian-based3 Information Sharing,” IEEE Communication Magazine, July 2012

[18] M. Waehlisch, D. Saucez, T. Schmidt, D. Kutscher, S. Eum, I. Psaras and K. Pentikousis, “ICN research challenges,” IETF Work in progress, 2014.

Authors

Hyung Su Lee:
1991: BS, Electronic Engineering, SungKyunKwan University
2011: MS, Department of Computer Engineering, SoongSil University
2014: Doctorate, Department of Computer Engineering, SoongSil University
Current position: Professor, Department of Information Security, Seoul Gangseo Campus, Korea Polytechnics
Areas of interest: Network security, cyber security, and information communication.
E-mail: hyungsu.lee@gmail.com

Jae-Pyo Park
1998: MS, Department of Computer Engineering, SoongSil University
2004: PhD, Department of Computer Engineering, SoongSil University
Current position: Professor, Graduate School of Information Science, SoongSil University
Areas of interest: Network security, information security
E-mail: pjerry@ssu.ac.kr

Jae-Kyung Park
1994: BS, Department of Computer Engineering, Dongguk University
1996: MS, Department of Computer Science, Hongik University
2002: PhD, Department of Computer Science, Hongik University
Current position: Professor, Department of Information Security, Seoul Gangseo Campus, Korea Polytechnics
Areas of interest: Network security, cyber security
E-mail: jakypark@kopo.ac.kr