한국컴퓨터정보학회 하계학술대회 논문집 제25권 제2호 (2017. 7)

# CCN을 활용한 네트워크 보안 변환 시스템

박재경°, 이형수*
°*한국폴리텍대학 서울강서캠퍼스 정보보안과
e-mail: jakypark@kopo.ac.kr°, hslee01@kopo.ac.kr*

# A Network Secure Translate System Using CCN

Jae-kyung Park°, Hyung-Su Lee*
°*Dept. of Information Security, Korea Polytechnic

● 요 약 ●

본 논문에서는 기존 인터넷 체계의 문제점을 보완하고 근본적인 대안을 제시하기 위해 CCN개념을 이용한 보안 강화 기법을 제안하고 이를 통해 네트워크의 안전한 전송 시스템을 제안한다. 또한 기존의 복잡한 구조와 사이버 공격 및 해킹에 쉽게 노출되는 TCP/IP 체계의 현재 인터넷 구조에서 네트워크 시스템구조를 단순화하고 획기적 성능 향상과 더불어 사이버 공격에 대응할 수 있는 기술을 제안하고 이를 프로토타입으로 설계하여 증명하고자 한다. 본 논문에서는 파일롯 시스템의 실험을 통하여 제안하는 CCN개념을 이용한 네트워크 보안 변환 시스템 기법의 우수함을 보인다.

**키워드:** 네트워크 변환(Network Translate), CCN, 네트워크 보안(Network Security)

## I. Introduction

현재인터넷은 단순히 정보의 공유 및 효율적인 측면에서 진화해왔지만 보안측면에서 인터넷은 그 자체로 안전하지 못하여 별도의 보안 메커니즘을 적용하고 있음에도 여전히 취약한 것이 사실이다. 지속되는 해킹에 따라 패치를 반복하는 체계로 부수적인 네트워크나 시스템 장비를 과다하게 요구하고 있으며 이에 따른 비용도 지속적으로 증가 있다. 최근 들어 단순한 공격방식이 아닌 랜섬웨어와 같은 범죄로 인한 피해가 가속화되고 있고 기업과 개인 모두 사이버 보안에 신경을 쓰지 않을 수 없는 상황이다.

이러한 인터넷의 문제점을 극복하고자 고안된 것이 CCN (Content Centric Networking) 기술로 현 인터넷의 근본적 보안 취약점인 호스트 중심에서 벗어나 콘텐트를 기반으로 하는 새로운 차세대 네트워킹 아키텍처를 제안하는 것이다. 즉, 인터넷에 접속되는 기기들끼리 상호 연결하는 데이터 채널을 제공하고, 해당 채널을 보호하는 최근 40여 년간의 인터넷 프로토콜 방식 대신에 네트워크 단에서 콘텐트를 사용자에게 안전하고 빠르게 제공하고자 하는 기술이다. 따지고 보면 사용자는 본인이 원하는 콘텐트가 어디에 있는지가 중요한 것이 아니며, 요즘 같이 하나의 네트워크 연결이 보편화된 환경에서 종단간의 데이터 채널을 안전하게 유지하기 위해서는 너무 많은 오버헤드가 필요하다. 콘텐트 중심 네트워킹에서는 콘텐트에 대한 정보를 획득하기 위해 필요한 인터넷 주소가 필요 없이, 콘텐트 자체를 네트워킹의 주인공이자 주체로 사용하는 것이다.

기존의 체계에서는 현재 지속적으로 진행되고 있는 보안의 문제를 해결하기 위한 방편으로 보안장비 도입, 망분리 등의 대책을 마련하여 보완하고 있지만 여전히 보안 측면에서는 미흡한 것이 현실이다. 본 논문에서는 이러한 기존 인터넷 체계의 문제점을 보완하고 근본적인 대안을 제시하기 위해 CCN개념을 이용한 인증 강화 기법인 콘텐트 인증 시스템(Content Authentication System)을 제안하고자 한다.

## II. Preliminaries

### 1. Related works

#### 1.1 TCP/IP 보안 이슈

보안성은 모든 종류의 통신에 있어서 중요시되고 있는 문제이다. 인터넷 역시 개발된 이래로 많은 보안 공격을 경험하였고, 이에 대한 해결책을 제시하여 왔다[1][9]. 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 때우기 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[2][8]. 또한 무선기기 및 네트워크의 제한된 특성은 취약성 보안 공격을 더욱 쉽게 만든 반면 기전의 유선망에서 사용해왔던 보안 대책들을 적용시키기 어렵도록 하였다. 따라서 무선으로의 인터넷 영역의 확장은 기존의 인터넷 보안성을 강화하는 측면에서 더욱 근본적인 접근을 요구하고 있다.

### 1.2 TCP/IP 보안 이슈

CCN(Contents Centric Network)은 기존 위치 중심인 IP 체계를 콘텐트 중심의 네트워크 체계로 구현하여 안전한 콘텐트 전송능력을 향상시키고 보다 강화된 보안체계를 제공하여 서비스 및 보안을 획기적으로 개선한 새로운 개념의 차세대 네트워크이다. CCN은 특정한 인증 이름 규칙을 콘텐트에 부여하여 IP가 없이도 콘텐트의 내용으로 데이터를 처리할 수 있는 메커니즘이다[3][10]. CCN을 이용할 경우 서비스 요청자 또는 악의적인 공격자는 콘텐트 서버에 접근자체가 불가하여 서버의 운영체제, 웹 서비스, 응용 서비스 등을 전혀 알 수 없다. 공격자가 요청을 통해 콘텐트를 받을 수는 있으나 이는 콘텐트 저장소에 저장된 캐시 내용을 받는 것이며 이러한 데이터 서비스 또한 정상적인 인증을 해결해야만 받을 수 있는 개념이다[4][5][11].

현재 인터넷 데이터 서비스의 규모는 매우 빠르게 증가하고 있다. IDC가 예측하는 인터넷 사용 인구와 데이터의 증가 추세는 계속 증가하는 추세이다[6][7][12]. 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[13][14]. 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 콘텐트 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. The Proposed Scheme

본 논문에서 제안하는 시스템은 다양한 위험요소들을 근본적으로 해결하기 위한 새로운 방식의 접근으로 네트워크 패러다임 자체를 미래 지향적 차세대 인터넷 패러다임인 CCN(Content Centric Network)을 활용한 새로운 콘텐트 인증 시스템이다. 현재뿐만 아니라 향후에도 콘텐트와 서비스는 인터넷의 핵심이다. 한편 보안도 반드시 적용해야 할 필수 요소이다. 그렇다고 해커들의 행동을 금지시킬 수는 없으며 해킹은 몇몇의 고급 기술의 직업이 아니다. 본 논문에서는 기존의 TCP/IP의 단점으로 나타난 보안의 문제를 어떻게 근본적으로 해결할 것인가에 대한 대안으로 차세대 네트워크인 CCN을 활용하여 TCP/IP의 단점을 극복하고자 한다. TCP/IP는 보안을 염두해 두지 않고 설계된 프로토콜로 40여 년간 많은 강점을 통해 현재의 인터넷을 이끌어 냈지만 보안의 문제는 날로 심각해져 가고 있다. 이러한 CCN 프로토콜을 활용하여 새로운 인증시스템을 제안하고 이를 제안시스템으로 구현하여 실험으로 증명하고자 한다. 제안시스템은 내부적으로 CCN 프로토콜을 사용하므로 TCP/IP 공격 자체가 의미없는 것으로 서로 다른 통신을 사용함으로 TCP/IP의 문제를 근본적으로 해결하고자 한다. 또한 제안시스템은 기존의 TCP/IP 네트워크와 호환을 해야 현재의 네트워크에 활용이 가능하므로 TCP/IP와의 호환도 지원한다.

본 논문에서 제안하는 인증 기술의 아키텍처는 CCN 메커니즘을 전달 방법으로 사용하지만 그림 3-3과 같이 CCN에 추가적으로 보안에 필요한 요소를 추가함으로 더욱 강력한 메커니즘을 제공한다. 우선 기존의 통신 방법인 TCP/IP와 내부망을 연결하기 위해 아웃바운드에서는 TCP/IP를 그대로 받아서 처리하는 호환 메커니즘을 적용한다. 이를 제안시스템 내부에서 CCN 프로토콜로 변환을 하여 처리하며 이때 기존의 TCP/IP에서의 보안상 문제점을 검토하기 위한 몇 가지의 보안 엔진을 추가로 탑재하여 기존 보안 문제를 해결할 수 있다.

- 기존 TCP/IP와 CCN의 연동을 통해 네트워크 대역폭 효율성 극대화
- CCN의 특성을 도입함으로 TCP/IP의 DDoS 공격과 같은 전형적인 보안 문제 해결
- 외부 해커의 악성코드 공격 및 동적 코드 공격 등의 공격을 인증시스템에서 추가 검증하여 알려지지 않은 공격에 대한 방어
- 내부 도메인 사용자의 악성코드 감염 등으로 내부 자료유출을 CCN의 네트워크 특성으로 방어
- 위의 제안시스템의 목표를 토대로 시스템을 설계하였으며 네트워크의 보다 효율적인 운영 및 기존 TCP/IP에서 빈번하게 발생하면서 치명적인 보안 문제를 본 제안시스템을 통해서 해결할 수 있다.

### 2.2 기능별 비교

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

Table 1. Compare with TCP/IP

| 항목 | TCP/IP | 제안시스템 | 비고 |
|---|---|---|---|
| 연결 방식 | 세션 연결 | 연결 없음 | 우수 |
| 대역폭 | 연결마다 적용 | 비연결 방식 | 우수 |
| 캐쉬 활용 | 없음 | 활용 | 우수 |
| DDoS 공격 | 방어 못함 | 연결 안됨 | 우수 |
| 데이터 보안 | 없음 | 암호화 지원 | 우수 |
| 데이터 무결성 | 없음 | 전자서명 지원 | 우수 |
| 취약점 | 다수 존재 | IP가 없으므로 기존 공격 취약점 전무 | 우수 |
| 구현 | 쉬움 | 어려움 | TCP/IP 우수 |
| 성능 | 보통 | 데이터 캐쉬로 빠른 서비스 | 우수 |

본 논문에서 제안하고자 하는 시스템은 기존의 TCP/IP 문제점을 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 및 사물인터넷을 통한 공격, 랜섬웨어 등의 악성코드 등이 CCN 기반의 제안시스템에서 무력해 지는 실험을 진행하였다. 본 논문에서의 실험은 Table 2와 같이 크게 4가지로 나누어 진행하였다.

Table 2. Test Result

| 번호 | 실험목적 | 실험 내용 |
|---|---|---|
| 1 | TCP/IP 호환성 | 상용 OS인 Windows 10 클라이언트에 인터넷 익스플로러를 통해 내부 Windows 8서버에 설치된 아파치 웹 서버에 접근하여 서비스 시도 |
| 2 | DDoS 공격 방어 | 기존/신규 종류의 DDoS 공격용 Flood 패킷들이 유입되어 네트워크 밴드위스 잠식이 시작되는 즉시, 모든 종류의 TCP/IP기반 Flood 패킷들을 전부 Garbage 및 Junk 패킷으로 분류(분석) / 인식하여 즉각 차단하는지 여부 판단 |
| 3 | Mirai 공격 방어 | DDoS 공격 방어의 패킷 차단 기능과 Policing 기능을 혼합 사용하여, 네트웍이 DDoS 공격에도 항상 서비스에 영향을 받지 않는(Uninterruptible) 상태로 유지되는지 판단 |
| 4 | 동적 코드 방어 | 내부 사용자에 의한 정보 유출 등으로 특정 서버 등에 대한 해커의 공격 역시 동적 코드와 같이 함수 코드를 담고 있는 경우 응답하지 않음. 내부 사용자가 특정 서버에 대한 정보(ID, 암호 등)를 해커에게 유출한 경우의 해킹에 대비하여, CAT 프로파일 기술 및 BBS VM을 통해 서버 및 서버 리소스에 대한 해커의 접근 차단 및 서버의 데이터가 외부로 유출되는 것, 또한, 원천적으로 차단하는지 판단<br>동적코드 종류 : ls(), lsc(), Net(), IP(), ICMP(), Ether(), display(), help(), show(), str(), send(), sr(), report_port(), srloop(), sniff() |

위의 4가지의 보안 문제는 현재 TCP/IP 환경에서 근본적으로 방어가 불가능한 공격 방식으로 현재도 많은 보안 제품 개발이나 이론적인 연구가 진행되고 있는 공격 방식이다. 이러한 총 4가지의 실험에 대한 결과를 분석하여 요약하면 Table 3과 같다.

Table 3. Test Summary

| 번호 | 실험목적 | 실험 결과 |
|---|---|---|
| 1 | DDoS 공격 방어 | 플러딩 공격 방어 성공 |
| 2 | Mirai 공격 방어 | Mirai 공격 방어 성공 |
| 3 | 악성코드 방어 | 악성코드 검출 성공<br>(단, 신규 악성코드 실험 진행하지 못함) |
| 4 | 동적코드 공격 방어 | 소스 내 동적코드 방어 성공 |

본 논문에서 제안한 시스템은 기존의 TCP/IP의 환경과 상호호환 실험을 통해 현재의 네트워크에서 활용가능함을 실험으로 증명하였다. 따라서, 현재의 TCP/IP에서 발생할 수 있는 보안의 문제를 해결할 경우 적용이 가능할 것으로 판단한다.

## IV. Conclusions

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

하지만, 본 논문에서 제안한 제안시스템이 기존 TCP/IP 보안제품을 대체하기 위해서는 추가적인 연동 테스트 및 많은 샘플을 통해 추가적인 실험을 진행해야 할 것으로 판단한다. 또한 내부적인 여러 보안 엔진들의 기능을 공개 소스를 활용해 구현하였으나 이를 최적화하는 작업이 필요할 것으로 보인다.

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

## REFERENCES

[1] Parc Homepage, http://www.parc.com/
[2] PSIRP Homepage, http://www.psirp.org/
[3] 4WARD Homepage, http://www.4ward-project.eu/
[4] PURSUIT Homepage, http://www.fp7-pursuit.eu/
[5] COMET Homepage, http://www.comet-project.org/
[6] SAIL Homepage, http://www.sail-project.eu/
[7] CCN & CCNx Homepage, http://www.ccnx.org/
[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] Mark Gritter and David Cheriton,“An architecture for content routing support in the Internet,” 3rd USENIX symposium on Internet technologies and systems, 2001 [3] T. Koponen et al, “A

Data-Oriented (and Beyond) Network Architecture,"ACM Sigcomm 2007

[10] Van Jacobson, et al,"Networking Named Content," ACM CoNEXT 2009

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

[12] Van Jacobson, et al, "Custodian-based Information Sharing," IEEE Communication Magazine, July 2012

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

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