http://dx.doi.org/10.7236/JIWIT.2012.12.4.111
JIWIT 2012-4-14

대용량 HD 영상콘텐츠 고속전송 VPN(Virtual Private Network)의 설계

Design of High-Speed VPN for Large HD Video Contents Transfer

박형일*, 신용태*

Hyoungyill Park, Yongtae Shin

요 약 다양한 방송사와 서로 다른 CP(Contents Provider)가 분산되어 있는 Data Center서버에서 VOD 서비스를 하고자 할 때, 서로 다른 CP 플랫폼들이 고화질 HD, 3DTV 비디오 등의 영상파일을 교환하기 위해 고성능 네트워크를 통하여 빠르게 전송할 수 있는 망을 빠르게 구성해야 한다. 본 논문은 Public망의 QoS와 보안성을 보완하는 선택적인 암호화 방안을 이용하여, 고속의 안전한 VPN(Virtual Privatr Network)을 생성하고 콘텐츠를 고속으로 대용량 영상파일을 전송하는 프로토콜을 제안한다. End to End의 Device가 대용량의 영상파일을 Parallel 전송으로 가용한 자원을 최대한 사용하면서 안전한 콘텐츠 전송이 가능한 고성능의 VPN을 구성하는 모델을 제안한다.

Abstract When broadcasters want immediately a variety of VOD files in a distributed server of them data centers and away contents provider, CPs of different platform to exchange high-quality HD, 3DTV video and other video files over the IP networks of high-performance that can be transferred quickly and must be configured quickly. This paper, by using an optional encryption method to complement a QoS and security of public network, suggests high speed and secure content transmission protocol such as VPN(Virtual Private Network) for large video files and big data. As configured high performance VPN, end to end devices use the best of available resources over public network by parallel transfer protocol and the secure content delivery network.

Key Words : High-speed Content Transfer, High-Performance VPN, Selective and Partial Chipher, SSL VPN

Ⅰ. 서 론

향후 방송사는 다양한 방송서비스 - Cable, 위성방송, IPTV, VOD, N-screen, 3DTV, UDTV, Smart TV 등 - 의 형태를 추구하는 새로운 미디어서비스를 위해 방송용 VoD서비스 클라우드 플랫폼를 구축하게 될 것이다. 이들은 방송사별로 별도 또는 통합된 형태의 다양한 구성이 될 수 있으며, 물리적 공간들도 서로 다르게 될 것이다. 서로 떨어져 있는 서버들이 사업자간에 서로에게 필요한 콘텐츠서비스를 전송하도록 요청되어져 있을 경우, 중요한 점은 최종 시청자에게까지 실시간성이 보장되도록 빠르게 End to End 서버에게 콘텐츠를 공급해야 해야 한다. “그림 1”은 다양한 방송서비스가 가능한 Open IPTV의 구조를 보여준다. 일반적으로 VoD서비스를 위

*정회원, 숭실대학교 컴퓨터학과
접수일자 : 2012년 3월 15일, 수정완료 : 2012년 7월 15일
게재확정일자 : 2012년 8월 10일

Received: 15 March 2012 / Revised: 15 July 2012 /
Accepted: 10 August 2012
*Corresponding Author: shin@ssu.ac.kr
Department of Computer Science, Soongsil University, Korea

한 IPTV Provider는 여러 CP들로부터 콘텐츠를 제공받아 방송서비스를 하게 된다.

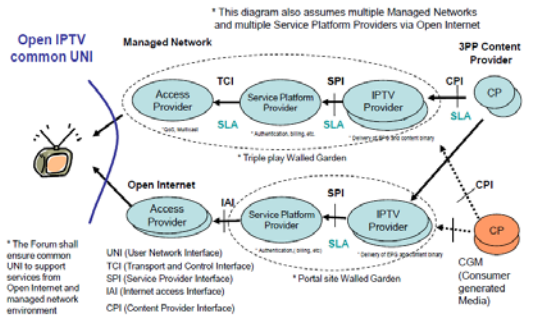

그림 1. Open IPTV Forum의 범위[1]
Fig. 1. Open IPTV Forum Scope[1]

CP들간의 인터페이스에서 Public IP Network을 통해서 서버 또는 IDC간에 전송을 할 경우 VPN을 구성하여야 안전한 전송을 보장 받을 수 있다. 그러나 일반적인 VPN의 구성은 많은 고성능 하드웨어와 전용망 등의 구성을 필요로 하기 때문에, 규모에 따라 경제적인 한계성을 가지고 있다. 특정한 전용망을 구성하지 않은 기업들은 콘텐츠의 교환을 위해 End to End VPN 망을 “그림 2”과 같이 구성할 수 있다.

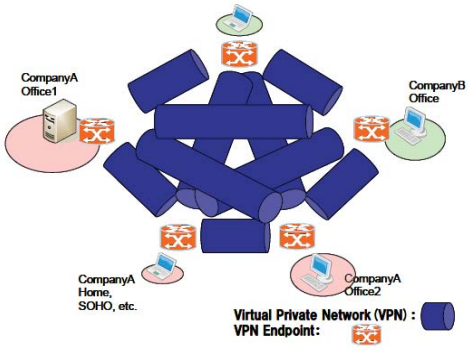

그림 2. Mesh VPN Topology[2]
Fig. 2. Mesh VPN Topology[2]

방송관련 회사들이 HD영상파일전송을 위해 VPN을 구성할 때, 전통적인 암호처리 방식은 모든 콘텐츠를 일률적으로 암호화를 적용하여 처리하는 것이다. 즉 입력되는 패킷에 대하여 콘텐츠의 환경은 고려되지 않고 모든 데이터에 대하여 암호처리가 적용되는 것이다. 이러한 방식은 용량이 비대한 멀티미디어 콘텐츠를 빠른 시간에 전달하는 데에는 많은 성능저하를 일으킨다. 이를 개선하기위해 고성능 Device를 이용하는 VPN을 사용할 수 있다. 본 논문에서는 Application 레벨에서 VPN을 구성하여, 경제적이고 안전하며, 고효율의 Network 전송이 가능한 VPN 구성을 위한 프로토콜을 제안하고자 한다.

이를 위해 2장에서는 관련 VPN과 멀티미디어의 안전한 전송에 관한 연구를 알아보고, 3장은 암호화와 성능향상에 관한 연구를 알아보고, 4장은 고성능 전송네트워크를 제안하고, 이에 대한 성능을 5장에서 점검하며, 6장에서는 제안한 VPN 구성에 대한 결론을 맺고자 한다.

II. 방송콘텐츠의 전송

다양한 서비스를 위한 방송용 클라우드서버 간에는 유무선 통합의 환경이나 모바일 환경에서의 전송되는 콘텐츠가 여러 종류의 단말에 적응적(Adaptive)으로 전달하는 것이 콘텐츠 관리 효율성 측면에서 필요하다. 따라서 서로 다른 방송 ISP간, 방송 클라우드서버들 간에 필요한 미디어를 빠르고 안전하게 공급하기위해 다양한 형태의 VPN이 구축 될 수 있다. IP VPN 기술은 인터넷에서 전송 시에 생길 수 있는 문제점들을 보완하여 데이터의 신뢰성과 품질보장, 불법적 접근을 막을 수 있어야 하고, 2절에서 언급되는 보안 이슈를 적절히 수용해야 한다.

1. VPN의 종류

대표적인 VPN은, 2계층의 PPTP, L2F 및 L2TP는 양단간의 원격접근을 위한 터널링 기술, 전송되는 패킷에 대한 인증, 암호화, 무결성을 지원하는 3계층의 IPSec, 전송데이터의 품질보장, 트래픽제어 및 효율적 패킷 전달에 효과적인 MPLS와 안전한 end to end 전송을 위한 SSL VPN 등이 대표적이다. 각 기술은 보안성 및 확장성 등에서 장단점이 있어서 각각의 특성을 이용하여 서비스를 구현하지만, 확장성과 성능이 낮다는 문제를 가진다. VPN의 다음과 같은 종류 들이 존재한다[3].

- Point to Point Tunneling Protocol (PPTP) : Microsoft와 다른 벤더들에 의해 개발된 표준 터널링 프로토콜.
- Layer Two Tunneling Protocol (L2TP) : IETF에서 개발된 L2F(Layer Two Forwarding)와 PPTP의 혼합형태.

- Internet Protocol Security (IPSec) : Network 계층에서 안전한 traffic 전송을 위한 IETF 표준 프레임워크.
- Secure Socket Layer (SSL) : Netscape에 의해 개발된 Application 계층의 보안프로토콜로써, 안전한 HTTP 웹을 위해 사용됨.
- Multi Protocol Label Switching (MPLS) : Data link 계층과 Network 계층의 사이에 존재하며, 효과적인 라우팅을 위해 Label을 사용함.

2. 차세대 IPTV 정보보호 요구사항

최근 이슈화 되고 있는 네트워크를 통한 방송서비스의 전송에 있어서, 중요한 점은 QoS을 보장할 수 있느냐는 것이다. 전통적인 암호처리 방식은 모든 콘텐츠를 일률적으로 암호를 적용하여 처리하는 것이다. 즉 입력되는 패킷에 대하여 콘텐츠의 환경은 고려되지 않고 일방적인 암호처리가 적용되는 것이다.

현재 상용화되어 있는 방송 콘텐츠와 서비스의 보안기술은 CAS와 DRM이 있다. CAS는 가입서비스의 종류에 따라 컨텐츠 이용을 제어할 수 있는 실시간형 컨텐츠의 시청권한을 제어하는 보안기술이고, DRM은 저작권을 보호하고 적법한 콘텐츠의 사용을 위해 암호화기술을 이용하여 불법적인 디지털콘텐츠의 복제와 유통을 방지하기 위한 보안기술로써 VoD사업자에게 잘 적용 된다[2]. 이들 인터넷을 이용한 TV 기술은 네트워크 보안 위협이나 각종 서버 및 단말기의 보안위협에 대응하기 위한 보안 메커니즘은 특정 콘텐츠의 특징에 국한되지 않고 사용되기 때문에 적절히 사용되어야 할 필요성이 있다. 따라서 ITU-T의 워크아이템문서 X.IPTVsec-2에서 IPTV를 위해 새롭게 제안되는 보안요구사항은 다음과 같다.

- Cryptographic and Perceptual Security : 암호 알고리즘 자체의 보안 강도가 중요하지만, 암호화된 상태로 재생하여 부분적인 영상해독이 가능해야 한다.
- Efficiency : 암호화 효율성을 위해 멀티미디어 실시간성을 제공하기 위하여, 콘텐츠를 선택적으로 암호화를 실시해야 한다.
- Compression ratio : 멀티미디어 암호 메커니즘이 멀티미디어의 압축률을 감소시키거나 압축률에 영향을 주어서도 안 된다.
- Format compliance : 암호화된 비디오 데이터는 표준 디코더와 호환성을 유지해야 한다.
- Error tolerance/Robustness : 암호 메커니즘이 오류 허용성/오류 강인성을 가져야 한다.
- End-to-End security : 정보보호위협을 야기시키는 중간의 트랜스코딩 노드는 복호화하지 않고 트랜스코딩해야 하며, End to End 보안을 유지해야 한다.
- Adaptive resolution : 암호 메커니즘이 다양한 전송대역, 화질, 화면크기의 단말을 지원할 수 있어야 하며, 이에 상응하여 정보보호 메커니즘은 보안 강도의 수준을 조절할 수 있어야 한다[4].

이러한 콘텐츠 전송을 위한 이슈사항들은 CP들 간의 VoD 콘텐츠 전송에서도 이슈가 된다. 따라서 멀티미디어 콘텐츠와 같은 대용량 비디오의 특성을 고려하면 경제성 및 암호화서비스 적용의 방대함에 컴퓨팅자원을 과도하게 사용하는 많은 단점을 가지고 있기 때문에, 새로운 정보보호 동향의 필요성이 요구되고 있다. 실시간(Real-Time), 비실시간(Non-Real Time)형 콘텐츠는 상황에 적합한 정보보호 요구조건을 만족해야한다.

Ⅲ. Secure 전송 프로토콜

1. SSL VPN

Public 네트워크에서 콘텐츠 전송을 위해 종단간 보안서비스 제공을 위해 적합한 SSL VPN은 클라이언트-서버 환경에서 TCP의 End to End 보안을 위한 프로토콜이다. 인증서(certificate) 확인과정을 통해 서버와 클라이언트의 인증(authentication)기능을 수행하고, 대칭키 암호화(symmetric cryptosystem)를 통해 기밀성(confidentiality)을 유지하고 메시지인증코드 MAC(Message authentication code)을 사용해 데이터의 위변조를 탐지할 수 있는 무결성(integrity)을 제공한다. 그리고 대칭키 암호화 알고리즘에 사용되는 비밀키는 공개키 암호화방식(asymmetric cryptosystem)을 이용한 키교환 알고리즘을 통해 설정된다. SSL은 TCP와 HTTP계층사이에서 동작하며, reliable transport protocol에서 동작하도록 되어있다. 따라서 UDP에서 동작은 적용되지 못한다.

SSL은 2계층으로 이루어져 있으며, Record layer는 상층에 위치하는 기밀성과 무결성 등의 보안서비스를 제공하며, 상층의 Handshake Protocol과 Change CipherSpec 프로토콜은 SSL의 보안파라미터를 설정하고 관리한다.

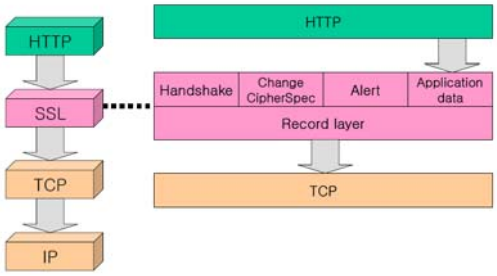

그림 3. SSL 프로토콜의 구조[5]
Fig. 3. Structure of SSL Protocol[5]

SSL은 먼저 Handshake 프로토콜을 이용하여 Record 프로토콜에서 사용될 보안파라미터를 설정하고, Change CipherSpec 프로토콜에 의해 사용 가능하도록 활성화 된다. Application 프로토콜이 응용계층 데이터를 Record 프로토콜로 전달하며, SSL 통신과정에서 생기는 오류는 Alert 프로토콜로 처리 된다. Handshake와 Change CipherSpec프로토콜 이후의 모든 데이터는 Record 계층을 통해 보호되어 전송된다[5].

현재 SSL은 사실상의 HTTP에서 사용하는 VPN 표준으로 자리 잡고 있으며, 대부분의 웹브라우저가 SSL을 지원한다. 그러나 SSL 사용은 키 생성, 교환 등에 많은 연산을 필요로 하기 때문에 그에 따른 클라이언트 및 서버와 네트워크의 성능저하를 피할 수 없고, 패킷을 암호화하기 때문에 라우팅을 결정하는 트래픽관리 어플리케이션의 기능을 발휘하지 못하므로 네트워크에서 고속의 전송성능에 제한을 받게 된다.

2. Secure한 전송을 위한 구조

Secure한 SSL의 Setup 과정은, Handshake 프로토콜을 기본으로 설정된다. SSL통신이 시작되기 전에, SSL 프로토콜 버전과 암호알고리즘(Key exchange, Secret Key, MAC)을 설정하고, 키 교환 알고리즘을 이용해서 서로의 비밀키를 공유하게 된다. “그림 4”는 SSL 통신을 위한 Handshake 프로토콜의 진행과정의 메시지를 보여준다.

Server와 Client는 X. 509와 같은 공캐키 Key Exchange 알고리즘에 따라 보안 Parameters를 수행하고, Finished 메시지를 서로 보내면서 보안 Parameter의해 보호된 통신을 하게 된다[5]. Secure한 Application Data전송을 위해 SSL통신의 Setup과정은 간편하면서 신뢰성을 준다.

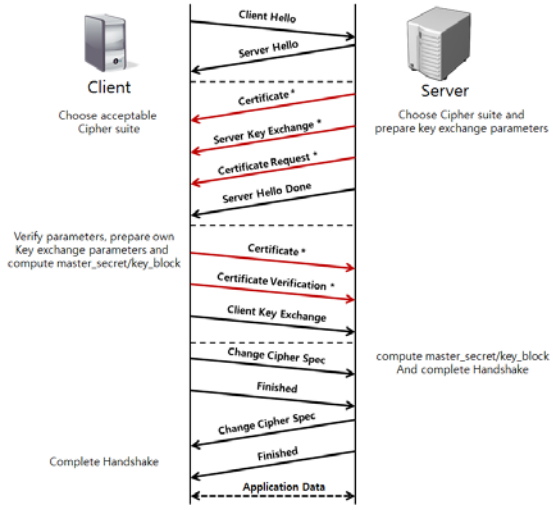

그림 4. SSL의 Setup (Handshake 프로토콜)[5]
Fig. 4. Setup of SSL (Handshake Protocol)[5]

3. 암호화의 종류

암호화는 아주 다양한 형태로 구분된다. 특히 SSL VPN은 공개키 암호화 알고리즘에 의해 안전한 채널을 Setup하여 서로의 비밀키(대칭키)를 공유하고 안전한 End to End 통신을 행한다. Data 전송의 비밀성을 위하여 암호화방식은 대칭키 암호화와 비대칭 암호화방식이 있다.

$$E(M, K_{ab}) = C, \quad D(C, K_{ab}) = M \qquad (1)$$

$$E(M, K_{+b}) = C, \quad D(C, K_{-b}) = M \qquad (2)$$

대칭키 암호화는 식(1)과 같이 암호화 Key와 복호화 key가 같은 형태로써, DES, AES 등이 대표적인 대칭키 알고리즘이다. “식(2)”는 Public Key 알고리즘이고 대표적인 비대칭키 알고리즘은 RSA가 있다.

비교적 빠른 암/복호화를 위한 대칭키 암호화는 스트림암호화 방식과 블록암호화 방식이 있다. 스트림암호화는 연속적인 데이터 입력을 하나씩 받으면서 암호화하며, 블록암호화 방식은 블럭단위의 정해진 비트 길이의 정보를 암호화하는 암호 방식이다. 블록암호화를 사용하는 SSL VPN은 고정된 사이즈 블럭 암호화조작에 적합하고, 스트림 암호는 시간의 변화에 따른 암호화조작에 적합하다[6,7].

Ⅳ. 고속전송 프로토콜

Public Network을 이용하여 대용량 방송콘텐츠의 전송할 경우, 확보 가능한 대역폭을 효율적으로 사용하는 프로토콜로 Parallel TCP를 이용한 고속전송은 매우 효과적이다.

TCP는 AIMD(Additive increase/Multiplicative Decrease) Congestion Control 알고리즘 때문에 high Bandwidth Delay Product (BDP)에는 잘 사용되지 않으며[8], 네트워크상에서 단일 TCP 채널 성능은 RTT와 Loss가 큰 통신에서는 Network 대역폭의 성능저하를 가져온다.

TCP에서 AIMD를 극복하고 링크의 대역폭 사용을 극대화하기위해서, "그림 5"와 같이 Multiple threads를 사용하여 end to end에 Multiple Transport를 실행하는 Parallel TCP 통신을 이용하면 고대역폭의 링크를 구성할 수 있다.

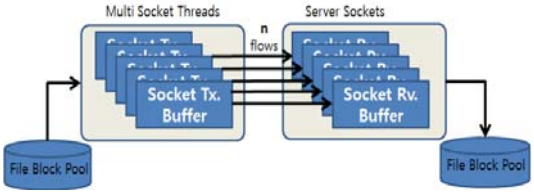

그림 5. Parallel TCP 전송 구조[9]
Fig. 5. Parallel TCP Transfer Architecture[9]

아래의 식(1)은 Single TCP Connection일 때, 전송성능에 RTT와 Buffer Size에 많은 영향을 준다는 것을 의미한다.

$$BW = \frac{MSS}{RTT\sqrt{\frac{2bp}{3}}} \quad (1)$$

$$BW_n = \frac{MSS}{RTT_n}\frac{n}{\sqrt{p_n}}\frac{c_1}{\sqrt{\frac{2b}{3}}} \quad (2)$$

$$BW = \sum_{1}^{ParallelLevel} BW_n \quad (3)$$

n: number of parallel flows
p: loss rate
RTT: round trip time
MSS: max segment size
b and c_1: constant

식(2), (3)에서 보듯이 Network의 대역폭은 Perallel TCP의 수에 비례하여 증가함으로써, Multiple Parallel TCP Connection은 고효율의 대역폭을 유지할 수 있음을 알 수 있다[10]. 아래 "그림 6"은 AIMD를 최소화하기위한 Parallel TCP 전송의 효율성을 보여준다.

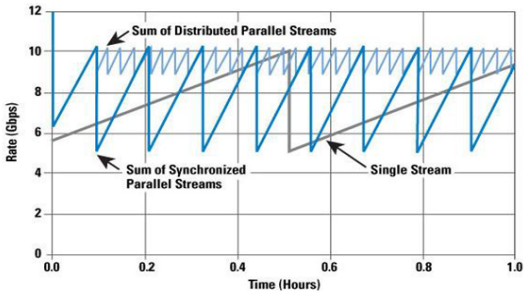

그림 6. Parallel TCP의 고효율성[9]
Fig. 6. High efficiency of Parallel TCP[9]

Ⅴ. Secure 멀티미디어 파일의 전송

On-demand 멀티미디어서비스를 위한 클라우드 서버들은 서로 대용량 영상파일을 빠르게 교환할 수 있어야 한다. 그리고 서비스를 위한 서버들이 안전하게 전송채널을 생성하고 암호화된 전송을 해야 한다. 이를 위해서 본장에서는 전송프로세스의 성능을 감소시키지 않으면서 최대 효율의 네트워크을 이용하면서, 중간의 전달과정에서 공격자에 의한 암호화, 복호화를 불가능하도록 End to End 보안을 보장하며, 정보보호 메커니즘이 보안강도의 수준을 제어할 수 있는 방법을 제안한다.

1. 구현방안

빠른 암호화와 복호화를 지원하기 위해 수백MB ~ 수GB 또는 TB에 달하는 모든 데이터에 대해 암호화를 실시하는 것은 전송을 위해 컴퓨터시스템 사이에서 과도한 자원을 소모하기 때문에 Network을 통한 전송이 매우 느려질 수밖에 없다. 따라서 대용량 고속파일전송을 위해 Parallel TCP 전송을 사용하는, 고속 VPN의 Setup 과정은 SSL의 Setup과정과 같이하면서 File Block Pool에서 생성되는 block의 일부를 암호화하여 생성된 특정 채널을 통해 전송하고, 서로 교환된 암호화 key로 복호화를 실시한다. "그림 7"은 고속전송의 도식과 선택된 부분 암호화의 구현방안을 보여준다.

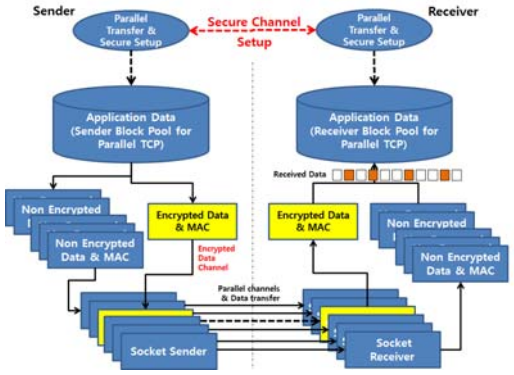

그림 7. 고속파일전송을 위한 Parallel 채널과 선택적이고 부분적인 암호채널의 생성과 전송

Fig. 7. Parallel TCP channels for high-speed transfer, selective and partial channel encryption

"그림 8"은 Application이 3-Handshake에 의해 의 VPN Setup과정과 Key Exchange을 거치고 난후, Data Block Pool에서는 Random하게 선정되는 암호화 채널로 전송하기위한 Data Block들을 암호화하여 Socket Sender를 통해 전송한다. 수신은 암호화된 Data를 수신한 채널의 Data를 분리하여 복호화 Key에 의해 복호화하고, 암호화되지 않고 전송된 Block들과 패킷을 재조립하여 완전한 Data를 생성하여 수신을 완료한다. 이를 Pool에서 암호화 Block을 생성하고 이를 정해진 Sequence 또는 TCP 전송규칙에 의해 전송함으로써, 선택적이고 부분적인 암호화 Block에 의해 안전한 VPN이 생성이 가능하다.

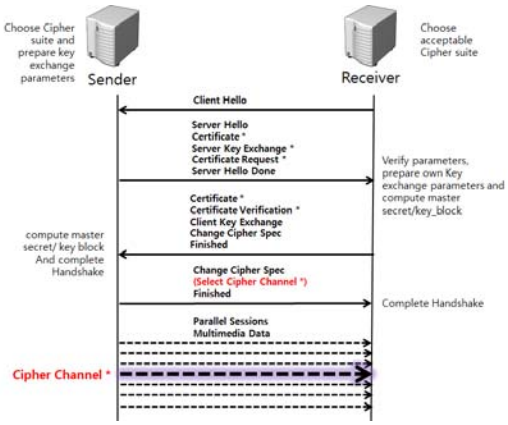

그림 8. Secure 채널의 생성과 전송을 위하 Handshakes

Fig. 8. Handshakes for creation and transfer of secure channel

2. 알고리즘의 고속성

Network의 사용을 극대화하기위해서 본 연구에서는 Parallel TCP Connection으로 AIMD에 의한 TCP 전송의 효율저하를 방지하면서 End to End 서버간의 사용가능한 Network자원의 사용을 극대화 할 수 있다.

Parallel TCP의 전송시험을 위해서는 Open Source 소프트웨어 Rapidant를 이용하여 N Flows에 대하여 "표 1"의 결과를 얻을 수 있다. "표 1"은 전송되는 파일의 TCP Overhead를 제외하고 제공되는 75Mbps의 Public Network의 대역폭을 거의 모두 사용하는 것을 볼 수 있다.

표 1. TCP의 Flow 수에 따른 네트워크 속도

Table 1. Transfer speed by the number of TCP Flows

TCP Flows n	Transfer Speed (Mbps)
1	47.84
2	49.56
3	50.92
4	52.08
5	55.28
6	60.88
7	64.72
8	70.32
9	69.12
10	69.20

표 2. SSL VPN을 이용한 전송 속도

Table 2. Transfer speed with SSL VPN

TCP Flows n	Transfer Speed with SSL (Mbps)	Delay ms
1	3.91	1,390
2	4.10	1,750
3	3.87	2,270
4	6.08	1,160
5	4.17	2,190
6	2.78	3,385
7	4.77	4,775
8	5.43	5,570
9	4.48	6,630
10	4.83	6,970

"표 2"은 네트워크의 모든 TCP 채널에 SSL 암호화를 적용함으로써 대용량의 파일을 전송하기 위해서 컴퓨팅 자원이 소모되고 네트워크 효율이 매우 저하 되는 것을 보여준다. 실험을 위해 네트워크 경로상에 SSL VPN 장비는 RSA_RC4_128bit_MD5로 암호화하여 네트워크의 성능을 실험하였다.

일부 채널에 대해 암호화전송을 실험하기 위해 “그림 9”처럼 SSL에 의해 일부만을 암호화하여 전송하는 Network 구성하고 네트워크 속도를 측정하였다. 실험에서 1 flow SSL 전송은 2.12Mbps을 보여주었고, 9 flows Parallel TCP 전송은 67.3Mbps의 속도로 전송함으로써, 사용가능한 네트워크의 대역폭을 최대한 사용(69.42Mbps)하는 결과를 보여주었다.

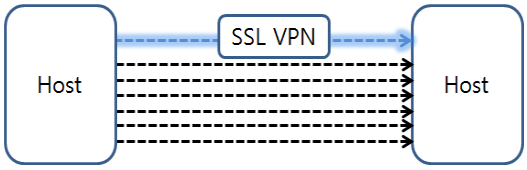

그림 9. SSL Flow를 가진 Parallel TCP 전송
Fig. 9. Mixed parallel transfer with SSL

따라서 제안하는 선택적 암호화를 적용하면 컴퓨터 프로세싱 자원 소모를 줄일 수 있고 Network 자원의 사용을 효율을 실현할 수 있다.

3. 콘텐츠의 안정성

멀티미디어 서버들의 콘텐츠 재전송(Store, Copy and Rebroadcast)이 고속화되는 것과 무관하게 End to End 정보보호서비스가 제공되기 위해서는 전통적인 알고리즘과 마찬가지로 제안되는 알고리즘 자체의 알고리즘도 강해야 한다.

전송되는 Parallel TCP 채널은 SSL VPN에서 제안하는 비대칭암호화 방식에 의해 Key를 교환하기 때문에 비교적 안전하다고 알려져 있다. Multi-TCP 채널 중의 하나를 Block 암호화 기반의 Key를 사용하는 가변의 충분한 길이의 Key를 사용함으로써 메시지 데이터 블록을 랜덤하게 암호화 가능하다. 또 다중으로 전송되는 모든 채널에 대한 데이터와 Control 정보를 가져야 원래의 데이터 복원이 가능한 Parallel TCP전송의 암호적인 특징과 특정 채널 또는 데이터 랜덤한 블럭에서만 전송되는 암호화 알고리즘방식으로 Public Network에서 고속의 VPN 역할을 감당할 수 있다.

Network으로 전송 중에 공격자에 의해 Sniffing 또는 Spoofing이 발생하여도 Plain Data 채널에 의한 복원만으로 전체의 멀티미디어 데이터를 복원하기는 힘들며, 암호화채널의 복원과 다중화된 데이터 블록의 조합은 더욱 어렵게 된다. SSL에서 블록 암호화는 3DES, AES 등의 암호화와 같이 Key를 반복해서 사용하지 않고 충분한 길이의 가변길이 부호화를 사용함으로써, 공격자에 의해 메시지의 복호화가 이루어져도 데이터의 완벽한 복원은 불가능하다. 즉 공격자의해 가로채기 된 멀티미디어 데이터의 복원이 이루어질 경우 실제 예상되는 현상은 영상미디어의 완전한 복원이 불가능하고 영상의 블록현상 또는 미 복원 Data 등으로 비정상적인 복원을 유발시킨다.

따라서 Parallel TCP를 이용하여 본 논문에서 제안하는 부분적 또는 선택적 VPN 메커니즘은 전송 Network 이나 Processing의 자원을 고효율화하면서도 방송콘텐츠의 전송 보안알고리즘으로 사용될 수 있다.

Ⅵ. 결론

본 논문은 가용 가능한 Public 네트워크을 최대한 이용하여 콘텐츠를 고속으로 전송하면서 E2E 정보보호 서비스를 제공하기위한 프로토콜을 제안한다.

전통적인 파일전송 메커니즘은 가용한 Network에서 충분한 효율을 발휘하지 못 할뿐만 아니라, 정보보호 메커니즘을 제공하지 못하고, Network상에서 정보보호를 위한 전통적인 VPN은 물리적인 Network의 구축 또는 Device가 필요하다. 하지만 E2E의 서비스가 무엇이고 서비스 레벨을 적응적으로 조절이 필요한 대용량 비디오파일의 전송로를 보호하는 것은 가용한 자원의 경제성을 고려해보아야 한다.

따라서 본 논문은 Parallel TCP를 기반으로 SSL Chiper 메커니즘을 선택적으로 적용하여, 정보보호 메커니즘 보안강도의 수준을 조절함으로써 E2E의 암호화와 복호화에 과도하게 사용되는 Processing 비용을 줄이고, 물리적인 Device없이 VPN을 생성함으로써 서비스 레벨에 적절한 정보보호 전송메커니즘을 제공한다.

Parallel TCP와 SSL VPN 메커니즘을 선택적으로 Flow에 적용하고 구현하는 방법들에 대한 것은 다양한 과제가 있을 수 있다. 하지만 별도의 E2E 정보보호를 위한 물리적 구축없이, 고화질 또는 다양한 방송서비스를 위한 VOD 서버, IDC 서버, P2P 서버들 간에서 콘텐츠의 전송을 급히 구축하여야하거나, 멀티미디어 및 방송서비스를 위한 개별사업자 CDN 간, Hybrid Cloud 서버간에 대용량 콘텐츠의 전송을 위한 응용이 가능하다. 이는 매우 경제적이고 서비스레벨에 따라 적응하는 정보보호메

커니즘으로 발전시킬 수도 있다.

참고문헌

[1] Open IPTV Forum e.V, “OIPF Release 2 Specification V2.1”, Open IPTV Forum, Vol.1, pp.5, Valbonne, 2011

[2] Koyama, T., "New Architecture for a VPN On-demand Interconnection System", Information and Telecommunication Technologies (APSITT), Kuching, Malaysia, 2010

[3] Ahmed A. Jaha, Fathi Ben Shatwan, and Majdi Ashibani, “Proper Virtual Private Network (VPN) Solution”, The Higher Institute of Industry, Misurata, Libya, 2008

[4] J.H. Nah, “ITU-T X.iptvsec-2: Functional requirements and mechanisms for secure transcodable scheme of IPTV”, TD0171. ETRI, Seoul, 2008

[5] S.B.Choi and C.H.Lim, “Comparison of products and classify of SSL accelerator”, Cryptography & Network Security Center Future Systems, Seoul, 2001

[6] M.J.B. Robshaw, “Stream Ciphers, RSA Laboratories Technical Report TR-701”, July 25, 1995

[7] Fauzan Mirza, “Block Ciphers And Cryptanalysis,” Royal Holloway University of London, 1998

[8] Xukang Lu, Qishi Wu, Nageswara S.V. Rao and Zongmin Wang, "On Parallel UDP-based Transport Control over Dedicated Connections Dedicated Connections", IEEE, 2010

[9] S.H. Song, "S/W High-Speed data transfer platform; Rapidant", the Seoul Data Engineering Camp Conference, Seoul, 2011

[10] Dong Lu, Yi Qiao Peter A. Dinda Fabi´an E. Bustamante, “Modeling and Taming Parallel TCP on the Wide Area Network,” IEEE, 2005

저자 소개

박 형 일(정회원)

- 2004년 8월 : 연세대공학대학원 컴퓨터공학과 졸업
- 2010년 2월 : 숭실대학교 컴퓨터학과 박사과정
- 1994년 9월 ~ 현재 : YTN 근무

<주관심분야 : 방송/통신/IT융합, 네트워크 가상화, Cloud computing, High-speed Data Transmission, Network Security \>

신 용 태

- 한양대학교 산업공학과(학사)
- Univ. of lowa 컴퓨터학과(석사)
- Univ. of lowa 컴퓨터학과(박사)
- 1995년 ~ 현재 : 숭실대학교 컴퓨터학과 교수

<주관심분야 : 컴퓨터 네트워크, 분산 컴퓨팅, 인터넷프로토콜, 초고속 통신망, 전자상거래기술, 인터넷보안>