Design of the Adaptive Encrypted Transmission Using a High Speed Parallel Transfer in the Open IPTV

Hyoungyill Park[1], Sangdo Lee[1], Yongtae Shin[1],
Department of Computing, Soongsil University,
511 Sando-Dong, Dongjak-Gu, Seoul, Korea
{harrypark58, piterlee}@gmail.com, shin@ssu.ac.kr

Abstract. For the transmission of large amount of HD contents in the open IPTV, wire and wireless networks for transfer should be able to guarantee necessary QoS or use the maximum resources provided by networks, and the transmission of secure network suited to transmission of contents is necessary. In this study as the available resources is made the best use of using the transmission of parallel TCP, a contents transmission method for safely transmitting the on-demand large amount of HD video to the STB of viewers through partial and adaptive encryption model is proposed. This proposed model can enable us to realize the efficiency of computing resources through adaptive end to end security and the effective use of best effort network with QoS not guaranteed.

Keywords: Adaptive Encryption, High-speed Transmission, Parallel TCP, HD Video, IPTV

1 Introduction

Many different forms of broadcasting services with Push or Pull method such as smart TV, Connected TV, and Open Architecture IPTV connected to internet have emerged [1]. The important thing in transmitting broadcasting services through the Internet is whether QoS can be guaranteed. The traditional encryption method is to uniformly process all the contents by applying encipherment [2]. Such a method causes to make many troubles in conveying large amount of HD multi-media contents within a time required to transmit. Accordingly maximizing the efficiency of available network and processing aappropriate encryption and decryption function are a very important factor in performance of real-time or similar multi-media broadcast system. Namely, the security of cipher algorithm itself shall be strengthened, but due to such strong securities the real-time of multi-media shall not be inhibited. In this study without regard to CAS and DRM system only new security architecture applicable to open internet environment is proposed.

2 Next Generation IPTV Information Protection Requirements

Currently the commercialized security technologies of broadcasting contents and services are CAS and DRM. CAS is the security technology to control the use right of contents to watch real-time contents, while DRM is the one to protect the illegal distribution of digital contents using the encryption technology for VOD business [2]. The security requirement newly proposed for IPTV in the work item document, X.IPTVsec-2 of ITU-T is as follows.

- Cryptographic and Perceptual Security.
- Efficient and selective encryption should be supported.
- The encryption mechanism should not either reduce the compression ratio of multi-media.
- Format compliance: The encoded video should be using the standard decoder.
- Error tolerance/Robustness: The encryption mechanism should have an error tolerance / error robustness.
- End to end security should be maintained.
- Adaptive resolution: The encryption mechanism should be supported various transmission band, picture quality, and coordinate the level of security strength [3].

The real-time type contents should be transmitted so as to be suited to the real-time stream, while the NRT(Non-Real Time) type contents should meet the high efficiency and information protection requirement suitable for uninsured Network transmission situation [4].

3. Related Works for High-speed and Secure Transfer

3.1 Parallel TCP for High-Speed Transfer of Large Files

IPTV should be transmitted at average 6~8Mbps in HDTV using H.264 compression video codecs of 1920*1080i pixel, which require still more bandwidth for 3DTV or UDTV(Ultra Definition TV). TCP which is quite widely used for communications is not suitable enough to use the available bandwidth by the characteristics of traditional protocol [5]. The expression (1) means that in case of Single TCP Connection, it greatly affects RTT and Buffer Size in transmission performance. In order to complement the decreased performance by AIMD (Additive increase / Multiplicative Decrease) phenomena occurred at Single TCP Flow and maximize the use of link bandwidth, Parallel TCP consisting of Multi sockets by multiple threads can compose the link with high bandwidth.

$$BW = \frac{MSS}{RTT\sqrt{\frac{2bp}{3}}} \quad . \tag{1}$$

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

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

As the Network bandwidth shown in the expression (2), using parallel TCP communication with multiple transports executed at end to end increases in proportional to the number of parallel TCP, multiple TCP connection can be found to maintain high efficiency bandwidth [6], [7].

3.2 SSL Algorithm for Secure Communication

SSL is an application protocol devised for E2E security of TCP under Client-Server environment, which conducts the authentication of server and client through identification process of certificate. The integrity to detect the forgery of data is offered by maintaining the confidentiality through symmetric cryptosystem and using MAC (Message authentication code). And the secret key used in symmetric cryptosystem algorithm is set through key exchange algorithm using Public Key encryption method. SSL is operated between classes of TCP and HTTP, which is set to operate at reliable transport protocol [8].

Client sends Client Hello message to the server, which responds by Server Hello message. At this time Client and Server set security parameters by exchange keys of each other. Communication SSL set an encryption algorithm using Handshake protocol, and shares their secret key and communicates with each other using public key exchange algorithm. Server and Client can make communication protected for a secure transmission of application data by setup of SSL. Especially for SSL VPN the safe channel will be set up by Public Key encryption algorithm, each other's secret key (symmetric key) will be shared, and the safe end to end communication will be made [9].

4. Design of Secure High-Speed Transmission

The security requirements necessary for this and the method to use network with maximum efficiency are proposed. As to perform encryption on all the data amounting to hundreds of MB ~ GB to support fast encryption and decoding consumes excessive resources between computer systems for transmission. Accordingly for a large capacity high speed file transmission while transmitting Parallel TCP, a part of blocks generated from file block pool will have to be encrypted, transmitted through generated specific channel, and decoded by encryption key exchanged to each other.

First for setup process of secure transfer the Cipher Suite for SSL protocol should be set up between Receiver and Server. Accordingly the end to end system is composed just like in a form of partial encryption and transmission by Cipher data channel transmitted on Parallel TCP Stream. Contents Provider shall exchange key by asymmetric encryption method proposed by SSL VPN when generating Parallel TCP channel transmitted for end to end information protection service together with high speedy contents transmission of server for multimedia service.

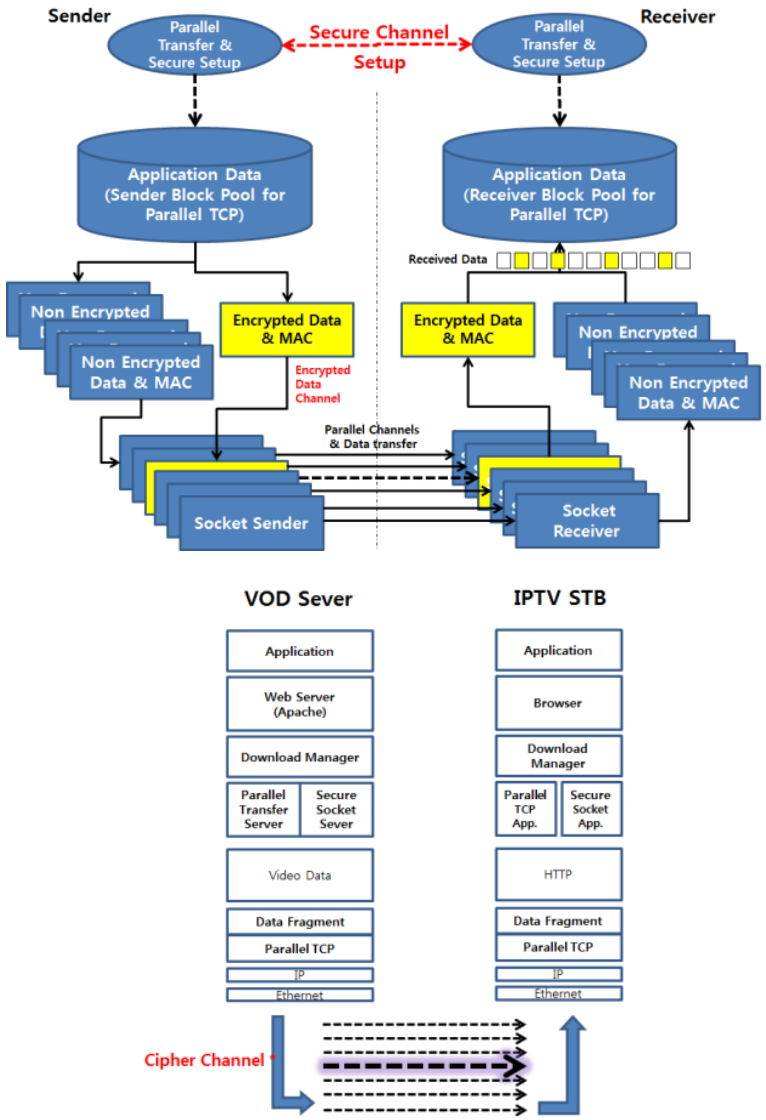

Figure 1. Creation of secure channel and transmission of video data in parallel transfer

The lowered efficiency of TCP transmission by AIMD shall be protected and the use of available network resources provided between Server and Receiver shall be maximized by making Parallel TCP connection for composition of reliable network to use available network resources as much as possible to guarantee QoS for transmission of VoD video file.

It is difficult to restore the entire multimedia data only with restoration by plain data channel even though Sniffing or Spoofing occurs by attacker during the transmission on IPTV Network, the restoration of encryption channel and combination of multiplexed data block will be more difficult. When the restoration of multimedia data intercepted by attacker for the actually expected phenomena it is impossible to make a complete restoration of video media, which causes to make abnormal restoration due to block phenomena of image or unrestored Data. Accordingly the partial, selective and adaptive encryption transmission mechanism proposed in this study using parallel TCP can find out the sufficient condition to make high efficiency of the transmission network or computer processing resources and to make secure multimedia.

5. Conclusion

This study is designed to provide E2E information protection service as partial and selected encryption transmission mechanism by retransmitting contents at a high speed using the available Public network as most as possible, which has also the advantage to adaptively control and protect the transmission channel of large capacity video file according to service level. Accordingly the Processing cost to be excessively used for encryption and decoding of E2E is reduced by selectively introducing SSL mechanism based on Parallel TCP, and controlling the level of information protection mechanism security strength, and the proper information protection transmission mechanism is adaptively offered to VOD service level without physical Device. For smart TV unapplied in premiere network it is possible to safely apply transmission of large capacity contents by application of simple STB without separate physical configuration for E2E information protection.

References

1. Open IPTV Forum, "OIPF Relese 2 Specification Volume 1 Overview V2.1," pp. 5, Tune. 2011
2. Korea Information Security Agency, "A study on the development of the IPTV security guide for the IPTV service provider," pp. 25-26, June. 2009
3. ITU-T "The first draft Recommendation X.iptvsec-2, Functional requirements and mechanisms for secure transcodable scheme of IPTV," 2008
4. Telecommunications Technology Associations, "TTAK.KO-07.0002/R1, Standard for Terrestrial Open Hybrid TV," pp. 11, 2011.12
5. Xukang Lu, Qishi Wu, Nageswara S.V. Rao and Zongmin Wang, "On Parallel UDP-based Transport Control over Dedicated Connections Dedicated Connections," 2010
6. Dong Lu, Yi Qiao Peter A. Dinda Fabi´an E. Bustamante, "Modeling and Taming Parallel TCP on the Wide Area Network," 2005.
7. Sunghak Song, "S/W High-Speed data transfer platform: Rapidant," Seoul Data Engineering Camp, June. 2011
8. S.B.Choi, C.H.Lim, "Comparison of products and classify of SSL accelerator," Cryptography & Network Security Center Future Systems, pp. 3-16, 2001
9. Lawrie Brown, Australian Defense Force Academy, http://williamstallings.com/Extras/Security-Notes, April, 1996