情 報 保 護 學 會 誌
第19卷 第3號, 2009. 6

IPTV 컨버전스 환경에서 콘텐츠 보안 기술 동향

나 재 훈*

요 약

차세대 IPTV 서비스는 4A (Any-time, Anywhere, Any-device, Any-content)를 특징으로 하는 통방 융합의 서비스이다. 4A 서비스는 일반 대중이 자유롭게 콘텐츠의 생성과 소비가 가능하며, 전송환경과 디바이스의 종류에 맞게 안전한 미디어 변환과 콘텐츠의 재사용을 가능하게 한다. 본 고에서는 멀티미디어 보안에 적합한 선택적(Selective) 보안의 필요성과 이를 근간으로 하여 End-to-End 보안서비스를 제공하는 Transcodable 보안과 현재까지의 연구동향을 살펴본다.

Ⅰ. 서 론

방송과 통신 서비스의 융합이 빠른 속도로 진행이 되고 있는 시점에서 여러 가지 기술 대안이 제시되고 있다. 그중에 콘텐츠에 대한 저작권 보호에 대하여 콘텐츠 제공자, 서비스 제공자 그리고 콘텐츠 이용자들도 매우 큰 관심을 표현 하고 있다.

콘텐츠 보안에 있어서 CAS (Conditional Access Service)와 DRM (Digital Right Management)의 메카니즘의 연동이 주요 이슈로 나타나고 있다. 그러나 두 개의 다른 보안 메카니즘의 연동을 위한 보안 이슈 보다는 콘텐츠를 보안하는 융합된 해결방안이 산업적인 효과가 더 크게 나타날 것으로 생각 된다.

본 논문에서는 4A (Any-time, Anywhere, Any-device, Any-content) 서비스 지원을 목표로 하는 차세대 IPTV 인프라가 갖추어야 할 콘텐츠 보호 기술에 대하여 살펴본다.

Ⅱ. 차세대 IPTV 보안 이슈

차세대 IPTV 서비스는 개방형, 환경적응형(Adaptive), 4A 서비스 제공을 목표로 한다. 이러한 인프라 환경에서 콘텐츠 보안을 위한 필수 요구사항은 아래와 같이 생각 될 수 있다.

- SCP(Service & Content Protection) 지원
- 환경적응적 미디어 보안 (Adaptive Security)
- 콘텐츠의 재전송 보안
- OSMU(One Source Multi Use)
- End-to-end 보안
- 이동성 지원(Vertical Hand-Off)
- 개인화 /커뮤니티 서비스

Ⅲ. Selective 보안의 필요성

텍스트를 암호화하는 전통적인 보안 방법을 멀티미디어에 적용한다면, 압축된 비트스트림에 통째로 암호를 적용하는 것이 당연한 방법으로 생각 한다. 그러나 암호를 하는 대상이 텍스트가 아니고 멀티미디어라 점을 고려 한다면, 다음과 같은 문제점들을 검토 하여야 한다.

1. Large data size
2. Limitedly allowed network's bandwidth
3. High transmission rate
4. Low computing powered device
   (limited memory, processing power, battery)

상기의 문제들은 네트워크상의 서버나 단말기들에게 콘텐츠의 전송 또는 암호처리에 큰 부하를 주기 때문에 실시간성을 제공할 수 없다. 그러므로 멀티미디어 보안 처리에 대한 부담을 줄이고, 원활한 영상 서비스 제공을 위하여 선택적(Selective) 암호방식이 필요한 것이다.

그리고 멀티미디어 보안에 있어서 보장되어야 할 요구사항으로 다음과 같이 5가지를 생각해 볼 수 있다.

* 한국전자통신연구원 (jhnah@etri.re.kr)

3.1 보안수준

주관적인 면이 강한 것이지만, 선택적 암호를 적용한 멀티미디어 데이터를 사람이 지적으로(Perceptual) 인식을 하여서는 안된다. 그리고 암호키나 암호문에 대한 해독에 대한 보안수준이 적정선을 유지하여야 한다.

3.2 효율성

암호양을 줄이거나 경량의 암호 알고리즘과 같은 방법을 이용하여 전송과 콘텐츠 보안 처리 지연을 발생하여서는 안된다.

3.3 압축률

멀티미디어 코덱의 압축률을 보안처리로 인하여 지대한 부정적인 영향을 미쳐서는 안된다.

3.4 Format Compliance

멀티미디어 데이터에 암호 처리된 암호문을 디코더가 처리할 수 있어야 한다.

3.5 오류 감내성(Error Tolerance)/Robustness

전송상에서 암호문에 발생된 한 비트 오류가 복호화 단계에서 다른 비트에 영향/파급을 주어서는 안된다.

IV. Transcodable 보안

Transcoding의 어휘적인 의미는 코드체계 1에서 코드체계 2로 코드를 변환하는 것이다. 그리고 Transcodable 보안은 암호화된 객체를 그대로 코드체계를 변환한다는 것이다. 그러나 이러한 기법은 아직 많은 기술적인 어려움이 있다. 기본적으로 코드체계가 Transcodable 보안을 수용할 수 있는 체계로 설계가 되어야 하며, 기본적으로 선택적 암호 방식을 채택하게 된다.

현재까지의 Transcodable 보안의 개념을 수용하는 기술의 예로서는 SVC (Scabalble Video Codec), JPSEC, MPEG-21 등과 같은 것들이 있다. SVC는 Scalable 개념을 갖고 있는 코덱이며, 콘텐츠 인코딩 과정에서 공간적 (spatial), 시간적 (temporal) 그리고 화질적 (SNR) 확장 가능한 특징을 이용함으로써 가능하다. 한 번의 압축된 비트스트림에서 서로 다른 여러 종류의 해상도, 화질, 프레임율을 갖는 영상을 다양한 디바이스와 다양한 네트워크 환경에서 적응적(Adaptive)으로 복원할 수 있으며 이단계에서 트랜스코딩이 이루어지게 된다.

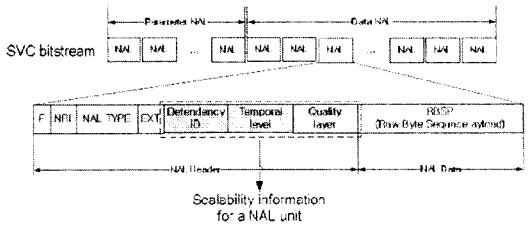
Transcodable 보안은 scalability 관점에서 크게 scalable 보안 기술과 non-scalable 보안기술로 분류할 수 있다. Scalable coding에서는 공간, 시간, 품질적 우선 순위에 따라 다양한 스케일러블 특성이 제공되며, non-scalable coding의 경우는 이와 비교하여 상대적으로 제한적인 방법으로 확장성을 제공하고 있다.

4.1 SSS (Secure Scalable Streaming) Framework[1][2]

SSS는 scalability를 지원하는 다양한 코덱 (Motion JPEG-2000, EBCOT, 3D Subband Coding, MPEG-4 FGS)에 대하여 secure scalable packet을 생성하고 secure transcoding을 지원하는 프레임워크이다[1]. SSS의 핵심은 scalable coding과 progressive encryption기술이다. Scalable coding은 encoding 단계에서 데이터의 공간, 시간, 품질적인 우선 순위를 가지도록 하여 중간 노드에서 비트스트림에 대한 truncation 혹은discarding만으로 특정 요구조건에 맞는 비트스트림을 얻을 수 있는 encoding scheme이다. Progressive encryption은 데이터를 순차적으로 암호화하고 복호화하는 방법으로써, 블록암호의 CBC (Cipher Block Chans) 방식과 스트림 암호가 이에 해당한다.

4.2 Layered Protection Scheme[3]

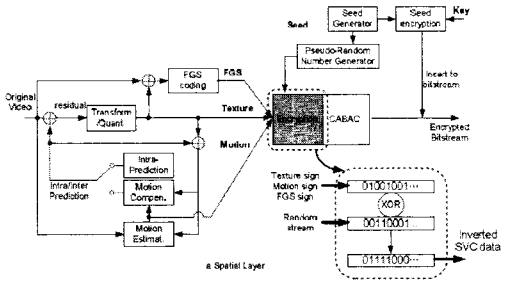
Layered Protection Scheme은 H.264/AVC SE인 SVC (Scalable Video Coding)를 대상으로 하며, SVC의 NAL (Network Abstraction Layer) 데이터에 대하여 레이어별 선택적 암호화를 수행하고 키를 부여함으로써 스케일러블 특성을 유지하면서 데이터의 보안을 제공하는 방식이다[3]. [그림 1]은 SVC NAL unit 구조를 나타낸 것으로서, 공간, 시간, 품질적 조합에 따라 선택적으로 레이어별 암호화를 수행할 수 있다.



〔그림 1〕 SVC bitstream의 NAL unit syntax

Protected Encoding Scheme은 SVC 인코딩 과정에서 레이어별 특정 파라미터를 선택적으로 암호화함으로써 scalable security를 제공하는 방식이다[4][5][6].

[4]에서는 [그림 2]와 같이 공간, 시간, 품질적 레이어에서 인코딩된 Texture, Motion, FGS의 부호비트에 대하여 CABAC (Context Adaptive Binary Arithmetic Coding) 직전에 암호화하여 비트스트림을 생성한다. 그리고 각 레이어별로 암호화된 비트스트림은 레이어별 암호화 키 관리를 부여함으로써 접근제어를 제공한다. 즉, 하위 레이어에 대한 키 권한을 가진 자는 상위 레이어의 콘텐츠를 복호화할 수 없고, 상위 레이어의 키 권한을 가진 자에 대해서는 하위 레이어의 키 권한을 가질 수 있도록 설계하였다. 이렇게 함으로써 SVC기반의 멀티미디어 서비스를 제공할 때 다양한 단말에 따른 접근제어를 가능하게 한다.



〔그림 2〕 SVC 레이어별 선택적 암호화

[5]에서는 기본 계층 (Base Layer)에 대해서는 DC, AC 계수 그리고 모션벡터를 선택적으로 스크램블링 기법을 사용하고, 추출된 정보들은 암호화 키 KBase를 사용하여 암호화하고, 상위 계층 (Enhancement Layer)에 대해서는 암호화 키 KEnhan를 사용하여 각각 인터 모드에서는 모션벡터의 크기를 변환하는 스크램블링 기법을 적용하고, 인트라 모드에서는 예측모드에 대해서 회전 변환하는 스크램블링 기법을 적용한다. 기본 계층과 상위 계층에 대하여 차별된 방식을 적용한 이유는 상위 계층에서는 하위 계층을 통해 복원된 영상을 참조 프레임으로 하여 예측한 영상과 원하는 scalability 영상에 대한 차이 정보가 계층별로 인트라 또는 인터 모드에 따라 코딩되므로, 상위 계층의 정보를 통해서 기본 계층보다 더 높은 공간, 시간, 품질의 영상을 얻을 수 있기 때문이다. 즉, 상위 계층의 경우는 기본 계층 보다 더욱 보안성이 높아야 한다는 가정이다.

한편, SVC의 상위 계층은 기본적으로 기본 계층의 정보를 사용하기 때문에 기본 계층을 보다 안전하게 암호화해야 한다는 관점에서 기본 계층의 경우, 인트라 예측 모드, 모션벡터 차이값, 그리고 텍스쳐 부호비트 등 세 가지 도메인을 암호화하는 방식이 제안 되었다[6]. 그리고, 상위 계층의 경우, 공간 및 품질적 레이어에 대해서는 레이어별 텍스쳐 부호 비트만 암호화하고, 시간적 레이어에 대해서는 모션벡트 차이에 대한 부호 비트만 암호화한다.

V. 결 론

멀티미디어 데이터에 대하여 전통적인 보안 방식과는 다르게, 선택적(Selective) 보안 메카니즘이 필요하다는 것을 살펴보았다. 그리고 선택적 보안 메카니즘을 기초로 Transcodable 보안 메카니즘에 대한 연구동향을 소개하였다. 이러한 메카니즘은 CAS/DRM 연동이 아닌 CAS, DRM이 통합된 SCP 개념을 구현할 수 있는 기초적인 메카니즘이 되는 것이다.

IPTV 콘텐츠의 안전한 재전송을 위하여 End-to-end 보안 서비스가 보장되어야 한다. E2E 보안 서비스를 제공하기 위하여 Trancodable 보안 메카니즘이 고안되었으며, 이는 선택적 암호 방식에 근간을 둔다. CAS와 DRM이 융합된 SCP 서비스를 제공하는 기술인 Transcodable 보안 기술을 기반으로 콘텐츠 보안 산업의 육성 및 IPR확보가 시급하다고 사료되며, 그 산업적 효과를 더욱 확대하기 위하여 국제표준 제정이 절실히 필요하다고 생각된다.

참고문헌

[1] Susie Wee and John G. Apostolopoulos, "Secure Scalable Streaming enabling Transcoding without

Decryption", 2001 ICIP, 2001.

[2] NECTAR, "Secure Scalable Multimedia Streaming", CANADA, http://www.dsp.utoronto.ca/nectar/projects/ssms/index.php.

[3] 헨드리, 김문철, 함상진, 이근식, 박근수, "스케일러블 비디오 부호화에 대한 계층적 보호 기법", 2006 한국방송공학회학술대회, 2006.

[4] Yong Geun Won, Tae Meon Bae, and Young Man Ro, "Scalable Protection and Access Control in Full Scalable Video Coding", IWDW 2006, LNCS 4283, 2006.

[5] 이승제, "H.264/AVC SE에서의 다중 암호화 기술을 이용한 저작권 보호", 고려대 석사학위논문, 2007.02.

[6] Su-Wan Park, Sang-Uk Shin, "Efficient Selective Encryption Scheme for the H.264/Scalable Video Coding(SVC)", 2008 Fourth International Conference on Networked Computing and Advanced Information Management, 2008.

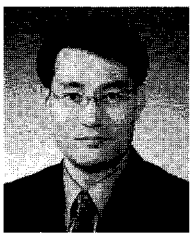
[7] John G. Apostolopoulos, "Secure Media Streaming & Secure Adaptation for Non-scalable Video", 2004 ICIP, 2004.

[8] Nithin M Thomas, Damien Lefol, David R Bull, David Redmil, "A Novel Secure H.264 Transcoder Using Selective Encryption", 2007 ICIP, 2007.

[9] Tien-Yan, Ting-Wei Hou, and Shau-Yin Tseng, "Hierarchical Key Management of Scalable Video Coding", Proc. of the Third International Conference on International Information and Multimedia Signal Processing, 2007.

[10] Shigue Lian, "Digital Rights Management for the Home TV Based on Scalable Video Coding", IEEE Trans. on Consumer Electronics, vol. 54, 2008.

〈著者紹介〉



나 재 훈(Nah Jae Hoon)

종신회원

1985년: 중앙대학교 컴퓨터공학과 공학사

1987년: 중앙대학교 컴퓨터공학과 석사

2005년: 한국외국어대학교 전자정보공학과 박사

1987년~현재: 한국전자통신연구원

<관심분야> IPTV보안, P2P 보안, IPv6/MIPv6 보안