모바일 환경에서 상황 정보에 기반한 적응형 암호화 기법에 관한 연구

장혜영*, 최종천*, 윤영민*, 조성제*
*단국대학교 정보컴퓨터학부
e-mail: {hychang, godofslp, maverick, sjcho}@dankook.ac.kr

A Study on Adaptive Cryptography Methods based on Context Information under Mobile Environment

Hye-Young Chang*, Jong-Cheon Choi*, Young-Min Yun*, Seong-Je Cho*
*Department of Computer Science, Dankook University

요 약

휴대폰, MP3 플레이어 등의 모바일 기기가 일반화되고 SoC(System-on-a-Chip) 기술이 발전하면서 모바일 콘텐츠의 이용 및 모바일 DRM(디지털 저작권 관리)에 대한 관심이 증가되었다. 모바일 기기의 경우 한정된 컴퓨팅 자원으로 인해 큰 멀티미디어 파일에 대한 암호화 연산의 오버헤드가 크며 그에 따른 전력 에너지 소모 또한 큰 부담이 된다. 본 논문에서는 모바일 환경에서 대상 데이터의 중요도 및 자원의 상태에 따라 에너지 소모를 줄일 수 있는 적응형 암호화 기법에 대해 제안한다. 제안하는 주요 방법으로, 저가의 콘텐츠에 대해서는 부분 암호화 기법 적용, 중간 가격 파일에 대한 다중 암호 방식의 적용, 모바일 기기의 사양에 따라 서로 다른 암호화 기법의 적용, 통신 상태나 배터리 용량에 따른 암호화 기법의 적용 등이 있다.

1. 서론

최근에 PDA, 휴대폰, MP3 플레이어 등 모바일 휴대 기기가 매우 일반화됨에 따라, 많은 사람들은 모바일 단말기를 사용하여 멀티미디어 콘텐츠(contents)를 더욱 더 많이 사용하게 될 것이다. 이에 따라 모바일 기기에서 디지털 콘텐츠 지적 재산권을 관리하기 위한 모바일 디지털 저작권 관리(Mobile Digital Rights Management, 즉 Mobile DRM)가 중요해지고 있으며, OMA(Open Mobile Alliance) DRM 및 마이크로소프트사의 윈도우 미디어 DRM과 같은 표준이 제시되고 있다[1, 2, 3].

DRM에서는 콘텐츠를 보호하기 위해 콘텐츠 파일을 암호화한 다음 배포하며, 적법한 사용자에게만 복호화 키를 전달하여 재생할 수 있도록 하고 있다. 유선 환경의 DRM과 같이 모바일 DRM 표준의 경우에도 콘텐츠 암호화를 위해 대칭형 블록 암호 방식인 AES 카운터(CTR) 모드를 사용하는 것이 일반적이다.

유선 환경과 달리, 모바일 단말기의 경우 CPU 처리, 메모리 공간, 배터리 파워 등과 같은 계산 자원들 면에서 매우 제한적이다. 이에 반해, 멀티미디어 콘텐츠 파일의 경우 데이터 용량이 매우 크며, 암·복호화 연산은 계산 중심적으로 큰 에너지를 소모시킨다.

이에 CPU 처리율(throughput)과 에너지 소모량 면에서 무선 환경에서 블록 암호 알고리즘인 AES와 스트림 암호 알고리즘인 RC4의 성능을 비교한 연구가 수행되었다[5, 6]. 그 연구 결과에 의하면, 데이터의 양이 90바이트 이하일 경우에는 AES가 더 좋은 성능을 보이고, 90바이트 초과할 경우에는 RC4가 훨씬 더 좋은 성능을 보인다[5, 6]. 그러나 안전도 면에서 RC4는 보안 취약성(vulnerability)을 가진다[8].

한편으로 멀티미디어 데이터 암호화의 부담을 덜기 위해 선택적 암호화(selection encryption)가 연구되었다. 선택적 암호화는 멀티미디어 데이터의 일부분을 암호화하거나 변형시켜, 만일 정상적으로 복호화하지 않고 재생할 경우, 멀티미디어 데이터의 품질을 시청하기에 적합하지 않도록 만드는 기법이다[9, 10, 11].

본 논문에서는 자원의 상태나 멀티미디어 콘텐츠의 중요도에 따라 적응력 있게 콘텐츠 및 통신 패킷을 암호화하는 방법을 제안한다. 즉, 주어진 상황정보(context information)에 따라 유연하게 디지털 콘텐츠 파일과 패킷을 암호화 또는 복호화하는 방법을 제안한다.

2. 관련 연구

휴대폰 벨소리, MP3 파일, 비디오 클립 등의 멀티미디어 파일의 크기는 작게는 200KB이고 크게는 700MB로 텍스트 파일에 비해 크기가 매우 크다. 이처럼 큰 파일을 휴대 단말기에서 AES(대칭키 암호화 방식의 표준으로 블록

암호화 기법)로 암·복호화를 수행하는 것은 에너지 소모 면에서 매우 오버헤드를 유발시킬 수 있다[5, 6].

멀티미디어 파일에 대한 선택적 암호화의 경우, 암호화되지 않은 부분으로부터 암호화된 부분의 데이터에 대한 정보를 알아낼 수 있다는 보안상의 문제가 존재한다. 또한 대부분의 선택적 암호화 기법은 멀티미디어 파일 압축 방식의 특성을 이용하므로 멀티미디어 파일 압축과 암호화가 서로 연관되어 있다. 때문에 멀티미디어 파일 압축과 암호화를 다른 계층으로 보면서 독립적으로 보안 기법을 적용하기 어려운 면이 있다[9, 10, 11].

상황인지(context-awareness) 기반의 시스템 모델에서 중심이 되는 상황 정보는 위치(location)나 시간(time) 등이다[8, 13]. 그러나 본 논문에서는 주로 암호화할 데이터의 크기 및 중요도(가격), 모바일 기기의 사양, 통신 상태 등을 상황 정보로 활용한다.

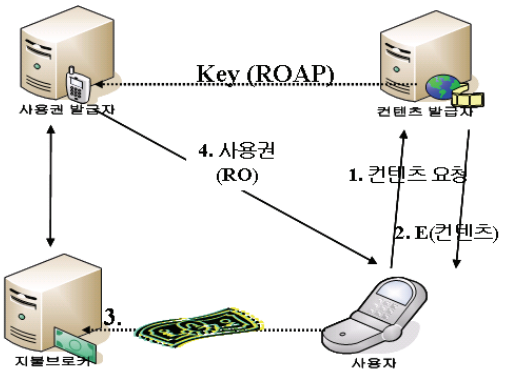

그림 1 OMA DRM

3. 모바일 환경에서 적응력있는 암호화 모델

본 논문에서 고려하고 있는 모델은 무선 환경의 클라이언트-서버 모델이며, 서버(콘텐츠 유통 서버 또는 콘텐츠 발행자 시스템)의 계산 자원은 무한대에 가깝다고 보며 클라이언트(소비자, 가입자)는 계산 능력 및 배터리 용량이 제한된 모바일 단말기이다. 세부적인 시스템 구조는 OMA DRM 모델에 따른다.

주어진 환경에서 에너지 소모를 줄이고, 적절한 보안 강도를 제공하며, 임의 데이터 블록에 대한 랜덤 접근을 지원할 수 있는 멀티미디어 콘텐츠 파일 암호화 기법에 대해 제안하고자 한다. 또한, 여기서 고려하는 멀티미디어 파일들은 크기가 커고 저가이며 서비스 품질(QoS: Quality of Service)에 민감하다. 주안점은 데이터 암호화 방식이며, 암·복호화 키 분배 및 관리는 다루지 않는다.

본 논문에서는 주어진 상황정보에 따라 적응력이 있게 수행되는 암호화 방식을 제안한다. 여기서 상황정보란 소비자 휴대 단말기의 모델/사양, 디지털콘텐츠의 가격/중요도 또는 크기, 통신(네트워크) 상태 등을 의미한다. 휴대폰 및 MP3 플레이어, PMP 등과 같은 이동 단말기의 경우 데스크톱 PC에 비해 계산 능력도 떨어지고 배터리 소모에 대해 매우 민감함으로 경량 암호화 방식이 좋다.

콘텐츠 파일이나 통신 패킷의 내용이 비밀(top secret 또는 secret)로 분류되었거나, 또는 암호화할 데이터 크기가 200KB 이하일 경우, 또는 가격이 10,000원 이상일 경우에는, 해당 데이터를 상용 시스템에서 사용되는 안전한 AES 알고리즘이나 공개키 방식으로 암호화한다. 그 예로, OMA DRM에서 권리 객체(right object)는 클라이언트의 공개키로 암호화되어 배포된다.

본 연구에서 제안하는 상황인식 기반의 암·복호화 기술은 다음과 같다.

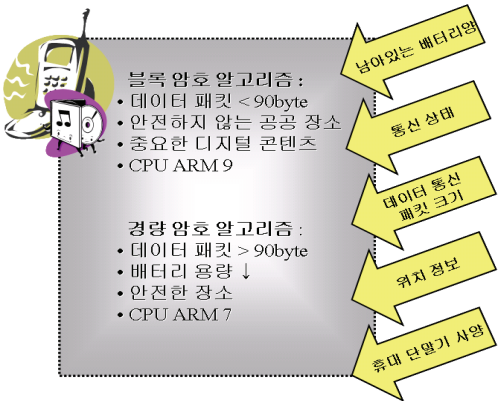

그림 2 상황정보에 기반한 암호화 기법

3.1 부분 암호화 방식

이 방식은 멀티미디어 파일의 크기가 200KB 이상이고, 가격이 1,000원이하인 콘텐츠에 대해 적용한다. 대상 파일의 크기 및 가격은 조정 가능하다.

이 기법은 암호화 시에 디지털콘텐츠의 일부분은 암호화하고 그 외 나머지 부분은 원래대로 평문으로 유지하는 방식이다. 커다란 디지털콘텐츠 파일 전체를 암호화하면 계산 부하가 크므로 파일의 특정부분만을 암호화하여 계산량과 에너지 사용량을 절약하자는 것이다. 첫 번째 방법으로, 멀티미디어 파일을 프레임(일정크기로 1초간 재생할 수 있는 분량의 크기) 단위로 분할하여, 짝수 번째 프레임들(0번, 2번, 4번등의 프레임)은 암호화하고 홀수 번째 프레임들(1번, 3번, 5번등의 프레임)은 암호화하지 않고 그대로 두는 방식이 그 예이다. 이 경우, 불법 사용자가 재생할 경우에는 1초 재생한 후 1초 재생 불가 과정이 반복되어 시청각 품질이 떨어지게 된다. 이 경우, 프레임의 크기를 좀 더 유연하게 조정하는 것도 고려할 사항이다.

두 번째로 디지털콘텐츠 파일의 헤더 부분만 암호화하고 나머지는 그대로 유지하는 방법을 적용할 수도 있다. 대부분의 멀티미디어 파일의 경우 헤더부분에 주요 정보가 있어 헤더만 암호화하더라도 어느 정도의 디지털콘텐츠 보호 효과가 있다. 만약, 멀티미디어 파일의 경우 중간 중간에 프레임 헤더가 존재한다면 각 프레임 헤더 부분도

암호화하는 방법을 적용하는 것도 가능하다.

제안하는 "부분 암호화 기법"은 기존의 "선택적 암호화"와 유사하나, 파일 압축과도 독립적으로 암호화를 수행한다는 점(구현이 용이하며, 이식성이 향상)과 어떤 경우에는 콘텐츠 파일의 헤더 부분만 암호화한다는 점(암·복호화되는 부분이 더 적음)에서 차이가 있다.

3.2 다중 코딩 방식을 적용한 파일 전체 암호화

이 기법은 디지털 콘텐츠 파일 전체를 암호화하는 것으로, 멀티미디어 파일의 크기가 500KB 이상이고, 가격이 1,000원~10,000원인 콘텐츠에 대해 적용된다. 대상 파일의 크기 및 가격은 조정 가능하다.

여기서 제안하는 방법은, 한 디지털콘텐츠 파일 전체를 암호화하기 위해 하나의 암호화 방식만을 사용하는 것이 아니라, 한 디지털콘텐츠 파일에 여러 방식의 암호화 알고리즘들을 적용하는 것을 말한다. 최근 상용 DRM 제품의 경우 디지털콘텐츠를 AES로 암호화하여 배포 관리하는 것이 일반적이다. AES의 경우 안전하기는 하지만 큰 데이터의 경우 에너지 소모량이 커서 모바일 단말기에서는 적용하기에 문제점이 있다.

본 기법의 주요 개념은, 암호화 시 디지털콘텐츠 파일의 일부분은 안전한 블록 암호화(AES, Triple DES 등)를 적용하고 나머지 부분은 계산량이 적은 경량 암호화(RC4와 같은 스트림 암호화, DES 등)를 적용하자는 것이다.

즉, 한 디지털콘텐츠 파일의 일부분은 AES를 적용하여 안전도를 높이고, 나머지 부분은 RC4를 적용하여 에너지 소모를 줄이고자 하는 방식이다. 예로서 디지털콘텐츠 파일을 프레임 단위로 분할하여 매 3번째 프레임은 AES 블록 암호화를 적용하고 나머지 부분은 RC4 스트림 암호화[12]를 적용하는 방식이다. 이 경우, 디지털콘텐츠 파일의 1/3은 안전한 블록 암호화, 2/3는 경량 암호화 방식을 적용한 후 유통된다.

3.3 상황 정보 기반의 파일 암호화 방식

본 방식에서는 휴대 단말기 사양(CPU 유형[1], 메모리 용량 등), 콘텐츠의 중요도 등에 따라 서로 다른 콘텐츠 암호화 방식을 제안한다.

먼저 휴대 단말기가 최신 모델(성능이 좋은 CPU, 큰 메모리, 네트워크 프로세서나 디지털 신호 프로세서 장착)인 경우에는 AES와 같은 안전한 블록 암호화 방식으로 디지털콘텐츠를 전체 암호화한다.

단말기 사양이 구형 모델일 경우에는 계산량 및 배터리 소모가 적게 부분 암호화, 또는 다중 코딩 방식을 적용한 파일 전체 암호화 등의 방법으로 디지털콘텐츠를 암호화하여 배포 및 관리한다.

매우 중요한 디지털콘텐츠(예로 기밀사항이나 고가의 정보를 포함한 PDF 문서 파일)의 경우에는 단말기 사양에 무관하게 AES와 같은 안전한 블록 암호화 방식으로 파일 전체를 암호화 하여 배포 및 관리한다.

디지털콘텐츠의 가치가 높지 않을 경우, 즉 저가의 휴대폰 벨소리, MP3 등의 디지털콘텐츠의 경우에도 부분 암호화, 또는 다중 코딩 방식을 적용한 암호화 등의 방법으로 디지털콘텐츠를 인코딩하여 배포 및 관리한다.

3.4 상황 정보 기반의 데이터 패킷 암호화 방식

본 방식에서는 남아있는 배터리 용량, 통신 상태, 데이터 통신 패킷의 크기 등에 따라 다른 패킷 암호화 방식을 제안한다.

무선 통신 시에 패킷 암호화에 사용되는 기본 암호화 알고리즘은 AES이다. 또한 데이터 패킷의 크기가 90바이트 이내일 경우에도 항상 AES를 사용하여 암호화한다. 그러나 패킷 길이가 90바이트를 초과하고 배터리 용량이 어떤 기준치(threshold) 이하로 떨어질 경우에는, 패킷 암호화 알고리즘으로 에너지 소모가 적은 RC4가 적용된다.

통신 상태에 따른 암호화 방식은 위치정보를 반영한 방식으로 모바일 클라이언트가 안전한 연구실 내부에 위치하는지 아니면 안전하지 않은 개방된 공공장소에 위치하는지에 따라 서로 다른 암호화 알고리즘을 적용하는 방식이다. 모바일 클라이언트가 안전한 연구실 내부에 위치하여 있다면 패킷은 RC4나 부분 암호화를 사용하여 암호화되어 전송된다.

만약, 클라이언트가 안전하지 않은 공공장소에 위치하여 있다면 패킷은 AES를 사용하여 암호화하여 전송된다.

4. 상황 정보의 우선순위

본 논문의 3절에서처럼 다양한 상황정보를 고려하다 보면 상황정보들 사이에 충돌이 발생할 수 있다. 예로 3.4절의 경우, 패킷 암호화에서 대상 패킷이 200바이트로 기밀 데이터를 포함하고 있는데 배터리 용량이 기준치 이하일 경우에 어떻게 할 것인가 하는 문제가 발생할 수 있다. 이 경우에는 안전도를 우선 고려하여 AES로 암호화하여 데이터를 전송할 수 있다. 즉, 상황 정보 및 암호화 방식에서 충돌이 발생하는 경우에는 다음과 같은 우선순위를 정하는 것이 필요하다.

암호화할 데이터의 중요도를 분류하여 그 값이 어떤 기준치 이상일 경우에는 AES로 전체 암호화를 적용한다. 즉, 안전도와 에너지 소모 면에서 충돌이 생기면 안전도를 우선 고려하여 암호화 방식을 적용한다.

5. 결론 및 향후 연구

휴대폰, PMP, MP3 등에서 유료 모바일 콘텐츠를 다루는 모바일 기기에서는 시스템 구현 이슈가 에너지 소모의 최적화, 적절한 보안 강도 유지 등이 있다. 휴대폰 벨소리,

1) 휴대폰의 경우, 구형 모델의 경우에는 CPU로 ARM 7 이하 모델을 채택하였으며, 스마트폰과 같은 최신 모델의 경우에는 CPU로 ARM 9 이상의 모델을 채택하고 있다.

MP3 파일, 비디오 클립 등의 콘텐츠 파일은 주요 비밀 문서에 비해 요구되는 절대적 안전도가 높지 않다. 본 논문에서는 휴대 단말기 상에서 콘텐츠 보호 및 패킷 암호화에 대한 적응력이 있는 암호화 기법을 제안하였다.

향후에는, 제안한 모델을 좀 더 구체화하고 실제로 구현하여 그 효용성을 분석할 계획이다.

참고문헌

[1] 한국정보과학회, 특집: DRM: 디지털 콘텐츠 저작권 보호, 정보과학회지, 제23권 8호, 2005.

[2] 한국정보처리학회, DRM 최신 국제표준 기술사양 분석 및 세계 유명제품 동향과 전망에 관한 연구, 한국소프트웨어진흥원, 2004.

[3] OMA DRM http://www.openmobilealloance.org.

[4] 김경중, 조성배, "상황인지 휴대폰 기술개발 동향", IITA주간기술동향, pp. 26-33, 2007.1.24

[5] Prasithsangaree, P., and Krishnamurthy, P., "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," In *Global Telecommunications Confercnce,* 3, 1445-1448, 2003.

[6] Prasithsangaree, P. and Krishnamurthy, P., "Analysis of tradeoffs between security strength and energy savings in security protocols for WLANs," In *Vehicular Technology Conference*, 7, 5219 - 5223, 2004.

[7] S. Fluher, l. Mantin, and A. Shamir, “"Weakness in the key scheduling algorithm of rc4,”" in the Eighth Annual Workshop on Selected Areas in Cryptography, 2001.

[8] Harry Chen, Tim Finin, and Anupam Joshi, "An Intelligent Broker for Context-Aware Systems", Adjunct Proceeding of Ubicomp 2003, pp. 12-15, Oct. 2003.

[9] B. Macq and J.-j. Wuisquater, "Cryptology for Digital TV Broadcasting," Proc. of IEEE, 83(6), pp. 944-957, Jun. 1995.

[10] C. P. Wu and J. Kuo, "Design of integrated multimedia compression and encryption systems,” in IEEE Transactions on Multimedia Vol.7, No.5, 2005.

[11] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video,” in IEEE Transactions on Multimedia, Vol. 5, 2003.

[12] R. Wash, Lecture Notes on Stream Ciphers and RC4.

[13] Guangsen Zhang and Manish Parashar, "Dynamic Context-aware Access Control for Grid Application", The Fourth International Workshop on Grid computing 2003, pp.101-108, 2003