이동 에이전트 기반의 컨텐츠 보호 기술

(A Contents Protection Technology based on Mobile Agent)

이경현* • 신 원**

1. 컨텐츠 보호 기술 개요

컴퓨터 기술과 네트워크 기술의 결합은 새로운 기술의 가능성을 제시하였고, 다양한 미디어의 융합을 통하여 새로운 멀티미디어 세상이 전개되기 시작했다. 쇼핑, 강의, 진료, 회의 등이 가상 세계에서 가능하게 되었으며 다양한 음악, 영화, 게임 등을 컴퓨터 네트워크를 통하여 실시간으로 즐길 수 있게 되었다. 즉, 인터넷을 통하여 텍스트, 이미지, 사운드, 동영상 등을 기반으로 하는 멀티미디어 컨텐츠를 누구나 쉽게 얻을 수 있고 이를 다시 복제, 배포할 수 있는 환경이 되었다. 이는 정보화 시대로 변화하면서 모든 미디어가 컴퓨터가 처리 가능한 디지털 데이터로 가공됨으로써 더 이상 원본과 복사본의 구분이 불가능하다는 것을 의미한다. 원본과 똑같은 품질을 가지고 거의 무한정으로 복제가 가능하고 네트워크를 통하여 빠른 시간에 배포가 가능하다는 것은 정보화 사회에서의 가장 큰 장점인 동시에 멀티미디어 컨텐츠에 대한 원작자의 저작권 자체가 위협받는 새로운 문제점으로 대두되고 있다. 최근 미국의 "냅스터", 국내의 "소리바다"와 같은 디지털 컨텐츠에 대한 저작권 논쟁은 이런 문제점을 극명하게 드러내는 실례로 볼 수 있으며 근본적인 대처 방안이 등장하지 않는 한 앞으로도 이와 같은 문제가 얼마든지 발생할 수 있는 가능성이 존재한다.

현재 멀티미디어 컨텐츠 복제 방지 기술로 제안되는 대표적인 기술로는 DRM(Digital Rights Management)과 워터마킹(Watermarking)을 들 수 있다. DRM은 컨텐츠의 복제는 허용하도록 하고 사용 권한에 제한을 두어 원작자의 권리를 사전에 보호하는 방식임에 비해, 워터마킹은 컨텐츠에 삽입되어 있는 특정 정보를 추적하여 원작자 또는 불법 배포자를 가려내는 사후 방식이다. 즉, 텍스트, 이미지, 오디오, 비디오 등에 멀티미디어 컨텐츠에 특정 저작권 정보를 사람의 시각 및 청각으로 구별할 수 없도록 삽입하는 기술이 바로 워터마킹이다. 이를 이용하여 소유권 분쟁 발생시 이미 삽입된 워터마킹을 검색, 추출하여 원작자를 찾을 수 있도록 한다. 이러한 워터마킹에 대한 연구는 이미 국내외적으로 광범위하게 진행되어져 오고 있으며 이를 응용한 다양한 제품들도 출시되고 있다.

본 고에서는 앞에서 언급한 첫 번째 기술인 DRM에 대하여 살펴보고, 이동 에이전트의 도입을 통한 DRM 시스템에 대하여 논의하도록 한다. 먼저 2장에서는 DRM 시스템의 기본 개념 및 동작을 살펴보고, 3장에서는 새로운 네트워크 기술로 각광받고 있는 이동 에이전트 및 보호 기술에 대하여 소개한다. 4장에서는 현재 DRM 시스템에서

*부경대학교 전자컴퓨터정보통신공학부
**부경대학교 전자계산학과

이동 에이전트가 도입가능한 부분을 살펴본 후 이를 적용한 동작 방식 및 요구사항을 논의하고, 마지막으로 5장에서 결론을 유도한다.

2. DRM 시스템 개요

DRM 시스템을 적용하는 업체에 따라 의미상의 차이점은 존재하지만, 일반적으로 DRM(Digital Rights Management)이란 "온라인 및 오프라인을 포함하는 다양한 채널을 통해 유통되는 디지털 컨텐츠를 불법 사용으로부터 보호하고, 이렇게 보호된 디지털 컨텐츠의 사용에 따라 발생하는 저작권 관련 당사자들의 이익을 지속적으로 관리해 주는 기술"을 이야기한다[1]. 즉, DRM이 적용된 멀티미디어 컨텐츠는 일정 금액의 사용료를 지불하여 정당한 사용 권한을 획득한 사용자에게만 컨텐츠 사용을 허가하도록 함으로써 디지털 컨텐츠의 무제한의 배포를 차단하는 것이다. 실제적으로는 디지털 컨텐츠에 대한 무제한의 복제가 가능하지만 그 사용 권한에는 특정한 제약을 두어 원작자의 권리를 보장하기 위한 방법이다. 다음 <그림 1>은 DRM 시스템의 동작 방식을 개략적으로 표현한 그림이다.

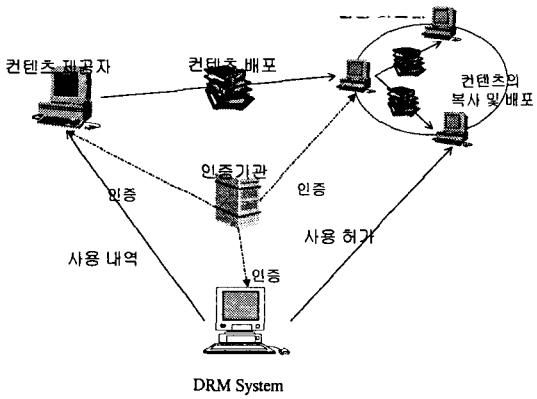


그림 1. DRM 시스템

DRM 시스템을 통한 컨텐츠 배포 및 사용은 다음과 같은 과정으로 이루어진다.

(1) 디지털 컨텐츠의 생성

컨텐츠 제공자는 제공할 디지털 컨텐츠와 이것의 사용에 대한 저작권 정보, 사용 방법, 지불 방식 등의 필수 규칙을 포함한 내용을 암호화된 파일 형태로 만든다.

(2) 디지털 컨텐츠의 배포

암호화된 컨텐츠는 인터넷 또는 CD-ROM, 디스켓 등과 같은 온라인 및 오프라인 매체를 통해 자유롭게 복제, 배포될 수 있으나, 정당하게 인증된 사용자만이 사용할 수 있도록 구성되어 있다.

(3) 디지털 컨텐츠의 사용과 재배포

컨텐츠에 대한 사용 권한은 사용자가 정당한 사용료를 지불한 후에 DRM 시스템으로부터 사용자 인증 과정을 거쳐 부여받을 수 있으며 인증된 후에는 원할 때 얼마든지 사용할 수 있는 권한을 가진다. 또한, 암호화된 컨텐츠는 누구나 복제 및 재배포가 얼마든지 가능하지만 인증 받지 못한 불법 사용자의 사용은 원천적으로 차단한다.

(4) 사용 내역 확인

DRM 시스템은 컨텐츠 제공자에게 사용자가 사용한 디지털 컨텐츠에 대한 내역을 제공함으로써 사용료를 결제할 수 있도록 한다. 전자화폐, 신용카드, 자동이체 등 다양한 방법이 사용 가능하다.

이러한 DRM은 원래의 목적에 맞게 동작하기 위해서는 다음과 같은 시큐리티 요구 사항을 만족해야만 한다[2]. 첫째, DRM 시스템은 우연한 사고뿐만 아니라 악의적인 변조에 대해서도 멀티미디어 컨텐츠를 보호할 수 있어야 한다. 만약 변조가 가능하다면 공격자는 사용 회수, 지불 방식 등을 수정하여 컨텐츠를 자유롭게 배포할 수 있는 취약성이 존재한다. 둘째, 불법적인 읽기에 대하

여 보호되어야 한다. 공격자는 컨텐츠 복호화 키나 DRM 액세스 코드와 같은 비밀 정보를 보고 DRM 시스템에 적용하여 공격할 수 있으므로 불법적인 읽기 공격에 대해서도 보호되어야 한다. 무엇보다도 공격자 입장에서는 오프라인에서 하드웨어 장치를 이용한 변조 및 읽기 공격도 수행할 수 있으므로 이러한 공격에도 견딜 수 있도록 강건하게 설계되어야 한다.

3. 이동 에이전트 기술 개요

3.1 이동 에이전트 개념

이동 에이전트는 독립적이고 자율적으로 원하는 정보를 찾아 네트워크 상을 이동하면서 여러 서비스를 수행하도록 구현된다. 다음 <그림 2>는 이동 에이전트의 동작 모습을 개략적으로 나타낸 그림으로 로컬에서 리모트 호스트로 이동한 후 작업을 수행하는 모습을 보여주고 있다[3]. 에이전트는 호스트 A에서 호스트 B로 이동하여 이미 정의된 인터페이스(Interface)를 통하여 B의 서비스 및 자원에 접근하여 원하는 정보를 얻어 원래의 서버 A로 전송한다. 원하는 정보를 얻은 후 에이전트는 또 다른 서버로 이전하여 이전과 같은 동작을 수행한다.

이동 에이전트는 사용자를 위해 자동적으로 행동하는 프로세스이며, 수행을 시작하면 자신이 생성된 시스템을 벗어나 네트워크를 통하여 한 장소에서 또 다른 장소로 옮겨다니며 원하는 정보를 수집한다.

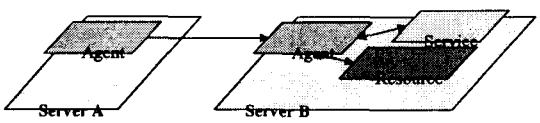


그림 2. 이동 에이전트의 동작

3.2 이동 에이전트 보호 기술

이동 에이전트의 수행은 다른 제 3자의 간섭을 받아서는 안되며, 이동 에이전트 내에 저장된 중요 상태 정보와 수행 코드 등이 이동 에이전트 외부로 누출되어서도 안된다. 그러나 이동 에이전트를 실행하는 서버는 이동 에이전트가 실행할 수 있는 환경을 제공하므로 만약 악의적인 목적을 갖는다면 에이전트 내부의 데이터 및 수행 코드까지도 접근할 수 있게 된다. 따라서 이에 대한 에이전트를 보호하는 방안이 마련되어야 하는데 현재까지 제한된 연구만이 진행 중이다. 지금까지 수행되었던 연구는 보안 방지를 목적으로 하는 Blackbox Security[4]와 Computing with Encrypted Functions[5], 보안 검출을 목적으로 하는 Cryptographic Traces[6]가 있다.

(1) Blackbox Security

F.Hohl은 악의적인 호스트에 대해 이동 코드를 보호하기 위해 Blackbox Security 개념을 제안하였다[4]. 여기서 에이전트는 하나의 블랙박스로 취급되기 때문에 만약 어떤 시점에서 에이전트 코드가 공격을 받지 않는다면 그것의 입출력 동작만을 실제 공격자가 관찰할 수 있다는 것이다. <그림 3>에서 보여주는 것과 같이, F.Hohl은 여러 변환 알고리즘을 통하여 실행 코드와 데이터 표현에서는 다르지만 같은 결과를 가지도록 원래 에이전트에서 Obfuscating 또는 Mess-up 알고

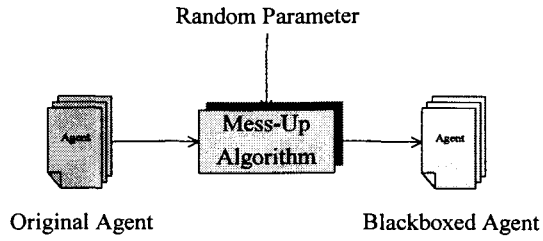


그림 3. 이동 에이전트의 블랙박스화

리즘을 통하여 새로운 에이전트를 생성하는 방안을 제안하였다. 새로 생성된 에이전트는 에이전트의 기능을 이해하기 위해 요구되는 분석이 임의의 공격자에 대해 가능한 많은 시간이 걸린다는 가정을 가진다. 이 에이전트를 목적지 호스트로 전송하여 원하는 작업을 수행하도록 한다.

(2) Computing with Encrypted Functions

T.Sander와 C.Tschudin은 이동 코드의 시큐리티 요구사항에 대한 일반적인 해결 방안을 제시하고, 이를 "Mobile Cryptography"[5]라 명명하고 "네트워크에서 이동하는 실행 코드의 정보 보호 측면에 관련된 수학적인 기술의 연구"라고 정의하였다. 이 방법은 이동 에이전트의 함수를 암호화하여 실행하는 방법이다. 여기서, 암호화란 원래의 함수와 수학적으로 같은 의미를 가지지만 형태는 다른 함수를 찾아 원래 함수를 치환함으로써 원래 함수의 연산 과정을 보여 주지 않으면서 같은 결과를 얻는 것을 의미한다[5]. 다음 <그림 4>는 Mobile Cryptography의 동작 방식을 설명하고 있다. 그러나 이동 에이전트를 동작시키기 위해 함수의 형태는 다르지만 동일한 결과를 생성하는 함수를 찾는 것은 사실상 힘들기 때문에 실제 구현에는 한계가 있다.

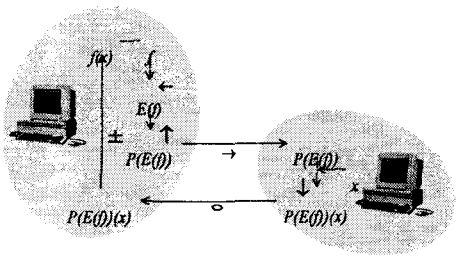


그림 4. CEF(Computing with Encrypted Functions)의 동작

(3) Cryptographic Traces

앞서 설명한 악의적인 호스트에 대한 에이전트의 정보 유출 방지에 목적을 두는 것과 반대로 G.Vigna는 이동 에이전트의 코드, 상태, 제어흐름에 대한 공격을 검출하는 것을 허용하는 암호 기술 기반의 실행 추적 메커니즘을 개발하였다[6]. 이 메커니즘은 어떤 가능한 에이전트 코드, 상태, 실행 흐름의 비합법적인 수정에 대한 검출을 목적으로 하고 있으며, "Trace"라 부르는 이동 코드의 실행동안 수집되는 데이터 분석에 기반한다. 여기서, Trace는 코드 실행 확인을 위해 사용된다. 에이전트 실행을 조작한 경우, 에이전트의 소유자는 호스트가 주장하는 연산이 에이전트에 의해 수행될 수 없음을 증명할 수 있다.

4. 이동 에이전트 기술을 이용한 DRM 시스템의 설계

DRM 시스템의 핵심은 멀티미디어 컨텐츠의 복제 및 배포는 얼마든지 허용하지만, 그 사용 및 열람에 있어서는 인증받은 사용자에게만 허가하도록 하여 불법적인 사용을 제한하는 것이다. 이를 위해서는 디지털 컨텐츠 보호 기술, 안전한 디지털 배포 기술, DRM 모듈 보호 기술 등이 필수적으로 구현되어야 한다. 즉, DRM 시스템의 목적을 이루기 위해서는 다양한 정보보호 기술 적용이 필수적인데, 대표적인 것이 데이터 암호화, 인증 및 서명 기술이다. 다음 <그림 5>는 DRM 시스템

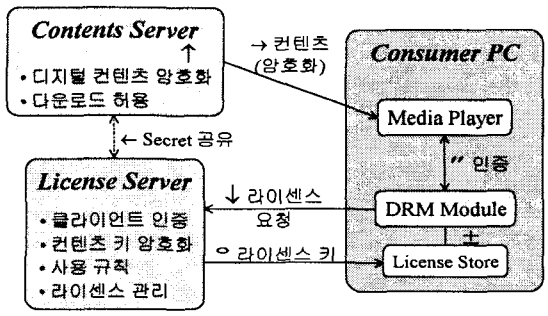


그림 5. DRM 시스템의 동작

의 일반적인 동작을 설명하고 있다.

DRM 시스템의 세부 동작을 살펴보면 먼저 ①에서 컨텐츠 생성자와 라이센스 서버 사이에 상호 협약을 통하여 각 디지털 컨텐츠에 대한 비밀 정보를 공유한다. 컨텐츠 서버는 ②에서 각 컨텐츠에 대한 비밀 정보를 이용하여 적절한 암호 기술을 사용하여 암호화하고 일반 사용자들이 다운로드받을 수 있도록 웹사이트 등을 통하여 공개한다. 일반 사용자는 자신의 원하는 컨텐츠를 검색하고 ③의 과정에서 암호화된 상태의 컨텐츠를 다운로드 받는데, 이를 다시 복제하거나 배포하는 것은 가능하지만 사용하거나 열람할 수는 없다. 사용자가 암호화된 컨텐츠를 사용하려면 DRM 모듈이 동작하면서 ④에서 정당한 허가를 위해 라이센스를 요청한다. 라이센스 서버는 클라이언트를 인증하고 사용 규칙에 따른 컨텐츠 사용을 위한 복호화 키를 ⑤에서 전송한다. ⑥에서는 도착한 라이센스에 대한 정보를 일정한 저장소에 안전하게 보관한다. 미디어 플레이어는 컨텐츠 사용을 위해 ⑦에서 저장소에 저장된 라이센스 정보를 얻기 위해 DRM 모듈에 요청하는데, 컨텐츠에 대해 정당한 라이센스 정보라면 사용 및 열람을 허가하고 라이센스 정보가 정당하지 않거나 없다면 허가하지 않는다.

DRM 시스템에서 "이동 에이전트 기술"은 디지털 컨텐츠 생성, 디지털 컨텐츠의 복제 및 배포, 라이센스 요청 및 클라이언트 인증, DRM 모듈 보호의 모든 부분에 직접 적용가능하다. 첫째, 다양한 디지털 컨텐츠를 생성하고 이에 대하여 각 라이센스 서버와 공유한 비밀키를 이용하여 암호화하고 사용자의 요청에 의하여 컨텐츠를 다운로드받을 수 있는 환경을 구축하기 위해서 이동 에이전트가 이러한 작업을 네트워크를 통하여 대신 수행할 수 있다. 둘째, 다운로드된 디지털 컨텐츠의 복제 및 배포에 있어 컨텐츠와 함께 이동 에이전트가 함께 이동한다면 각 컨텐츠에 대한 복제 및 배포 상황, 각 사용자의 동작 환경 등을 이동 에이전트가 조사하고 그 결과를 전송함으로써 컨텐츠 서버는 이를 통계화하고 다음 수요를 예측가능하다. 셋째, 사용자 입장에서 각 컨텐츠에 대한 라이센스 요청과 관련하여 클라이언트를 인증하는 과정에서 이동 에이전트가 포함된다면 시스템 자원, 네트워크 대역폭을 효율적으로 사용하면서도 사용자와의 상호작용을 처리할 수 있다. 다음 <표 1>은 DRM 시스템에서 이동 에이전트 기술 적용을 분류한 것이다.

특히, DRM 모듈 보호는 사용자 시스템에서 동작하면서 안전성을 계속해서 유지해야 하므로 단

표 1. 이동 에이전트의 DRM 시스템 적용

분 류	적용 내용	동작 시스템	요구사항
디지털 컨텐츠 생성	디지털 컨텐츠 암호화 컨텐츠 다운로드	컨텐츠 서버	효율성
디지털 컨텐츠의 복제 및 배포	컨텐츠 복제 추적 배포 상황 전송 사용자 분석	사용자 클라이언트	효율성, 사용자 개별화
라이센스 요청 및 클라이언트 인증	컨텐츠 사용 규칙 명세 클라이언트 인증 수행 라이센스 관리	라이센스 서버	효율성, 안전성
DRM 모듈 보호	DRM 모듈 보호 라이센스 관리	사용자 클라이언트	안전성, 견고성

순한 이동 에이전트 기술을 적용할 수 있는 것은 물론 3.2에서 설명했던 "이동 에이전트 보호 기술"이 직접적으로 도입될 수 있다. 컨텐츠를 사용하는 소비자 입장에서는 정당한 라이센스 없이 불법적으로 컨텐츠를 이용하려는 충분한 동기를 가지고 있고, 최근 하드웨어 및 소프트웨어의 성능이 향상되어 DRM 모듈을 오프라인 상에서 공격할 수 있는 환경도 갖추고 있다. 따라서, DRM 시스템에 대한 소기의 목적을 달성하기 위해서는 라이센스 정보보호를 위한 DRM 모듈 수행은 다른 제 3자의 간섭을 받아서는 안되며, 모듈 내에 저장된 중요 상태 정보와 수행 코드 등이 외부로 누출되어서도 안된다. 즉, 어떠한 실행 환경에서도 라이센스 정보 및 자체 모듈을 보호하기 위하여, 안전한 동작 수행이 보장되어야 하므로 악의적인 실행환경에서 이동 에이전트 보호와 같은 목적을 가진다. 실제 시스템 구현 측면에서는 이를 위하여 위조 방지를 위한 하드웨어 또는 소프트웨어 기술 등이 사용가능하다. 위조 방지 하드웨어(Tamper-Resistant H/W)의 경우는 스마트 카드 등 별도의 하드웨어 장비를 이용하여 사용가능하고 자체가 위조 방지 메커니즘을 포함함으로써 안전성을 보장받을 수 있다. 그러나 부가적인 하드웨어 장비의 도입이 필수적이고 유연성이 없어 시스템 환경에 따라 적절하게 대응하기 어렵다. 이와 반대로 위조 방지 소프트웨어(Tamper-Resistant S/W)는 부가적인 장비의 도움없이 소프트웨어만으로도 동작이 가능하지만 위조 방지 하드웨어와 비교하여 얼마나 안전한 동작을 보장하느냐 하는 문제와 구체적인 구현 상의 문제가 남아 있다. 최근에는 하드웨어의 도움없이 안전한 동작 수행을 보장할 수 있는 방법으로 연구가 진행되고 있고, 이를 이용하여 이동 에이전트 보호 기술에 직접 도입함으로써 DRM 시스템에 적용할 수 있을 것으로 사료된다.

DRM의 실제 동작 과정은 <그림 5>와 같이 이루어지는데, 사용자 측에서의 동작을 살펴보면 <그림 6>과 같다. 대부분의 디지털 컨텐츠는 네트워크를 통해 다운로드되거나 CD-ROM을 통하여 복제 및 배포된다. 이 컨텐츠를 사용하기 위하여 사용자는 라이센스를 부여받아야 하지만, 불법 사용자 또는 공격자의 입장에서는 DRM 모듈을 공격하여 암호화되어 저장된 라이센스 정보를 취득하거나 또는 DRM 모듈을 무용지물로 만들어 라이센스 정보 없이 컨텐츠를 사용하도록 시도할 것이다. 특히, 라이센스 정보 획득 후 디지털 컨텐츠는 사용자의 시스템에서 오프라인 상태가 되는데, 공격자 입장에서는 소프트웨어뿐만 아니라 하드웨어를 이용한 공격 방법도 동원할 수 있다.

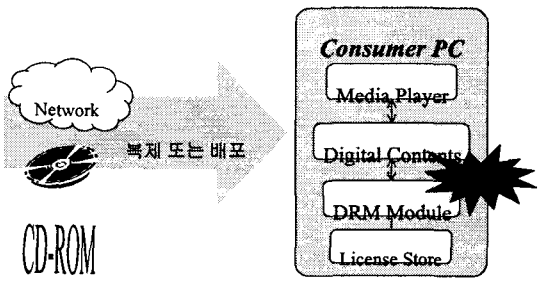


그림 6. 컨텐츠 배포 후 사용자 측에서의 동작

이를 방지하기 위해 위조 방지 소프트웨어를 적용할 수 있는데, 3.2에서 설명한 CEF가 효과적으로 쓰일 수 있다. 현재 암호화를 통하여 코드 수행을 보호하는 "EEF(Executing Encrypted Function)", "Self-Decrypting Program"과 코드 실행 분석을 어렵게 하는 "Code Obfuscation" 등의 방안이 제안되어 있다. 각 방안을 간단히 설명하면 EEF는 프로그램 동작을 암호화한 후 목적지에 전송하고 복호화 과정없이 암호화된 형태로 동작을 수행함으로써 해당되는 코드와 데이터 분석을 어렵게 하는 것이다. Self-Decrypting Program은

역시 암호화한 후 목적지에 전송하지만 코드 실행 시 필수적인 일부분만을 자체적으로 복호화하여 수행함으로써 부분적인 분석은 가능하지만 전체적인 프로그램 동작 분석을 어렵게 하는 방안이다. Code Obfuscation은 프로그램 코드를 뒤섞거나 재배치하여 통계적인 프로그램 패턴을 없앰으로써 데이터 구조 및 프로그램 분석을 어렵게 만드는 방안이다.

또한, 네트워크가 연결되어 항상 사용가능한 온라인 환경이라면 암호 기반 메커니즘인 Cryptographic Traces를 통하여 DRM 모듈의 코드, 상태, 제어흐름에 대한 공격을 검출하는 것을 허용하는 실행 추적 방법을 이동 에이전트와 함께 도입하여 컨텐츠 서버 또는 라이센스 서버 측에서 DRM 모듈에 대한 공격자의 공격 여부를 판단할 수도 있다.

<표 2>는 앞에서 설명하였던 DRM 모듈 보호 방안에 대하여 표로써 정리하였다.

5. 결 론

본 고에서는 디지털 컨텐츠 보호를 위한 기술 중 DRM의 개략적인 동작을 살펴보고, 네트워크의 새로운 패러다임으로 인식되는 이동 에이전트에 대한 개념을 설명하였다. 또한 DRM 시스템에 있어 이동 에이전트를 적용할 수 있는 부분을 살펴보고, 컨텐츠 소비자 측에서 동작하는 DRM 모듈을 보호하는 방법에 대하여 논의하였다.

멀티미디어 기술의 발달로 수많은 컨텐츠가 제작되고 유료화되어 다양한 부가가치를 창출하고 있으며, 네트워크 기술의 발달에 힘입어 멀티미디어 컨텐츠는 다양한 방법으로 가공·처리되어 전 세계에 배포되고 있다. 이와 관련하여 "디지털 컨텐츠에 대한 저작권 보호"라는 새로운 문제가 쟁점화되고 있으며 이를 보호하기 위한 다양한 기술들이 선보이고 있다. 그 중 DRM 시스템은 정당한 라이센스를 획득한 사람만이 컨텐츠를 사용하도록 허용하는 시스템으로써 네트워크 기술, 매체 기술, 암호화 기술 등이 복합된 멀티미디어 컨텐츠 보호 기술이다. 따라서, 안전한 DRM 시스템과 워터마킹 기술이 구축되어 운영된다면 원작자 입장에서는 각 컨텐츠에 대한 저작권 보호가 가능하고, 사용자는 각 컨텐츠에 대한 정당한 사용료 지불이 가능하고, 유통업자들은 디지털 컨텐츠의 효율적인 관리 및 안전한 배포를 책임질 수 있으므로 멀티미디어는 새로운 부가가치를 창출하는 또 다른 미디어로써 자리잡게 될 것이다.

참 고 문 헌

[1] http://www.intertrust.com/

[2] R.Vingralek, U.Maheshwari and W.Shapiro, "TDB: A Database System for Digital Rights Management", Technical Report, STAR-TR-01-01, InterTrust STAR Lab., 2001

[3] 신원, 박영호, 이경현, "이동 에이전트 시스템 시큐리티", 「'2000 한국통신정보보호학회 종합학

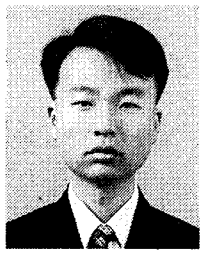
표 2. DRM 모듈 보호 기술

분 류	기 능	상 태	방 법
EEF	DRM 모듈 실행 보호 라이센스 정보 보호	오프라인	코드 암호화 상태에서 실행
Self-Decrypting Program		오프라인	코드의 암호화 후 복호화하면서 실행
Code Obfuscation		오프라인	코드 재배치 후 실행
Cryptographic Traces	DRM Trace 기록	온 라 인	Trace 유지 후 공격 여부 판정

술발표회 논문집」, pp.164-171, 2000
[4] F.Hohl, "Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts," In: G.Vigna (Ed.), Mobile Agents and Security, Springer-Verlag, Lecture Notes in Computer Science 1419, pp. 92-113, 1998
[5] T.Sander and C.Tschudin, "Towards Mobile Cryptography," International Computer Security Institute (ICSI), TR-97-049, 1997
[6] G.Vigna, "Cryptographic Traces for Mobile Agents," In: G.Vigna (Ed.), Mobile Agents and Security, Springer-Verlag, Lecture Notes in Computer Science 1419, pp.137-153, 1998
[7] 한국멀티미디어학회, 멀티미디어 컨텐츠 보호를 위한 워크샵, 2000
[8] http://www.metarights.com/
[9] http://www.uspto.gov/

이 경 현

- 1982년 경북대학교 사범대학 수학교육과 졸업(이학사)
- 1985년 한국과학기술원 응용수학과 졸업(이학석사)
- 1992년 한국과학기술원 수학과 졸업(이학박사)
- 1985년 2월~1993년 2월 한국 전자 통신 연구소 연구원, 선임 연구원
- 1993년 3월~현재 부경대학교(구 부산수산대학교) 전임강사, 조교수, 부교수
- 1995년 7월~1996년 7월 Univ. of Adelaide, 응용수학과, Australia 방문교수
- 1999년 7월~8월 Univ. of Tokyo, 객원 연구원
- 1997년 12월~현재 한국멀티미디어학회 학술이사
- 2001년 1월~현재 한국통신정보보호학회 논문지 편집위원
- 관심분야 : 정보보호론, 멀티미디어 정보보호, 네트워크성능 평가, 암호학, 재시도 대기체계론



신 원

- 1996년 부산수산대학교(현 부경대학교) 전자계산학과 졸업(이학사)
- 1998년 3월 부경대학교 전자계산학과 대학원 졸업(이학석사)
- 1998년~현재 부경대학교 전자계산학과 박사과정
- 관심분야 : 정보보호, 이동에이전트, 멀티미디어 통신, 암호이론, 네트워크 보안