공학석사 학위논문

적응적 보안 등급을 이용한 DRM 시스템 설계 및 구현

지도교수 정 목 동

이 논문을 공학석사 학위논문으로 제출함.

2004년 2월

부경대학교 대학원

컴퓨터공학과

김 환 조

김환조의 공학석사 학위논문을 인준함

2003년 12월 26일

주 심 공학박사 우 종 호 

위 원 공학박사 권 오 흠 

위 원 공학박사 정 목 동 

목 차

요약 iv

Abstract vi

제 1 장 서 론 1

제 2 장 관련연구 4

2.1 DRM 4

2.2 MAUT 8

2.3 X9.59 지불프로토콜 10

2.4 CONSEPP 12

제 3 장 적응적 보안 등급 알고리즘 13

3.1 알고리즘을 위한 계수 13

3.2 디바이스 성능 및 컨텐츠 가치의 환산 14

3.3 적응적 보안 정책 알고리즘 14

제 4 장 적응적 보안 등급을 이용한 DRM 시스템 17

4.1 시스템 구성 19

4.2 결제 과정 21

4.3 Superdistribution 23

제 5 장 구현 및 평가 29

제 6 장 결론 및 향후 연구 32

참고문헌 33

그 림 목 차

[그림 1] CA-based PKI DRM 시스템 ····· 6

[그림 2] X9.59 지불 프로토콜 ····· 11

[그림 3] Merchant 인증 과정 ····· 12

[그림 4] SecureModule 알고리즘 ····· 15

[그림 5] sysNet 알고리즘 ····· 16

[그림 6] MAUT 알고리즘 ····· 16

[그림 7] 제안 시스템 ····· 17

[그림 8] Management Agent ····· 18

[그림 9] 컨텐츠 결제 ····· 22

[그림 10] 컨텐츠 플레이 ····· 22

[그림 11] 결제과정 ····· 24

[그림 12] 라이센스의 XML Schema ····· 26

[그림 13] Superdistribution ····· 28

표 목 차

[표 1] DRM 시장 규모 및 전망 ····· 5

[표 2] 해외 DRM 관련 제품 현황 ····· 7

[표 3] 국내 DRM 관련 제품 현황 ····· 8

[표 4] 디바이스 성능에 대한 계수 ····· 13

[표 5] 디지털 컨텐츠 가치에 대한 계수 ····· 13

[표 6] 디바이스 성능 계수의 환산 값 ····· 14

[표 7] 디지털 컨텐츠 가치 계수의 환산 값 ····· 14

[표 8] 100byte 데이터에 대한 RSA와 ECDSA의 서명 및 검증시간 비교 ···· 30

적응적 보안등급을 이용한 DRM 시스템 설계 및 구현

김 환 조

부 경 대 학 교 대 학 원 컴 퓨 터 공학과

요약

인터넷이 발전함에 따라 디지털 컨텐츠의 사용과 유통이 늘어나고 있다. 그러나 디지털 컨텐츠의 손쉬운 복제와 유통 등의 특징으로 인해 저작권 문제가 발생하고 있다. 디지털 컨텐츠를 보호하기 위해 DRM(Digital Rights Management) 기술이 사용되고 있다. 하지만 현재의 컴퓨팅 환경이 유비쿼터스 환경으로 변해 가면서 다양한 종류의 디지털 컨텐츠와 디바이스들이 등장하면서 기존의 DRM 기술은 이에 능동적으로 대처하지 못하고 있다.

본 논문에서는 동적으로 암호화 알고리즘을 결정하는 적응적 보안 등급 알고리즘을 이용하여 유비쿼터스 환경에 능동적으로 대처가 가능한 즉, 다양한 특성을 가진 디바이스에서도 사용가능하며 다양한 종류의 디지털 컨텐츠에 대해서도 적용 가능한 MAUT 기반 DRM 시스템을 제안한다. 제안된 시스템은 사내의 기밀문서 관리 시스템이나 온라인 소프트웨어 판매, 전자 도

서관 등 다양한 분야에 적용이 가능하며, 사용자가 쉽고 편리하게 사용할 수 있고, 소비자의 기호를 만족시킬 수 있는 방법을 제시함으로써 디지털 컨텐츠 시장의 확대에 기여할 수 있을 것으로 예상된다.

Design and Implementation of a DRM System Using Adaptive Security Level

Hwan Jo Kim

Dept. of Computer Eng., Graduate School,

Pukyong National University

Abstract

Recently, the widespread use of Internet makes the usages and distribution of the digital contents so popular. On the contrary, a copyright problem is occurring due to the feature of easy reproduction and distribution of the digital contents. To address this problem, DRM technique has been used to protect digital contents. As the current computing environment changes into ubiquitous one, various kinds of devices and digital contents are shown. However, the existing DRM techniques can not deal with these devices and digital contents dynamically. Therefore, we need to develop a new DRM system

considering ubiquitous computing environment as well.

In this thesis, we propose a new DRM system which could be applicable in the ubiquitous environment. And the proposed system selects an encryption algorithm dynamically using adaptive security level algorithm based on MAUT technique. The system could be used in the various environments such as security document management system, online software marketing, e-library, and etc. The proposed method is expected to satisfy users' preferences and thus the system might be convenient and easy to use. Therefore, the proposed system could be used to enlarge the digital contents market securely.

1. 서 론

최근 인터넷의 고속화, 대용량화로 다양한 종류의 디지털 컨텐츠의 이용이 증가하고 있다. 디지털 컨텐츠는 아날로그 데이터의 복사와 달리 여러 번의 복사를 수행하여도 동일한 품질을 유지하며, 인터넷을 통해 접근이 매우 용이하다. 또한 디지털 컨텐츠는 인터넷을 통해 쉽고 빠르게 배포가 가능하며 복사에 소요되는 비용이 매우 적다. 이러한 특징들을 이용한 불법 복제로 디지털 컨텐츠의 저작권 문제가 발생한다. 따라서 인터넷상에서 발생하는 디지털 컨텐츠의 저작권 문제를 해결하기 위해 다양한 방법들이 널리 사용되고 있다.

DRM(Digital Rights Management)[1,2,3]은 암호화 기술을 이용하여 디지털 컨텐츠의 저작권과 이익을 보호하고 관리하는 기술이다. 디지털 컨텐츠는 디지털 컨텐츠 저작권자가 명시한 비즈니스 룰을 포함하여, 디지털 컨텐츠를 이용하고자 하는 사용자가 비즈니스 룰을 만족해야만 컨텐츠를 이용할 수 있다.

Secure Distribution[4]은 사용자에게 전달되는 컨텐츠를 사용자만이 복호화할 수 있도록 암호화해서 전달하는 기술이다. 정당한 사용자에게 전달된 컨텐츠를 악의의 사용자가 획득하더라도 복호화할 수 없기 때문에 불법 복제를 방지할 수 있다. 하지만 컨텐츠가 전달되는 순간에 암호화되기 때문에 서버의 부담이 크고 컨텐츠의 배포가 제한적인 한계점을 지닌다.

복사방지신호(Scramble)[4] 기술은 컨텐츠가 저장된 매체(비디오테이프, DVD, CD-ROM)에 특별한 복사방지신호(Scramble)를 삽입함으로써 컨텐츠를 보호하는 기술이다. 이 기술은 컨텐츠를 배포할 수 있는 매체가 제한된다는 점과 보호체계가 쉽게 풀릴 수 있다는 한계를 지닌다.

Watermarking[5,6]은 동영상, 이미지 등과 같은 디지털 컨텐츠에 상표, 로고 등과 같은 저작권 인증 데이터를 사용자가 인식할 수 없는 방식으로 삽입하는 기술이다. 추후에 저작권 문제가 발생했을 때 삽입된 인증 데이터를 추출하여 원래의 저작권자를 쉽게 판별할 수 있다. 하지만 이 기술은 디지털 컨텐츠의 불법 사용을 원칙적으로 방지할 수 없다는 한계를 지닌다.

DOI(Digital Object Identifier)[7]는 ISBN처럼 모든 디지털 컨텐츠를 식별할 수 있는 체계를 부여함으로써 저작권 정보를 등록하고 관리할 수 있는 식별자를 제공한다.

이처럼 다양한 저작권 보호 기술이 있지만 컨텐츠의 불법 사용을 방지하고 다양한 컨텐츠 비즈니스 모델을 가능하게 하는 DRM 기술이 가장 현실적인 솔루션으로 주목받고 있다.

그리고 현재의 컴퓨팅 환경이 유비쿼터스 컴퓨팅 환경으로 변해가면서 다양한 특성을 가진 디바이스들과 다양한 종류의 디지털 컨텐츠들이 등장하고 있다. 유비쿼터스 컴퓨팅 환경[8,9]이란 퍼베이시브 컴퓨팅(pervasive computing)이라고도 하며, 모든 네트워크 상에서 언제 어디서나 임의의 디바이스를 사용하여 어떤 정보라도 전달할 수 있고, 개인화 기능을 이용하여 사용자가 선택하는 언어 또는 적절한 형태로 정보를 전달할 수 있으며 사람과 컴퓨터 그리고 환경이 서로 상호 작용하는 기술이다. 디바이스들은 서로 다른 컴퓨팅 파워, 메모리, 기억장치, 전송속도 등의 특성을 가지며 디지털 컨텐츠들은 이러한 디바이스들에서 사용 가능한 다양한 형태를 지니고 있다.

하지만 현재 제공되는 DRM 시스템은 새로 등장하고 있는 디바이스들과 디

지털 컨텐츠들을 효율적으로 사용할 수 있는 방법을 제공하지 못하고 있다. 이는 현재의 DRM 시스템이 디바이스들과 디지털 컨텐츠 특성을 고려하지 않고 일률적인 보안 정책을 적용하기 때문이다. 따라서 서로 다른 특성을 가진 디바이스들과 서로 다른 형태를 가진 디지털 컨텐츠에 능동적으로 대응할 수 있는 보안 정책이 요구된다.

본 논문에서는 다양한 특성을 가진 디바이스들과 다양한 종류의 컨텐츠의 가치를 고려한 효율적인 적응적 보안 정책 알고리즘을 설계하고 논문에서 제시한 적응적 보안 정책 알고리즘을 이용한 컨텐츠 암호화 모듈을 설계하고 구현한다. 또한 제한된 자원과 컴퓨팅 파워를 가진 디바이스들도 사용가능한 결제 프로토콜을 제시하고 구현하여 전체 DRM 시스템을 설계하고 구현한다.

논문의 구성은 서론에 이어 2장에서는 DRM과 관련된 연구를 살펴보고, 3장에서는 다양한 특성을 지닌 디바이스들과 다양한 종류의 디지털 컨텐츠를 고려한 적응적 보안 정책 알고리즘에 대해서 기술하고, 4장에서는 논문에서 제안한 DRM 시스템에 대해서 설명한다. 5장에서는 구현 및 평가, 6장에서는 결론 및 향후 연구 과제에 대해서 기술한다.

2. 관련 연구

2.1 DRM(Digital Rights Management)

DRM[1,2,3]은 디지털 저작권 관리 시스템을 뜻하며 컨텐츠의 지적 재산권이 디지털 방식에 의해 안전하게 유지/보유 되도록 하는 시스템을 정의할 수 있다. 즉, 디지털 컨텐츠가 저작권자 및 유통업자의 의도에 따라 전자상거래를 통해서 안전하고 편리하게 유통될 수 있도록 제공되는 모든 기술과 서비스 절차 등을 포함하는 개념이다. 일반적으로 DRM 시스템이 갖춰야 할 기본 요건은 다음과 같다.

① 컨텐츠와 비즈니스 규칙의 패키징

컨텐츠 제공자는 판매할 컨텐츠와 적용할 비즈니스 규칙을 함께 암호화하여 안전하게 전달할 수 있는 방법을 제공해야 한다.

② 컨텐츠 배포

패키징된 디지털 컨텐츠를 인터넷, CD-ROM, e-mail 등을 통해 안전하게 최종 사용자에게 전달할 수 있는 방법을 제공해야 한다.

③ 컨텐츠의 구입 사용

디지털 컨텐츠에 대해서 정당한 지불을 한 사용자에 한해서 컨텐츠를 사용할 수 있는 라이센스를 제공할 수 있는 방법을 제공해야 한다.

④ Superdistribution

디지털 컨텐츠에 대한 정당한 라이센스를 가진 사용자가 다른 사용자에게 디지털 컨텐츠를 직접 또는 매체를 통해 간접적으로 전달할 수 있는 방법을

제공해야 한다. 디지털 컨텐츠를 전달받은 사용자는 디지털 컨텐츠에 대한 지불을 통해서만 디지털 컨텐츠를 사용할 수 있다.

⑤ 라이센스 백업 기능

OS의 재설치 등 어떤 이유로 라이센스를 분실했을 경우를 대비하여 라이센스를 백업하고 다시 사용자에게 제공할 수 있는 방법을 제공해야 한다.

⑥ 휴대용 단말기 지원

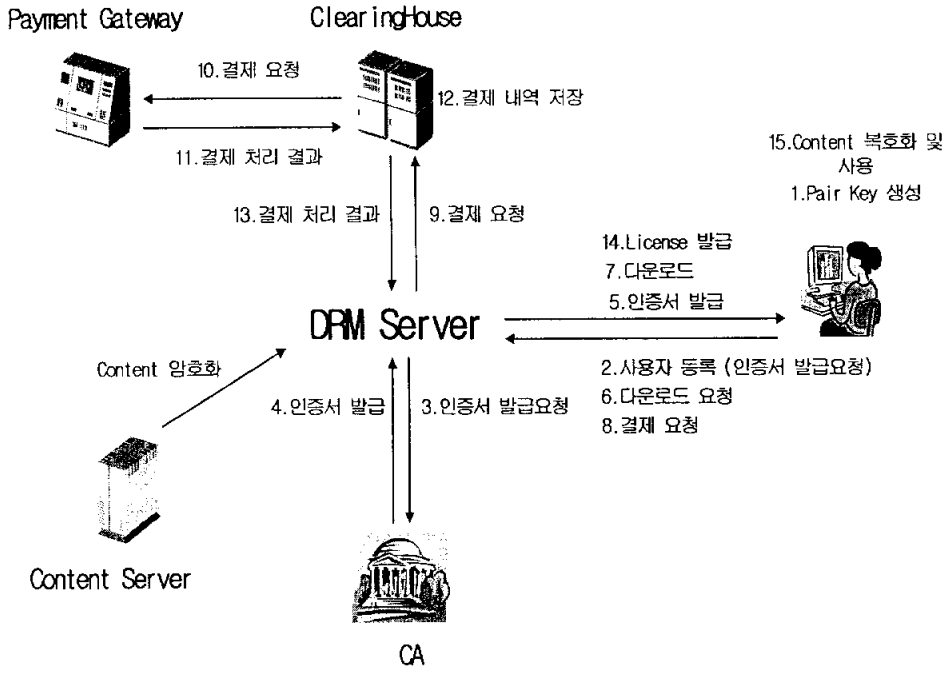
휴대폰과 같이 제한된 자원과 저성능의 컴퓨팅 파워를 지닌 디바이스들도 사용 가능한 방법을 제공해야 한다.

[그림 1]은 CA-based PKI DRM 시스템을 나타내고 있다. 이 시스템은 PKI를 이용하여 암/복호화를 수행하는데 이 방법은 휴대폰과 같은 저성능의 디바이스에서 이용하기에는 문제점이 있다. 이를 해결하기 위한 방법으로 PKI 대신 타원곡선 알고리즘(ECC)[10]을 사용하기도 한다.

[표 1]에서 볼 수 있듯이 DRM 시장은 폭발적인 증가를 보이고 있다. IDC는 DRM 시장이 2000년에는 $96 million이였으며 2005년까지 $3.57 billion으로 성장할 것이라고 전망하고 있다.

[표 1] DRM 시장 규모 및 전망 자료 : The DRM Landscape, IDC, 2001

년도	2000	2001	2002	2003	2004	2005	2000-20005년 CACR(%)
시장규모	96.0	218.8	543.8	1,188.6	2,132.6	3,568.6	106.1



[그림 1] CA-based PKI DRM 시스템

DRM 시장을 주도하기 위해 많은 업체들이 관련기술을 개발하고 연구에 투자하고 있다. 그 중 해외에서 InterTrust[11], Microsoft[12] 등의 회사들이 DRM 기술을 주도하고 있다. 이 중에서 InterTrust는 가장 먼저 DRM 기술을 개발한 회사로 현재 가장 높은 기술력을 보유하고 있는 것으로 평가된다. 그 뒤를 이를 Microsoft가 Windows Media Rights Manager를 이용한 오디오 및 비디오 부분에서 DRM 기술을 개발하고 있다. 국내에서 파수닷컴[13]을 비롯한 다양한 업체들이 DRM 기술을 개발하고 있다. 세계수준의 초고속통신망을 이용한 다양한 DRM 기술이 시험되고 있으며 이를 이용한 다양한 수익 모델을 개발하고 있다.

[표 2]와 [표 3]은 국내외의 주요 DRM업체와 관련 제품 현황을 나타낸 것이다. 각 업체들의 제품들을 살펴보면 대부분 고성능을 지닌 데스크탑 PC를 대

상으로 하고 있다. 몇몇 업체에서만 모바일 분야에서 이용할 수 있는 제품을 출시하고 있을 뿐 유비쿼터스 환경에서 등장할 다양한 특성을 지닌 디바이스들에 대한 고려는 없는 실정이다.

[표 2] 해외 DRM 관련 제품 현황

회사	제품명	특징
Microsoft	Windows Media Rights Manager	- 정당한 소유자만이 소유권자의 디지털 컨텐츠에 접근하고 플레이 할 수 있도록 관리 및 보호
IneterTrust	Rights/System	- 디지털 정보의 모든 전송 및 분배 단계에서의 보호 및 관리를 위해 총괄적인 DRM 시스템 개발 - Napster처럼 Peer to Peer distribution을 할 수 있음
Contentguard	DRM	- 저작권자가 사용 권한, 사용조건 등을 결정할 수 있게 함 - XrML을 이용한 DRM 개발
Liquid Audio	Liquid Player Liquid Audio SP3	- MP3를 포함한 다양한 디지털 음악 포맷을 지원하는 소프트웨어
Info2 Clear	GetaSong e-Book Suite, GetaSeal GetaCopy	- 문서보안과 음악파일 보안을 위한 DRM 기술 - 저작권자의 지적재산권을 보호해줄 수 있는 GetaSeal 소프트웨어와 PKI에 기반한 보안 웹 기술 사용
IBM	EMMS (Electronic Media Management System)	- 미디어의 디지털 분배를 위한 소프트웨어 솔루션 - 5개의 소프트웨어 툴 들이 컨텐츠 소유자와 디지털 전송 시스템에 대한 플랫폼 형성
Infra works	Digital Property Protection	- 전자메일, ftp, 서버기반의 다운로드, 다른 인터넷 전송 메커니즘을 통한 디지털 컨텐츠의 안전한 분배 제공

[표 3] 국내 DRM 관련 제품 현황

회사	제품명	특징
파수닷컴	FDS Fasoo DRM	기업문서보완솔루션 제공 InterTrust의 DRM 기술 도입 개인용 문서보안 솔루션 랩소디 출시
디지캡	Digicap DRM	MP3 저작권 보호기술 서비스 제공 오디오, e-Book, 이미지, 모바일에서의 DRM 제품 서비스 중
이지솔루션	e-Book	PDF용 DRM을 개발하여 e-Book 시장을 공략 중
삼성전자	Secu MAX	- MP3의 저작권 보호를 위한 복제방지 시스템 - 현재 SecuMAX 1.0이 상용화
비씨큐어	EDS CQ-Media	- 기업내 문서보안을 위한 DRM제품과 각종 디지털 저작권 보호기술인 CQ-Media제공
마크애니	SDMS등	- watermarking 전문 업체이나 최근 독자적인 DRM 솔루션 개발

2.2 MAUT(Multi-Attribute Utility Theory)

MAUT[14,15,23]은 다양한 Attribute에 따른 최적의 의사 결정 방법인 다중 속성 효용이론이다. Consequence에 대한 개인적인 호감(preference)을 utility 값으로 표현하고 Consequence에 대한 utility 값의 대입은 기대 utility를 최대화 시켜주는 쪽으로 이루어진다. 유틸리티 분석(utility analysis)은 의사 결정자(decision maker)가 원하는 제비뽑기(lottery)의 결과(consequence)를 분석해주는 분야로서 의사 결정자는 이들 결과에 대한 개인의 선호도(preference)를 유틸리티 수(utility number)로 표현하고 있다. 결국 유틸리티는 0과 1사이의 상대적인 값으로서 $u(x^o)$와 $u(x^*)$를 각각 가장 선호하지 않는 결과 유틸리티와 가장 선호하는 결과 유틸리티라고 두면 $u(x^o) = 0$, $u(x^*) = 1$로 나타낼

수 있다. 결과에 대한 유틸리티 수의 대입은 기대 유틸리티(expected utility)를 최대화시켜주는 쪽으로 이루어져야 한다. 즉, 기대 유틸리티의 최대화는 의사 결정자의 최적 행동의 기준이 된다. 유틸리티 함수를 선정하는 데 일률적인 방법이 있는 것은 아니지만 공통적으로 사용될 수 있는 과정은 대체로 다음과 같다.

선정 준비 : 결과 Q를 실수 x 에 사상시키는 평가 함수를 X 라고 하면 $x = X(Q)$이다. x 값의 크기와 바람직한 정도와의 관계를 정할 수 있다. 즉, 의사 결정자가 결과 x_1과 결과 x_2 중에서 어떤 것을 선호하는지 확인해 볼 수 있다.

독립성 확인 : Y와 Z가 덧셈 독립(additive independence), 유틸리티 독립(utility independence)인지 확인 해본다.

정성적인 성질 확인 : 유틸리티 함수가 단조(monotonic) 함수인지 확인한다. x_k가 x_j 보다 크면 x_k는 항상 x_j 보다 좋은 것인지 확인하고, 다음으로 유틸리티 함수 u가 모험 회피(risk averse), 모험 중립(risk neutral), 모험 노출(risk prone) 중에서 어떤 것인지 결정한다.

유틸리티 함수 결정 : 간단한 예로 의사 결정자의 유틸리티 함수가 x에서 단조 증가이고, 감소적인 모험 회피라고 가정하면, 이러한 특징을 만족시키는 유틸리티 함수는 다음과 같다.

$$u(x) = h + k(-e^{-ax} - be^{-cx})$$

여기서 a, b, c, k는 양의 상수이다. 일반적으로 유틸리티 함수 $u(x_1, x_2, \ldots, x_n)$가 덧셈 독립, 유틸리티 독립이면 u는 다음과 같다.

$$u(x_1, x_2,..., x_n) = k_1u_1(x_1) + k_2u_2(x_2) +... + k_nu_n(x_n)$$

여기서 모든 i 에 대해서 $u_i(x^o_i) = 0$, $u_i(x^*_i) = 1$. $u_i(x^o_i)$와 $u_i(x^*_i)$는 각각 가장 선호하지 않는 결과 유틸리티와 가장 선호하는 결과 유틸리티이다.

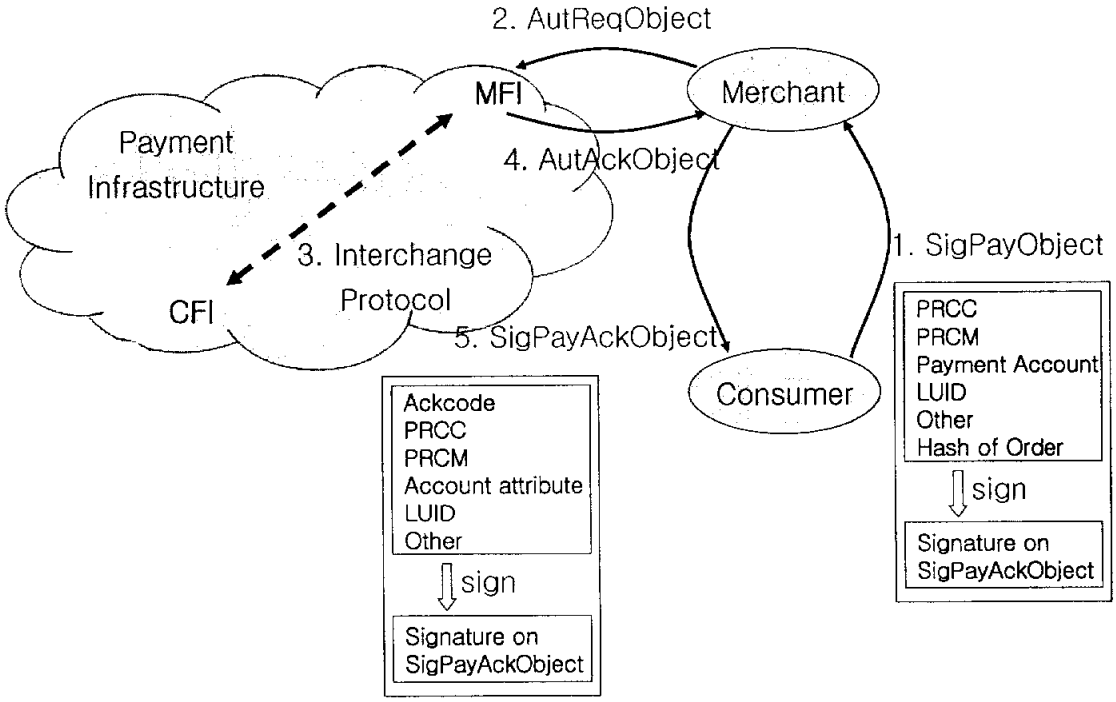
MAUT는 복잡한 의사 결정 문제를 여러 개의 작고 단순한 문제로 나누어 보다 용이하게 해결할 수 있는 논리적 기틀을 제공한다. MAUT는 다양한 곳에 사용될 수 있으며 특히 전자 상거래 분야에서 판매자와 구매자 사이의 여러 Attribute에 대해 협상하는 과정에서 많이 사용되고 있다.

기존의 전자 상거래에서는 가격이라는 하나의 변수를 가지고 협상을 수행했다. 이 방법은 구매자와 판매자의 욕구를 제대로 충족시키지 못하고 있다. 따라서 각 상품에 대한 특성들을 각각의 변수로 설정하고 각각의 변수들에 대해 구매자와 판매자의 선호도를 반영하여 협상하는 방법이 구매자와 판매자에게 보다 나은 서비스를 제공할 수가 있다. 이 때 MAUT를 이용할 수가 있다.

Pmart(Pukyong-mart)[15]는 가격 이외의 상품의 특성이나 보장기간, 서비스 정책 등 다양한 변수들에 대해 MAUT를 이용하여 협상할 수 있는 에이전트 중재에 의한 전자 상거래 프레임워크이다.

2.3 X9.59 지불프로토콜

X9.59[16,23]은 account 기반의 지불 방법에 대한 Finance Industry 표준이며 AADS(Account Authority Digital Signature)[16]에 바탕을 두고 있다. X9.59는 CA-based PKI[17,22]을 사용하지 않고 안전하고 편리한 지불 방식을 제공한다. [그림 2]는 X9.59의 지불 프로토콜을 나타낸다.



[그림 2] X9.59 지불 프로토콜

X9.59는 Consumer(사용자)와 Merchant(서비스 제공자)의 account/card number 대신 PRC(Payment Routing Code)를 사용한다. PRC는 FI가 할당한 account number이며 FI 내부에서만 실제의 account/card number를 찾을 수 있다. Consumer와 CFI, Merchant와 MFI는 서로를 신뢰하는 관계이다. 또한 CFI와 MFI는 서로 간에 신뢰하는 금융기관이다.

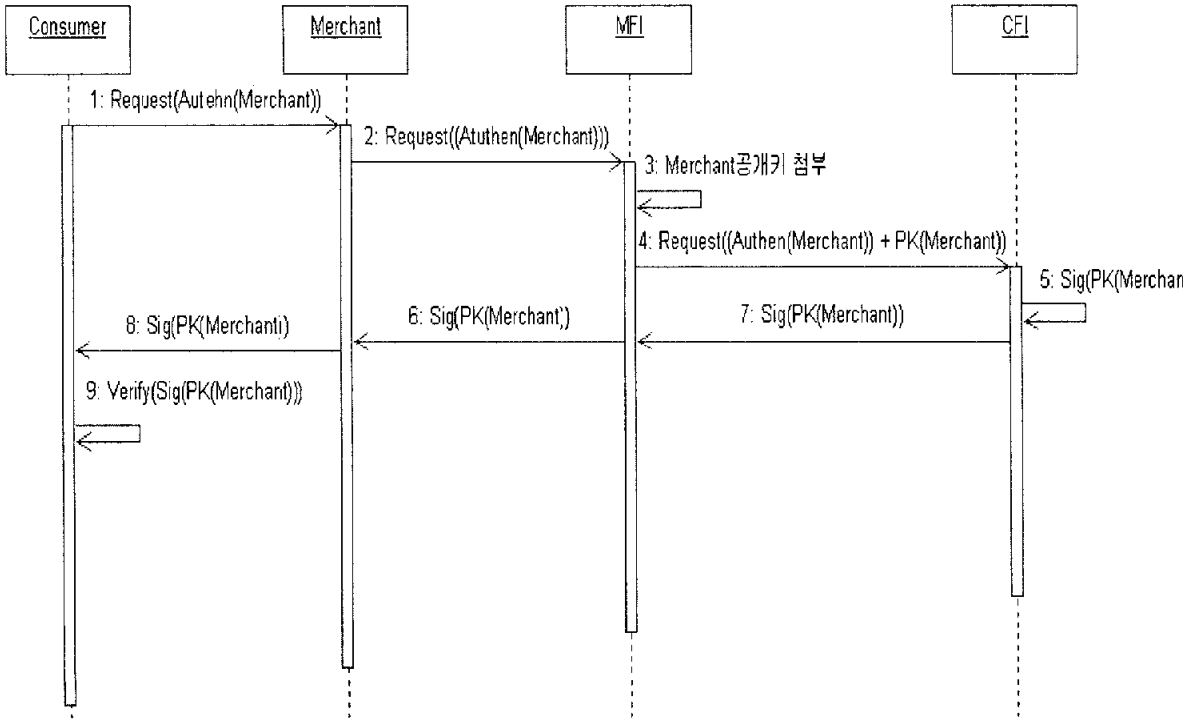
Consumer가 Merchant에 접속하여 서비스 혹은 물품에 대한 정보를 요청하고 선택한 다음 결제 요청 메시지를 생성하여 자신의 개인키로 서명한 다음 Merchant에게 전달한다. Merchant는 이 메시지를 자신이 등록한 MFI에게 전달하고 MFI는 Consumer가 등록한 CFI에게 메시지를 전달한다. CFI는 해당 Consumer의 공개키로 메시지의 서명을 검증하고 transaction을 처리한다. CFI

는 결제 요청 응답 메시지를 생성하고 자신의 개인키로 서명한 다음 MFI에게 전달한다. 이 메시지는 Merchant를 거쳐 Consumer에게 전달되며 Consumer는 CFI의 공개키로 서명을 검증하고 결제 처리 결과를 확인한다.

2.4 CONSEPP

CONSEPP(CONvenient and Secure Electronic Payment Protocol based X9.59)[17]은 X9.59를 기본 개념으로 하면서 X9.59가 가진 Merchant의 인증서 문제를 해결하기 위해 다음의 방법으로 해결하고 있다.

[그림 3]에 보듯이 Merchant의 공개키를 이용해 MFI가 보증하도록 하는 방법을 사용하고 있다.



[그림 3] Merchant 인증 과정

3. 적응적 보안 정책 알고리즘

이 절에서는 다양한 특성을 가진 디바이스와 다양한 종류의 디지털 컨텐츠의 가치를 고려하여 MAUT 알고리즘을 이용하여 최적의 보안 등급을 동적으로 결정하는 알고리즘을 소개한다.

3.1 알고리즘을 위한 계수

알고리즘을 위한 계수를 정의한다.

① 디바이스 성능에 대한 계수

[표 4] 디바이스 성능에 대한 계수

device (0.5)	k_1	*dNet*	네트워크 속도
	k_2	*dCpu*	디바이스의 CPU 성능
	k_3	*dRam*	디바이스의 RAM

② 디지털 컨텐츠 가치에 대한 계수

[표 5] 디지털 컨텐츠 가치에 대한 계수

content (0.5)	k_4	*cQuality*	디지털 컨텐츠의 품질
	k_5	*cExpire*	디지털 컨텐츠의 사용기간
	k_6	*dValue*	디지털 컨텐츠의 가격

디지털 컨텐츠의 가치와 디바이스의 성능을 동일하게 고려하기 위해 전체 가중치를 각각 .5로 결정한다.

3.2 디바이스 성능 및 컨텐츠 가치의 환산 값

다음의 [표 6]과 [표 7] 각각 [표 4]와 [표 5]에서 설정한 각 변수의 최선 값(x_i^*)과 최악 값(x_i^0)을 토대로 0 과 1 사이의 값으로 변환한 값이다. 예를 들어 CPU의 경우, *dCpu**가 3000Mhz이므로 환산 값을 구하는 공식은 식 1과 같다.

$$dCPU/dCPU^* = x_i/3000 \qquad \text{(식 1)}$$

[표 6] 디바이스 성능 계수의 환산 값

Attribute	x_i^0	x_i									x_i^*
dNet(kbps)	0	120	240	360	480	600	720	840	960	1180	1200
dCpu(Mhz)	0	300	600	900	1200	1500	1800	2100	2400	2600	3000
dRam(M)	0	160	320	480	640	800	960	1120	1280	1440	1600
환산된 값	0.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	1.0

[표 7] 디지털 컨텐츠 가치 계수의 환산 값

cQuality(등급)	0	1	2	3	4	5	6	7	8	9	10
cExpire(일)	0	1	2	4	8	16	32	64	128	256	∞
cValue(원)	0	500	1000	1500	2000	2500	3000	3500	4000	4500	5000
환산된 값	0.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	1.0

3.3 적응적 보안 정책 알고리즘

다음은 동적으로 디지털 컨텐츠에 적용할 보안 등급을 결정하는 알고리즘이다. [그림 4]는 적응적 보안 정책 알고리즘을 나타낸 것이다. 먼저 사용자 디

바이스의 정보를 획득한 다음 이를 이용하여 사용자의 디바이스가 최소한의 요구사항을 만족하는지를 검사하게 된다. [그림 5]는 사용자의 디바이스의 성능이 디지털 컨텐츠를 사용할 수 있는지를 검사하는 sysNet 함수이다. 만약 최소한의 성능에 못 미친다면 서비스는 거부된다.

```
function SecureModule return SecuLevel
static
  // 네트워크 디바이스의 성능
  네트워크 속도( dNet)                    // 서비스에 직접적인 영향
  CPU 성능( dCpu)                         // 보안 정책 처리에 직접적인 영향
  RAM 용량( dRam)                         // 보안 정책 처리에 직접적인 영향

  // 디지털 컨텐츠의 가치
  품질( cQuality)                         // 컨텐츠의 품질
  사용기간( cExpire)                      // 컨텐츠의 사용기간
  가격( cValue)                           // 컨텐츠의 가격
  step 1  // 최소한의 디바이스 성능 요구
    if sysNet() = SL0
      service deny;
  step 2
    MAUT()
return SecuLevel;
```

[그림 4] SecureModule 알고리즘

[그림 6]은 사용자의 디바이스 정보와 사용자의 선택한 정보를 가지고 MAUT를 이용해 보안 등급을 결정하는 MAUT 함수이다. 이 함수에서 결정된 보안 등급을 이용하여 디지털 컨텐츠를 암호화하게 된다.

```
function sysNet() return SecuLevel        // 최소한의 디바이스 성능 확인
  if ( dCpu = .1  or  dRam = .1  or  dNet = .1)
    SecuLevel = SL0                       // 최소한의 성능을 만족하지 못함
  return SecuLevel
```

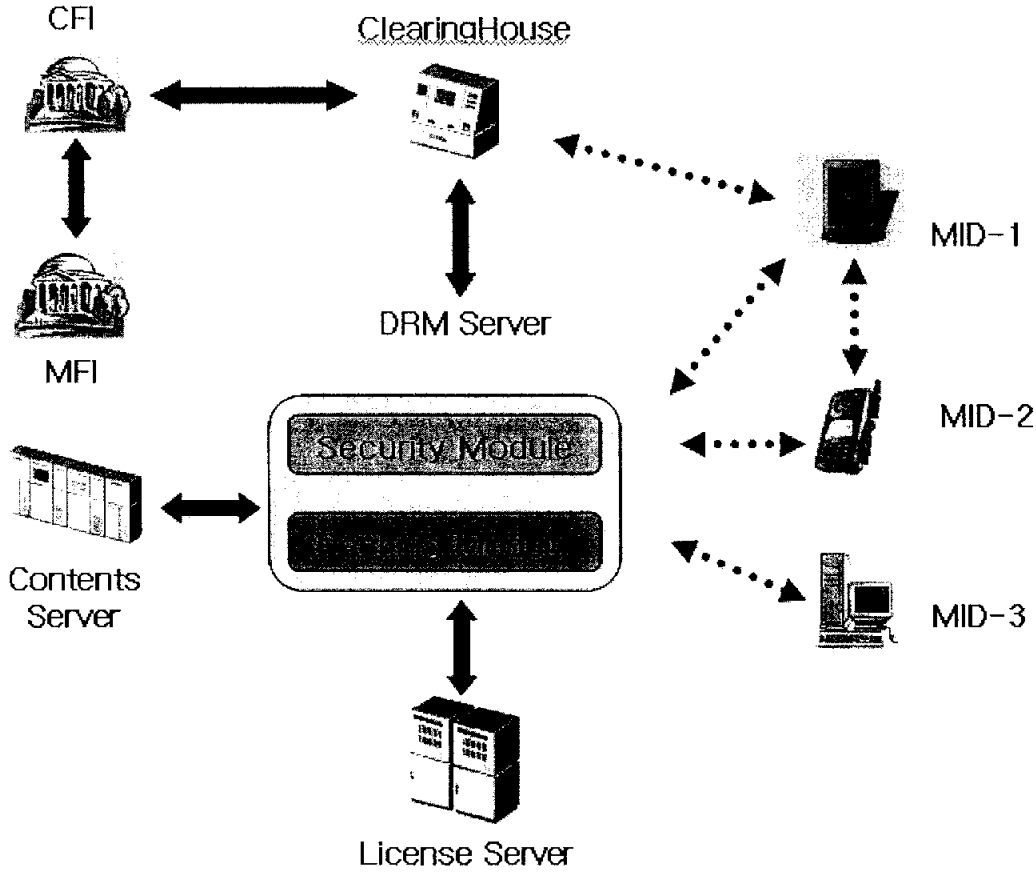
[그림 5] *sysNet* 알고리즘

```
function MAUT() return SecuLevel
  static:
    u(x_1, x_2, ... , x_n)          : 유틸리티 함수
    k_1, k_2, ... k_n               : 가중치, 선호도
    u(x_1, x_2, ... , x_n) ← k_1u_1(x_1) + ... + k_nu_n(x_n)
    // 모든 i에 대해 u_i(x_i^0) = 0, u_i(x_i^*) = 1, k_i는 상수
    // u(x_i), k_n은 사용자와의 통신에 의해서 결정

    for i = 0 to n
      if risk prone then  blog_2(x+1)
      else if risk neutral then  bx
      else if risk averse then  b(2^cx − 1), b, c > 0
    end

    switch( u(x_1, x_2, ... , x_n))     // 보안 등급 결정
      case( < 0.2) : SecuLevel = SL1;
      case( < 0.2) : SecuLevel = SL1;
      case( < 0.2) : SecuLevel = SL1;
      case( < 0.2) : SecuLevel = SL1;
      defalut SecuLevel = SL5;
return SecuLevel
```

[그림 6] *MAUT* 알고리즘

4. 적응적 보안 정책을 이용한 DRM 시스템

본 논문에서 제시한 DRM 시스템은 [그림 7]과 같다. 사용자는 DRM Server로부터 Management Agent를 자동으로 다운로드 받게 된다. 사용자의 디바이스에 다운로드 된 Management Agent는 사용자 디바이스의 정보의 송신, 라이센스 및 디지털 컨텐츠 관리 기능을 수행하며 TRS[19]를 지원한다. 또한 메시지의 서명 및 검증 기능과 키 관리 기능을 지원한다.



[그림 7] 제안 시스템

[그림 8]에서 볼 수 있듯이 Management Agent는 디지털 컨텐츠의 실행 관

리에 대한 "플레이어", Server 및 ClearingHouse에 대한 접속에 관한 "접속", 사용자 디바이스에 저장된 디지털 컨텐츠에 대한 관리에 대한 "검색" 그리고 다른 사용자에게 디지털 컨텐츠를 배포할 수 있는 Superdistribution에 대한 "선물" 메뉴를 가지고 있다. 제안한 시스템에서는 어떤 디지털 컨텐츠에 대해 정당한 권리를 가진 사용자 MID-1이 다른 사용자 MID-2에게 배포할 때 선물이라는 개념을 이용하여 디지털 컨텐츠에 대한 라이센스 비용을 대신 지불한다는 개념을 시나리오에 포함한다. 물론 사용자 MID-2는 다른 사용자로부터 전달받은 디지털 컨텐츠에 대한 라이센스 비용을 자신이 지불할 수 있다.

[그림 8] Management Agent

Management Agent를 다운로드 받고나서 사용자는 Management Agent를 통해서 사용할 디지털 컨텐츠를 선택하게 된다. 다음으로 디지털 컨텐츠의 품질(*cQuality*)을 선택한다. 다음으로 디지털 컨텐츠 사용기간(*cExpire*)을 선택한다. 마지막으로 디지털 컨텐츠의 가격(*cValue*)을 선택하게 된다. 각각의 정보와 함께 사용자의 디바이스 정보들도 함께 DRM Server로 전송된다. 전송

되는 디바이스 정보는 네트워크 속도(*dNet(kbps)*), CPU 성능(*dCpu(Mhz)*), 메모리 용량(*dRam(M)*)이다.

Security Module은 전달된 정보들을 이용하여 디지털 컨텐츠에 적용할 보안 등급을 결정한다. 먼저 디바이스 정보를 이용하여 [그림 6]의 sysNet 알고리즘을 통해 사용자의 디바이스가 최소한의 요구사항을 만족하는지를 검사한다. 만약 요구사항을 만족하지 못한다면 서비스는 거부된다.

만약 최소한의 요구사항을 만족한다면 각각의 정보들은 [표 6]과 [표 7]을 이용하여 환산 값으로 바꾸고 [그림 6]의 MAUT 알고리즘을 이용하여 보안등급을 결정하게 된다.

이런 과정을 거쳐 결정된 보안 등급은 Packaging Module에서 디지털 컨텐츠를 암호화할 때 사용된다.

4.1 시스템 구성

논문에서 제안한 시스템에서 가장 핵심이 되는 DRM Server는 크게 2개의 모듈로 이루어져 있다. 하나는 Management Agent가 전송한 사용자의 디바이스 정보와 컨텐츠의 가치를 이용해 디지털 컨텐츠를 암호화할 때 적용할 보안 등급을 결정하는 적응적 보안 등급 알고리즘을 구현한 Security Module이다. 다른 하나는 Security Module에서 결정한 보안 등급에 따라 실제로 디지털 컨텐츠를 암호화 하는 Packaging Module이다.

License Server는 사용자에게 발급된 라이센스를 관리하는 역할을 한다. 이 서버는 차후에 정당한 사용자가 라이센스를 분실하거나 재발급 요청을 할 경우를 대비하기 위해 존재한다. 만약 사용자가 디바이스의 분실이나 다른 디바

이스를 이용하여 디지털 컨텐츠를 사용하고자 할 경우 재발급 요청을 하면 License Server는 해당 사용자가 정당한 사용자인지를 판별하고 요청받은 라이센스가 올바른 것인지를 판별한 다음 사용자에게 발급해준다.

Contents Server는 컨텐츠 저작권자로부터 계약에 의해 제공된 컨텐츠와 비즈니스 룰, 그리고 관련 정보들을 관리하는 데이터베이스 역할을 수행한다. 사용자로부터 디지털 컨텐츠를 요청받은 DRM Server는 Contents Server에게 해당 디지털 컨텐츠를 요청한다. Contents Server는 요청받은 디지털 컨텐츠와 비즈니스 룰을 되돌려 준다.

ClearingHouse는 디지털 컨텐츠의 거래 내역을 저장하는 역할을 수행한다. 거래 내역을 저장하는 이유는 혹시 발생할지 모르는 이익 분배 문제에 대한 증거 자료를 보관하기 위해서이다. ClearingHouse는 사용자와 FI 사이에서 거래 내역과 관련된 정보를 보관하며 컨텐츠의 저작권자와 컨텐츠 제공자가 거래 내역을 요청하면 해당 정보를 제공한다.

사용자는 MID로 표현되는데 디지털 컨텐츠 제공자가 제공하는 디지털 컨텐츠를 사용하고자 하는 개체이다. MID는 IrDA나 Bluetooth 등을 통해 디지털 컨텐츠를 서로 주고받을 수 있다.

사용자 MID와 디지털 컨텐츠 제공자는 각자의 은행에 계좌를 개설하고 은행이 생성한 공개키 쌍과 PRC, 그리고 은행의 공개키를 제공받아 디바이스와 시스템에 보존한다. 이런 방식을 사용하는 이유는 제한된 자원과 저성능의 컴퓨팅 파워를 가진 사용자 MID의 디바이스를 이용하여 공개키 쌍을 생성하고 통신을 통해 은행의 공개키를 받는 것은 통신비용의 낭비가 심하기 때문이다.

4.2 결제 과정

사용자 MID-1은 DRM Server에 접속하여 먼저 Management Agent를 다운로드 받는다. 그리고 Management Agent를 통해 원하는 디지털 컨텐츠를 결정한 후 품질, 가격, 사용기간을 선택하고 DRM Server로 전송한다. Security Module은 적응적 보안 등급 알고리즘에 따라 보안 등급을 결정하고 이에 따라 패키징된 디지털 컨텐츠를 다운로드 받는다. 그리고 사용자는 디지털 컨텐츠에 대한 요금 지불을 하고 디지털 컨텐츠를 사용할 수 있는 라이센스를 획득한다. 다음과 같은 결제 과정을 거친 후 사용자는 디지털 컨텐츠를 사용할 수 있다.

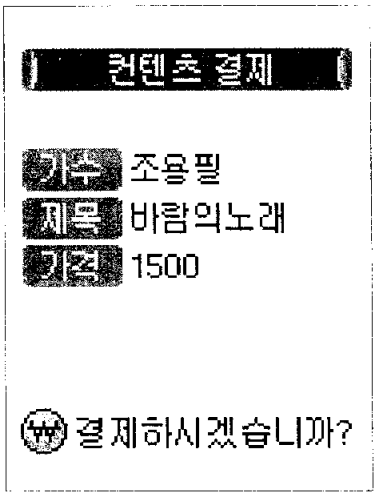
① 사용자 MID-1은 Management Agent를 이용하여 결제 요청 메시지를 생성하고 자신의 개인키로 서명한 다음 DRM Server에게 전달한다. 결제 요청 메시지에는 사용자 MID-1에 관한 정보와 등록 은행인 MFI의 주소와 PRC, 다운로드 받은 디지털 컨텐츠의 종류와 가격 등의 관련 정보를 포함한다.

② DRM Server는 결제 요청 메시지를 ClearingHouse에게 전달한다.

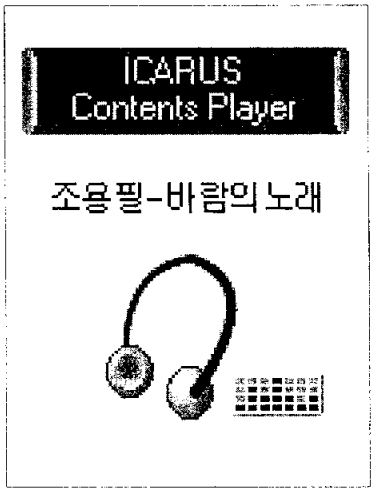
③ ClearingHouse는 전달받은 결제 요청 메시지를 디지털 컨텐츠 제공자의 등록 은행인 CFI에게 전달한다.

④ CFI는 결제 요청 메시지를 분석하여 사용자 MID-1의 등록은행인 MFI에게 전달한다.

⑤ MFI는 결제 요청 메시지를 분석하여 사용자 MID-1을 확인하고 사용자



[그림 9] 컨텐츠 결제



[그림 10] 컨텐츠 플레이

MID-1의 공개키로 메시지의 서명을 검증한다. 만약 서명 검증에 실패하면 이유를 결제 요청 응답 메시지에 포함해서 되돌려 준다. 서명 검증에 성공하면 메시지에 포함된 가격정보를 이용하여 CFI와 transaction을 처리한다. MFI는 처리 결과를 포함하는 결제 요청 응답 메시지를 생성하고 자신의 개인키로 메시지를 서명한 다음 CFI에게 전달한다.

⑥ CFI는 결제 요청 응답 메시지를 ClearingHouse에게 전달한다.

⑦ ClearingHouse는 결제 요청 응답 메시지를 분석하여 결제 요청의 성공 여부를 판별한다. 결제 요청이 성공했다면 거래 내역을 저장한 다음 메시지를 DRM Server에게 전달한다.

⑧ DRM Server는 결제 요청 응답 메시지를 분석하여 결제 요청의 성공 여부를 판별한다. 결제 요청이 성공했다면 License Server에게 사용자 MID-1의 정보와 해당 디지털 컨텐츠의 정보를 포함하는 라이센스 발급 요청 메시지를 생성하고 License Server에게 전달한다.

⑨ 라이센스 발급 요청 메시지를 전달받은 License Server는 사용자 MID-1의 정보와 디지털 컨텐츠의 정보 그리고 디지털 컨텐츠를 복호화하기 위해 필요한 정보들을 포함하는 라이센스를 생성하고 DRM Server의 개인키를 이용하여 서명한 후 DRM Server에게 전달한다.

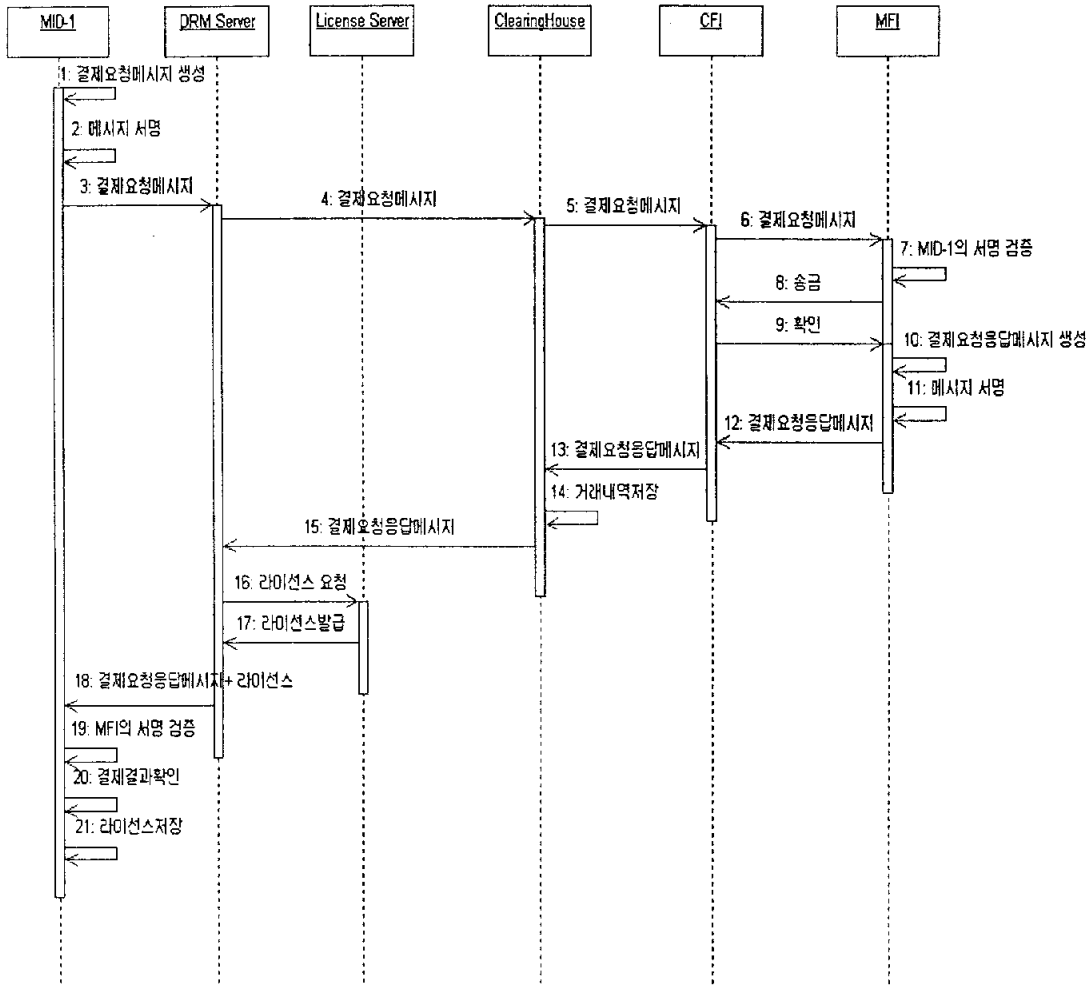
⑩ DRM Server는 라이센스와 결제 요청 응답 메시지를 사용자 MID-1에게 전달한다.

⑪ 사용자 MID-1은 Management Agent를 통해 MFI의 공개키를 이용하여 결제 요청 응답 메시지의 서명을 검증한 다음 결제 요청 결과를 확인한다. 그리고 함께 전달된 라이센스에 포함된 복호화 정보를 이용하여 디지털 컨텐츠를 복호화하여 사용한다.

[그림 11]은 앞에서 설명한 결제 과정을 순서 다이어그램으로 표현한 것이다.

4.3 Superdistribution

Superdistribution은 DRM 시스템이 제공해야하는 기본 기능으로 디지털 컨텐츠에 대한 라이센스를 소유한 사용자가 다른 사용자에게 직접 또는 간접적인 방법으로 배포하는 것을 의미한다. 이 절에서는 디지털 컨텐츠에 대한 라이센스를 소유한 사용자 MID-1이 다른 사용자 MID-2에게 디지털 컨텐츠를 배포하고 결제 과정을 통해 사용자 MID-2가 디지털 컨텐츠를 사용하는 과정에 대해서 기술한다. 배포된 디지털 컨텐츠는 정당한 지불을 통해 라이센스를 획득하지 못하면 사용할 수가 없다.



[그림 11] 결제 과정

최초 디지털 컨텐츠 사용자의 정보는 Owner에 저장된다. Superdistribution을 통해 다른 사용자들에게 배포를 하면 다른 사용자의 정보가 User1, User2, User3에 차례로 저장된다. 디지털 컨텐츠를 사용하고자 할 경우 Management Agent가 라이센스의 Owner 또는 UserInfo 내에 사용자의 정보가 있을 경우에만 사용을 허용한다. 가정에 따라 사용자 MID-1의 정보가 Owner에 저장된다. 본 논문에서 디지털 컨텐츠를 사용자 MID-2에게 전달할 때 요금은 사용

자 MID-1이 지불한다고 가정하고 있다. Superdistribution은 다음과 같은 과정을 통해 이루어진다.

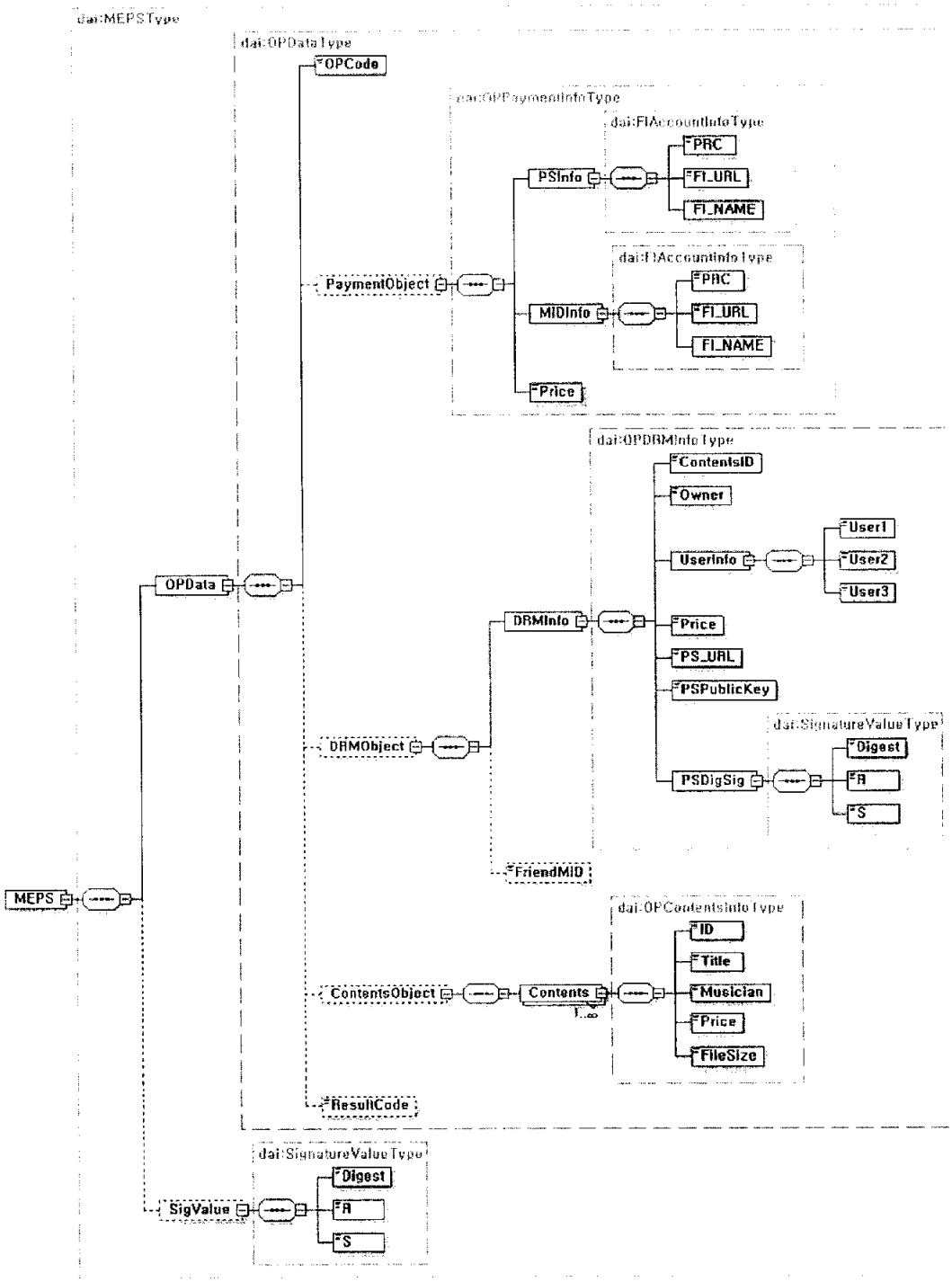
① 디지털 컨텐츠를 전달 받고자하는 사용자 MID-2는 Bluetooth나 IrDA 등의 수단을 이용하여 디지털 컨텐츠를 소유한 MID-1에 접속하여 디지털 컨텐츠를 전달받는다.

② MID-2는 자신에 관한 정보와 자신의 디바이스 정보를 MID-1에게 전달한다. MID-1의 Management Agent는 사용자 MID-2의 디바이스 정보를 DRM Server에게 전송하여 디지털 컨텐츠를 사용할 수 있는지 여부를 확인한다. 만약 사용 불가능이라면 사용 불가능이라는 메시지를 MID-2에게 전송하고 과정을 종료한다. 만약 사용 가능이라면 디지털 컨텐츠에 관한 정보와 MID-2에 관한 정보를 포함하는 결제 요청 메시지를 생성하고 서명한 후 ClearingHouse로 전달한다. 이렇게 하는 것은 DRM Server에게 걸리는 부하를 줄이고 사용자의 통신비용을 줄이기 위한 것이다.

③ ClearingHouse는 전달받은 결제 요청 메시지를 디지털 컨텐츠 제공자의 등록 은행인 CFI에게 전달한다.

④ CFI는 결제 요청 메시지를 분석하여 사용자 MID-1의 등록은행인 MFI에게 전달한다.

⑤ MFI는 결제 요청 메시지를 분석하여 사용자 MID-1을 확인하고 사용자 MID-1의 공개키로 메시지의 서명을 검증한다. 만약 서명 검증에 실패하면 이유를 결제 요청 응답 메시지에 포함해서 되돌려 준다. 서명 검증에 성공하면 메시지에 포함된 가격정보를 이용하여 CFI와 transaction을 처리한다.



[그림 12] 라이센스의 XML Schema

MFI는 처리 결과를 포함하는 결제 요청 응답 메시지를 생성하고 자신의 개인키로 메시지를 서명한 다음 CFI에게 전달한다.

⑥ CFI는 결제 요청 응답 메시지를 ClearingHouse에게 전달한다.

⑦ ClearingHouse는 결제 요청 응답 메시지를 분석하여 결제 요청이 성공했는지를 판별한다. 결제 요청이 성공했다면 거래 내역을 저장한 다음 사용자 MID-2의 정보를 포함하는 라이센스 요청 메시지를 DRM Server를 통해 License Server에게 전달한다.

⑧ 라이센스 요청 메시지를 전달받은 License Server는 메시지를 분석하여 사용자 MID-1을 확인하고 사용자 MID-1이 소유하고 있는 라이센스에 사용자 MID-2의 정보를 삽입하고 새로운 라이센스를 생성하고 DRM Server의 개인키로 서명한 후 DRM Server를 통해 ClearingHouse로 전달한다.

⑨ 새로운 라이센스를 전달받은 ClearingHouse는 결제 요청 응답 메시지와 함께 라이센스를 MID-1에게 전달한다.

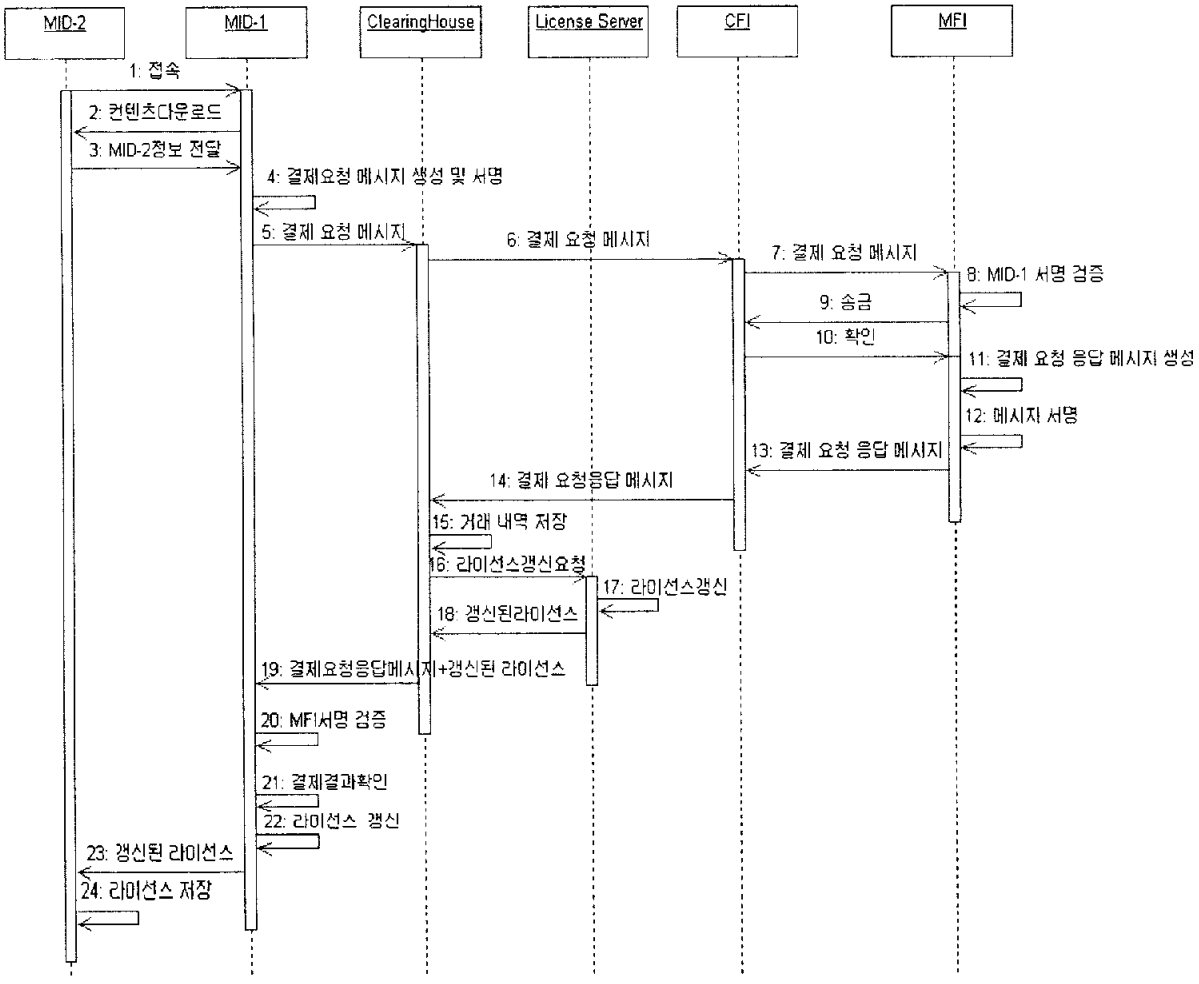
⑩ 사용자 MID-1은 Management Agent를 통해 MFI의 공개키를 이용하여 결제 요청 응답 메시지의 서명을 검증하고 결제 요청 결과를 확인한다. 그리고 새로운 라이센스를 기존의 라이센스로 교체를 하고 사용자 MID-2에게 새로운 라이센스를 전달한다.

⑪ 사용자 MID-2는 사용자 MID-1에게서 전달받은 라이센스를 자신에게 적용시킨 후 디지털 컨텐츠를 사용할 수 있다.

아직까지는 유선을 이용한 통신에 비해 휴대폰과 같은 무선 통신을 이용하

는 경우에는 통신비용이 상대적으로 높은 편이다. 따라서 사용자와 Server간의 무선 통신의 경우 횟수를 최대한으로 줄여야만 한다. 제안한 시스템에서는 사용자와 Server간의 통신이 최대한 효율적으로 이루어지도록 설계하였다.

[그림 13]은 Superdistribution을 순서 다이어그램으로 나타낸 것이다



[그림 13] Superdistribution

5. 구현 및 평가

제안 시스템에서 DRM Server, ClearingHouse, CFI, MFI, Content Server는 Windows 2000을 운영체제로 펜티엄급 PC들을 대상으로 구현하였다. Servlet으로 각 구성 객체들의 모듈을 작성하였으며 HTTP 프로토콜을 이용하여 통신한다. MID-1과 MID-2는 각각 iPAQ과 J2ME Simulator를 이용하여 구현하였으며 MID-3은 VC++ 6.0을 이용하여 구현하였다.

제안한 시스템에서는 암/복호화 알고리즘으로 공개키 알고리즘에 비해 상대적으로 적은 길이의 키를 가지고도 동일한 암호화 강도를 제공하며 저성능의 디바이스에서도 이용 가능한 알고리즘인 ECDSA 알고리즘을 이용하여 저성능의 디바이스를 사용할 수 있도록 하였다.

[표 8]은 J2ME Simulator에서 100byte 길이의 데이터를 대상으로 비슷한 암호 강도를 가진 것으로 알려진 1024bit의 RSA 알고리즘과 192bit의 ECDSA 알고리즘을 이용하여 서명과 검증에 걸리는 시간을 측정한 것이다. ECDSA 알고리즘이 RSA알고리즘에 비해 서명 시간이 적다는 것을 알 수 있다.

그런데 ECDSA 알고리즘을 이용한 서명 검증 시간이 RSA 알고리즘에 비해 많은 시간이 걸리는 것으로 나타났다. 이것은 아직까지 ECDSA 알고리즘의 구현이 최적화 되지 않았고 개선의 여지가 남아 있다는 것을 의미한다. 참고로 테스트에 사용한 RSA 알고리즘과 ECDSA 알고리즘은 BouncyCastle[20] 에서 제공하는 알고리즘 구현을 사용하였다.

[표 8]을 살펴보면 서명에 걸리는 시간이 약 22초 정도 걸린다. 22초란 시간은 사용자가 기다리기엔 너무나도 오랜 시간이다. 결제 과정을 살펴보면 MID측

에서 서명과 서명 검증이 각각 1번씩 발생한다. 따라서 알고리즘을 더 효율적인 구조로 만들어 서명과 검증 시간이 좀 더 적어지도록 만드는 것이 요구되며, 192bit보다 적은 크기의 키 사용을 통해 시간을 단축할 수 있다.

[표 8] 100byte 데이터에 대한 RSA와 ECDSA의 서명 및 검증 시간 비교

메시지의 크기	RSA 1024		ECDSA 192	
	서명	검증	서명	검증
MD5 128bit	31275	3401	224950	4504
SHA-1 160bit	32145	4487	224993	6256

그리고 라이센스를 표현할 때 권리명세 언어인 XrML[21]을 이용하여 표현함으로써 다른 라이센스와 호환이 될 수 있도록 고려하였다. XrML은 다른 DRM 시스템과 비즈니스 규칙이 호환되도록 하는 것을 가능하게 해준다.

기존의 DRM 시스템은 사용자의 디바이스가 일반 데스크탑 PC인지 PDA인지 휴대폰인지 고려하지 않고 일률적인 보안 정책을 적용을 함으로써 PDA나 휴대폰을 가진 사용자가 디지털 컨텐츠를 이용하는데 상당한 부하를 주는 암호화 알고리즘을 사용한다. 그리고 CA기반의 PKI는 강력한 암호화 강도를 제공함으로써 안전한 결제방식을 제공하지만 CA를 유지하기 위한 많은 비용과 저성능의 디바이스에서 사용하기에는 많은 부담이 있다는 문제점이 있다.

그러나 본 논문에서 제안한 적응적 보안 등급 알고리즘을 사용하여 디지털 컨텐츠에 적용할 암호화 알고리즘을 결정하면 디바이스에 최적화된 암호화 알고리즘을 결정할 수 있고 사용자의 기호를 암호화 알고리즘 결정에 반영함으로써 사용자의 만족도를 높일 수 있다. 또한 X9.59와 ECDSA 알고리즘을 사용하여 PKI를 사용하지 않고서 간단하면서도 PKI만큼 안전한 지불 프로토콜

을 설계하고 구축하였다. 따라서 저 비용으로도 시스템 구축이 가능하다는 장점이 있다.

사용자의 디바이스에서 동작하는 Management Agent는 TRS기능을 제공한다. 하지만 TRS의 구현은 OS레벨의 동작을 중간에서 가로채 제어해야 하는데 대부분의 가장 널리 사용되고 있는 Windows 운영체제는 소스를 공개하고 있지 않다. 또한 사용자 디바이스의 다양한 저장 공간을 고려해야만 하기 때문에 많은 어려움이 있다.

6. 결론 및 향후 연구

디지털 컨텐츠에 대한 저작권 문제를 해결하기위해 다양한 시스템이 제안되었고 그 중 DRM시스템이 가장 널리 사용되고 있지만 현재의 DRM 시스템은 유비쿼터스 환경에 그대로 적용하기에는 많은 문제점을 가지고 있다. 또한 디지털 컨텐츠의 종류도 제한되어 있으며, 사용자 환경에 관해서도 적응적으로 표현하기에는 많은 문제점이 있다. 본 논문에서는 이들 문제점을 해결하기 위하여 사용자 디바이스의 특성과 디지털 컨텐츠의 종류, 그리고 사용자의 선택에 따라 최적의 보안 등급을 결정함으로써 사용자의 만족도와 편리성을 충족시킬 수 있는 DRM 시스템을 제안하였다. 제안한 시스템은 PKI를 사용하지 않고서도 비슷한 암호화 강도를 제공하며, 안전하고 편리한 결제 프로토콜을 제시하였다. 기존의 시스템이 컨텐츠를 유포하는데 CD, e-mail 등과 같은 제한된 방법을 가지고 있었지만 제안한 시스템은 사용자간 IrDA, Bluetooth 등을 이용하여 쉽고 편리하게 직접 배포할 수 있는 방법을 제시하였다. 또한 디바이스의 성능에 최적화된 암호화 알고리즘을 사용함으로써 해당 디바이스에서 가장 효율적인 디지털 컨텐츠 사용을 추구할 수 있었다.

본 논문에서 제안한 시스템은 대상을 디지털 컨텐츠에만 제한하지 않고 기업 내에서 기밀문서 관리시스템이나 온라인 소프트웨어 판매, 전자 도서관 등 어떤 자원에 대한 보호가 필요한 시스템에 적용할 수 있다.

향후 연구 과제로 ECDSA 알고리즘을 최적화하여 전자서명을 서명하고 검증하는데 걸리는 시간을 최소화하는 방안에 대한 연구가 필요하다.

참고문헌

[1] F. Hartung, F. Ramme, "Digital Rishts Management and Watermarking of Multimedia Content for M-Commerce Application," *IEEE Communications Magazine*, Vol. 38, Issue 11, Nov.2000, pp.78-84.

[2] Qiong Liu, Reihaneh Safavi-Naini, "Digita Rishts Management for Content Distribution", citeseer.nj.nec.com/liu03digital.html.

[3] Joan Feigenbaum, Michael J. Freedam, "Privacy Enginnering for Digital Rights Management Systems," Digital Rights Management Workshop, 2001, pp.76-105.

[4] 강호갑, "소프트웨어 저작권 보호 기술", www.fasoo.com/sub_tech02.html

[5] P. Loo, N. Kingsbury, "Watermark detection based on the properties of error control codes", Vision, Image and Signal Processing, *IEEE Proceedings*, Vol. 150, Issue. 2, April.2003, pp.115-121.

[6] S. Craver, N. Memon et al., "Resolving rightful ownerships with invisible watermarking techique: limations, attacks, and implications", Selected Areas in Communications, Vol. 16, Issue. May. 1998, pp.573-586.

[7] DOI, www.doig.org

[8] IBM Pervasive Computing, www.ibm.com

[9] M. Satyanarayanan, "Pervasive Computing: Vision and Challenges," IEEE Personal Communications, Vol. 8, Issue. 4, Aug.2001, pp.10-17.

[10] Jin-Hee Han, Young-Jin Kim, Sung-IK Jun, "Implemation of

ECC/ECDSA cryptography algorithms based on Java card," MNSA 2002(ICDCS '02 Workshops), July.2002.

[11] InterTrust, www.intertrust.com/main/overview/indexhtml

[12] Microsoft, cryptome.rog/ms-drm-os2.htm

[13] 파수닷컴, www.fasoo.com

[14] R.L.Keeney, H.Raiffa, Decisions with Multiple Objective: Preferences and Value Tradeoffs, *John Wiley & Sons*, New York, NY, 1976.

[15] Mokdong Chung, Vasant Honavar, "A Negotiation Model in Agnet-mediated Electronic Commerce," *Proceedings of the IEEE International Symposium on Multimedia Software Engineering*, Taipei, Dec.2000, pp.403-410.

[16] American National Standard DSTU X9.59 Electronic Commerce for Finalncial Service Industry: Account Based Secure Payment Object, 2000.

[17] R. Housely, W. Ford et al., RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Internet Engineering Task Force, January.1999.

[18] Albert Levi, Certin K, "CONSEPP: Convenient and Secure electronic payment Protocol based on X9.59," Computer Security Application Conference 2001, ACSAC 2001, *Proceedings 17th Annual*, 10-14, Dec. 2001, pp.286-295.

[19] D. Aucsmith and Graunk, "Tamper Resistant Software: An

Implementation," in Proc. 1st International Workshop on Information Hiding, Springer Lecture Notes, 1986.

[20] BouncyCastle, bouncycastle.org

[21] XrML, www.xrml.org

[22] 김환조, 김만수, 정목동, "XML을 이용한 PKI 기반 CA 설계," 한국멀티미디어학회 추계학술대회 논문집, 2002. pp.259-262.

[23] 김환조, 채종우, 정목동 "X9.59를 이용한 DRM 기반 컨텐츠 유통 시스템 설계 및 구현," 한국멀티미디어학회 춘계학술대회 논문집, pp.771-774.

[24] M.S. Kim, H.J. Kim and M.D. Chung. "Design of a Secure E/M-Commerce Application which Integrates Wired and Wireless Environments," *Proceedings of the Third IASTED International*, Jul.2003, pp.259-264.

감사의 글

때론 선배로서 때론 친구로서 격려와 세심한 배려로 이끌어주신 정목동 교수님께 진심으로 감사를 드립니다. 그리고 본 논문이 이루어지기까지 아낌없는 충고를 해 주신 우종호 교수님과 권오흠 교수님께 감사드립니다. 또한 많은 가르침과 격려를 주신 학과의 여러 교수님들께 감사를 드립니다.

대학원 생활동안 힘들 때마다 따뜻한 격려와 위로를 해주신 창수형, 예쁜 희숙누나, 다투면서도 도움이 필요할 때 마다 손을 내밀어준 석주, 귀찮게 물을 때 마다 웃음으로 대해주던 채주형, 수진형, 봉기형에게도 감사의 마음을 전합니다. 그리고 2년간 함께 동고동락했던 성주와 윤희, 수 많은 밤을 같이 새며 프로젝트를 수행했던 종우와 정철이와 경현씨, 성록씨, 정식씨, 같이 고생했던 연구실 후배 지호, 재건, 해길, 힘들 때 마다 조언과 충고를 아끼지 않았던 정석선배, 광호선배, 제천선배에게도 마찬가지로 고마운 마음을 전합니다.

옆에 있으면서 어려울 때나 힘들 때 격려를 잊지 않던 여자친구, 힘들 때 술 한 잔 나눠 마시며 격려를 해준 동기들 세식, 상현, 정진, 용철, 성웅, 멀리 떨어져 있지만 항상 힘이 되어준 동생 환옥, 두석이에게 감사의 마음을 전합니다. 마지막으로 지금까지도 걱정을 하시는 아버님, 어머님께 이 지면을 빌어 감사와 사랑한다는 말을 전하며 끝을 맺고자 합니다.

2004년 2월 김 환 조 드림.