모바일 RFID 시스템에서의 보안 위협과 대안+

*정윤선, **김일중, ***최은영, ****이동훈
고려대학교 정보경영공학전문대학원
*jdbstjs@hanmail.net **wyvern99@korea.ac.kr
***bluecey@cist.korea.ac.kr ****donghlee@korea.ac.kr

Security threats and alternative of Mobile RFID system

*Yun Seon Jung **Il Jung Kim ***Eun Young Choi ****Dong Hoon Lee
Graduate School of Information Management and Security, Korea University

요약

RFID 시스템은 무선통신기술을 사용하여 직접 접촉하지 않고 RFID 태그 정보를 식별하는 자동식별기술을 말한다. RFID 시스템의 장점 때문에 바코드 대체 기술로서 주목을 받고 있다. 최근에, RFID 시스템은 모바일 단말기 안에 내장된 리더를 사용하여 사용자에게 유용한 정보를 제공하는 모바일 시스템으로 확대대고 있다. 모바일 RFID 시스템은 모바일 리더를 사용하여 물품의 정보를 얻는다. 그 다음 얻은 정보를 사용하여 무선이동통신 네트워크에서 사용자에게 다양한 부가 서비스를 제공한다. 모바일 RFID 시스템은 RFID 리더에 이동성을 결합했을 뿐만 아니라, 언제 어디에서나 실생활에 밀접한 물품에 대한 정보를 활용할 수 있다는 점에서 많은 주목을 받고 있다. 그러나 모바일 RFID 시스템은 정보누출, 추적성, 위조 등과 같은 RFID 시스템의 위협에 취약할 뿐만 아니라 모바일 리더의 이동성에 의해 사용자의 프라이버시가 쉽게 침해된다.

본 논문에서는 기존에 제안된 모바일 RFID 시스템에 관하여 살펴보고 모바일 RFID 시스템에서의 발생하는 추가적인 문제점을 지적한 후에 이에 대한 해결 방안을 제시한다.

Ⅰ. 서론

RFID (Radio Frequency IDentification) 시스템은 무선통신기술을 사용하여 직접 접촉하지 않고 RFID 태그 정보를 식별하기 때문에 기존의 바코드 시스템보다 많은 장점을 가지고 있다. 무선주파수를 사용하여 태그에 직접 접촉하지 않고도 한꺼번에 다수의 태그를 읽을 수 있다. RFID 태그는 바코드보다 다양하고 많은 양의 정보를 저장할 수 있을 뿐만 아니라 RFID 리더를 사용하여 태그에 새로운 정보를 기록하고 수정할 수 있다[1]. 모바일 RFID 시스템은 기존의 RFID 시스템의 장점과 모바일 시스템의 장점을 모두 가지고 있기 때문에 많은 연구가 이루어지고 있다[2,4,5,6,8,9,10,12]. 모바일 RFID 기술이란 기존 RFID 시스템에 휴대폰의 이동통신망을 결합한 것으로써, 개인이 소유하고 있는 휴대폰을 리더로 사용하여 상품에 부착된 RFID 태그로부터 정보를 얻고 이동통신망을 통해 정보를 활용하는 기술이다[3,11]. 모바일 RFID는 휴대폰에 RFID 리더를 내장함으로써 실생활에 더욱 밀접한 서비스를 제공하여 물류 및 유통 시스템에 국한되었던 RFID 응용 서비스가 더욱 확대될 것으로 예상된다[3]. 우리나라는 전국적인 휴대폰 서비스 사용자와 세계를 선도하는 모바일 기술을 가지고 세계 최초로 모바일 RFID 기술 개발을 시도하고 있지만 아직까지는 많은 문제점을 내포하고 있다. 기존 RFID 시스템에서 해결되지 못한 보안 위협 문제뿐만 아니라 RFID 리더가 휴대폰에 내장되어 누구나, 언제, 어디서나 리더를 이동시키고 사용할 수 있다는 점에서 추가적인 보안 위협을 발생시킨다. 그러므로 개인 프라이버시 침해 및 노출의 위협을 최소화하고 모바일 RFID 시스템에서 안전한 서비스를 제공하기 위해 새로운 보안 기술과 대안이 요구되어진다.

본 논문에서는 기존의 모바일 RFID 시스템에 관하여 살펴보고 모바일 RFID 시스템에서 발생하는 문제점을 지적한다. 그리고 문제점 해결하기 위한 방안을 제시한다.

+ "이 논문은 2006년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No.R01-2004-000-10704-0) "

Ⅱ. 모바일 RFID 시스템

2.1 구성요소

2.1.1 RFID 태그

RFID 태그는 리더로부터 질의를 받으면 RF신호를 이용하여 사물의 식별 코드를 전송하는 RFID 시스템의 기본 구성 요소이다. RFID 태그는 배터리의 존재 유무에 따라 수동

형 태그와 능동형 태그로 나뉘어진다. 수동형 태그는 리더로부터 받은 신호를 가지고 유도 전류를 만들어 태그의 전원으로 사용한다. 능동형 태그는 태그 자체에 배터리를 가지고 있어서 자체적으로 전원을 공급한다[1].

2.1.2 모바일 단말기

모바일 RFID 시스템에서 모바일 단말기는 프록시로 사용되는 단말기와 RFID 리더로 사용되는 단말기의 두 가지 유형이 제안되었다[2,3,6,9,12]. 프록시로 사용되는 단말기는 RFID 태그와 리더 사이에서 전송되는 값들에 대해 관리를 하고 프라이버시를 보호하는 역할을 한다. RFID 리더로 사용되는 단말기는 모바일 단말기 자체가 리더가 된다. 즉, 모바일 단말기를 통해 RFID 서비스를 제공하기 위해서 휴대폰 등에 RFID 리더기를 탑재한 것이다. 모바일 RFID 리더기는 태그로부터 전송받은 식별코드를 읽어 OIS 서버의 해당 정보를 휴대폰 단말기 상에 디스플레이 해준다. 리더기 장착 방법에 따라 휴대폰 내장형과 외장형(동글형)으로 구별된다.

2.1.3 백-앤드 네트워크

백-앤드 네트워크는 태그가 부착된 물품 정보를 공유하고 즉시 자동적으로 식별할 수 있도록 지원한다. 네트워크는 객체 디렉터리 서비스(Object Directory Service, ODS) 서버, 객체 정보 서비스(Object Information Service, OIS) 서버, 미들웨어로 구성된다.[3] ([그림1])

가. ODS 서버

ODS(Object Directory Service) 서버는 인터넷 주소 정보를 제공하는 DNS(Domain Name System)과 유사한 형태로써 RFID 상품 정보를 제공한다. 즉, 해당 식별 코드의 정보를 가지고 있는 서버의 위치(URL: Uniform Resource Location)를 알려준다.

나. OIS 서버

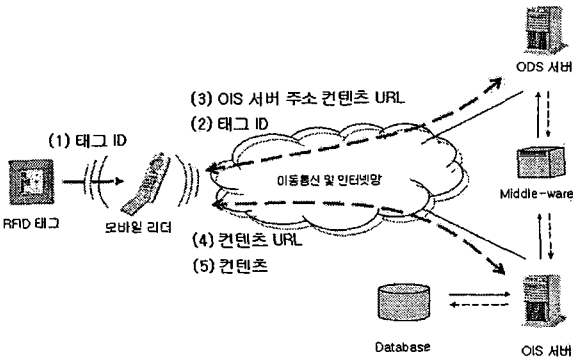
OIS(Object Information Service) 서버는 객체의 상세정보 및 이력정보를 관리하고, 태그의 식별 코드와 매치되는 컨텐츠를 저장한다.

다. 미들웨어

미들웨어는 모바일 RFID 리더를 통해 수집된 데이터를 처리하고, 데이터 필터링, 데이터 표현, 백-앤드 데이터베이스로의 데이터 전송 등의 기능을 제공한다.

2.2 모바일 RFID 네트워크 프로토콜

[그림 1]과 같이 모바일 RFID 리더기와 ODS 서버, OIS 서버간의 통신은 이동통신망 및 무선 인터넷망을 통해 이루어진다. (1) RFID 리더가 내장된 휴대폰으로 각 상품에 부착된 RFID 태그를 읽는다. (2) 모바일 RFID 리더는 태그로부터 얻은 태그 ID 정보를 이용하여 ODS 서버에게 태그 ID와 매핑되는 컨텐츠 URL을 요청한다. ODS 서버는 태그 ID와 그에 매핑되는 URL 정보를 저장하고 있는 서버를 말한다. (3) ODS 서버는 매핑되는 컨텐츠의 URL을 모바일 RFID 리더에게 전송한다. (4) 모바일 RFID 리더 역할을 하는 휴대폰은 전송받은 URL을 이용하여 해당 OIS 서버에 컨텐츠를 요청한다. (5) OIS 서버는 해당 컨텐츠를 휴대폰에 전송하여 사용자는 서비스를 제공받게 된다.[3,5]



[그림 1] 모바일 RFID 시스템 구성도

Ⅲ. 모바일 RFID 시스템의 보안 위협

모바일 RFID 시스템이 기존의 RFID 시스템과 크게 다른 점은 누구나 RFID 리더를 소유하고 사용할 수 있다는 점과 모바일 단말기가 이동통신망 및 무선 인터넷망과 같은 큰 네트워크와 연결되어 있다는 점이다. 따라서 모바일 RFID 시스템에서 추가적으로 발생하는 보안 위협은 이와 같은 사실에 기반을 둔다.

본 절에서는 모바일 RFID 시스템에서 발생할 수 있는 보안 위협에 대하여 살펴본다.

3.1 도청

RFID 시스템에서 RFID 태그와 리더는 무선 주파수를 사용하여 정보를 주고받기 때문에 제 삼자가 통신내용을 도청할 수 있다[1].

3.2 태그 위조 및 복제

공격자는 이전의 통신에서 도청한 정보를 정당한 리더에게 재전송하여 자신이 정당한 태그인 척 위장할 수 있다. 그리고 이전 값을 새로운 태그에 저장함으로써 복제된 태그를 생성해 낼 수 있다. 제 삼자가 불법적인 리더를 사용하여 태그의 정보를 수정하더라도 태그는 그것이 불법적인 리더에 의한 것임을 알아채거나 막을 수 없다. 따라서 RFID 태그는 제 삼자에 의해 내용이 변조될 수 있다[1].

3.3 위치 추적

RFID 시스템의 사용자는 제 삼자에 의해서 위치 추적될 수 있다. RFID 태그는 리더의 질의에 대해 항상 같은 값으로 응답을 한다. 따라서 사용자가 소유한 특정 태그를 추적함으로써 태그를 소지한 사용자의 위치를 파악할 수 있다. 모바일 RFID 시스템에서는 모바일 RFID 리더를 소지하고 이동하는 사용자에 대해서도 위치 추적이 가능하다[1]. 휴대폰에 내장된 RFID 리더는 태그로부터 얻은 정보를 가지고 이동통신망을 통하여 부가적인 서비스를 사용자에게 제공한다. 특정 휴대폰이 태그의 정보를 읽고 부가서비스를 받기위해 이동통신망에 접속하면 모바일 RFID 리더 사용자의 위치 추적이 가능하다. 그러므로 기존 RFID 시스템에서 발생할 수 있는 사용자 프라이버시 위협보다 더 심각한 위협이 된다.

3.4 정보 노출

상품을 구매한 후에 제 삼자가 상품의 정보를 읽어오는 것은 구매자의 프라이버시 침해가 된다. 리더를 소지하고 있

는 사용자는 본인의 동의를 구하지 않고도 구매자가 알리고 싶지 않는 정보를 얻을 수 있어 구매자의 프라이버시를 침해하게 된다[4].

3.5 무제한 정보 수집

리더는 RFID 태그가 상품포장에 가려진 상태에서도 원격으로 무선통신이 가능하기 때문에 도청, 위치추적, 개인 프로파일링 등을 통해 개인정보를 불법적으로 수집할 수 있다. 그리고 모바일 RFID 시스템에서는 개인 소유의 리더를 어디로든지 이동시킬 수 있으며 태그 스캐닝이 허가되는 특정 지역이 없기 때문에 태그 정보의 수집에 제한된 범위가 없다. 또한 RFID 리더가 휴대폰에 내장되면 누구나 RFID 리더를 소유할 수 있으므로 누구든지 쉽게 태그의 정보를 수집할 수 있다. 이렇게 수집된 정보들은 다른 곳에 악용될 수 있으며, 만약 네트워크에 유출된다면 기존 RFID 시스템의 프라이버시 침해 문제보다 더욱 심각한 문제를 발생시킬 수 있다[8].

Ⅳ. 기존의 모바일 RFID 시스템

기존의 모바일 RFID 시스템은 모바일 단말기의 유형에 따라 두 가지 유형으로 나눌 수 있다. 모바일 단말기가 프록시 역할을 수행하는 시스템과 모바일 단말기 자체가 RFID 리더가 되는 시스템이다. 일반적으로 RFID 시스템에서 저가형 태그가 많이 사용된다. 그러나 저가형 태그는 연산 능력에 한계가 있다. 이런 저가형 태그의 한계를 해결하기 위하여 프록시 기반의 시스템이 제안되었다. 여기서 모바일 단말기가 프록시의 역할을 수행한다.

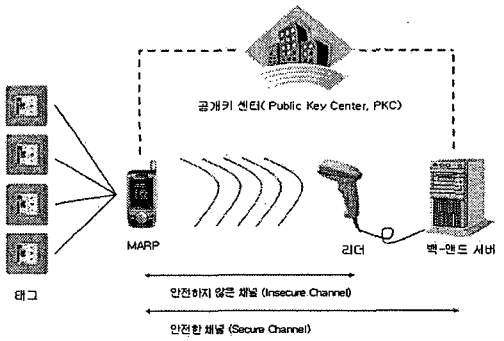
본 절에서는 기존에 제안된 두 가지 유형의 시스템들에 대하여 살펴본다.

4.1 모바일 단말기가 프록시를 수행하는 시스템

Rieback이 제안한 RFID 가디언(Gaurdian) 기법에서 모바일은 사용자가 소유하고 있는 상품에 대한 외부 리더의 접근을 통제한다[12]. 가디언 기법이 제공하는 기능은 다음과 같다: 첫째, 감시(Auditing) 기능을 제공한다. 둘째, 키 관리(Key Management) 기능을 제공한다. 셋째, 접근 제어 (Access Contorol) 기능을 제공한다. 넷째, 인증 (Authentication) 기능을 제공한다. 가디언이 태그를 대신해서 리더와의 인증 과정을 수행한다. 실제 태그가 인증 연산을 수행할 수 있는 능력이 없으므로 가디언이 대신 리더와의 인증 과정에 참여하여 외부에 인증을 받는다. 가디언 기법에서는 강력한 프록시를 사용하여 RFID 시스템의 문제점을 해결하고자 하였다. 프록시 역할을 수행하는 가디언이 태그의 정보가 노출되는 것을 막았으며 태그를 대신해서 인증 과정을 수행하는 등 위에서 언급한 기능들을 제공하도록 제안되었다. 그러나 과거에 소유했던 태그에 대한 정보를 저장함으로써 현재 태그를 소유하고 있지 않으면서도 소유하고 있는 것처럼 외부 리더를 속일 수 있다.

Juels가 제안한 High-Power 프록시 REP 기법은 가디언과 유사지만 더 향상된 기능을 제공한다. 프록시 REP 기법은 자체적으로 태그의 정보를 갱신함으로써 제 삼자가 태그에 의미 없는 값을 써 넣는 공격에 대한 취약성을 해결한다[2]. 그러나 가디언 기법과 프록시 REP 기법 모두 프록시가 외부의 모든 신호를 감지할 수 있다는 강력한 가정을 기반으로 하기 때문에 실제적으로 RFID 시스템의 문제를 해결하기에는 부적합하다.

이전 기법에서의 취약성을 해결하기 위해 MARP(Mobile Agent for RFID Privacy Protection)라는 기법이 제안되었다[6]. MARP 기법에서는 프록시의 역할을 수행하는 모바일이 특정 태그에 정보를 전송하는 것이 아니라 태그와 리더, 모바일이 동시에 동작한다. 이 기법은 모바일과 리더 사이에 공개키 시스템을 기반으로 구축되며 태그에는 해쉬 함수가 탑재된다([그림 2]). 모바일(MARP)과 리더는 랜덤 값을 사용하여 자신의 서명을 생성하고 리더가 속한 그룹의 공개키로 암호화한 값을 주고받는다. 또한 태그의 비밀 값에 해쉬 함수를 취함으로써 데이터베이스는 정당한 태그가 현재 통신에 참여하고 있으며 모바일(MARP)이 정상적으로 동작하고 있음을 알 수 있다. 태그와 모바일, 모바일과 리더, 리더와 데이터베이스 간에 랜덤한 값을 전송함으로써, 프라이버시 문제를 해결할 수 있다. 그러나 공개키 시스템을 기반으로 하기 때문에 추가적으로 외부 시스템이 구축되어야 하며, 외부 서버가 모든 키를 관리하므로 시스템은 외부 서버에 의존적이다.



[그림 2] MARP 기법의 시스템 구성도

4.2 모바일 단말기가 RFID 리더인 시스템

[4]에서 제안된 기법은 상품을 구매하기 전과 상품을 구매한 후의 두 과정으로 이루어져있다. 상품을 구매하기 전 과정은 매장 내에서 상품에 대한 신뢰성 있는 정보를 확인하는 과정이다. 각 매장의 로컬 서버는 상품에 대한 인증용 값 리스트를 미리 저장해둔다. 사용자가 매장에 들어가면 모바일 리더는 로컬 서버로부터 인증서와 인증용 값을 받는다. 상품을 구매한 후의 과정에서 사용자는 모바일 리더를 사용하여 구매한 상품에 대한 정보를 얻고 관리할 수 있다. 그러나 제 삼자는 사용자가 구매한 상품의 정보를 확인할 수 없도록 한다. 이 시스템에서는 구매 전과 구매 후 모두 상품에 대한 신뢰성 있는 정보를 제공하면서도 사용자의 프라이버시를 보호한다. 그리고 추가적인 외부 장비나 외부 서버 없이도 개인 정보 노출과 위치 추적을 방지한다.

[9]에서는 모바일 RFID 시스템에서 태그에 연결된 정보에 대해 개인 프라이버시를 보호하는 기술을 제안하였다. RPS(RFID user Privacy management Service) 시스템에는 OPRP(Owner-defined Privacy Reference Profile)와 PAG (Profile for Access Group)의 개념을 포함하고 있다. OPRP

와 PAG의 결합은 태그와 연결된 정보를 얼마만큼 가능하게 할 것인가에 대한 구매자의 결정을 나타낸다. 따라서 모바일 RFID 사용자는 RPS를 통하여 상품에 부착되어 있는 태그의 정보를 직접 컨트롤할 수 있다. 그러나 RPS 시스템은 전적으로 RPS 서버에 의존적이기 때문에 RPS 서버의 보안 수준이 시스템 전체의 보안 수준을 결정한다.

V. 모바일 RFID 시스템의 보안 및 프라이버시 요구사항

공격자는 RFID 태그와 리더 사이의 전송 값을 도청하여 공격에 사용할 수 있다. 태그와 리더 사이의 통신은 무선 주파수를 사용하기 때문에 도청 자체를 막을 수는 없지만, 값을 주고받을 때에는 반드시 암호화를 해야 한다.

RFID 태그는 리더의 질의에 대해 항상 같은 값으로 응답을 한다. 따라서 공격자는 항상 같은 값으로 응답하는 태그를 추적함으로써 소유자의 위치를 추적할 수 있다. 태그와 소유자 간의 연결성을 없애기 위해서는 태그 응답 값의 랜덤화가 가능해야 한다. 그리고 사용자는 위치 추적 방지를 위해서 작동중인 RFID 태그를 탐지할 수 있어야 하며 태그의 동작을 중지시킬 수도 있어야 한다[7].

사용자가 상품을 구매한 후에도 상품에 부착된 태그는 작동 중이다. 따라서 제 삼자가 사용자가 소지하고 있는 태그의 정보를 읽어옴으로써 사용자가 알리고 싶지 않는 정보까지도 노출이 된다. 따라서 구매 후 개인의 소유가 된 RFID 태그는 태그에 저장된 데이터에 대해 접근권한을 부여하여 프라이버시를 보호해야 한다[7].

RFID 태그는 이전 값을 저장하였다가 리더에게 재전송함으로써 정당한 태그인 척 위장할 수 있다. 그리고 이 값을 새로운 태그에 저장하면 복제된 태그가 생성된다. Rieback이 제안한 RFID 가디언(Gaurdian) 기법에서 과거에 소유했던 태그에 대한 정보를 저장함으로써 현재 태그를 소유하고 있지 않으면서도 소유하고 있는 것처럼 외부 리더를 속일 수 있었다. 이와 같은 공격을 막기 위해서는 이전 값을 재전송하지 못하도록 해야 한다.

휴대폰에 RFID 리더가 내장되면 누구나 쉽게 리더를 소지하고 태그의 정보를 수집할 수 있게 된다. 모바일 RFID 리더는 이동통신 및 무선 인터넷망과 같은 네트워크에 연결이 되어 있기 때문에 개인과 연관된 정보들에 대한 보안 및 관리가 요구된다. 그러므로 사용자가 모바일 RFID 리더를 사용하여 태그로부터 얻은 정보들이 이동통신 및 무선 인터넷망에 노출되지 않도록 수집된 정보들에 대한 보안 메커니즘이 필요하다. 그리고 모바일 RFID 시스템에 안전하고 적합한 정보통신 환경을 제공하기 위한 정보통신망법이 구체적으로 제정되어야 한다.

VI. 결론

모바일 RFID 시스템은 기존 RFID 시스템의 장점과 모바일 시스템의 장점을 모두 가졌다. 그리고 모바일 RFID 시스템은 리더가 휴대폰과 같은 모바일 단말기에 내장되며 모바일 RFID 리더를 가진 최종 소비자를 대상으로 서비스가 이루어진다. 그러나 모바일 RFID 리더를 소지하고 이동하는 사용자에 대해 개인의 프라이버시도 침해될 수 있으며, 리더의 보편화 때문에 개인 프라이버시 침해 문제가 더욱 심각해진다. 모바일 RFID 리더의 이런 문제점을 해결하기 위해 기존의 기법들이 제안되었지만 모바일 RFID 시스템에서의 보안위협을 해결하기에는 아직 충분하지 않다. 따라서 향후 각 응용 서비스 환경에 따른 보안기법들이 다양하게 연구될 필요가 있다.

[참고문헌]

[1] K.Finkenzeller, "RFID handbook", John Wiley & Sons. 1999

[2] A. Juels, P. Syverson, and D. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility", Center for High Assurance Computer Systems - CHACS 2005, LNCS 3856, pp.210-226 ,2005

[3] Hyung-Jun Kim, "모바일 RFID 표준기술 동향", TTA Journul, 2005.05

[4] Il-jung Kim, Eun-young Choi, Dong-hoon Lee, "모바일 기반의 RFID 프라이버시 보호 기법", 한국정보보호학회 동계정보보호학술대회 논문집 제 16권 제2호, pp.233-238, 2006년 12월 9일

[5] Inseop Kim, Byunggil Lee, Howon Kim , "Privacy-Friendly Mobile RFID Reader Protocol Design based on trusted Agent and PKI", CODSumer Electronics, 2006. ISCE '06. 2006 IEEE Tenth International Symposium on 28-01 June 2006 Page(s):1 - 6

[6] Soo-Cheol Kim, Sang-Soo Yeo, and Sung Kwon Kim, "MARP: Mobile Agent for RFID Privacy Protection", CARDIS 2006, LNCS 3928, pp. 300-312, 2006

[7]이홍섭, "RFID 프라이버시보호 가이드라인 해설서", 한국정보보호진흥원, 2005년 11월

[8] Hyangjin Lee, Jeeyeon Kim, "Privacy threats and issues in mobile RFID", Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on 20-22 April 2006 Page(s):5 pp.

[9] JooYoung Lee, Dooho Choi, HoWon Kim. "Practical Privacy Protection Mechanism for Networked RFID Environment", IWSEC 2006, October 2006

[10] M.Ohkubo, K.Suzuki, S.Kinoshita, "A Cryptographic Appreach to 'Privacy-Friendly' tag", RFID Privacy Workshop, Nov 2003.

[11] 박남제, "모바일 RFID 정보보호 표준화 동향 및 전망", TTA IT Standard Weekly, 2005.03

[12] M. Rieback, B. Crispo, A. Tanenbaum, "RFID Guardian: A Battery- powered Mobile Device for RFID Privacy Management", Australasian Conference on informaiton Security and Privacy - ACISP 2005, LNCS 3574, pp. 184-194, 2005