情報保護學會論文誌
第18卷 第1號, 2008. 2

Gen2 기반 RFID 시스템에 적합한 암호 기법 설계*

원 태 연†, 김 일 중, 최 은 영, 이 동 훈‡
고려대학교, 정보경영공학전문 대학원

Encryption scheme suitable to RFID Systems based on EPC Generation2*

Tae Youn Won†, Il Jung Kim, Eun Young Choi, Dong Hoon Lee‡
Graduate School of Information Management and Security, Korea University

요 약

RFID(Radio Frequency Identification) 시스템이란 태그(Tag)와 리더(Reader)가 무선주파수(Radio Frequency)를 이용하여 물리적 접촉 없이 데이터 통신이 가능한 자동 인식 시스템을 말한다. RFID 시스템은 태그에 쓰기(Re-write)가 가능하고 무선공간에서 다수의 태그를 동시에 인식 가능하다는 장점 때문에 바코드 시스템을 대체할 신기술로 주목받고 있다. 그러나 태그와 리더가 무선 주파수를 이용하여 통신하기 때문에 시스템 보안과 개인 프라이버시 침해의 문제를 발생시킨다. 이것을 해결하기 위한 많은 연구가 있었으며 그 결과 다양한 보안 기법들이 제안되었다. 하지만 제안된 많은 보안 기법들은 저가 기반의 Gen2 태그에는 적용하기 어렵다. 따라서 본 논문에서는 Gen2 기반의 RFID 시스템에 적합한 행렬(matrix)을 이용하여 암호화하는 기법을 제안한다. 그리고 RFID 장비를 사용하여 시뮬레이션을 해봄으로서 제안 기법의 효율성과 안전성을 분석하고 적용 가능한 응용 환경에 대해서 알아본다.

ABSTRACT

RFID(Radio Frequency Identification) system is an automated identification system that consists of tags and readers. They communicate with each other by RF signal. As a reader can identify many tags in contactless manner using RF signal, RFID system is expected to do a new technology to substitute a bar-code system. But RFID system creates new threats to the security and privacy of individuals, Because tags and readers communicate with each other in insecure channel using RF signal. So many people are trying to study various manners to solve privacy problems against attacks, but It is difficult to apply to RFID system based on low-cost Gen2. Therefore, We will propose a new encryption scheme using matrix based on Gen2 in RFID system in paper, and We will analyze our encryption scheme in view of the security and efficiency through a simulation and investigate application environments to use our encryption scheme.

Keywords : RFID, EPC, Gen2, Privacy Problem, Security

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템이란 식별정보를 저장하고 있는 초소형 태그(Tag)가 무선주파수(Radio Frequency)를 이용하여 리더(Reader)와 통

접수일: 2007년 8월 31일; 채택일: 2007년 11월 1일
* 본 연구는 서울시 산학연 협력사업(10665)의 지원으로 수행된 연구임
† 주저자, kucs226@korea.ac.kr
‡ 교신저자, donglee@korea.ac.kr

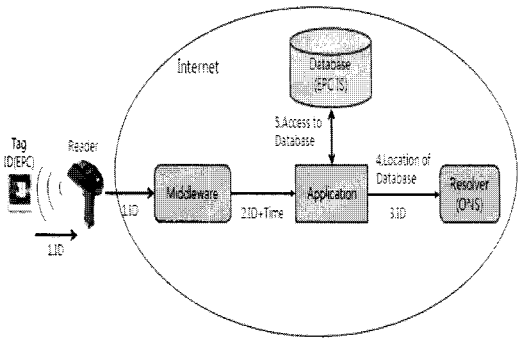
신을 함으로서 물리적 접촉 없이 데이터 송·수신이 가능한 자동 인식 시스템을 말한다. RFID 시스템은 태그에 쓰기(Re-write)가 가능하고 무선공간에서 다수의 태그를 동시에 인식 가능하다는 장점 때문에 바코드 시스템을 대체할 기술로 주목받고 있다[1]. 2006년 ISO 국제표준화 회의에서 EPCglobal에서 제안한 Class-1 Generation-2(이하 Gen2)가 UHF-RFID 규격에 기초한 ISO 18000-6의 신규타입(타입 C)으로 편입됨으로써 표준화 문제도 해결되어 RFID 산업에 활기를 불어넣고 있다.

하지만 무접촉, 비가시(Non-Line-of-Sight)라는 RFID 시스템의 장점이 시스템 보안 및 개인 프라이버시 침해 문제를 발생 시킨다. 예를 들어, 공격자는 사용자가 소지하고 있는 물건에 부착된 태그에서 리더로 전송하는 식별 정보를 도청함으로 해서 사용자가 무엇을 소지하고 있는지 알아 낼 수 있다. 또한 도청을 통한 특정 태그의 식별 정보를 알아내어 사용자의 위치를 추적할 수도 있다.

현재까지 이러한 RFID 시스템의 보안 및 프라이버시를 보호를 위한 많은 방법들이 연구되었다[8-16]. 그러나 제안된 방법들 대부분은 태그에서 암호학적 연산과 많은 저장 공간을 요구하므로[8-13] 전력, 처리 시간, 저장 공간, 게이트 수(7.5K~15K) 등의 자원적인 제약이 따르는 수동형 태그에는 사실상 적용이 불가능하다[5]. 또한 보안 및 프라이버시 문제를 완벽히 해결하지 못하는 취약성을 가지고 있다. 최근에 EPC Gen2 표준에 적합한 방법들이 활발히 연구되고 있다[14-16]. Karthikeyan et al.[14]은 XOR 연산과 행렬(matrix)만을 이용하여 태그와 리더를 인증하는 기법을 제안하였다. 하지만 이 제안 기법은 공유키를 업데이트 하기위해 리더가 태그에게 전송하는 데이터에 대하여 서비스 거부 공격을 한다면 비동기화 문제가 발생한다. 그리고 공유한 키가 업데이트되기 전에 인가되지 않은 리더의 요청에 대하여 태그는 똑같은 값으로 응답하게 되어 위치 추적 문제도 가지고 있다. 이 방법은 재전송 공격과 전방향 안전성에 대해서도 만족하지 못한다. Duc et al.[15]는 Gen2에서 제공하는 PRNG 함수와 CRC만을 사용하여 인증을 하는 기법을 제안하였다. 하지만 이 또한 서버와 태그의 공유키를 업데이트 하기위해서 리더가 태그에 전송하는 "End Session" 명령어에 대하여 서비스 거부 공격을 한다면 비동기화 문제가 발생한다. 그리고 리더에서 서버 쪽으로 전송하는 "End Session" 명령어를 공격자가 가로 챈다면 서버는 계속 이전에 공유키를 가지고 있기 때문에 태그가 리더에게 보냈던 이전 정보를 가지고 리더의 요청에 응답하는 재전송 공격을 하여 정상 태그인척 하면서 리더와 서버를 속일 수 있다. 이 제안 기법 역시 전방향 안전성을 만족하지 못하는 문제를 가지고 있다. 마지막으로 Chien and Chen[16]은 Karthikeyan et al.[14]와 Duc et al.[15]이 제안한 기법들을 향상 시킨 Gen2기반에서 보다 강력한 프라이버시 보호 기법을 발표하였다. 하지만 이 역시 두 번 연속 서비스 거부 공격을 통하여 비동기화 문제가 발생한다. 그리고 서버에서 태그와 상호 인증을 위한 많은 데이터를 소유하고 있어야 하므로 오버헤드가 크다[16]. Gen2 기반에서 제안된 방법들도[14-16] RFID 시스템의 보안 및 프라이버시 문제를 이와 같이 완벽히 해결하지 못하는 한계를 가지고 있으며 현재 Gen2 기반의 RFID 시스템에 곧바로 적용하기에도 어렵다.

따라서 본 논문에서는 암호학적 연산이 불가능 하고 저장된 값만을 단지 읽을 수만 있는 현재 Gen2 기반의 RFID 시스템에서 단지 태그의 식별 데이터에 대하여 그대로 노출될 수 있는 문제를 해결하기 위한 암호화 기법을 제한한다. 이는 태그의 식별 데이터에 대한 기밀성만을 제공함으로 객체의 위치 추적이 요구되는 제한된 RFID 응용 환경에서만 적용 가능하다. 또한 태그와 리더사이의 안전하지 못한 채널이고 리더와 서버 시스템 사이는 안전한 채널이라고 가정한다. 마지막으로 제안한 암호화 기법을 Gen2 기반 96비트 수동형 태그(Alien ALL 9440)와 RFID 리더(Alien9800) 그리고 서버컴퓨터(4.26GHz, RAM 1GB) 사용하여 시뮬레이션을 해봄으로서 실제 환경에서의 안전성과 효율성을 테스트 한다.

본 논문의 구성은 다음과 같다. 2장에서 EPC 네트워크 환경에서의 RFID 시스템을 설명하고 3장에서 RFID 시스템 보안 및 프라이버시 문제점을 소개한다. 4장에서는 행렬(matrix)을 이용하여 Gen2 기반 96비트 수동형 태그의 식별 정보를 암호화하는 기법을 제안하며 5장에서 제안한 기법을 적용하여 사용자 프라이버시를 보호할 수 있는 응용 환경을 알아본다. 마지막으로 6장에서 실제 환경에서의 시뮬레이션을 통한 효율성 및 안전성을 분석을 하고 7장에서 결론을 맺는다.



〔그림 1〕. 기본 RFID 시스템 구성도

Ⅱ. RFID 시스템 구성

Auto-ID 센터에서 제안한 기본적인 RFID 시스템은 태그를 이용한 국제표준객체코드인 EPC코드와 인터넷을 기반으로 원하는 객체의 이동 경로와 정보를 언제 어디서든지 실시간으로 파악할 수 있게 하기 위하여 개발되었다. [그림 1]처럼 기본적인 RFID 시스템은 태그(Tag), 리더(Reader), 미들웨어(Middleware), 응용 어플리케이션(Application), EPC 정보 서비스(EPC IS) 그리고 객체 이름 서비스(ONS)로 구성되어 있다[2].

2.1. 태그(Tag)

태그는 마이크로 칩과 안테나로 구성되어있다. Gen2 기반 태그는 EPC(Electronic Product Code) 표준에 따라 헤더(Header), 업체코드(Domain Manager), 객체코드(Object Class), 일련번호(Serial Number) 형식으로 식별정보를 마이크로 칩에 저장 하며 요청 명령에 따라 EPC를 리더에 전송한다.

태그는 일반적으로 전원 공급의 유무에 따라 수동형과 능동형 태그로 구분하는데 국제 표준인 Gen2 태그는 수동형 태그이다.

2.2. 리더(Reader)

리더는 RF모듈, 컨트롤 유닛, 그리고 안테나로 구성되어있다. 리더는 무선 주파수를 이용하여 태그와 통신을 하며 태그로부터 수신 받은 EPC를 미들웨어에게 전송한다.

2.3. 미들웨어(Middleware)

리더로부터 받은 EPC에 대하여 필터링 및 수집하는 실시간 제어 기능을 수행하며 처리된 데이터에 대해서는 응용 어플리케이션에 전송한다.

2.4. 응용 어플리케이션(Application)

미들웨어로부터 수신 받은 EPC를 사용하여 EPC 정보 서비스에 접근하여 관련 데이터를 얻는다. 그리고 얻은 데이터를 가공하여 사용자가 필요로 하는 서비스들을 제공한다.

2.5. EPC 정보 서비스(EPCIS, Electronic Product Code Information Service)

EPC와 관련된 과거 이동 정보 및 세부적인 데이터를 저장하고 있으면서, 응용 서비스의 요청이 있을 시 데이터를 제공한다.

2.6. 객체 이름 서비스(ONS, Object Name Service)

인터넷 환경에서의 DNS와 비슷한 기능으로 응용 어플리케이션의 요청한 특정 EPC에 대해서 관련된 데이터가 EPC 정보 서비스의 어느 위치에 저장되어 있는지 찾기 쉽게 도와주는 역할을 한다.

Ⅲ. RFID 시스템 보안 및 프라이버시 문제점

태그와 리더는 무선 공간에서 물리적 접촉 없이 무선 주파수를 이용하여 통신을 하며 태그는 리더의 요청에 따라 자신의 식별 정보를 아무런 제약이 없이 전송하게 된다. 이는 제 삼자의 RFID 시스템에 대한 공격 위협에 노출되기 쉬우며, 이로 인해 사용자 프라이버시를 침해할 수 있다.

3.1. 개인 정보 노출(Information Leakage)

EPC 구조에서의 Gen2 태그는 위에서 본거와 같이 업체 코드, 객체 코드, 일련 번호 등의 정보를 담고 있다. 공격자가 사용자가 소지한 물건의 고유 EPC를 태그로부터 도청하여 알아낸다면 업체코드 및 객체

코드 등을 보고 사용자가 무엇을 소지하고 있는지 고가의 물건은 아닌지 또는 돈을 얼마나 가지고 있는지 등의 정보를 사용자의 동의 없이 알아 낼 수 있다. 또한 공격자가 데이터베이스에 접근이 가능하다면 도청한 EPC와 관련된 데이터를 검색하여 보다 세부적인 사용자와 관련된 정보를 알아 낼 수도 있다.

3.2. 위치 추적(Location Traceability)

사용자가 태그가 부착된 상품을 소지하고 있다면 태그의 고유 식별 정보를 통하여 사용자와 연관성을 줄 수 있다. 따라서 공격자는 사용자가 소지한 특정 상품의 도청을 통하여 이동경로를 추적 할 수 있다.

3.3. 스푸핑 공격(Spoofing Attack)

공격자는 정당한 리더인 것처럼 가장하여 태그부터 고유 정보를 얻어 낸다. 그 후 공격자는 리더의 요청에 태그로부터 얻어낸 정보로 응답하여 마치 자신이 정상 태그인 척 리더를 속일 수 있다.

3.4. 재전송 공격(Replay Attack)

공격자는 도청을 통하여 태그에서 전송하는 고유 정보를 얻는다. 그 이후 리더의 요청에 대해 공격자는 정상 태그를 대신하여 자신이 이전에 도청을 통하여 얻었던 정보로 응답한다. 따라서 공격자는 정상인 태그인척 위장하여 정상 리더를 속일 수 있다.

3.5. 서비스 거부 공격(Denial of Service)

공격자는 매우 많은 수의 인가되지 않은 요청 명령을 태그에게 전송함으로 해서 정상적인 리더의 요청에 태그가 응답하지 못하도록 만들거나 또는 전파 방해 유도하는 신호를 리더에 전송하여 시스템을 방해 할 수 있다. 따라서 RFID 시스템이 제대로 작동하지 못하는 일이 발생 할 수 있다.

Ⅳ. 행렬(MATRIX)를 이용한 암호화 기법

본 절에서는 현재 RFID 기술 안에서 적용 가능한 태그에 저장된 데이터가 그대로 노출되어 정보가 유출되는 것을 해결할 수 있는 암호화 기법을 제안한다. 이 제안 기법은 태그의 응답이 고정되어 있으므로 물류, 유통과 같이 화물의 위치 추적이 필요로 되는 제한된 응용 환경에서만 적용 가능하다. 과정은 등록 과정과 식별 과정으로 나뉜다. 등록 과정은 태그가 부착된 객체를 발급하기 전에 관리 기관에서 행렬(matrix)을 이용하여 식별 번호를 암호화 하고 태그에 저장하는 과정이다. 식별 과정은 리더로부터 수신 받은 암호화된 데이터에 대하여 관리 기관에서 행렬(matrix)을 이용하여 복호화 하고 서비스를 제공하는 과정이다.

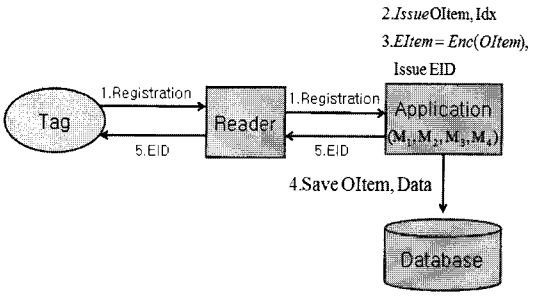
4.1. 용어 정의

[표 1]은 제안한 암호화 기법에서 사용하는 용어들의 정의이다.

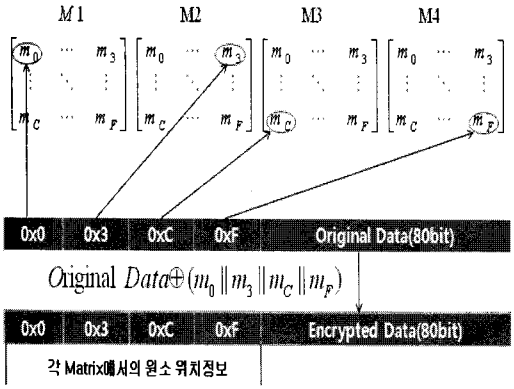
4.2. 등록 과정[그림 2]

〔표 1〕. 표기법

표기법	내용
OID	원본 식별 데이터
EID	암호화된 식별 데이터
OItem	원본 객체 데이터(80비트)
EItem	암호화된 객체 데이터(80비트)
M_i	4×4 행렬
m_i	16비트 난수
Enc	암호화 함수
Idx	Mi에서의 원소(mi)의 위치정보(16비트)
Dec	복호화 함수
⊕	Exclusive-OR
‖	Concatenation



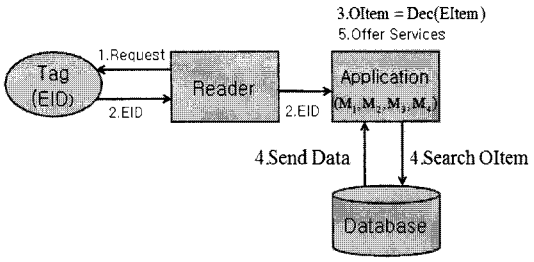
〔그림 2〕. 등록 과정



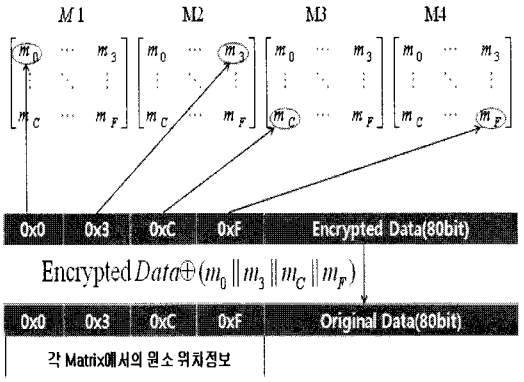
〔그림 3〕. 암호화 과정

1. 객체에 부착될 태그는 관리 기관(Application)에 발급 요청 한다.
2. 관리기관은 각각의 태그에게 유일한(Unique) 80비트 원본 객체 데이터 OItem과 16비트의 Index 정보 Idx를 생성한다. Idx는 암호화 시 키로 사용하게 될 4개의 행렬(M_1,M_2,M_3,M_4)에서의 원소 위치를 나타낸다, 4비트씩 나누어 16진수로 표현한다[그림 3].
3. 관리기관은 OItem(80비트)를 암호화 할 때 사용할 4개의 4×4 행렬(M_1,M_2,M_3,M_4)들을 사전에 미리 생성하여 저장한다. 각 행렬의 원소들은 20비트의 난수이며 서로 다른 값으로 구성되어 있다[그림 3].
   [그림 3]에서와 같이 생성한 4개의 16진수의 값 Idx를 사용하여 각각의 행렬(M_1,M_2,M_3,M_4)에서 20비트 난수 4개를 추출한 후 접합(Concatenation)을 통하여 80비트의 행렬키(matrix Key)를 생성한다. 그 다음에 80비트 행렬키(matrix Key)와 OItem(80비트)에 대하여 XOR 연산을 수행하여 암호화된 새로운 객체 데이터 EItem을 생성한다. 그리고 암호화 할 때 사용 하였던 Idx와 함께 새로운 암호화된 식별 데이터 EID를 생성 한다.
4. EID 생성 후 OItem과 객체와 관련된 정보(Data)를 데이터베이스에 저장한다.
5. 96비트 EID를 Gen2 태그에 저장하고 객체에 부착하여 발급한다.

4.3. 식별 과정 [그림 4]

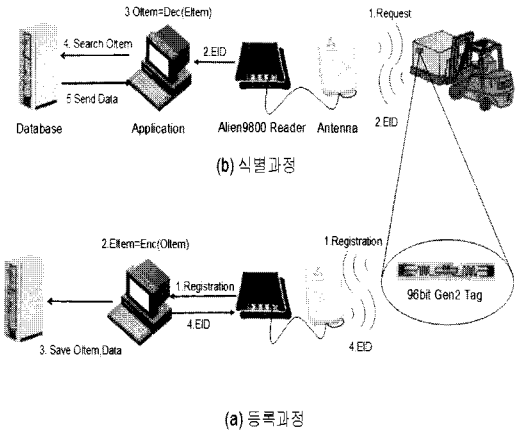


〔그림 4〕. 식별 과정



〔그림 5〕. 복호화 과정

1. 리더는 객체에 부착된 태그에게 EID 전송 명령을 한다.
2. 태그는 이에 대한 응답으로 EID를 리더에게 전송하고 리더는 이를 수신하여 관리 기관(Application)에 전송된다.
3. [그림 5]에서와 같이 관리 기관은 EID의 앞 16비트 Index 정보(Idx)를 사용하여 암호화 과정에서와 같이 4개의 행렬(M_1,M_2,M_3,M_4)에서의 20비트 원소들을 추출한다. 이렇게 4개의 행렬에서 추출된 20비트 길이의 4개의 원소들을 접합(Concatenation)하여 80비트의 행렬키를 생성하고 80비트의 암호화된 객체 데이터(EItem)와 XOR 연산을 통하여 원래의 원본 객체 데이터(OItem)로 복호화 한다.
4. 복호화 한 OItem과 데이터베이스에 저장되어 있는 원본 객체 데이터가 일치 하는지 여부를 확인한다.
5. 같다면 태그를 인증하고 관리 기관은 서비스를 제공한다.



〔그림 6〕. 본 기법의 응용 환경(물류, 유통)

V. 응용 환경[그림 6]

RFID 시스템은 항공 화물이나 항공 수하물, 택배 분야와 같은 물류, 유통분야에서 물품 추적, 출하 작업의 효율화, 환승시간의 단축이나 오배송의 방지 등에 활용되고 있다. 하지만 태그에 저장된 물품의 식별 정보가 도청을 통하여 공격자에게 그대로 노출되기 때문에, 공격자는 물품이 무엇인지 쉽게 알아 낼 수 있다. 만약 공격자가 상대 경쟁회사라면 도청을 통하여 물품의 정보를 알 수 낼 수 있다. 그리고 데이터베이스에 접근이 가능하다면 도청한 물품의 식별 정보와 일치하는 데이터를 찾아내어 물품과 관련된 보다 세부적인 정보까지 알아 낼 수 있다. 또한 물건을 구입한 사람에 대한 정보가 저장되어 있다면 보다 더 심각한 문제를 발생 시킬 수 있다. 따라서 리더의 요청에 따라 태그에서 전송하는 데이터에 대하여 암호화 하여 도청을 당하여도 공격자는 무엇인지 모르도록 하여야 한다.

이러한 점에서 우리가 제안한 기법을 물류, 유통 분야에 적용시킬 수 있다. 위의 [그림 6]에서와 같이 태그가 물품에 부착되어 배송되기 전에 (a)등록 과정을 통하여 고유 식별 정보를 암호하고 태그에 저장하는 과정을 거친다. 이를 통해 공격자가 도청을 통하여 태그의 고유 정보를 알아내더라도 암호화된 식별 정보이기 때문에 상품의 정보를 알아내는 것은 불가능하다. 그리고 (b)식별과정을 통하여 복호화가 정상적으로 완료된 물품에 대해서만 서비스를 받을 수 있기 때문에 정상적인 식별 과정을 거치지 않은 공격자는 암호화된 데이터를 가지고 데이터베이스에 접근하더라도 원본 식별 정보를 알 수가 없어 관련된 세부적인 정보를 검색하는 것을 불가능하다. 따라서 우리가 제안한 기법은 물류, 유통분야에서 물품의 식별데이터를 암호화 하는데 효율적으로 사용될 수 있다.

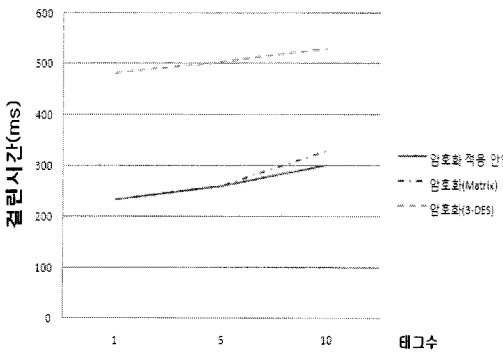
VI. 제안한 기법의 안정성과 효율성

본 절에서는 본 기법을 적용 하였을 때의 효율성과 안전성을 테스트 하였다. Gen2 기반 96비트 태그(Alien ALL 9440)와 리더(Alien 9800) 그리고 관리 기관으로서 서버컴퓨터(4.26GHz, RAM 1GB)로 구성된 실제 환경에서 테스트 하였다.

6.1. 효율성

효율성 테스트는 사전 등록과정을 통하여 암호화 하지 않은 태그, 행렬(matrix)로 암호화된 태그, 그리고 3-DES로 암호화된 태그를 각각 10개씩 만든다. 그리고 식별과정에서 암호화 하지 않았을 때의 데이터가 식별되었을 때까지의 걸린 시간, 행렬(matrix)로 암호화된 데이터를 복호화 하여 식별 되었을 때까지의 걸린 시간 그리고 3-DES로 암호화된 데이터를 복호화 하여 식별되었을 때까지의 걸린 시간을 측정하고 서로의 걸린 시간을 비교하였다.

[그림 7]에서 보듯이 행렬(matrix)를 이용한 방법은 암호화 하지 않았을 때와 측정 시간에서 큰 차이가 나지 않는다. 반면에 3-DES를 이용한 암호화 기법에 비해서는 걸린 시간이 크게 단축되는 것을 볼 수 가 있다. 이는 물류, 유통과 같이 한 번에 많은 수의 태그를 인식



〔그림 7〕. 태그 복호화 시뮬레이션 결과

하여 처리해야 할 때 각각의 객체에 대한 식별정보를 암호화하여 정보의 유출은 막으면서 동시에 많은 수의 태그를 식별할 수 있는 효율적인 방법이라고 할 수 있다.

6.2. 안전성

제안 기법은 원래의 객체 식별 데이터(OItem)를 행렬키(matrix key)를 사용하여 암호화 하고 이를 태그에 저장하여 발급하는 등록과정을 관리기관에서 거치게 된다. 따라서 공격자가 태그와 리더사이에서 도청을 통하여 암호화된 데이터(EID)를 알아내더라도 원래의 객체 식별 데이터(OItem)는 알 수 없으므로 물품의 내용이 무엇인지 알기가 어렵다. 이는 원래의 객체 식별 데이터(OItem)에 대하여 기밀성(Confidentiality)을 보장한다.

그리고 공격자가 태그와 리더사이를 도청하여 암호화된 데이터를 알아냈다 할지라도 복호화를 위해 알아야 하는 행렬(matrix)들은 관리기관을 통하여 안전하게 보관되어 있기 때문에 행렬키(matrix key)를 알 수가 없다. 그러나 만약 동일한 키를 사용하여 생성된 암호문이 존재 한다면 공격자가 4개의 인덱스 키 중 같은 인덱스 정보를 가지고 있는 태그들의 값을 도청하여 Partial Decryption이 가능할 수도 있다. 예를 들어 A의 암호화 시 사용한 인덱스 정보(Idx_{A1}, Idx_{A2}, Idx_{A3}, Idx_{A4})와 태그 B의 암호화 시 사용한 인덱스 정보(Idx_{B1}, Idx_{B2}, Idx_{B3}, Idx_{B4})가 하나만 틀리더라도 하나의 블록키(m_i)는 20비트이므로 2^{20}의 경우의 수가 존재하여 부분적으로 복호화가 될 지라도 그 부분 이외의 다른 부분들에 대해 알 수 없으므로 완전한 원본 식별 데이터를 복원해 낼 수 없어 안전하다고 할 수 있다. 그리고 인덱스 정보가 모두 같더라도 공격자는 도청하여 얻은 EID_A와 EID_B로부터 OID_A와 OID_B를 알아내기란 힘들다.

따라서 공격자는 원래의 식별 정보를 알아 낼 수 없기 때문에 공격자가 데이터베이스에 접근하더라도 물품과 관련된 보다 상세한 내용과 구입한 사용자의 자세한 정보를 알아내는 것은 불가능하다.

Ⅶ. 결 론

본 논문에서는 행렬(matrix)을 이용하여 태그의 식별 정보를 암, 복호화 하는 기법을 제안하고 물류, 유통 같은 응용 환경에서 적용 가능함을 보였다. 또한 실제 RFID 장비를 이용하여 효율성과 안전성을 테스트하였다. 등록 과정을 통하여 태그의 식별 정보를 암호화하고 태그에 저장함으로 해서 도청이 가능한 무선 공간에서 원래의 식별 정보가 그래도 노출되는 문제를 해결하였다. 이는 기밀성을 제공하며 정보 노출을 막는다. 그리고 관리기관에서 행렬(matrix)을 이용한 단 한번의 XOR 연산으로 복호화 하므로 연산량이 많지 않아 효율적인 것을 볼 수 있었다. 따라서 본 논문에서 제한한 기법은 출하 작업의 효율화 및 화물 추적과 같은 기능을 가지면서 화물의 정보를 보호해야하는 물류, 유통 등의 RFID 산업에서 사용될 수 있다. 하지만 현재 RFID 기술 기반에서 본 기법을 제안하였기 때문에 위치 추적이 가능하여 제한된 환경에서만 적용이 가능하다. 따라서 앞으로 RFID 기술의 발전에 맞추어 다양한 응용 환경에서도 적용 가능한 RFID 시스템의 보안과 프라이버시를 보호할 수 있는 방법을 연구 할 것이다.

참고문헌

[1] Damith Ranasinghe, Daniel Engels, and Peter Cole, "Low-Cost RFID Systems: Confronting Security and Privacy", Auto-ID Labs Research Workshop, 2004.

[2] Mitsuo Tsukada, "Recent Activities for RFID Standardization", NTT Technical Review, Vol. 4, No.1, pp. 56-60, 2006.

[3] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal, Vol. 24, Issue:2, pp. 381-394, 2006.

[4] Pedro Peris-Lopez, Julio Cesar Hernandez Castro, Juan M. Estevez-Tapiador, Arturo Ribagorda, "RFID Systems: A Survey on Security Threats and Proposed Solutions.", PWC2006, pp. 159-170, 2006.

[5] 박재민, Dang Nguyen Duc, Vo Duc Liem, 서영준, 김광조, "2세대 EPCglobal RFID 규격의 보안 취 약성 검토 및 개선 방안 연구", 충청지부 학술대회 논집, pp. 207-220, 2005.

[6] EPCglobal Inc., "Radio Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960MHz Version 1.0.9.

[7] Auto-ID Labs, Cambridge, UK, http://www.autoidlabs.org/Cambridge

[8] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, "Se-curity and Privacy Aspects of Low-Cost Radio Frequency Identi¯cation Systems," In Security in Pervasive Computing, 2003.

[9] Miyako Ohkubo, Koutarou Suzki and Shingo Kinoshita, "Cryptographic Approach to 'Privacyfriendly' Tags," In RFID Privacy Workshop, 2003.

[10] Dirk Henrici and Paul MÄuller, "Hash-based Enhancement of the Location Privacy for Radio-Frequency Identi¯cation Devices using Varying Identi¯ers," In PER-COMW, 2004.

[11] Keunwoo Rhee, Jin Kwak, Seungjoo Kim and Dongho Won, "Challenge-response Based RFID Authentication Protocol for Distributed Database Environment," In International Conference on Security in Pervasive Computing - SPC 2005, pp. 70-84, 2005.

[12] David Molnar and David Wagner, "Privacy and Security in Library RFID: Issues, Practices, and Architectures," In Conference on Computer and Communications Security - CCS'04, pp. 210-219, 2004.

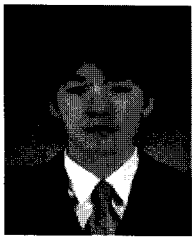
[13] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren and Kwangjo Kim, "Mutual Authentication Protocol for Low-cost RFID," In the Encrypt Workshop on RFID and Lightweight Crypto, 2005.

[14] Sindhu Karthikeyan and Mikhail Nesterenko, "RFID Security without Extensive Cryptography," In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 63-67, 2005.

[15] Dang Nguyen Duc, Jaemin Park, Hyunrok Lee and Kwangjo Kim, "Enhancing Security of EPCglobal GEN-2 RFID Tag against Traceability and Cloning," In the 2006 Symposium on Cryptography and Information Security, 2006.

[16] Hung-Yu Chien and Che-Hao Chen, "Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards," In Computer Standards & Interfaces, 2006.

〈著者紹介〉



원 태 연 (Tae Youn Won) 학생회원
2007년 2월 : 고려대학교 전산학과 졸업
2007년 3월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 정보보호, RFID 정보보호 기술, 무선 보안, 유비쿼터스

김 일 중 (Il Jung Kim) 학생회원
2005년 8월 : 고려대학교 전산학과 졸업
2005년 9월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 정보보호, RFID 정보보호 기술, 유비쿼터스

최 은 영 (Eun Young Choi) 학생회원
2001년 8월 : 고려대학교 수학과 학사
2003년 8월 : 고려대학교 정보보호대학원 공학 석사
2004년 3월~현재 : 고려대학교 정보보호대학원 박사과정
<관심분야> 암호 이론, 정보보호 이론, RFID 정보보호 기술, 유비쿼터스

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월 : 고려대학교 경제학사
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1993년 3월 ~ 1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보보호대학원 교수
<관심분야> 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술