2006년 한국산학기술학회 춘계 학술발표논문집

동적 ID 할당을 기반으로 하는 RFID 보안 프로토콜

이한권*, 유현중*, 박병수**, 조태경*
*상명대학교 정보통신공학과
**상명대학교 컴퓨터시스템공학과
e-mail:leehk0131@smu.ac.kr

RFID Security Protocol based on Dynamic ID Distribution

Han-Kwon Lee*, Hyeon-Joong Yoo*,
Byoung-Soo Park**, Tae-Kyung Cho*
*Dept of Information & Telecommunication Engineering,
**Dept of Computer System Engineering,
SangMyung University

요 약

RFID(Radio Frequency Identification) 시스템은 유비쿼터스 사회를 만들어 가기 위한 핵심 기술로서 기초기반 기술 및 사회기반 기술의 정비가 진행되어 가고 있으며, 우리나라에서도 IT839 전략의 신성장 동력의 하나로 추진되고 있다. 하지만 RFID에 대한 보안 문제로 인하여 적용 범위와 시기에 대하여 논란이 일고 있다. RFID 시스템은 정보 유출의 위험성을 내포하고 있으며, 개인의 위치 추적이나, 비접근 권한자의 위장행세 등의 사용자 프라이버시 보호에 대한 많은 문제점들을 수반한다. 본 논문에서는 리더와 태그간의 통신에서 태그 고유 ID를 사용하지 않고 리더로부터 사용할 임시 ID를 할당받아 통신을 수행함으로써 프라이버시를 보호할 수 있는 보안 프로토콜을 제안하고 있다.

1. 서 론

유비쿼터스 환경 구현에 있어 핵심적인 기술로서 주목받고 있는 RFID(Radio Frequency Identification) 시스템은 생산, 공급망관리, 재고관리 등의 분야에서 유용하게 사용되는 기술로서 산업계에서 많은 관심을 받고 있다. RFID는 바코드를 대체할 차세대 기술로 주목받고 있다. RFID를 이용함으로써 상품의 제조, 유통, 판매에 이르는 전 과정을 네트워크화, 지능화하고 이를 통해 생산 비용 절감과 효율성 향상 결과를 가져올 수 있다.

일반적으로 RFID 시스템은 식별정보(ID)를 저장하는 Tag, Tag 판독기능을 수행하는 리더, 호스트 컴퓨터와 응용프로그램으로 구성되는 애플리케이션 등 크게 세부분으로 구성되며, RFID Tag에 특정 전파를 노출시키면 RFID는 자신의 정보를 담고 있는 전파 신호를 방출하여 그 신호를 재수신하는 원리로 작동이 된다. 바코드에 비해서 저장능력이 뛰어나며 비접촉식이므로 리더와의 시야확보를 고려할 필요도 없으며 인식 속도가 빨라 물류시스템에서 바코드를 대체할 인식 시스템으로 많은 연구가 진행되고 있다.

하지만, RFID가 향후 국가 기간사업을 떠받치는 기반 및 생활 속의 IT 인프라로 자리 잡기 위해서는 정보보안 및 프라이버시 보호 문제를 극복해야 한다. 바코드에 비하여 편리성은 향상되었지만 태그의 정보를 누구든지 항상 읽을 수 있다는 점 때문에 정당하지 않은 사용자로부터 불법적인 접근이 가능하다.

따라서, 본 논문에서는 사용자 프라이버시를 보호할 수 있는 RFID 보안 프로토콜을 제안한다. 제안하는 프로토콜에서는 리더와 태그간의 통신에서 태그의 ID를 사용하지 않고 리더로부터 전송받은 임시 ID를 사용함으로써 보안 위협으로부터 안전성을 보

장 받을 수 있다.

2. 선행연구

RFID 시스템은 하드웨어적인 제약 사항으로 인해 보안상의 위협 요소들이 심각하게 많다. 이에 RFID 시스템의 환경에 대해 이해하고 적합한 해결책을 마련하는 것이 시급한 실정이다. 이에 따라 많은 관련 분야의 연구가 진행되고 있고, 그 대표적인 보안 프로토콜은 표 1과 같다.

표 1. RFID 시스템의 정보보호 기법 [1],[2]

보호 기법	내용
Kill 명령어	- Kill 명령을 사용해 정보를 소실하도록 하는 방법
Hash Lock	- 저장된 ID를 보호하기 위하여 해쉬함수로 metaID=H(ID)를 만들어 전송 - ID는 보호할 수 있으나 위치 추적 문제 발생
Randomized Hash Lock	- 여러개의 해쉬 값을 사용하여 전송 - 모든 태그에 대한 해쉬값을 계산해야 하기 때문에 서버/리더기의 계산량이 많아 부담
Hash Chain	- 해쉬를 반복 적용한 값을 계속 태그에 저장하고 다른 해쉬를 적용한 값을 리더기에 전달하는 방식 - Forward security를 주는 안전한 기법이나 태그의 계수에 비례하여 DB 연산 증가
Reencryption	- 공개키 암호를 이용하는 기법으로 유로화 지폐에 적용할 목적으로 개발 - 복잡한 프로토콜을 사용하여 통신 오류에 대한 대책이 미흡
Pseudonym Rotation	- ID의 노출을 막기 위하여 다수의 pseudonym을 사용하는 방식 - XOR 연산을 이용하여 이를 매번 갱신하는 기법이 제안되었으나 계산량이 많고 정확한 security의 설정에 어려움이 있음
HB+	- 1비트 인증을 반복하는 방식인 HB를 개선한 프로토콜 - 다수의 태그를 사용하는 환경에 적용하기에는 무리가 있음

3. 제안 프로토콜

현재 유통물류에 사용하기 위한 RFID 국제표준인 ISO 18000의 Part 6는 Type A, B, C로 구분되는데, 이 중에서 Type C가 EPCglobal의 Class 1 Generation 2를 통합한 규격이다. 이 규격에서는 Kill 명령을 기본적으로 내장하고 있지만, 일반적인 태그 접근에서도 난수에 기반한 접근 방법을 사용하고 있다. 아래 그림 1에서 볼 수 있듯이 ②에서 태그가 RN16이라는 난수를 생성하여 리더로 보내고, 리더는 이 난수를 가지고 태그를 식별하여 ACK 신호를 보내면, 방금 전에 그 난수를 보낸 태그만 자신의 코드를 응답하고 다시 리더가 Req_RN 명령으로 난수를 보내면 맞는 태그만이 새로운 난수(handle)를 생성하여 응답한다. 이후 리더는 이 handle을 가지고 태그의 메모리 영역에 접근하게 된다[3][4].

그림 1에서와 같이 새롭게 표준화된 ISO의 18000-6 Type C에서는 충돌 중재 과정에서 태그 ID 대신에 난수를 사용하고, Kill 명령어와 Access password를 추가하는 등의 보안에 대한 부분을 표준에서 정의하고 있다.

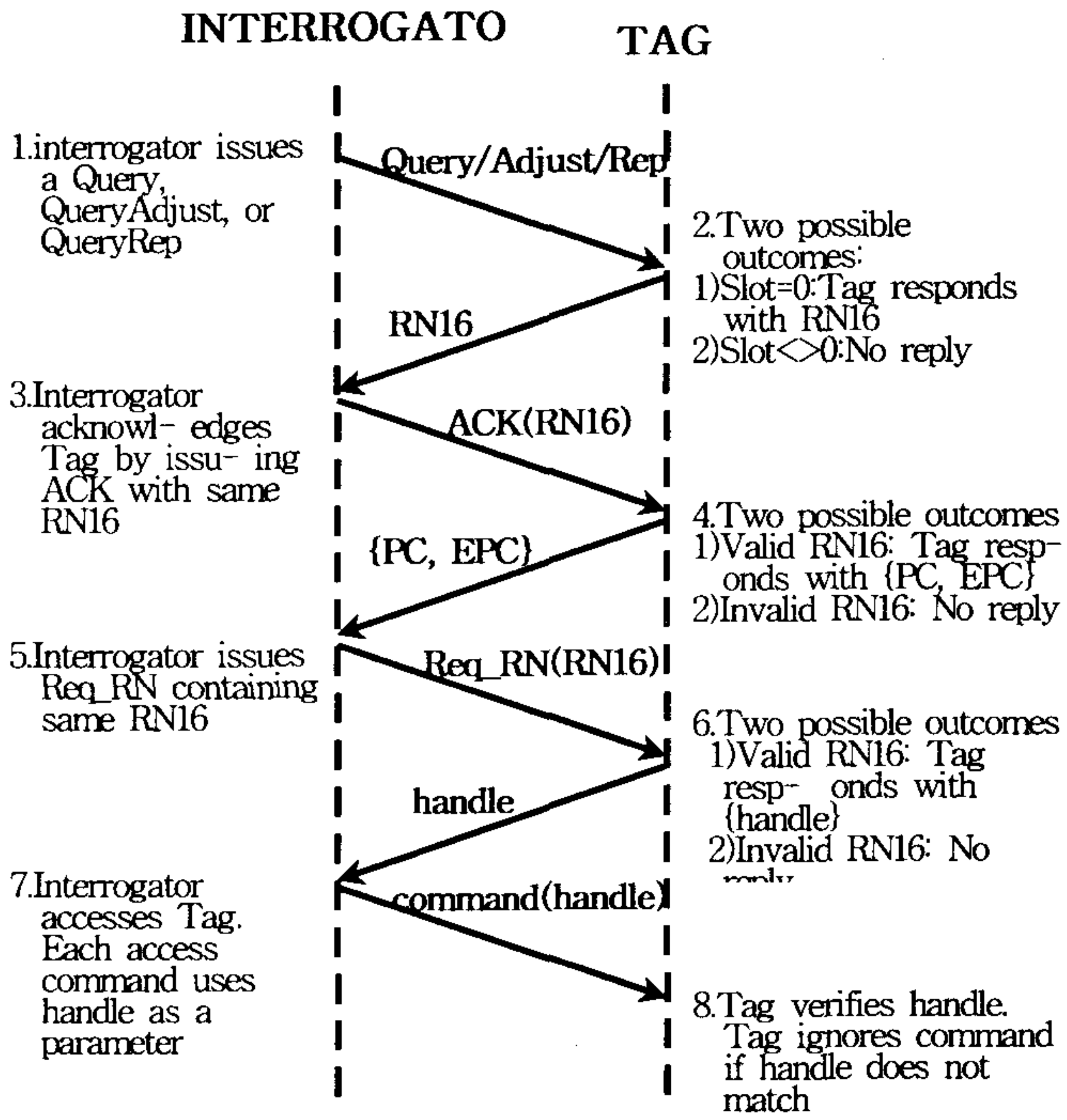

그림 1. RFID 리더와 태그간의 충돌 중재 및 접근 과정

하지만, 선택된 태그로부터 리더로의 전송되는 데이터에는 EPC code와 같은 태그의 정보를 나타내주는 데이터들이 있기 때문에 허가받지 않은 리더의 도청으로 인한 위치추적 및 복제와 같은 문제점이 발생할 수 있다.

따라서 본 논문에서는 이러한 문제점을 해결할 수 있는 리더와 태그간의 안전한 프로토콜을 제안한다. 리더와 태그간에 데이터 전송시 태그는 리더에게 서로간에 통신에 사용할 임시 ID를 부여받고, 부여받은 임시 ID를 이용하여 리더와 통신함으로써 위치추적 등의 보안 문제를 해결할 수 있다.

3.1 사전준비단계

인증단계에 앞서 태그와 리더 및 백엔드 서버는

인증에 필요한 여러 가지 정보들을 저장해 둔다. 그림 2에서와 같이 태그는 사용되기 전에 발급자가 미리 보안에 사용할 키들과 그 키를 나타내는 키 인덱스를 태그에 저장하며, 백엔드 서버의 데이터베이스에도 동일한 키들과 그 인덱스를 저장하여 둔다. 이때 키의 개수는 n<m으로 DB는 많은 수의 키들을 준비한다. 또한 서버는 태그에 할당할 ID들을 미리 준비하여 둔다. 태그는 자신의 고유 ID와 동적 ID를 따로 저장하고 있으며, 모드에 따라 고정 ID를 사용하거나 동적 ID를 사용하게 된다.

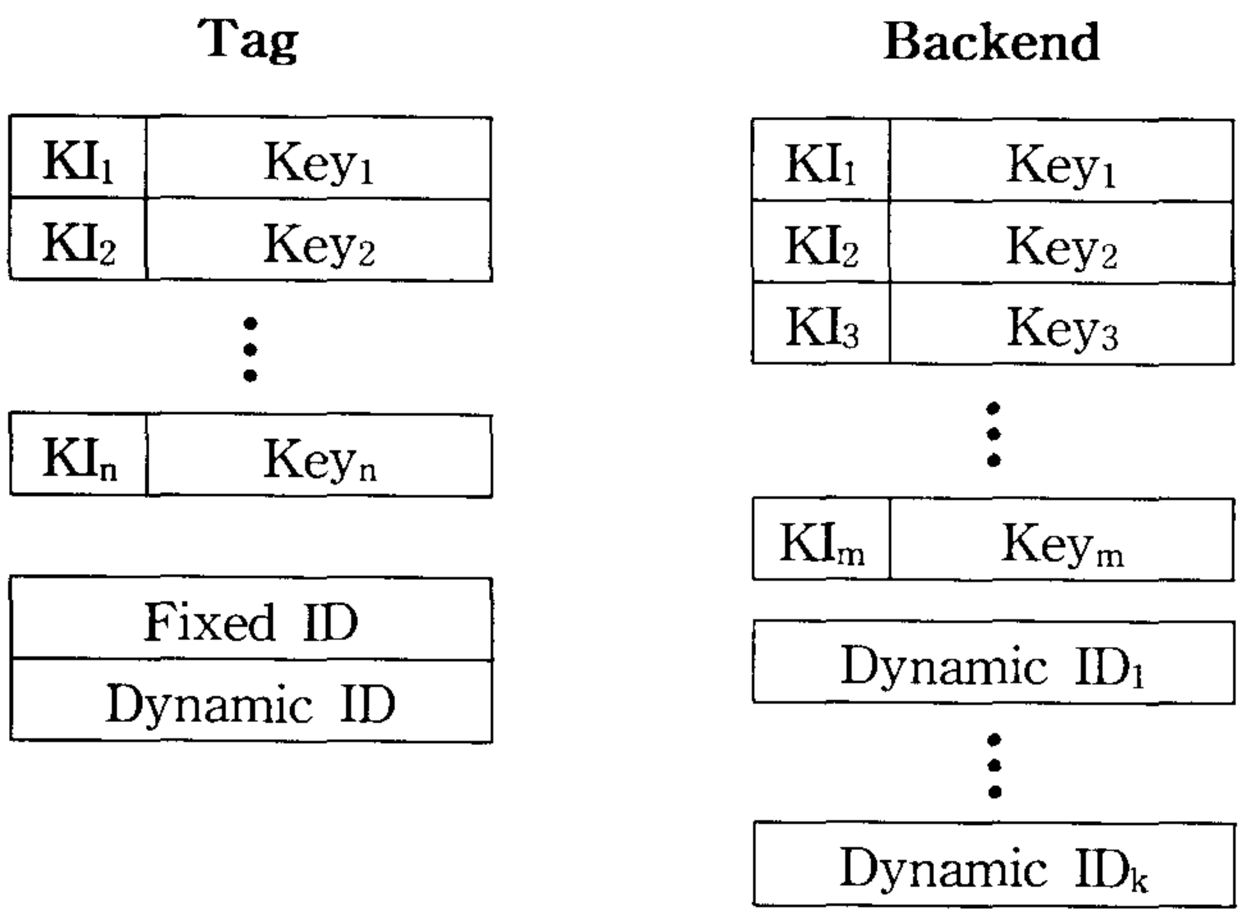

그림 2. 태그 및 백엔드 저장 정보

3.2 인증단계

사전 준비단계에서 부여된 비밀키와 난수 발생기를 이용하여 태그에 대한 리더의 인증과정을 거치며 데이터 전송에 사용될 동적 ID를 할당 받는다. 그림 3에서 프로토콜의 동작 흐름을 나타내고 있다.

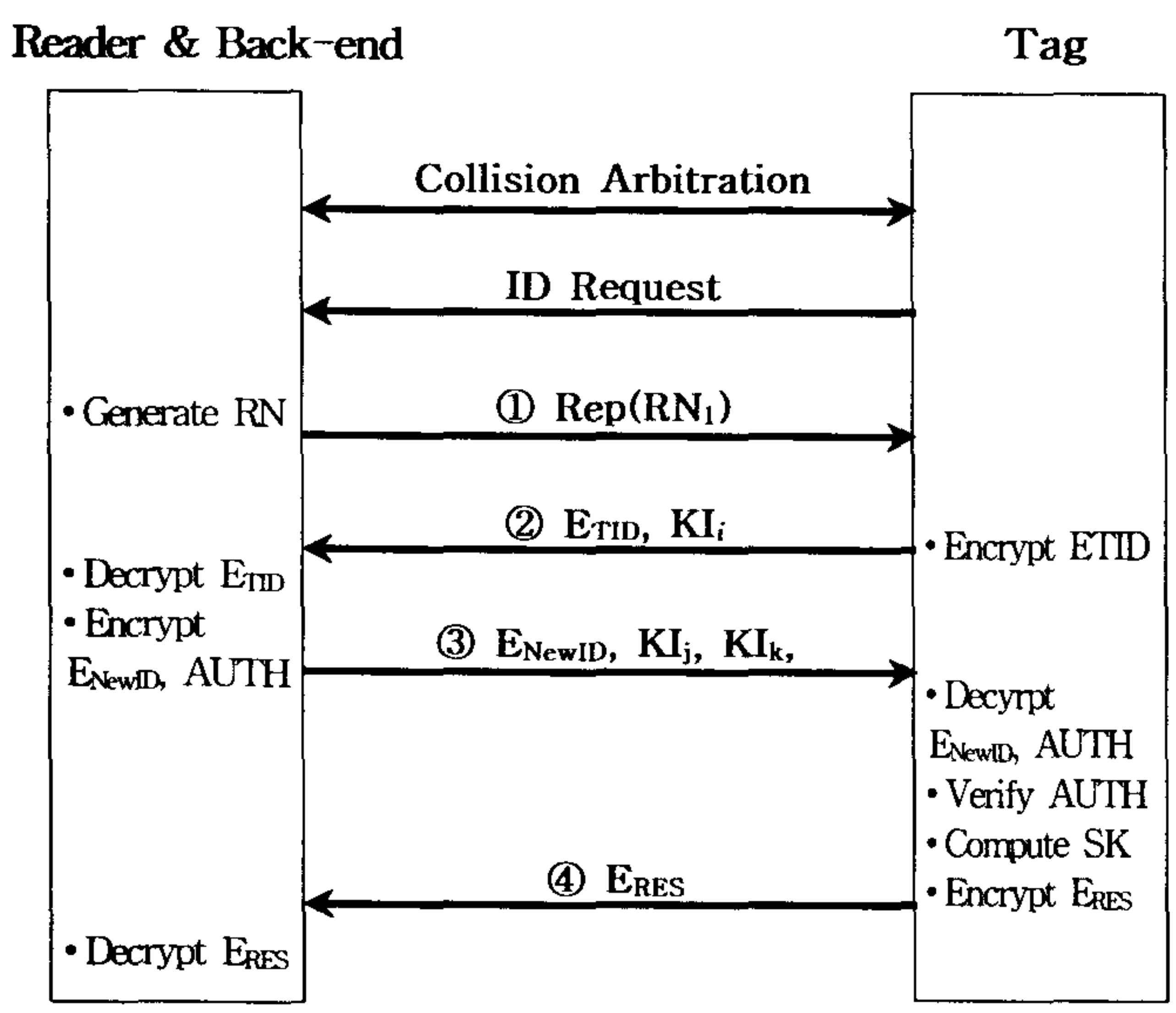

그림 3. 인증 프로토콜

① 태그로부터 ID 요청을 받은 리더는 난수를 생성하고 태그에게 전송한다.

② 태그는 전송받은 난수 RN_1과 태그의 ID를 XOR 계산하고 태그가 가지고 있는 키를 이용하여 E_{TID}를 계산하고, 사용된 키값에 해당하는 키 인덱스 KI_i를 리더에게 전송한다.

$$E_{TID} = E_{Ki}(TID \ xor \ RN_1)$$

③ 리더는 E_{TID}를 복호하여 TID를 통해 태그가 가지고 있는 키를 알 수 있다. 태그가 가지고 있는 키 중 임의로 한 개를 선택하여 태그가 사용하게 될 ID를 암호화한다. 그리고 다른 한 개의 키를 사용하여 인증 값 $AUTH$를 생성한 후, 사용한 키에 해당하는 두 개의 키 인덱스와 함께 태그에 전송한다.

$$E_{NewID} = E_{Kj}(TID \ xor \ NewID)$$
$$AUTH = E_{Kk}(NewID \ xor \ K_j)$$

④ 태그는 전송받은 E_{NewID}, $AUTH$를 복호화하고 TID와 XOR을 거친 후 새로운 ID를 할당받게 된다. $NewID$를 이용하여 인증 값 $AUTH$를 계산하여 동일한 인증값을 가지면 자신의 메모리 영역에 $NewID$를 저장하게 된다. 성공적으로 저장이 완료되면 태그는 두 개의 키 K_j, K_k를 이용하여 세션 키 SK를 이용하여 E_{RES}를 생성하고 전송한다. 리더에서는 E_{RES}를 복호화하여 자신이 전송한 New_ID와 동일할 경우 ID 정보를 백엔드에 저장하고 인증과정을 종료한다.

$$SK = (K_j \ xor \ K_k)$$
$$E_{RES} = E_{SK}(RN_1 \ xor \ New\_ID)$$

본 논문에서는 RFID 시스템의 하드웨어 자원의 제약 사항을 고려해 RC5와 같이 하드웨어적으로 구현하기 쉽고 그 적용 가능성이 높은 암호 알고리즘을 적용한다.

제안한 RFID 보안 프로토콜은 도청 및 위치 추적 등에 대한 안전성을 갖는다. 태그와 리더간에 전송되는 것은 난수 RN과 키 인덱스(KI), 암호화된 ID(E_{TID}, E_{NewID}) 이므로 암호화된 ID를 해독하기에 충분한 데이터를 수집할 수 없다. 그리고 이 프로토콜이 수행하는 동안에는 태그의 ID를 암호화 하여 전송하고 태그의 ID와 부여된 ID의 상관관계는 백엔드만이 알고 있기 때문에 위치 추적 공격으로부터도 안전하다. 또한 본 프로토콜에서는 상호 인증을 기반으로 하고 있기 때문에 상대방과 동일한 키를 가지고 있지 않고서는 상대방을 속일 수 없으므로,

스푸핑 공격이나 재생 공격으로부터도 안전하다.

4. 결 론

RFID 시스템은 공급망 관리를 시작으로 생산, 재고관리 분야는 물론 다양한 산업 전반에서 관심을 받고 있다. RFID는 바코드를 점차 대체하고, 나아가 유비쿼터스 환경을 조성하기 위한 기반으로 그 발전이 예상되고 있다. 하지만 보안 문제와 프라이버시 보호에 대하여 해결해야할 문제를 가지고 있다. 현재 프라이버시 보호를 위한 많은 연구들이 진행중이지만 아직은 실제 적용 가능한 연구 결과들이 미흡한 실정이다.

본 논문에서는 이러한 연구의 일환으로 리더로부터 동적으로 태그의 ID를 할당받아 리더와 태그간에 통신에서 가변적인 ID를 사용함으로써 여러 가지 보안위협으로부터 안전한 인증 프로토콜을 제안하였다. 제안한 프로토콜은 프라이버시 보호 측면에서는 그 안전성이 입증되었지만 태그가 많은 양의 계산을 한다는 문제점을 가지고 있다. 향후 저가형 태그 구현을 위해서는 암호화 강도를 유지하면서 태그의 계산량이나 메모리 용량을 줄일 수 있는 연구가 계속되어야 할 것이다.

참고문헌

[1] 최은영, 이동훈, "RFID 정보보호 기술 동향," 정보처리학회지 제12권 5호, 2005.

[2] A. Juels, "RFID Security and Privacy: A Research Survey," to appear at IEEE Journal on Selected Areas in Communication, 2006.

[3] ISO/IEC 1800-6, "Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz", International Standard, ISO, 2005.

[4] EPCglobal, "EPC^{TM} Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9", 2005.

[5] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A Cryptographic Approach to "Privacy-Frendly" Tag," RFID Privacy Workshop, 2003.

[6] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Springer, In Conference of Cryptographic Hardware and Embeded Systems 2004 Proceedings, pp. 357-370, 2004.

[7] 박진성, 최명렬, "고기능 RFID 태그를 위한 보안 프로토콜," 대한전기학회 전기학회논문지 54P권 4호, pp.217-223, 2005. 12.