한국산학기술학회논문지
Vol. 7, No. 6, pp. 1155-1159, 2006

난수 기반의 ID 할당을 이용한 프라이버시 보호 RFID 시스템

박진성[1*], 최명렬[2]

A Privacy Protection RFID System using Random basis ID Allocating

Jin-Sung Park[1*] and Myung-Ryul Choi[2]

요 약 본 논문에서는 난수 기반의 ID를 동적으로 RFID 태그에 부여함으로써 태그의 ID 추적으로 인해 태그 소유자의 프라이버시가 침해당할 소지를 제거할 수 있는 RFID 시스템을 제안한다. 현재 RFID 시스템의 취약한 문제점으로 사생활 침해의 문제가 대두되고 있다. 이는 RFID 태그에 저장되는 ID를 추적함으로써 발생하고 있으며 본 논문에서는 이러한 문제점을 방지하기 위해 태그에 난수 기반의 ID를 필요할 때마다 동적으로 할당함으로써 ID 추적이 불가능한 RFID 시스템을 제안한다. 이러한 시스템은 대형 할인매장에서 손님들에게 태그를 나누어 주고 프라이버시를 보호하면서 그 이동 경로를 추적하여 고객정보를 축적하는 RFID 시스템에 적용할 수 있다.

Abstract In this paper, we have proposed a privacy protection RFID system using random number based ID allocation. Currently, there are rising issues about privacy violation in RFID system. This issues caused by tracking the ID of tag which present unique identity of tag. The proposed system dynamically allocates random basis ID to tag, then the tag can not be traced. The random ID allocation procedures of this system can be operate in cryptographic mode or normal(non-cryptographic) mode. This system can be applied to privacy protected customer tracking RFID system in mega-outlet stores which tracing customer's moving path.

Key words : Security, Privacy, RFID, Random ID

1. 서 론

근래 들어 RFID 시스템은 공급망 관리, 생산, 재고관리 분야는 물론 모바일, 근태관리, 주차장 관리 등 다양한 산업 전반에서 관심을 받고 있다. 현재 유통물류 분야에서는 바코드를 대체한다는 전제를 바탕으로 작고 값싼 태그에 대한 집중적인 연구가 진행되고 있으며 그에 따른 보안 문제와 프라이버시 보호 또한 해결해야할 문제이다[1]. 저가형 RFID 태그의 경우 단일의 고정된 ID를 저장하고 있기 때문에 이를 도청하면 위치 추적과 이동 경로를 파악할 수 있어 개인의 사생활 침해가 가능하며, 위조된 ID를 구별할 수 없는 등의 보안 문제가 그 대표적인 예이다[2]. 이러한 문제를 해결하기 위해 다양한 보안방식이 연구되고 있으나, 모두 저가형 RFID 태그를 목표하고 있어 그 구현과 보안성에 상당한 제약이 따른다. 그러나 이러한 보안 문제는 약간의 추가 기능을 보강한 RFID 태그를 사용하여 해결될 수 있는 문제이다[3]. 본 논문에서는 간단한 추가 기능을 탑재한 RFID 태그와 그에 적합한 난수 기반의 동적 ID 할당을 이용하여 프라이버시를 보호할 수 있는 RFID 시스템을 제안한다. 이 시스템은 고정된 ID 때문에 발생하는 보안 문제를 해결하기 위해 필요시마다 난수 기반의 새로운 ID를 태그에 부여하고 서버는 부여된 새 ID를 통해 태그를 인식하게 하면 설령 공격자가 ID를 추적한다 하더라도 태그의 이전 ID와 새로 부여된 ID간의 상관관계를 알 수 없기 때문에 위치 파악이 불가능하다.

[1](주)씨이엔
[2]한양대학교 전자컴퓨터공학부
*교신저자: 박진성(asicman7@yahoo.ac.kr)

2. 난수 기반 ID 할당 프로토콜

2.1 준비 단계

그림 1과 같이 태그는 사용되기 전에 자신의 고유 ID(태그 ID)를 가지고 있으며, 랜덤 ID를 저장할 공간, 그리고 리더기의 호출에 응답할 때 랜덤 ID(Random ID)를 사용할지 태그 ID를 사용할지를 나타내는 랜덤 ID 사용 플래그(Random ID Flag)를 저장한다. 일반적인 동작에서는 태그 ID를 이용하여 리더와 통신하지만, 프라이버시 보호가 필요한 환경에서는 랜덤 ID를 부여받아 저장하고 랜덤 ID 사용 플래그를 설정하여 랜덤 ID를 사용하게 된다.

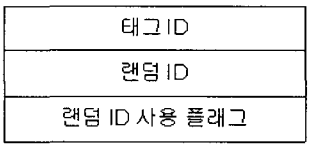

그림 1. 태그 메모리의 구성

2.2 랜덤 ID 할당 단계

그림 2에 랜덤 ID 할당 프로토콜에 대한 흐름도가 나타나 있다. 랜덤 ID의 할당은 프라이버시 보호가 필요한 환경에 들어가는 입구에서 수행될 수 있으며 리더가 태그를 감지하고 랜덤 ID를 부여하는 과정이다.

① 리더는 프라이버시 보호 영역에 진입하는 태그를 인식하기 위해 전파를 발신한다.
② 이 전파 영역에 진입한 태그는 자신의 태그 ID를 응답한다.
③ 리더는 난수 기반의 새로운 ID를 생성하여 태그에게 이 랜덤 ID를 전송한다.
④ 태그는 리더가 보내온 랜덤 ID를 자신의 랜덤 ID 메모리 영역에 저장한 후, 랜덤 ID 사용 플래그를 설정(set)하여 앞으로는 이 랜덤 ID로 응답하게 된다.

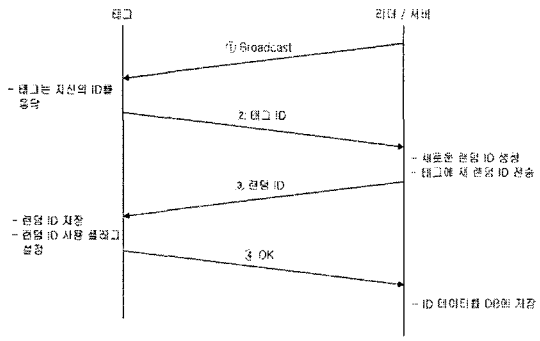

그림 2. 랜덤 ID 할당 프로토콜

2.3 랜덤 ID 사용 단계

위 2.2절의 ④ 단계에서 랜덤 ID 사용 플래그가 설정되었기 때문에 프라이버시 보호 영역에 진입한 태그는 리더의 호출에 자신의 랜덤 ID를 응답하게 된다. 이렇게 응답된 랜덤 ID는 그 보호 지역 내에서만 고유하며, 언제라도 변경될 수 있기 때문에 추적이 불가능하다.

2.4 랜덤 ID 삭제 단계

그림 3에 랜덤 ID 삭제 프로토콜에 대한 흐름도가 나타나 있다. 랜덤 ID의 삭제는 프라이버시 보호 영역에서 벗어나면서 할당받은 랜덤 ID를 지우거나 혹은 랜덤 ID 사용 플래그를 재설정(reset)하여 더 이상 태그가 랜덤 ID를 사용하지 않게 한다.

① 리더는 프라이버시 보호 영역을 벗어나는 태그를 인식하기 위해 전파를 발신한다.
② 이 전파 영역에 진입한 태그는 자신의 랜덤 ID를 응답한다.
③ 리더는 그 랜덤 ID가 더 이상 사용되지 않음을 DB에 저장하고, 모두 '0' 값으로 설정된 랜덤 ID를 전송한다.
④ 태그는 리더가 보내온 값이 '0' 인 랜덤 ID를 자신의 랜덤 ID 메모리 영역에 저장한 후, 랜덤 ID 사용 플래그를 재설정하여 앞으로는 랜덤 ID를 사용하지 않고 태그 ID로 응답하게 된다.

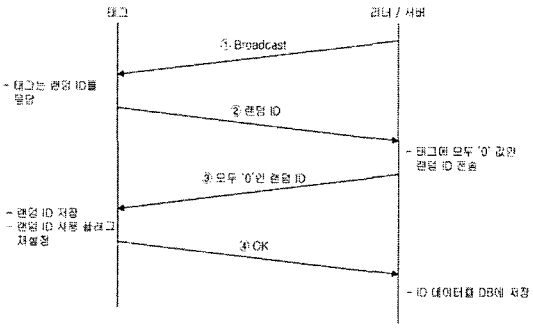

그림 3. 랜덤 ID 삭제 프로토콜

2.5 암호화된 난수 할당 프로토콜

위의 2.1절에서 2.4절에 설명된 ID 할당 방식은 할당되는 ID가 암호화되지 않은 상태에서 전송된다. 이러한 평문 상태의 ID 전송을 도청하는 경우를 방지하기 위해 암호화를 적용할 수 있다. 암호화를 적용하게 되는 경우 그림 4와 같이 다음 순서로 처리하게 된다 [3].

① 리더는 프라이버시 보호 영역에 진입하는 태그를 인식하기 위해 전파를 발신한다.

② 이 전파 영역에 진입한 태그는 난수 R을 생성하여 자신의 태그 ID와 함께 응답한다.

③ 리더는 태그의 현재 ID로부터 그 태그에 저장된 키 셋(IK1....IKn)을 알 수 있으며, 그 키 중에서 하나를 임의로 선택하여 암호화하여 EID를 생성하고, 그에 따른 인증값 M1을 생성한다. EID를 생성함에 있어 단순히 랜덤 ID만을 암호화하지 않고, 랜덤 ID와 R의 XOR 연산 결과를 암호화한 이유는, 스푸핑 공격과 재생공격을 막기 위해서이다. 계산이 끝나면, 태그로 암호화에 사용된 키의 인덱스 IK, EID와 M1을 전송한다. 여기서 E() 함수는 T-DES나 SEED와 같은 대칭형 암호화 연산이며, MAC() 함수는 E() 함수를 CBC(Cipher Block Chaining) 모드로 연산하여 그 최종 결과의 최상위 일부분만을 취하는 함수이다.

$$EID = E(ID \ xor \ R) \quad (1)$$

$$M1 = MAC(ID) \quad (2)$$

④ 태그는 IK가 지정하고 있는 키를 사용하여 전달된 EID를 복호화하고 자신이 생성한 R로 XOR 연산을 수행하여 랜덤 ID를 추출한 후 인증값을 계산하고 전송되어온 M1과 비교한다. 동일한 인증값을 가지면 자신의 랜덤 ID 메모리 영역에 이 ID를 저장한다. 성공적으로 저장이 완료되면 M2를 생성하여 리더기에 응답으로 보낸다. 여기서 | 기호는 데이터 연접 연산을 나타낸다.

$$M2 = MAC(R \mid ID) \quad (3)$$

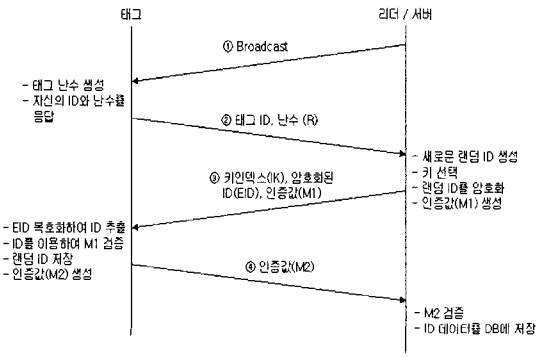

그림 4. 암호화된 랜덤 ID 할당 프로토콜

태그에 암호화된 ID 할당을 사용한 경우, 그 랜덤 ID의 삭제는 별도의 암호화된 삭제 프로토콜을 사용하지 않고 위의 2.4절 내용을 그대로 사용한다. 이는 랜덤 ID 삭제에 있어서는 데이터를 암호화할 필요가 없기 때문이다.

3. 프라이버시 보호 RFID 시스템

여기서는 위의 2장에서 설명한 랜덤 ID 할당 프로토콜을 이용하는 프라이버시 보호 RFID 시스템을 설명한다. 이러한 시스템은 사용자의 익명성과 프라이버시를 보장하면서도 사용자의 이동 경로를 추적하여 매장에 머무르는 시간, 머무르는 장소, 사용자별 동선, 구매 패턴 등을 파악하고자 하는 대형 할인매장에 적용하기 적합하며, 본 장에서도 그림 5에 나타난 대형 할인매장의 예를 들어 시스템의 동작을 설명한다.

3.1 프라이버시 보호 영역 진입

태그를 소지한 사용자가 프라이버시 보호 영역의 입구에 접근하면, 입구측 리더는 2.2절에 설명된 프로토콜에 따라 태그를 감지하고 새로운 랜덤 ID를 생성하여 태그에 부여한다. 좀 더 높은 수준의 보안이 필요하다면 2.5절에 설명된 암호화 프로토콜을 이용하여 랜덤 ID를 부여한다. 입구를 지난 태그는 새로 부여된 랜덤 ID를 호출의 응답으로 발신하게 된다.

3.2 프라이버시 보호 영역

대형 할인매장의 주요 요소에는 RFID 리더가 설치되어 태그가 지나가거나 접근하면 태그의 랜덤 ID를 읽어 관리 서버로 전송한다. 관리 서버는 그 지역의 리더에서 읽혀진 랜덤 ID를 기반으로 머무른 시간과 거쳐간 경로를 계산하게 되며, 이는 고객 관리 정보와 매장의 혼잡도 측정, 새로운 진열대 배열 등의 기초 자료로 활용할 수 있다. 더 나아가 이러한 자료를 활용하여 고객들이 모여들어 혼잡한 구역과 한산한 구역을 구별하고, 한산한 구역으로 고객을 유인하기 위해 긴급 세일을 실시하는 등의 이벤트를 통해 실시간으로 매장의 혼잡 상황을 해소할 수도 있다.

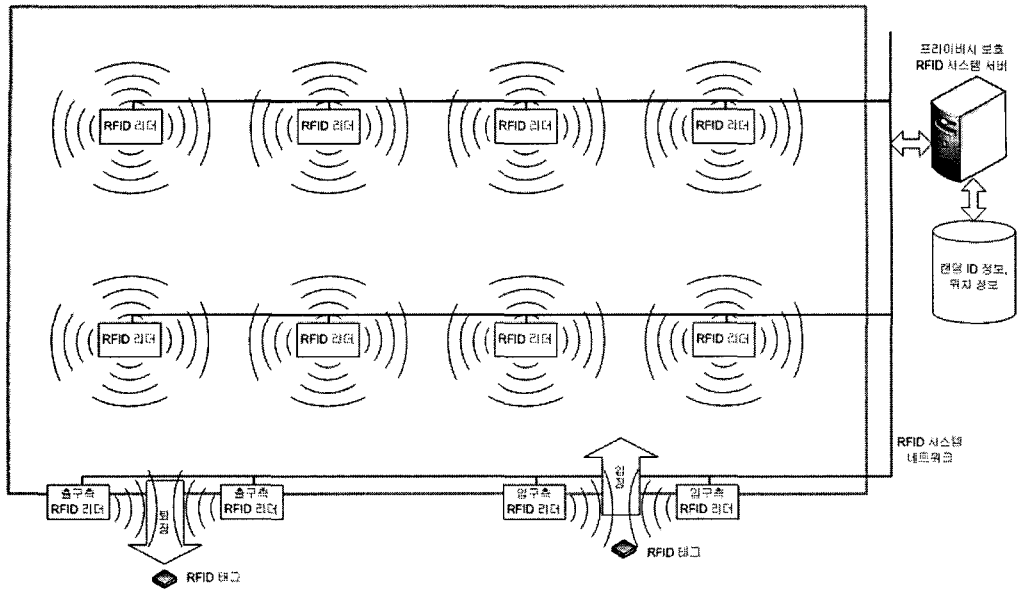

그림 5. 프라이버시 보호 RFID 시스템의 동작

3.3 프라이버시 보호 영역 퇴장

할인매장을 벗어나는 출구에 접근하게 되면 출구측 리더는 2.4절에 설명된 랜덤 ID 삭제 프로토콜을 이용하여 태그에 저장된 랜덤 ID를 '0' 으로 초기화한다. 이는 프라이버시 보호 영역 밖에서 발생할지도 모르는 랜덤 ID 추적을 방지위한 조치이다. 또, 이와 동시에 랜덤 ID 사용 플래그가 재설정되므로 프라이버시 보호 영역을 벗어나는 태그는 리더의 호출에 랜덤 ID가 아닌 자신의 태그 ID를 응답하게 된다.

4. 결 론

현재 RFID 시스템의 취약한 문제점 중 하나로 사생활 침해 문제가 대두되고 있는데, 이는 RFID 태그에 저장되는 ID를 추적함으로써 발생하고 있으며, 이러한 문제점을 방지하기 위해 본 논문에서는 태그에 난수 기반의 ID를 필요할 때마다 동적으로 할당함으로써 ID 추적이 불가능한 RFID 시스템을 제안하였다. 이 시스템은 고정된 ID 때문에 발생하는 보안 문제를 해결하기 위해 일반적인 환경에서는 자신의 고유 ID를 사용하고, 프라이버시가 필요한 환경에서만 난수 기반의 새로운 ID를 태그에 부여함으로써 서버는 부여된 새 ID를 통해 태그를 인식하게 하면 설령 공격자가 ID를 추적한다 하더라도 태그의 이전 ID와 새로 부여된 ID간의 상관관계를 알 수 없기 때문에 위치 파악이 불가능하다는 점이 특징이다. 이미 산업자원부의 지원하에 RFID 시범사업으로 대형 할인매장에서 고객의 이동경로 등을 추적하는 RFID 시스템이 구축되어 운용된바 있으나, 고정된 태그 ID를 이용하는 방식을 사용하였다. 본 논문에서 제안한 프라이버시 보호 시스템은 대형 할인매장에서 손님들에게 태그를 나누어 주고, 이 태그에 부여되는 ID가 랜덤하게 할당됨으로 인해 프라이버시를 보호하면서 그 이동 경로, 구매 성향 등을 추적하여 고객정보와 판매 관련 정보를 축적할 수 있는 장점을 가지고 있다.

참고문헌

[1] S.E.Sarma, S.A.Weis, and D.W.Engels, "RFID Systems, Security & Privacy Implications", White Paper, Auto-ID Center, MIT, 2002.

[2] S.A.Weis, S.Sarma, R.Rivest, and D.Engels, "Security and Privacy Aspect of Low-Cost Radio Frequency Identification Systems", Springer-Verlag, First International Conference on Security in Pervasive Computing, LNCS 2802, pp.201-212, 2004.

[3] 박진성, "동적 ID 할당을 이용한 고기능 RFID 태그용 보안 프로토콜", 한국산학기술학회논문지, 제7권 제4호, pp. 642-648, 9월, 2006.

박 진 성(Jin-Sung Park) [정회원]

- 1995년 2월 : 한양대학교 제어계측공학과 (공학사)
- 1997년 2월 : 한양대학교 제어계측공학과 (공학석사)
- 2006년 2월 : 한양대학교 제어계측공학과 (공학박사)
- 2000년 ~ 2002년 : (주)마니네트웍 개발팀장
- 2003년 ~ 2004년 : 노틸러스효성(주) 개발팀 과장
- 2005년 5월 ~ 현재 : (주)씨이엔 연구소장

<관심분야>
스마트카드, RFID, 정보보호

최 명 렬(Myung-Ryul Choi) [정회원]

- 1983년 2월 : 한양대학교 전자공학과 (학사)
- 1985년 12월 : 미시간 주립대학교 컴퓨터공학과 졸업 (공학석사)
- 1991년 3월 : 미시간 주립대학교 컴퓨터공학과 졸업 (공학박사)
- 1991년 3월 ~ 10월 : 생산기술연구원 전자정보실용화센터 조교수
- 1991년 11월 ~ 1992년 8월 : 생산기술연구원 산하 전자부품종합기술연구원 선임연구원
- 1992년 ~ 현재 : 한양대학교 전자컴퓨터공학부 교수

<관심분야>
SoC/ASIC 설계, 디스플레이, Smart Card/RFID 응용