수동형 RFID 태그를 위한 보안 프로토콜 설계 및 분석

김인섭° 이병길 김호원
과학기술연합대학원°, 한국전자통신연구원 RFID/USN 보안연구팀
{kis64388°, bglee, khw}@etri.re.kr

Security Protocol Design and Analysis for passive RFID Tag

Inseop Kim° Byunggil Lee Howon. Kim
University of Science & Technology°, RFID/USN Security Research Team, ETRI

요 약

모든 사물에 고유 식별 정보(Unique Product Identifier)가 부착되어 사물의 개별 관리 및 컴퓨팅 환경을 구성하는 RFID(전자식별) 기술이 다양한 응용 및 구현 기술을 위해 활발하게 연구되고 있다. 하지만 수동형 태그 기반 RFID 시스템은 태그 자체의 자원 제약성 때문에 인가되지 않은 사용자에 의한 악의적인 태그 정보 노출이 용이하고, 그 결과 개인의 프라이버시 및 정보의 기밀성이 위협받게 된다. 비록 이를 예방하기 위해 다양한 보호 기법이 제안 되고 있지만 수동형 태그에 적용하기 힘들거나(예: Hash 기반 메커니즘) 보안에 취약하다. 따라서 본 논문에서는 태그 코드 암호화와 리더 인증 관리를 통해서 수동형 태그에 적합하고 프라이버시 보호 및 기밀성을 제공할 수 있는 메커니즘을 제안하고자 한다.

1. 서 론

사물에 고유 식별 정보와 간단한 프로세싱 모듈을 내장(태그)하고 외부 장치(리더)와 Air Interface를 통해서 통신하는 RFID 기술은 정보 운용 환경과 연계되어 혁신적인 유비쿼터스 인프라를 형성할 것이다. 또한 태그에 Smart Sensor가 내장되어 센서 간 네트워크를 이루는 USN(Ubiquitous Sensor Network)환경이 구성 될 것이다. 이와 관련하여 지금은 Pervasive RFID 시스템을 위한 저비용 수동형 태그 기반의 활발한 연구가 진행되고 있다. 그러나 수동형 태그 자체의 자원 제약적인 특성으로 인해 강력한 보안 기능을 구현하기 힘들고 이 때문에 물품에 대한 정보 노출 및 태그 소유자의 위치 추적 문제가 발생하게 된다. 이런 문제를 해결하기 위한 많은 기법이 제안 되고 있지만 실제 수동형 태그에 적용하기 힘들거나(예: Hash-Chain[3]) RFID 시스템의 효율적 활용 및 태그의 Life-Cycle을 저해(예: Kill Tag[5])한다. 따라서 본 논문에서는 EPC(Electronic Product Code-RFID 태그 입력용 상품식별코드인 전자상품코드) 프로토콜을 기반으로 이러한 수동형 태그에 적합한 Security 및 프라이버시 보호 기법을 제안하고자 한다.

2. EPC 기반의 시스템 모델

2.1 수동형 EPC C1G2 태그

수동형 태그는 자체 Power 생성 및 공급 루틴이 없어 외부(즉, RFID 리더)에서 전원을 공급해 주어야하고 자원이 제약되어 있기 때문에 태그 Security를 위한 암호화 등 복잡한 계산을 수행할 수 없다. 수동형 C1G2(Class-1 Generation-2) 태그는 860-960MHz에서 리더에 동작하고 Read/Write 모두 가능하다. 태그의 응답은 리더의 지속적인(continuous wave) RF 신호를 이용하여 리더로 태그 정보 Signal을 backscatter 함으로써 이루어진다.

2.2 EPC 기반 RFID 시스템

[그림 1]은 간략한 EPC 기반 RFID 시스템 동작 구조를 보여주고 있다. 리더는 Challenge-Response 방식(1,2)으로 태그의 EPC 코드를 받아서 이를 미들웨어에 전송한다. 태그는 리더의 요청 때 마다 보안 메커니즘 없이 EPC 코드 자체를 제공한다. 미들웨어는 ODS(Object Directory Service, DNS 기능과 유사)에 EPC 코드와 매핑 되는 정보서버(IS)의 URL을 요청하고 그 결과 받은 URL을 통해서 해당 태그의 정보를 저장하고 있는 서버에 사용자의 요청을 전송한다(3,4,5,6). IS는 사용자 질의 결과를 미들웨어를 통해서 사용자 리더 혹은 어플리케이션으로 전송해 준다(7,8).

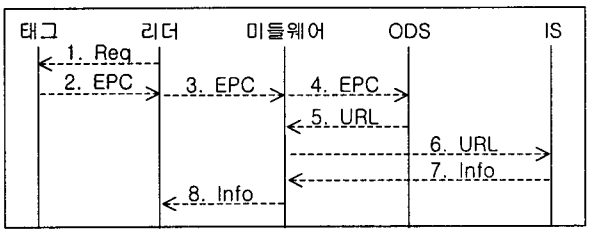

그림 1 EPC 기반 RFID 시스템

2.3 Security & Privacy 취약점

[그림 1]에서 태그-리더 구간은 무선 환경이므로 다른 구간에 비해 안전성이 떨어진다. 비인가 리더를 통해 태그 Skimming 혹은 Cloning 등의 부정당한 행위는 태그 Security 및 소유자의 프라이버시를 위협한다. 따라서 인가된 리더만이 태그의 정보를 제공 받고 부당한 리더의 공격을 효과적으로 예방할 수 있는 방법이 안전한 EPC 기반 RFID 시스템 구성을 위해 제공되어야 한다. 또한 EPC 코드를 부당한 리더가 획득해서 정보 서버로 접근 하는 문제 해결을 위해 EPC 코드는 보호되어야 한다.

3. 기존의 제안된 RFID 보안 메커니즘

3.1 RFID의 Security 및 프라이버시 문제

RFID 시스템 환경에서 Security 및 프라이버시 관련 문제는 태그 소유자의 허가 없이 리더를 이용해 소유자의 태그 정보를 취합(malicious collection)하고, 취합한 데이터를 이용해서 소유자 위치를 추적(Location Tracking)하는 것이다.

3.2 기 제안된 보호 방법[2][3][4][5]

참고 문헌[2][3][4]는 태그 소유자의 위치 추적을 예방하기 위한 방법들을 보여준다. 위치 추적은 태그가 리더로 보내는 응답메시지가 매번 동일함으로써 가능하다. 따라서 이들은 태그 응답 메시지를 매번 변경함으로써 추적을 효과적으로 회피하는 방법을 제안하고 있다. [5]에서는 부당한 리더의 태그 접근을 원천적으로 막기 위한 방법을 제시하고 있다. 어느 순간 태그를 무효화(deactivate)하거나 태그로 접근하는 신호를 차폐시킴으로서 리더의 요청을 무시한다.

4. 제안하는 RFID 보안 프로토콜(Proposed Protocol)

4.1 용어 정의 (Symbol Definition)

본 논문에서 제안하는 프로토콜을 이해하기 위한 용어 설명을 테이블 1에서 보여주고 있다.

표 1 Symbols

Symbol	Definition
E_K	K를 Key로 하는 대칭 암호화
EPC	Electronic Product Code
K{T-S}	태그와 인증 서버가 공유하는 비밀 키
$\{E_{EPC}\}$	K{T-S}를 이용하여 EPC 암호화 값
F(A)	A를 입력으로 하는 해쉬 함수
$\{H_{EPC}\}$	EPC 코드를 해쉬한 값
r	태그가 생성한 난수
K{R-S}	리더와 인증 서버가 공유하는 비밀 키
R_{cert}	인증 서버가 발급한 리더 인증서
R_{ID}	리더 고유 식별자
R.A.T	리더 인증을 위한 데이터베이스 테이블
T.A.T	태그 인증을 위한 데이터베이스 테이블
R.N.G	난수 생성기
N.G	Nonce 생성기
R_N	랜덤하게 생성된 Nonce
⊗	Exclusive-OR
D_K	K를 Key로 하는 복호화

4.2 시스템 구조 및 보안 프로토콜

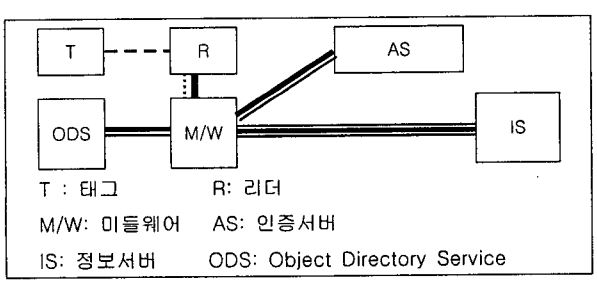

그림 2 시스템 Architecture(Communication Parties)

[그림 3]은 RFID System 및 본 논문에서 제안하는 통신 개체들(Communicating Entities)을 도식화 하고 있다. [그림 4]는 이를 기반으로 제안하는 프로토콜에서의 통신 흐름을 설명하고 있다.

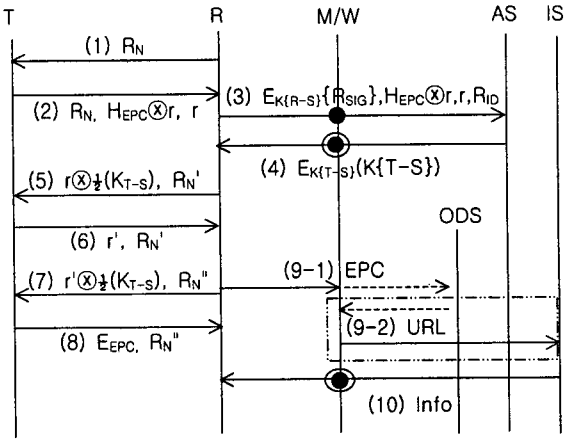

그림 3 Protocol Flow Diagram

(1) R은 T와 통신하기 위한 첫 단계(ITF - Interrogator talks first)로 Nonce 생성기(N.G)를 이용해서 R_N을 생성하고 이를 태그에 전송한다.

$$R \rightarrow T : Req\{R_N\}$$

(2) T는 R로부터 받은 에너지를 이용하여 랜덤 변수 r을 생성하고 저장하고 있는 H_{EPC}와 r을 Exclusive-OR한 결과 값과, r 그리고 R로부터 받은 R_N을 응답 데이터에 포함하여 R에 전송한다.

$$M = H_{EPC} \otimes r$$
$$T \rightarrow R : Res\{M, r, R_N\}$$

(3) R은 T의 응답 데이터에서 R_N을 확인하고 맞으면 나머지 데이터를 자신의 메모리에 저장(Caching)하고 AS에 T의 응답에서 R_N을 제외한 나머지 데이터와 R을 인증하기 위한 R_{SIG}를 K_{R-S}를 이용하여 암호화 하고 R_{ID}를 인증 요청 패킷에 포함하여 AS에게 T의 암호화된 EPC를 복호화하기 위한 Symmetric Key, K_{T-S}를 요청한다.

$$Verify\ R_N$$
$$E_{KR-S}(R_{SIG})$$
$$R \rightarrow AS[via\ M/W] : Req\{E_{K(R-S)}(R_{SIG}), M, r, R_{ID}\}$$

(4) AS는 R의 요청에 대해 우선 자신이 관리하는 DB 테이블 가운데 R을 인증하기 위한 R.A.T로 부터 R의 R_{ID}를 탐색하여 Shared key, K_{R-S}를 찾아 R이 전송한 데이터를 복호화 하여 R의 Signature R_{SIG}를 검증한다. 검증 되면, R이 전송한 r을 이용해서 M에서 H_{EPC}를 복원하고 T.A.T에서 H_{EPC}와 관련된 key, K_{T-S}를 찾아 K_{R-S}로 암호화하여 R에 전송한다.

$$Verify\ R_{SIG}$$
$$H_{EPC} = M \otimes r$$
$$AS \rightarrow R\ [via\ M/W\ or\ Directly] : Res\{E_{K(R-S)}(K\{T-S\})\}$$

(5) R은 AS가 전송한 데이터를 자신의 K{R-S}를 이용하여

복호화하여 요청하고 자하는 태그의 K{T-S}를 획득한다. R은 새로운 Nonce R_N을 생성하고 K{T-S}의 절반과 (3)에서 캐쉬했던 r을 X-OR한 결과를 T에 전송한다. 이때 R은 태그로 하여금 또 다른 난수를 요청 한다.

$K\{T-S\} = D_{K\{R-S\}}(E_{K\{R-S\}}(K\{T-S\}))$
$R \rightarrow T : Req\{\frac{1}{2}(K\{T-S\}) \otimes r, R_N'\}$

(6) T는 $\frac{1}{2}K\{T-S\} \otimes r$ 에서 r을 제외한 $\frac{1}{2}K\{T-S\}$를 임시 저장하고, R에게 새로 생성한 난수 r'과 R_N' 을 전송한다.

$T \rightarrow R : Req\{r', R_N'\}$

(7) R은 R_N'를 검증하고 또 다른 Nonce $R_N"$를 생성한다. (5)에서 남은 $\frac{1}{2}K\{T-S\}$와 r'를 X-OR한 결과와 $R_N"$를 T에 전송한다.

$Verify\ R_N'.$
$R \rightarrow T : Req\{\frac{1}{2}(K\{T-S\}) \otimes r', R_N"\}$

(8) T는 R로부터 받은 K{T-S}를 자신의 것과 비교하여 동일하면 R에게 끝으로 E_{EPC}와 $R_N"$ 보내준다.

$T \rightarrow R : E_{EPC}$

(9) R은 T에서 받은 E_{EPC}를 K{T-S}를 key로 하여 복호화를 한다. 그 결과 구해진 EPC 코드를 M/W에 전송하면(9-1) M/W는 ODS에 Directory Service를 요청하여 해당 태그 정보가 저장된 IS 주소를 획득하고 마침내 해당하는 IS에 접근하게 된다.(9-2)

$D_{K\{T-S\}}\{E_{EPC}\}$
$R \rightarrow M/W : EPC$
$M/W(by\ ODS): EPC \rightarrow URL$
$M/W \rightarrow IS : Req\_Information$

(10) IS는 R의 요청을 처리하고 그 결과를 R에게 전송해 준다. 이때 IS-R은 M/W를 통하거나 직접 통신할 수 있다(⊙).

$IS \rightarrow R : Res\_Information$

4.3 제안 기법의 Security Analysis 및 장. 단점 분석

4.3.1 Security Analysis

- 태그의 EPC가 암호화되어 저장 되며 인증 서버에 의해 인증된 정당한 리더만이 태그의 정보를 복호화 할 수 있다. 암호화가 계산환경이 풍부한 Trusted Device를 통해서 행해지고 태그에 쓰여 지기 때문에 강력한 암호화 알고리즘을 이용할 수 있고, 이는 태그 EPC의 안전성을 보장한다.

4.3.2 장점 분석

1) 위치 Tracking 문제 해결

- R에 대한 T의 응답(2)(6)(8)은 항상 변하게 된다. T는 R을 위한 응답 메시지를 구성하기 위해 매번 다른 난수를 생성함으로써 *메시지 freshness*를 제공하며 이는 동일 데이터에 의한 인가되지 않은 Location Tracking을 예방할 수 있다.

2) 태그 경량화 (light-weight Tag)

- 태그는 강한 fresh 응답을 위한 난수 생성 및 비밀 키 비교 루틴 기능만 요구하므로 경량화 할 수 있다. R은 지속적인 태그의 컴퓨팅을 위해 CW(continuous wave)를 보내주고 이는 위의 *light-weight 태그*를 효과적으로 작동시킬 수 있다.

3) 보강된 태그 인증

- R은 (3)에서 캐쉬한 H_{EPC}를 (10)에서 T로부터 받은 E_{EPC}를 복호화 하고 해쉬 함수를 적용한 값과 비교할 수 있다. 이 두 값이 동일하면 R은 태그의 인증을 확신 할 수 있다.

$H_{EPC} = H(D_{K\{T-S\}}(E_{EPC}))$

4.3.3 단점 분석

- 리더는 사용 전에 인증서버로부터 인증을 받아야 하고 제안된 보안 메커니즘을 위하여 인증 서버가 제공되어야 한다.
- 인증서버는 Single-Point-Failure(혹은 DOS공격) 및 다른 외부 위협으로부터 안전하게 보호되어야 한다.

5. 결론

본 논문에서는 태그 소유자 프라이버시 보호를 위해 EPC를 암호화 하여 전달하며, 태그와 AS간 상호인증이 가능하고 인가된 리더에게만 정보서버 접근을 허가 하는 프로토콜을 제안하였다. 또한 태그 정보를 이용하기 위해 리더는 적법한 인증 절차를 거쳐야 하고 인증 서버는 안전하게 이를 관리하며 태그 EPC 암호화와 리더 및 태그 인증이 강화되었기 때문에 부당한 태그, 리더를 무력화할 수 있다. 따라서 제안하는 기법은 안전한 수동형 태그를 위한 적합한 메커니즘을 제공할 수 있을 것으로 판단된다.

참고 문헌

[1]EPCglobal: EPC*TM* Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz Version 1.0.7

[2]Ari Juels, Ravikanth Pappu "Squealing RFID-Enabled Banknotes" In R. Wright, ed., Financial Cryptography '03

[3]M. Ohkubo, K. Suzuki and S. Kinoshita,"Cryptographic Approach to "Privacy-Friendly"Tags,"RFID Privacy Work-shop, http://www.rfid.edu.com, 2003

[4]P. Golle, M. Jakobsson, A. Juels, and P. Syverson. Universal re-encryption for mixnets, 2002. In submission.

[5]Ari Juels, Ronald L Rivest, Michael Szydlo "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy" 10th ACM Conference on Computer and Communications Security, 2003

[6]RFID HANDBOOK "Fundamentals and Applications in Contactless Smart Cards and Identification" second edition