韓國컴퓨터情報學會 論文誌
第16卷 第11號, 2011. 11.

2011-16-11-3-3

OTP와 일회성 난수를 사용한 AES 알고리즘 기반의 개선된 RFID 상호 인증 프로토콜

윤 태 진*, 오 세 진**, 안 광 선***

Improved RFID Mutual Authentication Protocol using One-Time Pad and One-Time Random Number Based on AES Algorithm

Tae-Jin Yun*, Se-Jin Oh**, Kwang-Seon Ahn***

요 약

RFID 시스템은 무선 주파수를 이용하기 때문에 도청, 위치 추적, 스푸핑 공격, 재전송 공격과 같은 공격에 취약하다. 이를 해결하고자 RFID 시스템의 상호 인증 기법과 암호화 기법이 활발히 연구되고 있다. 그러나, 과거 AES(Advanced Encryption Standard)를 이용한 대칭키 기반의 프로토콜은 고정키 문제와 보안 취약성을 안고 있어 본 논문에서 기존 프로토콜의 보안 취약성을 증명하고, OTP(One-Time Pad) 기법과 AES를 이용한 프로토콜을 제안하여 보안 취약점을 보완하고 연산, 하드웨어 오버헤드를 감소하고자 한다. 제안 프로토콜은 리더와 태그 간 데이터를 암호화하고, 리더의 일회성 난수 사용하여 상호 인증을 한다. 그리고, S.Oh 프로토콜을 비롯한 기존 프로토콜과 비교 분석으로 보안성과 서버, 리더, 태그의 연산량 측면 등 효율성에서 상대적으로 우수함을 보인다.

▸ Keyword : RFID 시스템, AES 알고리즘, 상호인증, 일회성난수

Abstract

Because RFID systems use radio frequency, they have many security problems such as

• 제1저자 : 윤태진 교신저자 : 안광선
• 투고일 : 2011. 08. 19, 심사일 : 2011. 09. 04, 게재확정일 : 2011. 09. 17.
* 경운대학교 모바일공학과(Dept. of Mobile Engineering, Kyungwoon University)
** 경북대학교 전자전기컴퓨터학부(Graduate School of Electrical Engineering and Computer Science, Kyungpook National University)
*** 경북대학교 컴퓨터학부(School of Computer Science and Engineering, Kyungpook National University)

eavesdropping, location tracking, spoofing attack and replay attack. So, many mutual authentication protocols and cryptography methods for RFID systems have been proposed in order to solve security problems, but previous proposed protocols using AES(Advanced Encryption Standard) have fixed key problem and security problems. In this paper, we analyze security of proposed protocols and propose our protocol using OTP(One-Time Pad) and AES to solve security problems and to reduce hardware overhead and operation. Our protocol encrypts data transferred between RFID reader and tag, and accomplishes mutual authentication by one time random number to generate in RFID reader. In addition, this paper presents that our protocol has higher security and efficiency in computation volume and process than researched protocols and S.Oh's Protocol. Therefore, our protocol is secure against various attacks and suitable for lightweight RFID tag system.

▸ Keyword : RFID Systems, AES Algorithm, Mutual Authentication, One time ramdom number

I. 서 론

RFID(Radio Frequency Identification) 기술은 ISO 18000-2~7에서 규정한 무선 주파수를 이용한 비 접촉 방식의 자동인식 기술이다. RFID 시스템은 정보를 제공하는 태그, 판독 기능을 하는 리더, 그리고 데이터를 처리하는 서버로 구성된다. RFID 시스템은 바코드에 비해 많은 데이터 처리과 인식 속도로 물류 시스템 뿐만 아니라 가축 관리, 산업 자동화, 교통 요금 지불 시스템 등 많은 분야에서 널리 활용되고 있다[2,3]. 하지만 RFID 시스템 특성상 무선채널을 사용하므로 도청과 같은 악의적인 공격과 개인 위치 추적, 정보 노출 등 프라이버시 침해와 같은 문제점이 있다. 이를 해결하기 위해서 Kill 명령어, 암호화 기법과 상호인증 기법이 연구되고 있다. 암호화 기법에는 해시함수, 대칭키 암호화 알고리즘이 있다. 그러나 자원적 제약이 큰 수동형 태그에 5,000 게이트 미만의 해시함수 구현은 불가능하다. 대칭키 기반의 AES 알고리즘은 안전성이 검증되었고, M. Feldhofer 등에 의해 RFID태그에 적용한 사례가 있다[4-6]. 하지만 RFID 태그에 적용하기 위해서는 키 분배와 같은 문제점을 해결하여야 한다. 또한 리더와 태그 간 데이터전송은 인증된 객체에게 전달되어야 하므로 상호 인증 기법 또한 빼놓을 수 없다.

본 논문에서는 AES와 일회성 난수사용을 기반으로 하는 RFID 상호인증 프로토콜을 제안한다. 제안 프로토콜의 경우 AES 알고리즘으로 무선 상의 데이터를 안전하게 암호화 하며, 일회성 난수를 적극 활용하여 암호화된 메시지를 매 세션 가변적인 값이 출력되도록 제안한다. 또한 인증 절차를 통하여 공격자의 접근을 거부하도록 하였다. 2장에서는 AES 대칭키 알고리즘이 RFID 시스템에 적합함과 기존 RFID 인증 프로토콜의 문제점에 대해 살펴보고 3장에서는 본 논문에서 제안한 개선된 프로토콜에 대해서 서술한다. 4장에서는 기존 프로토콜과 제안 프로토콜의 안전성과 효율성을 비교 분석하며, 마지막으로 결론을 맺는다.

II. 관련 연구

1. RFID 시스템에 적용 가능한 암호화 기법

RFID 시스템의 다양한 문제점을 해결하기 위해 암호화 기법이 사용되어 진다. 해시 함수의 경우 전 방향 안전성이 우수하여 암호학적 기법의 하나로 많이 사용되고 있다. 해시 기반의 Hash-Lock 프로토콜, Randomized Hash-Lock 프로토콜은 메시지를 안전하게 암호화하여 전송하지만 서버에서 태그 ID를 찾아내기 위해 평균 ⌈m/2⌉번의 해시 연산이 필요하다[7]. 많은 수의 태그를 인식해야하는 RFID 시스템에서 이는 서버에 부하를 가지게 된다. 또한 SHA 계열의 해시 함수를 하드웨어로 구현 한다면 20,000~25,000 게이트 이상이 소요되는 문제점을 지니게 된다. 그러므로 자원 제약이 따르는 수동형 태그에 해시 함수를 구현하는 것은 현실적이지 못하다.

AES(Advanced Encryption Standard)는 1987년 NIST에서 DES(Data Encryption Standard)를 대신할 새로운 암호화 알고리즘으로 채택된 것으로, V. Rindael에 의해 제안한 알고리즘이다[8, 9]. 이를 바탕으로 M.

Feldhofer 등은 3,595 게이트 크기의 8bit로 동작하는 AES를 설계하였다[4]. 이후, Mark Jung, 구본석 등에 의해 4,000 게이트 미만의 AES 암·복호화 가능한 연산기를 구현하여 AES가 수동형 RFID 태그에 적합함을 입증하였다[5,6].

2. 대칭키 기반 기존 프로토콜의 문제점

그림1은 M. Feldhofer의 AES를 이용한 인증 프로토콜로서 M. Feldhofer가 제안한 인증 프로토콜[4,10]의 경우 공격자가 연속적으로 난수 RA를 태그에게 보내게 되면 태그는 대칭키 K로 암호화 한 EK(RA)로 태그의 위치를 추적할 수 있다. 그리고 리더와 태그사이에서 전송되는 데이터를 획득하여 스푸핑 공격, 재전송 공격으로 정당한 리더로 인증 받을 수 있다. 뿐만 아니라, 리더의 난수 RA와 EK(RA)를 이용하여 공격자는 전수조사를 통한 대칭키 K를 획득할 수 있는 문제점을 가지고 있다.

Toiruul 등도 대칭키의 문제점인 키 분배 문제를 해결하고자 키 값을 지속적으로 갱신하는 AES를 이용한 인증 프로토콜을 제안하였다[11]. 프로토콜상에서 서버가 리더를 통해 태그에게 전달한 EK(K1⊕K2)는 정당한 서버일 경우 올바른 K, K1, K2를 사용하여 암호화한 값이기 때문에 태그에서 서버를 인증할 수 있다. 그러나 서버에서 태그 인증 절차가 없는 점은 공격자에게 공격의 여지를 주게 되며, Toiruul의 프로토콜은 주장과는 다르게 상호인증이 아니게 된다. 또한 K1과 K2는 일정한 방식으로 갱신을 하지만 암호화에 사용되는 대칭키 K는 고정되어 있어 물리적 공격으로 인한 대칭키가 노출될 수 있다. 그리고 태그가 EK(K1⊕K2⊕IDK)를 서버에 전송하는 과정에서 공격자가 전파 방해하여 비동기화 공격이 가능하고 이로 인해 서비스 거부 공격으로 이어져 시스템 전체를 마비시킬 수 있다. 그림 2는 Toiruul 등이 제안한 프로토콜이다.

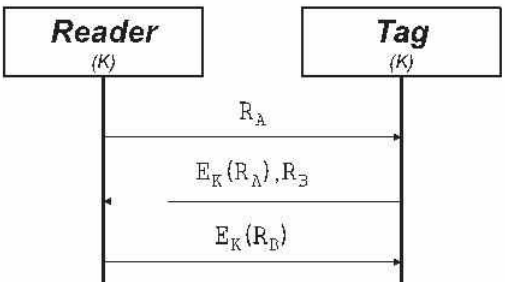

그림 1. M. Feldhofer의 프로토콜
Fig. 1. M. Feldhofer's Protocol

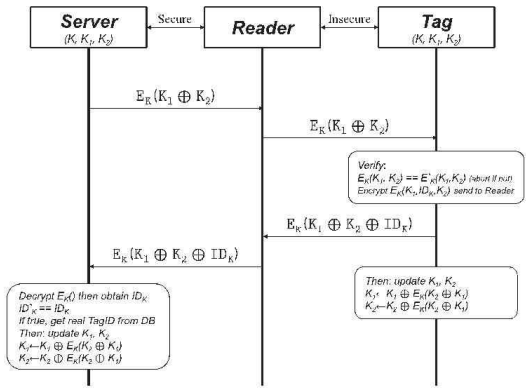

그림 2. Toiruul의 프로토콜
Fig. 2. Toiruul's Protocol

M. F. Mubarak 등은 TPM(Trusted Platform Module)을 사용한 RFID 상호 인증 프로토콜을 그림 3과 같이 제안하였다[12]. 서버, 리더, 태그의 난수와 K, B, IB, IR, IT를 사용하여 다양한 공격에 안전하다고 주장하였다. 그러나 리더와 태그간의 데이터 전송을 도청공격으로 획득하고, 불법 리더가 정상적인 리더로 위장하여 태그에게 EK[(IR, IB, NC)]를 연속해서 전송하면 고정된 응답 값 즉, EK[(IT, NC)]으로 응답하게 되어 개인 프라이버시 문제가 발생한다[13]. 이처럼 검증된 암호화 기법은 물론 다양한 공격에도 안전한 인증 프로토콜 설계 또한 매우 중요하다.

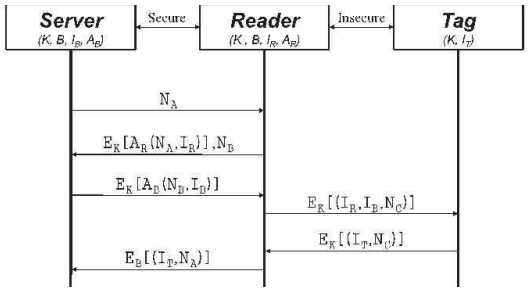

그림 3. M. F. Mubarak의 프로토콜
Fig. 3. M. F. Mubarak's Protocol

그림 3과 같이 S. Oh 등은 일회성 난수를 암·복호화 키로 사용하는 프로토콜을 제안했다[1]. 매 세션 새로운 리더, 태그 난수 Rr, Rt를 암호화 메시지와 암호화 키로 사용하여 상호인증 과정을 통해 태그의 ID를 전달하는 프로토콜이다. 고정된 대칭키를 사용하지 않고, 일회성 난수를 사용하기 때문에 RFID 시스템의 다양한 공격에 안전하다. 그러나 최초 리더가 태그에게 전달하는 대칭키값을 마스크와 단순히 XOR하

는 방법으로 전달하는 경우 OTP기법을 이용한 방법에 비해 안전하지 못해 보완이 필요하며, 암복호화 연산이 태그에서 3회, 리더에서 3회 수행되어, 다수의 태그와 리더간 전송되는 데이터량을 고려해 감소시킬 필요가 있다. 또한, 자원적 제약이 있는 수동 태그에서 암·복호화가 수행되어 수동 태그에 대한 하드웨어 오버헤드와 전력소모량, 수행시간 등이 암호화만 수행할 경우보다 증가한다. 그래서, 보안성과 효율성 측면에서 보완하여 개선할 필요가 있다.

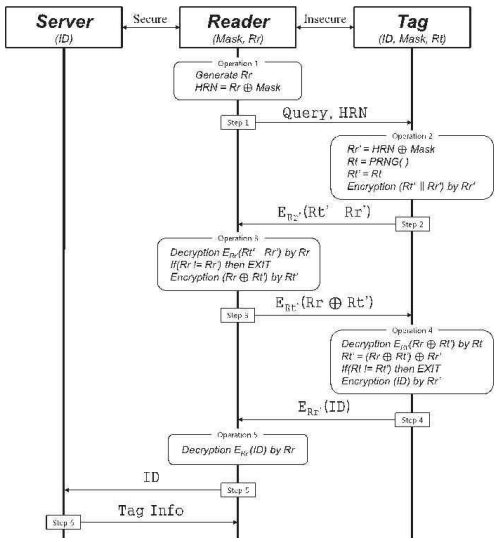

그림 4. S. Oh의 프로토콜
Fig. 4. S. Oh's Protocol

3. OTP(One-Time Pad)

이 암호 기법은 1917년 미국 AT&T사의 Gilbert S. Vernam이 처음 제안하였으며[14], Claude Shannon이 OTP가 완벽한 안전성을 가지고 있음을 검증하였다[15,16]. OTP는 eXclusive-OR 연산을 이용하여 암·복호화를 수행하고, OTP를 사용하기 위한 조건은 비밀키는 랜덤하게 생성하여야 한다. 그리고 한번 사용한 비밀키는 다시 사용하지 않아야하며, 평문과 비밀키의 길이가 동일해야하는 특징을 지니고 있다. OTP의 평문(m), 비밀키(k), 암호문(c)을 수식으로 나타내면 다음과 같다.

$m = m1\ m2 \cdots mn \in \{0,1\}n$ (1)

$k = k1\ k2 \cdots kn \in \{0, 1\}n$ (2)

$c = c1\ c2 \cdots cn;\ ci = bi \oplus ki,\ 1 \le i \le n$ (3)

III. 본 론

1. 제안 프로토콜

AES와 일회성 난수사용을 기반으로 하는 RFID 상호 인증 프로토콜을 제안한다. 인증 절차에서 사용된 데이터는 일회성 난수를 사용하며, 리더 난수를 안전하게 전달하기 위하여 OTP기법을 사용한다. 또한 본 논문의 AES 암·복호화시 사용되는 키는 일회성 난수를 사용하여 대칭키의 고정된 키를 사용하는 문제점을 해결한다. 제안 프로토콜은 태그 인증 단계와 리더 인증 단계로 구성되어 있고, 그림 5는 대칭키 기반의 일회성 난수를 이용한 RFID 상호 인증 프로토콜인 MAPOS(rfid Mutual Authentication Protocol using One-time random number based on Symmetric key)를 나타낸다.

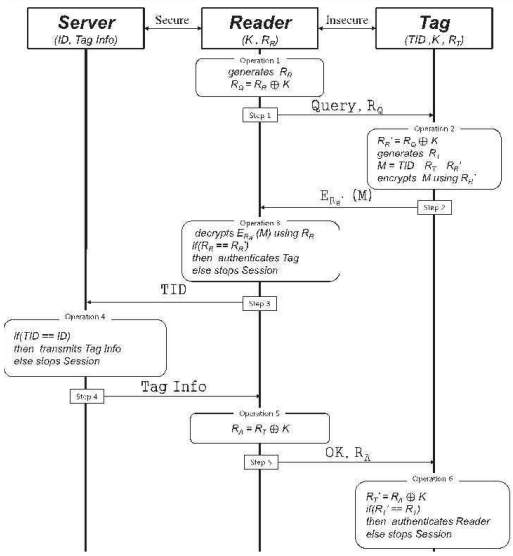

그림 5. MAPOS
Fig. 5. MAPOS

1.1 제안 프로토콜의 가정 사항과 용어 설명

본 논문에서 MAPOS는 다음과 같은 가정 사항에서 동작이 가능하다. 첫째, 리더와 태그에는 동일한 대칭키 K가 안전하게 초기화되고 보관되어 있다. 둘째, 서버와 리더 간에는 공격자의 공격에 안전한 통신채널이 이루어지고 있으며, 리더와 태그 사이는 공격자의 공격에 취약한 무선 채널 구간이다. 셋째, 태그는 AES를 이용한 암호화가 가능하며, 서버와 리더는 AES를 통해 암·복호화가 가능하다. 마지막으로 리더와 태그는 난수를 생성할 수 있으며, 태그는 리더로부터 전원 공급을 받는 수동형 태그로 가정한다.

표 1은 본 논문의 제안 프로토콜에서 사용되는 용어를 나타낸 것이다.

표 1. 용어 설명
Table 1. Notations

표기법	설명
RR	리더에서 생성한 난수
RT	태그에서 생성한 난수
TID	태그의 ID
ID	서버 DB상의 태그의 ID
K	대칭키
⊕	eXclusive OR 연산
‖	연접 연산자
E( )	AES 암호화
Tag Info	태그 정보

1.2 태그 인증 단계

그림 6는 MAPOS의 태그 인증 단계를 나타낸 것이다.

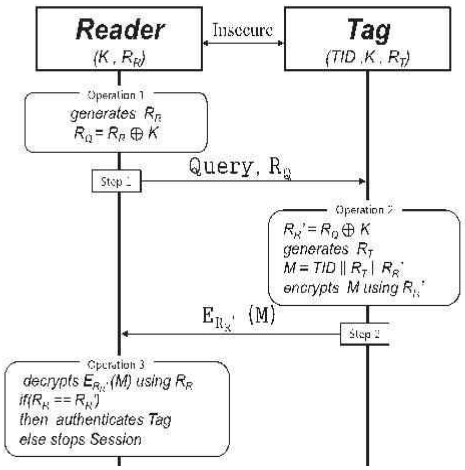

그림 6. 태그 인증
Fig. 6. Tag authentication

첫 번째 단계는 초기 질의 단계로 리더가 태그에게 전송되는 Query, RQ로부터 시작된다. 이때 전송되는 RQ는 리더가 생성한 일회성 난수 RR과 K를 OTP 암호화한 값이다. 리더 난수 RR을 생성하여 사용한 뒤 추후 통신에서도 사용되지 않기 때문에 완전 암호계 판정법을 만족한다.

```
Step 1.
Reader      generates RR
:           RQ = RR⊕K
Reader → Tag : Query, RQ
```

태그는 리더에게 Query, RQ를 받아 대칭키 K로 RQ를 복호화하여 RR'을 획득한다. 그리고 TID와 RT, RR'을 연접하여 RR'을 암호화 키로 사용하여 AES로 암호화한 ERR'(M)를 리더에게 전송한다.

```
Step 2.
Tag     RR' = RQ⊕K
:       generates RT
        M = TID ‖ RT ‖ RR'
        encrypts M using RR'
Tag → Reader : ERR'(M1)
```

ERR'(M)를 받은 리더는 난수 RR을 사용하여 복호화한다. 복호화하여 리더가 생성한 난수 RR과 태그가 전송한 RR'이 같을 경우 리더를 인증한다. 만약 다를 경우 세션은 종료된다.

```
Step 3.
Reader      decrypts ERR'(M) using RR
:           if(RR == RR')
              authenticates Tag
            else
              stops session
Reader → Back-End-Server : TID
```

1.3 리더 인증 단계

그림 7은 MAPOS의 리더 인증 단계를 나타낸 것이다.

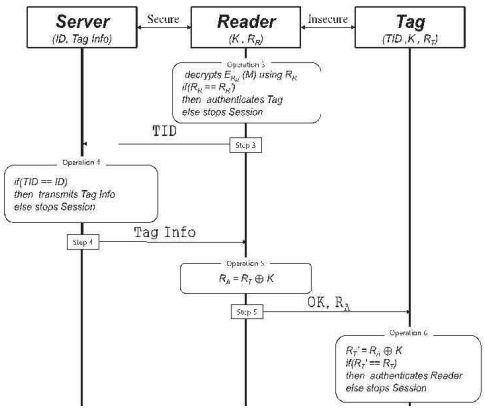

그림 7. 리더 인증
Fig. 7. Reader authentication

리더가 태그를 인증하게 되면 TID를 서버에게 전송한다. TID를 받은 서버는 TID를 DB(Data Base)에서 검색하여 태그 정보를 찾아낸다. TID에 해당되는 ID가 없을 경우 세션은 종료된다. TID가 DB가 저장하고 있는 ID와 동일하면 해당되는 태그의 정보(Tag Info)를 리더에게 전송한다.

```
Step 4.
Server      searches for TID in the DB
:           if(TID = ID)
               transmits Tag Info
            else
               stops session
Server → Reader : Tag Info
```

서버로부터 Tag Info를 받은 리더는 태그의 정보를 획득하고 태그의 난수 RT와 K를 XOR 연산한 RA를 생성하여 OK와 함께 태그에게 전송한다. 태그는 리더에게 RA를 받아 K로 XOR 연산하여 RT'을 얻는다. 이때, RT와 RT'을 비교하여 같으면 리더를 인증하게 된다. 만약 다를 경우 세션을 종료한다.

```
Step 5.
Reader
:           RA = RT⊕K
Reader → Tag : OK, RA
Tag :       RT' = RA⊕K
            if(RT' = RT)
               authenticates reader
            else
               stops session
```

IV. 비교 분석

본 장에서는 기존 프로토콜과 MAPOS의 보안성 및 효율성을 비교 분석한다.

1. 기존 프로토콜과의 연산량 비교

표 2는 기존 프로토콜과 제안 프로토콜의 연산량을 표로 나타낸 것이다. M. Feldhofer의 프로토콜은 연산량에서 우수함을 볼 수 있지만, 2장에서 언급한바와 같이 보안 측면에 많은 문제점이 있다. Toiruul의 프로토콜은 태그와 서버에 XOR 연산과 암·복호화가 많은 점은 시스템에 부하를 줄 수 있으며, 인증 과정이 완벽하지 않아 서버에 m번의 연산을 한다는 점은 공격자에게 DoS(Denial of Service) 공격을 할 수 있는 여지를 주고 있다. M. F. Barak의 프로토콜은 많은 암·복호화 키를 보유하여 안전성 측면에서 우수하지만 많은 연산량은 RFID 시스템에 부하를 주며, 여러 개의 대칭키를 관리하지 않기 때문에 보안 정책에 맞지 않는다. S. Oh 프로토콜은 서버에서 태그 ID를 찾는 과정만 있어 서버의 부하를 최소화 하지만 다수의 태그를 읽어야 하는 리더에 부담이 크며, 수동형 태그에 암·복화 가능한 AES 연산기를 구현해야하므로 태그의 게이트 수가 늘어나게 된다.

표 2. RFID 프로토콜의 연산량 분석
Table 2. The Computation Analysis of RFID Protocols

프로토콜 / 항목	M. Feldhofer's Protocol	Toiruul's Protocol	M. F. Barak's Protocol	S. Oh's Protocol	MAPOS
태그 난수 생성	1	-	1	1	1
리더 난수 생성	2	-	1	1	1
서버 난수 생성	-	-	1	-	-
태그 XOR 연산	-	4	-	2	2
리더 XOR 연산	-	-	-	2	2
서버 XOR 연산	-	4	-	-	-
태그 암·복호화	2	2	2	3	1
리더 암·복호화	2	-	7	3	1
서버 암·복호화	-	2	5	-	-
서버 연산량	-	m번	m-n번	m-n번	m-n번

m : 리더가 인식할 수 있는 범위의 태그 수
n : 불법태그 수

2. 기존 프로토콜의 보안 분석

표 3는 본 논문에서 제안한 프로토콜과 기존 연구된 프로토콜을 보안 분석한 자료이다. M. Feldhofer의 프로토콜의 경우 리더와 태그 간 전송되는 데이터를 AES로 암호화하였기 때문에 도청 공격에 안전하지만, 노출된 난수 값을 태그에게 연속적으로 보내게 되면 동일한 응답 값으로 태그의 위치를 추적할 수 있다. 그리고 리더와 태그 사이의 모든 데이터를 도청 공격으로 획득하여 태그에게 스푸핑 공격, 재전송 공격하여 태그의 정보를 획득할 수 있다. Toiruul의 프로토콜의 경우도 AES를 이용한 상호 인증을 수행하여 다양한 공격에 안전하지만, 서버와 태그가 수행하는 키 갱신 과정은 키에 대한 비동기화 공격으로 시스템 전체가 무너지는 사태가 발생할 수 있다. M. F. Mubarak의 프로토콜은 다양한 암호화

키와 ID를 사용하여 여러 유형의 공격에 안전하지만, 태그의 고정된 응답 값으로 위치 추적을 방어할 수 없다. 그리고 많은 양의 연산량과 키 관리는 RFID 시스템의 효율성 측면에서 매우 좋지 못하다. S. Oh의 프로토콜은 일회성 난수를 상호인증 과정에서 비교하기 때문에 스푸핑 공격, 재전송 공격을 사전에 방어하고, AES로 암·복호화시 일회성 난수를 사용하기 때문에 대칭키 기반의 암호화기법의 문제점인 고정된 키 사용을 해결하지만 태그에 많은 암·복호화 과정은 수동형 태그에서의 효율성은 낮다. 이는 표 2의 결과와 같이 S. Oh 프로토콜의 리더와 태그의 암·복호화가 각각 3회이고, 제안 프로토콜의 리더와 태그의 암·복호화가 1회로 제안 프로토콜이 개선되었다.

표 3. RFID 프로토콜의 보안 분석
Table 3. The Security Analysis of RFID Protocols

프로토콜 / 항목	M. Feldhofer's Protocol	Tsiu's Protocol	M.F. Mubarak's Protocol	S. Oh's Protocol	MAPOS
도청	안전	안전	안전	안전	안전
위치 추적	취약	안전	취약	안전	안전
스푸핑 공격	취약	안전	취약	안전	안전
재전송 공격	취약	안전	안전	안전	안전
대칭키	고정	고정	고정	가변	가변
키전송	-	-	-	취약	안전

3. 제안 프로토콜의 보안 및 효율성 분석

본 절에서는 RFID 시스템에 대해 공격자가 취할 수 있는 공격 유형을 토대로 제안 프로토콜의 보안 및 효율성 대해서 기술한다.

3.1 도청 공격(Eavesdropping Attack)

리더와 태그 간의 데이터 전송은 무선 채널 상에서의 데이터 전송으로 공격자에게 도청 공격을 받을 수 있다. 하지만 제안 프로토콜의 경우 가장 완벽한 암호화 기법인 OTP를 사용하기 때문에, 평문을 복호화 할 수 없고 비밀키를 획득 할 수 없다. 또한 AES를 이용한 암호화된 데이터는 안전하게 암호화되어 공격자가 알 수 없는 값이며, 대칭키의 근본적 문제인 고정된 키 사용을 일회성 난수로 대체하여 공격자의 복호화 가능성은 매우 희박하다.

3.2 위치 추적(Location Tracking)

위치 추적은 공격자가 태그에게 동일한 요청을 하여 동일한 응답 값이 전송되는 것을 이용한 공격법이다. 이는 태그의 응답 값을 매 세션 가변적인 값으로 방어 할 수 있다. 제안 프로토콜의 경우 리더의 난수와 태그의 난수를 포함하여 보내기 때문에 항상 가변적인 값이다. 그러므로 공격자가 동일한 요청에 의한 위치 추적 공격은 안전하다.

3.3 스푸핑 공격(Spoofing Attack)

스푸핑 공격은 정당하지 않은 리더나 태그가 정당한 것처럼 속여 인증을 통과하는 공격법이다. 상호 인증을 하지 않는 프로토콜의 경우, 스푸핑 공격에 취약할 수 있다. 제안 프로토콜은 OTP로 안전하게 암호화된 RR과 RR'의 비교를 통해 상호인증 과정을 거치므로 스푸핑 공격에 안전하다.

3.4 재전송 공격(Replay Attack)

재전송 공격은 도청 공격으로 획득한 데이터를 재전송하여 인증 과정을 통과하고 태그의 정보를 획득하는 것을 말한다. 제안 프로토콜은 인증과정과 가변적인 데이터를 생성하기 위한 리더난수, 태그난수가 포함되어 재전송 공격에 안전하다.

3.5 효율성 및 서버 연산량

해시 함수를 사용할 경우 하드웨어적 큰 부담이 있기 때문에 수동형 태그에 부적합하다. 그러나 본 논문에서는 수동형 태그에 적합함이 입증된 AES 알고리즘을 사용하고, 표2에서와 같이 제안 프로토콜의 인증과정과 전송 데이터량을 최소화하고, 태그에서 복호화 연산이 필요없어 태그 하드웨어 오버헤드를 태그당 3,595게이트로 S.Oh프로토콜 3,992게이트보다 줄여 효율성 면에서 상대적으로 우수하다. 뿐만 아니라 인증과정을 통과해야 태그의 TID가 서버에 전달되어 서버의 DB에서 태그의 정보를 찾기 때문에 불법 태그의 접근을 막을 수 있다. 리더가 인식할 수 있는 범위의 전체 태그의 수를 m개, 그 중 불법 태그의 수를 n개가 존재한다면, 불법 태그는 인증 과정을 통과하지 못하므로 서버에 TID가 전달되는 태그의 수는 m-n개이다. 이는 서버에 대한 DoS 공격에 매우 안전하다.

V. 결 론

최근 바코드 대체 기술로 RFID 기술이 각광 받고 있다. 그러나 RFID 시스템의 특성상 무선 채널을 이용하기 때문에

도청, 위치 추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격 등에 취약하다. 이를 해결하고자 해시 함수, 대칭키 알고리즘, 상호인증과 같은 기법들이 연구되고 있다. 수동형 RFID 태그의 경우 매우 제한된 자원을 가지기 때문에 해시 기반의 프로토콜은 현실적으로 사용이 불가능한 시점이다. 그러나, M. Feldhofer, 구본석, Mark Jung 등에 의해 AES를 4,000 게이트 미만으로 구현하여 수동형 태그에 적합함을 입증하였다. 그렇지만 대칭키 암호화의 근본적인 키 분배 문제로 키가 노출되고 모든 시스템이 공격되는 결정적인 단점이 있다.

본 논문에서는 기존 프로토콜과 달리 OTP 기법을 이용하여 S. Oh 프로토콜에서 단순히 마스크와 XOR하는 방법보다 리더와 태그 간 교환되는 일회성 난수를 더 안전하게 전달한다. 안전하게 전달된 리더의 일회성 난수는 AES로 암호화할 때 암호화키로 사용하여 대칭키의 고정된 키를 사용하는 문제점을 보완하였다. 그리고 리더의 일회성 난수를 활용한 상호 인증 기법은 스푸핑 공격, 재전송 공격에 안전하고, 리더와 태그의 난수를 포함하여 암호화하기 때문에 항상 가변적인 값으로 위치추적에 안전하다.

제안 프로토콜은 리더에서 태그 인증하여 불법 태그를 사전에 차단하는 과정과 인증 후 서버에서 정당한 태그 정보를 검색하는 과정은 서버의 부하를 최소화하여 서버에 대한 DoS 공격을 방어할 수 있다.

S. Oh 프로토콜과 비교하여 태그, 리더상의 암복호화를 각각 3회에서 1회로 감소시켰고, 태그상에서 복호화할 필요가 없어 수동형 태그상에 구현할 게이트 수에서 태그당 3,595게이트로 3,992게이트보다 약 10% 감소시켰고, 리더와 태그간 데이터 송수신량에서 태그와 리더간 세션당 384비트로 512비트에 비해 25% 감소시켜 대규모 다중 태그 시스템에서 부하를 줄일 수 있다.

참고문헌

[1] S. Oh, K. Chung, C. Jung, K. Ahn, "An RFID Mutual Authentication Protocol using One-time Random Number," Journal of Security Engineering, Vol. 7, No. 3, June. 2010.

[2] K. Finkenzeller, *"RFID Hand Book: Fundamentals and Applications in Contactless Smart Card and Identification, Second Edition,"* John Wiley & Sons Ltd., July. 2003.

[3] P. H. Cole, *"Fundamentals in RFID part1, Korean RFID course,"* 2006, http://autoidlab.eleceng.adelaide.edu.au/education/FundamentalsInRfidPart1.pdf

[4] M. Feldhofer, S. Dominikus, Rijmen, J. Wolkerstorfer, "Strong Authentication for RFID Systems Using The AES Algorithm," ICCHES, pp. 357-370, August. 2004.

[5] B. Koo, G. Ryu, S. Yang, T. Chang, S. Lee, "Low-cost AES Implementation for RFID tags," Journal of KIISC, Vol. 16, No. 5, pp. 67-77, October. 2006.

[6] M. Jung, Horst Fiedler, and Reneé Lerch, "8-Bit Micrcontroller System with Area Efficient AES Coprocessor for Transponder Application," Workshop on RFID and Lightweight Crypto, pp. 32-43, July. 2005.

[7] J. Ha, J. Park, J. Ha, H. Kim, S. Moon, "Low-cost Authentication Protocol Using Pre-synchronized Search Information in RFID System," Journal of KIISC, Vol. 18, No. 1, pp. 77-87, February. 2008.

[8] J. Daemen, V. Rijmen, *"The Design of Rijndael,"* AES-The Advanced Encryption Standard, Springer-Verlog, Berlin, Heidelberg, New York, March. 2002.

[9] J. Daemen, V. Rijmen, *"AES Proposal: Rijndael, Version2,"* Submission to NIST, March. 1999.

[10] M. Aigner and M. Feldhofer, "Secure Symmetric Authentication for RFID Tags," Telecommunication and mobile computing - TCMC 2005, March. 2005.

[11] B. Toiruul, K. Lee, "An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems," IJCSNS, September. 2006.

[12] M. F. Mubarak, J. A. Manan, S. Yahya, "Mutual Attestation Using TPM for Trusted RFID Protocol," In 2nd International Conference on Network Applications, Protocols and Services-NETAPPS 2010, Kedah, Malaysia, September. 2010.

[13] M. F. Mubarak, J. A. Manan, S. Yahya, "A Critical Review on RFID System towards Security, Trust,

and Privacy (STP)," 2011 IEEE 7th International Colloquium on Signal Processing and its Applications, pp. 39-44, March. 2011.
[14] Gilbert S. Vernam, "U.S.Patent 1,310,719. Secret signaling system," July. 1919.
[15] C. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol. 28, pp. 656-715, October. 1949.
[16] Jiao-Hongqiang, Tian-Junfeng, Wang-Baomin, "A Study on the One-Time Pad Scheme Based Stern-Brocot Tree," ISCSCT 2008, pp. 568-571, December. 2008.

저 자 소 개

윤 태 진

1994: 경북대학교 컴퓨터공학과 공학사
1996: 경북대학교 컴퓨터공학과 공학석사
1998: 경북대학교 컴퓨터공학과 박사수료
현 재: 경운대학교 모바일공학과 교수
관심분야: 정보보안, 임베디드시스템
Email : tjyun@ikw.ac.kr

오 세 진

2009: 경운대학교 컴퓨터공학과 공학사
2011: 경북대학교 전자전기컴퓨터학부 공학석사
현 재: 경북대학교 전자전기컴퓨터학부 박사과정
관심분야: 정보보호, 임베디드시스템
Email : 170m3@knu.ac.kr

안 광 선

1972: 연세대학교 전기공학과 공학사
1975: 연세대학교 전기공학과 공학석사
1980: 연세대학교 전기공학과 공학박사
현 재: 경북대학교 컴퓨터학부 교수
관심분야: 정보보호, 임베디드시스템
Email : gsahn@knu.ac.kr