시프트 연산과 난수를 이용한 가변적 대칭키 기반의 RFID 상호인증 프로토콜

정회원 이 재 강*, 준회원 오 세 진*, 정회원 정 경 호**, 이 창 희***, 안 광 선*°

RFID Mutual Authentication Protocol Using Nonfixed Symmetric Key Based on Shift Computation and Random Number

Jaekang Lee* *Regular Member*, Sejin Oh* *Associate Member*,
Kyungho Chung**, Changhee Lee***, Kwangseon Ahn*° *Regular Members*

요 약

RFID 시스템은 무선 주파수를 이용하여 태그의 정보를 얻는 기술이다. 그러나 무선 주파수를 이용하는 특성으로 도청, 위치추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격에 취약하다. 그래서 RFID 프로토콜이 안전하고 프라이버시를 위해 암호학적 기법과 상호인증 기법이 사용되어 진다. 본 논문에서는 기존의 프로토콜의 문제점을 알아보고, 다양한 공격에 안전한 프로토콜을 제안한다. 뿐만 아니라 시프트 연산과 난수를 이용한 가변적 대칭키 생성으로 비밀키에 대한 문제점을 해결한다.

Key Words : RFID, Authentication, Protocol, AES, Shift

ABSTRACT

RFID system is a technique to obtain information of tag using radio frequency. Specificity of RFID systems using radio frequency has many problems that is eavesdropping, location tracking, spoofing attack, replay attack, denial of service attack. So, RFID protocol should be used cryptographic methods and mutual authentication for security and privacy. In this paper, we explain the problem of past protocol and propose the nonfixed symmetric key-based RFID mutual authentication protocol using shift computation and random number. Proposed protocol is secure from various attacks. Because it use shift operation and non-fixed symmetric key.

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 유비쿼터스 컴퓨팅 환경에서 핵심기술로 여겨지고 있다. RFID 시스템의 구성요소는 리더(Reader), 태그(Tag), 서버(Server)로 구성되어 있으며, 리더가 브로드 캐스트 한 신호를 태그가 수신하여 태그의 정보를 리더에게 전송하고, 태그의 정보를 서버의 데이터베이스에서 검색하는 구조로 되어있다. 그러나 무선 주파수를 이용하는 특성으로 인해 도청, 위치추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격 등에 매우 취약하다[1-5]. 이러한 문제점을 해결하기위해 상호인증, AES, 해시함수, 공개키 암호화 알고리즘과 같은 다양한 연구가 활발히 진행되고 있다. 본 논문에서는 기존의 프로토콜 고찰로 다양한 공격에 방어할 수 있는 방안을 모색하고, 효율성과 안전성을 보장하는 RFID 상호인증 프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는

* 경북대학교 전자전기컴퓨터학부 임베디드 시스템 연구실({10004oke, 170m3, gsahn}@knu.ac.kr), (° : 교신저자)
** 경운대학교 컴퓨터공학과(mccart@ikw.ac.kr), *** 계명문화대학 컴퓨터학부(chlee2k@live.co.kr)
논문번호 : KICS2011-12-640, 접수일자 : 2011년 12월 29일, 최종논문접수일자 : 2012년 4월 24일

관련연구로써 RFID 시스템의 공격유형에 따른 보안 요구사항과 AES, 해시함수 기반의 기존 프로토콜에 대해 알아본다. 3장에서는 제안하는 프로토콜을 상세히 기술하고, 4장에서는 기존 프로토콜과 제안프로토콜과의 비교분석을 한다. 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

RFID 시스템의 리더와 태그는 안전하지 않은 통신채널에서 데이터를 전송하기 때문에 다양한 공격에 취약하다. 본 장에서는 다양한 공격유형에 따른 보안 요구사항을 알아보며, Toiruul과 고훈 프로토콜을 예로 들어 RFID 프로토콜 설계 시 키 업데이트와 상호인증이 보안상에서 얼마나 중요한지를 살펴본다.

2.1. 공격 유형에 따른 보안 요구사항

2.1.1. 도청공격

도청공격은 공격자가 리더와 태그 간에 송·수신되는 데이터를 획득하여 태그의 고유 식별정보(ID)를 획득하는 공격이다. 이를 해결하기 위해서는 암호학적 기법을 사용하여 공격자가 도청공격으로 데이터를 획득하더라도 알 수 없거나 의미 없는 값이어야 한다.

2.1.2. 위치추적

위치추적은 리더의 연속적인 요청에 태그의 동일한 응답 값으로 태그의 위치를 추적하는 공격법이다. 공격자는 위치추적으로 태그를 소지한 개인의 위치 또는 이동경로를 알 수 있게 되는 문제점이 있다. 그러나 태그의 응답을 항상 가변적으로 하여 위치추적을 손쉽게 해결할 수 있다.

2.1.3. 스푸핑 공격

스푸핑 공격은 정당한 리더 또는 태그로 위장하여 인증절차를 통과하는 공격법이다. 따라서 공격자는 정상적인 태그인척 위장하여 정상 리더를 속일 수 있다. 하지만 상호 인증 과정을 통하여 정당성 유무를 판별한다면 해결할 수 있다.

2.1.4. 재전송 공격

재전송 공격은 리더의 요청에 대한 태그의 고유 식별 정보를 도청한 후 리더의 요청에 대해 공격자는 정당한 태그로 가장하여 도청한 정보로 요청·응답하는 것이다. 그러나 리더와 태그 간 송·수신되는 데이터를 가변적으로 처리하고 인증과정을 거친다면 방어할 수 있다.

2.1.5. 서비스 거부 공격

서비스 거부 공격은 공격자가 서버 또는 리더, 태그에게 많은 양의 요청 명령으로 인한 부하 또는 스푸핑 공격과 재전송 공격으로 인한 인증절차를 통과하여 강제 키 업데이트와 같은 공격으로 이루어 질 수 있다. 그러므로 상호 인증을 통해 사전에 공격자를 차단하여야한다.

2.2. Toiruul 등이 제안한 프로토콜

Toiruul 등은 대칭키의 문제점인 고정된 키 문제를 해결하고자3개의 비밀키를 이용한 AES 기반의 상호인증 프로토콜을 제안하였다[6]. 3개의 비밀키의 $K, K1, K2$는 서버와 태그사이 공유하는 암호키이고 모든 태그에 동일하게 저장되어 있다. 인증 과정은 그림 1과 같다.

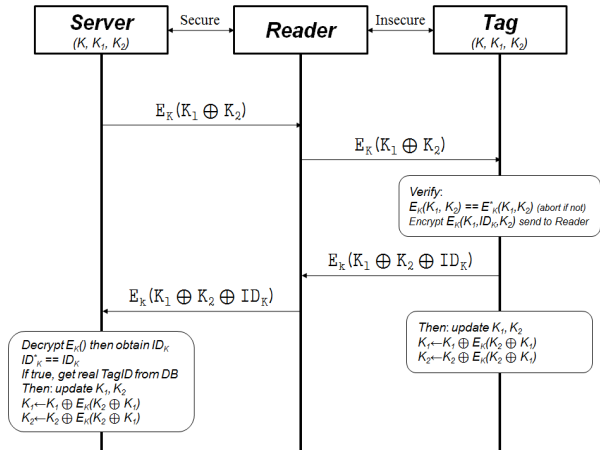


그림 1. Toiruul 프로토콜
Fig. 1. Toirull's Protocol

1 단계 : 서버는 $K1$과 $K2$를 XOR연산하고 대칭키 K를 사용하여 AES로 암호화한 $E_K(K_1 \oplus K_2)$를 리더에게 전송한다.

2 단계 : 리더는 $E_K(K_1 \oplus K_2)$를 서버에게 전송받아 태그에게 전송한다. $E_K(K_1 \oplus K_2)$를 받은 태그는 태그가 가진 K, K_1, K_2로 서버가 생성한 $E_K(K_1 \oplus K_2)$와 동일한 연산을 수행하여, 두 값이 같으면 태그는 리더를 인증한다. 만약 값이 다를 경우 공격자로 간주하여 통신을 종료한다.

3 단계 : 리더 인증이 성공하였을 경우, 태그는 K_1, K_2, ID_K를 XOR연산하여 K로 암호화한 $E_K(K_1 \oplus K_2 \oplus ID_K)$를 생성하여 리더에게 전송한다. 그리고 태그는 K_1과 K_2를 업데이트한다.

4 단계 : 리더는 $E_K(K_1 \oplus K_2 \oplus ID_K)$를 태그에게 전송받아 서버에게 전달한다. $E_K(K_1 \oplus K_2 \oplus ID_K)$를 받은 서버는 태그와 같이 연산하여 동일한 값이 나타날 경우 태그를 인증하게 된다. 그리고 인증이 성공하였을 경우 서버는 K_1과 K_2를 업데이트한다.

Toiruul 프로토콜은 키 업데이트로 인하여 다른 정당한 태그가 통신을 못하는 상황이 발생한다. 정당한 태그1이 정상적으로 통신하여 키가 업데이트 된 후, 태그2가 리더와 통신하게 되면, 키 값은 바뀌어 져있기 때문에 인증에서 실패하게 된다. 이는 키 업데이트로 인하여 정당한 태그임에도 불구하고 스스로 서비스 거부 공격을 자초하게 된다.

2.3. 고훈 프로토콜

고훈 등은 Henrici and Muller가 제안한 해시기반 인증 프로토콜의 위치추적, 스푸핑 공격, 재전송 공격에 취약함을 입증하고 문제점을 개선한 프로토콜을 그림 2와 같이 제안하였다[7]. 인증 과정은 다음과 같다.

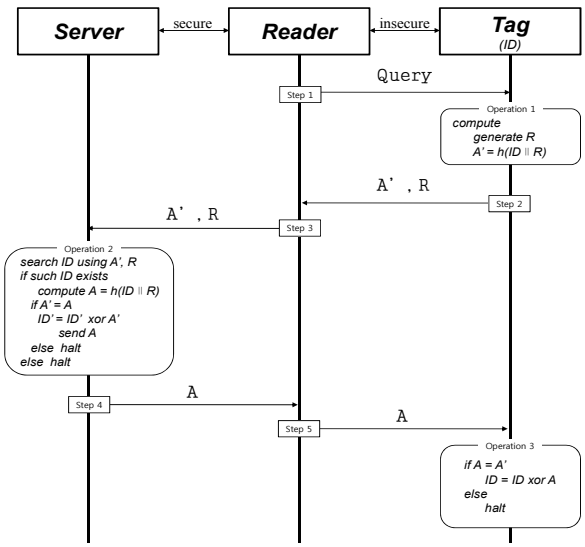


그림 2. 고훈 프로토콜
Fig. 2. Ko's Protocol

1 단계 : 리더는 태그에서 Query를 전송한다.

2 단계 : Query를 전송 받은 태그는 난수 R을 생성하여 태그 고유 식별 정보 ID와 연접하여 해시한 A'과 R을 리더에게 전송한다.

3 단계 : A', R을 받은 리더는 서버에게 전송한다.

4 단계 : A' R을 받은 DB는 DB에 저장된 모든 ID와 태그난수 R을 연접하여 해시 연산한 A'에 대해 검증한다. 검증과정을 통과 하였을 때, ID를 A'과 XOR 연산하여 갱신하고 DB가 생성한 A를 리더에게 전송한다.

5 단계 : 리더는 DB가 전송한 A를 태그에게 전송한다. A를 받은 태그는 A에 대한 검증을 수행하고, ID를 갱신한다.

고훈 프로토콜은 서버에서 전송된 A'이 전 방향 보안성을 충족하지 않기 때문에 재전송 공격으로 인한 태그의 ID 강제로 변경시킬 수 있다. 방법은 다음과 같다.

공격 1 단계 : 공격자가 정상적인 모든 태그에게 Query를 전송하여 A', R를 전송받는다.

공격 2 단계 : 공격자는 정상적인 모든 태그에게 받은 A'을 재전송 한다.

공격 3 단계 : 정상적인 태그는 공격자가 보낸 A'과 태그가 생성한 A'이 같으므로 ID를 갱신한다.

공격 4 단계 : ID가 갱신된 후 정상적인 리더와 태그는 인증 과정에서 실패하게 되고, 공격자는 재전송 공격을 이용한 서비스 거부 공격을 성공하게 된다.

Ⅲ. 제안 프로토콜

본 장에서는 RFID시스템의 다양한 공격에 안전하고 대칭키, 키 업데이트의 문제를 해결한 프로토콜을 제안한다. 제안 프로토콜은 세션키 생성, 가정사항 및 표기법, RFID 프로토콜의 태그인증, 리더 인증과 태그정보획득 단계로 구성된다.

3.1. 세션키 생성

본 논문에서 제안하는 프로토콜은 매 세션 새로운 비밀키를 생성한다. 비밀키는 리더의 난수 Rr의 상위 7 비트에 의해 생성된다. 그림 3은 비밀키 생성 과정을 나타낸 것이다.

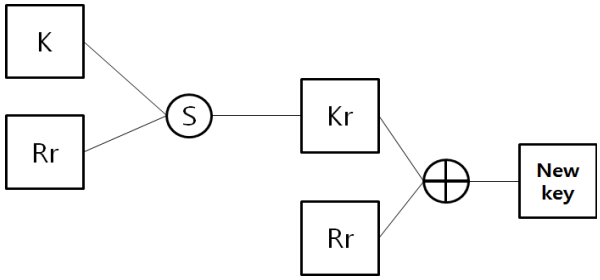


그림 3. 비밀키 생성 과정
Fig. 3. The Process of Generating Secret Key

대칭키 K는 리더의 난수 Rr의 상위 7비트의 값을 이용하여 시프트 연산한 Kr을 생성하고, Kr과 Rr을 XOR 연산하여 새로운 비밀키를 생성하게 된다. Rr의 상위 7 비트에 의한 시프트 연산 과정은 그림 4와 같다.

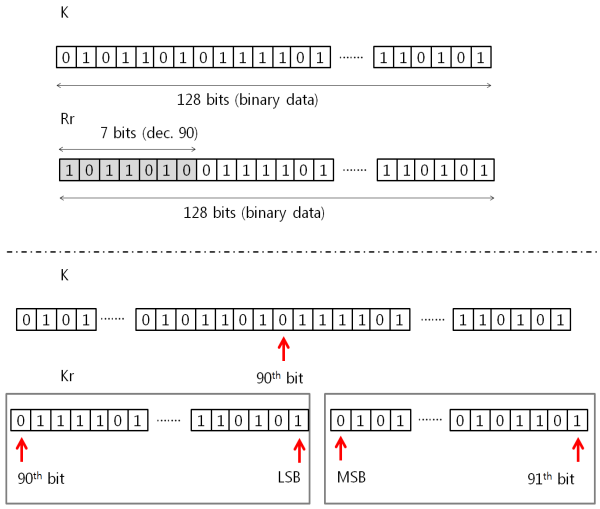


그림 4. Shift 연산
Fig. 4. The Shift Operation

시프트 연산은 리더의 난수의 상위 7비트의 2진수 값을 10진수로 변환한 값을 K의 시프트 기준 비트로 선정한다. 선정된 비트를 최상위 비트까지 왼쪽 시프트 연산한다. 그리고 기준비트의 좌변 비트들을 시프트 연산한 비트의 우변으로 위치시킨다. 이렇게 시프트 연산된 Kr을 난수 Rr과 XOR 연산을 수행하여 새로운 비밀키를 생성한다.

3.2. 가정 사항 및 표기법

제안 프로토콜의 가정 사항은 다음과 같고 표 1은 제안 프로토콜의 표기법을 나타낸 것이다.

표 1. 표기법
Table 1. The Notations

표기법	내용
ID	태그의 고유 식별 값
Rr	리더에서 생성한 난수
Rt	태그에서 생성한 난수
K	대칭키
Kr	Shift() 함수를 이용한 변환키
‖	연접 연산자
⊕	eXclusive-OR (XOR) 연산
E()	AES 블록 암호문
Shift()	키 변환 함수

1) 서버와 리더 사이는 안전한 통신 채널이며 공격자의 공격에 안전하다.
2) 리더와 태그 사이는 무선 상의 통신 채널이며 공격자의 공격에 취약하다.
3) 모든 태그에는 각각 자신의 고유 식별 정보 ID를 저장하고 있다.
4) 리더와 태그는 난수를 생성할 수 있다.
5) 리더와 태그는 대칭키 기반의 AES 암호화 연산 및 XOR 연산이 가능하다.
6) 리더는 AES 복호화 연산이 가능하다.
7) 리더와 태그가 생성한 난수는 처음 세션이 연결될 때 마다 새로이 생성된다.

3.3. 제안 프로토콜

본 논문에서는 AES 알고리즘을 기반으로 고정된 비밀키 문제와 키 갱신에서의 서비스 거부 공격의 문제를 해결하기 위하여 시프트 연산을 설계하였다. 제안 프로토콜의 전체 구성은 태그인증, 리더인증, 태그 정보 획득으로 구성되어 있다. 그림 5는 본 논문에서 제안한 프로토콜이다.

3.3.1. 태그 인증 단계

상호 인증 과정 중 태그 인증 단계는 리더가 태그에게 Query(질의)를 보내면서 시작된다. 그림 5의 (a)태그인증 영역이 태그 인증 단계를 나타낸 것이다.

1) Operation 1.

초기 질의 단계에서 리더는 난수 Rr를 생성한다. 그리고 $Query$와 Rr을 태그에게 함께 전송한다.

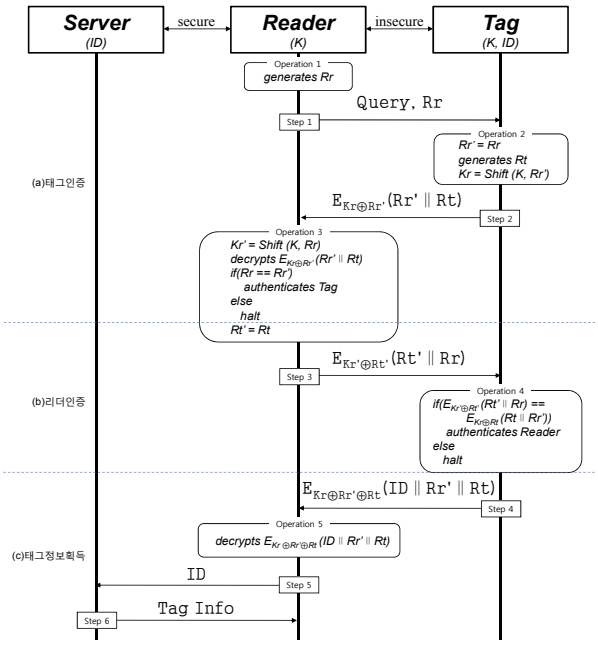


그림 5. 제안 프로토콜
Fig. 5. The Proposed Protocol

2) Operation 2.

태그는 리더로 부터 받은 Rr'과 K를 $Shift(K, Rr')$연산을 통하여 Kr을 생성한다. 그리고 리더로 받은 Rr'과 태그가 생성한 난수 Rt를 연접하고 $Kr \oplus Rr'$한 키를 사용하여 AES로 암호화 한다. AES로 암호화한 $E_{Kr \oplus Rr'}(Rr' \parallel Rt)$ 값을 리더에게 전송한다.

3) Operation 3.

Operation 3에서는 리더가 태그로 받은 $E_{Kr \oplus Rr'}(Rr' \parallel Rt)$를 복호화해서 정상적인 태그인지 검증하는 단계이다. 리더는 K, Rr를 $Shift(K, Rr)$연산을 통하여 Kr'를 생성하고 $Kr' \oplus Rr$을 사용해 $E_{Kr \oplus Rr'}(Rr' \parallel Rt)$를 복호화하여 Rr', Rt'를 획득한다. 이때 리더의 Rr과 Rr'이 같을 경우 태그를 인증하고, 만약 다를 경우 공격자로 간주하여 세션을 종료한다.

3.3.2. 리더 인증 단계

태그 인증이 성공적으로 수행될 경우 리더 인증 단계가 진행된다. 그림 5의 (b)리더인증 영역이 리더 인증 단계를 나타낸 것이다.

1) Operation 3.

Operation 3에서 태그 인증 과정이 완료되면 리더가 생성한 Kr'과 Rt'을 XOR연산한 값을 암호화 키로 사용한다. 그리고 Rr과 Rt를 연접하고, $Kr' \oplus Rt'$키로 AES 암호화한 $E_{Kr' \oplus Rt'}(Rt' \parallel Rr)$를 Step 3와 같이 태그에게 전송한다.

2) Operation 4.

리더에게 $E_{Kr' \oplus Rt'}(Rt' \parallel Rr)$를 받은 태그는 $E_{Kr \oplus Rt}(Rt \parallel Rr')$를 생성하여 비교한다. $E_{Kr' \oplus Rt'}(Rt' \parallel Rr)$과 $E_{Kr \oplus Rt}(Rt \parallel Rr')$이 같을 경우 리더를 인증하고, 만약 다를 경우 공격자로 간주하여 세션을 종료한다.

3.3.3. 태그의 정보 획득 단계

그림 5의 (c)태그정보획득이 다음 과정을 나타낸 것이다.

1) Operation 4.

리더 인증이 완료되고 태그는 리더에게 태그의 고유 식별 정보 ID를 전달하는 과정을 진행한다. 태그는 ID, Rr', Rt를 연접하여 암호화 한다. 태그는 $Kr \oplus Rr' \oplus Rt$를 암호키로 사용하여, Step 4와 같이 $E_{Kr \oplus Rr' \oplus Rt}(ID \parallel Rr' \parallel Rt)$를 리더에게 전송한다.

2) Operation 5.

태그로부터 $E_{Kr \oplus Rr' \oplus Rt}(ID \parallel Rr' \parallel Rt)$를 전송받은 리더는 $Kr' \oplus Rr \oplus Rt'$키로 복호화여 태그의 고유 식별 정보 ID를 서버에게 전달한다. 서버는 리더로부터 받은 태그의 ID를 데이터베이스에서 검색하여 얻은 결과 값 Tag Info를 리더에게 전송하고 완료된다.

Ⅳ. 비교 분석

본 장에서는 기존 프로토콜과 제안 프로토콜의 보안성 및 효율성을 비교 분석한다.

4.1. 보안성 분석

AES와 대칭키 $K, K1, K2$를 이용한 Toiruul의 프로토콜은 AES 암호화 알고리즘을 사용하기 때문에 공격자가 도청공격으로 리더와 태그사이의 데이터를 획득하더라도 알 수 없는 값이기 때문에 도청

공격에 안전하다. 그러나 도청 공격으로 획득한 데이터를 태그에게 무차별적으로 요청한다면, 그에 대한 동일한 응답 값으로 위치추적을 할 수 있다. 또한 2장에서 알아본바와 같이 키 업데이트의 문제로 스푸핑 공격, 재전송 공격, 서비스 거부 공격이 이루어지는 점은 프로토콜 설계 자체의 문제로 보여진다.

고훈의 프로토콜은 해시함수와 리더의 난수를 이용하여, 다양한 공격에 안전하다고 주장한다. 그러나 정상적인 리더로 위장하여 정상적인 모든 태그에게 Query를 전송하여, 각 태그의 A', R 응답을 받아 A'을 재전송 공격할 경우 모든 태그의 ID가 갱신되는 문제점이 발생하게 된다. 이러한 문제점은 공격자가 재전송 공격을 통한 서비스 거부 공격이 가능하다. EPC Global Class1 Gen2의 경우 태그의 ID는 96비트이다. 앞서 설명한 공격으로 A'와 R를 이용하여 96비트에 대한 전수조사로 태그의 ID를 획득할 수 있는 큰 문제점을 지니고 있다.

본 논문에서 제안한 프로토콜은 AES와 리더, 태그의 난수를 이용하여 암호화하기 때문에 위치추적에 안전하며, 암호화된 데이터의 일부를 상호인증 과정을 하기 때문에 스푸핑 공격, 재전송 공격, 서비스 거부 공격에 매우 안전하다. 또한 시프트연산과 난수를 이용한 새로운 대칭키를 생성하는 점은 다수의 태그와의 동기화를 유지하고, 대칭키 알고리즘의 고정된 키 사용의 문제점을 해결하는 장점을 가지고 있다. 표 2는 기존 프로토콜과 제안 프로토콜의 보안성 측면에서의 비교 분석한 내용이다.

표 2. RFID 프로토콜의 보안 분석
Table 2. The Security Analysis of RFID Protocols

프로토콜 / 공격유형	Toiruul 프로토콜	고훈 프로토콜	제안 프로토콜
도청공격	안전	취약	안전
위치추적	취약	안전	안전
스푸핑 공격	취약	취약	안전
재전송 공격	취약	취약	안전
서비스 거부 공격	취약	취약	안전
상호인증	불만족	불만족	만족
기타	키 업데이트 의미 없음	무선 상의 노출된 A'을 재전송 공격하여 ID를 강제 업데이트 가능	시프트 연산과 난수를 이용한 가변적 대칭키 생성

4.2. 효율성 분석

Toiruul이 제안한 프로토콜은 난수를 사용하지 않기 때문에 난수 생성에 대한 효율성은 높다. 그러나 난수 대신 비밀키 K, K_1, K_2를 사용하기 때문에 키 관리에 대한 문제점이 발생하게 된다. 또한 상호인증을 수행함에도 불구하고 서버에서 DB검색 시 불법 태그의 요청에도 다양한 연산을 수행하는 문제는 올바른 상호인증이 아님을 입증하며, 효율성 높은 프로토콜이라고 판단할 수 없다.

고훈 프로토콜은 태그에서 1회의 해시연산으로 해시기반의 프로토콜 중에서 태그에 대한 효율성이 매우 높다. 하지만 4.1절에서 언급한바와 같이 공격자가 ID를 획득하기 때문에 서버에서 불법 태그를 포함한 해시연산이 이루어지는 점은 물론 불법 태그가 정상적인 통신이 가능하기 때문에 보안을 고려하지 않고 효율성만을 염두하는 점은 바람직하지 못하다. 그러므로 연산량에서는 우수할지라도 보안 측면에서 많은 문제점을 보인 프로토콜이다.

제안 프로토콜은 고훈 프로토콜에 비해 연산량이 많은 점은 있지만 리더와 태그 간 안전하게 상호인증 후 태그의 ID를 서버에게 전달하기 때문에, 서버에 대한 부하가 상당히 적다. 그리고 대칭키 암호화 알고리즘을 사용하는 프로토콜은 고정된 키 사용에 대한 문제점을 해결하고자 하는데, 본 논문에서 제안하는 프로토콜은 Toiruul 프로토콜과 달리 고정된 비밀키 K를 난수 값에 의한 시프트 연산과 XOR 연산으로 새로운 대칭키를 생성하기 때문에 키 관리 측면에서 우수하다. 표 3은 기존 프로토콜과 제안 프로토콜의 효율성 분석을 표로 나타낸 것이다.

4.3. 기존 대칭키 기반의 RFID 프로토콜과의 특성 비교

RFID 시스템의 이슈화와 더불어 보안 및 개인 프라이버시의 문제의 대두화로 다양한 대칭키 기반의 RFID 프로토콜이 제안되었다. 본 절에서는 다양한 대칭키 기반의 RFID 인증 프로토콜과 제안 프로토콜과의 특성을 표 4와 같이 비교하였다.

대칭키 기반의 RFID 인증 프로토콜은 M. Feldhofer 등이 RFID 태그에 적용이 가능한 AES 알고리즘과 상호인증 프로토콜제안을 시작으로 발전하였다. 모든 태그에 동일한 키를 가지는 대칭키는 사용에서의 편리함과 고정된 키 사용으로 보안의 문제점을 지니고 있다.

표 3. RFID 프로토콜의 효율성 분석
Table 3. The Computation Analysis of RFID Protocols

내용 \ 프로토콜	Toiruul 프로토콜	고훈 프로토콜	제안 프로토콜
태그난수생성	-	1	1
리더난수생성	-	-	1
서버난수생성	-	-	-
태그XOR연산	4	1	3
리더XOR연산	-	-	3
서버XOR연산	4	1	-
태그의 암·복호화 연산	E2	H1	E3
리더의 암·복호화 연산	-	-	E1, D2
서버의 암·복호화 연산	E2	H1	-
비밀키의 수	3	-	1
서버의 DB 검색	$\lceil \frac{m}{2} \rceil$	$\lceil \frac{m}{2} \rceil$	$\lceil \frac{m-n}{2} \rceil$

E: AES 암호화, D: AES 복호화
H: 해시연산, m: 리더 인식 범위의 전체 태그 수
n: 불법 태그의 수

이를 해결하기 위에 많은 사람들이 다수의 키, 가변적 키를 사용하는 프로토콜을 제안하였지만 보안의 문제점을 여전히 지니고 있는 실정이다.

제안 프로토콜의 경우 기존의 프로토콜에 비해 다소 많은 라운드 수, 리더, 태그간의 총 비트 수가 많지만 상호 인증 과정을 거친 후에 태그의 ID를 전송하기 때문에 안전하다. 또한 제안 프로토콜은 보안성 측면을 만족하는 동시에 상호인증을 위한 최소한을 연산을 수행하기 때문에 전체적인 측면에서 효율적이다.

V. 결 론

RFID 시스템은 무선을 이용한 자동인식 기술로 각광 받고 있지만, 무선을 이용하는 특징으로 도청, 위치추적, 스푸핑 공격, 재전송 공격, 서비스 거부 공격과 같은 공격에 매우 취약하다. 최근 AES 알고리즘, 해시 함수를 이용한 상호인증 프로토콜이 연구되고 있는 가운데 키 업데이트로 인한 문제로 RFID 시스템 전체가 공격자의 공격에 취약함을 본 논문에서 알아보았고, 프로토콜 설계 시 보안 요구사항을 기술하였다.

표 4. 기존 대칭키 기반의 RFID 프로토콜과의 특성 비교
Table 4. The Comparison of Symmetric Key-based RFID Protocols

내용 \ 프로토콜	Ref [4]	Ref [5]	Ref [6]	Ref [9]	제안 프로토콜
태그난수생성	1	-	-	1	1
리더난수생성	1	1	-	1	1
서버난수생성	-	-	-	1	-
태그 XOR 연산	-	2	4	-	3
리더 XOR 연산	-	1	-	-	3
서버 XOR 연산	-	1	4	-	-
태그의 암복호화	2	1	2	2	3
리더의 암복호화	2	2	-	7	3
서버의 암복호화	-	1	2	5	-
비밀키의 수 (비밀키의 형태)	1 (고정)	2 (고정)	3 (고정)	4 (일부가변)	1 (가변)
암호 알고리즘	AES	AES	AES	AES	AES
총 라운드 수 (태그정보 획득포함)	6	5	5	7	6
리더, 태그 간 총 송·수신 비트 수	320 bits	288 bits	256 bits	256 bits	416 bits
인증 방법	상호인증	단순인증	상호인증	상호인증	상호인증
보안 사항	취약	취약	취약	취약	안전

본 논문에서는 수동형 RFID 태그에 적합한 AES 알고리즘을 사용하고, 매 세션 새로이 생성되는 비밀키와 리더, 태그의 난수를 이용한 상호인증 프로토콜을 제안하였다. 제안 프로토콜의 비밀키 생성은 리더가 생성하는 난수의 상위 7비트에 의해 시프트 연산이 이루어지고, 시프트 연산한 값과 난수를 XOR하여 각 단계별로 암·복호화 키로 사용하였다. 또한 리더와 태그사이에서 상호인증이 이루어지고 태그의 *ID*를 서버에 전달하여 태그 *ID*에 대한 정보를 데이터베이스에서 검색하기 때문에 기존의 프로토콜에 비해 안전하고 서버에 부하가 매우 적다.

참 고 문 헌

[1] CHES2009, “Workshop on Cryptographic Hardware and Embedded systems”, http://www.chesworkshop.org/, 2009.

[2] 김대중, 전문석, “일회성 난수를 이용한 안전한

RFID 상호인증 프로토콜 설계", *정보과학회논문지*, 제35권, 제3호, pp. 243-250, 2008. 06.
[3] 하재철, 박제훈, 하정훈, 김환구, 문상재, "검색 정보 사전 동기화를 이용한 저비용 RFID 인증 방식", *정보보호학회 논문지*, 제18권, 제1호, pp. 77-87, 2008. 02.
[4] M. Feldhofer, S. Dominikus, Rijmen, J. Wolkerstorfer, "Strong Authentication for RFID Systems Using The AES Algorithm", *ICCHES*, pp. 357-370, 2004.
[5] 이남기, 장태민, 전병찬, 전진오, 유수봉, 강민섭, "AES 암호 프로세서를 이용한 강인한 RFID 인증 프로토콜 설계", *한국정보처리학회 논문집*, 제15권, 제2호, pp.1473-1476, 2008. 11.
[6] B. Toiruul, K. Lee, "An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems," *IJCSNS*, Sep. 2006.
[7] 고훈, 김배현, 권문택, "RFID 환경에서 보안 통신을 위한 안전한 인증 방안에 관한 연구", *정보보안논문지*, 제5권, 제3호, pp. 59-65, 2005. 09.
[8] M. Feldhofer, S. Dominikus, Rijmen, J. Wolkerstorfer, "Strong Authentication for RFID Systems Using The AES Algorithm", *ICCHES*, pp. 357-370, 2004.
[9] 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, Sep. 2010.

이 재 강 (Jaekang Lee) 정회원

2002년 2월 가야대학교 컴퓨터공학과 학사
2005년 8월 경북대학교 컴퓨터공학과 석사
2009년 3월~현재 경북대학교 전자전기컴퓨터학부 박사과정
<관심분야> 임베디드 시스템, RFID, 리눅스 파일시스템, 정보보호

오 세 진 (Sejin Oh) 준회원

2009년 2월 경운대학교 컴퓨터공학과 학사
2011년 2월 경북대학교 전자전기컴퓨터학부 석사
2011년 3월~현재 경북대학교 전자전기컴퓨터학부 박사과정
<관심분야> RFID, 충돌방지, 정보보호, 프로토콜, 임베디드 시스템

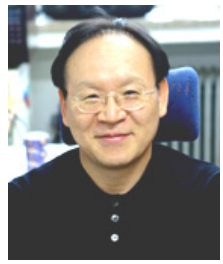
정 경 호 (Kyungho Chung) 정회원

2000년 2월 대구대학교 컴퓨터정보공학과 학사
2002년 2월 경북대학교 컴퓨터공학과 석사
2011년 2월 경북대학교 컴퓨터공학과 박사
2005년 3월~현재 경운대학교 컴퓨터공학과 교수
<관심분야> 임베디드 시스템, RFID, 정보보호

이 창 희 (Changhee Lee) 정회원

1992년 2월 경북대학교 컴퓨터공학과 학사
1994년 2월 경북대학교 컴퓨터공학과 석사
1998년 8월 경북대학교 컴퓨터공학과 박사
1998년 9월~현재 계명문화대학 컴퓨터학부 교수
<관심분야> RFID, 임베디드 시스템, 시험구조

안 광 선 (Kwangseon Ahn) 정회원



1972년 2월 연세대학교 전기공학과 학사
1975년 2월 연세대학교 전자공학과 석사
1980년 2월 연세대학교 전자공학과 박사
1977년 3월~현재 경북대학교 컴퓨터공학과 교수
<관심분야> 임베디드 시스템 설계, RFID