논문 2011-4-9

# AES 알고리즘을 이용한 수동형 태그의 RFID 보안 강화 프로토콜에 관한 연구

# A Study On RFID Security Enhancement Protocol Of Passive Tag Using AES Algorithm

김창복*, 김남일**

**Chang-Bok Kim, Nam-Il Kim**

**요 약** 최근 수동형 태그에 적용 가능한 경량의 AES 대칭키 알고리즘의 연산회로가 개발되면서, RFID 시스템에 AES 대칭키 암호화 기법을 이용한 보안 프로토콜이 제안되고 있다. 본 논문은 수동형 태그에 부착된 경량의 AES 연산기와 난수 발생기를 이용한 RFID 시스템의 보안 강화 프로토콜을 제안하였다. 제안 프로토콜은 서버, 리더, 태그에 모두 AES 알고리즘과 난수생성기가 있으며, 매 세션마다 난수에 의해 다른 비밀키로 메시지를 암호화하여 전송한다. 리더와 태그의 상호인증은 태그난수와 리더난수를 이용하였다. 본 논문의 제안 프로토콜은 기존 상호인증 프로토콜의 인증단계를 줄이고, 태그의 연산량을 감소였으며, 리더와 태그간 Air Zone의 통신단계를 줄임으로서, 모든 공격유형에 견고하고 안전한 프로토콜로서 증명되었다.

**Abstract** Recently arithmetic circuit of lightweight AES symmetric key algorithm that can apply to passive tag have been developed, then security protocol of RFID system using AES symmetric encryption techniques have been proposed. This paper proposed security enhancement protocol of RFID system using lightweight AES arithmetic circuit and random number generator of passive tag. The proposed protocol have AES algorithm and random number generator at server, reader, tag, and transmit encrypted message by separate secret key using random number at each session. The mutual authentication of tag and reader used reader random number and tag random number. As a result, proposal protocol reduce authentication steps of the existing mutual authentication protocol, and reduce amount of computation of tag, and demonstrate as secure protocol to every attack type of attacker by decrease communication step of Air Zone.

**Key Words** : RFID, Hash Algorithm, AES Algorithm, Mutual Certification, Information Security

## Ⅰ. 서 론

RFID(Radio Frequency IDentification)기술은 물리적 접촉 없이 정보인식과 수정이 가능한 장점으로, 유비쿼터스시대의 핵심기술로서 발전하고 있다. 특히, 태그의 성능 대비가격이 향상되면서, 다양한 분야에 RFID기술을 접목하는 융합기술이 급격히 발전하고 있다[1]. 그러나 리더와 태그간 Air Zone에 무선주파수로 정보를 전송함으로써 발생하는 보안문제는 RFID기술의 발전과 확산을 저해하는 요소가 되고 있다[2]. 최근, RFID 시스템의 보안 문제를 해결하기 위해 기존의 보안 알고리즘과 프로토콜을 적용하려는 연구가 활발히 진행 중이다.

*정회원, 가천의과학대학교 정보공학부 교수
**종신회원, 가천의과학대학교 정보공학부 교수(교신저자)
접수일자 2011.6.7, 수정일자 2011.7.19
게재확정일자 2011.8.12

RFID기술의 상용화를 위해서는 저렴한 태그의 개발이 필수적이며, 이를 위해 태그의 게이트 수를 최소화하여야 한다. 따라서 RFID시스템의 보안기술은 한정된 게이트를 가진 수동형 태그의 연산능력을 고려한 암호 알고리즘과 상호인증 프로토콜이 필요하다[3]. 해시함수나 공개키 기반의 암호화는 충분한 안전성을 보장받지만, 태그에 많은 저장공간과 연산능력이 필요하기 때문에, 수동형 태그에 현실적으로 적용하기 어렵다. 최근, M. Feldhofer 등은 수동형 태그에 구현 가능한 대칭키 알고리즘인 AES를 약 3,000개의 게이트로 저 전력 8비트 AES 연산기를 설계하였다[4]. M. Feldhofer의 연구결과 이후로 태그에 적용 가능한 저전력 AES에 관한 연구가 지속되고 있다.

본 논문은 대칭키 AES 알고리즘이 태그에 부착할 수 있는 최근의 연구결과를 근거로 AES 알고리즘을 이용한 정보보호 프로토콜을 제안하였다. 제안 프로토콜은 서버, 리더, 태그에 모두 AES 알고리즘과 난수생성기가 있으며, 매 세션마다 난수에 의해 다른 비밀키로 메시지를 암호화하여 전송한다. 리더와 태그의 상호인증은 태그난수와 리더난수를 이용하였다. 또한, 기존 상호인증 프로토콜의 인증단계를 줄이고, 태그의 연산량을 감소였으며, 리더와 태그간 Air Zone의 통신단계를 줄임으로서 모든 공격유형에 견고하고 안전한 프로토콜이다.

## II. 관련연구

### 1. RFID 보안위협

RFID 시스템은 태그(Tag), 리더(Reader), 백-엔드 서버(Back-end Server)로 구성된다. 태그는 마이크로 칩과 안테나로 구성되어 있으며, 소규모의 연산 및 저장 능력을 가지고 있다. 리더는 태그가 전송하는 정보를 읽거나 다시 쓰는 역할을 수행하며, 태그의 정보를 서버에 전송하기도 한다. 리더는 태그에 비해 더 큰 저장공간과 더 좋은 연산능력이 있어, 다양한 암호알고리즘을 처리할 수 있는 능력을 가진다. 백-엔드 서버는 리더나 태그의 정보를 저장하고 관리하며, 연산능력이 낮은 태그나 리더를 대신하여 복잡한 연산을 수행하기도 한다.

RFID 시스템은 서버와 리더간 기존의 유선통신에 의한 공격 뿐 아니라, 리더와 태그간 무선주파수를 사용하기 때문에, Air Zone에 대한 공격에 매우 취약하다. RFID 정보의 침해를 유발하는 공격기술은 태그에 대한 공격, Air Zone에 대한 공격, 리더에 대한 공격이며, 공격유형은 도청, 위치추적, 재전송, 스푸핑, 서비스거부 등이 있다.

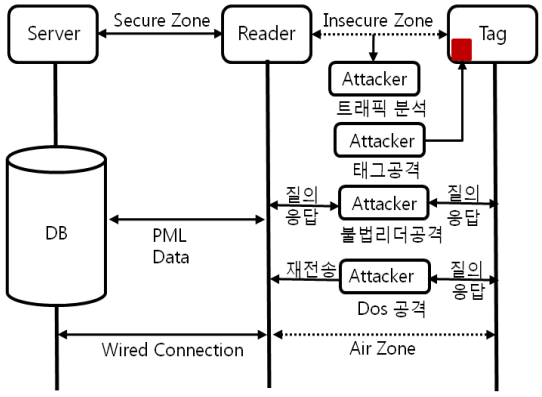


**그림 1. RFID 시스템 공격유형**
**Fig. 1. RFID system attack type**

트래픽분석은 Air Zone에 대한 공격으로, 태그와 리더간의 통신을 도청하여 정보를 획득하며, 특정 지역에서 특정 태그의 트래픽을 분석하여 위치를 추적하는 유형이다. 태그 공격은 태그 메모리를 공격하여 태그의 내용을 삭제, 변경, 위조 등의 공격이다. 리더 공격은 불법리더가 정상적인 리더로 가장하여, 정상적인 태그로부터 정보를 수신한 후, 다시 리더에게 재사용하는 공격이다. 서비스 거부공격은 태그 또는 리더에게 반복적인 질의를 전송하여, 태그나 리더의 작동을 불능 상태로 만드는 공격이다. 이외에도 교란 태그를 사용하여 리더의 정상적인 활동을 방해하는 버퍼오버플로, 정상적인 태그의 전파를 교란하여 리더의 식별을 방해하는 주파수 교란 공격이 있다.

### 2. RFID 보안 기법

#### (가) 해시함수 기법

해시-락(Hash-lock)기법은 태그에 일방향 해시함수가 있으며, 태그가 기본적으로 정보를 제공하지 않는 Lock상태에 있다. 만약, 리더가 서버에 의해 태그의 키를 해시한 metaID에 해당하는 정상적인 키 값을 보유하면, 태그는 정보를 제공할 수 있는 Unlock상태가 되어, 태그의 ID를 제공하는 기법이다[5].

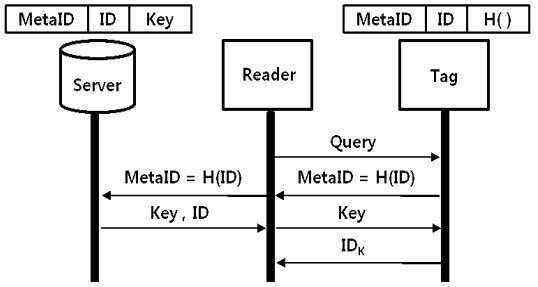


**그림 2. 해시-락 인증**
Fig. 2. Hash-lock certification

해시-락기법은 리더와 태그간에 인증이 완료된 후, 실제 정보인 ID가 노출된다. 따라서 도청 방지를 위해서 Unlock시간은 매우 짧아야 하는 부담이 있다. 또한, 태그에서 리더에 전송되는 metaID는 매 세션마다 동일한 메시지이므로 위치추적이 가능하다. 만약, 공격자가 metaID를 수신하여, 악의적인 태그 안에 저장하고, 정당한 태그로 위장하면, 공격자는 서버로 부터 키를 얻을 수 있다. 이때 공격자는 다시 정당한 리더로 위장하여, 이 키를 태그에게 전송한다면, 태그는 위장 리더를 정당한 리더로 인증하여 ID를 전송하게 되어 수푸핑 공격에 안전하지 않다.

랜덤화 해시-락(Randomized hash-lock)기법은 해시함수가 있는 태그에 난수생성기를 추가한 태그를 가정하고 있다[5]. 즉, metaID 대신 난수를 이용한 확장기법으로, 매 세션마다 태그의 출력 값들을 다르게 하여, 리더에게 전송하는 기법이다.

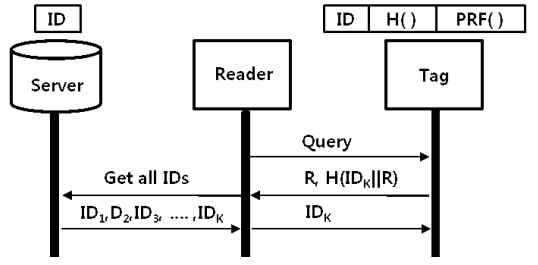


**그림 3 랜덤화 해시-락 인증**
Fig. 3. Randomized hash-lock certification

랜덤화 해시-락기법은 랜덤함수를 이용하여, 위치추적을 해결하였지만, 마지막 단계에서 $ID_k$가 암호화 과정 없이 태그로 전송하므로 도청문제가 발생한다. 또한, 공격자가 태그에서 리더에 전송되는 R, $H(ID_k||R)$를 도청하여 위장 태그가 정당한 태그로 인증 받을 수 있는 수푸핑 공격에 대해 안전하지 않다.

해시체인(Hash chain)기법은 두 개의 일방향 해시함수를 사용하는 기법이다[6]. 즉, 태그가 리더에게 응답할 때 사용하는 함수와 태그의 초기 정보 값을 갱신할 때 사용하는 함수가 있다.

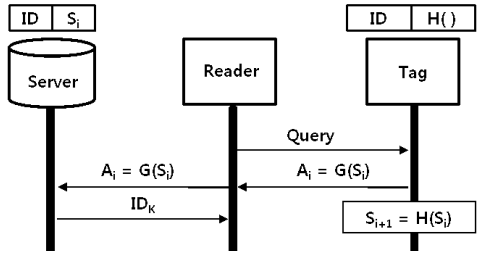


**그림 4. 해시 체인 인증**
Fig. 4. Hash chain certification

해시 체인 기술은 서로 다른 두 개의 해시함수를 이용하여 위치추적에 안전하게 설계하였지만, 서버의 연산량이 많고 2개의 해시함수는 부담이 크므로 서비스 거부 공격에 취약하며 재전송 공격에도 위험하다.

RFID 시스템에서 정보보안을 위해서 수동형 태그에 해시회로를 설계하는 것은 지금까지의 실험에 의해서 현실적으로 불가능한 게이트 수가 필요하다.

### (나) 암호화 알고리즘 기법

암호화 알고리즘 기법은 정보보안에 있어 다양한 공격유형에 안전하고 정보보안 요구사항을 만족할 수 있어, RFID시스템에 적용하고자 하는 연구가 지속되고 있다. 비대칭키 기법은 대칭키 기법에 비해 키 관리가 간단하며, 더 좋은 확장 가능성을 가진다. 그러나 비대칭키 기법은 대칭키 기법보다 연산속도가 느리고, 암호 효율성과 강도가 떨어지는 단점이 있다. 비 대칭키 기법은 전력소모, 연산속도, 연산회로의 게이트 수 등에서 해시함수 기법과 마찬가지로 수동형 태그에 적용하기에는 현실적으로 불가능하다.

M. Feldhofer 등은 수동형 태그에 적용 가능한 32비트 AES를 3000개 정도의 게이트를 이용하여, 저 전력이면서 효율적인 8비트 AES 연산기를 설계하였다. M. Feldhofer의 연구결과 이후로 수동형 태그에 적용 가능한 저전력 AES연산기에 관한 연구가 현재까지 꾸준히 이어오고 있다. M. Feldhofer는 태그와 리더가 동일한 대칭키에 의해 메시지를 암호화하여 상호인증을 수행하는

프로토콜을 제안하였다[7].

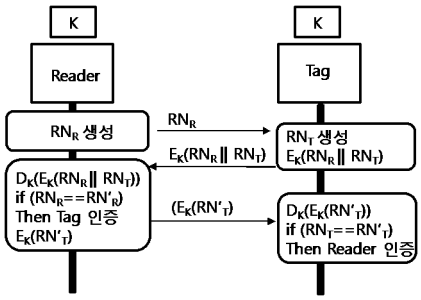


그림 5. M. Feldhofer 인증
Fig. 5. M. Feldhofer certification

M. Feldhofer 인증기법은 태그와 리더가 난수 생성과 AES연산이 가능하며, 대칭키를 공유하고 있어, 태그와 리더가 서로 공유한 대칭키와 난수를 이용하여 메시지를 암호화하여, 서버의 동작없이 상호인증을 수행한다. M. Feldhofer 인증기법은 리더난수 $RN_R$이 Air Zone에 노출되고 있어 재전송, 수푸핑 공격이 가능하며, 제한된 능력을 가진 RFID 시스템에서 서버 없이 인증을 수행함에 의해 서비스 거부 공격에 취약하다.

B. Toiruul은 서버와 태그에 저장된 두 개의 비밀키를 이용한 상호인증 프로토콜을 제안하였다[8]. B. Toiruul 인증기법은 서버와 태그는 두 개의 랜덤 비밀키 $K_1$과 $K_2$를 가지고 있으며, 서버는 모든 태그의 $ID_K$와 실제 $ID_K$의 정보인 TagID의 쌍을 관리한다. 태그와 서버는 모두 암복호화가 가능하며, 암호화에 사용되는 비밀키를 공유하여 가지고 있다.

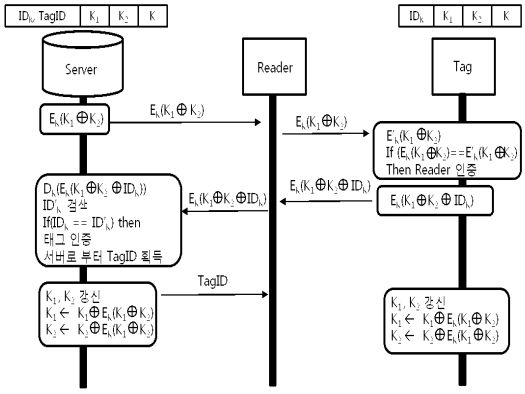


그림 6. Toiruul 인증
Fig. 6. Toiruul certification

Toiruul's 인증 프로토콜은 태그와 서버에 저장되어 있는 비밀키 $K_1$, $K_2$를 사용하여, 각 세션마다 XOR 연산을 통해, 비밀키를 변경하여 메시지를 전달하기 때문에, 도청을 비롯한 다양한 공격에 안전하다. 그러나 태그에서 키 관리를 위한 메모리의 효율성 문제와 암호화와 키를 갱신하는 연산이 다소 복잡하다. 또한, 태그마다 각각 다른 키를 사용할 경우 서버의 계산량이 증가하여, 서비스 거부공격에 의해 태그의 비동기화 문제로 사용할 수 없게 될 수 있다.

국내의 연구에서 대칭키 알고리즘을 이용한 상호인증 프로토콜인 $S^2$MAS(Sequential Symmetric key based Mutual Authentication Scheme)를 제안하였다[9].

$S^2$MAS는 태그와 리더간의 교환되는 메시지를 보호하기 위해 각 단계마다 변경되는 난수와 XOR연산을 이용하여, 순차적인 키 변환을 통해 키 값이 노출되는 문제를 해결하였다. 난수는 상호인증과 비밀키로 사용하여, 태그의 인증, 리더의 인증, 암호키 생성 기능을 가진다. 프로토콜의 상호인증은 리더난수를 통해 태그를 인증하며, 태그난수를 통해 리더를 인증한다. 서버난수는 태그를 통해 서버로 전달되어 서버에서 태그의 정보를 검색하여 리더에 전송함으로서 프로토콜이 종료된다. $S^2$MAS는 난수에 의해 변환된 키를 사용하여 메시지를 암호화 전송함으로써, 도청, 위치주적, 스푸핑공격에 안전하다.

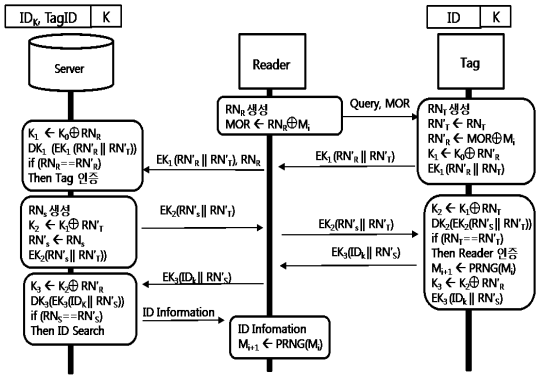


그림 7. $S^2$MAS 인증
Fig. 7. $S^2$MAS certification

$S^2$MAS는 $M_i$의 동기화를 위해 태그와 리더에서 MOR 값의 갱신이 이루어지는데, 만약 공격자가 태그에서 리더에 전송되는 $EK_3(ID_K \| RN'_S)$의 메시지에 대해 서비스 거부공격을 시도한다면, 갱신과정 중 태그와 리

더간의 통신의 실패로 갱신정보의 비동기화로 인해 태그를 사용할 수 없는 경우가 발생 할 수 있다. 또한, S²MAS의 인증단계는 8단계로서 일반적인 상호인증 프로토콜에 비해 늘어났으며, 연산 능력이 부족한 태그에 많은 암복호화 및 XOR연산 등 많은 연산량이 부담이 될 수 있다.

## Ⅲ. 제안 인증 프로토콜

본 논문은 국제표준인 Gen2가 수동형 태그에 16bit 길이의 난수를 생성하는 난수생성기가 태그에 부착되어있다는 것[10]과 경량의 연산기능을 가진 AES 연산기를 수동형 태그에 부착 가능하다는 최근의 연구결과 근거를 두어, AES 알고리즘을 이용한 정보보호 시스템을 제안한다. 제안 프로토콜은 M. Feldhofer 프로토콜에서 리더와 태그에 대칭키를 사용하는 인증기법과 S²MAS 프로토콜에서 난수와 XOR 연산을 통해 각 단계마다 암호키를 생성하여 메시지를 전송하고 인증하는 인증기법을 응용하여, 프로토콜의 단계를 줄이고, 태그의 연산량을 줄이며, 리더와 태그간의 Air Zone 통신을 최소화하고, 리더와 서버간의 유선통신의 공격을 방어할 수 있도록 하였다. 제안 프로토콜은 서버, 리더, 태그에 동일한 대칭키를 보유하고 있으며, AES암호화 연산기와 매 세션마다 난수를 생성하는 난수생성기를 보유한다.

제안 프로토콜은 리더의 쿼리문과 리더난수를 대칭키로 암호화하여 태그에 전송함으로 부터 시작된다. 태그에서 리더의 암호문을 복호화하여, 리더에서 전송된 쿼리문과 태그의 쿼리문이 동일하지 않으면, 태그는 리더의 질의에 응답하지 않음으로써, 세션은 종료하게 된다. 만약, 리더에서 전송된 쿼리문과 태그의 쿼리문이 동일하면, 리더와 태그의 인증을 위해 태그와 리더의 난수를 이용하여 인증한다. 인증 후에 서버는 태그의 정보를 데이터베이스에서 검색하여 리더의 대칭키로 암호화하여 리더에 전송한다. 최종적으로 리더는 대칭키로 복호화하여 태그정보를 획득함으로써 세션이 종료된다. 다음은 본 논문의 단계별 프로토콜이다.

단계 1 : 리더는 리더난수 $RN_R$을 생성하여, 쿼리문과 $RN_R$을 연접하여, 대칭키로 암호화하여 태그에 전송한다.

단계 2 : 태그는 전송된 암호문을 복호화하여, 쿼리문과 $RN_R$를 획득한다. 만약 복호화된 쿼리문이 태그의 쿼리문과 동일하다면, 태그는 Unlock하여, 상호인증 프로토콜을 진행하며, 동일하지 않으면 lock하여 상호인증 프로토콜을 종료한다.

if(Query==Query′) then Tag Unlock
else Tag Lock

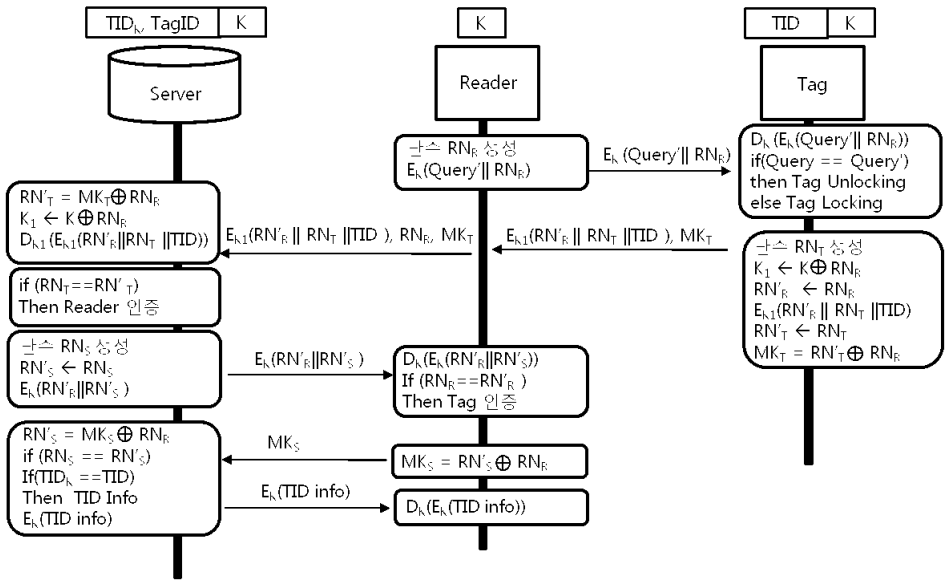


**그림 8. 제안 인증 프로토콜**
Fig. 8. Proposal certification protocol

단계 3 : 태그는 태그난수 $RN_T$를 생성하고, $RN_R$을 이용하여 새로운 비밀키 $K_1$을 생성하며, $RN'_R$, $RN_T$와 태그 ID인 TID를 연접하여 암호화한다. 또한, 리더인증을 위해 $RN'_T \oplus RN_R$ 연산을 하여 $MK_T$를 생성한다.

단계 4 : 태그는 $E_{K1}(RN'_R||RN_T||TID)$, $MK_T$를 리더에 전송한다.

단계 5 : 리더는 $E_{K1}(RN'_R||RN_T||TID)$, $MK_T$, $RN_R$를 서버에 전송한다.

단계 6 : 서버는 리더난수 $RN_R$을 이용하여, $MK_T \oplus RN_R$ 연산하여 $RN'_T$를 획득한다. 또한, $RN_R$을 이용하여 태그와 동일한 비밀키 $K_1$을 생성하며, $RN_T$, $RN'_R$, TID를 복호화한다.

단계 7 : 서버는 복호화된 $RN_T$와 리더에서 전송된 $RN'_T$을 이용하여, 리더를 인증한다.

if ($RN_T$ == $RN'_T$) then Reader 인증
else 인증 프로토콜 종료

단계 8 : 서버 난수 $RN_S$를 생성하여, $RN'_R$, $RN'_S$를 연접하여 대칭키로 암호화한다.

단계 9 : 리더는 대칭키로 복호화된 $RN'_R$과 리더의 $RN_R$을 이용하여, 태그를 인증한다.

if($RN_R$==$RN'_R$) then Tag 인증
else 인증 프로토콜 종료

또한, $RN'_S \oplus RN_R$연산을 하여 $MK_S$를 생성한다.

단계 10 : 리더는 리더난수 정보가 포함된 $MK'_S$를 서버에 전송한다.

단계 11 : 서버는 리더로부터 전송된 $MK'_S$를 이용하여 $RN'_S$를 획득한다. 만약 $RN'_S$가 서버난수 $RN_S$와 동일하면 TID를 통해, 태그정보를 검색한다.

if($RN_S$ == $RN'_S$) then Tag Info research
else 인증 프로토콜 종료

단계 12 : 서버는 리더의 대칭키로 태그 정보를 암호화하여 리더에 전송한다.

단계 13 : 대칭키를 보유한 리더는 서버에서 전송된 태그정보를 복호화하여 획득한다.

## Ⅳ. 제안 프로토콜 분석

본 논문에서 제안한 프로토콜을 분석하기 위해 RFID 시스템의 공격 유형인 도청, 위치추적, 재전송, 스푸핑, 서비스거부 등과 보안 요구사항인 기밀성 익명성 상호인증, 위조방지 등에 대해서 분석한다. 다음은 공격유형에 대한 분석내용이다.

1. 도청 : 서버, 리더, 태그가 모두 대칭키를 보유하여, 모든 단계에서 암호화된 메시지로 통신하므로 공격자의 도청에 안전하다. 또한, 단계 4에서 $MK_T$가 노출되지만 $RN_T$와 $RN'_R$값을 알 수 없기 때문에 안전하다.
2. 위치추적 : RFID 시스템은 Air Zone의 도청문제를 해결하지 못하면 위치추적의 보안문제가 발생한다. 본 논문은 모든 메시지가 난수를 암호화하여 전송되며, 매 세션마다 난수에 의해서 변경된 비밀키로 암호화하여 전송하므로 위치추적에 안전하다.
3. 재전송 : 공격자가 단계 1의 메시지를 재전송 공격에 이용하려면, 이전 세션에 정보를 이용하여, 현재 세션에서 단계 4의 연계된 메시지를 생성할 수 있어야 한다. 그러나 단계 1의 메시지는 암호화되어 있으며, 매 세션마다 $RN_R$에 의해 갱신되므로 이전의 정보를 이용할 수 없다. 또한, 위장 태그는 대칭키 K를 보유하지 않기 때문에 서버에 전송된 암호메시지는 $K_1$으로 복호화 할 수 없다. 따라서 서버는 $RN_T$와 $RN'_R$을 알 수 없으므로 인증이 실패되어 세션이 종료된다.
4. 수푸핑 : 공격자는 단계 4에서 악의적인 리더를 이용하여 메시지 $E_{K1}(RN'_R||RN_T||TID)$, $MK_T$를 도청할 수 있다. 이 메시지는 위장 태그에 저장하여 다시 정당한 리더에게 전송한다. 리더는 이 메시지를 단계 5에 의해 아무 의심 없이 $RN_R$과 같이 다시 서버로 전송한다. 서버는 이 메시지를 정상적으로 복호화하여 위장 태그를 인증 할 수 있다. 그러나 리더에서 태그를 인증하기 위해서는 리더의 대칭키가 있어야 하지만 위장된 리더는 대칭키가 없으므로,

**표 1. 기존 인증기법과 제안기법의 안전성 비교**
Table.1. Safety compare of existing authentication techniques and proposed authentication technique

| 인증기법 | 공격유형 | | | | | 보안 요구유형 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 도청 | 위치 추적 | 재전송 | 수푸핑 | DOS | 기밀성 | 익명성 | 전방향 안전성 | 상호 인증 | 위조 방지 |
| 해시락 | × | × | × | × | ○ | △ | × | △ | △ | × |
| 랜덤해시락 | ○ | △ | × | × | × | △ | △ | △ | △ | × |
| 해시체인 | ○ | △ | × | △ | × | △ | ○ | ○ | △ | ○ |
| M. Feldhofer | △ | × | △ | × | × | ○ | × | × | ○ | △ |
| Toiruul | ○ | ○ | ○ | ○ | × | △ | ○ | ○ | ○ | ○ |
| $S^2$MAS | ○ | ○ | ○ | ○ | × | ○ | ○ | ○ | ○ | ○ |
| 제안프로토콜 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

단계 9에서 태그의 인증 실패로 세션은 종료하게 된다.

5. 서비스 거부 : 공격자가 대량의 태그를 물리적으로 복사하여, 서비스 거부 공격을 하는 경우에, 위장된 태그는 단계 2에서 암호화된 쿼리문을 복호화 할 수 없기 때문에, 위장된 태그는 Unlock될 수 없어 인증 프로토콜을 종료하게 된다. 따라서 서비스 거부 공격에 안전하다.

이와 같이 제안 프로토콜은 모든 공격유형에 안전함을 증명하였다. 다음은 RFID 시스템의 보안 요구사항에 대한 분석이다.

1. 기밀성 : 모든 메시지가 암호화 메시지로 전송되므로, 대칭키를 보유하지 않은 공격자는 의미없는 데이터이기 때문에 기밀성이 보장된다.
2. 익명성 : 매 단계 및 세션마다 난수에 의해 다른 값이 생성되므로, 공격자는 어느 지점의 리더에서 읽혀지고 있는지 추적할 수 없다.
3. 상호인증 : 서버, 리더, 태그가 동일한 대칭키를 보유하기 때문에 기본적인 상호인증 기능을 가지고 있다. 또한, 난수 $RN_T$와 $RN_R$을 이용해 리더와 태그가 상호인증을 하고 있다.
4. 전방향안정성 : 공격자가 태그를 추적하기 위해 태그에서 전송되는 모든 정보를 수집한다 하더라도 정보의 연관성으로 예측할 수 없다.
5. 위조방지 : 공격자가 태그나 리더의 위조를 수행하려면 재전송 공격이나 스푸핑을 통해 정당한 정보를 획득해야만 가능하지만, 제안 프로토콜은 재전송이나 스푸핑 공격에 안전하다.

제안 프로토콜은 서버, 리더, 태그에 모두 동일한 대칭키를 보유하여, 대부분의 공격유형에 견고한 $S^2$MAS기존 상호인증 프로토콜의 인증단계를 줄이고, 서비스 거부공격에 의해 비동기화로 태그를 사용할 수 없게 되는 문제를 제거하였다. 또한, 태그의 연산량을 감소였으며, 리더와 태그간 Air Zone의 통신단계를 줄임으로서 모든 공격유형에 견고하고 안전한 프로토콜이다.

## V. 결 론

RFID 시스템은 무선 통신을 이용한 기술이므로, 공격이 일반 네트워크 환경에 비해 용이하다. 최근, RFID 시스템의 정보보호를 위해, 기반 기술로서 암호화 알고리즘에 대한 연구가 진행되고 있다. 본 논문은 수동형 태그에 16bit 길이의 난수를 생성하는 난수생성기와 경량의 AES 연산기를 부착 가능하다는 최근의 연구결과를 근거를 두어, AES 알고리즘을 이용한 정보보호 시스템을 제안하였다. 제안 프로토콜은 M. Feldhofer 프로토콜에서 리더와 태그에 대칭키를 사용하는 인증기법과 $S^2$MAS 프로토콜에서 난수와 XOR 연산을 통해, 각 단계마다 암호키를 갱신하여 메시지를 전송하고 인증하는 인증기법을 응용하여, 태그, 리더, 서버 모두 대칭키 알고리즘을 사용함으로써, 프로토콜의 단계를 줄이고, 태그의 연산량을 줄이며, 리더와 태그간의 Air Zone 통신을 최소화하

고, 리더와 서버간의 유선통신의 공격을 방어할 수 있는 프로토콜이다. 제안 프로토콜은 RFID 시스템의 공격 유형인 도청, 위치추적, 재전송, 스푸핑, 서비스거부 등과 보안 요구사항인 기밀성 익명성 상호인증, 위조방지 등에 대해서 안전한 것으로 증명된다.

## 참 고 문 헌


[1] 정보통신부, 한국정보보호진흥원, "RFID 프라이버시 보호 가이드라인", 9, 2007.

[2] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security Analysis of a Cryptographically-Enabled RFID Device", In Proceeding 14th USENIX Security Symposium, pp. 1-16, 2005.

[3] A. Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, pp. 381-394, Feb. 2006.

[4] M. Feldhofer, and C. Rechberger, "A Case Against Currently Used Hash Functions in RFID Protocols", On the Move to Meaningful Internet Systems, LNCS 4277, pp. 372-381, 2006.

[5] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", In Security in Pervasive Computing, LNCS 2802, pp. 201-212, 2005.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A Cryptographic Approach to 'Privacy-Friendly' tag", RFID Privacy Workshop, 2003.

[7] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm", Cryptographic Hardware and Embedded Systems, LNCS 3156, pp. 85-140, 2004.

[8] B. Toiruul, and K.O. Lee, "An Advanced Mutual Authentication Algorithm Using AES for RFID Systems", International Journal of Computer Science and Network Security, Vol. 6, No. 9B, pp. 156-162, Sep 2006.

[9] 鄭京鎬, "대칭키 기반의 순차적 키 갱신을 이용한 RFID 상호 인증 프로토콜", 慶北大學校工學博士學位論文, 12. 2010.

[10] EPCglobal Inc., "Radio Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz-960MHz Version 1.0.9.", http://www.EPCgloballinc.org


## 저자 소개


**김 창 복(정회원)**

• 2008년 2월 : 인천대학교 컴퓨터공학과 (공학박사)
• 2011년 8월 현재 : 가천의과학대학교 정보공학부 교수
<주관심분야 : 이동통신, 인터넷보안, 임베디드 시스템, 센서네트워크>

**김 남 일(종신회원)**

• 2000년 8월 : 건국대학교 전자공학과 (공학박사)
• 2011년 8월 현재 : 가천의과학대학교 정보공학부 교수
<관심분야 : 컴퓨터네트워크,트래픽제어, 유비쿼터스, 유헬스케어, BcN>