

인덱스 처리 기법과 난수 사용을 기반으로 하는 초경량 RFID 인증 프로토콜 설계

강현우*, 이우진**

*현대오토에버, **경북대학교 컴퓨터학부

e-mail : hsdevils@gmail.com

The Design of An Ultra-Lightweight RFID Authentication Protocol Using The Index Processing Techniques and Random Numbers

Hyunwoo Kang*, Woo jin Lee**

*Hyundai Autoever

**School of Computer Science and Engineering, Kyungpook National University

요약

수동형 RFID 는 제한된 자원으로, 무선채널을 사용하는 기술이다. 하지만 여러 보안 문제점이 있으며, 이를 해결하기 위한 각종 암호화 기법이나 알고리즘을 활용한 인증 프로토콜이 발표되었다. AES 와 해시는 대표적인 암호화 알고리즘으로써 그 안정성이 검증되었지만, EPC Global 에서 규정한 통신 횟수를 만족하기 힘들다. 본 논문에서는 인덱스 처리 기법과 난수 사용을 기반으로 하는 초경량 RFID 인증 프로토콜을 제안한다. 이 프로토콜은 산술·논리연산자를 사용하여 주요 보안 문제를 해결하였다. 그리고 RFID 에 최저 통신횟수를 만족하도록 구현 가능한 프로토콜을 작성하였다.

1. 서론

RFID(Radio Frequency Identification) 시스템은 ISO 18000-1~7 에서 규정된 무선 주파수를 이용한 비접촉 방식 자동인식 기술이다. 특히 수동형 UHF RFID 의 경우 태그 가격이 저렴하며, 인식 거리가 비교적 길고, 기존의 바코드에 비해서 저장 할 수 있는 데이터의 양이 많아 산업 분야에서 널리 활용되고 있다. 하지만 수동형 RFID 는 제한된 자원으로 무선채널을 사용하므로 도청, 위치 추적, 정보 노출 등의 보안 문제점이 있다. 이러한 문제점을 해결하기 위하여 암호화 기법이나 알고리즘을 활용한 RFID 인증프로토콜이 필요하게 되었다. 최근 발표된 암호화 기법 중에 해시기법과 공개키 알고리즘은 RFID 시스템에 일어날 수 있는 다양한 공격에 충분한 안전성을 제공하고 있다. 하지만 위 알고리즘을 구현하기 위해서는 많은 하드웨어 자원이 필요하다. 따라서 한정된 자원을 가진 태그에서는 위 알고리즘을 구현하는 것은 한계가 있다. Martin Feldhofer 는 RFID 태그에서 사용 가능한 저전력 AES 알고리즘[1]이 발표하였고, 이를 이용한 프로토콜이 많이 발표되고 있다. 하지만 대칭키 기반인 AES 는 기본적으로 키 분배문제가 있다. 뿐만 아니라 저전력 AES 알고리즘을 구현하기 위해 기존의 32 비트 AES 를 8 비트 연산으로 설계하여 EPC Global[2]에서 요구하는 초당 100 회 통신을 만족하지 못한다. 따라서 적용에는 문제가 있지만 표준을 만족하지 못하는 암호화 방식이다.

Peris-Lopez[3][4][5], 최은영[6] 등은 최근 이러한 문제점을 보완한 초경량 인증프로토콜을 발표하였다. 이 프로토콜은 산술·논리연산자를 사용하여 RFID 시스템의 주요 보안 문제를 해결하였고, 1000 게이트 내외로 프로토콜을 작성하여 태그에 구현이 가능하며, 최저 통신횟수도 만족하여 현실적으로 가장 적합한 프로토콜이다. 하지만 비동기화 문제와 인덱스 값이 해킹되는 문제점이 T. Li[7]의 논문에서 제시된 바 있다.

본 논문에서는 비동기화 문제와 T. Li[7]의 능동 공격을 인덱스 처리기법을 개선한 초경량 RFID 인증 프로토콜을 설계한다. 더불어 RFID 시스템에서 일어날 수 있는 일반적인 공격 역시 고려하여 현실적으로 사용 가능한 프로토콜을 설계한다.

본 논문의 구성은 다음과 같다. 2 장에서는 기존 초경량 RFID 인증프로토콜과 문제점에 대해 살펴보고 3 장에서는 제안한 개선된 프로토콜에 대해서 서술한다. 4 장에서는 제안된 인증프로토콜의 보안과 효율성 분석하며 마지막으로 결론을 맺는다.

2. 관련 연구

초경량 인증 프로토콜은 논리·산술연산자를 이용하여 자원 소비를 최소화 하는 인증 기법이다. 이러한 프로토콜은 1000 게이트 정도의 효율적인 기법이지만 비동기화 공격 및 태그 완전 노출될 수 있는 문제점이 있다. 하지만 최소 하드웨어 요구조건과 EPC Global 의 요구사항을 충족하는 유일한 기법이다. 본

장에서는 최근 발표된 경량 인증프로토콜을 살펴보고 이들이 가진 문제점을 알아보도록 한다.

2.1. Peris-Lopez 의 초경량 프로토콜

Peris-Lopez 는 초경량 인증프로토콜인 LMAP[3]을 시작으로 이를 보완한 M2AP[4], EMAP[5]를 연이어 발표했다. 이 프로토콜의 특징은 논리·산술 연산자와 암호화를 위한 K1~K4 의 키를 사용한다. 그리고 고정된 96 비트의 ID 를 사용하며 태그 식별을 위한 index-pseudonym(IDS)를 사용한다. 인증을 위한 단계는 총 3 단계로 이루어지며 과정은 다음과 같다.

단계 1: Tag identification

- (1) 리더 → 태그: hello
 (2) 태그 → 리더: IDS⁽ⁿ⁾

단계 2: Mutual authentication

- (1) 리더 → 태그: A||B||C
(2) 태그 → 리더: 풀 1 찬조

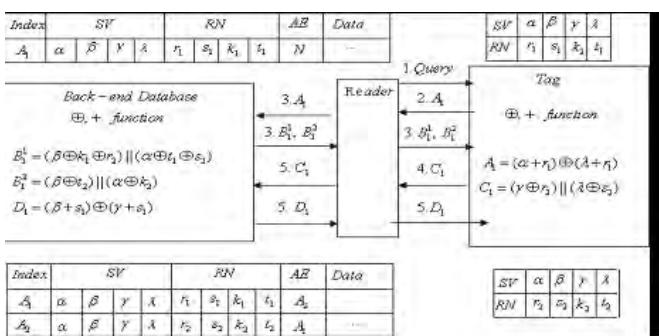
<豆 1> Peris-Lopez's Mutual authentication: Tag→Reader

LMAP[3]	M2AP[4]	EMAP[5]
T→R:D	T→R:D E	T→R:D E
A= $\text{IDS}^{(n)} \oplus K1^{(n)} \oplus n1$,	A= $\text{IDS}^{(n)} \oplus K1^{(n)} \oplus n1$,	A= $\text{IDS}^{(n)} \oplus K1^{(n)} \oplus n1$
B= $(\text{IDS}^{(n)} \vee K2^{(n)}) \oplus n1$,	B= $(\text{IDS}^{(n)} \wedge K2^{(n)})$	B= $(\text{IDS}^{(n)} \vee K2^{(n)}) \oplus n1$
C= $\text{IDS}^{(n)} \oplus K3^{(n)} \oplus n2$,	$\vee n1$,	C= $\text{IDS}^{(n)} \oplus K3^{(n)} \oplus n2$
D= $(\text{IDS}^{(n)} + ID)$	C= $\text{IDS}^{(n)} \oplus K3^{(n)} \oplus n2$,	D= $(\text{IDS}^{(n)} \wedge K4^{(n)}) \oplus n2$
$\oplus n1 \oplus n2$.	D= $(\text{IDS}^{(n)} \wedge ID) \wedge n2$,	E= $(\text{IDS}^{(n)} + ID) \oplus n1$.
	E= $(\text{IDS}^{(n)} + ID) \oplus n1$.	$n2 \oplus ID \oplus K1^{(n)}$

단계 3: IDS 와 비밀키 갱신

Peris-Lopez의 프로토콜의 가장 큰 문제점은 리더의 요청에 태그는 항상 같은 응답인 IDS⁽ⁿ⁾으로 한다는 것이다. 이것은 T. Li[7]의 방법으로 ID 까지 유출되는 방법이 연구되었다. 뿐만 아니라 비정상 종료에 의해 비동기화 공격 또한 일어날 수 있다.

2.2. 최은영의 프로토콜[6]



(그림 1) 최은영의 프로토콜[6]

그림 1 은 최은영의 프로토콜을 나타낸 것이다. 이 프로토콜은 앞서 소개한 Peris-Lopez 의 프로토콜과 마찬가지로 Index 를 이용한 초경량 프로토콜의 하나이

다. Index 값을 두 개 저장하고 있으므로 비동기화 공격에 대비하고 있어 Peris-Lopez 이 가지는 비동기화 공격 문제는 해결되었지만 리더의 요청에 항상 같은 index 값을 보내기 때문에 T. Li 의 능동적 공격에는 여전히 약하다는 것을 알 수 있다. 그리고 연속적인 비동기화 공격에는 약점이 있다.

3. 제안 프로토콜

본 장에서는 RFID 시스템에 알려진 일반적인 공격과 초경량 RFID 상호 인증프로토콜에 대한 능동 공격에 안전한 인덱스 처리기법을 개선한 초경량 인증 프로토콜을 제안한다. 이 프로토콜은 논리·산술연산자를 이용한 암호학적 기법을 적용하여, 서버와 태그 모두 인증을 거치는 상호 인증을 수행한다.

3.1. 초기 가정 및 용어

제안하는 RFID 시스템의 구성은 서버, 리더, 태그로 구성되며 태그는 수동형 UHF 태그이다. 태그와 리더 사이의 통신 채널은 무선 주파수를 사용하므로 안전하지 않은 (Insecure) 채널이며 서버와 리더 간의 통신 채널은 안전한 (Secure) 채널이라고 가정한다. 그리고 태그와 서버는 논리 · 산술 연산이 가능하며, 리더와 서버는 난수를 태그는 유사난수를 발생 시킬 수 있다. 표 2 은 제안한 프로토콜에 사용되는 표기법을 나타내며 초기화 단계는 제안 프로토콜의 실행을 위한 준비 단계로서 다음과 같다.

<표 2> 제안 프로토콜의 표기법

표기법	내용	표기법	내용
ID	태그 ID	\oplus	XOR
IDS	Index-pseudonym	\wedge	OR
Rr	리더난수	\vee	AND
Rt_n	n 번째 태그 난수	+	더하기
Rs_n	n 번째 서버 난수	-	빼기
K_n	n 번째 키	PRNG()	유사난수생성
X	New/Old 임시저장소	Random()	난수생성
 	연결 연자		

- 1) 서버는 모든 태그 ID 를 저장하고 있다. 이때 인덱스 값인 IDS 와 키 값인 K1~K6 는 초기화 되어 있으며, 같은 ID 의 태그와 동일한 값이 저장된다.

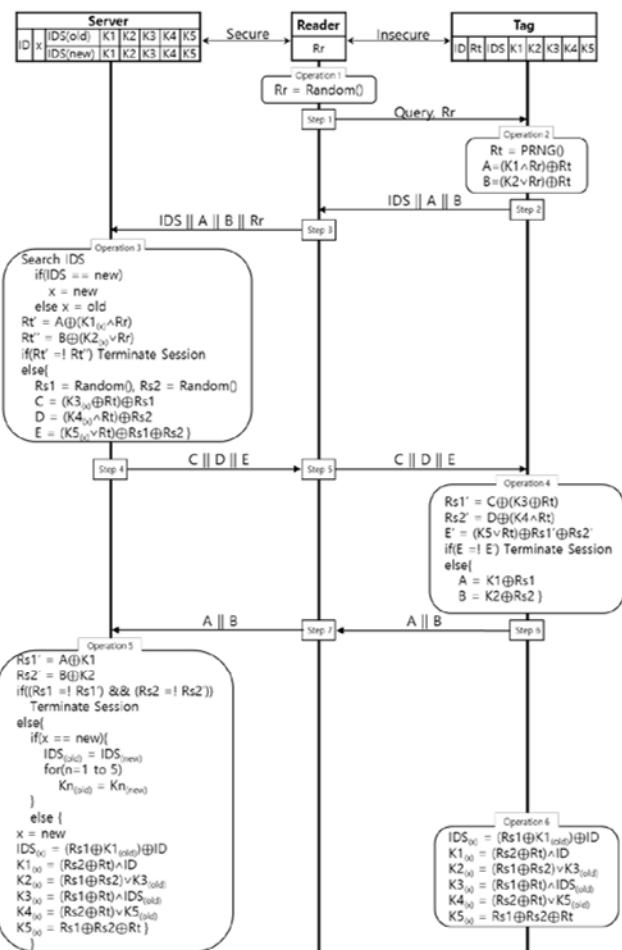
- 2) 태그 역시 ID 와 IDS 그리고 K1~K5 의 값이 안전하게 초기화 되어 저장되어 있다. 이때 값은 서버에 저장되어 있는 값과 동일한 값이 저장되어 있다.

3.2 상세 프로토콜

본 논문에서 제안한 프로토콜은 일반적인 초경량 RFID 인증프로토콜과 달리 Query 를 받은 후 IDS 와 인증 값 A, B 를 함께 보내고 서버는 태그를 인증 후에 다음 단계를 진행 함으로써 능동공격에 강인한 설계를 하였다. 그리고 임시 저장소인 x 를 이용하여 old 값과 new 값을 별도로 관리하여 비동기화 공격에

도 안전한 프로토콜을 설계하였다. 뿐만 아니라 논리·산술연산을 이용하여 암호화 하므로 암호화 하드웨어 최소 요구 사항인 $20\mu\text{W}$, 5000 게이트 이내 설계와 EPC Global[2]에서 요구하는 초당 100 회 통신을 모두 만족할 수 있다. 본 논문에서 설계한 프로토콜은 질의 단계, 태그와 서버의 상호인증 단계, 그리고 키 갱신단계까지 총 세 부분으로 이루어진다.

그림 2는 본 논문에서 제안한 인덱스 처리기법을 개선한 초경량 RFID 인증 프로토콜의 전체 구성을 나타내며 각각의 단계는 다음과 같다.



(그림 2) 제안프로토콜의 전체구성

3.2.1 질의 단계

Operation1에서 리더난수 Rr 과 함께 Query를 태그에게 보낸다. 이렇게 하면 Rr 은 직접적으로 노출되지만 키와 태그난수와 함께 연산되어 사용하므로 직접적인 노출에 의한 문제점을 최소화할 수 있다.

3.2.2 상호 인증 단계(태그)

Operation 2에서는 리더로부터 받은 리더 난수 Rr , 유사난수 Rt , 그리고 $K1, K2$ 를 이용하여 A, B 를 생성한다. 생성된 A, B 는 IDS 와 함께 리더로 보낸다. 리더는 받은 메시지에 Rr 을 연접하여 서버로 보낸다.

Operation 3에서 서버는 IDS 를 검색하여 $K1 \sim K5$ 를 찾는다. 이 때 IDS 가 ID 에서 old 인지 new 인지를 알아내고, 이 값을 x 에 저장한다. 그리고 서버는 자신이 가지고 있는 $K1, K2$ 와 리더로부터 받은 Rr 을 이용하여 Rt' 와 Rt'' 를 생성한다. 생성된 Rt' 와 Rt'' 를 비교하여 값이 같으면 정상 태그로 태그가 인증된다.

3.2.3 상호 인증 단계(서버)

Operation 3에서는 서버 난수를 만들어 $Rs1$ 과 $Rs2$ 에 저장한다. 그리고 태그를 인증할 때 만든 Rt 와 $K3 \sim K5$ 을 이용하여 C, D, E 를 만든다. 앞서 태그를 인증할 때와 마찬가지로 C 와 D 에는 서버난수가 하나씩 연산에 이용되고, E 에는 $Rs1$ 과 $Rs2$ 모두 연산에 이용되므로 이 난수들은 태그에서 서버를 인증할 때 사용된다. 만들어진 C, D, E 는 리더를 통해 태그까지 전달된다. Operation4에서는 태그는 자신이 가지고 있는 $K3 \sim K5$ 와 Rt 를 이용하여 $Rs1'$ 와 $Rs2'$ 를 만들어 E' 를 생성한다. 태그는 직접 생성한 E' 와 서버로부터 받은 E 를 비교하여 같으면 정상서버이며 상호인증이 종료되고 다음 통신에서 쓸 IDS 와 $K1 \sim K5$ 을 갱신할 수 있다.

3.2.4 IDS 와 키 갱신 단계

서버는 태그인증을 정상적으로 마친 후 Operation 5에서는 A, B 를 수신 후 IDS 와 키 값 갱신 작업을 수행한다. 서버 측 키 갱신 작업은 우선 A 와 B 를 확인하여 태그를 다시 한번 인증하고 old 와 new 값을 가진 x 의 값을 비교하는 것부터 시작한다. x 가 new 값 즉 이전 세션이 정상인 경우 기존 IDS 와 Kn 을 모두 old 에 저장한다. 만약 x 값이 old 일 경우 그 값은 그냥 두고 new 값만 갱신한다. 이러한 과정은 만약 세션이 중간에 비정상 종료 되거나 비동기화 공격을 받더라도 서버는 old 값과 new 값을 모두 저장하고 있어 태그 정보를 잃어버리는 일을 막아준다. x 값을 확인하고 IDS 와 키 값의 교체를 완료하면 IDS 와 Kn 을 갱신한다. 이때 서버난수, 태그난수, IDS 그리고 ID 를 논리연산자와 산술연산자를 이용하여 조합한다.

태그 측에서는 서버인증이 정상적으로 종료된 후 IDS 및 키 값 갱신작업을 시작한다. 태그 측에서는 x 값을 따로 저장하지 않으므로 이를 판별하는 과정만 생략될 뿐 이하 과정은 서버 측 IDS , 키 값 갱신 방법과 동일하다.

4. 제안한 프로토콜의 보안 및 효율성 분석

본 장에서는 기존 프로토콜과 제안 프로토콜을 비교 분석하고 RFID 시스템에 대해 공격자자 취할 수 있는 공격 유형을 토대로 제안한 인증 프로토콜의 보안과 안전성 그리고 효율성 대해서 기술한다.

4.1 보안성 분석

4.1.1 도청(Eavesdropping), 재전송 공격(Relay attack)

RFID 시스템에서 리더와 태그 사이의 통신은 무선 채널로서, 불안전한 채널이라고 가정하였다. 따라서 리더와 태그 사이의 통신내용은 언제든지 도청될 수 있다. 하지만 통신의 내용이 도청 당하더라도 공격자에겐 무의미한 값이어야 한다. 제안된 프로토콜의 경우 모든 단계에서 난수를 발생시켜 조합 하므로 도청을 한다 하더라도 도청 값으로부터 아무것도 유추를 하거나 재사용을 하지 못한다.

4.1.2 경량 프로토콜에 대한 T.Li 능동 공격

T.Li[7]가 LMAP, M2AP, EMAP에 적용된 분석 방법은 다음과 같다. 인증 과정에서 전송되는 메시지의 한 비트를 변형하고, 인증 여부를 확인한다. 그 후, 이로부터 비밀키의 해당 비트 정보를 얻어내는 것이다.

이 공격은 요청이 있으면 태그는 IDS를 서버에 보내고 서버는 항상 응답을 하기 때문에 분석이 가능한 것이다. 본 논문에서는 이러한 문제점을 해결하기 위하여 IDS와 인증 메시지인 A, B, C를 함께 보낸다. 서버는 정상적인 태그로 인증되어야 인증 메시지를 태그로 응답하므로 T.Li의 능동 공격에 자유롭다.

표 3은 제안한 프로토콜과 Hash Chin[8], AES[1], Peris Lopez 그리고 최은영의 알고리즘의 안전성을 도청, 재전송 공격, 위치추적, 서비스 거부 공격, 비동기화 공격, T.Li[7]의 능동 공격에 대하여 비교 및 분석한 결과이다.

<표 3> 기존 프로토콜과 제안 프로토콜의 안정성 비교

구분	도청	재전송 공격	위치 추적	Dos 공격	비동기화 공격	T.Li[7]의 능동공격
Hash Chin[8]	○	○	△	X	X	-
Feldhofer[1]	○	○	○	X	○	-
Peris Lopez[5]	X	○	X	△	X	X
최은영[6]	X	○	X	△	○	X
제안 프로토콜	○	○	△	△	○	○

4.2. 효율성 분석

900MHz 대 주파수를 이용하는 수동형 RFID 태그에서 사용할 수 있는 최대 전력량은 $20\text{ }\mu\text{W}$ 이다. RFID 칩 제조에 사용하는 CMOS 공정을 이용하여 $20\text{ }\mu\text{W}$ 이내로 회로를 설계할 경우 우리가 사용할 수 있는 게이트 수는 5000 게이트 내외다. 따라서 회로설계는 5000 게이트를 넘지 않게 설계해야 한다. 그리고 EPC Global에서는 초당 100 회 통신을 만족하는 프로토콜을 설계하여야 한다고 표준에서 명시하고 있다. 두 가지 주요 제약사항과 함께 프로토콜 라운드 횟수, 그리고 서버 부하를 기준으로 표 4에서 비교 분석 하였다.

<표 4> 효율성 비교 분석

구분	Hash Chin[8]	Feldhofer [1]	Peris Lopez[5]	최은영[6]	제안 프로토콜
게이트 수	20,000 ↑	5,000 ↓	1,000 ↓	1,000 ↓	1,000 ↓
통신 100	○	X	○	○	○
프로토콜 회전	4 회	3 회	4 회	5 회	3 회
서버 부하	매우 큼	보통	보통	보통	보통

5. 결론

RFID 시스템은 무선기술을 이용한 자동인식 기술로 최근 다양한 분야에서 그 사용이 증가되고 있다. RFID 시스템의 사용 증가와 함께 가장 큰 문제로 떠오르고 있는 것은 바로 보안문제이다. RFID 태그는 반도체 공정기술의 발전으로 매우 저가로 칩이 생산될 수 있어 만들어진 기술이기 때문에 가격에 매우 민감하여 쉽게 하드웨어 성능을 끌어올릴 수 없다. 그러므로 보안 문제를 해결하기 위해서는 알고리즘을 경량화 하여야 한다.

본 논문에서는 인덱스 처리기법을 개선하여 최근 가장 큰 문제점으로 떠오르고 있는 능동 공격과 비동기화 공격문제를 해결한 초경량 RFID 인증 프로토콜을 설계하며 현실적으로 사용 가능한 프로토콜을 제시하였다.

참고문헌

- [1] M.Feldhofer, J.Wolkerstorfer, and V.Rijmen, "AES implementation on a grain of sand." IEE Proceedings Information Security, Vol. 152, Issue 1, pp. 13–20, October 2005.
- [2] EPCglobal, EPCglobal Tag Data Translation (TDT) 1.0 Ratified Standard Specification, 1-107, 2006.
- [3] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiaidor, A. Ribagorda, "LMAP: A Real Leightweight Mutual Authentication Protocol for Low-cost RFID tags," Workshop on RFID security, RFIDSec 06, pp.137-148, July 2006.
- [4] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiaidor, A. Ribagorda, "M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID tags," Proceedings of UIC 2006, pp.912-923, December 2006.
- [5] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiaidor, A. Ribagorda, "EMAP: An Efficient Mutual-Authentication Protocol for Low-cost RFID tags," Proceedings of OTM Federated Conferences and Workshops: IS Workshop 2006. pp. 352-261, January 2006.
- [6] 최은영, 최동희, 임종인, 이동훈. "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜," 정보보호학회논문지, 제 15 권, 제 5 호, 2005 년 10 월.
- [7] T. Li, R. H. Deng. "Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol," Proceeding of AReS 2007, April 2007.
- [8] M. Ohkubo, K. Suzuki, and S. Kinoshita "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID," the Soft Computing and Intelligent Systems (SCIS 2004), pp.719-724, September 2004.