SSG기반 개선된 RFID 인증 프로토콜

박 택 진*

Improved RFID Authentication Protocol Based on SSG

Taek-Jin Park*

요 약

최근 유비쿼터스 환경에서 바코드 대신 RFID가 대치되었지만, RFID 는 무선 주파수를 사용하기 때문에 프라이버시와 보안성에 많은 문제점을 가지고 있다. 첫째는 비인가 리드가 임의 RFID 태그의 ID 정보를 쉽게 읽어 들일 수 있고, 둘째는 공격자가 수집한 태그 ID 정보를 이용하여 합법적인 리더에게 인가된 태그인 것처럼 쉽게 속일 수 있다. 본 논문에서는 SSG 기반 개선된 RFID 인증 프로토콜을 제안하였다. SSG 알고리즘은 LFSR 과 선택로직만으로 구성되어 있다. 따라서 RFID 태그와 같은 극히 제한적인 자원을 갖는 시스템에서 하드웨어 구현이 가능하며, 출력 비트 스트림은 의사난수로 사용함으로써 다양한 공격에 안전하다. 제안한 프로토콜은 SSG를 기반으로 하기 때문에 안전하고 효율적이다.

ABSTRACT

Recently, RFID is substituted for bar codes according to advance in the ubiquitous computing environments, but the RFID system has several problems such as security and privacy because it uses radio frequencies. Firstly, unauthorized reader can easily read the ID information of any Tag. Secondly, Attacker can easily fake the legitimate reader using the collected Tag ID information,such as the any legitimate tag. This paper proposed improved RFID authentication protocol based on SSG. SSG is organized only one LFSR and selection logic. Thus SSG is suitable for implementation of hardware logic in system with extremely limited resources such as RFID tag and it has resistance to known various attacks because of output bit stream for the use as pseudorandom generator. The proposed protocol is secure and effective because it is based on SSG.

Keywords : RFID system, Authentication, Protocol, Random number generator, SSG

Ⅰ. 서 론

RFID(Radio Frequency IDentification) 는 특정 주파수 대역을 이용하여 원거리에서도 대상물을 인식할 수 있고, 각종 데이터를 주고 받을 수 있도록 하는 초소형 칩(Chip)으로 차세대 유비쿼터스(Ubiquitous) 컴퓨팅의 핵심 기술이라 할 수 있다. 일반적인 바코드(Bar Code)와는 달리 무선

* 강릉영동대학교 의료전자과 (tjpark@gyc.ac.kr)
접수일자 : 2011년 09월 18일, 수정일자 : 2011년 11월 12일, 심사완료일자 : 2011년 12월 09일

으로 인식할 수 있어 객체(Object)를 감지기에 직접 접촉할 필요가 없고 최대 512KB의 메모리를 가지며 응답속도(100ms 이하)가 빠르다. 또한, 한 번에 여러개의 RFID 태그(Tag)를 인식할 수 있다. 이러한 RFID 시스템은 최근 들어 물류 및 유통 시스템에서 기존의 바코드를 대신해서 다양하게 활용될 수 있는 자동 인식 시스템의 하나로 각광 받고 있으며, 다양한 형태의 서비스, 구매, 재고 관리 등 산업 전반에 걸쳐 획기적인 변화를 가져올 것으로 예상된다. 그러나 RFID 시스템을 구성하는 디바이스(Device)간의 통신 채널이 무선 환경이라는 특수성 때문에 도청을 통한 위조 또는 추적 등 보안적인 취약점을 내포하고 있다. 유비쿼터스 컴퓨팅 환경에서는 각각의 디바이스들이 생활 곳곳에 널리 퍼져 있고 이러한 디바이스를 통해서 어느 곳에서나 정보를 이용할 수 있다. 이것은 어느 곳에서나 정보유출이 가능하고 정보유출은 심각한 개인 프라이버시(Privacy) 침해를 가져온다. 따라서 유비쿼터스 환경에서는 보안기술이 필수적이다.

지금까지 이러한 프라이버시 침해문제를 해결하기 위해 많은 연구가 진행되어 왔으며, 킬(Kill)명령어기법[1],해쉬-락기법(Hash-Lock)기법[1,2,3,4],확장된 해쉬-기법(Randomized Hash-Lock)기법[1,4], 외부재암호기법[5],블로커 태그(Blocker-tag) 기법[6], 해수체인(Hash-Chain)기법[7], 그리고 해쉬기반 ID 변형기법[8] 등이 대표적인 예이다.

그러나, Lee, H. & Hong, D. (2006)[9]는 기존의 방법과 다른 SSG(Self Shrinking Generator)에 기반한 태그 인증기법을 제안하였다. 태그 인증 기법에 사용되는 SSG 알고리즘은 W.Meier & O. Staffelbach[10]에 의해 EUROCRYPT94 개발된 것으로써, 출력 비트 스트림(bits stream)를 발생시키기 위해 하나의 LFSR(Linear Feedback Shift Register) 과 선택 로직(Selection Logic)만으로 구성되어 있다. SSG 는 RFID 태그 와 같이 극히 제한적인 자원을 갖는 시스템에서 하드웨어 구현이 매우 용이하고 최적화 할 수 있다. 또한 매 번 생성되는 출력 비트 스트림이 의사난수 역할을 하기 때문에 다양한 공격에 안전하다. 그러나 Lee, H. & Hong, D. 가 제안한 시스템에서는 태그가 매번 인증 세션마다 고정된 metaID 가 전송되기 때문에 공격자는 태그에 대한 위치 추적 이 가능하다는 단점이 있다. 제안한 프로토콜은 매번 세션마다 metaID 값이 새롭게 생성하고, 태그에서 해쉬 연산을 하지 않기 때문에 위치추적에 안전하고 효율적이다.

II. RFID 보안 고려 사항

RFID 시스템은 RFID 태그와 리더(Reader) 사이에 물리적인 접촉 없이 통신이 가능 하다는 특징으로 프라이버시에 관한 문제를 완전하게 보장받을 수 없다. 이러한 특징 때문에, RFID시스템을 구성 하는 경우, 다음과 같은 공격 방법들에 안전하도록 RFID시스템을 설계하여야 한다.

2.1 재전송 공격(Replay Attack)

이 공격의 경우, 공격자는 프로토콜에 능동적으로 참여할 수 없으나 RFID 리더와 태그 간에 상호 전송되는 메시지를 도청(Eavesdropping) 할 수 있다. 이는 단지 프로토콜에서 전송되는 0과 1로 구성된 메시지를 획득 할 수 있다는 것을 의미한다. 공격자는 이러한 도청을 통해 재전송 공격을 수행 할 수 있다. 재전송 공격인 경우, RFID 리더와 RFID 태그 사이에서 전송되는 메시지를 획득함으로써 정당한 RFID 리더나 RFID 태그로 위장 할 수 있다. 이러한 공격이 가능한 이유는 프로토콜이 수행되는 매 세션(Session)마다 동일한 인증 정보를 이용하기 때문이다. 따라서 이를 예방하기 위해서는 공격자가 전송 되는 메시지를 통해 중요한 정보를 획득하기 어렵게 프로토콜을 설계하여야 하며, 매 세션마다 다른 인증 정보를 이용하여야 한다.

2.2 스푸핑 공격(Spoofing Attack)

스푸핑 공격은 공격자가 정당한 RFID 리더로 가장하여 RFID 태그로부터 인증 프로토콜에 필요한 정보를 획득하고, 이 정보를 이용하여 정당한 RFID 태그로 가장하는 공격방법을 말한다. 이 공격을 수행하는 경우, 위치를 추적하고 싶은 RFID 태그에게 계속 하여 질의를 전송함으로써

RFID 태그를 소유하고 있는 주체의 위치를 파악할 수 있어 프라이버시를 침해할 수 있다. 이를 예방하기 위해서는 공격자가 정당한 RFID 리더로 가장하는 것이 어려워야 하며, 세션마다 RFID 태그의 응답이 변화할 수 있도록 난수 등을 이용해서 프로토콜을 설계해야 한다. 또한, 서로 다른 두 응답에 대해서는 동일한 RFID 태그로부터 전송된 메시지임을 구별할 수 있도록 해야 한다.

2.3 트래픽 분석 공격(Traffic Analysis Attack)

트래픽분석 공격은 RFID 리더와 RFID 태그간의 정보를 도청 할 수 있는 공격자가 도청된 내용을 이용하여 인증 프로토콜에 필요한 비밀 정보를 분석하는 공격방법을 의미한다. 이를 방지하기 위해서는 공격자가 도청된 정보를 이용하여 비밀정보와 그렇지 않는 정보를 구분 할 수 있어야 한다.

2.4 위치 프라이버시

RFID 시스템에서 RFID 태그는 의도하지 않게 자신의 위치 정보를 불법적인 RFID 리더에게 전송함으로써 RFID 태그를 소유한 주체는 프라이버시를 침해할 수 있다.따라서 이를 방지하기 위해서는 매 세션마다 갱신되는 RFID 태그의 ID를 사용함으로써 공격자로부터 프라이버시를 보호하여야 한다. 또한 두개의 서로 다른 응답 메시지에 대하여 공격자는 동일한 RFID 태그로부터의 응답인지 구분 할 수 없어야 한다.

2.5 서비스거부 공격(Denial of Service Attack)

서비스 거부 공격은 RFID 리더와 RFID 태그 사이에 전송되는 정보를 통해 유용한 정보를 얻지 못하지만 RFID 리더와 RFID 태그 사이에 통신을 방해할 수 있는 잡음을 첨가 하거나 통신 내용을 왜곡하는 공격방법이다. 이를 예방하기 위해서는 RFID 시스템의 통신을 방해할 수 있는 요소를 사전에 제거하여야 한다.

2.6 물리적 공격(Physical Attack)

물리적 공격은 RFID 태그를 의도적인 도난이나 훼손하는 공격방법을 의미한다. 이를 예방하기 위해서는 RFID 태그를 소유하는 주체가 RFID 태그와 유기적인 결합을 갖도록 설계하여야 하며 외부의 훼손에 대한 저항 정도를 높여야 한다.

Ⅲ. 제안 프로토콜

3.1 SSG(Self-Shrinking Generator)

SSG는 W.Meier & O. Staffelbach[10]에 의해 제안되었다. SSG 는 한 개의 LFSR와 선택로직만을 사용하여 GF(2)에서 m-비트 수열(m-bit sequence)을 생성한다. SSG는 스트림 암호의 키생성자로 사용한다. LFSR의 출력 비트 스트림에서 짝수번째 비트 는 선택 비트로 사용하고 홀수번째 비트는 출력으로 사용한다.

$a_0, a_1, a_2, \cdots$ 일 때 출력비트 스트림 에 대해서 $a_{2i} = 1$인 경우 a_{2i+1}가 SSG 출력비트 스트림으로 사용된다. SSG는 하드웨어 구현에 최적화되어있으며, 아직까지 알려진 공격 알고리즘이 존재하지 않는다. SSG 알고리즘의 구조는 다음과 같다.

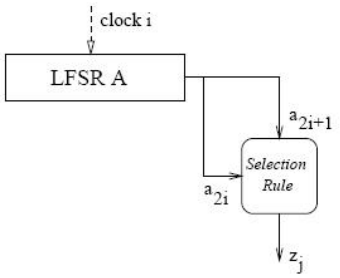

그림1 SSG
Fig. 1 SSG

3.2 제안프로토콜의 구조

본 논문에서 제안하는 프로토콜은 기본적으로 SSG 알고리즘의 안전성에 기반 한다. 제안한 프

로 토콜은 SSG를 이용하기 때문에 태그에 별도의 의사난수 발생기가 필요없다. 제안한 프로토콜에서 사용되는 파라메터는 다음과 같으며, 그림[2]는 제안하는 프로토콜의 기본구조를 나타낸 것이다.

[파라메터]

- ID : 태그 고유의 비밀인증 정보.
- $SSGz_j$: SSG의 출력 값. 태그와 데이터베이스에 SSG 알고리즘이 구현 되어있다.
- $Meta-ID[P,N]$: $Meta-ID$의 Previous 와 New값.
- $Counter-ID[P,N]$: $Counter-ID$의 Previous와 New값. 태그와 데이터베이스의 동기를 위해 사용한다.
- K : 비밀값
- S : 리더가 매 세션마다 생성하여 태그에게 전송하는 난수 n 비트
- $\|$: 연접(Concatenate function).
- $\oplus$: XOR(Exclusive OR)
- R_{tag} : 태그가 생성한 난수
- R_{DB} : DB가 생성한 난수
- $K[P,N]$: 비밀값의 Previous와 New값
- $Meta-ID(N)$: New 생성된 $Meta-ID$ 값
- RNG : Random Number Generator

[구성]

제안한 프로토콜은 다음과 같이 구성되어 있다.

- Tag : SSG,ID $Meta-ID[P,N]$, $Counter-ID$,K,값을 저장하고 있으며, XOR 연산을 4번 수행한다.
- Reader : 난수 발생기 S만 가지고 있으며, 연산은 수행하지 않는다.

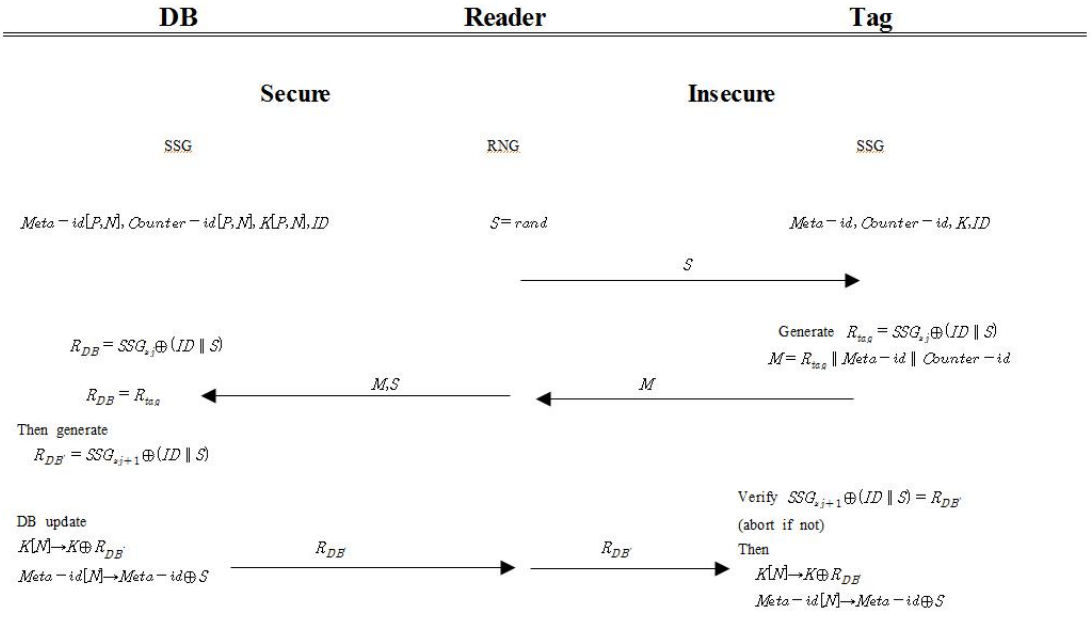

그림2 제안프로토콜의 구조
Fig.2 Structure of proposed protocol

- DB : $Counter-ID[P,N]$, $K[P,N]$ $Counter-ID,ID$ 값과 SSG를 저장하고 있으며, XOR 연산을 4번 수행 한다.

3.3 인증과정

- (Step 1 : 리더) 리드는 태그에게 난수S 를 브로드 캐스팅(Broadcasting)한다.
  리드→태그 : S
- (Step 2 : 태그) 태그는 $SSGz_j$와 ID와 리드의 난수를 연접한 후 XOR하여 새로운 난수 R_{tag}를 생성한다. R_{tag}, $Meta-ID$, $Counter-ID$를 연접하여 리드에 송신한다.
  태그→리드 : M
- (Step 3 : 리드)리드는 태그로부터 수신한 M과 S를 DB로 전송한다.
  리드→DB : M, S
- (Step 4 : 백 엔드 데이터베이스)수신한 R_{tag}와 DB에 저장된 ID와 S를 연접하여 $SSGz_j$와 XOR 한 값을 비교하여 태그를 인정한다.
  계산된 $R_{DB}=SSG_{zj}\oplus(ID \parallel S)$와 수신한 $R_{tag}=SSG_{zj}\oplus(ID \parallel S)$를 비교하여 인증한다.
  새로운 $R_{DB'}=SSG_{zj+1}\oplus(ID \parallel S)$를 생성하여 리드를 통하여 태그에 보낸다. 새로운 키 $K[N]\rightarrow K\oplus R_{DB'}$와, 새로운 $Meta-id[N]\rightarrow Meta-id\oplus S$를 생성하여 DB를 업 데이트 한다.
- (Step 5 : 리드) DB에서 수신한 $R_{DB'}$를 태그에 전송한다.
- (Step 6 : 태그) 수신한 $R_{DB'}$와 태그가 생성한 $R_{tag'}=SSG_{zj+1}\oplus(ID \parallel S)$ 와 비교하여 백 엔드 DB를 인증하고 K와 $R_{DB'}$를 XOR 하여 새로운 키 $K[N]\rightarrow K\oplus R_{DB'}$와, 새로운 $Meta-id[N]\rightarrow Meta-id\oplus S$를 생성한다.

3.4 제안하는 프로토콜의 안전성

3.4.1스푸핑공격에 대한 안전성

매 인증 세션마다 SSG와 S 난수를 사용하여 새로운 난수 $R_{tag'}$를 사용하기 때문에 스푸핑 공격이 불가능하다.

3.4.2 재전송공격에 대한 안전성

공격자가 정당한 리더를 가장하여 S 를 전송하여도 매 세션마다 마다 SSG(스트림암호) 출력과 $R_{tag'}$가 변하기 때문에 획득한 정보로는 재전송 공격이 불가능하다.

3.4.3 트래픽분석 및 위치추적에 대한 안전성

공격자가 정당한 리더로 가장하여 지속적으로 고정된 R_{tag}전송하여도 매 세션마다 $R_{tag'}=SSG_{zj+1}\oplus(ID \parallel S)$ 로 변화기 때문에 공격자는 응답이 동일한 태그인지 알 수 없다.

3.4.4 메시지 가로 채기공격(man-in-the-middle Attack)에 대한 안전성

공격자가 R_{tag}를 임의로 변경하여 리드에게 전송한다면 R_{DB}와 서로 다르기 때문에 무결성을 검증 할 수 있고 메시지 가로 채기공격에 안전하다.

3.4.5정보 전송방해에 대한 안전성

제안하는 프로토콜은 상호 인증(DB와 태그)을 제공함으로서 정보 전송 방해를 인지 할 수 있다.

		해쉬락 기법	화장된 해쉬락 기법	해쉬쉬 체인기 법	해수기 반ID변 형기법	개선된 IDqus 형기법	SSG기 반기법(9)	제안한 프로토 콜
메모리	태그	1.5L	1L	1L	1L	3L	2L	4L
	DB	2.5L	1L	2L	8L	4L	4L	4L
연산량	태그	-	R:1 ,H:1	H:2	H:3	H:2	H:1,XO R:3	XOR:4
	리더	-	H:T/2	-	-	-	H:1	-
	DB	-	-	H:(T/2)i	R:1 H:3	H:(T/2) i	-	XOR :4
연산도 구	태그	HF	RG HF	2HF	HF	2HF	HF SSG XOR	SSGX OR
	리드	-	HF	-	-	-	HF	-
	DB	-	-	2HF	RG HF	2HF	HF SSGXO R	SSGX OR

표1 기존의 프로토콜과 제안프로토콜의 효율성비교
Table 1 Comparison of efficiency between proposed protocol and related protocol

-L: 데이터 필드 크기를 L로 가정
-R : 난수 발생기 연산
-H : 해쉬 함수 연산
- i : 해쉬 함수를 적용한 횟수
-RG : 난수발생기
-HF : 해쉬함수
-T : 태그에 저장된 태그 정보의 개수
-XOR : Exclusive OR

	해쉬-락 기법	확장된 해쉬-락기법	해쉬체인기법	해쉬기반ID 변형 기법	개선된 해쉬 기반 ID변형 기법	SSG 기반 기법 [9]	제안한 프로토콜
스푸핑 공격	×	×	×	×	○	○	○
재전송 공격	×	×	×	○	○	○	○
트래픽 분석공격	×	×	○	○	○	○	○
위치정보 노출공격	×	×	○	×	×	×	○
정보 전송 방해 공격	○	○	○	○	○	○	○

표2 기존의 프로토콜과 제안 프로토콜의 안전성비교
Table 2 Comparison of security between proposed protocol and related protocol

IV. 결론

RFID 시스템은 유비쿼터스 환경에서 객체를 자동인식 함으로서 생활에 많은 편리함을 제공하고 있으나, 다양한 프라이버시 침해를 야기 시킬 수 있다. 지금까지 사용자의 프라이버시 침해를 보호 할 수 있는 방법에 대한 많은 연구가 진행되어 왔으나 기존에 제안 된 여러 보안 기법은 유비쿼터스 환경에 적용하기에는 많은 문제점들이 있다.

본 논문에서는 SSG를 기반으로 안전하고 효율적인 RFID 인증 시스템을 제안 하였다. 제안한 인증기법은 meta id가 매 세션마다 변하기 때문에 위치 추적이 불가능하다. 또한 SSG는 하드웨어적으로 최적화 할 수 있고, 아직까지 알려진 공격 알고리즘이 존재하지 않는다.

참고문헌

[1] S. A Weis, S. E. Sarma, R.L. Rivest, and D. W. Engels,"Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing 2003, LNCS2802,pp.201-212, Springer-Verlag, 2004.

[2] S. Sarma, S. Weis, D. Engeles, "RFID systems and security and privacy implications", in : Workshop on Cryptographic Hardware and Embedded Systems(CHES), LNCS No. 2523, pp.454-469, 2002.

[3] S. Sarma, S. Weis, D. Engeles,"RFID systems & security and privacy implications",Whitepaper MIT-AUTO ID-WH--14,MIT AUTO-ID CENTER, 2002.

[4] S. A. Weis,"Security an Privacy in Radio-FrequencyIdentification Devices" MS Thesis. MIT. May, 2003.

[5] A. Juels and R. Pappu, Squealing Euros : Privacy Protection in RFID -enabled Banknotes", LNCS 2742, pp103-121, 2003.

[6] A. Juels, R. L.Rivest, M.SZydlo, "The BLocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", Procedding of 10th ACM Conference on Press,2003.

[7] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-cost RFID", Proceedings of the SCIS 2004, pp.719-724, 2004.

[8] D. Henrici, and P. Mller, " Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifier", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and communication Workshops(PERCOMW'04), pp.149-153, IEEE, 2004.

[9]. Lee, H. & Hong,D. The tag authentication scheme using self-shrinking generator on RFID system, World Academy of Science, Engineering and Technology Vol. 18 , pp. 52-57. 2006.

[10] W.Meier,S. Staffelbach,"self-shrinking generator", Advances in Cryptology EUROCRYPT'94, volume 950 of LNCS, pages 205-214. 1994.

저자약력

박 택 진(Taek-Jin Park) **정회원**

2005 KAIST/성균관대학교 전기전자 컴퓨터공학과 박사

1987.1~1993.2 한국통신 기술과장

1993.3~ 현재 강릉영동대학교 의료전자과 부교수

<관심분야> 정보보호 및 암호, 암호 알고리즘, 초타원곡선 암호, 해쉬 함수등