안전하고 효율적인 RFID 인증 프로토콜*

서재우*, 염대현*, 이필중*

포항공과대학교 전자전기공학과*

Secure and Efficient RFID Authentication Protocol

Jae Woo Seo*, Dae Hyun Yum*, Pil Joong Lee*

Department of Electronic and Electrical Engineering, POSTECH*

요 약

Radio Frequency Identification (RFID) 시스템은 기존의 바코드를 대신하면서 생산, 공급망 관리, 재고 관리등의 분야에서 중요한 역할을 할 것으로 기대되어지고 있다. 뿐만 아니라, 일상 생활에서도 RFID의 활용 분야는 다양하여 가까운 미래에는 우리 사회 전반에서 중요한 요소로 자리 잡을 것이다. 하지만, RFID 시스템에는 아직 해결해야 될 문제가 남아 있다. 태그로 부터의 원하지 않은 정보 유출로 인한 privacy와 security 문제가 여기에 해당된다. 이 문제를 해결하기 위해서 많은 RFID 인증 프로토콜들이 제안 되었지만, 다소의 문제점들을 가지고 있었다. 본 논문에서는 기존에 제안된 해쉬 함수 기반의 인증 프로토콜들의 문제점들을 분석하고, spoofing 공격 및 location privacy등에 대해 안전하고 효율적인 새로운 프로토콜을 제안한다.

Keywords. RFID 시스템, 해쉬 함수, 인증 프로토콜

I. Introduction

Radio Frequency Identification 시스템은 비접촉식 자동 인식 시스템으로 생산, 공급망 관리, 재고 관리 등에 유용하게 사용될 수 있다. 지난 30년간에 걸쳐서 물류 및 제품 인식 및 관리에는 바코드가 사용되어져 왔다. 1973년에 고안되어진 UPC(Universal Product Code)가 우리가 주변에서 흔히 볼 수 있는 바코드이다. 최근에는 RFID가 바코드를 대처할 수 있는 새로운 아이템으로 떠오르면서, 소비자 시장을 잠식해 나가고 있다. 바코드와는 달리 RFID는 비접촉식으로 여러 개의 아이템을 한 번의 스캔으로 인식할 수 있어, 바코드보다 효율적으로 제품을 관리 할 수 있다. 전 세계에서 매일 스캔 되어지는 바코드가 50억개 이상이라는 것을 고려하면[1], RFID의 잠재적 이익은 결코 적지 않다. 하지만 불행하게도 RFID의 비접촉 무선 인식 기술은 개인의 privacy와 조직의 security를 위협하는 치명적인 문제를 제공한다. 예를 들어 식별 가능한 정보를 그대로 전송하는 태그의 경우, 태그와 리더의 통신 내용을 제 3자가 쉽게 도청 할 수 있다. 도청을 통해 모인 데이터들은 태그 소유주들의 비밀 정보를 유출한다가거나 다른 정보들과 연계 될 경우, 더욱 큰 문제를 야기 하게 된다. 그리고 태그가 방출하는 고유 넘버는 태그 소유주의 이동경로를 파악하여 위치 추적을 가능하게 해 준다. 그러므로 RFID 시스템에 대한 연구 뿐만이 아니라, 시스템의 응용으로 인해 발생하는 여러 security, privacy 문제를 해결하는데도 많은 연구가 이루어져야 한다.

RFID 시스템에 사용되어지는 태그는 능동

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음

형 태그와 수동형 태그로 구분 되어진다. 능동형 태그는 보드상에 파워를 가지고 있어서, 혼자서도 신호를 발산 할 수 있다. 그리고 계산 능력이 높아서 암호학적 알고리즘들을 사용 할 수 있다. 하지만 수동형 태그는 리더가 보내는 전파로 작동하며, 계산 능력과 메모리의 양이 제한되어 계산량이 많은 암호학적 알고리즘들을 적용할 수 없다. 그래서 기존 통신 환경에서 사용되어 왔던 인증 프로토콜들을 RFID에 적용하는 것은 불가능 한다. 본 논문에서 앞으로 언급하는 태그는 계산 능력과 메모리가 극히 제한되어 있는 low-cost RFID 태그로 규정한다. 지금까지 low-cost RFID 상에서 privacy와 security를 보장하기 위한 많은 방법들이 제시되어져 왔다. 그 중에서 우리가 관심을 가지는 분야는 해쉬에 기반한 RFID 인증 프로토콜이다. 남은 장에서 우리는 일반적인 RFID 인증 모델에서 안전하다고 제안되어져 왔던 프로토콜들의 문제점을 분석하고, 개선된 인증 프로토콜을 제안 할 것이다.

II. 가정 및 공격 모델

1. RFID 시스템 가정

RFID 시스템은 기본적으로 태그, 리더, back-end Database로 구성되어진다. back-end Database와 리더의 통신은 유선으로 연결되어 있고 메모리와 계산 능력이 상대적으로 제한되어 있지 않기 때문에 암호학적 알고리즘을 사용 할 수 있는 안전한 채널이라고 가정한다. 반면, 리더와 태그 사이의 통신은 무선 구간으로 공격자가 개입할 수 있는 오픈 채널이라고 가정한다. 공격자는 리더와 태그의 통신 내용을 도청 혹은 기록하여 replay 공격이나 spoofing 등을 할 수 있다.

2. 공격 모델

기존에 제안 되어졌던 인증 프로토콜들은 존재하는 공격 방법들에 대해 안전하다는 것을 보이므로써, 제안한 프로토콜이 안전하다는 것을 보였다. 그 내용을 정리해 보면 다음과 같은 4가지의 공격 방법들이 제시 되어진다.

- **Eavesdropping** - 리더와 태그간의 통신 방식은 무선 구간으로 공격자는 통신 내용을 쉽게 엿들을 수 있다. RFID 시스템에서 eavesdropping은 불가피하다고 가정하더라도, 공격자는 통신 내용으로부터 privacy와 security를 위협하는 어떠한 정보도 알 수 없어야 한다.

- **Spoofing** - spoofing이란 정당하지 않은 개체를 정당한 것처럼 속여 인증과정을 통과하거나 통신을 방해하는 것을 말한다. spoofing은 대상에 따라 2가지로 나누어진다. 정당하지 못한 태그가 리더를 속이거나, 혹은 정당하지 못한 리더가 태그를 속이는 경우이다. 위 공격 방법을 막기 위해서는 태그와 리더간의 인증이 요구 되어진다.

- **Location privacy** - RFID의 태그가 리더의 질문에 항상 동일한 값으로 응답을 할 경우, 공격자는 태그의 위치 변화를 감지 하므로써, 이동경로를 파악할 수 있다. 태그와 리더 사이의 통신에서는 항상 동일한 값이 사용되는 경우가 없어야 한다.

- **Message loss** - 공격자의 고의적인 통신 방해나 시스템의 문제로 인해 인증 세션이 비정상적으로 종료되어 태그와 back-end Database의 동기가 어긋날 수 있다. 이 때 Database는 태그의 ID를 잃어버리거나, ID를 찾기 위해서 exhaustive search가 요구 되어진다. 이와 같은 문제는 태그와 Database가 동기를 맞추어야 하는 동기식(synchronous) 프로토콜에서 발생한다.

다음 장에서는 제시된 공격 모델들에 대해서 안전한 프로토콜을 설계하기 위해서 고려해야 될 사항들과 효율성 측면에서 고려해야 될 사항들을 살펴 볼 것이다.

III. 프로토콜 설계 시 고려 사항

1. 안전성 측면

Eavesdropping - 태그와 리더간의 통신 내

용을 공격자가 도청하는 것을 막을 수는 없다. 그렇지만 해쉬 함수의 일방향성을 이용하여 공격자가 통신을 도청하더라도 tag의 정보를 알수 없도록 하여야 한다.

Spoofing - 첫 번째, 공격자가 태그로 가장하는 경우를 방지하기 위해서 리더는 태그에게 인증을 요구해야 한다. 인증 방식은 랜덤한 값을 태그에게 주고, 태그로부터 그 값에 의존하는 응답을 요구하는 것이다. 여기서 리더에 대한 태그의 응답은 태그만이 만들어 낼 수 있어야 한다. 이럴 경우, 공격자는 리더의 질문에 응답할 수 없다. 두 번째, 공격자가 리더로 가장하여 태그에 접근하더라도 eavesdropping에 대해 안전하다면, 공격자는 태그의 정보를 알수 없다.

Location privacy - 태그는 리더와 공격자의 질의에 대해 매 번 다른 값으로 응답하여야 하며, 공격자는 태그의 다음 응답을 추측할 수 없어야 한다. 이 조건을 만족하기 위해서 태그는 랜덤한 값을 만들어 낼 수 있어야 한다.

Message loss - 이 문제는 동기식 프로토콜에서 공격자가 태그에게 질의를 해서 동기값을 고의적으로 어긋나게 만들기 때문에 발생한다. 이를 막기 위해 동기값을 고정시킬 경우, location privacy에 안전하지 못하게 된다. 다른 방법으로는 비동기식(asynchronous) 프로토콜을 고려할 수도 있지만 비동기식 프로토콜은 exhaustive search를 해서 ID를 확인하기 때문에, 효율성이 떨어진다. 하지만 태그와 Database만이 알고 있는 키를 사용할 경우, 비동기식 프로토콜에서 exhaustive search를 하지 않고 ID를 확인할 수 있다.

2. 효율성 측면

태그에서의 해쉬 연산 - 태그의 계산 능력은 극히 제한되어 있다. 그래서 계산량이 많은 연산은 사용 할 수 없다. 설계 시 해쉬 연산은 최소가 되도록 설계하여야 한다.

태그와 리더의 패스 - 태그와 리더 사이의 패스가 많아질수록 태그의 부담은 커진다. 또한 같은 시간 리더가 스캔 할 수 있는 태그의 개수도 줄어든다. 효율적인 RFID 시스템의 적용을 위해서 리더와 태그의 패스는 최소화 되어야 한다.

R/W 메모리 - 태그에 들어가는 메모리의 개수는 태그의 가격을 결정하는 중요한 요소이다. 이 중에서 R/W 메모리는 다른 메모리들(ROM, RAM)에 비해서 더 많은 비중을 차지한다. 프로토콜 메모리의 사용을 최소화하도록 설계해야 한다.

ID 변경 - 리더의 질의 때마다, 태그의 ID가 변하는 프로토콜은 ID의 관리를 위해 부가적인 노력을 요구한다. 또한 다른 태그끼리 같은 ID를 공유하는 경우가 발생할 수 있다. 태그의 ID

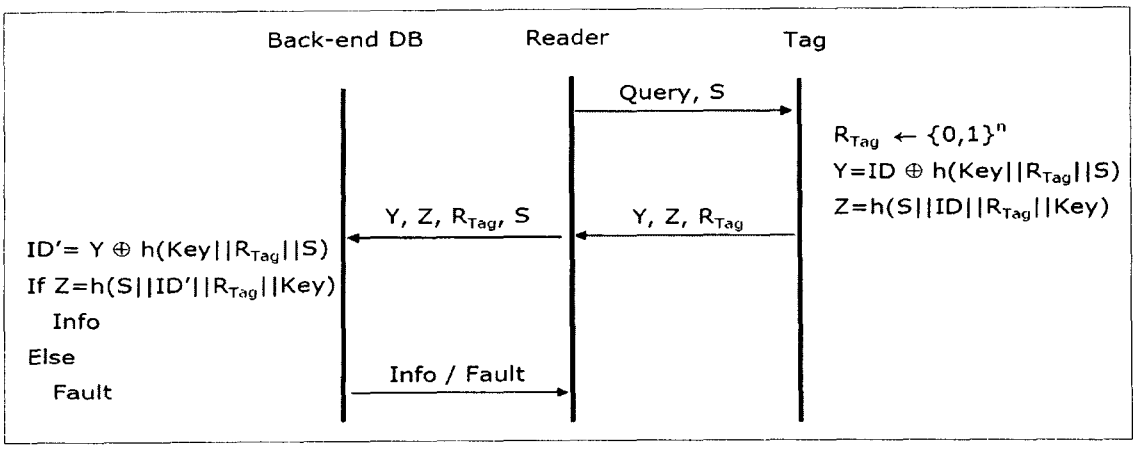

그림1. 제안하는 프로토콜

관리를 용이하게 하기위해서는 ID가 변하지 않은 프로토콜을 사용해야 한다.

IV. 제안하는 프로토콜

1. 프로토콜

우리가 제안하는 프로토콜은 모든 태그와 back-end Database가 동일한 Key를 소유하고 있다고 가정한다. 그림1은 제안하는 프로토콜에서 태그의 인증 과정을 나타낸 것이다.

- **프로토콜에 사용되는 파라미터**

  *ID : 태그의 고유 인식 번호
  *Key : 태그와 ID가 가지고 있는 비밀키
  *R_{Tag}, S : pseudo-random number.
  *h(): one way hash function
  *|| : 문자열 연접.
  *⊕: XOR.

- **프로토콜 인증 과정**

태그가 인증 되어지는 과정은 다음과 같다

1단계: 리더는 태그에게 질의를 하면서 pseudo random number S를 보낸다.

2단계: 질의를 받은 태그는 pseudo-random number R을 뽑아서 $Y=ID\oplus h(key||R_{Tag}||S)$와 $Z=h(S||ID||R_{Tag}||key)$을 계산하여 Y, Z, R_{Tag}을 리더에게 보낸다.

3단계: 리더는 태그에게 보내었던 S와 Y, Z, R_{Tag}을 같이 back-end Database에 보낸다.

4단계: Database는 Y로부터 태그의 ID'를 복원하고 정당한 ID인지를 확인하기 위해 $h(S||ID'||R_{Tag}||Key)$을 계산하여 Z와 비교한다. 만약 복구 되어진 ID'이 태그의 ID와 동일하다면 Database는 태그를 정당하다고 인정하고 태그의 정보를 전송하지만 그렇지 않을 경우에는 리더에게 Fault를 내보낸다.

2. 안전성 및 효율성 분석

표1은 제안하는 프로토콜을 기존의 프로토콜들에 대해서 안전성과 효율성 측면에서 비교한 것이다. 표1은 제안하는 프로토콜이 기존의 프로토콜보다 안전하면서 효율적이라는 것을 보여 준다.

V. 결론

지금까지 본 논문에서는 프로토콜 설계 시, 고려사항을 분석하고 새로운 프로토콜을 제안하였다. 제안한 프로토콜은 기존의 프로토콜이 만족하지 못했던 모든 공격에 대해 안전하며, 서버에서의 계산량 과다로 인해 시스템에 적용이 불가능 했던 것과는 달리, 효율적인 RFID 인증 프로토콜이 요구되는 시스템에도 적용이 가능하다.

구 분		[2]	[3]	[4]	[5]	[6]	[7]	[8]	제안하는 프로토콜
안전성	Eavesdropping	O	O	O	O	O	O	O	O
	Spoofing	X	X	O	O	O	X	O	O
	Location privacy	O	X	O	O	O	O	X	O
	Message loss	X	X	X	X	X	X	X	O
효율성	태그에서 해쉬 연산	1	3	2	2	1	3	2	2
	리더와 태그 사이의 패스	2	3	2	3	3	4	3	2
	R/W 메모리	필요 없음	필요	필요	필요 없음	필요	필요	필요	필요 없음
	ID 변경 여부	ID 고정	ID 변경	ID 고정	ID 고정	ID 고정	ID 변경	ID 변경	ID 고정

표1. 프로토콜 비교

[참고문헌]

[1] EAN International and the Uniform Code Council. http://www.ean-int.org

[2] S. A. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identification systems. Frist International conference on Security in Pervasive Computing, SPC 2004.

[3] D. Henrici and Paul Muller. Hash-based Enhancement of Location Privacy for Radio Frequency Identification Devices using Varying Identifiers. PerSec04 at IEEE PerCom, 2004.

[4] M. Ohkubo, K. Suxuki and S. Kinoshita. Cryptographic Approach to "Privacy-Friendly" 태그s. RFID privacy workshop, MIT MA USA, 2003.

[5] J. Kwak, K. Rhee, S. h. oh, S. J. Kim, and D. G. Won. RFID System with Fairness Within the Framework of Security and Privacy. ESAS 2005.

[6] E. Y. Choi, S. M. Lee, and D. H. Lee. Efficient RFID Authentication Protocol for Ubiquitous Computing Environment. EUC Workshops 2005.

[7] J. Kang and D. Nyang. RFID Authentication Protocol with Strong Resistance Against Traceability and Denial of Service Attacks. SAS 2005.

[8] S. M. Lee, Y. J. Hwang, D. H. Lee, and J. I. Lim. Efficient Authentication for Low-Cost RFID Systems. ICCSA 2005.