RFID 시스템에서의 태그 보안을 위한 경량화 프로토콜의 분석

김정태*

Analyses of Light-weight Protocol for Tag Security in RFID System

Jung Tae Kim*

요 약

RFID 는 유비쿼터스 환경하에서 필수불가결한 기술이 되도 있다. 그러나 RFID 의 본질적인 단점으로 인하여 프라이버시와 같은 보안적인 취약점을 기자고 있다. 따라서 본 논문에서는 RFID 시스템의 관점하에서 태그에서의 보안적인 취약점 및 이럴 해결하기 위한 여러 가지의 프로토콜에서의 문제점을 분석하였다. 최근에는 반도체 공정 기술의 발전과 경량화프로토콜의 발전으로 인하여 태그에서의 보안성이 향상되고 있는 중이다.

ABSTRACT

Radio Frequency Identification(RFID) has been considered as an key infrastructure for the ubiquitous society. However, due to the inherent drawbacks, RFID causes var- ious security threats like privacy problems, tag cloning, etc. This paper analyses the security risk analysis process from the perspective of the RFID tag life cycle, identify the tag usage process, identify the associated vulnerability and threat to the confidentiality, integrity and availability of the information assets and its implications for privacy, and the mitigate the risks

키워드
RFID 프로토콜, 인증 알고리즘, 보안성, 취약점 분석

Key word
RFID Protocol, Authentication Algorithm, Security, Vulnerability Analyses

* 종신회원 : 목원대학교(교신저자, jtkim3050@mokwon.ac.kr)

접수일자 : 2011. 10. 28
심사완료일자 : 2011. 10. 28

Ⅰ. 서 론

일반적으로 RFID 기술은 유비쿼터스 환경하에서의 원거리에 있는 물체를 인식하는 기술 중의 하나이다. RFID(Radio Frequency Identification)는 각종 물체에 소형 칩을 부착해 사물 및 센서노드와 같은 주변 환경정보를 무선 주파수로 전송 및 처리하는 비접촉식 인식 시스템이다. 1980년대부터 등장한 RFID 시스템은 근거리 통신 또는 무선 식별 시스템이라고도 불린다. 전형적인 RFID 시스템은 태그, 리더기, 백 엔드 서버로 구성되어 있다. 일반적으로 리더기는 태그의 반응을 서버에 전달하는 역할을 한다. 백 엔드 서버는 태그의 반응에 대한 태그에 대한 정보를 인증하는 역할을 한다. 최근에는 이러한 RFID 시스템이 많은 응용 분야에 사용되고 있으며 보안성과 취약성에 대한 많은 문제를 야기 시킨다. 일반적으로 RFID 태그는 물체, 동물, 사람등과 같은 인식을 위한 방법으로 무선을 사용하여 부착된다. 이러한 이유로 인하여 악의적인 많은 현상들이 태그의 정보를 유출하기 위한 여러 가지의 방법 등이 제시되고 있다. 하지만 RFID는 무선 주파수를 이용한 태그와 리더간의 통신으로 인해 RFID 보안 및 사용자의 프라이버시 침해라는 문제점을 야기한다. 현재가지 이러한 문제점을 해결하기 위한 다양한 방법들이 연구되고 있다 [1]. 따라서 저가의 RFID 시스템을 구성하기 위한 필수적인 요구조건이 필요하다. 이러한 저가의 시스템에서 발생하는 기본적인 위협 요소와 보안성에 대한 취약점은 다음과 같은 보안성을 만족하여야 한다. 외부의 공격자는 다양한 공격을 시도하여 RFID 시스템에 대한 보안 및 프라이버시에 대한 문제를 야기 시킬 수 있다. 태그와 리더기 사이의 무선통신을 도청할 수도 있고, 정당하지 않은 리더기를 이용하여 태그로 부터 얻은 정당한 정보를 리더기의 요청에 의해 스푸핑 공격(Spoofing Attack) 을 할 수 도 있다. 공격자는 도청한 데이터를 재전송하는 재생 공격(Reply Attack)과 메모리에 저장된 정보를 알아내기 위해 별도의 암호학적인 보안성을 가지지 않는 저가의 태그에 대한 물리적인 공격(Tampering Attack)을 시도할 수도 있다. 또한 보안 요구사항 이외에도 개인정보 노출이나 위치 정보 추적 등의 프라이버시 위협에 대한 요소도 존재한다.

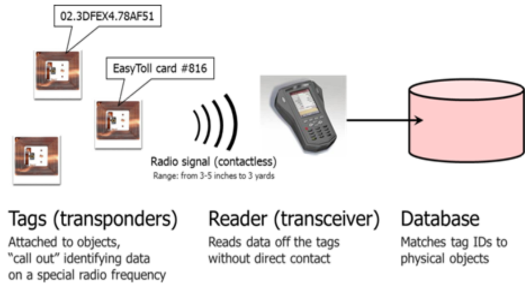

그림 1. 기본적인 RFID 시스템 구성도
Fig. 1 Configuration of basic RFID System

저가의 RFID를 설계하기 위해서는 태그 측에서의 계산 성능에 관련된 문제이다. 이러한 문제는 제한된 연산 능력, 저 용량의 메모리, 낮은 전력 등의 문제를 가진다.

Ⅱ. 관련 연구

저가의 RFID를 위한 보안 기법을 내장한 설계가 많이 연구되고 있으나, 기존의 방법인 일방향 해쉬함수를 사용한 기법들이 사용되었는데, 이는 저가의 태그 구현에 적합하지 않다. 이러한 연구와는 상반된 개념으로 태그에 해쉬함수를 지원하는 구조로 설계할 경우, 태그의 저용량 리소스로 인하여 고비도의 암호 알고리즘을 제공하기는 불가능 한다. 그러나, 이러한 기법은 보안상의 취약성을 가진다. 최근에 Li 등은 오직 bitwise XOR에 기반한 랜덤수를 가진 저가에 적합한 인증 프로토콜을 제안하였다 [2]. 기존의 암호화 기법인 암화화 알고리즘, 해쉬함수 등과 같은 종래의 암호학적인 요소기술이 아닌 단순한 XOR와 Substring을 사용한 방법을 제시하였다 [3]. RFID 시스템에서 보안성을 위협할 수 있는 공격으로 도청, 트래픽 분석 등의 수동적 공격과 위조, 서비스 거부 공격 등의 능동적 공격들이 있으며, 이런 공격들로부터 안전한 RFID 시스템 설계를 위해서는 전달되는 인증 정보의 기밀성 및 무결성, 태그 식별 정보의 익명성 등의 기본적인 보안 요구사항이 만족되어야 한다. 하지만 RFID 시스템의 경우, 연산 능력과 저장 능력에 제한이 있으므로 기존의 공개키 방식이나 대칭키 방식의 암호화 알고리즘을 적용하기는 적절하지 않다.

초기 RFID 보안 대책으로 kill tag, faraday case, active jamming, blocker tag를 이용한 방식들이 알려졌으며 이

후 해쉬 연산을 이용한 해쉬락, 재암호화, 해쉬체인 방식 등이 소개되었다[2]. 최근에는 경량화된 대칭키 및 공개키 암호에 대한 연구가 활발히 연구되고 있다.. 이러한 보안 문제점을 해결하기 위한 많은 연구결과들이 발표되었다. Air Juels 가 발표한 논문에 따르면 저가 소형의 RFID 태그 사용에 있어 프라이버시와 인증 문제를 주요 보안 주제로 언급했으며, 이를 극복하기 위한 방법으로 태그 Killing, 태그 Sleeping 과 같은 물리적인 기법, 암호학적인 재암호화 방법과 같은 정보 변경 방법, RFID Enhancer Proxy 방법들이 발표되었다[3]. 그러나 지금까지 발표된 연구결과의 대부분은 태그 내부에서의 실질적인 대칭키 암호 연산을 통한 보안 문제 해결로 접근하는 연구결과를 찾아보기 힘들다. 특히 수동형 RFID 태그가 가지는 자원 제약적인 환경 때문에 실제적인 표준 알고리즘인 AES 알고리즘을 사용하는 프로토콜의 사용이 현재 개발 진행 중에 있다.

일반적으로 저가형 태그는 배터리가 없어 제한적인 연산 능력과 메모리 공간을 가진 것으로 간주되고 있다. 하지만 기술적인 발전으로 인하여 최근에는 저가형 태그에 적합한 암호 알고리즘에 대한 연구가 활발히 진행중에 있으며 A.Bogdanov 등은 저가형 태그 보안을 위한 보안 프리미티브의 요구사항인 2000 게이트 이하, 10uW 이하의 소비 전력, 10,000 클럭 사이클을 만족하는 암호학적 해쉬 함수의 구현이 가능하다는 연구 결과를 발표하였다[4]. 또한 M Feldhofer 등은 AES(Advanced Encryption Standard) 역시 저가형 태그에 구현이 가능하다는 연구 결과를 발표하였다[5].

Ⅲ. 보안 및 프라이버시 요구사항

일반적으로 위에서 언급한 위협 요소를 해결하기 위해서는 RFID 프로토콜은 다음과 같은 요구사항을 충족하여야 한다[6].

1) 기밀성(Confidentiality) : 태그와 리더사이의 모든 통신이 공격자에게 도청되더라도 어떠한 의미 있는 정보도 노출되지 않아야 하는 성질을 말한다. 즉 악의적인 제 3자가 도총을 하더라도 어더한 정보를 획득할 수 없어야 한다.
2) 태그에 대한 익명성(Tag anonymity) : 공격자가 태그와 리더와의 통신을 통해서 태그의 위치를 추적하거나 감사할 수 없어야 한다는 성질을 말한다. 이러한 성질을 만족하기 위해서는 프로토콜 상에서 구별 불가능성(Indistinguishability)와 전방향 안전성(Forward Secrecy)를 만족해야 한다. 구별 불가능성이란 태그에서 전송되는 정보를 통해서는 어떠한 태그로 부터 정보인지 구분을 할 수 없어야 하며, 전방향 안전성은 태그의 현 데이터가 노출되더라도 이전의 데이터가 추적되지 않아야 한다는 성질이다.
3) 상호 인증(Mutal Authentication) : 상호 인증은 태그와 리더가 서로 정당한 객체임을 확인하는 과정이다. 어느 한 방향의 인증 과정이라도 만족하지 않는다면 공격자는 재생 공격이나 스푸핑 공격을 통하여 태그나 리더에 대한 위조가 가능하다.

일반적으로 성능 분석을 위하여 다음의 3가지의 요소를 측정한다.

1) 계산적인 오버헤드(Computational overhead)
2) 저장 오버헤드(Storage overhead)
3) 통신 오버헤드(Communication overhead)

위의 관점에서 보면 태그에 해쉬함수 혹은 RNG (Random Number Generator)를 사용하면 태그의 제작시에 가격적인 면에서 가격이 상승할 수 있다. 암호 연산을 위해 사용 가능한 크기는 현재의 기술로 5K 이하의 기술로 집적화될 수 있으며, 가격은 수 센트 이내로 가능하다. (그림2)는 태그의 일반적인 특성을 도식화 한 그림이다.

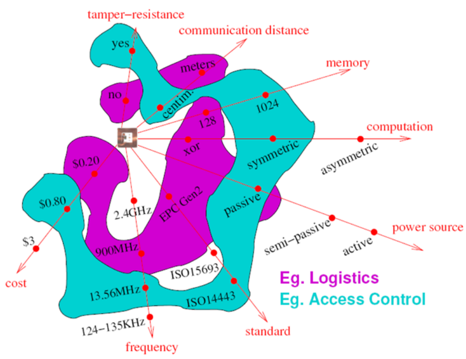

그림 2. 태그의 특성
Fig. 2 Characteristics of Tag

Ⅳ. 보안성 향상을 위한 기법

현재까지 제안된 RFID 인증기법을 태그에서의 연산 능력과 저장능력에 따라 크게 네 가지 형태로 분류하면 첫째, 중량 인증방식은 해시함수, 암호화, 공개키 알고리즘 등 전통적 암호기법을 사용하는 프로토콜이다. 둘째, 단순인증 방식은 난수생성기와 일방향 해쉬함수를 사용하는 프로토콜이다. 셋째, 경량인증방식은 EPC class-1 Gen-2 가 PRNG와 CRC만 지원하기 때문에 해쉬함수를 사용하지 않고 난수 생성과 CRC만 사용하는 프로토콜이다. 넷째, 초경량 인증방식은 xor, and, or 같은 간단한 비트연산만을 사용하는 프로토콜이다 [6]. 저가의 태그는 제한적인 연산능력과 저장 공간의 한계로 인해 대칭키, 공개키, 해쉬 같은 전통적인 암호기법의 사용이 힘들다. 이러한 저가형 태그를 위한 저비용의 안전한 인증기법과 암호기법의 연구를 필요로 하고 있다. 다음은 안전한 RFID 시스템을 위한 현재까지 연구 중인 대표적인 프로토콜이다 [7].

1) 해쉬기반 프로토콜(Hash-based Protocols)
2) LPN 기반 프로토콜(LPN based Protocols)
3) 초경량 프로토콜(Ultra-light Protocols)
4) Universial Composability Protocols
5) 다중 태그 스캐닝 프로토콜(Multi Tag Scanning Protocols)
6) 거리 반송 프로토콜(Distance bounding Protocols)
7) RFID에 대한 부채널 분석 및 방지 (Side channel analysis and protection)

일반적으로 RFID 프로토콜의 취약성을 살펴보면 다음과 같다 .프로토콜의 보안성을 강화하기 위하여 일반적인 연산적인 방법이 태그에서의 용량에 의하여 기존의 방법이 사용되기가 어렵다. 따라서 태그에서의 정보를 유출하기 위한 외부의 여러 가지의 공격에 대한 방법을 고려하여야 한다. 따라서 다음의 사항을 고려하여야 한다.

- Secrecy/Authentication
- Indistinguishables/Tracking/Passive Repaly
- Forward Security

표 1. 서로다른 프로토콜에서의 보안 분석[8]
Table. 1 Comparison of Security Analyses for Different Protocols[8]

	LMAP	M2AP	EMAP	SASAI	JK
Mutual Auth.	0	0	0	0	0
Eavesdropping	X	X	X	0	0
Replay attack	X	X	X	X	0
Spooping	X	X	X	X	0
DOS	X	X	X	X	0
Location Tracking	X	X	X	X	Δ
Forward attack	X	X	X	X	Δ

따라서 기존에 발표된 여러 가지의 프로토콜을 정리를 해 보면 다음과 같다. 랜덤 수 적용 기법을 사용한 경우로서 일반적으로 태그는 리더로 부터 쿼리를 받을 때마다 자신의 메타아이디를 리더로 보냄으로써 응답한다. 그러면 리더는 그 메타아이디를 서버에 전달한다. 하자만 태그가 반복적으로 동일한 메타아이디를 사용하기 때문에 공격자에게 쉽게 파악 당할 수 있다. 이에 Weis 등은 임의의 접근 제어가 가능한 랜덤 수 발생기를 고안하였다. 의사 난수 발생기 및 CRC 기법으로 EPC global C1 GEN2 RFID 태그를 이용한다. 여기에는 의사 난수 발생기와 CRC(Cyclic Redundancy Code)를 사용한다. 프로토콜의 경우 한번 실행 후 그 다음의 실행에서 인이 성공하기 이전 과정에서의 공격을 예방 하지는 못하는 문제로 인하여 서비스 거부 공격 (Denial of Service attack)이 서버와 태그 사이의 일관성을 영원히 파괴시킬 수 있다. 만약 고정된 EPC 코드와 접근키 PIN의 기밀이 누설된다면, 이전단계 추적 방지 기능 또한 제공되지 않게 된다. 최근에 많이 연구되고 있는 분야인 상호 인증 기법이다. 서버의 데이터베이스는 인증키와 접근키 두개의 복사본을 가지고, 이를 이용해서 성공적으로 세션을 마친다. 하지만, 이 프로토콜 역시 신뢰할 수 없는 리더에 대해서는 고려하지 않은 단점이 있어 공격자들의 표적이 될 수 있다. 이렇게 제안된 대부분의 프로토콜들은 태그에 복잡한 해쉬 함수 혹은 암호적인 기능을 하는 함수를 요구하고 있다. 또한 최근에는 JK 프로토콜과 같이경량화프로토콜을 사용하기 위하여 XOR연산을 사용하여 키 값을 분리하여 암호화강도를 향상시키기 위한 방법등이 연구되고 있다.

V. 결 론

RFID는 유비쿼터스 환경에서 센서네트워크과 물체의 인식 기술에서 반드시 해결해야 될 부분이 보안성 문제이다. 따라서 본 논문에서는 이러한 RFID 시스템에서 요구되는 보안성 문제와 보안성을 향상시키기 위한 기법에 대해 분석하였다. 태그에서의 연산능력의 부족으로 인하여 위협요소가 발생하고 있다. 따라서 이러한 문제점을 해결하기 위한 성능 분석 및 위협요소에 대한 분석이 필수불가결하다. 또한 이러한 요소를 해결하기 위한 방법중의 하나로 경량화된 프로토콜을 제안하여 문제를 해결하기 위한 여러 가지의 연구가 진행중에 있다. 이 또한 디지털논리로 구현 할 경우 태그에서의 면적의 문제로 인하여 해결이 어려움에 처할 수 있다. 다하서 반도체 칩의 공정 및 간단한 프로토콜의 개발이 필수적인 대안으로 자리를 잡을 것으로 생각된다.

감사의 글

이 논문은 2011년도 교육과학기술부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2011-0026950)

참고문헌

[1] Chien, H., & Chen, C. Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. Computer Standards &Interfaces, 29(2), 254 - 259. 2007.

[2] Hung-Yu Chien and Chen-Wei Huang, "A Lightweight Authentication Protocol for Low-Cost RFID", Journal of Sign. Process Syst.,DOI 10.1007/s11265-008-0281-8, 2008

[3] Shijie Zhou, etcs "A lightweight anti-desynchronization RFID authentication protocol", Inf Syst Front, DOI 10.1007/s10796-009-9216-6, 2009

[4] Jung-Hyun Oh, etcs, "A Secure Communication Protocol for Low-cost RFID System", Seventh International Conference on Computer and Information Technology, pp.949-954, 2007.

[5] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "EMAP: A Efficient Mutual Authentication Protocol for Low-Cost RFID Tags," Proc. OTM Information Security Workshop (IS '06), pp. 352-361, 2006.

[6] H.-Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 4, 2007, pp.337-340.

[7] Faouzi Kamoun. "RFID System Management: State-of-the Art and Open Research Issues" IEEE Transactions on Network and Service Management, V.6, N. 3, pp.190-205, Sep. 2009

[8] J.D.H, etcs, "Strong Authentication and improving privacy with ultra-weight RFID authentication Protocol", KIISC, v.19, n.19, pp.81-91, 2009

저자소개

김정태(Jung Tae Kim)

2001년 8월 : 연세대학교 대학원 전자공학과 박사
1991년 8월~1996년 2월 : 한국전자통신연구원(ETRI) 선임연구원
2002년 10월~현재 : 목원대학교 전자공학과 교수
※관심 분야: Network Security, 보안 컨설팅, RFID& USN Security, ASIC Design.