센서 태그를 이용한 보안 장치 구현

김상춘*, 박지만**

요 약

센서 모듈을 이용한 물리적인 정보보호 기능을 제공하는 수동 SID 센서 태그를 제안한다. 제안한 보안 센서 태그는 기본적으로 직렬 I/O 인터페이스 모듈, 제어 모듈, 센서모듈로 구성된다. 본 논문에서는, 저항 기반의 센서 신호 데이터를 비교하고 암호화하여 센서 태그의 정보보호 기능을 나타냈다. 제안한 수동형 SID 센서 태그는 상품의 안전, 위조 및 변조 식별, 등을 실시간으로 관리할 수 있다. 또한, 변환기를 이용한 수동형 SID 센서 태그는 광범위한 물리적 정보보호 응용에 활용될 것으로 기대한다.

A security implementation based on the sensor tag

Sang-Choon Kim*, Ji-Mann Park**

ABSTRACT

This paper describes a passive SID sensor tag that provide physical security functions based on a sensor interface module. It elementarily consists of a serial I/O interface, control module, and sensor module. In this paper, it show tamper-proof security functions by comparison and encryption with the sensor signal data using the physical resistors. The passive SID sensor tag can be realized by the real time management for the safety, forgery, and so on. The proposed SID tag embedded with a sensor module is expected to find wide physical security applications.

Key words : RFID, SID, Physical Security

접수일(2011년 3월 10일), 수정일(1차: 2011년 3월 21일), 게재확정일(2011년 3월 23일)

* 강원대학교/정보통신공학과
** ETRI/한국전자통신연구원

1. 서 론

대부분의 센서 태그는 태그 내부에 배터리(battery)를 포함하는 능동 센서 태그이다. 최근 들어, 배터리 없이 센서 인터페이스 모듈을 내장한 수동 RFID(Radio Frequency Identification) 태그 칩이 소개되었다[1]-[3]. 이러한 센서 장치가 포함된 RFID 태그는 계측 제어분야에서 응용하고 있다[4]-[5]. 기존에 있어서, 센서 태그는 센서와 태그가 각각 분리되어 계측 시스템에서 주로 사용되어 왔다.

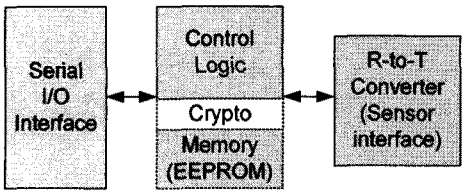
현재, 시장에서 활용되는 보안 RFID 태그는 데이터 공격에 대항하여, 태그와 리더기 사이의 데이터를 암호화하여 통신한다. 이를 위해, 암호 알고리즘을 하드웨어 또는 소프트웨어로 구현하여 RFID 태그 칩으로 제작한다[6]-[7]. 최근에, 이러한 보안 태그도 지능화된 다양한 공격에 정보 보호된 데이터가 해독되는 사례가 발생한다. 이러한 지능화된 공격의 예로, 태그 자체를 물리적으로 복제하거나 태그의 메모리에 저장된 데이터를 탬퍼-탐침(tamper-probe)하는 방법이 있다.

이에, 본 논문은 이러한 공격에 대항하여 센서와 SID(Serial Identification) 태그를 융합한 보안을 제안한다. 물리적인 센서의 센서 값을 정보 보호 데이터로 활용한 사례는 없었다. 제안하는 수동형 센서 태그는 측정된 데이터를 물리적 보안 개념으로 활용하는 새로운 것이다. 본 논문의 센서 내장형 보안 SID 센서 태그는 고가의 농수산물, 의약품, 음료, 미술품, 상품권, 등에 부착하여 사용할 수 있다. 이들 상품에 있어서, 음료와 의약품의 뚜껑을 개방하거나, 미술품 및 농수산물의 포장지를 개방할 때, 부착된 태그의 센서 저항이 변화한다는 것을 알 수 있다. 본 논문의 수동형 SID 센서 태그는 센서의 변화를 인식하여, 이들 상품의 진품명품, 안전관리, 위조 및 변조 검사, 등 다양한 관리를 실시간으로 실현할 수 있다.

2. 센서 태그의 보안 장치

센서 태그는 무선 기반의 RFID 센서 태그와 유선 기반의 SID 센서 태그로 구별된다. 이들은 I/O 인터페이스로 구별하였고, 본 논문은 유선 기반의 직렬 인터페이스 모듈을 갖는 SID를 사용하여 정보보호 기능을 실현한 것이다. SID 시스템의 인터페이스 동작에 따르면, 리더기는 태그에 질의 요청하고, 태그는 리더기에 대응하는 응답을 보낸다.

그림 1은 변환기를 이용한 물리적인 보안 기능을 가지는 수동형 SID 태그를 나타냈다. 이 그림에서는 저항차-시간차 변환기를 이용한 수동형 SID 태그는 EEPROM(R/W) 메모리 사용한다[8].



(그림 1) 수동현 SID 센서 태그

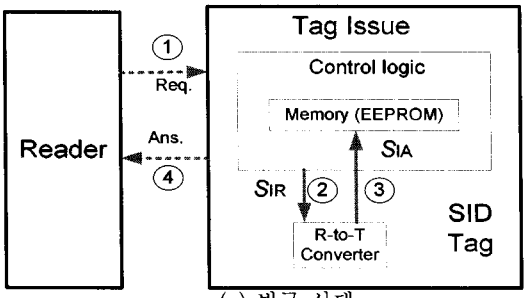
정상적인 보안 SID 시스템은 데이터 침입자에 대항하여 리더기와 태그 사이의 통신에 있어서 중요한 데이터를 암호화하여 보호한다. 본 논문에서는, 이러한 데이터 보호를 한층 더 강화하기 위해, 센서 모듈 즉, 저항차-시간차 변환기를 이용하였다. 또한, 본 논문에서, 센서 인터페이스를 내장한 SID 태그는 암호 기반의 정보보호 기능을 부가하여 물리적인 재사용 방지 기능을 제공한다. 바꾸어 말하자면, SID 태그가 몇몇 물리적 침입 흔적과 태그의 파괴된 모양이 발생할 때, SID 시스템에서 이를 실시간으로 쉽게 감지할 수 있다. 이러한 센서를 이용한 물리적인 보안 기술은 새로운 정보보호 개념이다.

재사용 방지 보안 태그를 제공하기 위해, 센서 인터페이스를 내장한 SID 태그는 센서의 저항 값을 측정한 디지털 코드 값을 메모리에 저장 또는 리더기를 통해 안전한 서버에 저장한다.

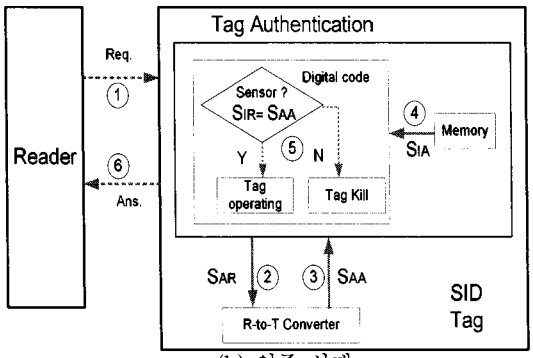
먼저, EEPROM 메모리를 포함한 센서 인터페이스를 내장한 수동형 보안 태그의 동작 시나리오를 그림 2에 나타냈다. 그림 2는 센서 모듈에 의거한 보안 응용에 대한 두 가지 동작 상태를 보여 준다. 먼저, 하나는 발급 상태이고, 또 다른 하나는 발급된 센서 태그를 사용자가 이용하는 상태 즉, 인증 상태를 의미한다. 초기에, 발급 상태에서 리더기는 태그에 명령을

전송하고, 태그는 그림 2(a)에서 보여주는 것처럼 정보보호 알고리즘으로 처리하며, 다음으로 정상적인 물리적인 조건에서 동작하는 현재 초기 센서 값 SIA, 물리적으로 안전한 메모리(EEPROM) 에 저장 하고, 그 결과를 리더기에 알려준다. 이렇게 정상적으로 발급된 SID 태그는 상품에 부착되어 사용하게 된다.

그림 2(b)는 태그의 인증 상태를 보여준다. 인증 상태에서 샘플된 센서 값을 SAA라고 가정하자.



(a) 발급 상태

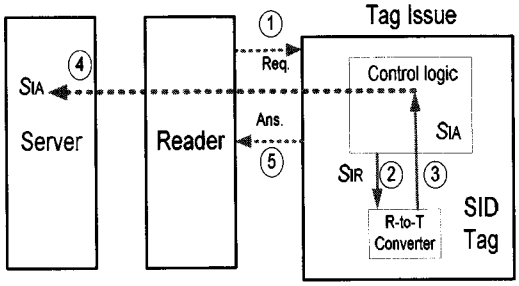


(b) 인증 상태

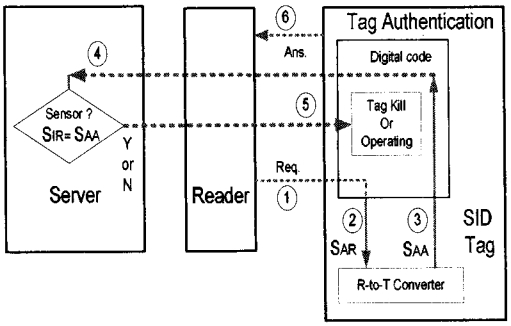
(그림 2) 메모리가 내장된 재사용 방지 센서 태그

인증 상태의 알고리즘에 있어서, 측정된 센서 저항 값 SAA이 정상적으로 샘플되고 저장된 초기 센서 값 SIA와 차이가 있으면, 태그는 물리적인 보안 침입이 현재 상태에서 일어났다고 결론을 내린다. 그런 다음, 태그의 동작은 중단되며, 태그 자체를 사용하지 못하게 처리된다. 따라서, 이는 물리적인 재-사용 방지에 대한 정보보호 SID 태그의 새로운 형태라고 할 수 있다.

또한, SID 태그의 초기 물리적인 값을 안전한 서버에 저장하여 처리하는 센서 인터페이스를 내장한 수동형 보안 태그의 동작 시나리오를 그림 3에 나타냈다.



(a) 발급 상태



(b) 인증 상태

(그림 3) 서버와 연동한 재사용 방지 센서 태그

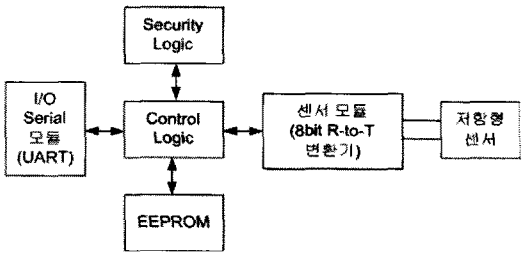
그림 3도 마찬가지로 센서 모듈에 의거한 보안 응용에 대한 두 가지 동작 상태를 보여 준다. 초기에, 발급 상태에서 리더기는 태그에 명령을 전송하고, 태그는 그림 3(a)에서 보여주는 것처럼 정보보호 알고리즘으로 처리하며, 다음으로 정상적인 물리적인 조건에서 동작하는 현재 초기 센서 값 SIA, 안전한 서버에 저장하고, 동시에 그 결과를 리더기에 알려준다. 이렇게 정상적으로 발급된 SID 태그는 상품에 부착되어 사용하게 된다. 한편, 초기 값의 데이터를 서버에 저장할 경우, 초기 값이 임의의 램덤 값을 가지므로 센서 태그의 구성은 기본적으로 입출력 인터페이스, 제어 논리, 센서 인터페이스로만 구성하여도 계측 및 태그의 물리적 안전장치를 실현할 수 있다.

그림 3(b)는 태그의 인증 상태를 보여준다. 인증 상태에서 샘플된 센서 값을 SAA라고 가정하자. 인증 상태의 알고리즘에 있어서, 측정된 센서 저항 값 SAA이 정상적으로 샘플되고 서버에 저장된 초기 센서 값 SIA와 차이가 있으면, 태그는 물리적인 보안 침입

이 현재 상태에서 일어났다고 결론을 내린다. 그런 다음, 태그의 동작은 중단되며, 태그 자체를 사용하지 못하게 처리된다. 따라서, 이 또한 물리적인 재-사용 방지에 대한 정보보호 SID 태그의 새로운 형태라고 할 수 있다.

3. 물리적 보안 장치 구현 및 검토

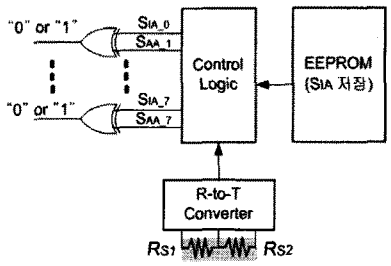
본 논문에서 센서 모듈은 저항차-시간차 변환기이다. 이는 8bit A/D 변환기를 적용하였다[8]. 또한, 물리적 보안 장치를 구현하기 위한, SID 센서 태그를 그림 4에 나타냈다.



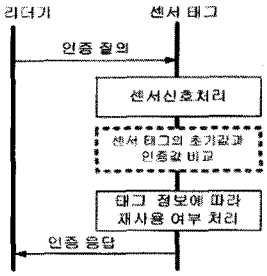
(그림 4) 제안한 SID 센서 태그

앞의 그림 4에 있어서, SID 태그의 보안은 발급 초기의 센서 값에 대응하는 디지털 코드를 안전한 EEPROM에 발급 초기 값 SIA을 저장한다. 그런 다음, 실제 사용에서 저항형 센서의 센서 값인 새로운 디지털 코드, 인증 값 SAA와 안전한 EEPROM 메모리에 발급 초기 값 SIA를 비교하여 물리적으로 안전 여부를 판단한다. 두 개의 값이 일치하면, 다음 동작으로 처리된다. 만약 일치하지 않으며, 정상적인 동작을 멈추게 된다. 즉, 태그 자체를 다시는 사용할 수 없도록 물리적 또는 논리적으로 만들어 재사용 방지로 처리된다. 이러한 과정에 있어서, 센서 태그와 리더 사이의 정보 전달은 암호화된 직렬 통신이다.

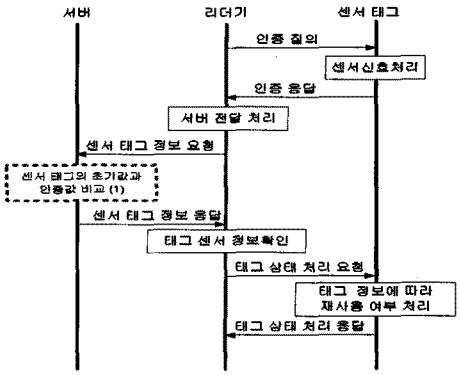
그림 5(a)는 EEOROM을 내장한 SID 센서 태그에서 초기 값과 인증 값의 비교 동작이 "0" 또는 "1"이라는 것을 보여준다.



(a) EX-OR에 의거한 센서 데이터 비교



(b) 센서 태그에서 인증



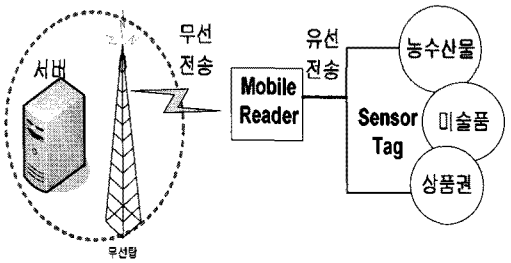
(c)서버에서 인증

(그림 5) 센서 태그의 초기 값과 인증 값의 비교

또한, 이는 초기에 저장된 초기 값, SIA와 태그 사용 중에 인지되는 인증 값, SAA을 EX-OR 게이트로 비교한 결과 "1"이 발생하면, 태그에 물리적인 공격이 가해졌다는 것을 간략하게 검출할 수 있다는 것을 보여준다. 다시 설명하면, 센서 태그의 초기 값(SIA)은 8bit 디지털 데이터이고, 인증 값(SAA) 8bit를 서로 비교하여 전체가 "0000 0000"이면, 정상동작을 진행한다. 한편, "1111 1111"이면, 태그를 더 이상 사용하지

못하도록 처리한다.

이러한 시스템 운영은 안전하게 발급된 태그가 데이터 정보를 암호화하여 리더기와 연동하여 사용된다. 그림 6은 생활환경에서 사용되는 센서 태그의 응용분야를 나타낸 것이다. 이 센서 태그는 고가의 상품, 농수산물품, 의료용품 등에 부착되어 이용되며, 이들 물품을 변조, 위조, 목적으로 태그를 조작할 경우 센서의 값이 변동되어 초기의 센서의 값과 일치하지 않으므로 태그는 리더기에게 상품이 문제가 있음을 알려준다. 또한, 리더기에게 전달 정보는 네트워크 (모바일) 망을 통해 실시 시간으로 정보 이용자에 전달될 수 있다.



(그림 6) 센서 태그의 응용 분야

4. 결 론

물리적 보안 기능을 만족시키는 수동형 SID 센서 태그를 제안하였다. 이들 수동형 SID 센서 태그는 응용 환경에 따라 다양한 센서 태그로 구성할 수 있다. 끝으로, 본 논문에서 기술한 수동형 SID 센서 태그는 센서와 SID 태그를 이용한 보안 분야의 새로운 응용이며, 향후 다양한 센서를 적용하여 상품의 진품명품 식별, 안전 관리, 등에 USN 시스템과 연동하여 많은 물리적 정보보호 장치 응용에 활용할 수 있을 것이다.

참고문헌

[1] K. Opasjumruskit, T. Thanthipwan, O. Sathusen, P. Sirinamarattana, P. Gadmanee, P. Pootarapan, N.Wongkomet, Rs A. Thanachayanont, and M. Thamsirianunt, "Self-Powered Wireless Temperature Sensors Exploit SID Technology," IEEE Pervasive Computing, IEEE vol.5, no. 1, pp. 54-61, Jan.-March 2006

[2] J. Marjonen, R. Alaoja, H. Ronkainen, M. Aberg, "Low power successive approximation A/D converter for passive SID tag sensors" Baltic Electronics Conference, 2006 International, pp.1-4 Oct. 2006

[3] Kohvakka, M.; Hannikainen, M.; Hamalainen, T. D., "Wireless sensor prototype platform" Industrial Electronics Society, 2003. IECON '03., pp.1499-1504, Nov. 2003

[4] Hai Deng, Murali Varanasi, Kathleen Swigger, Oscar Garcia, Ron Ogan and Elias Kougianos, "Design of Sensor-Embedded Radio Frequency Identification (SE-SID) Systems" Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation, pp. 792-796, June 2006

[5] Olivier Chevalerias, Terence O'Donnell, Daithí Power, Gerald Duffy, Gary Grant, Seán Cian O'Mathuna, "Inductive Telemetry of Multiple Sensor Modules", Published by the IEEE CS and IEEE ComSoc, pp. 46-52, 2005

[6] Mooseop Kim, et al, "Low Power AES Hardware Architecture for Radio Frequency Identification", IWSEC 2006, LNCS4266, pp. 357-368, 2006

[7] Madan Mohan, Vidyasagar Potdar, Elizabeth Chang, " Recovering and Restoring Tampered SID Data using Steganographic Principles" Industrial Technology, 2006. ICIT 2006. IEEE International Conference on, pp 2853-2859, Dec. 2006

[8] Ji-Man Park and Sung-Ik Jun, "A Resistance Deviation-to-Time Interval Converter for Resistive Sensors" 2008 IEEE International SOC Conference, pp 101-102, Sept. 2008

[저 자 소 개]

김상춘 (SangChoon Kim)
1986년: 한밭대학교 전자계산학과 학사
1989년: 청주대학교 전자계산학과 석사
1999년: 충북대학교 전자계산학과 박사
1983년~2001년: 한국전자통신연구원
정보보호연구단
2001년~현재: 강원대학교
정보통신공학과 부교수
email : kimsc@kangwon.ac.kr

박지만 (Ji-Man Park)
1997년 청주대학교 이공대학
전자공학과(박사)
1998년3월~현재: 한국전자통신연구원
책임연구원
email : parkjm@etri.re.kr