보안 JPMP-SID Tag를 활용한 사고 상황 ID 기록 시스템 설계

최장식*, 최성열**, 김상춘***

요 약

JPMP SID Tag는 센서 모듈을 이용한 물리적인 정보보호 기능을 제공하는 보안센서태그로써 저장되는 데이터의 복제 및 위조가 불가능한 특징을 가진다. 따라서 JPMP SID Tag저장되는 데이터의 진정성, 무결성, 원본성을 가지게 되어, 데이터의 보안이 요구되는 곳에 응용될 수 있다. 이 논문에서는 이러한 JPMP SID Tag가 가지는 물리적 보안 특징을 활용하여 사고 원인 규명이 필요한 도난 및 차량 사고를 대상으로 하여 디지털 증거를 획득 및 보호하고자 하는 시스템을 제안한다. 또한 제안 시스템에서는 JPMP SID Tag의 접근 제어를 위한 2차적인 제어로직을 구성하여, 제안 시스템의 소프트웨어 보안을 보완하고자 하였다.

Design of Accident Situation ID Recording System using JPMP-SID Security Tag

Jangsik Choi*, Sungyeol Choi**, Sangchoon Kim***

ABSTRACT

JPMP SID Tag is the security senor tag to provides physical information protective function using sensor module, has impossible feature to copy and fake the data which is stored in the tag. So data which is stored in the JPMP SID Tag has authenticity, integrity, originality. Therefore JPMP SID Tag could be applied in the place where the security of data is demanded. This paper propose the system using the JPMP SID Tag to acquire and protect digital evidence where cause investigation of accident is necessary. Also, proposed systems is complement of software security with composition secondary control logic for JPMP SID tag access control.

Key words : SID, JPMP, Physical Security Issue, Physical Security

접수일(2011년 05월 30일), 수정일(1차: 2011년 06월 17일), 게재확정일(2011년 06월 20일)

* 강원대학교/컴퓨터정보통신공학과
** 강원대학교/정보통신공학과
*** 강원대학교/전자정보통신공학부(교신저자)

1. 서 론

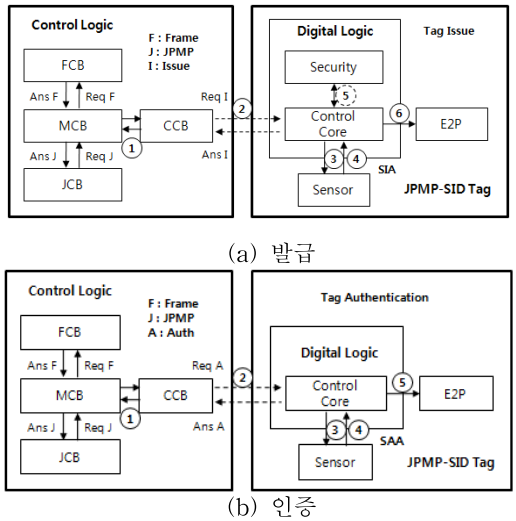
JPMP-SID Tag는 센서 모듈을 이용해 물리적인 보안 기능을 제공하는 수동 SID(Serial Identification) 센서 태그로써 I/O인터페이스 모듈, 제어 모듈, 센서 모듈로 구성되어 있다. 기존에는 센서와 SID 태그가 각각 분리 되어 계측 시스템에 주로 활용되고 있지만 JPMP-SID Tag와 같이 센서와 SID 태그를 연동해 데이터 정보보안 기능을 제공하지 않고 있다[1][2].

현재 시장에서는 태그와 리더사이에 정보보안을 위해 데이터를 암호화하여 통신하고 있지만 최근에 지능화된 다양한 공격으로 암호화된 데이터가 해독되는 사례가 발생한다. 이에 센서와 SID 태그를 융합해 보안을 제공하는 JPMP-SID Tag는 태그에 부착된 센서 저항의 변화를 인식하여 진품명품, 안전관리, 위조 및 변조 검사 등 다양한 관리를 실시간으로 실현하게 해준다[3].

이 논문에서 제안하는 시스템은 이러한 JPMP-SID Tag의 직렬 I/O 인터페이스 모듈을 통해 센서 태그와 통신하여 사고 발생 상황을 감지한 후 해당 고유 ID를 기록하고, 사고가 발생한 이후 관련 ID를 조사하여 사고의 재구성을 위한 디지털 증거를 확보한다. 이에 제안 시스템은 디지털 증거의 보안이 필요하며, 일상생활에서 발생할 수 있는 차량 및 도난 사고에 적용하여 고가 장비 분실 또는 차량 접속 사고의 디지털 증거의 능력을 보장하고자 한다.

2. ID 인증 및 복제 방지

제안하는 시스템은 크게 JPMP 제어 블록(JCB: JPMP Control Block), 메인 제어 블록(MCB: Main Control Block), 통신 제어 블록(CCB: Communication Control Block), 프레임 제어 블록(FCB: Frame Control Block)으로 구성되어, 사고의 발생 또는 요청에 따라 JPMP-SID Tag의 데이터를 읽거나 쓰기 기능을 수행한다. JPMP-SID Tag에 데이터를 읽고 쓰기 위해서는 JPMP 만의 발급과 인증과정 그리고 따로 요구되는 규격과 절차를 준수하며 수행해야 한다[4].



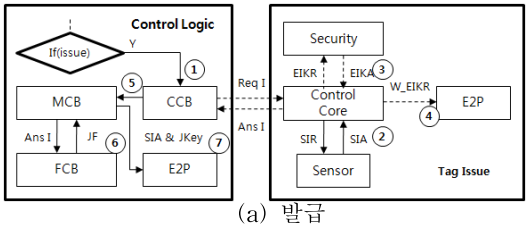
(그림 1) JPMP-SID Tag 발급 및 인증

제안하는 시스템은 사고 발생에 관여하는 ID를 기록하기 위해 (그림 1) JPMP-SID Tag 발급 및 인증의 (a)발급 단계를 수행하게 된다. (a)발급에서 Control Logic의 메인 제어 블록에서는 프레임 제어블록과 JPMP 제어 블록에게 명령어 및 JPMP 프레임을 요청 및 응답받은 후 통신 제어 블록에게 JPMP-SID Tag에게 Req I(Issue)를 요청한다. 이에 JPMP-SID Tag는 Digital Logic 내부의 Sensor에게 SIA(Sensor Issue Answer)를 요청 및 응답 받은 후 이를 Security를 통해 암호화 시켜 E2P에 저장하여 완료한 메시지 Ans I(Issue)를 Control Logic에게 전달한다. 여기서 SIA는 JPMP-SID Tag가 복제 여부와 진품인지 확인할 수 있는 중요한 키가 된다. (b)인증 단계에서는 제안 시스템에서 이전에 JPMP-SID Tag에 기록한 내용을 읽기 위한 단계 이다. [그림 1]의 (b)에서 메인제어 블록인 (a) 발급단계와 유사하게 JPMP 인증에 관여하는 명령어 및 프레임을 응답받아 통신 제어 블록을 통해 JPMP-SID Tag에게 Req A(Auth)를 요청한다. 이에 JPMP-SID Tag는 먼저 이전에 기록한 SIA와 Sensor로부터 응답 받은 SAA(Sensor Auth Answer)을 비교하여 JPMP-SID Tag의 복제 여부를 인증하게 된다. 인증이 성공하였을 경우 Control Logic이 요청한 정보를 E2P에서 읽어 Ans A메시지를 전달하게 된다. 만약 여기서 SIA값과 SAA의 값이 동일하지 않을 경우 Control

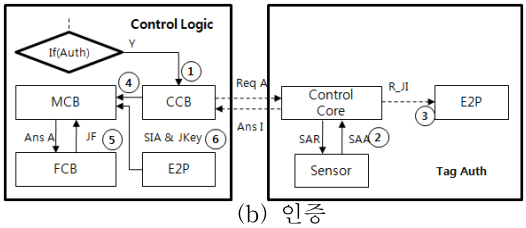
Logic는 이전에 기록한 사고 ID를 읽을 수 없게 된다. 즉 JPMP-SID Tag의 사고 관련 정보 기록은 제안 시스템 내부의 Control Logic에서만 이루어 질 수 있으며, 사고 관계자의 고의적인 의도에 의해 ID기록 및 복사가 불가능해진다.

3. 2차 접근 제어를 위한 제어 로직(Control Logic)

JPMP-SID Tag에 기록되는 데이터는 암호 모듈에 의해 암호화 되어 E2PROM에 저장된다. 이 값을 읽어서 복호화 시킬 경우 3-DES 복호화 알고리즘을 사용하는데 키의 방출 문제와 인증 값이 노출 될 수 있다는 2차적인 보안 문제가 발생한다. 따라서 이 과정을 제안 시스템의 Control Logic에 위치시켜 외부에 노출을 방지 하고자 한다.



(a) 발급



(b) 인증

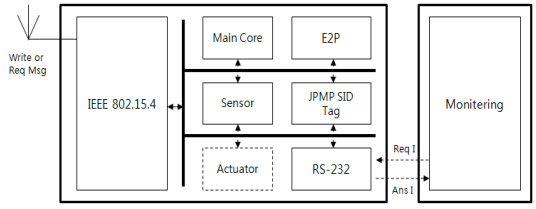
(그림 2) 인증 값과 키 보호를 위한 제어 로직

(그림 2)는 인증 값과 키 보호를 위한 제어 로직이다. (a)발급 단계에서 제어로직은 Issue의 프로토콜을 확인한 후 통신 제어 블록에서 Req I를 JPMP-SID Tag에 전송하게 된다. 이에 JPMP-SID Tag의 Control Core는 SIA를 응답받으며, 전송된 Req I에서의 암호화 키를 분류하여 Security를 통해 암호화된 EIKA(Encryption Issue Key Answer)을 받아 E2P에 저장한 후 Ans I에 SIA값을 저장하여 제어 로직에 전달한다. 제어로직에서는 프레임 제어 블록을 통해 JF(JPMP Frame) 응답을 받아 Ans I로부터 SIA값과 JKey(복호화 키)를 E2P에 저장한다. (b)인증 단계에서는 제어로직이 Auth를 확인하였을 경우 통신 제어 블록을 통해 JPMP-SID Tag에 Req A를 전달하게 되며, 이에 JPMP-SID Tag는 Sensor로부터 SAA를 응답받고, E2P에서 JI(JPMP Information)을 읽어 Ans I를 제어 로직에 전달한다. 제어 로직의 메인 제어 블록은 프레임 제어 블록을 통해 Ans A에서 JF의 응답을 받아 E2P에 저장된 SIA를 비교하며 JF의 암호화된 데이터 영역을 JKey를 통해 복호화를 수행한다. 이와 같이 제어 로직을 통해 외부에서 직접적으로 JPMP-SID Tag에 접근하는 것을 방지 하며, 정해진 Auth, Issue의 프로토콜과 프레임 규격을 제한함으로써, 고위적인 JPMP-SID Tag의 데이터 조작을 방지할 수 있다.

4. ID 발급 및 인증과 제어 로직 구현

4.1 구현 및 인증

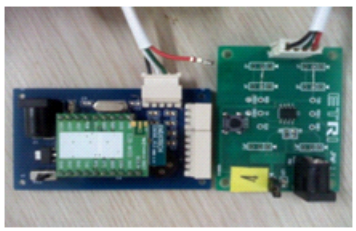
(그림 3)은 제안 시스템의 구성도이다. 제안 시스템은 무선 통신을 위한 IEEE 802.15.4 규격의 통신 모듈, 제어 로직 동작을 위한 메인 코어(Main Core), 정보를 저장하기 위한 메모리(E2P), 사고 유무를 판단하기 위한 센서, 사고 msg를 저장하기 위한 보안 태그(JPMP-SID Tag), 사고 여부를 알려주는 엑츄에이터(Actuator), 외부 모니터링을 위한 시리얼(RS-232) 그리고 제안 시스템의 정보를 모니터링 하기 위한 윈도우 기반의 모니터링 응용 프로그램으로 구성되어 있다.



(그림 3) 제안 시스템 구성도

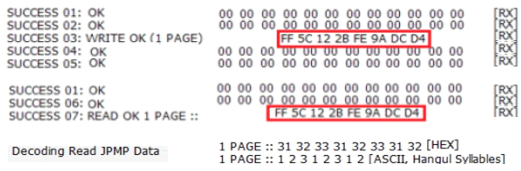
(그림 4)는 구현된 제안 시스템이다. JPMP-SID Tag는 UART(Universal asynchronous receiver/transmi

tter)로 연결하였으며 메시지는 JPMP 통신 프레임과 프로토콜 규칙을 준수하여 송수신한다. 메인 코어는 8비트 마이크로 컨트롤러를 사용하였으며, ID의 인증과 복제 방지 그리고 2차 접근제어를 위한 제어 로직을 수행한다.



(그림 4) 제안 시스템 구현

(그림 5) ID의 발급 및 인증 그리고 제어 로직을 수행한 결과를 모니터링한 결과이다. SUCCESS 01에서 05까지는 JPMP-SID Tag에 ID를 기록하는 과정으로 SUCCESS 03번에서 암호화되어 저장된 ID메시지를 확인할 수 있다. JPMP-SID Tag에 저장된 ID값에 접근하기 위해 SUCCESS 01에서 07까지 명령어를 수행하여 SUCCES 07에서 JPMP-SID Tag에 저장된 ID값을 읽을 수 있다. SUCCESS 07에서 읽은 값과 SUCCESS 03에서 읽은 값이 동일함으로 데이터의 무결성을 확인할 수 있다. 여기서 읽은 ID값은 3-DES로 암호화되어 있기 때문에 ID 발급 및 인증에서 기록한 SIA와 JKey를 통해 복호화하여 실제 데이터를 Decoding Read JPMP Data에서 확인할 수 있다. 복호화 되어 16진수로 표현된 값을 다시 ASCII코드로 변환하여 1PAGE에서 확인하였다.



(그림 5) 제안 시스템 ID 발급 및 인증

현재 JPMP-SID Tag에 저장할 수 있는 데이터는 32PAGE의 각각 8Byte를 기록할 수 있기 때문에 총 256Byte의 데이터를 입력시키고 읽을 수 있다.

제안 시스템은 IEEE 802.15.4의 ZigBee 모듈을 사용하였으며, 각 제안 시스템간의 사고 발생 이벤트를 주기적으로 발생하여 통신거리를 고려한 결과 개활지에서 100m이내의 정상 응답을 확인할 수 있었으나, 벽과 코너가 존재하는 공간에서는 20m이상 통신 거리를 확보하는데 어려움이 있었다.

4.2 선행연구와의 비교

디지털 데이터의 증거 능력을 보장하고자 하는 연구들은 대부분 컴퓨터와 네트워크 분야에서 많이 이루어지고 있지만 일반적인 생활분야에서 빈번히 발생하는 고가 장비의 도난 및 차량 사고에 대해서는 많은 연구가 이루어지고 있지 않다. 또한 관련 연구 분야에서도 인명 사고로 이어지는 차량 사고를 중심으로 하여 디지털 증거의 무결성을 보완하고자 하는 연구들이 이루어지고 있다.

선행연구 [5]에서는 자동차 블랙박스에 고유한 IPv6의 IP를 할당하여, 실시간 정보를 블랙박스와 서버에 저장함으로써 사고 발생 이후 무결성을 보장하고자 하였다. 여기서 사용하는 서버의 데이터베이스와 블랙박스의 저장매체는 사용자 권한을 취득할 경우 증거의 수정이 가능하므로 디지털 증거의 능력을 보장 받기 어렵다. 따라서 저장되는 매체의 보안과 데이터의 원본성, 진정성을 보장할 수 있는 연구가 필요하다.

[6]에서는 모바일 장치를 활용해 자동차 영상블랙박스를 설계하여 차량 사고 발생시 사고 원인해결을 위한 디지털 증거를 제공하고자 하였다. 하지만 이 연구에서는 디지털 증거의 증거 능력 보장을 위한 보안 기법을 언급하고 있지 않다. 또한 [7]에서는 차량용 블랙박스의 프로토타입(Prototype)을 제안하고 있으며, 관련 데이터들을 E2PROM에 저장하고 분석을 위해 특정 컴퓨터에 저장하게 된다. 하지만 E2PROM을 특성상 데이터를 쓰고 지우는 것이 가능하기 때문에 디지털 증거의 증거 능력을 보장 받기 힘들다.

[8]에서는 스마트카드와 서명 그리고 인증기관의 공개키를 통해 데이터의 재생공격, 삽입, 교체, 부인 방지 등을 통해 차량용 블랙박스에 저장되는 디지털 증거의 무결성을 보장하고자 하였다. 이 연구와 제안 시스템은 소프트웨어적인 접근제어와 시스템 접근을 위해 인

증키를 사용하는 유사점을 가지고 있지만 제안 시스템에서는 JPMP-SID Tag의 물리적 보안 특징을 활용하여 데이터 저장 매체의 복제에 대한 원본성을 입증할 수 있다.

본 논문에서 제안하는 시스템은 기존 연구들이 소프트웨어 중심의 디지털 증거 능력 보장을 위한 제안과 달리 JPMP-SID Tag를 활용하여 디지털 저장 매체의 물리적 보안 및 접근제어의 특징의 장점을 가진다.

5. 결 론

제안 시스템은 암호화 알고리즘과 키 인증 등의 소프트웨어 보완과 하드웨어적인 접근제어와 JPMP-SID Tag를 사용함으로서 얻을 수 있는 물리적 보안을 함께 사용하여, 1차적으로 JPMP-SID Tag의 물리적 보안으로부터 발생할 수 있는 키 유출 및 SIA유출에 대해 제어 로직을 구성하여 소프트웨어로 2차 접근 제어를 적용하였다. 여기서 제안 시스템에서의 JPMP-SID Tag의 인증 및 발급 단계와 제어 로직은 센서태그를 이용한 물리적 보안 시스템을 응용하기 위해 필요한 소프트웨어적 시나리오를 제안하고 있으며, JPMP-SID Tag가 가지는 키 및 SIA, SAA, JF를 보호하고자 제안되었다. 이러한 물리적 및 소프트웨어 보안이 함께 이루어진 제안 시스템의 응용분야가 사고 분야가 될 경우 저장되는 디지털 정보의 증거 능력을 보장할 수 있다.

하지만 응용 분야에 있어서 제안 시스템은 텍스트 형식의 데이터를 저장하기 때문에 정보의 저장 유형이 제한된다. 따라서 물리적 보안 장치 JPMP-SID Tag가 가지는 저장 매체의 한계를 E2P의 확장이나 타 저장 매체 사용 그리고 메인 코어의 사양 등을 높이는 방법에 대한 연구가 필요하다.

참고문헌

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

[2] 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

[3] 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

[4] 박지만, 김영세, 박영수, 전성익, “수동 RFID 센서 태그를 이용한 계측 및 물리적 보안 시스템”, 제4회RFID/USN우수연구논문집, 2008

[5] 김윤규, 김범한, 이동훈, "차량용 블랙박스 시스템을 위한 실시간 무결성 보장 기법", 정보보호학회논문. 19(6). pp. 50-61, 2009

[6] 김진일, 윤장혁, 김진수, “모방일 장치를 이용한 자동차 영상블랙박스 설계”, 한국정보기술학회 하계학술대회 논문집. pp. 364~367, 2009

[7] A. Kassem, R. Jabr, G. Salamouni, and Z.K. Maalouf, "Vehicle Black Box System", IEEE. SysCon-IEEE International Systems Conference pp. 1-6, 2008

[8] 박대우, 서정만. “자동차의 블랙박스를 이용한 실시간 포렌식 자료 생성 연구”, 한국컴퓨터정보학회논문지. 13(1). pp. 253-260, 2008

[著者紹介]

최 장 식 (Jangsik Choi)

2009년 강원대학교 공학대학
정보통신공학과 학사
2011년 강원대학교 공학대학
정보통신공학과 석사
2011년~현재 강원대학교
컴퓨터정보통신공학과
박사 재학 중

email: ksakdma0529@kangwon.ac.kr

최 성 열 (Sungyeol Choi)

2010년 강원대학교 공학대학
정보통신공학과 학사
2011년~현재 강원대학교
공학대학 정보통신공학과
석사 재학 중

email: ligntrune@kangwon.ac.kr

김 상 춘 (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