화물 컨테이너 보호를 위한 RFID 보안장치 기술 동향

강유성 | 김호원 | 정교일
한국전자통신연구원

요 약

RFID 기술은 유비쿼터스 사회로 가는 첫걸음으로 인식되면서 많은 연구와 활용방안이 논의되고 있다. 항만 물류의 화물 컨테이너 보호 분야도 그 좋은 예이다. 즉, 화물 컨테이너를 안전하게 잠그고 열며, 화물 정보를 보호 하기 위한 전기적 잠금 장치로써 RFID 기술이 활용될 수 있다.

본 고에서는 화물 컨테이너 운송의 안전성을 지원하기 위한 국제 표준화 현황을 살펴보고, 실제 상용화에 박차를 가하고 있는 대표적인 RFID 장치인 전자봉인(eSeal)과 컨테이너 보안장치(CSD)의 기술적 특징에 관하여 논한다. 본 고에서의 주요 관심은 전자 장치로서의 화물 컨테이너 보호용 RFID 태그와 리더 기술이며, 특히 화물 컨테이너의 중요 데이터를 보호하여 컨테이너 운송 시스템의 효율성과 보안성을 동시에 향상시킬 수 있는 데이터 보호 요구사항을 정리하며 결론을 맺는다.

I. 서 론

유비쿼터스 사회로 가는 그 첫걸음에 RFID (Radio Frequency Identification) 기술이 위치하고 있음이 널리 인식되면서 많은 연구와 활용방안이 논의되고 있다. 화물 컨테이너 보호 분야도 그 좋은 예이다.

2004년 American Shipper 자료에 따르면 우리나라의 연간 컨테이너 수송량은 45만 TEU(Twenty Feet Equivalent Unit)로 세계 6위를 기록하고 있다. 우리나라 수송량의 약 55%인 25만 TEU는 미국과의 교역 물량인데, 미국은 9.11 이후에 자국에 출입하는 화물 컨테이너에 RFID를 활용한 전자장치를 향후 수년 내에 실용화하는 계획을 세우고 연방통신위원회, 국방부, 상무부, 전문기업 등 민관이 공동으로 협력하여 안전무역체계(Smart Secure Tradelanes)를 준비하고 있다[1]. 또한 미국 정부는 2012년부터 미국으로 반입되는 모든 컨테이너 화물에 대해 운송 도중 컨테이너가 개폐되지 않았음을 확인할 수 있도록 미국 세관이 인정한 보안장치를 장착해야만 미국내 반입을 허락하는 법률을 통과시켰다[2].

화물 컨테이너의 안전하고 효율적인 운송 및 화물 정보의 안전한 전달을 지원하는 대표적인 보안장치로는 전자봉인(eSeal: Electronic Seal)과 컨테이너 보안장치(CSD: Container Security Device)가 있다.

전자봉인(eSeal)은 화물 컨테이너의 문에 설치되며, 컨테이너의 문이 비정상적인 형태로 개폐되거나 또는 비정상적인 개폐가 시도될 경우 이를 감지하여 주변의 리더에게 알리고 그 이력을 유지하는 역할을 한다. 화물 컨테이너용 전자봉인 장치는 ISO TC104 SC4 WG2(국제표준화기구의 화물 컨테이너 기술위원회 산하 자동장치 인식 작업그룹)에서 국제 표준화 작업을 진행했으며, 표준문서 번호는 ISO

본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행되었음. [2005-S-088-03, 안전한 RFID/USN을 위한 정보보호 기술].

18185 규격번호를 가지고 있다. ISO 18185 규격은 세부적으로 ISO 18185-1부터 ISO 18185-5까지 5개의 파트로 구분되어 표준문서가 작성되었다. 따라서 능동형 RFID 기술을 사용하는 전자봉인 장치의 기술적 특징을 살피기 위해서는 ISO 18185 표준문서를 분석할 필요가 있다.

컨테이너 보안장치(CSD)는 화물 컨테이너의 내부에 장착되며, 컨테이너 화물의 분실, 도난, 컨테이너 위치 추적 및 컨테이너 침입 탐지의 기능을 수행한다. 컨테이너 보안장치는 국제 표준화와는 별도로 미국의 GE를 중심으로 산업체 생산품으로 등장한 상태이다[3].

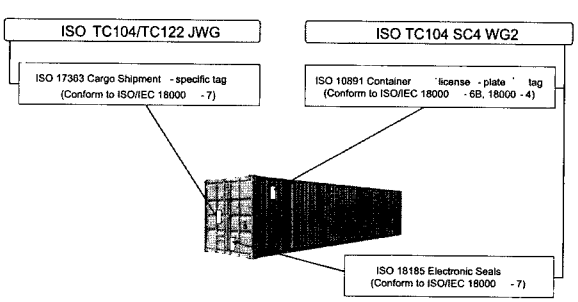
2007년 하반기 현재까지는 ISO 국제 표준화를 통해 논의된 전자봉인(eSeal)과 산업체 생산품인 컨테이너 보안장치(CSD) 중 어느 기술이 실제 항만 물류에서 사용되게 될지는 미지수이다. 따라서 화물 컨테이너 보호 또는 화물 정보의 보호를 지원하는 RFID 기술 동향을 파악하기 위해서는 전자봉인과 컨테이너 보안장치의 기술적 특성을 살피는 것이 필요할 것이다.

본 고는 화물 컨테이너 보호 및 화물 정보의 보호를 지원하는 전자 장치로서의 RFID 태그와 리더 기술에 초점을 맞추며, 이를 위하여 다음과 같은 순서로 구성된다. 제 II장에서는 화물 컨테이너 운송의 안전성과 정보의 보호를 위한 RFID 보안장치의 국제 표준화 현황을 살펴보고, 제 III장과 제 IV장에서 각각 전자봉인과 컨테이너 보안장치의 주요 기술적 특성을 살펴본다. 전자봉인과 컨테이너 보안장치가 중요 데이터 보호를 위한 구체적인 보안기술을 공개했더라면 보안성 분석 및 성능 분석이 뒤이어 설명되어야 하지만 현재는 구체적인 기술이 공개되지 않은 상황이라서 제 V장에서는 화물 컨테이너 운송 시스템의 효율성과 보안성을 동시에 향상시킬 수 있는 데이터 보호 요구사항을 정리하고, 제 VI장에서 결론을 맺는다.

II. 화물 컨테이너용 RFID 장치의 국제표준화 현황

ISO TC104 화물 컨테이너(Freight Container) 기술위원회는 화물 컨테이너의 외형적 규격, 용어의 정의, 컨테이너 분류, 봉인 방법, 활용 절차 등에 관한 전반적인 표준화 업무를 담당하고 있으며, 현재 3개의 부위원회(Sub Committee: SC1, SC2, SC4)가 활동 중이다. 그 중 SC4 인식 및 통신(Identification and Communication) 부위원회는 화물 컨테이너를 자동적으로 인식하기 위한 통신 프로토콜과 데이터 구조, 코딩 방식 등의 표준화를 담당하고 있으며, 현재 3개의 작업그룹(Working Group: WG1, WG2, WG3)이 활동하고 있다. 이러한 작업그룹 중 WG2 컨테이너 및 컨테이너 관련 장비의 자동 인식(Automatic Equipment Identification for containers and container related equipment) 작업그룹이 전자봉인의 표준화 업무를 담당하고 있다.

즉, 전기적인 특성을 지닌 RFID 장치를 사용하여 화물 컨테이너를 봉인하기 위한 노력의 일환으로 구성된 작업그룹이 ISO TC104 SC4 WG2이다. 이 작업그룹은 싱가포르에서 1999년 3월 30일 첫 미팅을 시작으로 본격적인 활동을 시작하였다[4]. 2007년 5월에 제 21차 회의까지 진행된 WG2에서는 화물 컨테이너에 부착할 전기적인 장치로써 전자봉인(eSeal, 문서번호 ISO 18185)에 대한 표준화를 마무리 지었으며, 컨테이너 태그(Container tag, 문서번호 ISO 10891)에 대한 표준화를 진행하고 있다. 그리고 WG2의 표준화 영역은 아니지만, 전자봉인, 컨테이너 태그와 함께 화물 컨테이너에 부착될 RFID 장치 중 하나가 화물 정보를 담는 화물 태그(Shipment tag)이다. 이는 ISO TC122/TC104 JWG(Joint Working Group)에서 표준화를 담당하고 있으며, 문서번호는 ISO 17363이 할당되어 있다. (그림 1)은 국제표준 그룹에서 논의하고 있는 화물 컨테이너용 RFID 장치의 표준문서 번호와 표준화 그룹의 관계를 정리한 그림이다. 각각의 표준문서에 대한 구체적인 현황은 다음과 같다.



(그림 1) 화물 컨테이너에 부착되는 RFID 장치

1. 전자봉인 국제표준화 현황

ISO 18185 규격번호로 표준화가 진행된 전자봉인은 5개 파트로 구분되어 있으며, 2007년 상반기에 최종 국제표준 초안(FDIS: Final Draft International Standard)에 대해 각 국가별로 전자 투표가 실시되었고, 모든 파트가 찬성으로 마무리되어 최종적으로 국제표준(IS: International Standard)으로 발간되었다.

ISO 18185-1 통신 프로토콜(Communication protocol) 표준은 통신 프로토콜에 관한 규격으로써, 전자봉인과 리더 사이의 명령 및 응답 패킷 구조 및 각 필드의 기능과 포맷을 정의하고 있다[5].

ISO 18185-2 응용 요구사항(Application requirements) 표준은 전자봉인이 영구적인 식별자를 반드시 가지도록 정의하고 있으며, 건전지 상태, 잠금/열림 시간 통보가 포함되어야 함을 정의하고 있다[6].

ISO 18185-3 환경 특성(Environment characteristics) 표준은 전자봉인 사용 환경에 관한 규격으로써, 온도, 충격, 진동, 습도, 기상조건, 바다의 안개, 모래와 먼지, 그리고 전자기적 환경에서 동작 가능해야 하는 범위를 정의하고 있다[7].

ISO 18185-4 데이터 보호(Data protection) 표준은 전자봉인 데이터 보호 기술을 목표로 했던 규격이었지만, 현재는 데이터 및 장치 인증이 필요하다는 선언적 표현만 기록되어 있을 뿐이며, 구체적인 데이터 보호에 대한 기술적 특성은 전혀 없는 상태에서 마무리되었다[8].

ISO 18185-5 물리 계층(Physical layer) 규격은 전자봉인과 리더 사이의 물리계층 특성에 관한 규격으로써, 최초에는 ISO/IEC 18000-7 규격을 준용하는 433 MHz 통신 방식만을 정의하였으나, 최종안에는 전자봉인이 433 MHz 통신과 2.4 GHz 통신을 동시에 지원해야 하며 또한 120 kHz 대역의 저주파 근거리 통신도 지원해야 하는 멀티밴드 물리계층 규격이 필수 구현사항으로 정의되었다[9].

2. 컨테이너 태그 국제표준화 현황

WG2에서 전자봉인과 함께 표준화 작업을 진행하는 규격이 컨테이너 태그에 관한 사항이다. 전자봉인이 화물 컨테이너의 안전한 운송을 위해 고려된 기술인 반면, 컨테이너 태그는 컨테이너 식별자만을 신속하게 전달하여 컨테이너 확인 고려된 기술이다.

ISO 10374.2 RF 자동 인식(Automatic Identification) 표준은 1991년에 발간되었던 ISO 10374를 확장하여 ISO 10374.2로 명명한 규격으로서 컨테이너 식별자를 지닌 수동형 RFID 태그를 대상으로 하고 있다. 구체적으로는, 컨테이너 태그의 장착 위치, 컨테이너 태그가 지녀야 할 정보, 운송 시 활용 절차, 그리고 통신 규격으로써 ISO/IEC 18000-6 Type C를 준용함을 정의하고 있다[10]. 그러나, 실제 항만 환경에서 컨테이너가 적재되어 있는 모습에 따라서는 현재의 표준이 기술적인 문제로 인하여 컨테이너 식별자를 제대로 읽을 수 없다는 의견이 제기된 상황이다. 이에 따라, 2007년 상반기까지의 논의에서는 현재의 ISO 10374.2 기술이 아닌 새로운 기술을 신규로 정의해야 한다는 주장과 현재의 ISO 10374.2 규격에 기술적인 향상을 추가하면 된다는 주장이 나오게 되었다. 결국, 2가지 의견이 모두 받아들여져서 현재의 ISO 10374.2 규격은 기술적인 향상을 포함시켜 계속 발전시킴과 동시에 현재의 ISO 10374.2를 대체할 신규 제안은 별도로 진행이 될 예정이다. 신규 제안될 컨테이너 태그 규격의 문서 번호는 ISO 10891이 될 예정이며, 향후에 ISO 10891은 ISO 10374.2의 기술을 모두 포함시킬 계획으로 표준화가 진행되고 있다.

3. 화물 태그 국제표준화 현황

ISO 17363 RFID의 공급망 응용 - 화물 컨테이너(Supply chain application of RFID - Freight containers) 표준은 2007년 5월에 최종 국제표준 발간이 승인되었다. 구체적인 내용으로는 화물 태그가 최소 256 바이트 이상의 정보를 가져야 하고, 저장 정보에 대한 보안성 유지, 프라이버시 유지가 필요하고, 통신 규격으로는 ISO/IEC 18000-7 규격을 준용한다는 내용을 담고 있다[11]. 그러나 저장 정보에 대한 보안성 보장을 위한 기술적 내용은 전혀 정의되어 있지 않기 때문에 데이터 보호, 접근 제어, 키 관리 등의 보안 이슈는 여전히 큰 숙제로 남아 있는 상황이다.

III. 전자봉인(eSeal) 장치

화물 컨테이너의 효율적인 운송과 비정상적인 개폐 감지

를 지원하는 대표적인 RFID 보안장치로 언급되는 전자봉인은 국제표준의 위상을 지니고는 있지만 기능적인 측면에서 보면, 기존의 기계적 봉인장치에 단순히 원격에서 자동식별만을 지원하는 전기적 특징만 추가된 형태이다.

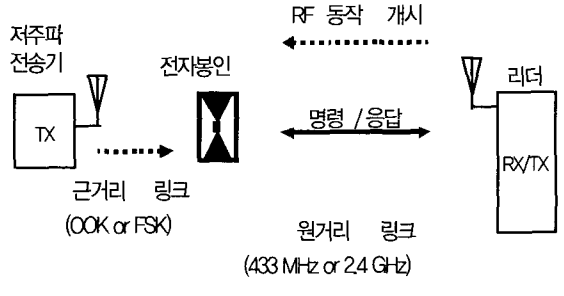
1. 전자봉인 기능적 특성

제 II장 1절에서 설명하였듯이 전자봉인은 멀티밴드 물리계층 규격을 지원해야 한다. 즉, 타입 A 물리계층은 433 MHz 원거리 링크와 OOK(ON-OFF Keying) 근거리 링크로 구성되며, 타입 B 물리계층은 2.4 GHz 원거리 링크와 FSK(Frequency Shift Keying) 근거리 링크로 구성된다. 전자봉인과 직접적으로 관련된 주요 표준문서 및 특성은 〈표 1〉과 같이 요약될 수 있다.

〈표 1〉 전자봉인 특성

구 분	표 준 문 서	특 성
기계적특성	ISO 17712	금속 케이블 봉인장치[12], 재사용 불가
원거리 통신 특성	타입 A: ISO/IEC 18000-7 타입 B: ISO/IEC 24730-2	433 MHz 능동형 RFID[13] 2.4 GHz 위치인식 서비스[14]
근거리 통신 특성	타입 A: OOK 변조 타입 B: FSK 변조	123 kHz ~ 125 kHz 116 kHz ~ 126 kHz
데이터 보호	ISO 18185-4	기술 규격 없이 요구사항만 정의됨

기술적으로 살펴보면 타입 A와 타입 B는 전혀 다른 기술이다. 전자봉인이 2개의 타입을 동시에 구현하고 있기 때문에 433 MHz 통신이 허용되는 국가에서는 타입 A 리더와 통신할 수 있고, 433 MHz 주파수 대역이 허용되지 않는 국가에서는 타입 B 리더와 2.4 GHz 대역에서 통신할 수 있으며, 저주파 근거리 통신의 도움으로 컨테이너 위치를 파악할 수 있는 장점이 있다.



(그림 2) 전자봉인 시스템 구성도

(그림 2)는 전자봉인 시스템을 구성하는 3가지 요소인 저주파 전송기, 전자봉인, 리더 구성을 보이고 있다[9]. 저주파 전송기(Low Frequency Transmitter)는 컨테이너의 위치 파악을 돕는 역할을 하며, 일반적으로 특정 위치에 고정되어 있다. 저주파 전송기는 일정한 시간 동안 자신의 식별자(LF transmitter ID)를 브로드캐스팅하므로 어떤 저주파 전송기의 영역 내에 들어온 전자봉인들은 모두 저주파 전송기의 식별자를 수신하게 된다. 이러한 저주파 전송기 식별자 수신은 저속의 근거리 통신으로 이루어진다.

그리고 전자봉인과 리더의 통신에 있어서는 원거리의 리더가 전자봉인을 깨우는 동작을 선행해야 하고, 그 이후에 명령을 보내고 이에 대한 응답을 수신한다. 대표적인 명령으로는 전자봉인 식별자(Seal ID)를 요청하는 'Collection' 명령이 있으며, 전자봉인에서는 'Collection' 명령을 수신하면 자신의 식별자를 응답한다. 또한 전자봉인은 저주파 전송기 식별자와 전자봉인 상태 정보(예를 들면, Sealed 또는 Opened)를 리더에게 전달할 수도 있다. 따라서 리더는 저주파 전송기 식별자를 수신하여 컨테이너가 어느 저주파 전송기 근처에 있음을 파악할 수 있고, 컨테이너의 잠금 상태가 어떤 상태인지 확인할 수 있다.

전자봉인은 전자봉인 상태 정보 이외에 컨테이너 화물 정보와 같은 중요 데이터를 가지지 않는다는 이유 때문에 데이터 보호 기술을 적용하지 않고 있다. 그러나 전자봉인의 근본적인 역할인 컨테이너 개폐 진위에 대한 원격 확인을 위해서는 잠금(Sealed) 또는 열림(Opened) 이벤트를 보호해야 할 정보로 정의할 수 있다. 즉, 언제 열리고 닫혔는지를 아무나 알 수 있다면 악의적인 공격자가 그 정보를 읽은 후에 컨테이너 문을 열고 물건을 바꿔치기 한 후에 다시 동일한 정보를 가진 새로운 전자봉인으로 컨테이너 문을 잠그면 도착지에서는 여전히 이전의 잠금 정보만을 읽게 되므로 이는 보안상 취약점이 된다. 따라서, 전자봉인의 상용화를 위해서는 반드시 데이터 보호에 대한 대책을 강구해야 할 것으로 판단된다.

2. 전자봉인 지적재산권 현황

전자봉인의 타입 A, 타입 B 물리계층 규격은 현재 미국 주요업체에서 지적재산권을 가지고 있다고 주장하는 상황이다.

타입 A에서 정의하고 있는 전자봉인과 리더 사이의 433 MHz 통신 규격은 미국의 SAVI가 지적재산권을 가지고 있다고 주장하는 ISO/IEC 18000-7 표준의 주요특징을 그대로 준용하는 것으로서, 2007년 5월 2일자 RFID Journal 기사에 따르면 미국의 SAVI는 2007년 6월 30일부터 ISO 18185 라이센싱 프로그램을 가동시킬 예정임을 밝힌바 있다[15]. 그리고 이와는 별도로 미국 SAVI는 2006년 8월부터 ISO/IEC 18000-7 라이센싱 프로그램을 진행하고 있는 상황이다. 결국, 화물 컨테이너에 전자봉인이 적용될 경우 ISO 18185 라이센싱 이슈는 크게 부각될 수 있을 것이다.

타입 B에서 정의하고 있는 전자봉인과 리더 사이의 2.4 GHz 통신 규격은 ISO/IEC 24730-2 표준의 주요특징을 그대로 준용하는 것으로서, 저주파 근거리 통신 규격은 미국의 WhereNet이 지적재산권을 가지고 있다고 주장하는 Magnetic FSK와 관련된 내용을 담고 있다. 2007년 4월 26일자 RFID Journal 기사에 따르면, 미국의 WhereNet은 저주파 Magnetic FSK 기술과 관련된 라이센싱 프로그램을 진행하고 있다고 밝히고 있다[16].

3. 전자봉인 제조업체 준수사항

ISO 18185-4 표준은 데이터 보호를 위한 기술적 특성을 담고 있지는 않지만, 부록 부분에서 전자봉인 제품의 제조업체가 따라야 하는 조항을 정의하고 있는데 주요 내용은 다음과 같다[8].

제조업체는 반드시 제조설비에 대한 ISO 9001 인증 또는 그와 동등한 인증을 유지해야 하고, 또한 ISO 18185-4 표준을 준수하고 있음을 확인 받기 위해 제조업체의 설비와 문서에 대하여 임의적인 불시의 조사를 수용해야 하며, 이러한 조사는 적절한 제3의 조사기관(예를 들면, 정부 대행기관 또는 공인된 독립기관)에 의해 수행되어야 함을 명시하고 있다. 그리고 제조업체는 법률이 허용하는 범위 내에서 모든 고용인에 대한 배경조사(background check)를 해야 하고, 제조업체는 1년에 1번씩 제3의 독립된 검사기관에게 생산제품의 샘플을 제출해야 함을 명시하고 있다.

또한 제조업체는 유일한 물리적인 일련번호 또는 식별자를 가진 리더를 생산해야 함을 명시하고 있는데, 이는 현재 ISO 18185 표준이 정의하고 있는 2 바이트의 질문기(Interrogator) 식별자와는 별도로 정의되는 리더 식별자를 의미하는 것이므로 제조업체의 재량이 아니라 표준화되는 것이 바람직할 것으로 보인다.

그리고, 제조업체는 모든 전자봉인의 물리적/전기적 식별자 및 각 전자봉인과 관련된 정보인 전자봉인 타입, 생산날짜, 주문날짜, 배송날짜, 판매수탁자 이름을 기록하고 7년 동안 보관해야 하며, 법적권한기관이 요구할 시 즉시 해당 정보를 제공해야 하며, 도매업자와 재판매자도 전자봉인과 관련하여, 출처, 식별자, 주문처 등을 기록하고 7년 동안 보관 및 제공의 의무를 다해야 함을 명시하고 있다.

IV. 컨테이너 보안장치(CSD)

전자봉인은 국제표준 논의를 통해 등장한 기술인 반면 컨테이너 보안장치는 국제표준화 작업 없이 미국의 GE에서 독자적으로 개발한 RFID 장치이며, GE와 더불어 유럽의 지멘스, 한국의 삼성물산, 일본의 미쓰비시 등의 산업체를 중심으로 상용화가 추진되고 있는 기술이다. 따라서 본 고에서는 현재까지 공개된 제품 제원을 중심으로 그 기능적 특성을 살펴보고자 한다.

1. 컨테이너 보안장치 기능적 특성

기능적인 측면에서 보면, 컨테이너 보안장치는 컨테이너 침입 여부를 확인하고 컨테이너 문의 개폐 상태 감지 및 컨테이너 이동상황에 대한 정보 제공이 가능하다. 그리고, 컨테이너 보안장치는 장착 위치를 컨테이너 내부로 규정하고 있으며, 악조건 해상 환경에 대한 견고성을 보장한다. 컨테이너 보안장치의 주요 특성은 〈표 2〉와 같이 요약될 수 있다[17].

〈표 2〉 컨테이너 보안장치 특성

구 분	특 성
기계적특성	· 컨테이너 내부 장착 · 악조건 해상환경의 내성 및 견고성 · 재사용 가능 · 화물 정보, 공급망 데이터 보유
통신 특성	· 2.4 GHz ISM 대역, ISO/IEC 18000-4 · 500개 이벤트 정보 저장
데이터보호	· AES-128 암호 지원 · Kerberos IETF RFC 1510

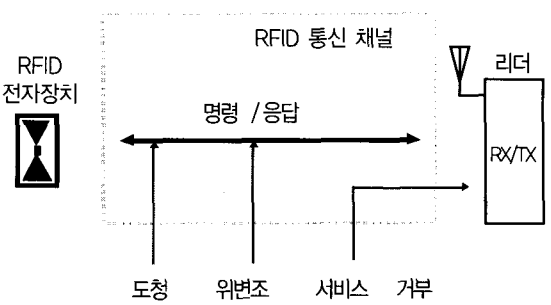
현재까지 공개된 컨테이너 보안장치의 특징과 제원만을 놓고 보면, 컨테이너 보안장치는 기능적인 측면에서는 컨테이너 위치 인식 기능을 제외하면 ISO 국제표준인 전자봉인, 컨테이너 태그, 화물 태그의 기능을 모두 포함한다고 볼 수 있다. 통신 주파수 대역은 2.4 GHz 대역으로서 전세계 모든 지역에서 별도의 허가없이 사용할 수 있도록 목표하고 있으며, 화물 정보와 공급망 관리 정보 및 컨테이너 이동상황과 관련된 이벤트를 보유할 수 있다. 또한 보유하고 있는 데이터의 안전한 전달을 위하여 Kerberos 네트워크 인증 서비스와 AES-128 데이터 암호화 기법을 사용함으로써 한층 보안성을 강화시킨 장점이 있다. 위와 같은 전기장치로서의 기능외에 전자봉인과 차이를 이루는 또 다른 특징 중 하나는 장착 위치가 컨테이너 내부라는 것이다. 전자봉인은 최종 목적지에서 봉인 케이블을 절단하거나 봉인장치 자체를 파손하므로 재사용이 불가능 하지만, 컨테이너 내부에 장착된 컨테이너 보안장치는 최종 목적지에서 컨테이너 개봉 후에도 보유 데이터만 초기화시킨 후 다시 사용할 수 있다.

컨테이너 보안장치는 화물 컨테이너 운송 과정에서 요구되는 효율성과 보안성을 만족시키기 위해 산업체에서 개발된 제품인 관계로 범용적인 기술과 독자적인 기술이 혼합된 상태이다. 2.4 GHz 통신, AES-128 암호화 연산, Kerberos 네트워크 인증 서비스 등은 널리 사용되고 있는 범용적인 기술인 반면, 컨테이너 내부 장착 후 센싱을 통해 컨테이너 개폐 여부를 판단하고 이벤트를 저장하는 기법에 대해서는 미국 GE에서 지적재산권을 보유하고 있다고 알려져 있다.

현재까지 컨테이너 보안장치에 대한 라이센싱 프로그램이 공개된 것은 없지만 화물 컨테이너 보호용 RFID 전자장치의 시장 형성 과정에서 상용화와 맞물려 컨테이너 보안장치의 라이센싱 이슈도 부각될 수 있는 여지가 남아있는 실정이다.

보유하는 정보 관점에서 현재의 전자봉인과 컨테이너 보안장치의 차이점을 분석해 보면, 전자봉인은 화물 정보의 저장이 없고, 컨테이너 보안장치는 화물 정보 및 이동상황에 대한 정보를 저장하고 전달할 수 있다는 차이가 있다.

비록 현재의 전자봉인이 데이터 보호와 관련된 기술적 정의가 없는 상황이지만 초기 전자봉인의 표준화 과정에서는 전자봉인이 가지는 데이터를 전자봉인 식별자(Seal ID), 태그 식별자(Seal Tag ID), 태그 생산자 식별자(Seal Tag Manufacturer ID) 및 각 응용에서 요구되는 비밀정보(Confidential Information) 등으로 규정하고, 이를 보호하기 위한 기술을 정의하기 위해 노력했었다.



(그림 3) RFID 전자장치 취약점 분석

전자봉인의 데이터 보호를 위한 표준화 작업의 일환으로 보안 취약점에 대한 분석이 선행되었다. 그 결과 (그림 3)과 같은 도청, 위변조, 서비스 거부 공격에 취약하다고 판단하여 이를 극복하는 방향으로 표준화를 진행하고자 했었다. 그러나 최종 확정된 전자봉인 데이터 보호 표준문서는 전자봉인이 비밀정보를 가지지 않는다는 전제조건을 제시하면서 어떠한 보호 기술도 명시하지 않고 있다. 그러나 전자봉인이 지닌 모든 데이터가 어차피 공개되는 정보이기 때문에 도청 공격은 무시할 수 있지만 데이터 위변조와 서비스 거부 공격에는 여전히 취약할 수 밖에 없다. 따라서 현재 발간된 전자봉인 데이터 보호 규격은 향후에 전자봉인이 비밀정보를 가진다고 가정하고 차기 버전에서는 반드시 보안 키를 사용한 암호 알고리즘 동작으로 데이터 보호가 이루어져야 함을 제안하고 있다.

전자봉인 표준화 과정에서의 이러한 고민은 컨테이너 보안장치의 개발 과정에서도 동일하게 적용되었을 것으로 보인다. 그 결과, 컨테이너 보안장치는 AES-128 암호 알고리

즘 및 Kerberos 네트워크 인증 서비스를 사용하고 있다고 밝히고 있다. 하지만 구체적인 동작 절차와 계층적 키 관리 등이 공개되지 않은 상태라서 보다 정확한 보안성 분석은 어렵다.

현재까지의 상황은 적절한 보안성 보장이 어려워 보이므로 전자봉인, 화물 태그, 컨테이너 보안장치 등의 차세대 규격은 반드시 (그림 3)의 보안 취약점을 극복할 수 있는 기술적 내용을 담아야 할 것이다. 뿐만 아니라, 저장되어 있는 비밀정보에 대한 부인 방지를 위하여 비밀정보 쓰기 동작을 수행하는 기관의 전자서명(Digital Signature)을 포함해야 하며, 공격자가 정상적인 패킷을 구한 후에 이를 재전송하여 시스템의 반응을 이끌어 내고자하는 재전송 공격도 방어해야 할 것이다.

화물 컨테이너 운송의 효율성과 보안성을 향상시키기 위한 차세대 데이터 보호 규격이 포함해야 하는 보안 서비스는 〈표 3〉과 같이 정리할 수 있다.

〈표 3〉 화물 컨테이너 보호를 위한 보안 서비스

보안 서비스	설 명
상호 인증 (Mutual Authentication)	RFID 전자장치와 리더가 서로 정당한 권한을 가지고 있음을 증명하고 확인할 수 있는 특성
데이터 기밀성 (Data Confidentiality)	RFID 전자장치와 리더 사이의 통신 데이터를 암호화하여 도청을 방어할 수 있는 특성
데이터 무결성 (Data Integrity)	RFID 전자장치와 리더 사이의 통신 데이터가 위변조될 경우 이를 알아낼 수 있는 특성
저장 데이터의 부인방지 (Non-Repudiation of Stored Data)	RFID 전자장치에 저장되어 있는 비밀정보를 허가받은 기관이 기록했음을 보장하는 특성
서비스 거부 공격 방어 (Immunity to Denial of Service)	위장 리더 또는 위장 RFID 전자장치가 대량의 메시지를 유입시키는 경우에 이를 공격으로 판단하여 방어할 수 있는 특성
재전송 공격 방어 (Replay Protection)	공격자가 정상적인 패킷을 구한 후에 이를 재전송하는 공격을 방어할 수 있는 특성
계층적 키 관리 (Key Hierarchy Management)	마스터 키 및 세션 키의 안전한 생성, 저장, 전달, 사용과 관련된 키 관리 특성

VI. 결 론

화물 컨테이너 운송은 항만 물류, 항공 물류와 같이 비교적 대규모로 이루어지며, 전 세계를 대상으로 하여 국가간 무역에서 중요한 역할을 한다. 화물 컨테이너 자체의 효율적 운송도 중요하며, 컨테이너에 실려있는 화물에 대한 정보도 안전하게 유지되어야 한다.

화물 컨테이너의 안전하고 효율적인 운송 및 화물 정보의 보안성 유지를 위하여 RFID 전자장치를 적용하려는 노력이 진행되어 왔으며, 본 고에서는 그 대표적인 장치로서 언급되는 전자봉인(eSeal)과 컨테이너 보안장치(CSD: Container Security Device)를 분석하였다.

〈표 4〉는 두 장치를 기능적인 측면에서 비교분석한 결과를 정리한 것이다.

〈표 4〉 전자봉인과 컨테이너 보안장치 비교

구 분	전자봉인	컨테이너 보안장치
사용 주파수	433 MHz, 2.4 GHz 멀티밴드	2.4 GHz ISM 밴드
위치인식 기능	있음	없음
화물정보 저장	없음 (화물정보 저장을 위해서는 화물 태그를 별도로 사용해야 함.)	있음
컨테이너 개폐 확인	가능	가능
장착 위치	컨테이너 외부	컨테이너 내부
데이터 보호 기술	없음 (화물 태그도 데이터 보호기술 없음)	있음
국제표준 여부	ISO 18185에 해당됨	해당 국제표준 없음
대표적 상용 업체	미국 SAVI	미국 GE
재사용 여부	재사용 불가	재사용 가능

화물 컨테이너 운송은 테러 물자와 밀수품 운반에도 악용될 수 있기 때문에 모든 국가가 안전하고 투명한 운송을 목표로 한다.

본 고에서는 이러한 목표에 부합될 수 있는 RFID 전자장치의 현재 기술 동향을 분석하고자 했다. 본 고에서 미처 다루지 못한 최신 보안장치가 존재하여 그 기술에 대한 분석이 작성된다면 본 고의 내용을 포함시켜 비교 분석하면 훨씬 충실한 원고가 될 것으로 판단된다.

화물 컨테이너 운송과 관련된 산업체와 국가기관에서 RFID 전자장치를 상용화함에 있어서, 국가별 주파수 정책, 물류 비용의 적정성, 기술의 신뢰도, 국제적인 호환성, 관련 업체 및 국가기관들의 합의 등 다양한 조건을 고려하여 제품을 선택하고 인프라를 구축해야 할 것이다. 그러한 선택의 과정에서 본 고의 내용이 도움이 되기를 희망한다.

참 고 문 헌

[1] 전자신문, http://www.etnews.co.kr/news/detail.html?id=200503240097.

[2] 한국경제, http://www.hankyung.com/news/app/newsview.php?aid=2007082341891&intype=1.

[3] GE Security CommerceGuard System, http://www.gesecurity.com/GESecurity/News/CommerceGuard/CG-System-Brochure.pdf.

[4] Goh Hock Nguan, Report of the meeting of ISO/TC 104/SC 4/WG 2 held on 30 March 1999 - 1 April 1999 in Singapore.

[5] ISO, ISO 18185-1 Freight containers - Electronic seals - Part 1: Communication protocols. 2007.

[6] ISO, ISO 18185-2 Freight containers - Electronic seals - Part 2: Application requirements. 2007.

[7] ISO, ISO 18185-3 Freight containers - Electronic seals - Part 3: Environmental characteristics. 2007.

[8] ISO, ISO 18185-4 Freight containers - Electronic seals - Part 4: Data protection. 2007.

[9] ISO, ISO 18185-5 Freight containers - Electronic seals - Part 5: Physical layer. 2007.

[10] ISO, ISO 10374.2 Freight containers - RF Automatic Identification. 2006.

[11] ISO, ISO 17363 Supply chain application of RFID - Freight containers. 2006.

[12] ISO, ISO 17712 Freight containers - Mechanical seals. 2003.

[13] ISO/IEC JTC1, ISO/IEC 18000-7 Information Technology, Automatic Identification and Data Capture Techniques - Radio Frequency Identification(RFID) for Item Management - Air Interface - Part 7: Parameters for an Active RFID Air Interface Communications at 433 MHz. 2004.

[14] ISO/IEC JTC1, ISO/IEC 24730-2 Information Technology, Real-time locating systems(RTLS) - Part 2: 2.4GHz air interface protocol. 2006.

[15] RFID Journal, Savi Technology Announces IP Licensing for Cargo E-seals, http://www.rfidjournal.com/article/articleview/3287/.

[16] RFID Journal, ISO Ratifies 2.4 GHz RTLS Standard, http://www.rfidjournal.com/article/articleview/3277/.

[17] GE Security CommerceGuard System, http://www.gesecurity.com/GESecurity/News/CommerceGuard/CG_CSD_specs.pdf.

약 력

강 유 성

1997년 전남대학교 학사
1999년 전남대학교 석사
2005년 ~ 현재 한국과학기술원 박사과정 재학중
1999년 ~ 현재 한국전자통신연구원 선임연구원
관심분야 : RFID 보안, 보안 프로토콜, WLAN 보안, 부채널 분석

김 호 원

1993년 경북대학교 학사
1995년 포항공과대학교 석사
1999년 포항공과대학교 박사
1998년 ~ 현재 한국전자통신연구원 팀장
관심분야 : RFID 보안, USN 보안, 부채널 분석, 암호 칩 설계, IC카드

정 교 일

1981년 한양대학교 학사
1983년 한양대학교 석사
1997년 한양대학교 박사
1982년 ~ 현재 한국전자통신연구원 그룹장
관심분야 : IC카드, RFID/USN보안, 바이오 인식, 암호 알고리즘, 보안 프로토콜