CSD 기반의 컨테이너 안전운송 응용 서비스 개발

추영열* · 최수영**

Development of Application Service for Secure Container Transport Based on CSD

Young-yeol Choo* · Su-Young Choi**

본 연구는 지식경제부 지방혁신사업 지원으로 수행되었음 (B0009720)

요 약

본 논문에서는 컨테이너의 육상, 해상 수송간 안전운송을 위해 CSD 시스템에 기반한 응용 서비스 개발에 대해 기술한다. CSD 시스템에 기반하여 표준에 따른 응용 서비스 및 보안 서비스의 개발과 개발결과의 테스트 과정에 대해 기술하였다. CSD에 의한 보안기능 외에 운송중의 재난 예방을 위해 온도, 습도 및 충격센서를 이용한 컨테이너 화물 상태감시 기능도 개발되었다. 응용 서비스와 CSD 시스템간에 교환되는 메시지 기밀성을 위해 데스크탑 PC 이상의 시스템 환경과 8 bit CPU 환경에서 각각 RC5, AES-128 알고리즘에 따른 암/복호화 기능을 구현하였다. 암/복호화 시간에 대한 측정 결과, 두 알고리즘 모두 사용 가능함을 확인하였다.

ABSTRACT

In this paper, we describe application service development for secure land and marine transport based on CSD (Conveyance Security Device) systems. Based on CSD systems, we present application service and security service according to relevant standards as well as test procedure of developed services. Exploiting temperature, moisture, impact sensors, state monitoring function of container freight was developed to prevent disaster during transportation in addition to security function with CSD. For confidentiality of messages exchanged among application service entity and CSD systems, Encryption and decryption functions going by RC5 and AES-128 algorithms were implemented at desktop PC and 8 bit CPU environments, respectively. Measuring the elapsed time during encryption and decryption shows that two algorithms are allowable for the application service.

키워드

전자봉인, CSD, RC5, AES-128, 지능형 컨테이너

Key word

E-Seal, CSD, RC5, AES-128, Intelligent Container

* 종신회원 : 동명대학교 컴퓨터공학과 (교신저자, yychoo@tu.ac.kr)
** 정회원 : (주)지능기계

접수일자 : 2011. 08. 12
심사완료일자 : 2011. 09. 05

Ⅰ. 서 론

화물 컨테이너의 안전하고 효율적인 운송 및 화물 정보의 안전한 전달을 지원하는 대표적인 보안장치로는 전자봉인(E-Seal : Electronic Seal)과 CSD(Conveyance Security Device)가 있다[1]. 전자봉인의 경우 ISO TC 104SC4WG2에서 표준화 작업을 진행하여 국제 표준 ISO 18185로 제정되었다는 장점이 있어 이에 대한 연구가 수행되어 왔다[2-5]. 그러나 ISO 18185 표준은 데이터 보호기술이 정의되어있지 않고 실제 구현을 위한 구체적 사양의 제정이 미비하여 구현시 상호호환성(interoperability)이 보장되지 않는 문제점이 있다[6-9]. 이에 따라, 이를 보완하기 위한 연구에 대한 필요성이 제기되어 왔다.

CSD는 2007년 12월 12일 미국의 DHS (Department of Homeland Security)에서 RFI (Request For Information)발표되었으며[10] 전자봉인과는 달리 표준화 기구가 아닌 GE 등을 중심으로 유럽의 지멘스, 한국의 삼성물산, 일본의 미쓰비시 등의 산업체들의 연합에 의해 상용화가 추진되고 있다. CSD는 컨테이너의 내부에 설치되며 컨테이너 봉인시점 (Point of Arming, POA)에서 중간지점(Intermediate Terminal Point, ITP)을 거쳐 도착항(Trip Terminal Point, TTP)까지 보안성을 보장한다. 이를 위한 보안기능을 정의하고 있다. 아래의 표 1은 CSD의 기능적 특성에 대한 요약이다[1].

표1. CSD 특성
Table 1. CSD characteristics

구분	특성
기계적 특성	• 컨테이너 내부 장착 • 악조건 해상환경의 내성 및 견고성 • 재사용 가능 • 화물정보, 공급망 데이터 보유
통신 특성	• 2.4GHz ISM 대역, ISO/IEC 18000-4 • 500개 이벤트 정보 저장
데이터 보호	• AES-128 암호지원 • Kerberos IETF RFC 1510

[3]의 연구는 표1에서 요구되는 CSD tag 및 리더 장비의 개발에 대한 것으로, 본 논문에서는 [3]의 CSD를 기반으로 한 보안상태 감시 응용서비스 개발과 온도, 습도, 충격 센서를 이용, 실시간으로 컨테이너의 상태를 모니터링 함으로써 컨테이너의 안전운송을 담보하기 위한 응용 서비스 개발에 대해 기술한다. 이에 더하여, CSD와 응용 서비스 사이의 정보 교환시 메시지의 기밀성 보장을 위한 암복호화 알고리즘 개발에 대해 설명한다. 본 논문의 구성은 다음과 같다. 2장에서 구현된 CSD 기반 안전운송 서비스 및 구성요소들에 대해 설명한다. 3장에서 구현된 응용서비스의 동작 테스트 방법에 대해 기술하였다. 4장에서는 DCP와 CSD 장비 사이의 송수신 데이터의 기밀성 보장을 위해 구현된 암/복호화 알고리즘의 성능측정 결과에 대해 설명하고 5장에서 결론을 맺는다.

Ⅱ. 시스템의 구현

2.1. 개요

제안하는 CSD 기반 안전수송 응용은 다음의 그림1과 같이 5가지의 구성요소를 통해 구현된다. 컨테이너 정보와 봉인상태를 인식하고 리더에게 전송하는 CSD와 CSD에게 일련의 명령을 요청하고 CSD의 정보를 인식하는 리더, 이 리더를 직접 제어할 수 있는 Reader Control Program, 그리고 리더와 TCP/IP 통신을 통해 CSD의 정보를 저장하고 리더에게 암호화 키를 분배하는 DCP, 컨테이너 상태정보, 위치 및 보안 상태를 화주, 선주 등 고객에게 알려주는 서비스 DB로 구성된다. 본 연구 범위는 그림1에서 사각형으로 표시된 DCP 와 서비스 서버 부분이다.

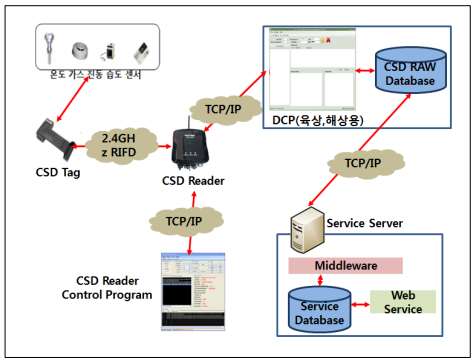

그림 1. 안전운송 System의 구성
Fig. 1 Configuration of secure transport systems

2.2. 구성 요소들의 기능

2.2.1 CSD 리더

CSD 와 2.4GHz 대역에서 통신하는 모듈로서, CSD에 저장된 정보를 요청하기 위한 읽기 모듈과 태그에 새로운 정보를 저장하기 위한 쓰기 모듈을 갖는다. CSD 리더는 고정형 외에 휴대용으로DHS-designated security agent에 의해 조작되는 SHHR (Secure Handheld Reader) 단말이 있다.

2.2.2 CSD 태그

CSD 태그는 컨테이너 개폐 정보이외에 컨테이너 상태정보를 파악하기 위하여 온도, 습도, 충격 센서가 추가로 부착된다. 데이터를 암호화하기 위한 암호화 모듈이 내장되어 있다. 컨테이너 화물정보 및 모든 경고 이벤트를 기록/유지한다.

2.2.3 DCP (Data Consolidation Point)

DCP는 육상 운송시 관련 서비스를 제공하는 육상용 DCP와 해상 운송시의 안전 서비스 제공을 위한 해상용 DCP로 나뉘어 구현되었다.

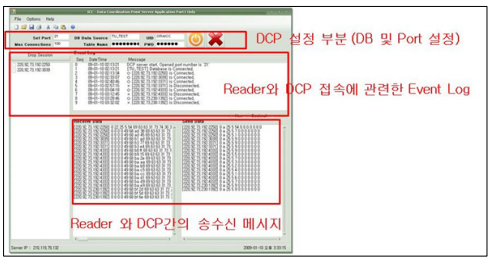

그림 2. 육상용 DCP 응용 화면
Fig. 2 DCP application display for land transport

- 육상용 DCP

구현된 DCP 응용에서는 각 리더의 ID와 패스워드를 수신받아 암호화키를 분배하는 역할을 하며, 리더로부터 받은 CSD의 Data를 DB에 저장하고 그 이력을 유지한다(그림2 참조). 여러 대의 리더와 통신하기 위하여 1:N 통신이 가능하도록 개발이 되었으며, 리더로부터 받은 Data의 암호화/복호화에는 AES-128 및 RC5 암호화 알고리즘이 사용되었다. DCP만이 접속 가능한 User Information DB에서 수신한 리더의 ID와 패스워드를 비교하여 암호화 키를 할당하게 된다. 리더와 연결되었을 시 트리구조로 관리 할 수 있는 'Status View'와 접속에 관련한 Event Log를 나타낼 수 있는 화면과 CSD 리더와 송・수신 데이터를 보여주는 Receive/Send View 화면을 개발하였다.

CSD 리더와 데이터베이스 및 사용자 인터페이스와의 통신시에는 [10]에서 정의된 요구사항에 따라 TCP/IP 기반 XML 메시지를 사용한 통신 프로토콜을 사용한다.

- 해상용 DCP

구현된 해상용 DCP 프로그램은 컨테이너를 운송하는 화물선에서 각 컨테이너의 상태정보를 모니터링하기 위한 프로그램이다. 개발된 화면 및 기능은 CSD가 부착된 컨테이너의 위치를 파악하기 위한 BAY 화면, 컨테이너 ID, CSD ID, 온도, 습도 등의 컨테이너 상태를 모니터링 할 수 있는 'Senssing Data View'화면, 각 컨테이너의 정보를 요청하여 모니터링 할 수 있는 'Send Data Viewer'화면 등을 포함한다. 또한 요청한 컨테이너의 온도, 습도를 실시간으로 표시하는 'Senssing Data Value'창이 존재한다. 각 컨테이너의 CSD 상태정보를 수신하여 각 화물에 대한 위험물 DB와 연동하여 경고발생을 3단계로 구분하여 사용자에게 알려주는 기능을 가진다. 위험물 DB는 4,300개의 tuple을 가지고 있으며 물질명, UN NO., HS NO., CAS NO., 인화점, 녹는점, 끓는점, 비중, 취급주의 사항 등으로 구성되어있다. 그림 3은 개발된 해상용 DCP화면의 예이다.

그림 3. 해상용 DCP 화면
Fig. 3 DCP application display for marine transport

2.2.4 Reader Control Program

Reader Control Program의 화면 구성은 DCP에서 인증을 받기 위한 아이디와 패스워드를 입력하는 'User Information'창과 각 컨테이너의 CSD에 명령을 송신하기 위한 'CSD_Information'창, 그리고 리더에게 일련을

명령을 송신하기 위한 'Command Option'과 'Command' 창으로 나뉘어진다. 리더로부터 받은 CSD정보를 표시하기 위한 'Status Message'창과 송신한 메시지와 수신한 메시지를 확인하기 위한 Receive 및 Send Message View 창이 있다. 또한 리더에 저장되어 있는 EventLog를 수신하여 표시하고 저장하는 기능이 있다(그림 4 참조).

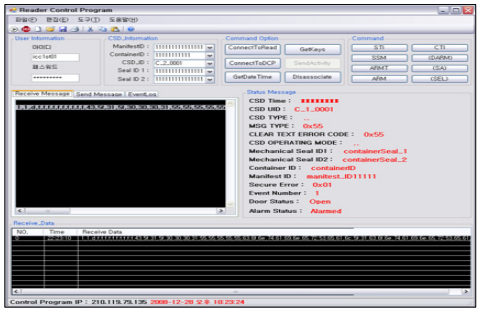

그림 4. CSD 리더 컨트롤 프로그램
Fig. 4 CSD Reader Control Program

2.2.5 Service DB & Middleware

Service DB는 CSD의 상태정보 및 화물의 임계치 값, 컨테이너 정보, 화물의 정보 와 같은 다양한 정보를 화주, 선주 등 고객에게 제공하기 위한 DB와 데이터 처리를 위한 미들웨어로 구성된다. Service DB의 주요 구성은 다음과 같다.

- CSD information table
- Container profile table,
- Cargo profile table,
- Danger cargo profile table,
- Truck profile,
- Vessel profile,
- User profile

각 profile간의 관계는 그림 5와 같다. user profile은 CSD 시스템 관리자 및 사용자(화주, 선사 등)의 정보가 저장되어 있다. Container profile은 컨테이너 정보, 즉 컨테이너 ID 번호, Seal 번호, CSD Tag 번호, 화물의 이름, 화물의 HS 코드 번호, 출발지, 도착지, 경유지 등의 정보가 수록되어 있으며, 컨테이너의 임계치가 저장된다. Cargo profile은 일반 화물에 대한 HS 코드 번호와 화물명, 임계치 값, 위험시 대처방안등이 등록되어 있다.

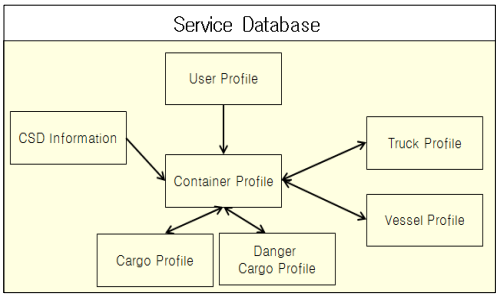

그림 5. Service DB 구성 블럭다이어그램
Fig. 5 Block diagram of Service DB configuration

Danger cargo profile 은 국제해사 기구에서 규정한 IMDG 코드를 기반으로 위험화물에 대한 정보들 (IMDG 코드번호, HS코드 번호, 화물명, 임계치, 대처방안)이 저장되어 있다. 그리고 Truck profile의 경우 육상 운송시 사용되는 트럭차량 번호, 운송사, 기사명, 기사연락처, 컨테이너 번호 등이 등록되어 있다. Vessel profile은 해상 운송중 선박의 정보가 수록이 된다. 선사명, 선박명, 적재되어 있는 컨테이너 번호로 구성이 되어 있다. CSD information은 DCP에서 수신되어 지는 CSD 정보가 저장되며, CSD Tag 번호, 컨테이너 번호, 온도, 습도, 충격, 계폐여부, 위치정보 데이터가 저장된다. 이와 같은 정보들을 취합하여, 고객에게 화물의 위치 및 현재 상태, 그리고 이상발생시 경보기능을 포함하다. CSD information에 CSD 정보를 저장하기 위해선 DCP에 저장되어있는 정보를 Service DB로 저장되어야 한다. 하지만 Service DB와 DCP DB는 별도의 시스템으로 데이터 처리 및 전달용 미들웨어가 필요하다. 기능은 아래와 같다.

- 이기종 DB 동시 사용시 데이터 호환성
- DCP에 저장되어있는 CSD 정보 조회
- Service DB에 저장된 CSD 정보와 비교
- 새로운 CSD정보인 경우 Service DB에 정보갱신

Ⅲ. CSD 기반 운송 서비스 테스트

구현된 안전운송 응용 서비스의 실제 동작 여부 및 [10]에 규정된 요구사항의 만족 여부를 검증하기 위해 다음과 같이 실제 테스트를 수행하였다.

3.1. 점검 방법

출발지로부터 도착지까지 다음의 기능에 대한 점검이 실행되었다.

- 3개 거점에 걸친 육상운송 : 양산 ICD → 백양터널 → 부산 감만 CY
- CSD 및 네트워크 장비 내륙운송 기능 점검
- 육송용 C/P의 운송중 CDMA 통신기능 점검

출발지에서는 컨테이너에 CSD 및 네트워크 장비를 부착하고 계측기를 삽입한다. 그 후 CSD의 기능을 활성화 하고 화물정보를 생성한 후에 DCP에 저장하게 된다. 운송차량에는 차량용 C/P (Consolidation Point)를 탑재한다. 점검 내용은 아래와 같다.

- 컨테이너에 CSD, 네트워크 장비, 계측기 부착
- CSD 기능 활성화
- 화물정보를 생성하고 DCP에 저장
- 운송차량에 차량용 C/P 탑재 기능 확인

그 다음 경유지에서의 점검 사항은 다음과 같다.

- 온도, 습도, 충격 센서로부터의 화물상태정보 변화 실시간 감시
- 차량용 C/P의 CDMA 기능을 통한 실시간 화물상태 확인
- 주용 거점 통과 시 위치 및 화물상태정보 확인

마지막으로 도착지에서의 점검 사항은 다음의 내용을 포함한다.

- 고정형 리더를 통한 입고 확인
- 컨테이너 봉인 및 화물 상태를 확인
- 장비 기능종료 및 제거
- 봉인해제 상태 확인

위와 같은 방법으로 실제 테스트 수행 결과 응용 서비스는 정확히 요구사항에 따라 기능이 동작함을 확인하였다.

Ⅳ. 구현된 암호화 기능의 성능측정

구현된 안전운송 서비스 시스템에 RC5 암호화 알고리즘 및 AES-128 암호화 알고리즘을 탑재하여 그 성능을 분석하는 실험을 하였다. 이와 같이 서버 수준의 DCP와 태그로 사용되는 8비트 CPU (ATmega128 ZETA)에서 RC5 와 AES-128 암호화 알고리즘을 구현하여 그 성능을 측정하였다. 이는 CSD가 낮은 계산능력 및 메모리 용량을 가진 시스템에 의해 구현될 것을 고려하여 적은 용량을 가진 시스템에서의 구현가능성을 검증하기 위함이다. 암호화 되는 부분은 [10]의 요구사항에 따라 데이터 영역에 한정된다. 따라서, 암복호화가 요구되는 중요 데이터의 길이는 128바이트 이하이다.

평문 데이터를 8 바이트 씩 암호화를 진행한다. 8 바이트 의 평문을 4 바이트 씩 A와 B로 나누어 수열 S로 암호화 연산을 수행한다. 부속키로 구성된 키 수열은 단일 암호화나 복호와의 암호화 키 보다 훨씬 길다. 이러한 특성은 암호문 분석을 더욱 어렵게 할 수 있으며, RC5는 2개의 모든 블록에 대해서도 연산 작업을 수행하여 보안 강도를 높일 수 있다. AES-128 암호화 알고리즘은 128 비트의 암호화키를 외부에서 직접 입력받아 16 바이트 씩 암호화를 수행되었다. 각 알고리즘의 secret key는 128 비트를 사용하였고 RC5 알고리즘은 16라운드 CTS (Cyper Text Stealing) 모드이며, AES-128 알고리즘은 10 라운드 CTS 모드이다. 실험 결과 각각 100회 씩, 다섯 번 측정한 결과의 평균값을 표2에 요약하였다.

표 2. DCP와 CSD에서의 암복호화 시간
Table 2 Encryption/decryption time at DCP and CSD.

Data length (byte)	RC5 지연시간 (μ sec)		AES-128 지연시간 (μ sec)	
	DCP	CSD	DCP	CSD
16	4.5	120	540	2,500
32	6.5	210	1,090	4,000
64	9.5	420	2,101	7,000
128	15.3	850	4,250	13,000

실험결과 RC5의 암호화 처리속도가 8 비트 CPU에서도 우수함을 알 수 있다. 그러나 AES-128의 경우에도 128 바이트의 데이터일 경우 지연의 최대값이 13 msec 정도로 10여초에 달하는 전체 서비스 응답시간에 비추어 성능의 차이를 현격히 감지할 수 있는 수준은 아니다.

Ⅴ. 결 론

본 논문에서는 컨테이너의 육상, 해상 수송간 안전운송을 위해 CSD 장비에 기반한 응용 서비스를 구현한 결과에 대해 기술하였다. 국내에서 개발된 CSD 장비를 기반으로 이를 지원하기 위한 [10]의 문서에 규정된 응용 서비스 및 보안 서비스를 구현하였고 실제 이를 테스트 과정에 대해 기술하였다. CSD 태그의 확산을 위해서는 장비의 가격이 중요한 요소가 될 것이다. 이를 고려하여 8 비트 CPU 환경과 DCP와 같이 데스크탑 PC 이상의 시스템 환경에서 각각 RC5, AES-128 암/복호화 알고리즘을 구현하고 이의 성능을 측정하였다. 측정결과 8 비트 CPU 환경에서도 [10]에서 요구하는 송수신 데이터의 길이가 짧아 두 알고리즘 모두 사용 가능함을 확인하였다. 또한 개발된 응용 서비스는 [10]의 요구사항 외에 컨테이너 내부의 상태를 감지하여 재난을 예방하는 기능도 포함하고 있다. 개발된 서비스는 기업체와의 협력을 통해 상품화 추진 예정이다.

참고문헌

[1] 강유성, 김호원, 정교일, “화물컨테이너 보호를 위한 RFID 보안장치 기술 동향”, 한국통신학회지 제24권 제 11호 PP. 43-50, 2007. 11.

[2] 추영열, 최수영, ISO 18185 기반의 컨테이너 안전수송 시스템 구현, 한국해양정보통신학회 논문지, 14권 4호, pp. 1032 ~1040, 2010.4.

[3] Seoung Park, Taekhyun Kim, Hoon Choi and Yunju Baek, “Design and Implementation of Low-Power Container Security Device″, Proc. of 7th Int’l Conf. on Information Technology, pp. 1189-1194, 2010.

[4] Hyung Rim Choi et. el., ″Development of design technique for the performance improvement of ConTracer″, Proc. of 13th Int’l Conf. on Advanced Communication Technology, pp. 179-182, 2011.

[5] Su Jin Kim; Guofeng Deng; Sandeep K. S. Gupta, Murphy-Hoye Mary, Intelligent networked containers for enhancing global supply chain security and enabling new commercial value, Proceedings of 3rd. International Conference on Communication Systems Software and Middleware, pp. 662-669, Jan. 2008.

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

[7] ISO, ISO 18185-1 Freight containers - Electronic seals - Part 2 : Application requirements. 2007.

[8] ISO, ISO 18185-1 Freight containers - Electronic seals - Part 3 : Environmental characteristics. 2007.

[9] ISO, ISO 18185-1 Freight containers - Electronic seals - Part 4 : Data protection. 2007.

[10] U.S. Department of Homeland Security, CONVEYANCE SECURITY DEVICE(CSD) REQUIREMENTS, Version 1.2 Dec. 10. 2007

감사의 글

본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2011-(C-1090-1121-0006))

저자소개

추영열(Young-yeol Choo)

1986년 2월 서울대학교 제어계측공학과졸업.
1988년 2월 동 대학원 석사.
2002년 2월 포항공과대학 박사.
1988년 6월~1994년 6월 포항산업과학기술연구원 선임연구원.
1994년 7월~2002년 8월 포스코 기술연구소 책임연구원.
2002년 9월~현재 동명대학교 컴퓨터공학과 부교수.
2005년 1월~7월 독일 Fraunhofer IESE Visiting Scientist.
2006.11~ 현재 U-Port ITRC 센터장.
※관심분야: WSN, Ambient Intelligence, 컴퓨터통신, 공장자동화, 네트워크 보안

최수영(Su-Young Choi)

2008년 2월 동명대학교 컴퓨터공학과 학사.
2010년 2월 동 대학원 석사.
2010년 4월 ~ 현재 (주)지능기계 연구원
※관심분야: USN, Embedded system, E-Seal, Network Security