

## IoT 기반 컨테이너 보안 장치 및 시스템 성능 평가

Performance Evaluation of Advanced Container Security Device(ACSD) system based on IoT(Internet of Things)

---

저자 (Authors)	문영식, 최성필, 이은규, 김재중, 최형림 Young-Sik Moon, Sung-Pill Choi, Eun-Kyu Lee, Jae-Joong Kim, Hyung-Rim Choi
출처 (Source)	<a href="#">한국정보통신학회논문지 17(9)</a> , 2013.9, 2183-2190 (8 pages) <a href="#">Journal of the Korea Institute of Information and Communication Engineering 17(9)</a> , 2013.9, 2183-2190 (8 pages)
발행처 (Publisher)	<a href="#">한국정보통신학회</a> The Korea Institute of Information and Communication Engineering
URL	<a href="http://www.dbpia.co.kr/Article/NODE02255749">http://www.dbpia.co.kr/Article/NODE02255749</a>
APA Style	문영식, 최성필, 이은규, 김재중, 최형림 (2013). IoT 기반 컨테이너 보안 장치 및 시스템 성능 평가. 한국정보통신학회논문지, 17(9), 2183-2190.
이용정보 (Accessed)	한국산업기술대학교 183.101.133.*** 2018/07/01 17:55 (KST)

---

### 저작권 안내

DBpia에서 제공되는 모든 저작물의 저작권은 원저작자에게 있으며, 누리미디어는 각 저작물의 내용을 보증하거나 책임을 지지 않습니다. 그리고 DBpia에서 제공되는 저작물은 DBpia와 구독계약을 체결한 기관소속 이용자 혹은 해당 저작물의 개별 구매자가 비영리적으로만 이용할 수 있습니다. 그러므로 이에 위반하여 DBpia에서 제공되는 저작물을 복제, 전송 등의 방법으로 무단 이용하는 경우 관련 법령에 따라 민, 형사상의 책임을 질 수 있습니다.

### Copyright Information

Copyright of all literary works provided by DBpia belongs to the copyright holder(s) and Nurimedia does not guarantee contents of the literary work or assume responsibility for the same. In addition, the literary works provided by DBpia may only be used by the users affiliated to the institutions which executed a subscription agreement with DBpia or the individual purchasers of the literary work(s) for non-commercial purposes. Therefore, any person who illegally uses the literary works provided by DBpia by means of reproduction or transmission shall assume civil and criminal responsibility according to applicable laws and regulations.

## IoT 기반 컨테이너 보안 장치 및 시스템 성능 평가

문영식 · 최성필 · 이은규\* · 김재중 · 최형림

### Performance Evaluation of Advanced Container Security Device(ACSD) system based on IoT(Internet of Things)

Young-Sik Moon · Sung-Pill Choi · Eun-Kyu Lee\* · Jae-Joong Kim · Hyung-Rim Choi

Intelligent Container R&D Center, Dong-A University, Busan, 604-714, Korea

#### 요 약

본 논문에서 소개하는 컨테이너 보안 장치(ConTracer)는 컨테이너 내부에 부착되어 컨테이너 내부의 온도/습도 및 컨테이너에 가해지는 충격 감지 등 컨테이너의 운송 중 상태 확인 가능하다. 또한 컨테이너 문이 2inch 이상 열리는 것을 1초 이내에 감지하고 GPS/GLONASS 등을 이용하여 수집한 글로벌 위치를 포함하는 컨테이너의 상태 정보를 IoT (Internet of Things) 기반 통신을 이용하여 실시간으로 원격지 서버로 정보를 전송한다. 본 연구에서는 국내외 컨테이너 보안 장치들의 개발동향에 대해 알아보고, 국내 이동통신사를 통하여 글로벌 로밍서비스를 이용하여 국내에서 출발하여 해외로 이동하는 실제 컨테이너 화물에 컨테이너 보안장치를 적용하여 실제 사례를 들어 소개하는 컨테이너 보안장치 시스템의 성능을 평가하고 이를 검증한다.

#### ABSTRACT

Container Security Device (ConTracer) which is suggested in this study is to monitor temperature, humidity, and impact inside of the container while the container is transported. ConTracer could also give information to users when a door of the container is opened over 2 inch within 1 second. Additionally, GPS/GLONASS based global position and status information about container are transmitted to a remote server using IoT (Internet of Things) based communication. In this research, we are looking into the development trend of global container security devices; and applying ConTracer to real freight transport from domestic to overseas using Global Roaming Service which is offered for domestic Mobile Communication Companies as well. As a result, we estimate the performance of ConTracer and verify it.

**키워드** : 컨테이너 보안장치 (ACSD), ConTracer, IoT (Internet of Things), 가상경계

**Key word** : Advanced Container Security Device (ACSD), ConTracer, IoT (Internet of Things), Geo-Fence

접수일자 : 2013. 07. 17 심사완료일자 : 2013. 08. 16 게재확정일자 : 2013. 08. 30

\* Corresponding Author Eun-Kyu Lee(E-mail:jabanora@dau.ac.kr, Tel:+82-51-200-5607)

Intelligent Container R&D Center, Dong-A University, Busan, 604-714, Korea

**Open Access** <http://dx.doi.org/10.6109/jkiice.2013.17.9.2183>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.  
Copyright © The Korea Institute of Information and Communication Engineering.

## I. 서 론

2001년 9·11 테러 이후 국제해사기구(IMO)를 중심으로 국제 해상운송의 안전을 강화하기 위한 노력이 시작됐고, 그 결실로 2004년 7월부터 ‘국제항해선박 및 항만시설의 보안에 관한 국제협약’인 ISPS Code가 발효되기 시작했다. 이는 국제항해선박과 관련 항만시설에 대하여 보안등급별 보안활동을 이행하기 위한 보안계획서를 작성·시행하고, 이를 승인 받도록 하는 한편, 선박보안 경보장치 등 보안장비를 갖추도록 보안조치를 의무화한 것이 핵심이다. 특히, 9·11 테러사건 이후 미국을 중심으로 한 국제사회는 공·항만 등 주요 물류거점에 대한 보안조치를 대폭 강화해왔으며, 최근에는 특정 물류거점 뿐만 아니라 내륙운송·통관 등 공급사슬망(Supply Chain) 전체에 걸쳐 테러위험을 최소화하기 위해 eSeal를 사용하고 있다. 또한 미국은 9·11 테러 이후 안전과 보안업무를 총괄하는 국토안보부(DHS)를 창설하고, 해운보안법, 항만보안법, 9·11 테러방지권고이행법률 등을 연이어 제정하는 등 자국에 대한 테러위험을 원천차단하기 위해 전 방위적으로 물류보안체계를 강화했다. 더욱이 컨테이너 화물을 수출하는 모든 운송인에게 화물 적재 24시간 전에 신고하도록 한 제도를 비롯해 외국 항에서의 미국행 화물 사전검색제도(Container Security Initiative), 민·관 협력 반테러보안제도(C-T PAT) 등 강화된 보안제도를 개발·시행하는 등 가장 적극적인 움직임을 보였다.

특히, DHS (Department of Homeland Security)의 CSI는 보안 강화 정책 중 하나로 세계 20대 항만 국외 컨테이너 안전 협상 체결을 통한 미국 반입컨테이너 보안을 위한 내용을 담고 있으며 CSI가 발표된 후에는 미국으로 반입되는 모든 컨테이너 화물은 보안요구사항을 만족시켜야 한다. CSI의 보안요구사항 중 미국 세관직원 파견에 의한 선적화물 사전 검사 실시와 미국으로 반입되는 모든 컨테이너 화물에 대해 전자적 봉인 장치(CSD) 사용을 의무화하는 것이다[1].

하지만 기존 컨테이너 전자 봉인장치 들은 주로 능동형 RFID 기술을 이용하여 컨테이너의 운송 과정중 항만, 터미널 등 특정 거점에서 컨테이너 상태 문 개폐 여부를 확인해 왔다. 그 대표적인 것으로는 ISO/IEC 18185를 기반으로 하는 433MHz 또는 2.4GHz 능동형 RFID 기술을 이용한 전자봉인(eSeal: Electronic Seal)

과 미국 국토안보부(DHS : Department of Homeland Security)에서 2.4GHz IEEE 802.15.4 표준 기술을 바탕으로 하는 컨테이너 보안장치이다[2].

능동형 RFID와 IEEE 802.15.4 표준을 이용한 컨테이너 보안장치는 이를 인식하고 정보를 읽어오기 위한 리더가 설치되어 있는 곳에서만 컨테이너 보안장치의 정보를 확인 할 수 있어 실시간으로 컨테이너의 상태 정보를 수집하는데 제약이 있으며, 초기 리더의 설치 등 모니터링 인프라 구축에 많은 비용이 들어 컨테이너 보안장치의 활성화에 어려움이 있다. 또한 컨테이너 보안장치의 사용자들이 컨테이너의 상태정보 중 컨테이너의 도착시간을 예상하기 위해 실시간 위치정보에 대한 요구사항이 날로 증가하고 있어 GNSS (Global Navigation Satellite System)기술과 IoT (Internet of Things)기술을 적용한 컨테이너 보안장치의 개발이 필요하게 되었다.

따라서 본 연구에서는 2장에서 컨테이너 보안장치의 발전 동향에 대해서 알아보고, 3장에서 본 연구를 통해 개발한 DHS CSI요구하는 컨테이너 보안장치의 기본 기술 스펙들을 만족하면서 GNSS 및 IoT 기술이 적용된 컨테이너 보안장치 및 ConTracer를 이용하여 구성한 시스템에 대해서 소개한다. 또한 4장에서 본 연구를 통해 개발한 컨테이너 보안장치를 한국을 출발하여 유럽으로 이동하는 컨테이너에 실제로 부착하여 실시간으로 이동 경로 및 특정지역에 진입 하였을 경우 실시간으로 관리자에게 사실을 통보할 수 있는(Geo-fence) 기능에 대해서 검증하고 5장 결론부에서 결과 정리 및 향후 발전과제를 제시하는 순서로 설명 하겠다.

## II. 컨테이너 보안 장치의 발전 동향

그림 1에서 보는 바와 같이 컨테이너 보안장치는 초기 1회용 기계적 봉인 장치(Mechanical Seal)인 실에서 시작하여 2000년대 중반 Active RFID 기술을 이용한 eSeal과 CSD로 발전하였다. eSeal과 CSD는 주파수는 상이하지만 Active RFID 기술을 사용하여 정보를 전송하는 방식은 동일하다[3].

eSeal과 CSD의 큰 차이점은 재사용 가능 여부와 컨테이너의 부착 위치로 구분 할 수 있는데 eSeal은 컨테이너의 외부에 부착되어 메커니컬 실과 같이 일회용으로 사용되는 반면, CSD의 경우 컨테이너 내부에 장착

되고 재사용이 가능한 것이 특징이다[4][5].

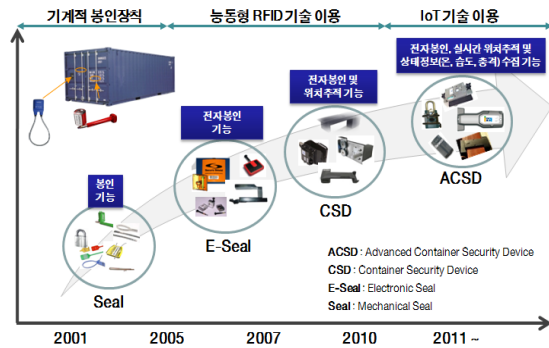


그림 1. 컨테이너 보안 장치의 발전 방향

Fig. 1 Future direction of the container security device

2010년 이후 CSD의 통신 방식인 Active RFID의 짧은 통신거리(30m 내외)에 대한 제약과 인프라 구축비용의 부담과 이동통신 기술의 발달로 인해 컨테이너 보안 장치의 통신 기술로 이동통신 기술을 활용한 IoT (Internet of Things) 개념이 적용된 ACSD (Advanced Container Security Device) 개념의 진화된 컨테이너 보안장치가 개발되었다[6]. ACSD는 기존 CSD의 특징과 함께 GNSS 기술을 이용하여 위치를 정확하게 파악하고 컨테이너 내부의 온도, 습도, 충격 등 상태 정보와 문 개폐 여부를 파악하여 실시간으로 WCDMA/GSM 등 이동통신 기술을 이용하여 글로벌 하게 운송되는 컨테이너의 상태 및 위치정보를 이미 구축되어 있는 이동통신 인프라를 이용하여 원격지로 전송할 수 있는 컨테이너 보안 장치이다. 아래 3장에서 소개 하고자 하는 ‘IoT 기반 컨테이너 보안장치’는 ACSD의 요구사항을 만족한다.

### III. IoT 기반 컨테이너 보안 장치 및 시스템 소개

#### 3.1. IoT 기반 컨테이너 보안 장치 소개

본 연구를 통해 소개하는 컨테이너 보안 장치는 Container와 Tracer의 합성어로 글로벌 컨테이너 운영 환경에서 실시간으로 컨테이너의 상태 및 위치를 원격지 서버로 전송이 가능한 ACSD의 요구사항을 만족하는 컨테이너 보안장치이다.

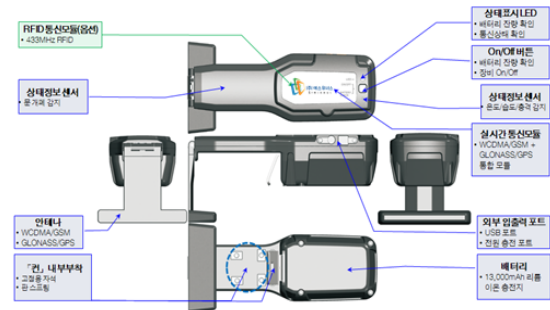


그림 2. 컨테이너 보안 장치

Fig. 2 Container Security Device

그림 2에서 보이는 바와 같이 기존의 Active RFID를 기반으로 하던 것과 달리 ConTracer는 글로벌 실시간 통신을 위하여 GSM/WCDMA 통신 모듈을 장착하였으며, 글로벌 정밀 위치 확인을 위하여 GPS 및 러시아의 위성항법 시스템은 GLONASS를 동시 이용할 수 있는 GNSS 모듈을 사용하였다. ConTracer는 ISO668을 만족하는 모든 드라이 컨테이너 문의 내부에 장착이 가능하도록 설계되어 컨테이너 운송 중 외부로부터의 충격에 의한 파손을 최소화 하였다. 컨테이너 내부에 장비의 주요부분이 위치하면서 안정적인 통신을 위하여 안테나 부분이 컨테이너 외부로 노출 되도록 설계 구현되었다[7].

또한 컨테이너 보안 장치의 기본 기능은 컨테이너 문 열림 감지기능은 미국 국토안보부에서 제시한 문 열림 기준은 2inch 이상 열림뿐만 아니라 컨테이너 문이 반복하여 여닫히는 횟수 등을 1초 이내에 감지하여 원격지 관리자에게 전달이 가능하도록 구현되었다.

글로벌 정보 전송 시 IoT를 위해 433MHz Active RFID 기술과 이동통신 기술을 동시에 구현하여, 433MHz Acvite RFID 인프라가 구축되어 있는 국내에서는 통신요금이 발생하지 않는 433MHz Active RFID 기술을 활용하고, 그 외 433MHz Active RFID 인프라가 구축되어 있지 않은 지역에서는 이동통신을 사용하도록 구현되었다. 아무런 인프라가 구축되어있지 않는 해상구간에서는 정보를 전송할 수 없어 이는 장비 내부 비휘발성 메모리 내에 정보를 저장하였다가 통신이 원활한 지역에 도착하였을 경우 정보를 한꺼번에 원격지 서버로 전송하여 정보의 손실을 최소화 하도록 구현하였다.

표 1. 기존 ACSD와 본 연구를 통해 개발한 ConTracer의 기능 비교

Table. 1 Comparison with existing devices

구분	Kirsen	Triton	ConTracer
위치정보	GPS	GPS	GLONASS, GPS
상태확인 (옵션)	온도, 습도, 충격, 기울기, 빛	온도, 습도, 충격, 빛	-
상태확인 (필수)	문개폐	문 개폐	온도, 습도, 충격, 문 개폐
원격설정 제어	○	×	○
무게	<1,500g	150g	<720g
연속사용	1~3년 (1일 2회 정보 전송)	-	최대 50일 (1일 24회 정보 전송)
동작환경	-30~85℃	-40~60℃	-30~60℃
통신 (필수)	GSM/GPRS (Quad Band)	GSM/GPRS (Quad Band),	WCDMA/GSM /GPRS
통신 (선택)	Satellite, RFID	Zigbee	433MHz RFID
배터리	-	Li-Ion 5,000mAh	Li-Ion 13,000mAh

표 1은 해외에서 개발된 ACSD와 본 연구에서 소개하는 컨테이너 보안장치와의 기능을 비교하여 보여준다. 가장 큰 특징으로는 ConTracer는 컨테이너 내부의 온도, 습도, 충격 등 상태정보를 항상 수집 및 제공하며 국내에서 실시간 이동통신이 가능하도록 WCDMA 기능을 필수적으로 채택한 반면 Kirsen 및 Triton 장비는 컨테이너 내부 상태 정보 수집은 옵션으로, WCDMA 통신기능은 제공하지 않아 국내에서는 실시간 서비스를 제공받지 못한다[8][9].

### 3.2. 컨테이너 보안 장치 시스템 구성

컨테이너 보안 장치를 이용한 컨테이너 화물 모니터링 시스템은 크게 컨테이너에 부착되어 컨테이너의 위치 및 상태를 확인 원격지 서버로 정보를 전송하는 컨테이너 보안 장치와 컨테이너 보안 장치에서 보내오는 정보를 원격지에서 수집하는 정보 수집용 서버(DCP), 그리고 사용자(관리자)에게 정보를 제공하는 모니터링 프로그램으로 크게 구성된다. 그림 3은 ConTracer를 이용한 컨테이너 모니터링 시스템의 구성 예를 나타낸다.

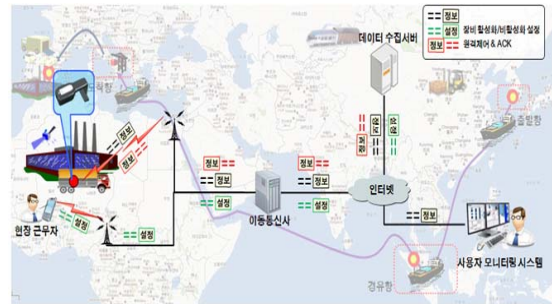


그림 3. ConTracer를 이용한 컨테이너 보안 시스템  
Fig. 3 Container Security System Using the ConTracer

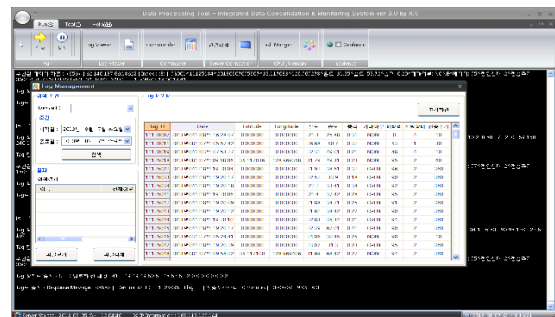


그림 4. 정보 수집용 서버(DCP)  
Fig. 4 Data Consolidation Point(DCP)

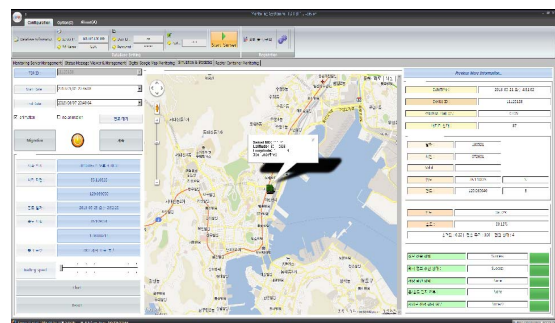


그림 5. 사용자 모니터링 프로그램  
Fig. 5 User monitoring program

그림 4는 다수의 ConTracer에서 정보를 동시에 수집하여 사용자에게 정보를 제공할 수 있도록 해주는 정보 수집용 서버 프로그램이다. 정보 수집용 서버는 정보 수집뿐만 아니라 사용자 모니터링 프로그램을 통해 사용자가 설정한 장비의 설정 변경 정보를 저장하고 있다가 운영

중인 ConTracer에서 보내온 정보에 대한 서버의 응답으로 ConTracer에게 설정 정보를 전달하여, ConTracer의 운영 중 능동적으로 장비의 전송 주기 및 정보를 전송할 정보 수집용 서버 IP/Port 변경, ConTracer 내부 메모리 삭제, 433MHz Active RFID 태그 기능 On/Off, 장비 전원 강제 Off 등 장비의 원격 제어가 가능하다.

그림 5는 정보 수집 서버를 통해 수집한 정보들을 사용자에게 제공하기 위한 모니터링 프로그램이다. 사용자들은 이 모니터링 프로그램을 통해 글로벌하게 이동하는 컨테이너들이 실시간 상태 정보 및 위치를 한눈에 파악할 수 있으며, 필요 시 특정 장비의 운영 정보를 리포트 형식으로 출력할 수 있다. 또한 운영이 완료된 장비를 대상으로 시뮬레이션 기능을 이용하여 이전 운행 중 특정 지역에서 어떤 상태로 인 장비의 설정을 원격지에서 변경할 수도 있으며, 컨테이너의 불법 문 개폐 발생 및 특정 지역 진입 등에 대한 정보를 팝업형태로 사용자가 인지하기 쉽도록 제공해준다.

## IV. 컨테이너 보안 장치의 실증 테스트

### 4.1. 컨테이너 보안 장치의 실증 테스트 준비

본 연구에서는 개발한 컨테이너 보안 장치의 실증 실험을 위하여 국내 파주 공장에서 출발하여 폴란드 공장까지 총 7곳의 주요 거점을 통해 운송되는 화물 컨테이너에 컨테이너 보안 장치를 부착하고 약 27일간 연속해서 컨테이너의 내부 상태 및 위치 정보 모니터링을 진행하였다.

본 실증 테스트에서 ConTracer의 컨테이너 내부 온도/습도 감지 기능 및 충격 감지기능, 위치 확인 기능 및 특정 위치에 컨테이너가 도착했을 때 실시간으로 관리자에게 알려주는 Geo-Fence 기능 등을 중점으로 검증하였다. 또한 장비 회수 후 실시간으로 전송한 정보와 장비 내부에 남아있는 로그 정보를 비교 정보의 손실이 발생하였는지에 대한 확인도 함께 진행 되었다.

### 4.2. 컨테이너 보안 장치의 부착

국내 출발지 파주 공장에서 컨테이너에 화물을 적입한 후 컨테이너 보안 장치를 그림 6과 같이 파손을 최소화 하면서 내부 상태를 모니터링 하기 위하여 컨테이너 보안 장치의 주요 부분이 컨테이너 내부에 위치하면서

GNSS 위성신호의 수신 및 IoT 통신이 원활하게 하기 위해 안테나 부분은 컨테이너 외부 문 양쪽에 있는 충격 방지 가드 내에 위치하도록 부착하였다.



그림 6. ConTracer의 컨테이너 부착  
Fig. 6 Attached ConTracer

### 4.3. 컨테이너 보안 장치 정보 전송 주기 및 Geo-Fence 기능 설정

본 컨테이너 보안 장치의 실증 실험에서는 ConTracer의 정보 전송 주기를 아래 표 2와 같이 설정하고 정보 전송 주기에 따라 서버에 수신되는 데이터의 수를 확인하였다. 확인 결과 정보전송 주기에 따른 정보가 221개, 국내 및 해외에서의 운송 도중 충격 인터럽트에 의해 발생한 정보 34개 등 총 255개의 정보가 서버로 정상적으로 수신되었으며, 장비 회수 후 ConTracer내부에 저장된 로그를 확인 한 결과도 동일하게 255개의 정보가 남아 있는 것을 확인 하였다.

또한 수신된 정보 중 주요 거점 9곳을 대상으로 Geo-Fence 기능 검증을 위하여 거점의 위·경도를 서버에 DB화하고 장비에서 수신한 위치 정보를 이용하여 특정 지역의 진출입 여부를 확인하고 사전에 설정한 사용자의 SMS와 e-mail을 통해 능동적으로 컨테이너의 특정 지역 진입, 진출 여부에 대한 알람을 제공한다.

### 4.4. 컨테이너 보안 장치 실증 테스트 결과

컨테이너 보안 장치의 실증 테스트 결과 2012년 10월 11일 국내를 출발하여 2011년 11월 6일 폴란드에 도착할 때 까지 그림 7에서 보이는 경로 및 주요거점들을 통과하며 약 27일에 걸쳐 255개의 정보를 국내에서는 WCDMA 통신을 이용하고 중국 YingKou항부터 폴란드 도착지 까지 운송되는 구간에서는 GSM 자동로밍을



통하여 실제 컨테이너가 운영되는 동안에 수집하였으며, 이를 바탕으로 실제 컨테이너의 위치 등을 확인 할 수 있었다.

**표 2.** 컨테이너 보안 장치 실증 테스트 중 정보 전송 주기 설정 및 실제 정보 전송 횟수

**Table. 2** Container Security Device information transfer during the test period setting and the actual number of the transfer of information

구간	정보 전송 주기 (분)	전송 횟수 (서버 수신 정보)			정보 전송 누락 횟수
		주기 전송	인터럽트	총 수신	
국내 내륙 → 인천항	60	6	10	16	0
인천항 → 벨라루스	180	191	22	213	0
벨라루스 → 도착지	60	22	-	22	0
소 개		221	34	255	0

27일 동안 표 2와 같이 컨테이너 보안장치의 정보 전송 주기를 설정하였을 때 배터리 소비량은 약 31% (100% → 69%까지 소비)이었으며, 운송 중 컨테이너에 가해지는 충격에 의한 인터럽트 발생 장소를 확인 한 결과 항만에서 컨테이너의 상·하역 작업 시, TSR 철송 중 산악지역 통과 시에 충격 임계치로 설정한 3G이상의 충격을 감지하여 이를 원격지 서버로 전송 한 것이었다.

컨테이너의 내부 상태 확인과 관련하여서는 그림 7에서 보이는 바와 같이 온도, 습도의 변화 정도를 그래프로 확인 할 수 있었으며, Geo-fence 기능의 확인 결과 표 3과 같이 컨테이너 보안 장치에서 보내온 주요 거점 9곳의 진출입 결과와 실제로 확인한 컨테이너의 주요 거점 진출입 결과와 최대 6시간 이내 오차를 보이며 일치하는 것을 확인 할 수 있었다.

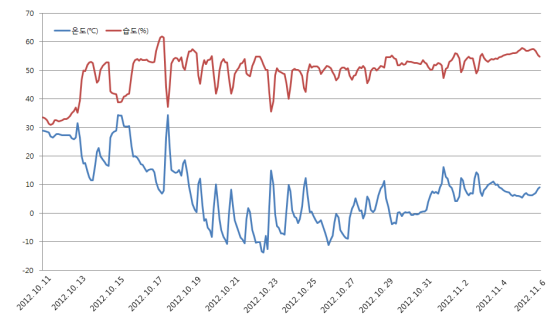
마지막으로 국내에서 폴란드 도착지까지 운송되는 동안 불법적인 문 열림은 감지되지 않았으며, 폴란드 도착지 도착 후 장비를 회수하는 과정에서 컨테이너 문의 열림을 정확히 감지하는 것을 확인 하였으며, 운송 중 컨테이너에 부착한 컨테이너 보안 장치가 정상적으로 컨테이너에 부착되어 외관상으로 특별한 물리적 파손이 없는 상태로 테스트 장비를 회수하고 실증 테스트

를 완료 하였다.

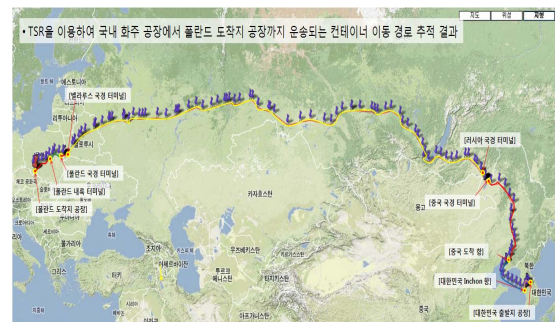
**표 3.** 한국 폴란드 간 이동 중 주요 거점 통과 결과

**Table. 3** Moving to Poland from Korea through the results of the key points

No.	국가	거 점	거점 도착	거점 출발	거점 간 이동 시간
1	Korea	Paju 공장	-	10/11	1일(3시간)
2	Korea	Inchon 항	10/11	10/14	1일
3	China	Yingkou항	10/15	10/16	2일
4	China	Manzhouli 터미널	10/18	10/18	1일(3시간)
5	Russia	Zabaikalsk 터미널	10/18	10/19	16일
6	Belurs	Brest 터미널	11/3	11/4	1일(3시간)
7	Poland	Malaszewicze 터미널	11/4	11/5	2일
8	Poland	Warsaw 터미널	11/5	11/6	1일
9	Poland	Wroclaw 공장	11/6	-	-



**그림 7.** ConTracer의 컨테이너 내부 온도/습도 감지 그래프  
**Fig. 7** Container inside of the container temperature / humidity sensing graph Using the ConTracer



**그림 8.** 테스트에서의 ConTracer 이동 경로  
**Fig. 8** In tests of the moving path ConTracer

## V. 결 론

본 연구를 통해 소개한 컨테이너 보안 장치는 ACSD의 요구사항을 만족 하면서 사용자들의 “글로벌 실시간 물류 가시성 확보”에 대한 요구를 만족 시켜줄 수 있는 장비다. 본 연구를 통해 소개한 ConTracer를 이용하여 국내에서 출발하여 TSR을 이용 약 27일간의 운송기간을 거쳐 폴란드 까지 운송되는 실제 컨테이너 화물의 이동 경로 및 상태정보를 실시간으로 모니터링하고 특정 지역에 컨테이너의 도착 여부를 Geo-Fence 기능이 통하여 SMS 및 e-mail을 통하여 사용자에게 능동적으로 알림이 이루어진 것을 확인할 수 있었다.

실증 테스트에서 확인한 ConTracer의 기능들을 실제 물류모니터링 시스템에 적용하면 실시간 컨테이너의 위치를 기반으로 예상 도착 시간 등을 계산하여 글로벌 물류의 정시성 확보 및 재고관리 분야에 상당히 기여할 것으로 예상된다.

향후 과제로 다수의 컨테이너 보안장치를 이용하여 장거리 해외 물류구간에 대한 추가 적용 테스트 등을 통해 장비 배터리 성능의 확인과 동절기에 TSR 구간에 서의 장비 운영에 대한 추가 테스트가 필요할 것으로 보인다.

### 감사의 글

본 연구는 2013년도 건설교통연구원의 교통체계효율화사업 지원(12교통체계-자유06)에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.



문영식(Young-Sik Moon)

부산대학교 컴퓨터공학과 석사

※관심분야: 항만물류, 컨테이너 보안 장치, 임베디드 시스템, RFID 시스템

## REFERENCES

- [1] U.S Department of Homeland Security Customs and Border Protection, Conveyance Security Device (CSD) Requirements, Version 1.2, December 10, 2007.
- [2] Eun Kyu Lee, Young Sik Moon, Joong Jo Shin, Jung Rock Shon, Sung Pill Choi, Chae Soo Kim, Jae Joong Kim, Hyung Rim Choi, “Pilot case for Container Security Device (CSD) based on Active RFID,” The Korea Institute of Maritime Information & Communication Sciences, Vol.8, No.2, pp.238-243, April. 2010.
- [3] Yousung Kang, Howin Kim, KyoilChung, “Technology Trends of RFID Security Device for cargo container”, KICS Journal(J-KICS), Vol. 24, No11, pp. 43-50, November 2007.
- [4] “RFI: The Container Security Device,” 2005. [Online]. Available : <http://www.hsarpabaa.com/Solicitations/CSD-RFI-ver-8.pdf>
- [5] Hyung Rim Choi, Jae Joong Kim, Moo Hong Kang, Joong Jo Shin, Jung Rock Shon, Young Sik Moon, Eun Kyu Lee “A Study on The Development of Container Security Device (CSD) based on Active RFID”, KICS Journal (J-KICS) Vol.35, No.2, pp.244-251, 2010. 2.
- [6] “DRAFT: Advanced Container Security Device”, 2004. [Online] Available : [https://www.fbo.gov/index?s=opportunity&mode=form&id=8def7d6022d365b5fcf0ff62ea049c38&tab=core&\\_cview=1](https://www.fbo.gov/index?s=opportunity&mode=form&id=8def7d6022d365b5fcf0ff62ea049c38&tab=core&_cview=1)
- [7] Young Sik Moon, Hyung Rim Choi, Hyung Rim Choi, Joong Jo Shin, Jung Rock Shon, Sung Pill Choi, “Study on the Improvement of Container Security Device(ConTracer) Communication Performance”, KICS Winter Conference pp. 51-52, February 2012.
- [8] “Kirsens Monitoring System” [Online] Available : <http://www.kirsensecurity.com/en/solutions-container-monitoring-products-and-applications.php>
- [9] “Triton brochure” [Online] Available : [http://www.starcomsystems.com/wp-content/uploads/2013/02/TRITON\\_english\\_2\\_mail.pdf..](http://www.starcomsystems.com/wp-content/uploads/2013/02/TRITON_english_2_mail.pdf..)





**최성필(Sung-Pill Choi)**

동아대학교 항만물류공학 석사

※관심분야: 물류항만, 냉동컨테이너 시스템, 컨테이너 보안 장치



**이은규(Eun-Kyu Lee)**

건국대학교 전자정보통신공학과 박사 수료

※관심분야: 능동형 RFID 시스템, 컨테이너 보안장치, 안테나 설계



**김재중(Jae-Joong Kim)**

서울대학교 토목공학과 공학박사

※관심분야: 항만계획, 항만운영



**최형림(Hyung-Rim Choi)**

KAIST 경영과학과 경영과학박사

※관심분야: 항만물류시스템, RFID/USN