

비컨 주기와 채널 탐색 기간을 고려한 저전력 CSD의 설계 및 구현

(Design and Implementation of Low-power CSD Considering Beacon Period and Channel Scan Time)

김택현^{*} 박세영^{*}
(Taekhyun Kim) (Seyoung Park)

최훈[†] 백윤주^{**}
(Hoon Choi) (Yunju Baek)

요약 컨테이너 보안 장치(CSD)는 기존 RFID Tag와 달리 컨테이너 내부에 장착하여 물리적 보안을 강화하였고 데이터를 이중으로 암호화함으로써 정보에 대한 보안을 강화한 장치이다. CSD는 배터리로 동작하기 때문에 전원을 효율적으로 사용해야 한다. 따라서 수면 기간과 채널 탐색 기간을 반복하는 저전력 메커니즘이 필요하다. 그러나 이들 기간을 조절함에 따라 에너지의 효율성과 네트워크 연결성의 trade-off가 발생한다. 본 논문에서는 저전력 CSD를 구현함에 있어 비컨 주기와 채널 탐색 기간을 조절하여 이 문제를 해결하고자 하였다. 그 결과 95% 이상의 네트워크 연결성을 보장하고 일반적인 AA 배터리를 장착하여 최대 16일의 수명을 보장하는 것을 볼 수 있었다.

· 이 논문은 부산대학교 자유과제 학술연구비(2년)에 의하여 연구되었음.
· 이 논문은 2009 한국컴퓨터종합학술대회에서 '비컨 주기와 채널 탐색 기간을 고려한 저전력 CSD의 설계 및 구현'의 제목으로 발표된 논문을 확장한 것임

^{*} 정 회 원 : 부산대학교 컴퓨터공학과
malicemind@embed.re.kr
psy3822@embed.re.kr
hara_eslab@embed.re.kr

^{**} 종신회원 : 부산대학교 컴퓨터공학과 교수
yunju@embed.re.kr
(Corresponding author)

논문접수 : 2009년 8월 14일
심사완료 : 2009년 11월 3일

Copyright©2010 한국정보과학회: 개인 목적이나 교육 목적인 경우, 이 저작물의 전체 또는 일부에 대한 복사본 혹은 디지털 사본의 제작을 허가합니다. 이 때, 사본은 상업적 수단으로 사용할 수 없으며 첫 페이지에 본 문구와 출처를 반드시 명시해야 합니다. 이 외의 목적으로 복제, 배포, 출판, 전송 등 모든 유형의 사용행위를 하는 경우에 대하여는 사전에 허가를 얻고 비용을 지불해야 합니다.

정보과학회논문지: 컴퓨팅의 실제 및 레터 제16권 제1호(2010.1)

키워드 : 컨테이너 보안 장치, IEEE 802.15.4, 저전력

Abstract A Container Security Device (CSD) which is different existing RFID Tag strengthens the physical security as mounted inside the container and the information security as encrypts doubly a data. CSD must use the resources efficiently in order to operate with the battery. Therefore, it needs low-power mechanism which repeats the sleep period and channel scan period. However, by adjusting these periods, the trade-off occurs between energy efficiency and network connectivity. In this paper, we implement low-power CSD and resolve this problem by adjusting beacon period and channel scan time. As a result, We guarantee the network connectivity 95% or more and maximum life up to 16 days using common AA batteries.

Key words : Container Security Device, IEEE 802.15.4, low-power

1. 서론

기존의 RFID tag나 전자 봉인 장치는 화물의 처리 시간, 보안 등이 강화되었으나, 여전히 외부의 물리적인 공격에 대한 문제점과 정보 보안 측면에서 문제점을 지니고 있다. 이에 따라 보안 측면에서 더 높은 보안성을 지닌 장비의 규격이나 보안 프로토콜에 대한 요구가 증가하고 있다.

2007년 말, 미국 국토안보부에서는 컨테이너 보안 장치(CSD)에 대한 규격을 발표하였다[1-3]. CSD는 컨테이너 내부에 장착하여 물리적인 보안을 강화하고 CSD에게 명령을 내리는 CSD 리더와 CSD 간의 명령 및 데이터는 이중으로 암호화한다. 그리고 암호화에 대한 키(key)를 DHS의 Data Consolidation Point(DCP)에서 관리함으로써 화물의 정보에 대한 보안 수준을 높였다.

CSD는 IEEE 802.15.4b[4]방식을 채택하였고 컨테이너 내부에 부착되어 동작하며, CSD 리더와 통신하기 위해서 전 채널 탐색을 반복 수행한다. 그리고 리더의 비컨 신호를 받게 되면 리더의 네트워크에 연결되어 CSD 표준 규격에 의거하여 컨테이너 검수에 필요한 정보를 주고 받는다.

CSD는 배터리로 동작하며 컨테이너 안에 부착된다. 그래서 출발지부터 도착지까지 배터리 교환 없이 계속 동작해야 하고, 동작 중에는 표준 규격을 준수하기 위해서 최소 1초 주기로 도어 상태를 감지해야 한다. 그러므로 CSD는 한정된 전원을 효율적으로 사용하기 위한 방법이 필요하다.

전원의 효과적인 사용을 위해 수면 기간을 최대한 늘리고 채널 탐색 기간을 최소로 하면 에너지 효율을 높일 수 있다. 그러나 리더의 비컨 신호를 놓쳐 네트워크

에 연결되지 않는 문제가 발생한다. 반면에 수면 기간을 최소로 하고 채널 탐색 시간을 최대로 하면 리더와의 연결에는 문제가 없지만 에너지 효율이 낮아진다. 따라서 수면 시간과 채널 탐색 시간을 최적으로 조절하는 것이 중요하다.

본 논문에서는 이러한 문제의 해결을 위해 저전력 동작이 가능한 CSD를 설계 및 구현하였다. 비컨 주기와 채널 탐색 시간을 조절하고, 실험함으로써 연결성과 에너지 효율성을 동시에 만족하는 값을 찾았자 한다.

논문의 구성은 다음과 같다. 2장에서 배경 지식, 관련 연구 내용에 대해 소개하고, 3장에서 CSD의 설계 및 구현, 4장에서 실제 실험 결과를 통해 성능을 제시하고 마지막 5장 결론에서는 논문의 기여 및 향후 연구 과제에 대해 설명한다.

2. 관련 연구

CSD는 Container Security Device 혹은 Conveyance Security Device의 약자로 컨테이너에 장착되는 보안 기능이 있는 장치를 통칭하는 단어이다. 현재의 CSD는 2.4GHz 대역에서 IEEE 802.15.4b 방식으로 통신하고 컨테이너의 내부에 장착되어 컨테이너 도어의 개폐를 감지하는 방식을 통해 장치 자체의 물리적인 보안을 높이며, HMAC-SHA256[5], AES128[6] 알고리즘을 사용한 이중의 암호화 기법을 통해 기존의 여타 컨테이너 보안 장치들에 비해 데이터 보안을 강화한 장치이다.

CSD의 시스템은 CSD, CSD Reader, DCP 등으로 구성한다. CSD는 CSD리더와 IEEE 802.15.4의 스타 토폴로지로 네트워크를 구성한다. CSD 리더는 WPAN의 코디네이터(Coordinator)로 동작한다. CSD들은 주변에 있는 CSD 리더의 네트워크에 참여해 명령과 데이터를 주고받는다. 하나의 네트워크에 참여하면 리더와의 연결이 끊어지기 전까지는 다른 리더와는 통신하지 않는다. CSD와 리더 간의 명령과 데이터들이 각각 다른 순서와 방식을 통해 암호화되고, 명령의 종류에 따라 암호화/비암호화 방식으로 나뉘기 때문에 보안성이 높다.

CSD 리더는 고정형(Fixed Type)와 이동형(Hand-Held Type)으로 구분되며, 이동형 리더는 다시 장착(Arming)만을 위한 장착용 리더(Arming Reader)와 검수 과정을 위한 SHHR(Secure Hand Held Reader)로 구분한다.

DCP는 웹 서버의 형태로 존재하고 리더를 통해 CSD에 명령을 내리고 CSD로부터의 데이터를 리더로부터 받는다. 리더와 DCP 간에는 SOAP Data format을 이용하여 통신한다. DCP는 DHS가 관리하며 CSD가 장착될 때부터 해제될 때까지 CSD의 화물 관련 정보와 이벤트 로그 등을 관리한다.

3. 저전력 CSD의 설계 및 구현

3.1 규격을 준수한 CSD의 설계 및 구현

본 논문에서 설계한 컨테이너 보안장치의 전체 하드웨어 설계는 그림 1과 같다. CSD 규격의 기능을 실행하기 위한 모듈들이다. 그리고 그림 2는 본 논문에서 구현한 CSD 하드웨어와 목업이다. 프로세서와 RF 트랜시버는 하나의 칩으로 결합되어 있는 상태이다. 그 외의 모듈들은 프로세서에 연결되어 명령과 데이터를 주고 받는다.

CSD를 위한 프로세서와 RF 트랜시버의 선정에서 가장 중요하게 생각해야 할 것은 CSD의 규격 지원 여부, 낮은 소비 전력, 다수의 외부 입력포트 지원여부이다. CSD의 통신 규격을 만족하기 위해 RF 트랜시버는 2.4GHz 대역에서 통신하며 IEEE 802.15.4 표준을 지원해야 한다. 또한 무선 신호 송수신 시 소모하는 전류량이 적어야 한다. 본 논문에서 설계한 CSD는 무선 신호 송수신을 위한 RF 트랜시버로서 TI사의 CC2430ZF128을 사용하였다[7].

CC2430은 무선 신호 송수신 시 수십 밀리암페어 단위의 낮은 전류를 소모하며, 저전력 동작을 위한 다양한 전력 모드를 제공한다. 이를 이용해 CSD의 동작에 적합한 전력 모드를 선택해 사용할 수 있어 본 논문에서

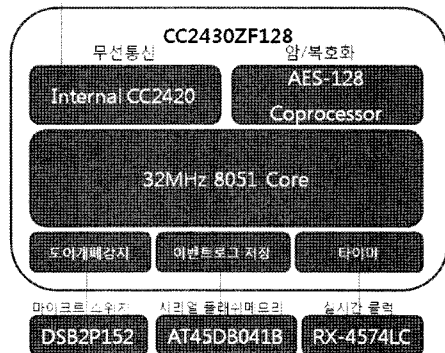


그림 1 저전력을 고려한 컨테이너 보안장치의 전체 하드웨어 설계

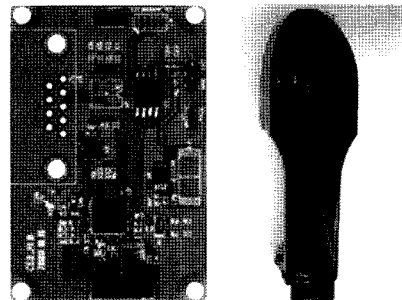


그림 2 저전력을 고려한 컨테이너 보안장치

설계하는 CSD의 요구사항에 적합하다. CSD의 저전력 모드 동작을 위한 전력 모드로 PM(Power mode)3을 선택하였다. PM3은 CC2430의 전력 모드 중 가장 적은 전류를 소모하며 외부의 인터럽트를 이용해 저전력 모드에서 액티브 모드로 복귀할 수 있게 되어 있다.

CSD의 모든 메시지에는 현재 시간을 기록해야 한다. 그래서 이 시간을 기록하기 위한 RTC(Real Time Clock)로서 RX-4574LC를 사용하였다[8]. RX-4574LC의 기능 중에 일정 간격으로 외부 인터럽트를 발생하는 기능이 있어 CSD는 PM3모드에서 액티브 모드로 복귀할 수 있다.

CSD는 여행 중의 모든 이벤트를 기록해야 하며 천개 이상의 이벤트 로그를 기록할 수 있어야 한다. AT45DB014B는 시리얼 플래쉬 메모리로서 512kbyte의 용량을 가지고 있어 기록하기에 적합하다[9].

DSB2P152는 컨테이너 도어의 미세한 개폐를 감지할 수 있는 장치이다[10]. CSD에 2개가 부착되어 각각 도어의 open, close 상태를 감지한다. 도어가 개폐될 때 이 스위치는 CC2430에게 외부 인터럽트를 발생시킴으로써 도어 개폐 여부를 감지한다.

IEEE 802.15.4는 TI사에서 제공하는 TIMAC을 사용하고 CSD의 표준 문서에 따라 네트워크 계층과 어플리케이션 프로토콜을 구현하였다.

3.2 저전력 동작을 위한 메커니즘

CSD의 동작 중에서 가장 빈도가 높고, 가장 전류를 많이 소모하는 동작은 무선 신호 수신이다. 수신 시도 시간이 길어질수록 배터리의 수명이 짧아지게 되므로, CSD의 저전력 동작은 배터리를 최대한 적게 소모하면서 어떻게 효율적으로 CSD의 기능을 구현할 것인가에 중점을 두어야 한다.

CSD는 컨테이너의 정보를 수집하기 위해서 출발지, 출발항, 종착지 단 3곳에서만 몇 초 동안 리더와 통신이 이루어진다. 그리고 나머지 기간은 리더의 비컨을 수신하기 위해 계속 무선 신호 수신을 시도한다. 따라서 전체 과정에 1%도 되지 않는 리더와의 통신 시간을 위해서 무선 신호 수신 모드로 동작한다. 이것은 배터리 소모로 이어져 배터리의 수명을 단축시키게 된다. 그러므로 CSD는 대부분 기간 동안은 전력 소비가 거의 없는 수면 상태로 대기하고, 리더와의 연결을 위해 일정 기간 동안은 채널 탐색 과정을 수행한다[11].

CSD 리더는 2.4GHz 대역의 11번에서 26번 채널 중 사용 가능한 가장 빠른 채널을 사용하여 비컨을 보낸다. CSD는 비컨을 수신하기 위해서 전 채널을 탐색하고 만약 비컨을 수신하면 근처에 리더가 있다고 판단하여 리더의 네트워크에 연결을 시도한다.

그림 3은 CSD의 기본적인 동작 흐름을 나타내고 있다. CSD는 전 채널에서 CSD 리더의 비컨을 반복적으

로 탐색한다. 탐색에 일정 횟수 이상 실패하게 되면 일정 기간 동안 수면 혹은 유휴 상태에 들어가고, 그 기간 이후 다시 탐색을 시작한다. 탐색 도중 리더의 비컨을 수신하게 되면 CSD 리더에 associate 요청 메시지를 전송하고 이것이 리더에 의해 승인되면 리더와 네트워크를 구성하여 통신을 하게 된다. 이때 CSD는 리더의 비컨에 의한 Guaranteed Time Slot(GTS) 구간 내에서 리더의 명령을 받고, 할당된 타임 슬롯에서 그에 대한 응답을 보내게 된다. 리더와의 네트워크를 구성한 상태에서 일정 기간 동안 비컨을 수신하지 못하거나, 리더로부터 Disassociate 명령을 수신하는 경우 네트워크에서 연결을 종료한 후 동일한 리더와의 통신을 곧 바로 재개하는 것을 방지하기 위해 일정 기간 유휴 상태에 머무르게 된다[3]. 그림 4는 수면 기간과 채널 탐색 기간이 변화되는 것을 전류량으로 보여준다.

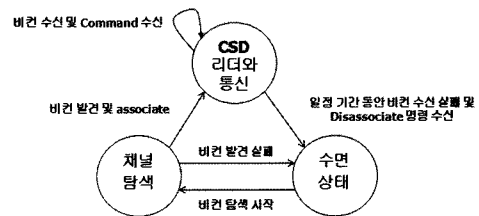


그림 3 기본적인 CSD의 동작

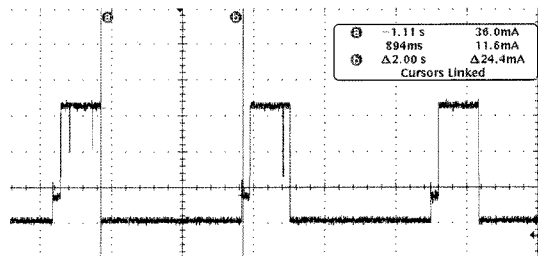


그림 4 수면 기간과 채널 탐색 기간의 전류량

컨테이너의 도어 개폐 여부는 최소 1초마다 주기적으로 감지함으로써 실시간으로 도어 개폐 여부를 확인할 수 있어야 한다. 본 논문에서는 주기적으로 개폐 여부를 확인하는 방법 대신 인터럽트 방식으로 도어 개폐가 될 때만 동작하는 방식으로 전력 소비에 미치는 영향이 거의 없다고 판단한다. 그리고 이 방법은 실시간으로 개폐 여부를 확인할 수 있으므로 표준 규격에 적합하다고 할 수 있다.

3.3 비컨 오더와 채널 탐색 기간의 조절

채널 탐색 도중에 사용되는 전력은 비컨 신호를 수신하기 위해 무선 신호를 수신하는 기간이기 때문에 많은 전원을 소비한다. 그래서 이 수신 전력 소비를 최소화할 수 있다면 CSD가 저전력으로 동작할 수 있다. 그러나

이 수신 기간을 최소화한다면 주기적으로 발생하는 비컨과 타이밍이 어긋나 CSD가 리더 주변에 있는데도 불구하고 리더의 네트워크에 연결이 되지 않아 리더와 통신을 하지 못하는 경우가 발생한다.

그리고 저전력으로 동작하기 위해서 수면 시간을 최대화한다면 리더가 비컨을 보내고 있는 기간에도 수면 모드로 동작하기 때문에 비컨 신호를 못 받고 계속 수면 상태로 대기하는 경우가 발생하게 된다. 이 장에서는 CSD의 연결성을 보장할 수 있는 최대 수면 시간과 전력을 가장 적게 사용하는 최소 채널 탐색 시간으로 조절하고 분석하였다. 그리고 네트워크 연결의 또 다른 요인인 비컨 주기를 조절하였다.

우선 전 채널 탐색 시간을 조절하였다. 전력을 가장 많이 사용하는 수신 기간을 늘리는 방법은 저전력에 있어서 효과적인 방법이 아니다. 그러므로 전 채널 탐색 시간은 IEEE 802.15.4에서 가장 최소화한 496ms부터 시작하여 리더의 비컨 신호 수신 여부를 실험하였다. 496ms로 채널 탐색을 하여도 리더의 비컨 신호를 받는 것은 문제가 없었다. 그러므로 채널 탐색 시간은 496ms로 정하였다.

수면 모드 기간은 길면 길수록 저전력에 유리하다. 그러나 리더와의 연결성 문제가 발생하며 CSD 표준규격에 어긋나게 된다. 그러므로 네트워크 연결성을 보장할 수 있는 최대 수면 시간을 분석하였다. CSD 표준규격의 최대 전송거리는 30m 이상이며 컨테이너 운송차량의 최대속도는 15.7m/s이다. 그러므로 컨테이너 운송차량은 리더의 비컨 신호가 도달하는 가장 먼 곳에서 리더까지 도달하는 시간이 약 2초이다. 그래서 수면 모드 기간을 2초로 설정하였다.

비컨은 저전력을 고려하지 않아도 되는 리더가 보낸다. 그러므로 CSD 저전력 정책에 아무런 영향을 주지 않는다. IEEE 802.15.4에서 비컨 오더를 조정하여 비컨 주기를 조정할 수 있다. 이 비컨 오더를 최소로 하여 비컨 주기를 최소화한다. 그러므로 CSD가 수면 모드에서 깨어나 비컨을 수신할 확률이 높아진다.

4. 성능 평가

지금까지 CSD의 설계 및 구현에 대해서 알아보았다. 본 논문에서 제안하는 CSD의 채널 탐색 전류 소모를 측정하여 CSD의 수명을 예측하여 그 성능 평가한다. 그리고 리더의 비컨 주기를 조정하여 실제 CSD가 네트워크에 연결할 때 성공 확률을 분석한다.

일반적인 AA 배터리 2800mAh를 장착하는 것을 기준으로 하였다. 채널 탐색 시간과 수면 시간의 전류를 측정함으로써 본 논문에서 구현한 CSD의 소비 전류량을 계산하였다. 채널 탐색 시간의 전류는 MCU On, All

channel scan, Shut down 총 3단계로 구분할 수 있고, 수면 시간과 합쳐서 총 4단계구간으로 나누어 그림 5와 같이 전류를 측정하였다.

전류 측정 계산 결과 약 16일 정도 배터리를 유지할 수 있는 결과가 나왔다. 전류 측정 결과를 증명하기 위해서 그림 6과 같이 RF영향을 차단할 수 있는 차폐박스에 CSD를 넣고 하루에 한번 리더와의 통신 실험했을 때 16일 후 리더와 통신을 할 수 없었다. 그러므로 전류를 측정하여 계산한 결과와 일치되는 것을 확인할 수 있었다.

네트워크 연결 성공 확률 실험은 실내에서 리더를 켜놓은 상태에서 CSD를 리더 통신 거리 안에서 동작시키는 방법으로 CSD가 CSD 리더의 네트워크에 연결되는 시점의 채널 탐색 시간을 카운팅하는 실험을 하였다. 비컨 오더는 2, 3, 4로 적용하여 100회 반복 실험을 하였다. 비컨 오더에 따른 시간간격은 그림 7과 같다. 채널 탐색 시간 측정은 그림 8과 같이 오실로스코프를 이용하였다.

• MCU On: 0.112s * 8.6mA = 0.85mAs
• All channel scan: 0.496s * 33mA = 16.37mAs
• Shut down: 0.0028s * 14.2 = 0.040mAs
• 수면 기간: 2s * 1.06632 = 2.2mAs
• 한 구간 당 총 전류량: 0.8512mAs + 16.37mAs + 0.040mAs + 2.2mAs = 19.50mAs
• 한 구간 당 총 시간: 0.112 + 0.56 + 0.0028 + 2 = 2.67s
• CSD가 1초당 사용한 전류량: 19.50mAs / 2.67s = 7.29mA
• 배터리 총 전류량 : 2800mAh = 1008000mAs
• 배터리 수명: 10,080,000mAs / 7.29mA = 1,382,716s = 23,045m = 384h = 약 16일

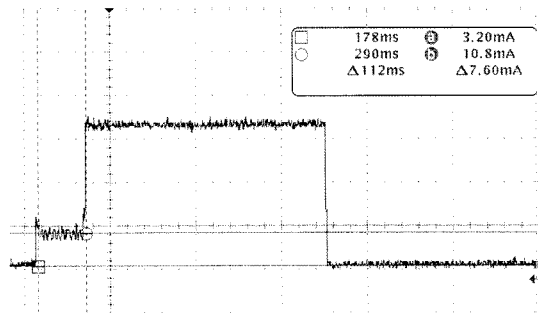


그림 5 전류 측정 화면(MCU On)

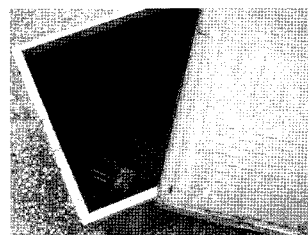


그림 6 차폐박스 실험 환경

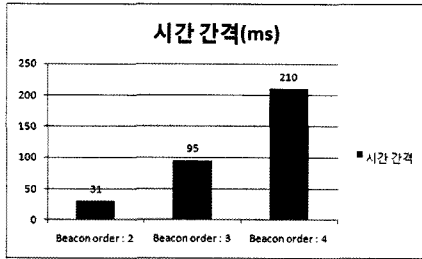


그림 7 비컨 오더에 따른 시간간격

표 1 Associate 성공 시점 평균(100회 실행)

	Beacon order : 2	Beacon order : 3	Beacon order : 4
성공시점평균	1.1	2.05	4.1

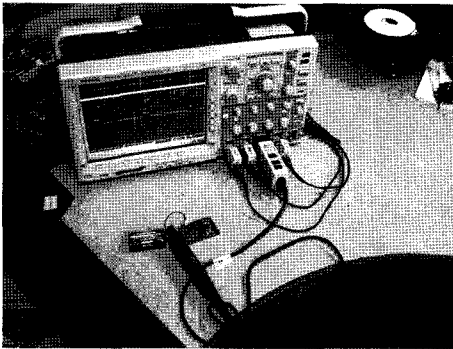


그림 8 네트워크 연결 성공확률 실험 환경

CSD와 리더와의 통신 거리는 최대 30m이고 이것을 반경으로 통신 가능한 최대 이동 거리는 60m이다. 그리고 컨테이너 운송차량의 최대 속도는 15.7m/s이며 시간으로 환산하면 약 4초이다. 수면 모드 주기가 2초이기 때문에 최소 2번의 시도 안에 네트워크 연결이 가능해야 한다. 그러므로 표 1을 참고로 비컨 오더를 3 이하로 하면 CSD의 성능에 아무런 지장을 주지 않는다. 비컨 오더를 2로 하면 비컨 간격이 너무 좁아 CSD가 패킷을 주고받는 과정에서 비컨을 잃어버리는 문제가 발생하였다. 그러므로 가장 적합 비컨 오더는 3인 것을 알 수 있다.

5. 결론 및 향후 계획

항만 물류에서 컨테이너의 물동량이 많아짐에 따라 RFID의 중요도가 높아지고 있지만, 이를 위한 보안에 관련된 RFID 제품의 개발은 아직 미미한 실정이다. 본 논문에서 제안하는 저전력 컨테이너 보안장치는 CSD의 표준 규격을 준수한다. 그리고 배터리의 수명을 향상시키기 위해 전력을 적게 소모하는 하드웨어를 이용한 하드웨어 플랫폼과 저전력 동작 기법들을 설계하였다.

본 논문에서 제안한 저전력 CSD는 비컨 주기, 채널 탐색 기간, 수면 기간을 효과적으로 조절하여 일반적인 AA 배터리로 동작하여 최대 16일 동안 동작하며, 이동 중에 리더와 연결 시도할 때 95% 이상의 연결 신뢰성을 보장한다.

향후 저전력 기능을 향상시킬 수 있는 추가적인 하드웨어의 조사와 안테나의 조사에 따른 향상된 통신 성능 확보를 통해 수명을 더욱 증대시킬 수 있도록 하는 연구가 진행될 것이다.

참고 문헌

- [1] Conveyance Security Device (CSD) Requirement Document Baseline version 1.2, December 10, 2007.
- [2] Conveyance Security Device (CSD)-to-CSD Reader Interface Control Document (ICD) Baseline version 1.0 December 10, 2007.
- [3] CSD Reader-to-Data Consolidation Point (DCP) Interface Control Document (ICD) Baseline version 1.0.
- [4] IEEE 802.15.4. Revision b, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), 2006.
- [5] HMAC-SHA256 Secure Hash Standard, Federal Information Processing Standards Publication 180-2.
- [6] AES128 Advanced Encryption Standard Federal Information Processing Standards Publication 197.
- [7] CC2430, A True System-on-chip solution for 2.4GHz IEEE 802.15.4 / ZigBee(TM) (Rev.F).
- [8] RX-4574LC, <http://www.epsontoyocom.co.jp/english/product/RTC/set02/rx4574lc/index.html>.
- [9] AT45DB014B 4-megabit 2.5-volt or 2.7-volt Data-Flash, <http://www.atmel.com>.
- [10] DSB2P152, <http://www.daesungmicro.co.kr/>.
- [11] Seyoung Park, Taekhyun Kim, Hoon Choi, Hyuntae Cho and Yunju Baek, "Design and Implementation of Low-Power 2.4GHz Active RFID Tag," *Proc. Of Ubiquitous Convergence Technology 2008*, pp.134-136, 2008.