ISO 18185 기반의 컨테이너 안전수송 시스템 구현

추영열* · 최수영**

Implementing Secure Container Transportation Systems Based on ISO 18185 Specification

Young-yeol Choo* · Su-Young Choi**

본 연구는 지식경제부 지방 혁신사업 지원으로 수행되었음.(B0009720)

요 약

이 논문에서는 ISO 18185 표준에 따른 컨테이너의 전자봉인과 출발지부터 목적지에 도달할 때까지 화물의 보안 상태를 감시하는 컨테이너 안전수송 감시 시스템의 구현 결과를 기술한다. 전자봉인 표준의 경우 기밀성(confidentiality)에 대한 사양이 정의되어 있지 않아 도청과 같은 보안공격에 취약하다. 이를 위해 RC5와 AES-128 표준에 따른 암호화/복호화 기능을 구현하고 그 성능을 비교하였다. 실험결과는 암·복호화 시간 지연에서 RC5가 우수함을 보였다. 아울러 데이터의 길이가 증가 할수록, 낮은 CPU 성능에서는 더욱 유리하다. 그러나 Tag와 리더 사이의 통신시간을 포함한 응답시간에서는 암호화 처리시간이 차지하는 비중이 1% 미만으로 RC5와 AES-128 사이에 의미있는 성능 차이가 없어 두 사양 모두 사용 가능함을 확인하였다.

ABSTRACT

This paper describes implementation of electonic seal (E-Seal) of a container based on ISO 18185 standard and development of monitoring systems checking E-Seal device and cargo states in the container for secure transportation from departure to destination. For lack of definition on confidentiality support in ISO 18185-4 standard, it is vulnerable to security attack such as sniffing. To cope with this, we developed encryption/decryption functions implementing RC5 and AES-128 standards and compared their performance. Experimental results showed that RC5 outperformed AES-128 in terms of time delay. In addition, RC5 had an advantage under the condition of large sized messages as well as CPUs with low performance. However, the portion of encryption/decryption processing time was less than 1 percent of response time including communication delay between E-Seal tags and readers. Hence, the performance difference between RC5 and AES-128 standards was trivial, which revealed that both specifications were allowable in developed systems.

키워드

ISO 18185, E-Seal, RFID, RC5, AES-128

Key word

ISO 18185, 전자봉인장치, 무선인식장치, RC5, AES-128

* 동명대학교 컴퓨터공학과 (교신저자)

** 동명대학교 컴퓨터공학과

접수일자 : 2010. 02. 09

심사완료일자 : 2010. 03. 23

Ⅰ. 서 론

전 세계 물동량의 80%이상은 컨테이너를 이용하여 운송되고 있다 [1]. 그러나 이중 2 ~ 4% 만이 각 국가에 운송될 때 검사를 받는다. 미국의 911 테러 이후 국제 물류에서는 화물 컨테이너의 운송을 보다 안전하고 효율적으로 관리하기 위하여 수・출입 절차에 대한 규제가 강화되고 있다. 이를 위해 미국 뿐 아니라 유럽 등 각국 정부 및 기구를 통해 조례와 규정들이 제정되고 있다. Automated Targeting System(ATS), Customs Trade Partnership Against Terrorism (CTPAT), Container Security Initiative (CSI), and Smart & Secure Trade lanes (SST) 등이 중요한 사례이다[2],[3].

화물 컨테이너의 안전하고 효율적인 운송 및 화물 정보의 안전한 전달 지원을 위해 대표적인 보안장치로는 전자봉인(E-Seal : Electronic Seal)과 컨테이너 운송 보안장치 (CSD: Conveyance Security Device)가 있다. E-Seal은 ISO TC 104SC4WG2에서 국제 표준화 작업을 진행하고 있으며, ISO 18185규격번호를 가지고 있다[4-8]. 그러나 E-Seal에는 정보보호 규정이 없어 이에 대한 보완이 필요하다.

한편, CSD는 2007년 12월 12일 미국의 DHS (Department of Homeland Security)에서 RFI (Request For Information)가 발표되었으며 전자봉인과는 달리 표준화 기구가 아닌 GE 등 기업체 들을 중심으로 상업화가 진행되고 있다. 아래의 표 1은 전자봉인과 컨테이너 보안장치의 특성 비교이다[9-12].

표 1. 전자봉인 과 컨테이너 보안장치의 특성
Table 1. Characteristics of E-Seal and CSD

구분	E-Seal	CSD
사용주파수	433MHz, 2.4GHz	2.4GHz
위치인식	있음	없음
화물정보 저장	없음	가능
컨테이너 개폐확인	가능	가능
장착위치	컨테이너 외부	컨테이너 내부
데이터보호	없음	있음
국제표준	ISO18185	없음
재사용여부	불가	가능

2005년 8월 31일에 발표된 ISO 18185-4 규격은 전자봉인이 비밀정보를 가지지 않는다는 전제조건 하에 어떠한 보호기술도 명시하지 않고 있다. 그러나 도청공격 자체도 Tag Parameter 영역에 중요한 데이터 입력되어 있을시 악의적인 공격자에 의해 정보유출이 가능해 진다. 특히, 데이터 위변조에는 대단히 취약하여 화물의 도난, 또는 내용물이 바뀔 수 있는 등 보안상의 위험이 있다.

E-Seal은 국제표준 논의를 통해 등장한 기술인 반면 CSD는 미국의 GE에서 독자적으로 개발한 RFID장치이며, GE와 더불어 유럽의 지멘스, 한국의 삼성물산, 일본의 미쓰비시 등의 산업체를 중심으로 상용화가 추진되고 있다. CSD는 화물컨테이너 운송과정에서 요구되는 효율성과 보안성을 만족시키기 위해 AES-128 (Advanced Encription Standard 128) 암호화 알고리즘, Kerberos 네트워크 인증서비스를 정의하고 있다 [13].

이 논문에서는 ISO 18185 E-Seal 표준에 따라 컨테이너의 봉인으로부터 목적지에 도달할 때까지 화물의 보안 상태를 감시하는 컨테이너 안전수송 감시 시스템의 구현하여 비교한 결과를 기술한다. E-Seal 표준의 경우 기밀성(confidentiality)에 대한 사양이 정의되어 있지 않음을 고려, RC5와 AES-128을 구현, 두 시스템의 성능을 비교한다. 또한, 항만 운영시스템인 TOS (Terminal Operation System) 서버와의 연동에 대해 기술한다.

본 논문의 구성은 다음과 같다. 2장에서 RC5와 AES-128암호화 알고리즘에 기반한 컨테이너 상태감시 시스템의 HW 및 SW에 대하여 기술한다. 3장에서는 E-Seal System에 적용된 암호화 모듈의 성능을 측정하고 응답시간, Tag의 인식거리 실험 및 결과에 대해 기술하고, 마지막으로 4장에서 결론을 맺는다.

Ⅱ. 컨테이너 상태 감시 시스템

이 장에서는 컨테이너 안전 수송을 위해 개발된 컨테이너 감시 시스템의 구조와 RC5와 AES-128 암호화 기능 개발에 대해 기술한다.

2.1 E-Seal 시스템

E-Seal 시스템의 전체적 구성은 그림 1과 같다.

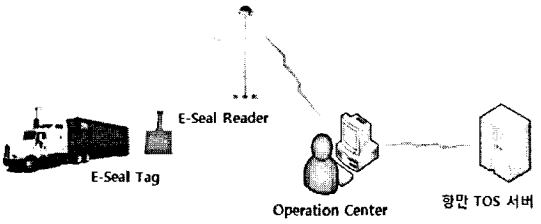

그림 1. E-Seal 시스템 구성
Fig. 1. E-Seal system configuration

컨테이너의 보안상태 감시를 위하여 컨테이너에 E-Seal Tag를 부착하여 Tag와 E-Seal Reader 송·수신하는 정보를 사용자 Application에서 실시간 또는 정보 요청시 마다 받아보도록 설계 하였다. E-Seal Tag와 Reader와는 ISO/IEC 18000-7 규격을 준용하는 433MHz 통신방식의 RFID 통신이며[14], Reader와 사용자 Application은 TCP/IP 소켓통신으로 이루어진다. 항만 TOS와 사용자 응용 역시 TCP/IP 소켓통신으로 이루어진다. 컨테이너 화물의 운송 흐름은 최초 컨테이너에 화물이 적입되는 송화주에서 컨테이너 화물을 선적 후, E-Seal Tag를 부착하고 Tag를 활성화 시킨 후, 화물정보를 생성하여 저장하게 된다.

도착항에 도착한 컨테이너는 Reader의 인식 반경 내로 진입하면 Reader는 Operation Center에 Tag의 상태 및 화물정보를 발송하게 되고, 이 정보는 다시 항만 TOS 서버에 전달되어 초기(선적 시)에 부착된 Tag인지를 인증하게 되고 항만 내에서 필요한 정보를 파싱하여 일련의 작업을 수행하게 된다.

2.2 E-Seal System의 동작과정

E-Seal System에서는 두 가지 통신 프로토콜을 가진다. 첫 번째로 Operator와 Reader간 IP통신이며, 두 번째가 Reader와 Tag간 RF통신이다. 아래의 그림 2는 E-Seal System에서의 통신 단계를 보여주며, 각 단계의 동작은 표 2에서 나타내었다.

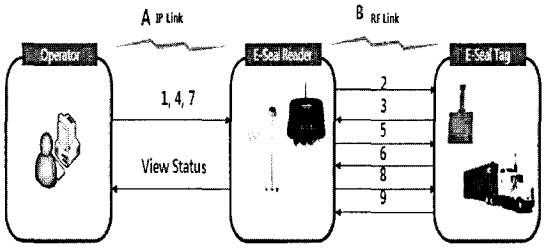

그림 2. E-Seal 시스템 통신 과정
Fig. 2. E-Seal system communication procedures

표 2. 각 통신 단계별 동작
Table 2. Operation at each communication step

순번	내용
A	E-Seal Reader와 Application 시작
B	E-Seal Reader는 Tag와 커뮤니케이션 관계 성립
1	Operator는 Wake 요구
2	E-Seal Reader는 Tag 에 Wake 요청
3	Tag는 E-seal Reader에게 Wake 응답 발송
4	Operator는 운송정보 입력
5	E-Seal Reader는 Tag에 운송정보 발송
6	Tag는 E-Seal Reader에 응답
7	Operator는 상태 정보 요구
8	E-Seal Reader는 Tag에 상태 정보 요청
9	Tag는 Reader에 상태 정보 발송

최초 E-Seal Reader와 Tag간 커뮤니케이션 관계가 수립되어야한다. 그 후 Operator는 소켓을 이용하여 Reader에게 접속하여 일련의 행동을 취하게 된다. 아래에서 [9]에 따른 각 단계별 동작과 메시지 형태를 설명한다.

- 1 단계 : Operator는 Tag를 깨우기 위하여 'Wake'명령을 Reader에게 전송한다.
- 2 단계 : Operator로부터 요청받은 Wake 명령을 Tag에게 전송하게 된다. 이때 전송하는 Wake 명령은 Broadcast하여 Reader 인식 반경 내에 있는 모든 Tag에게 전송된다.
- 3 단계 : Reader로부터 받은 'Wake'명령으로 Tag는 Active 상태가 되고 이에 응답메시지를 생성하여 Reader에게 응답하게 된다.

• 4 단계 : Operator는 Tag의 메모리 공간에 운송화물 정보를 기입하기 위하여 화물정보데이터와 함께 TagID를 실어 Reader에게 전송한다. Tag의 메모리 공간에 기입되는 정보는 EPCglobal의 GID-96 (General Identifier-96)의 규격에 따라 구현하였다. 아래의 표 3은 GID-96의 구조를 나타낸다[15].

표 3. GID-96의 구조
Table 3. Structure of GID-96

	Header	EPC Manager	Object Class	Serial Number
비트수	8	28	24	39
용량	0011 0101	268,435,456	16,777,216	68,719,476,736

• 5 단계 : Reader는 Operator로부터 받은 data와 자신의 ID를 기입하여 Tag에게 전송하게 된다.
• 6 단계 : Tag는 Reader로부터 받은 data를 자신의 메모리 공간에 저장하게 된다.
• 7 단계 : Operator는 수시로 Tag의 상태를 요청하기 위하여 Inventory신호를 Reader에게 보내게 된다.
• 8 단계 : Reader는 Operator에게 받은 명령을 Tag에게 전송하게 된다.
• 9 단계 : Tag는 자신의 상태를 Reader에게 전송하게 된다. Tag의 상태정보는 아래의 표 4와 같다[4-8].

표 4. 봉인 상태 메시지 필드
Table 4. Seal status message field

Bit Seal Status							
15	14	13	12	11	10	9	8
Mode field				01 - Unsealed and open 10 - Sealed and closed 11 - Open 00 - Reserved		Reserved	Ack 1 = NAK 0 = ACK

Bit							Battery Status
7	6	5	4	3	2	1	0
Reserved		Seal type			Reserved	Reserved	Battery 1 = low 0 = good

최종 Tag의 상태 메시지는 Reader로부터 사용자에게 전송하게 되는데 Tag의 상태는 'Unsealed and open', 'Sealed and close', 'Open'의 3 가지 형태로 그 의미는 다음과 같다.

1) Unsealed and open: Tag를 Seal하지 않았고 컨테이너 Door도 open된 상태.
2) Sealed and close: Tag도 Seal되었고 컨테이너 문도 닫힌 상태.
3) Open: Tag와 컨테이너가 개방된 상태

2.3 E-Seal System H/W 구현

본 논문에서 제안하는 E-Seal System은 그림 3과 같이 4가지의 H/W 구성요소를 가진다. 각 모듈의 기능은 다음과 같다.

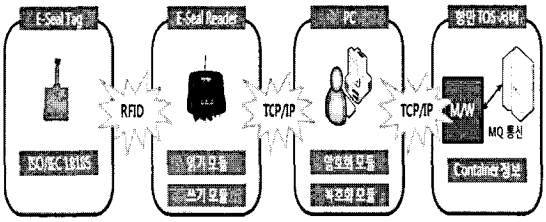

그림 3. E-Seal 시스템 하드웨어 연결
Fig. 3. E-Seal system H/W connection

• PC
그림 1에서 언급한 Operation Center 역할을 담당하는 부분으로 컨테이너에 대한 데이터를 관리하고, 태그의 상태 및 처리과정을 제어할 수 있도록 하기 위한 HMI기반의 항만 모니터링 시스템이다. tag와의 송수신 정보에 대한 암호화 및 복호화 모듈을 갖는다.
• E-Seal Reader
E-Seal Tag와 433MHz 대역에서 통신하는 모듈로서, 태그 정보에 대한 읽기, 쓰기 기능이 구현되었다.
• E-Seal Tag
Tag의기본적인정보로는 TgaID +RSSI +Seal +Battery 그리고 40bytes 의 메모리 공간을 가진다. 이 메모리 공간에 화물정보 및 데이터를 저장하게 된다.
• 항만 TOS 서버
Tag의 data 영역에 들어간 정보 이외의 컨테이너 정보를 저장하고 있는 서버로서 User의 요청에 의해 정보를 제공하는 역할을 한다.

- 항만 M/W
  항만 TOS서버 내에 구현되며 TCP/IP 규약에 따라 메시지 큐 방식으로 구현하였다.

2.4 E-Seal System S/W 구성

E-Seal Tag의 data 영역이 제한되어 있기 때문에 많은 컨테이너 정보를 모두 저장할 수 없게 된다. 그러므로 Tag에 들어간 정보이외의 정보를 수신하기 위해서는 TOS 서버에 접속하여 Data를 획득한다. 또한 컨테이너 화물에 대한 데이터를 운영자에게 표시해주고 운영자가 처리과정을 제어할 수 있도록 하기위해 HMI (Human Machine Interface) Software를 이용하여 항만 모니터링 프로그램을 제작 하였다. HMI Software는 Wonderware의 InTouch Ver. 10이 사용되었다. E-Seal의 정보의 수집을 위해 TCP/IP로 연결되는 DLL Driver를 제작하였다. 수신된 데이터는 곧바로 Application에 표시되고 DDE (Dynamic Data Exchange) 통신을 통해서 구현된 GUI 화면을 통해 조업자에게 제공된다.

가. DDE 통신 I/O 서버

DDE는 윈도우즈 환경에서 Application 간에 서로 데이터를 주고받을 수 있도록 마이크로소프트에 의해 디자인된 프로세스간 통신 방식으로 클라이언트/서버 모델에 따른다. 제어 프로그램에서 획득한 E-Seal Tag의 정보를 DDE 통신을 통하여 상태 감시 프로그램으로 전달되고 최종 GUI 프로그램에서 E-Seal의 상태 및 컨테이너 정보를 조업자에게 보여준다. 아래의 그림. 4는 DDE통신을 통한 E-Seal 시스템 SW 흐름도이다.

InTouch로 작성한 응용에서는 E-Seal의 상태정보를 실시간으로 모니터링 할 수 있고 E-Seal Tag Memory영역에 컨테이너에 대한 일련의 정보를 암호화하여 저장할 수 있게 하였다. 또한 불법적인 컨테이너 개폐에 대해서는 알람경보를 발생시켜 관리자에게 경고 메시지를 발생한다.

Application 기능은 아래와 같다.

- E-Seal Reader와의 TCP/IP 소켓 통신
- E-Seal Tag의 Wake Up 기능
- 화물정보를 기입하기 위한 Write 기능
- 화물정보를 읽기위한 Memory Read 기능
- Tag의 상태를 읽기위한 Inventory 기능
- Tag의 개폐여부에 따른 알람 기능
- 항만 TOS 서버와의 연동 기능

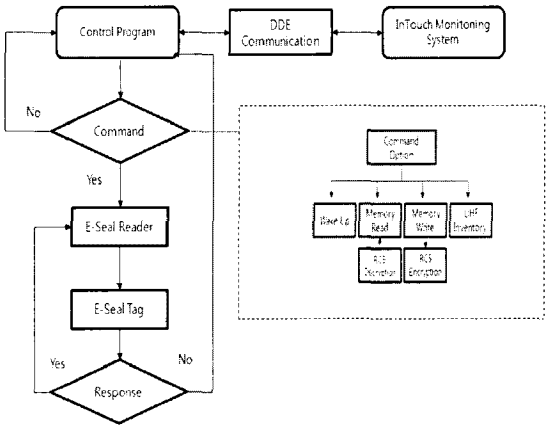

그림 4. E-Seal 시스템 S/W 흐름도
Fig. 4. E-Seal system S/W flow chart

그림 5는 개발된 E-Seal 상태 감시 시스템의 한 화면이다.

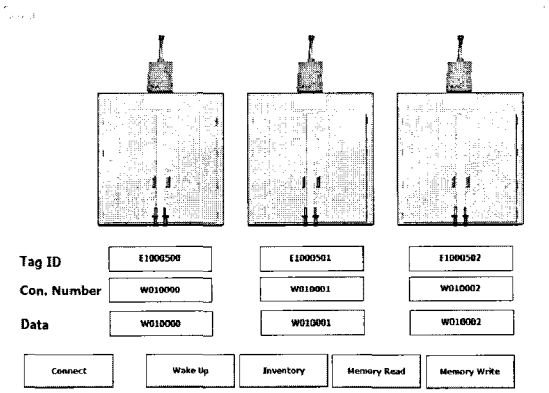

그림 5. 구현된 서버 화면
Fig. 5. A GUI display implemented in server

나. 암호화/복호화 단계

악의적인 공격자로 하여금 도청공격으로부터 주요 변수 데이터를 보호하기 위하여 데이터 암호화 알고리즘을 PC에 적용한다. 작성한 Application에서는 RFC2040에 정의되어 있는 RC5 대칭키 알고리즘과 AES-128 알고리즘을 사용하여 Tag 데이터를 암호화 한다. 본 연구에서 RC5는 가변적으로 키 길이를 지정할 수

있으므로 보안성 강도를 높일 수 있으며, 제한된 메모리를 가진 시스템에 적합하다[12].

본 연구에서 암호화되는 데이터는 Message Type, Message Subtype, Parameter로 구성되어 있다.

III. 실험 결과 및 분석

3.1 RC5 와 AES-128 기반 성능 비교

본 연구에서는 E-Seal 장비가 계산능력이 제한됨을 고려하여 RC5와 AES-128 알고리즘의 처리 부하에 대한 실험을 수행하였다. RC5와 AES-128 암호화 알고리즘은 128bit의 암호화키를 외부에서 직접 입력받아 16bytes씩 블록 암호화를 수행한다. RC5는 16라운드 CTS (Cipher Text Seal) 모드이며, AES-128 알고리즘은 10라운드 CTS 모드를 사용하였다[16].

실험결과는 아래의 표 5와 그림 6에 나타내었다. 본 실험의 환경은 Intel(R) Core(TM)2 CPU 6400, 2.13GHz, 1.98GB RAM이다. 각 단계별 실험은 100번의 횟수에서 획득한 데이터의 평균값이며, 최초 data를 암호화 함수에 할당하는 순간부터 암호화 완료 시점까지의 처리시간이다. 암호화 및 복호화 알고리즘을 성능이 우수한 PC 단에서 처리하기 때문에 처리시간이 매우 빠르다. 실험 결과에서 보듯이 RC 5알고리즘의 처리 속도가 AES-128 알고리즘 보다 우수한 것을 확인할 수 있다. 하지만 실제 구현 환경이 32비트 PC가 아닌 8비트 등의 내장형 시스템이 될 경우를 고려한다면 암호화 계산에 사용되는 시간이 AES-128의 경우 4.25 msec, RC5의 경우 25.5 μsec로 암호화가 reader에서 실행되므로 구현이 가능한 계산량이다. 그러나 계산 시간이 메시지의 길이에 비례함을 고려하면 RC5가 유리함을 알 수 있다.

표 5. RC5와 AES-128 암/복호화 처리 속도
Table 5. Encryption/Decryption speed of RC5 and AES-128

Data Length (byte)	delay(μsec)	
	RC5	AES-128
16 bytes	5.4	540
32 bytes	8.1	1090
64 bytes	13.8	2101
128 bytes	25.5	4250

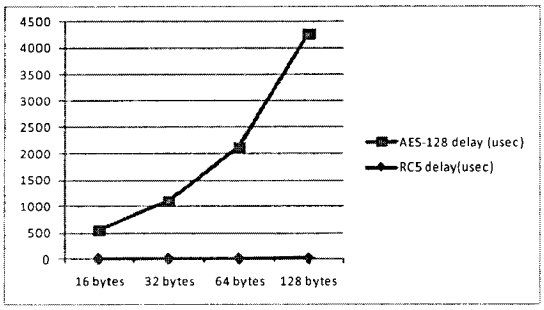

그림 6. RC5와 AES-128 암/복호화 처리 속도
Fig. 6. Encryption/Decryption speed in RC5 and AES-128

3.2 Reader에 요청 후 응답시간

RFID 시스템에서 가장 중요한 요인 중 하나는 RFID Reader에 요청을 한 후 응답을 수신할 때까지의 turn around 지연이다. 암호화 과정이 포함된 Tag의 응답 과정은 다음과 같다.

- 응용 프로그램은 Reader로 Wake 명령 송신
- Reader는 이 명령을 Tag로 송신
- Tag는 Wake 응답을 Reader로 송신
- Wake 응답 신호를 수신한 Reader는 응용으로 응답 메시지 송신
- 응용 프로그램은 적용된 암호화 알고리즘(RC5, AES-128)으로 Data를 암호화한 후, Reader로 Write 명령 송신
- Reader는 Tag로 Write 명령 전달
- Tag는 Write 명령을 잘 받았다는 응답신호를 Reader로 송신
- Reader는 응용으로 응답 메시지 송신

위와 같은 과정을 거쳐 응용프로그램으로 수신되는 시간은 암호화 과정을 제외하고 표 6과 같이 약 7.215sec였다. RC5와 AES-128알고리즘 수행 시간은 100배 정도의 차이를 보이나 통신을 포함한 응답시간에서 이 시간은 거의 영향이 없음을 보여준다. 통신지연시간은 일반적으로 다음과 같이 3가지 요소로 구성된다.

통신지연 (communication delay) =
+ 처리지연 (processing delay)
+ 전송지연 (transmission delay)
+ 전파지연 (propagattion delay)

처리지연은 통신과정에서의 SW, HW 처리에 소요되는 지연시간을, 전송지연은 네트워크 카드의 전송속도와 메시지의 길이에 따라 결정되는 지연시간을, 전파지연은 전송 매체별 신호의 전달속도에 의해 결정되는 지연시간을 각각 나타낸다. 암/복호화 알고리즘에 소요되는 시간은 앞절의 실험결과 5msec 이하였고 메시지의 길이도 128 바이트 이하로 10Mbps의 전송속도에서 1msec 이하이다. 또한, 전파의 전달 속도는 300,000 Km/sec이므로 본 실험에서의 최소거리(10m) 와 최대거리(40m)간의 차 30m 는 30m/3x108m/sec = 0.1 μsec로써 전파지연시간은 거의 무시할 수 있다. 따라서, 지연시간의 대부분이 Wake 신호의 처리 등 과정상 총 7개의 프로세스 기동시간 즉, 처리지연에서 발생하는 것으로 분석된다. 하지만 암호화될 Data의 양이 늘어나면, CPU의 계산 성능이 낮을수록 RC5가 상대적으로 성능면에서 유리하다.

표 6. RC5와 AES-128의 응답 시간
Table 6. Response time of RC5 and AES-128

Data Length (byte)	RC5 delay (sec)	AES-128 delay (sec)
16 bytes	7.21500	7.21554
32 bytes	7.21500	7.21510
64 bytes	7.21501	7.215210
128 bytes	7.21502	7.21542

3.3 Reader와 Tag의 거리에 따른 응답시간

Reader의 성능을 측정하기 위해 Tag를 10m, 20m, 30m, 40m 로 거리를 변화하면서 Tag가 Reader의 요청에 반응하는지를 측정하였다. 이 과정은 Reader로부터 Inventory 신호를 받은 Tag가 자신의 상태 정보를 응답하는 시간으로 최대의 배터리 상태에서 실험하였다. 실험 결과는 아래의 표 7, 그림 7과 같이 평균응답시간이 4.01sec였다.

표 7. E-Seal 시스템의 거리에 따른 응답 속도
Table 7. Transmission delay in E-Seal System

Distance(m)	E-Seal(sec)
10m	3.859
20m	4.312
30m	3.766
40m	4.125

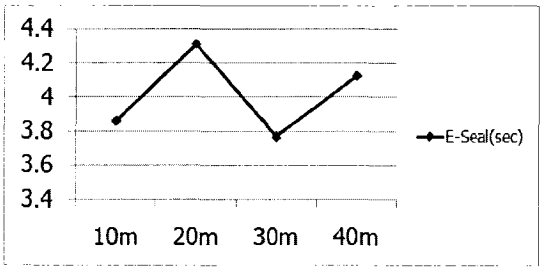

그림 7. E-Seal 시스템의 거리에 따른 응답 속도
Fig. 7. Transmission delay in E-Seal System according to distances

앞 절에서의 turn-around 시간과 비교하면 7.215 (sec) - 4.01 (sec) = 3.205 (sec) 의 평균지연시간 차이가 있다. 즉, 응용 프로그램의 Wake 과정, 암/복호화 프로세스의 기동과정, 리더가 결과를 응용프로그램에 전달하는 과정이 이 시간에 소요됨을 알 수 있다. 본 연구의 구현 환경이 리더를 포함하여 실시간 운영체제가 아닌 PC 상에서 이루어짐에 따라 각 프로세스가 invoke 되고 전송 메시지를 기다리는 프로세스의 context switching time 등에서 지연이 발생되는 것으로 분석된다. 그래프에서 거리별로 응답시간이 일정하지 않은 것은 비실시간 운영체제 하에서 시스템의 상태에 따라 통신처리 SW의 동작 시간에 차이가 있고 측정 오차가 포함된 것으로 분석된다.

즉, 통신 지연의 오차 범위가 암/복호화 처리지연을 훨씬 상회함으로써 응답지연을 줄이기 위해서는 실시간 운영체제 및 처리과정을 구현한 SW의 단순화가 필요한 것이로 분석된다.

Ⅳ. 결론

본 논문에서는 컨테이너의 안전 수송 서비스를 위해 ISO 18185 사양을 기반으로 한 컨테이너 상태 감시시스템 개발에 대하여 기술하였다. 또한, ISO 18185-4 표준규약이 어떠한 보호기술을 적용하지 않고 있어 보안상의 취약점을 보안하기 위하여 RC5암호 알고리즘과 AES-128 표준에 따른 보안서비스를 구현하였다. 구현된 두 알고리즘의 성능을 비교 분석하였다. 또한, E-Seal Reader와 Tag의 거리에 따른 응답시간을 측정함

으로써 향후 항만에서의 실제 적용 환경을 실험하였다. 항만 시스템에의 적용을 고려하여 항만 작업자의 작업 편의성을 위한 조업 화면을 개발하여 E-Seal Tag의 상태를 실시간으로 파악할 수 있도록 하였다. 향후 E-Seal Tag에 온도, 습도, 충격 등의 화물 상태를 함께 감시하여 화물의 상태까지 서비스할 수 있는 시스템으로 확장할 예정이다. 또한 CSD의 경우와 암호화 알고리즘을 8비트로 구현하였을 때에 대한 성능 연구가 필요하다.

감사의 글

본 연구는 지식경제부 지방 혁신사업 지원으로 수행되었음.(B0009720)

참고문헌

[1] Stefen Schaefer, "Secure Trade Lane: A sensor network solution for more predictable and more secure container shipments," *Proc. of OOPSLA'06*, pp. 839-845, Oct. 2006

[2] 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. Int'l Conf. on Communication Systems Software and Middleware*, pp. 662-669, Jan. 2008.

[3] Pu Yunming, Jiang Jingui and Lin Yicong, "Research on container monitoring security infrastructure," *Int'l Conf. on Convergence Information Technology*, pp. 2030-2033, Nov., 2007.

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

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

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

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

[8] ISO, ISO 18185-1 Freight containers - Electronic seals - Part 5 : Physical layer 2007.

[9] 강유성, 김호원, 정교일, "화물 컨테이너 보호를 위한 RFID 보안장치 기술 동향," 한국통신학회지 제24권 제 11호, pp. 43-50, 11. 2007.

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

[11] William Stallings, *Cryptography and Network Security : Principles and Practice*, 2nd Edition, Prentice Hall, 1999

[12] Freight Container - Identification and Communication, Electronic Seals - Part4 : Data Protection

[13] 김주해, 최은영, 이동훈, "A security model for duplication resistant eSeal," 정보보호학회논문지 제17권 제 5호, pp. 111-116, 10. 2007

[14] 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

[15] 안재명, 이종태, 오해석 공저, EPCglobal Network 기반의 RFID 기술 및 활용, Global출판사, 2007

[16] D.Henrici and Paul Muller, "Hash-vased en-hancement of location privacy for Radio Frequecy Identification devices using varying identifiers," *PerSec'04 at IEEE PerCom*, pp.149-153, 2004

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 부산IT융합부품
연구소 연구원
※관심분야: USN, Embedded system, E-Seal, Network Security