RFID 기반 국제 물류 서비스의 보안 정책

황정희*, 신문선**, 황익수***, 김현철***
*남서울대학교 컴퓨터학과
**건국대학교 컴퓨터시스템전공
***한국무역정보통신(주)
e-mail: jhhwang@nsu.ac.kr

Security Control of International Logistic Service based on RFID

Jeong Hee Hwang*, Moon-Sun Shin**, Ik-Soo Hwang***, Hun-Chul Kim***
*Dept. of Computer Science, Namseoul University
**Dept. of Computer Science, Kon-Kook University
***KTNET

요 약

RFID 기술은 유비쿼터스 환경을 구현하기 위한 핵심기술 중 하나로 기술 개발과 시범사업 등을 통해 충분한 성장 가능성과 기술력 향상이 기대된다. 특히 물류 환경에서 RFID 기술 기반의 물류 환경 관리는 비용 및 납기의 개선 등에 큰 효율성을 가져올 수 있다. 이 논문에서는 RFID 기반의 국제 물류 프로세스에 대한 보안 위험 요소를 분석하고 이에 대한 보안 요구사항 및 보안 정책 방안을 기술한다.

1. 서론

RFID(Radio Frequency IDentification) 시스템은 무선 통신 기술을 이용하여 직접 접촉하지 않고 RFID 태그 정보를 식별할 수 있기 때문에 기존의 바코드 시스템보다 많은 장점을 갖는다. 즉, 주파수를 사용하여 태그에 직접 접촉하지 않고도 한 번에 다수의 태그를 읽을 수 있다. 이러한 RFID의 장점 때문에 기존의 표준화된 제품을 대량 생산하는 방식에서 탈피하여 RFID 시스템을 기반으로 하는 고객의 다양한 요구에 맞추어 제조, 납품하는 대량 맞춤 서비스가 보편화되고 있으며 SCM(Supply Chain Management)을 위한 비즈니스 솔루션이 등장하게 되었다[1,2]. RFID를 이용한 제품의 제조 및 유통과정에서 제품의 흐름에 대한 가시성을 확보할 수 있어 업무 효율성이 향상되고 전체적인 물류 유통흐름에서 보다 효과적인 재고 관리 및 제품 추적이 가능하며, 제품 무결성이 향상되고 제품 손실률을 줄일 수 있는 장점이 있다[2,3,4]. 그러나 RFID기반의 국제 물류 서비스 플랫폼에서의 효율적인 물류처리 서비스에서는 우선적으로 물류 정보의 보안 문제를 해결해야 한다. 제품 정보에 대한 보안뿐만 아니라 도용, 위치 추적, 물리적 공격 등 RFID 기반 물류 환경의 특성상 나타나게 되는 여러 가지 위협에 대한 Security와 Privacy 문제가 드러나고 있으며 이는 RFID기술 기반 물류 환경 관리의 기술발전과 보급을 저해하는 요인이 되고 있다.

EPCglobal Network[5,6,7]는 RFID 태그 정보의 구조, 의미, 전달방법에 대한 표준을 제공하고, 개별기업은 EPCglobal Network 상에서 발생하는 정보를 각 기업과 기관의 방화벽 안에서 개별적으로 관리하고, 이 정보는 ONS(Object Naming Service)와 Discovery Service를 통해 공유하는 방식으로 운영된다. 이렇게 EPCglobal Network는 거대한 물류환경에서 EPC정보의 분산관리와 전달 효율성을 높일 수 있으나 각 기업과 기관의 방화벽과 같은 보안계층으로만 위협요소를 모두 제거할 수 없으며 국제물류 서비스 플로우상에서 나타나는 위협에 대한 태그 보안, 물류 보안, 인증, 접근제어 등의 보안문제에 대한 해결책은 현재 미비한 단계이다.

따라서 이 논문에서는 RFID기반의 국제 물류 서비스 플랫폼에서의 신뢰성과 제품 무결성의 보장 및 EPC Network 상에서 물류 정보와 사용자 정보를 보호하기 위해 EPCglobal의 보안 가이드라인을 기반으로 하는 국제 물류 서비스에서의 보안 요구사항 및 보안 정책방안을 기술한다.

2. 관련연구

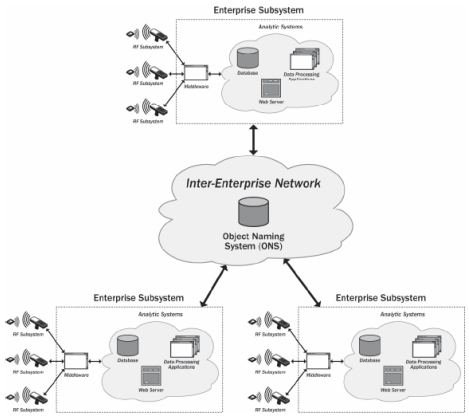
EPCglobal 아키텍처 프레임워크는 EPC(Electroic Product Code)를 사용하여 공급/유통망 강화라는 공동 목표를 위해 서비스하는 것이다. 즉, EPCglobal과 위임기관이 운용하는 코어서비스(EPCglobal Core Service)와 데이터 인터페이스, 소프트웨어, 하드웨어 관련 표준(EPCglobal Standard)의 종합이다. EPCglobal과 EPCglobal Architecture Framework 요소를 사용하는 개별 가입자와 상호작용하는 시너지 효과를 비공식적으로

이 연구는 지식경제부 uGLP성장동력기술개발사업(한국무역정보통신)의 지원에 의하여 연구되었음

"EPCglobal Network"라고 한다[5].

EPCglobal 네트워크란 EPC 코드와 RFID 기술을 바탕으로 제품에 식별번호를 부여하고 정보를 저장할 수 있는 공간을 네트워크로 연동하여 공급자, 수요자, 그리고 소비자가 제품에 관련된 정보를 알 수 있게 해주는 시스템이다. 즉, RFID 리더와 같은 여러 데이터 자원에서 하나 이상의 EPC 데이터를 수집하고, 사용자의 요구에 맞게 필터링 및 그룹화 하여 다양한 형태로 보고하거나 EPCIS에 처리된 데이터를 저장할 수 있는 표준이며, 애플리케이션 비즈니스 로직과 인프라스트럭처 컴포넌트 사이에 독립성을 제공한다.

이러한 EPCglobal 네트워크기반의 RFID 응용 시스템은 다양한 응용분야에서 기본적으로 (그림 1)과 같은 Inter-Enterprise Architecture 프레임 기반으로 적용 가능하다. 오픈 네트워크 형태이든지 혹은 클로즈드 네트워크을 기반으로 하든지 기본 구조는 (그림 1)과 같은 형태의 엔터프라이즈 서브시스템의 연동을 통해서 응용서비스를 수행하게 된다.



(그림 1) Inter-Enterprise Architecture

RFID 기반의 국제 물류 프로세스를 위한 기본적인 구성요소로 태그(tag), 리더(reader), 안테나(antenna)가 있다.

RFID Tag는 기본적으로 상품코드인 EPC가 기록된 라벨 형태의 RFID IC칩과 전파를 송수신하는 안테나로 구성되어있다[8]. 리더기는 태그와 정보를 송/수신하는 장치로 태그에서 수집된 정보를 관리시스템으로 전송하고 안테나, 제어장치, RF장치, 통신장치로 구성된다. 응용프로그램을 수행하는 PC 혹은 기타 단말기와 Serial[RS232-C, RS422등] 혹은 랜 통신(TCP/IP)으로 연결되며, RFID 신호를 암호화/디코딩하는 역할을 수행한다[9]. 그리고 안테나는 리더기에서 보내온 신호를 공간으로 방사하는 역할 및 Tag에서 보내 온 시그널을 수신하여 리더기로 보내는 역할을 수행한다[10].

3. RFID 시스템의 보안 요구사항

이 절에서는 RFID 시스템의 주요 구성요소인 태그, 리더기, 안테나에 대한 보안 위험 및 이를 고려하는 보안 요구사항을 기술한다.

3.1 태그(tag) 보안

기본적인 물품 코드 정보를 포함하고 있는 태그에 대한 보안 정책 방안으로 태그에 패스워드를 부여하여 인증하는 방식을 사용한다. 패스워드는 도청을 막기 위해 주변 환경을 물리적으로 보호하는 차원에서 사용될 수 있으므로 각각의 태그에 지정해야 한다. 그리고 태그 간에 서로 다른 패스워드를 지정하여 공유할 수 없도록 해야 한다. 이러한 태그의 패스워드 부여와 더불어 안전한 보안을 위해 태그에 데이터를 저장하기 전에 데이터에 대한 암호화를 하는 것이 필요하다. 패스워드가 누출되어 태그에 접근했을 때에도 데이터에 대한 암호화로 인해 실제 데이터를 읽을 수 없도록 하는 방법이 필요하다.

RF 인터페이스에서 리더기와 태그간의 교류가 자주 발생하지 않는 태그에 대해 일시적으로 정지(turn off)가 가능하도록 한다. 이것은 공격자로부터의 도청이나 공격을 줄일수 있는 방법이 될 수도 있다. 그러나 이와 같은 일시적 정비 방법은 태그와 리더기간의 교류 횟수에 대한 예측을 할 수 있는 경우에 적용할 수 있다. 또한 이와 같은 방법의 하나로 태그를 비활성화(deactivate)상태에 두고 있다가 스위치가 켜지면 다시 RF와 태그가 교류할 수 있도록 활성화하는 방법도 가능하다.

리더기는 주기적으로 태그의 지속적인 존재와 동작 상태를 확인할 수 있는 모니터링을 수행하여 태그에 인증받지 않은 접근자의 탐지 및 예기치 않은 데이터 교환 등을 즉시 식별할 수 있도록 해야 한다.

이와 같은 태그 보안 정책과 더불어 태그와 관련하여 신호를 전송하고 받는 radio frequency는 태그의 수행에 있어 태그의 동작 범위, 속도, 데이터 전송률과도 연관된다. 그러므로 태그가 반응할 수 있는 범위, 주파수의 충돌 가능성, 주파수 변화에 따른 태그의 이동성 등을 고려해야 한다.

3.2 리더기(reader) 보안

리더기와 태그 간의 커뮤니케이션을 위해서는 표준을 따라야 한다. 이를 위해 일반적으로 같은 벤더의 태그와 리더기가 사용된다. 리더의 형태에는 유선 리더와 무선 리더가 있다. 유선 리더는 고정된 위치에 있으면서 리더에 접근하여 태그를 읽는 형태가 있다. 이러한 예로써 신호위반 카메라가 이에 속한다. 그리고 무선 리더는 이동 가능한 리더를 의미한다. 모든 리더기는 태그와 소통할 수 있는 RF 서브시스템이 있다. 그리고 엔터프라이즈 서브시스템과 소통할 수 있는 인터페이스가 있다. 엔터프라이즈 서브시스템 인터페이스는 분석 및 처리를 위해 리더로부터 엔터프라이즈 서브시스템의 컴퓨터까지 RFID 데이터

의 전송을 지원한다.

각 리더기에는 허용되는 power output 과 duty cycle이 있다. duty cycle는 장치가 일정기간동안 에너지를 방출하는 시간의 퍼센트(1분에 30초 소통시-50%)를 의미한다. passive tag와 통신하는 리더는 active tag와 통신하는 것보다 더 큰 power output를 필요로 한다. 강력한 power의 duty cycle를 가진 리더가 더 먼 거리로부터 또는 정확하게 태그를 읽는다. 그러나 너무 강력한 power의 출력은 도청 위험을 증가시킬 수 있으므로 이를 고려해야 한다.

리더기는 일반적으로 다양한 안테나 타입을 사용하여 태그와 소통할 수 있다. 특히, 분리된 안테나(detachable antenna)는 리더의 요구사항에 맞게 선택적으로 적용될 경우에 적합하다. 그러므로 안테나의 특징들을 기반으로 하여 태그와 안테나의 커뮤니케이션 방법을 이해하고 이를 고려해야 한다. 또한 여러 개의 태그가 근접해 있을 때 리더기가 특정 태그를 식별하고 처리할 수 있는 개별화(Singulation)할 수 있어야 한다. 리더기가 특정 태그에게 질의를 보낼 때 리더기는 여러 개의 태그로부터 동시에 응답을 하지 말아야 한다. 즉, 태그는 랜덤하게 주어지는 번호에 일치할 때 응답하고, 리더기는 충돌되는 태그가 없다는 것을 확인하여 태그와 지속적으로 소통해야 한다.

3.3 안테나(antenna) 보안

태그에서 보내온 신호를 수신하는 안테나를 위한 보안 정책 방안으로 가장 일반적인 방법은 부서지기 쉬운 안테나를 사용하는 것이다. 이것은 RFID 태그는 공격자가 태그를 수정 및 변경하거나 태그를 제거하는 것을 방지하기 위해 위조가 불가능하도록 공격자의 접근했을 때 안테나가 오작동을 일으켜 태그에 접근할 수 없도록 하는 방법이다.

그리고 안테나의 사용에 있어 비즈니스 응용에 따라 적당한 무선 주파수(Radio frequency)를 선택해야 한다. 주파수 사용에 있어서 고정된 주파수(fixed frequency)를 사용하는 것은 무선 신호에 대한 방해 및 충돌을 효과적으로 줄일 수 있기 때문이다.

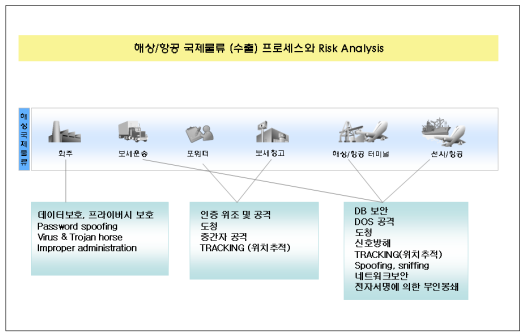
RF 시스템의 운영자(operator)는 리더기 또는 능동 태그로부터 전송된 RF 에너지 레벨을 조정하여 보안에 대비할 수 있다. 즉, 안테나의 일부 타입은 전송된 RF 에너지의 방향을 조정할 수 있도록 되어 있기 때문에 이러한 안테나의 조정을 통해 보안에 대비할 수 있다. 또한 안테나와 관련된 전파 범위에 전자기의 보호(electromagnetic shielding) 장치 및 제한할 수 있는 방법을 마련하는 것이다. 이것은 RF 신호를 보호구역 외로 전파되는 것을 방지할 수 있도록 하여 외부로 부터의 안테나와 관련된 동작 자체를 차단시키는 것이 중요하기 때문이다.

이러한 안테나의 보안 요소를 고려하여, 태그와 소통할 수 있는 충분한 범위 그리고 리더기의 요구사항에 맞는 안테나를 선택하여 적용해야 다른 주파수의 방해를 최소화 하고 도청 가능성을 줄일 수 있다.

4. 국제물류 프로세스에서의 보안 정책

수출 비즈니스 프로세스를 간단히 설명하면, 생산된 제품을 태깅하고 패킹하고 상자를 트럭에 싣고 통합창고로 이동한다. 상자를 팔레트 위에 쌓고 트럭에 적재하여 통합창고 게이트를 통과한다. 통합창고의 게이트를 통과하여 항구 터미널에 도착하게 되고 운송할 선박에 컨테이너를 적재하는 과정을 거친다.

(그림 2)는 물류 수출 프로세스 플로우 상에서 발생할 수 있는 EPCglobal Network 침해 유형을 연관 지어 도식화한 것이다.



(그림 2) 수출 프로세스 플로우 상에서의 보안 위협 요소

각 프로세스 단계에서 발생할 수 있는 위험요소 및 이에 대한 보안 정책을 기술하면 다음과 같다.

■ 상자 및 팔레트 : 태그 프린팅

태그에 저장된 데이터를 보호하기 위하여 태그에 개인 정보와 같은 프라이버시 침해를 유발할 수 있는 정보를 저장하지 않거나 최소화하여 정보가 유출되었을 때에도 쉽게 식별할 수 없도록 해야 한다. 그리고 태그에 사용되는 식별자 형식을 노출되지 않도록 고유의 방법을 선택해야 공격자가 식별자에 대한 예측을 불가능하게 할 수 있다. 태그에 데이터를 저장하기 전에 패스워드 방식 및 암호화하여 정보의 직접적 접근을 방지해야 한다. 또한 데이터 손실이 발생했을 지라도 데이터를 다시 복구할 수 있도록 백업 시스템을 준비해야 한다. 태그 데이터를 보호하기 위한 방법으로 태그 명령어(command)의 사용을 제한하거나 더 이상 사용하지 않는 태그에 대한 kill feature를 적용하여 정보가 유출될 가능성을 줄이는 것도 보안 위험요소를 방지할 수 있다.

■ 컨테이너(트럭차량): e-Seal

물류는 운송중일 때 보안에 가장 취약한 점이 있기 때문에 더욱 주의해야 한다. DOS 공격이나 인증되지 않는 사용자의 접근 및 위치 추적 등과 같은 보안 위협요소들을 방지할 수 있는 보안 정책이 필요하다. 이를 위해 공격 가

능한 거리를 예측하여 추가적인 장비 보안 및 위치 추적이 가능하지 않도록 주기적으로 태그의 지속적인 존재와 동작 상태를 모니터링 하는 방법들이 필요하다.

■ 포워더

물류의 수출과 수입에 있어 제 3자에 해당하는 포워더에 관한 보안 정책으로는 정보의 접근 범위 및 운송 정책에 대한 기밀 보안 사항을 유지할 수 있도록 MOA(Memorandum Of Agreement) 또는 MOU(Memorandum Of Understanding)에 대한 약정의 협약이 필요하다. 그리고 제 3자 기업체의 직원들의 보안 정책들을 잘 숙지하고 있는지 점검을 수시로 해야 정보 유출을 예방할 수 있다.

■ 통합창고 : 게이트

물품을 보관하는 통합창고에서는 물리적인 접근 제어를 최소화 하기 위해 전파 범위에 전자기의 보호(electromagnetic shielding) 장치 및 접근을 제한할 수 있는 방법을 마련하는 것이 필요하다. 즉, RF 신호를 보호 구역 외로 전파되는 것을 방지할 수 있도록 하여 외부로부터 태그와 관련된 동작 자체를 차단시킬 수 있는 electronic shielding과 같은 방법들의 적용 가능성을 고려하는 정책이 필요하다. 그리고 추가적인 보안 방법으로 태그를 비활성화 하여 태그와의 전자적 통신을 통해 물품 정보가 공격받지 않도록 미리 예방하는 정책이 필요하다.

■ 항구터미널 및 선박 : 컨테이너 적재

항구 터미널에서는 선박에 물품을 적재하는 물품 이동 과정을 수반하므로 접근이 허용된 사용자에 한해서만 물품의 운반 과정에 참여해야 하고, 보안 정책에 준하는 행동이 잘 지켜지고 있는지 모니터링 해야 한다. 또한 보안 정책에 위반하는 행동 및 물품의 적재 방법이 발견되었을 때 즉시 위반 사항을 보고하고 이를 통제 및 확인하는 절차가 빠르게 이루어질 수 있도록 사전에 시스템 및 물품 수송과 관련된 직원들의 임무를 분담하고 직원간에 상호 감시를 하도록 하는 철저한 교육이 필요하다.

국제 물류의 프로세스 플로우상에서 발생할 수 있는 위험 요소 및 보안 위협에 대비하기 위해서는 각 단계별에서의 태그 타입과 사용 주파수 그리고 네트워크상에서 이루어지는 시스템 인증 및 사용자 인증에 대한 보안 요구사항을 시스템 분석과 네트워크를 동시에 고려하는 다양한 측면에서의 철저한 준비가 필요하다.

5. 결론

최근 RFID기반 물류 환경은 비즈니스 효율성을 대폭 개선할 수 있을 뿐만 아니라 제품의 제조 유통과정에서 제품과 제품의 정보에 대한 가시성과 제품의 무결성을 확보할 수 있게 하여 업무의 효율성이 향상되고, 물류 통합 서비스 플랫폼에서의 효과적인 재고관리는 물론 제품 추적이 가능하여 제품 무결성과 과잉재고방지, 제품 손실율을 줄일 수 있게 되었다. 그러나 RFID기반의 국제 물류 서비스 플랫폼에서의 효율적인 물류처리 서비스에서는 물류 정보의 보안 문제를 해결하기 위해 보안 위험 요소를 분석하고 이에 대한 보안 정책이 필요하다. 따라서 이 논문에서는 RFID기반의 국제 물류 서비스를 위한 보안 위험 요소를 분석하여 이를 대비하기 위한 RFID 시스템의 기본 구성요소인 태그, 리더기, 안테나에 대한 보안 요구사항을 기술하였고, 물류 프로세스 플로우 상에서 발생할 수 있는 단계별 보안 위협 사항에 대한 보안 요구사항 및 정책방안을 제시하였다. 향후 연구에서는 물류 프로세스 상에서 분석된 보안 요구사항을 반영할 수 있는 보안 모델의 설계에 대한 연구가 지속적으로 수행될 것이다.

참고문헌

[1] 대한상공회의소, "http://scm.korcham.net/download/SCM_guide.pdf, 2005

[2] 안규희, 이기열, 정목동, "RFID 애플리케이션을 위한 엔터프라이즈 애플리케이션 프레임워크와 비즈니스 프로세스 모델," 한국정보과학회 가을 학술 논문집, 제 33권 제2호, 2006.10

[3] 최길영, 성낙선, 모희숙, 박찬원, 권성호,"RFID 기술 및 표준화 동향", 전자통신동향분석 제22권 제3호, 2007. 6

[4] 산은경제연구소. "RFID산업의 동향과 전망", 2007.09

[5] EPCglobal. "The EPCglobal architecture framework final version", July 1,2005

[6] EPCglobal. "EPC Information Services(EPCIS) Version 1.0 Specification", April 12, 2007

[7] EPCglobal. "Object Naming Service(ONS) Version 1.0", October 4,2005

[8] EPCglobal, "EPCglobal Tag Data Standard Version 1.3 Ratified Specification", http://www.epcglobalinc.org, March 8, 2006.

[9] EPCglobal, "Reader Protocol Standard, Version 1.1 Ratified Standard," http://www.epcglobalinc.org, June 21, 2006.

[10] 안재명, 이종태, 오해석, (주)리테일테크 기술연구소, "EPCglogal 네트워크 기반의 RFID 기술 및 활용", 글로벌, 2007.