Green IT를 적용한 선박 네트워크 보안 시스템 연구

백종일* · 박대우* · 안재민** · 장영현*

*호서대학교 벤처전문대학원 IT응용기술학과

**호서대학교 벤처전문대학원 정보경영학과

Ship network security system research that apply Green IT

Jong-Il Baek* · Dea-Woo Park* · Jae-Min An** · Young-Hyun Chang*

*Dept. of, IT application technology, Hoseo Graduate School Of Venture

**Dept. of, Information Management, Hoseo Graduate School Of Venture

E-mail : jibaig101@empal.com, prof1@paran.com, onebit@paran.com, baewhaoa@paran.com

요 약

IT가 미래산업의 주역이 되어가면서 Green IT에 대한 이슈가 늘어가고 있어 자원 재활용, 독성물 사용 절제, 에너지 절약 등이 강조되고 있다. 선박에 구축되는 네트워크 시스템의 Green IT 실현을 위한 근본적인 목적은 자원을 효율적이고 안전하게 사용하는 것이고 이를 위해서 시스템의 부하를 줄 수 있는 악의적인 접근을 통제하여 악성봇 등으로 인한 불필요한 하드웨어 낭비를 절제할 수 있는 네트워크 보안체계에 대해 연구 하였다.

ABSTRACT

As IT becomes leading part of futurity industry, issue about Green IT is being on the increase and resources recycling, toxicity water use resection, saveenergy etc. are emphasized. Fundamental purpose for Neteuwokeusiseutem's Green IT realization that is constructed on ship studied about network security system that can control access that use resources as efficient and safe and is enemy of evil which can give subordinate of system for this and resect unnecessary hardware waste by back more.

키워드

그린 IT(Green IT), 네트워크 시스템(Network system), 네트워크 보안(Network Security), 접근통제(Access control)

Ⅰ. 서 론

최근 십 수년간 우리나라가 일본을 제치고 세계 조선 제1국이 되면서 조선산업에 관한 관심이 부쩍 높아지고 있다. 그러나 조선산업을 떠받치고 있는 세세한 산업분야에 관하여서는 여전히 무관심속에 있다. 조선산업은 종합산업으로서 가구산업에서부터 중공업에 이르기 까지 전후방 산업에 미치는 영향이 크다.

또한 선박의 종류는 다양하여 선박마다 탑재되는 기자재의 종류도 다르다. 그러나 종류가 다른 조선기자재라 하더라도 최근의 경향은 모두 IT화 되고 있다는 사실에는 모두 동일하며, 해운환경변화와 IT부품의 신뢰성 향상으로 IT화의 속도가 급 가속되고 있다는 것이다.

선박은 다른 공산품과는 달리 해양환경과 인근 해역국가의 환경에 막대한 영향을 끼칠수 있으므로 UN산하의 IMO(International Maritime Organization)에서 제정하는 국제협약에 따르게 되어 있다. 최근에 서해에서 발생한 유조선의 기름유출사고를 보면 한 척의 선박사고가 해양환경과 인근 해역국가에게 얼마나 많은 피해를 끼치는가를 우리는 피부로 느끼고 있다.

그러나 2006년도에 IMO에서 뜨거운 감자는 e-Navigation에 관한 것이며 국내에서도 대응책마련을 위하여 각 부처에서 많은 노력을 하고 있다.

e-Navigation이라는 말을 직접적으로 사용한 것은 2005년 11월 영국의 교통부장관 Stephen이 Royal Institute of Navigation에서 e-Navigation의 필요성을 강조한 데서 기인하지만 사실은 최근 EU에서의 대형 해사관련프로젝트와 일련의 사건을 발생순으로 나열해 보면 태동의 원인과 의도를 분석할 수 있다[1].

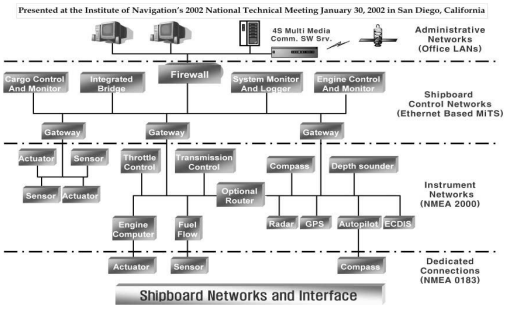

그림 1. e-Navigation 환경에서의 선박시스템의 구성

그림 1은 e-Navigation 환경에서 선박시스템을 도시한 것이며, 선박네트워크는 선박의 각종 기자재사이의 정보교환을 위한 인스트루먼트네트워크, 시스템의 제어감시를 위한 쉽 보드 제어네트워크, 4S통신과 선박관제 네트워크 등 세 종류로 구성되어 있다. IEC에서는 선박의 인스트루먼트 표준 네트워크로서 IEC 61162-3 (NMEA2000)을, 쉽 보드 제어네트워크로서는 IEC 61162-4(MiTS)를, 4S통신과 선박관제네트워크는 LAN을 선정하였다.

II. 본 론

선박은 철 구조물로 이루어진다는 특성으로 인해 선내 네트워크 구축에 있어 여러 가지 제약조건을 가지고 있다. 선내 유선 네트워크 케이블은 포설시에 Spare를 고려하여 여유 있는 케이블 포설을 원칙으로 하고 있으며, 선박내의 전원잡음을 고려하여 Shield 케이블을 사용하고, 설치류에 의한 파손방지를 위해 케이블 보호 장치를 고려하며, 네트워크 기술의 급격한 발전을 고려하여 최대 네트워크 용량을 고려하여 광케이블 또는 네트워크 케이블을 포설하고 있다.

최근 무선 LAN 기술이 발전하면서 선박에서도 무선 LAN을 적용하고 있고, ZigBee 등을 이용하여 선내 기관 상태감시 등에 활용하고자 하는 연구를 시도하고 있다. 그러나 선박은 선실과 선실사이에 철 구조물로 간혀있는 구조를 가지고 있어 일반적인 무선통신에 사용되는 전자파의 급격한 감쇄로 사용범위가 매우 제한되고 있다. 따라서 선박에서의 통신 네트워크는 기존의 유선 네트워크를 중심으로 무선 네트워크를 융합하여 사용하는 것이 이상적이라 할 수 있다.

기존의 유선 네트워크에 전력선 통신모뎀을 이용하여 유사시 백업 통신 네트워크를 구축하고, ZigBee, WLAN, UWB, RFID 등의 다양한 무선 센서 네트워크를 유선 네트워크에 융합하여 다양한 통신환경을 구축하고 선박의 모든 정보를 위성통신 혹은 이동통신 시스템을 이용하여 육상의 인터넷 환경과 연동하는 것은 매우 중요하다.

이를 위해서는 유무선 정보통신 기술을 융합하여 지능형 선박에 필요한 통신기술 모델을 제시하고, 네트워크에 구성된 기관 및 엔진, 각종 센서와 계기, 제어기 등을 자율적으로 구성 관리하고 원격감시 및 제어 운용이 가능하도록 구성하며, WLAN, ZigBee, RFID 및 PLC, Optic, Ethernet, Fieldbus 등의 다양한 유무선 네트워크 연동의 통합화 통신 플랫폼 구축하여 네트워크를 구성하는 계기/센서의 자동 구성관리 및 상호연동, 장애처리를 수행할 수 있는 시스템 개발이 필요하다. 특히, 선박의 철 구조물 환경에서 다양한 해상환경에 대하여 전자파의 주파수 전달특성에 대한 실험연구를 통해 선박 내 무선 통신기술에 대한 지속적인 기술개발이 필요하다.

2.1 선박의 네트워크 보안 시스템

■ 해상항해정보시스템(MarNIS)

유럽연합(EU)의 해상항해정보시스템(MarNIS)는 해상교통의 안전과 효율성을 지원하기 위하여, 해상정보관리, 항해통신 및 정보시스템 기술지원, 해상 위험분석 및 예방, 항만 운영의 효율성과 선박정보 및 서비스에 대하여 종합적으로 연구하였다. 특히 해상정보통신서비스를 위한 해상 통신 및 정보서비스에 대해 중점적으로 다루었으며, 향후 e-Navigation과 선원의 복지향상을 위한 해상통신 요구사양도 제시하고있다.

■ 해양전자고속도로(MEH)

혼잡한 해상교통량이 발생되는 말라카/싱가폴 해협의 해양전자고속도로(MEH, Marine Electronic Highway) 구축 사업이 해협 연안국 및 이용국과 국제해사기구, 국제환경기금, 국제수로기구, 국제유조선선주협회, 세계은행 등에 의해 추진되고 있다. MEH는 전자해도출력장치(ECDIS)를 중심으로 해상교통관제(VTS), 선박모니터링시스템(VMS), 전자해도(ENC), 자동선박식별시스템(AIS) 및 해상기상정보시스템 등을 통합·운영하는 육상의 해양안전종합관제시스템을 구축하고, 궁극적으로 실시간 체계적이고 종합적으로 선박의 안전항행을 유도함으로써, 해양사고를 방지하고, 해상에서의 인명과 재산, 그리고 해양환경 보호 체계를 구추하기 위한 사업니다.

■해상도메인 인식(MDA)

선박, 항공기, 화물, 선원 등을 실시간 감시하고, 가능한 한 육상으로부터 먼 곳에 있는 위협을 조기에 확인하기 위한 해상 도메인 인식에 도달하기 위한 감시 센서 및 플랫폼으로써, 레이더, 카메라, 부이, 해상 플랫폼, 항공기 등의 해안감시 시스템과 단거리 자동선박식별시스템(AIS), 장거리AIS, 장거리 선박위치추적(LRIT) 등을 이용한다.

■해양안전종합정보시스템(GICOMS)

우리나라의 경우에는 해양수산부 주관으로 해양안전종합정보시스템(GICOMS) 사업을 추진하고 있다. 해양안전종합정보시스템은 정보기술(IT)을 활용하여 범국가적 해양재난안전관리 체제를 마련하고, 선박모니터링을 통한 소형선박 및 어선의 조난체계 개선으로 인명피해를 최소화할 뿐만 아니라, 해적, 테러우범 해역내 국내 수출입화물의 안전한 수송로 확보를 목적으로 추진하고 있다.

■ 지능형 수로 시스템(IWS)

미국해안경비대(USCG)의 지능형 수로시스템(IWS, Intelligent Waterway System)과 수로정보네트워크(WIN, Waterway Information Network)를 들 수 있다. IWS는 선박 운항에 안전성을 보장하고 정부기관 및 업체 간의 정보공유를 형성하기 위한 전자정보 네트워크라 할 수 있다. IWS는 선박의 충돌 회피, 선박 교통흐름 관제, 선박 모니터링을 담당하는 AIS(Automatic Identificatio -n System), 항행통보와 해도, 그리고 항행에 필요한 정보의 전송에 관련된 MIDEP(Marine Information Data Exchange Program), 항해사에게 실시간의 종합정보 제공을 목적으로 하는 AN-SAR(Advanced Navigation System - Augmented Reality), 그리고 위의 사항을 거미줄처럼 연계시키는 WIN으로 구성되어 있다[2].

2.2 선박의 네트워크에 대한 공격

■ 라우팅 공격

센서네트워크 환경에선 노드의 ID를 위장하거나 가짜 라우팅 정보를 제공하고, 라우팅 프로토콜을 조작함으로서 쉽게 공격 받을 수 있다. 공격용 노드는 다수 노드의 ID를 가장하여 무선 통신 대역을 많이 확보하게 된다. 이 경우, 타노드는 공격용 노드로 라우팅을 시도하게 되어 정상적인 네트워킹이 불가능하게 된다. 또한, 공격용 노드는 라우팅 프로토콜의 헛점을 악용하여, 가짜 acknowledge 응답을 주위 노드에 보낼 수도 있다. 또한, RF 신호 강도와 같은 라우팅 정보를 조작하여 보냄으로서 주위 노드들이 공격용 노드에 접속을 선호하도록 가장할 수 있다. 즉, 가짜 라우팅 비용 정보를 제공하여 정상적인 네트워킹을 막는 방법이다.

■ 도청

무선 통신 정보는 브로드캐스팅 되기 때문에, 이러한 도청은 더욱 손쉽게 가능하다. 도청을 방지하기 위해서는 전술한 것처럼 센서노드간에 통신되는 데이터에 대하여 암호화를 통해 기밀성이 보장되어야 한다. 이를 위해 IEEE 802.15.4표준 규격에선 AES 암호를 사용하여 기밀성을 보장하도록 하고 있다. 하지만, AES와 같은 암호 알고리즘을 사용하기 위해선 키 분배 문제가 발생하는데, 이에 대해선 표준 규격 등에서 구체적으로 제안하는 기술이 없다.

■ 데이터 위변조

센서네트워크를 구성하는 노드에 대한 인증 기능이 없는 경우, 공격용 노드가 쉽게 네트워킹에 참여할 수 있게 된다. 이 경우, 공격용 노드는 도청으로부터 수집한 패킷 정보, ID 정보를 활용하여 정보에 대한 위변조 공격을 할 수 있다.

■ 물리적 공격

센서네트워크는 옥외에 설치되어 외부 환경 정보를 센싱하여 이를 처리하는 목적으로 많이 사용되기 때문에, 쉽게 외부의 물리적인 공격에 노출되기 쉽다. 센서네트워크에 대한 물리적인 공격으로는 물리적인 손상이나 절취 등이 가능하다. 이러한 경우에는 전류 센서 등을 사용해서 절취 등을 발견하여 대응할 필요가 있다. 소비전력이나 방사되는 전자파 정보와 같은 부채널 정보(sidechannel information)를 사용하여 키 값과 같은 주요 정보를 알아내는 방법이 있다. 이 기법으로는 SPA(simple power analysis attack)와 DPA(differential power analysis attack), EM(electromagnetic attack) 공격 등이 있다. 또 SPI 버스나 JTAG 포트, EEPROM에 대한 공격으로 주요 데이터나 시스템 프로그램, 하드웨어 설계 데이터에 대한 공격 및 역공학적 공격 기법이 있다[3].

2.3 Green IT를 적용한 선박 네트워크 보안 시스템

선박의 네트워크 시스템은 독립된 시스템이기 때문에 불법 침입으로 인한 기기 오작동 등의 치명적인 취약점이 존재한다. 선박 네트워크 시스템의 안정적인 Green IT를 구현하기 위해서는 선박 내에서 운영되는 유/무선 통신기기들의 보안이 필요하다. 이를 위해서는 그림 2와 같이 각 통신기기들의 기기인증을 통한 신뢰성 있는 접근체제를 갖추어야 한다.

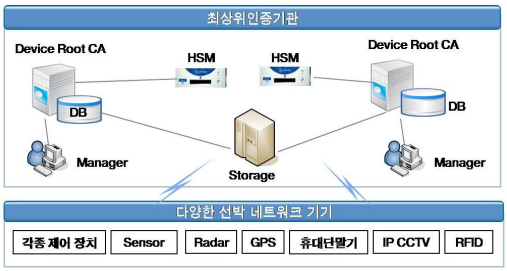

그림 2. 선박 네트워크 기기인증 개념도

각종 기기, RFID, Sensor 등은 접근권한 확인 및 수집정보 암호화를 수행하고, 휴대단말기는 기기인증서로 인가된 기기만 운영가능하게 하고 통신정보 위/변조 확인 및 암호화를 수행한다. IP CCTV는 영상정보서버 접근권한 확인, 영상정보 위/변조 확인 및 암호화를 수행한다.

공인인증기관 기기인증 관련 시스템, 선박의 다양한 네트워크 기기 등에 탑재되는 기기 인증서 처리 S/W, 기기인증서 주입 S/W 등의 구현을 위해 기기 식별번호(MAC, Serial 등)의 유일성 확인 기능을 갖춘 기기인증서생성 및 발급시스템

을 구축하고, 기술규격에 따른 기기인증서 검증이 가능한 기기인증서 처리 S/W를 개발한다.

표 1은 기기에 탑재된 기기인증서 이용 및 관리를 위해 해당 기기에 탑재되는 기기인증서 처리 S/W의 안전 및 신뢰성 검증을 위한 기기인증서 처리 S/W의 구현적합성 검증 범위이다.

표 1. 기기인증서 처리 S/W의 구현적합성 검증 범위

대상	주요내용
암호 알고리즘	· 공개키 암호 알고리즘(RSA, ECDSA 등) 처리 기능 · 해쉬 암호 알고리즘(SHA-1, SHA-2 등) 처리 기능 · 대칭키 암호 알고리즘(SEED 등) 처리 기능 등
기기인증서 관리	· 기기인증서 및 비밀키 저장 형식 · 전자서명 생성에 이용되는 비밀키 보호 기술 · 기기인증서 및 비밀키 전달 형식 · 기기인증서 갱신·폐지 기능 등
기기인증서 이용	· 기기인증서를 이용한 전자서명 생성 · 기기인증서 기반 암호화 통신 기능
기기인증서 검증	· 기기의 기기인증서 검증을 위한 인증서 체인 획득 기능 · 기기의 기기인증서 상태확인 기능 · 기기의 기기인증서 경로검증 기능

2.4 Green IT 적용에 따른 효과 분석

선박 네트워크 시스템의 보안체계 강화로 인한 암호기술 적용은 고비용의 많은 수학적 연산을 요구하기 때문에 전력 소비량이 높다. 사용기기의 저사양 CPU 및 메모리, 건전지를 통한 전력공급 방식의 제한이 기반이 되어야 하는데 이를 위해 저전력, 초경량의 암호기술이 필요하다[4].

2.4.1 기존 암호기술의 경량화

저전력, 초경량 암호기술을 적용할 경우 전력은 5~15%가 줄어들고 논리회로 갯수도 40% 밖에 들지 않는다. RFID/USN에 경량 암호기술을 적용하면 연간 1만 2211톤의 탄소 배출을 줄일 수 있다.

표 2. 암호기술의 경량화를 적용한 수치

알고리즘	공개키 알고리즘(RSA)			
	기존		경량화	
	서명	검증	서명	검증
소비전력(㎼h)	151.8	4.44	84.45	3.30
알고리즘	관용암호 알고리즘(AES)		해쉬 알고리즘 (SHA-1)	
	기존	경량화	기존	경량화
소비전력(㎼h)	0.336	0.018	0.211	0.104

2006년 기준 산업에 공급된 태그는 37억개이며 이중 암호 기술이 들어간 태그는 약 80%인 30억개에 이를 것으로 보고 계산한 수치다.

표 2는 기존 암호기술의 경량화를 통한 알고리즘 별 소비전력 수치를 나타낸 표이다.

2.4.3 기기 인증 서비스 경량 암호 기술 적용

표 3은 기기 인증 서비스 경량 암호 기술 적용시 전력 절감 효과를 암호기술 활용율과 우리나라의 보유선박 수를 감안하여 나타냈다.

표 3. 기기 인증 서비스 경향 암호 기술 적용시 전력 절감 효과

경량 암호 기술 적용시 전력 절감 효과	
연간 절감 전력	5,636㎼h x 3회(시간당) x 24H x 30D x 12M x 800(보유선박) x 1,000(선박당 인증 대상 기기) = 116,868kW
암호기술 활용율 · 서명/검증 각 1회(RSA) x 8회 · 서명시 메시지 해쉬 2회(SHA-1) x 8회 · 개인키 복호화(AES) x 8회 · 메시지 암/복호화 1000회(AES)	

III. 결 론

유비쿼터스 사회의 가속화로 인해 네트워크로 연결되는 기기들이 기하급수적으로 늘어나고 있다. 이러한 다양한 기기들이 정보제공 주체로 등장함에 따라 해당 기기에 대한 정보보호 수준의 강화가 요구되고 있다. 선박에서 사용되는 다양한 네트워크 기기들의 안정성 확보를 위한 최상위 인증기관을 구축하여 불법 침입과 유해 활동을 방지하고 선박의 중요기기 오작동 등의 위협으로부터 선박 네트워크 시스템을 안전하게 보호하여야 한다. 또한 저전력, 초경량 암호 기술을 개발하여 강력한 인증 보안체계에 따른 암호 기술의 전력소비율을 최소화함으로써 차세대 성장동력인 녹색성장 Green IT의 초석이 될 것이다.

참고문헌

[1] 서기열, 오세웅, 조득재, 박상현, 서상현, “E-Navigation을 위한 항만 정보네트워크 구현방안”, 한국해양정보통신학회논문지, 10권 11호, p.1927, 2006년

[2] 서기열, 서상현, “차세대 해상항법체계(e-Navigation)의 구현 방향”, 대한전자공학회지, 34권 11호, p.37-45, 2007년 11월

[3] 김호원, 이석준, 오경희, “센서네트워크 보안 시굴 개발 동향”, 한국정보보호학회지, 18권 2호, p.33-39, 2008년 4월

[4] 문보경, “녹색성장, 그린 시큐리티, 저전력·초경량 암호프로그램 이용을“, 전자신문, 2009년 4월