한국항해항만학회지 제36권 제1호(Vol. 36, No. 1), pp. 1~7, 2012 (ISSN-1598-5725/eISSN-2093-8470)
Journal of Navigation and Port Research
DOI : http://dx.doi.org/10.5394/KINPR.2012.36.1.1

안전한 e-Navigation을 위한 해상교통관제 시스템의 정보교환 보안구조 설계

이병길* · 한종욱* · 조현숙* · †박남제

* 한국전자통신연구원, †제주대학교

A Security Architecture of the inter-VTS System for shore side collaboration of e-Navigation

Byung-Gil Lee, Jong-Wook Han*, Hyun Suk Cho*, † Namje Park*

* *Electronics and Telecommunications Research Institute, Daejeon, Korea*
†*Department of Computer Education, Teachers College, Jeju National University, Jeju, Korea*

요 약 : 해양 분야에서 "e-Navigation"의 개념이 2005년 처음 소개된 이후, 최근 2~3년 전부터 국제해사기구(IMO)와 항로표지협회(IALA)에서 이행전략과 기술 표준화가 급속히 추진되고 있다. 특히 해상교통관제시스템(VTS : Vessel Traffic Service)은 항행지원정보교류가 가능한 육상국으로서 선박 통항의 안전과 효율성을 증진시키고 환경을 보호하는 e-Navigation의 핵심적 시스템으로 인식되고 있다. 최근 IALA VTS Committee에서는 출항에서 도착항까지 항행지원을 위하여 VTS 시스템간 정보 교류(IVEF:Inter-VTS Data Exchange Format)에 대한 요청으로 표준화가 진행되고 있다. 그러나 이러한 해상의 실시간 선박 교통흐름 정보는 국가적으로도 보안에 민감한 정보로서, 테러 등 역기능에 대한 우려가 있어, 안전한 정보교환은 필수적인 요소이다. 따라서 본 논문에서는 상호연동을 위한 보안 프로토콜을 설계하고 안전한 데이터 전송을 위한 보안 구조를 제시하고자 한다.

핵심용어 : VTS, e-Navigation, IVEF, Inter-VTS, Domain Security

Abstract : *A concept of the "e-Navigation" was introduced in 2005 and implementation strategies are under way by IMO/IALA in the maritime safety area. Specially VTS is an important maritime traffic monitoring and aids to navigation system which is aims to improve safety, navigation efficiency and protect the marine environment. The demand of the inter-VTS networking has been increased and standardization is underway for realization of shore side collaboration for maritime safety in IALA. But there may be security problems in the inter-VTS networks if they have not proper security mechanism. The hacking of realtime ship position and sensitive maritime surveillance information caused a critical accident of vessel, human life and environment by terrorist. This paper aims to design of a secure inter-VTS network structure and related security protocol for secure sharing of sensitive maritime data.*

Key words : *VTS, e-Navigation, IVEF, Traffic Monitoring, Inter-domain Security*

1. 서 론

해상분야에서는 2005년부터 "e-Navigation"의 개념이 도입되었고, IALA(International Association of Lighthouse Authorities)를 중심으로 최신정보기술의 접목을 통한 e-Navigation 표준화 및 이행전략이 적극적으로 추진되고 있다(IALA, 2010a;IALA, 2010b). IMO에서 추진중인 e-Navigation은 선박운항에 있어서 전자적 방법 또는 지능화된 차세대 기술에 의해 선박간 및 선박과 육상간 해상정보의 조화로운 수집, 통합, 교환, 표현 및 분석을 제공하여 해상에서의 안전과 보안, 그리고 해양환경보호를 극대화하는 것을 목적으로 한다.

해상의 교통관제센터의 수집된 실시간 트래픽 정보는 센터간 연동을 통하여 특정선박의 실시간 정보를 필요로 하는 선주, 기관 등으로 전달되어 출항부터 도착항까지 실시간 안전을 확인할 수 있다.

즉, IALA에서는 해상교통관제시스템(VTS) 시스템간 해상교통 정보의 실시간 정보교환에 대한 표준화가 진행중이며, IVEF(Inter VTS Data Exchange Format) 표준은 다음과 같은 주요정보의 교환을 목적으로 한다.

- Real-time Tracking positions
- Static Vessel Information

* 연회원, bglee@etri.re.kr 042)860-1689
연회원, hanjw@etri.re.kr 042)860-4940
연회원, hscho@etri.re.kr 042)860-1900
† 교신저자 : 연회원, namjepark@jejunu.ac.kr 064)754-4914

- Voyage related Information

그러나, 현재의 IVEF 및 VTS간 연동 프로토콜은 보안에 대한 절차나 메시지 그리고 정책 등은 구현사항으로서 표준으로 정의되고 있지 않은 상태이다(IALA, 2010c). 즉, 이것은 최소한의 네트워크 안전성을 보장하기 위한 명시적 수준의 전송 보안, 데이터 무결성에 대한 기준에 대해서도 내용이 없으며, 상호간의 안전한 정보교환이 이루어지기 위하여 어떠한 수준의 보안성이 지켜져야 하는지에 대한 표준이나 요구사항이 없는 상태이다. 이는 국가간 정보교환을 위해서는 민감한 정보의 전달이 될 수 있어, 상호 다른 개별적인 모든 경우를 고려하여야 하므로 상당히 복잡한 보안 구조가 될 수도 있다(B.Garnier, 2010).

따라서 본 논문에서는 VTS 운용자들이 표준 IVEF로서 상호 연결을 원할 때, 보안 정책 및 보안 요구 메시지를 보내고 상호 속성에 따라 자동 연결이 가능한 보안 구조를 제시하고자 한다.

본 논문은 2장에서는 VTS 시스템 개요, IVEF의 의미 및 상호 연동 구조에 대하여 기술하고, 3장에서는 보안 요구사항, 보안메시지 구조 및 보안 구조 설계에 대한 모델을 설명하며, 4장에서 보안의 중요성에 대하여 언급하고, 5장에서 결론을 맺는다.

2. 본 론

2.1 VTS 시스템의 개요

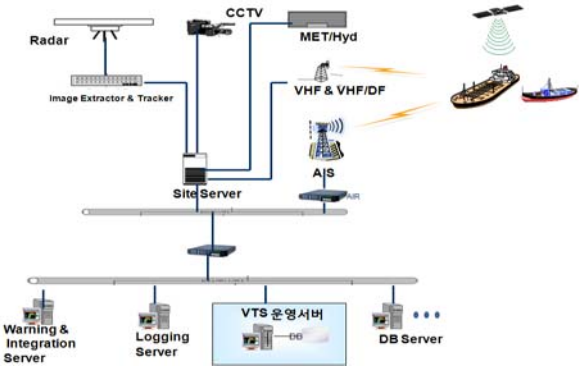

Fig. 1 System Architecture of VTS

일반적으로 VTS 시스템을 구성하는 요소는 다음 Fig. 1과 같으며, VTS센터에는 관제사의 운용시스템과 로그 및 각종 DB 서버 그리고 위험경고 및 센서융합시스템이 존재한다. 원격지에는 다양한 센서(CCTV, Radar, DF, MET 등)와 이로부터 물표의 위치 등의 정보를 수집/처리하는 시스템과 AIS기지국으로 구성된다. 레이더영상 추출 및 추적기는 핵심적 장비로 원격사이트 장비에 포함되어 개발되기도 한다. 일반적으로 원격 시스템이 관제센터로 실시간 정보전달이 되고, 관제사의 관제정보는 AIS, VHF 등의 통신망을 이용하여 선박으로 전달된다.

유럽에서는 FP(Framework Programme)프로젝트를 통하여 VTS, VTMIS(Vessel Traffic Management & Information System), PCS(Port Control Management Service)의 이름으로 차세대 해상교통관제관련 기술을 포함한 e-Navigation 연구를 추진하였다. 유럽에서 수행한 MarNIS 프로젝트에서는 선박의 동적·정적 정보와 해역의 기상, 지형, 환경 등 다양한 정보를 여러 가지 매체를 통하여 수집, 안전하고 효율적인 정보처리를 통해 항행지원과 SAR(Search and Rescue) 서비스를 제공하는 것을 목적으로 하고 있다(IALA, 2010b). 특히 멀티미디어 해상 통신을 위하여 해상 광해역 통신망기술에 대한 연구를 진행하였으며, 실제적인 서비스 실현 및 국제적 표준화를 주도하기 위하여 지속적인 후속 연구개발이 추진되고 있다.

2.2 VTS간 상호 연동을 위한 필요성

IALA의 VTS Committee에서는 모든 운항 가능한 수역에서의 안전, 보안과 해운의 효율성, 그리고 해양환경보호를 증진하는 수단과 서비스의 프레임워크로 정의하고 있고 이를 MARCH(Maritime Transport Collaboration and Harmonization)로 명명하고 있다. 이러한 서비스 구조는 해상교통감시 및 관제에서 한 단계 더 나아가 비즈니스서비스 뿐만 아니라 해양 컴퓨팅 환경에서 e-Navigation의 개념이 적용되어 새로운 서비스 형태로 진화되고 있는 것을 의미한다(IALA, 2010b).

해상의 다양한 정보 수집과 처리에 대한 기술이 급속히 발전하고, 해상의 상황인지, 위해도 기반 항행지원 등 운항중인 선박이 필요한 정보서비스를 실시간 제공하도록 하는 것을 목적으로 하는 것이다. 이때, 해상의 정보 수집/처리/생성/공유/제공 서비스를 위하여 선박으로부터 정보를 수집하거나 육지 시스템 (shore-based network)간 정보 교환이 신뢰성 있게 제공되어야 할 것이다.(IALA, 2010c).

IVEF 서비스는 IALA-AISM의 e-navigation 워킹그룹에서 현재 개발중인 육상시스템(shore-based network)간 구조에서 게이트웨이(Gateway) 서비스에 해당된다(IALA, 2010c). 즉, IVEF 서비스를 요청하는 클라이언트가 다른 외부 3자의 시스템으로서 VTS와 연동하는 구조를 가질 수도 있으므로 상호 신뢰성을 갖는 네트워크의 게이트웨이 보안서비스를 수행하여야 한다.

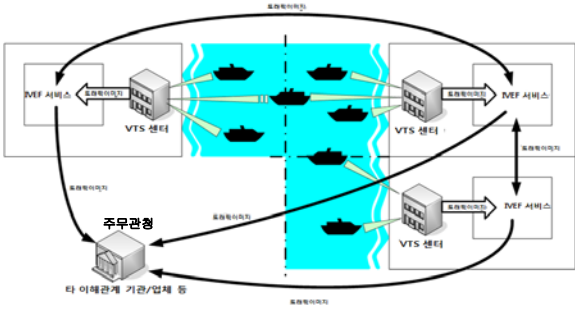

Fig. 2 VTS and IVEF Service 구조

Fig. 2는 VTS 센터가 이웃 관제센터, 관제지역내 관리기관 또는 관계되는 다른 사용자 및 기관과의 IVEF 정보를 교환하는 구조를 나타내고 있다. 그림에서 보듯이 트래픽 정보는 IVEF 서비스를 통하여 인접 시스템에 필요한 정보를 제공한다.

Fig. 2에서 보듯이, 기본적으로 IVEF 서비스는 도메인간 상호 연동할 수 있는 구조로서 서비스가 정의되어야 한다. 또한, 실제 서비스 환경을 고려한 IVEF서비스를 위하여 육상국 시스템(Shore based system)인 지역 VTS간, 국가 VTS간, 이해관계 기관 또는 업체와 안전한 구조로 상호 연동될 수 있어야 한다.

3. 서비스 구조 및 보안 구조

3.1 VTS 도메인간 연동 서비스 구조

여기서의 도메인간 연동 서비스(게이트웨이서비스)는 지역적 혹은 글로벌하게 연결되는 구조이므로 실제 환경에서는 Fig. 3과 같은 구조를 가질 수 있다.

Fig. 3 VTS의 도메인 서비스 구조

Fig. 3의 구조는 항만 VTS(항구 입출항 관제), 연안 VTS(연안 구역 관제), National VTS(해외 이동 선박에 대한 관제), 그리고 도메인 본부(HQ:Headquarter)VTS(국가단위 등 큰 범위에서의 정책관리와 게이트웨이 역할을 하는 VTS)라 할 수 있는 도메인내의 모든 VTS를 총괄하는 VTS 도메인 본부 센터가 존재할 수 있다. VTS 도메인 본부센터는 다른 도메인과 정책 및 권한을 관리하고 상호 연결을 관리할 수 있으며, VTS 도메인 본부 센터에 의해 상호 계층적 구조로서 다른 부처소속 기관하의 센터일지라도 관제권을 서로 이양함으로서 관제에 대한 역할이 자연스럽게 분리되는 구조가 된다.

3.2 상호 연동 도메인간 보안 요구사항

도메인간 연동하는 구조에서 권한에 따른 상호 데이터 제공, 공유 및 안전한 연동서비스를 위하여 서비스 측면을 고려한 보안 요구사항은 다음과 같이 정의할 수 있다. 이에 대한 근거로서는 먼저 IALA의 V-145에서 보안요구사항의 정의는 없지만 “안전한 연결”이라는 표현과, “접근권한”이라는 언급을 참고로 하고, 해당서비스영역에서 보안위협을 분석하였다. 즉, 불법 접근, 서비스방해공격, 메시지위변조, Replay공격, 서비스거부 공격 등의 침해가 가능하다. 이러한 보안위협환경에서, 인증된 도메인간에 안전하게 가용한 정보만을 송수신하도록 지원할 수 있는 보안요소 분석하고 권한에 대한 책임성을 부여할 수 있는 보안기술과 사업측면을 검토하여 정의하였다. 추가적으로 국가적 핵심시설인 경우, 사이버 보안 요구사항 외에 물리적 보안요구사항이 요구되며, 해상교통관제 시스템의 경우에도 해당된다고 본다.

- **인증(Authentication)** : 서비스의 이용할 대상에 대한 검증이며, 서비스 이용자와 공급자 모두에게 관계됨. 또한 도메인간 연결을 위한 시스템간(M2M:Machine to Machine) 그리고 이러한 IVEF 서비스를 제공 받으려는 사용자도 해당됨

- **인가(Authorization)** : 서비스에 대한 권한 검증임. 서비스 클라이언트에게만 관계됨. 도메인간 연결을 위한 시스템간 그리고 이러한 IVEF서비스를 제공 받으려는 사용자도 해당됨

- **데이터보호(Data protection)** : IVEF 클라이언트와 송수신되는 데이터의 안전성으로서 무결성, 기밀성이 해당됨. 실제교환 되는 시스템간 또는 사용자와 시스템간 데이터 모두 관계됨

- **서비스에 대한 Business보안** : 서비스제공자인 VTS 센터의 IVEF 관리자와 이용자간의 사업 측면보안이며, 서비스를 요구하는 이용자 또는 사업자와의 협상과 제공자의 요금 등 사업정책에 따라 정해짐

- **물리적보안(Physical security)** : IVEF 클라이언트와 서버 시스템이 존재하는 장소, 상호 연결된 관제센터장소 및 네트워크에 접근할 수 있는 장소에 대한 물리적 접근통제에 대한 보안이며, 스카다 등 안전성에 대한 잠재위협이 큼

3.3 도메인간 IVEF 보안 메시지 정의

본 절에서는 도메인간 IVEF 서비스를 요구하고 서비스를 제공하기 위하여 보안 절차를 추가하고 절차에 필요한 메시지를 정의하고자 한다. 이는 IVEF 서비스를 요청하고 이를 확인

하여 상호 보안 정책에 따라 상호 보안 설정을 하는 과정에 해당된다.

Fig. 4와 같이 기본적으로 VTS 센터의 IVEF 관리자와 안전한 세션 연결을 만들고, 초기 설정 절차시에 상호 검증될 수 있는 공개키 기반으로 보안절차를 추가하도록 한다.

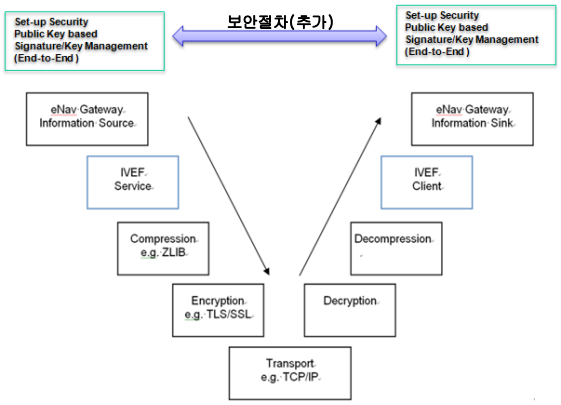

Fig. 4 IVEF의 세션 연결 절차

Table 1 IVEF message definition with security

메시지	From	To	설명
제어정보 메시지			
IVEF Security Service Request	Both	Both	IVEF 보안서비스요청
IVEF Security Attribute Request/Response	Both	Both	IVEF 보안속성 서비스요청/응답
IVEF Security Service Confirm	Both	Both	IVEF 보안 서비스 응답에 대한 검증결과
Login	User	Server	IVEF 사용자 식별
Login Response	Server	User	로긴 응답
Logout	User	Server	서비스 로그아웃
Ping	Both	Both	Heartbeat 메시지
Pong	Both	Both	Heartbeat메시지의 응답
Service Request	User	Server	새로운 서비스를 포함한 서비스요청
Service Request Response	Server	User	서비스요청의 응답
Server Status	Server	User	자동적으로 응답가능한 서버의 상태메시지
실시간 위치 데이터 메시지			
Vessel Data Track based	Server	User	위치에 관점을 둔 선박의 위치 및 항해궤적 정보
Vessel Data Plan based	Server	User	항로계획에 관점을 둔 선박의 위치 및 운항궤적 정보

또한 VTS센터는 IVEF 관리자를 통하여, 정보를 수신할 관심지역, 갱신주기, 통항하는 특정대상 등과 같은 각기 다른 종류의 데이터 보안 요구사항을 정의 할 수 있는 구조가 되어야 한다(IETF, 2008; 이 등 2010; 장 등 2007). 이러한 요구사항을 정의하기 위하여는 보안 속성을 상호 정의하고 확인할 수 있어야 한다. 본 논문에서 추가 정의된 보안 메시지는 Table 1과 같다.

Table 1에서 보안 메시지의 보안 서비스요청 메시지(IVEF Security Service Request)를 통하여 VTS센터의 IVEF 관리자는 서명된 보안 서비스를 요청한다. 이때 상대 서버는 해당 메시지를 검증하고, 보안에 대한 정책을 요청(IVEF Security Attribute Request)하거나 응답(IVEF Security Attribute Response)하게 된다. 보안서비스를 요청한 VTS센터에서 요구하는 보안성이 최종 확인되는 경우, 확인하는 메시지(IVEF Security Service Confirm)를 보냄으로써 보안 서비스가 시작된다. 여기에서 정의된 상대에 대한 인증 및 정보의 우선순위 그리고 접근 권한에 맞는 통항 교통 이미지 데이터 서비스를 제공하기 위하여, 보안 서비스 요청 메시지에 검증될 수 있는 보안 정책과 보안속성이 포함되어 있어야 한다.

또한 보안 서비스 요구를 클라이언트에서 요구할 수도 있지만, 트래픽 데이터의 제공자인 VTS센터에서 요구하는 경우가 일반적일 것이다. 보안 서비스에서 인증, 권한검증이 확인된 후에 상대에게 확인 응답을 하게 되는 구조로 설계됨으로써 안전한 상호연관(Association)이 만들어 질 수 있다(Arifin B 등 2011; Frejlichowski D 등 2008).

IVEF서비스는 클라이언트에게 제공되는 데이터에 관한 권한설정을 통하여 개별적인 정보의 제한을 두도록 설계되어야 한다. 이러한 제한을 둘 수 있는 보안 서비스 처리 흐름도에 대한 제시는 다음 Fig. 5와 같이 정의할 수 있으며, 상호 제한은 데이터를 제공하는 자의 정책에 의해 정의된다.

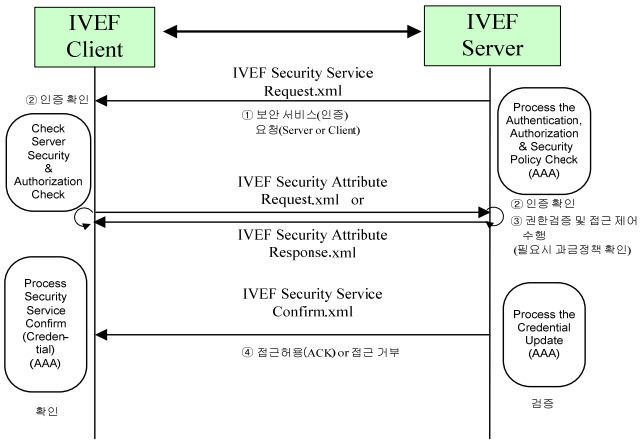

Fig. 5 IVEF의 보안 메시지 처리 절차

Fig. 5와 같이 보안 서비스 Basic IVEF 서비스의 보안 모델은 단지 인증과 권한검증(인가)의 항목만으로 정의 될 수 있지만, 이는 Business모델과 연계될 수 있어야 한다.

여기에서 도메인간 정보 교환은 사업적인 측면에서 과금정책에 대한 교류도 속성정보를 이용하여 정의될 수 있으며, 추가적으로 사업적 정책요소 또한 상호 정의 될 수 있다.

그리고, 안전한 보안 서비스를 제공하기 위해서는 데이터 보호와 신뢰관계를 정립하는 공개키 기반의 기본 인프라가 요구되며, 비밀키의 전송과정에 대해서는 기본 보안인프라의 키 전달메커니즘을 통하여, 안전한 채널프로토콜을 정의하고 이를 상호 제공함으로서 수행될 수 있다.

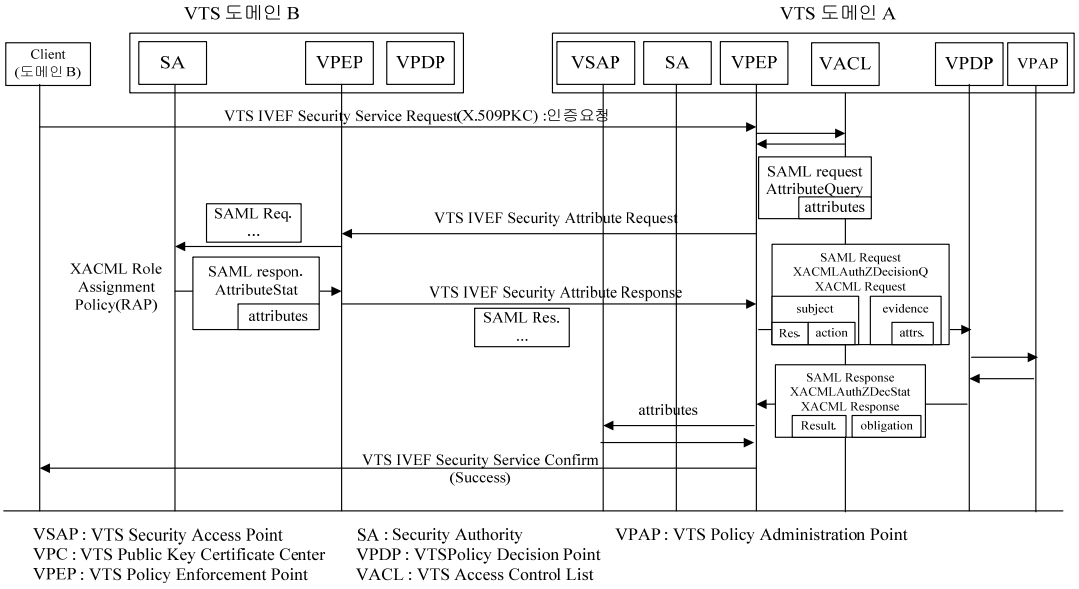

Fig. 6 도메인간 XML 기반 IVEF 보안 처리 흐름도

3.4 도메인 보안요소 정의 및 처리 흐름도

본 절에서는 정의된 보안 메시지를 이용하여 도메인간 상호 보안요소를 정의하고 구체적인 절차를 정의한다. 즉, Fig. 6에서는 VTS 도메인 B에서 VTS 도메인 A로 접근하여 보안 메시지를 이용하여 연동하는 부분에 대한 보안 처리 흐름도를 나타낸다. 기본적인 보안 구조는 XML기반 기 표준 프로토콜을 사용하며, IVEF를 위한 속성은 IVEF 보안메세지의 속성 교환 프로토콜을 사용하여 확장된다.

도메인간에 연동시 한 도메인내에서의 정책의 처리를 위한 절차 및 권한에 따른 접근처리 절차는 Fig. 7과 같다.

도메인간 IVEF 서비스를 요청하여, 접근제어 기반의 권한 관리 기능으로 ID/Password 기반한 VTS IVEF 서비스 기본 인증 메커니즘은 다음과 같다. M2M 경우 사용자는 시스템이 된다.

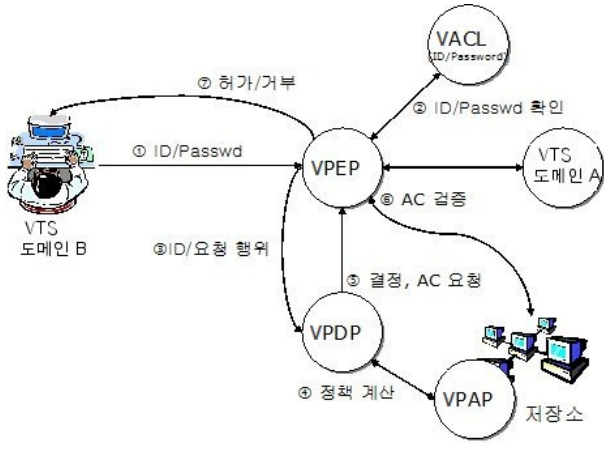

Fig. 7 접근제어기능을 이용한 VTS 도메인간 기본 권한관리 인증 메커니즘 절차

1) 사용자는 시스템 자원 또는 응용 서비스를 이용하기 위해서 접근요청을 보낸다. 이 때, 접근요청은 기존 방법과 동일하게 사용자 ID와 패스워드로 구성된다.

2) 접근제어 모듈의 VPEP는 접근요청을 수신한 후, 사용자의 ID 와 패스워드를 접근제어목록에서 확인한다. 여기까지의 과정은 기존 방법과 동일하다.

3) 사용자의 ID와 패스워드를 확인한 VPEP (VTS Policy Enforcement Point)는 사용자의 신원정보(ID)와 사용자가 요청한 행위(읽기, 쓰기, 실행)을 VPDP (VTS Policy Decision Point)에게 전송한다.

4) VPDP는 VPAP(Policy administration point)로부터 정책을 로드하여 사용자가 요청한 행위에 대해서 적절한 권한을 소지하고 있는 사용자인지를 판단한다. 이를 위해서 사용자, 자원, 환경 속성과 정책을 이용해서 인가 여부를 결정해야 한다.

5) VPDP는 판단 결과를 VPEP에게 전달한다. 즉, 허가/거부여부를 VPEP에게 전달한다. 이 때, 결과가 '허가'인 경우는 사용자의 속성인증서를 검증하여 속성인증서가 유효한 경우 사용자의 요청을 허가하도록 한다. 추가적인 보안 속성조건이 필요한 경우, 요청하여 응답을 받아서 검증하여 허가하도록 한다.

6) VPEP는 저장소에서 사용자의 속성인증서를 다운로드 받아 유효성을 검증한다. 유효한 인증서인 경우, 사용자의 접근을 허가한다.

이와 같이 접근제어 기능을 이용한 VTS간 기본 권한관리 인증 메커니즘 절차 경우는 VTS 서비스 시스템이 복잡해지고 접근제어에 소요되는 비용이 증가하여 기존 시스템에 비해 큰 이점을 얻을 수 없지만, 접근제어 시스템의 통합이 용이하다는 장점이 있다. XACML 및 X.509 PMI(Privilege Management Infrastructure) 등의 표준 기술을 사용하기 때문에 새롭게 추가되는 시스템에서 접근제어가 필요할 경우에 접근을 판단하는 부분은 새로 구현될 필요가 없다.

즉, 새롭게 추가되는 개방형 접근제어 기능을 이용한 VTS간 기본 권한관리 인증 접근제어 시스템은 사용자와 VPEP간의 통신 부분만 추가되면 되고, 나머지는 부분은 이미 구현된 부분을 그대로 이용하면 된다. 독립적으로 운영되어야 하는 시스템이라도 접근제어 기능 부분은 재사용이 가능하기 때문에 서비스 시스템 추가 시 접근제어를 위해 소요되는 비용을 절감할 수 있다.

Fig. 8에는 VTS간 상호 연동을 위한 조건부 사용자 접근제어 메커니즘을 나타낸다.

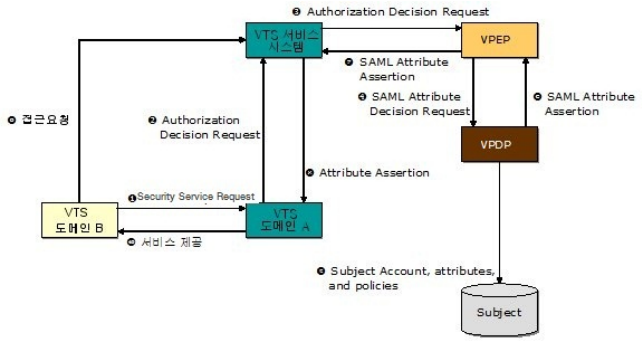

Fig. 8 VTS간 상호 연동을 위한 조건부 사용자 접근제어 메커니즘

VTS간 상호 연동을 위한 조건부 사용자 접근제어 메커니즘은 VTS 도메인 B가 내부 서비스 시스템을 통해서 시스템이 아닌 외부에서 제공하는 전체 VTS 서비스 시스템에 접근하는 경우로 다음과 같이 동작한다. VTS 도메인 B 사용자는 전체 VTS 서비스 시스템의 인증 및 권한부여 메커니즘에 의하여 자신의 계정을 개설하고 VTS 서비스 시스템에도 자신의 계정을 개설한다. 전체 VTS 서비스 시스템이 VTS 도메인 B 사용자의 접근을 허가하기 전에, VTS 서비스 시스템은 전체 서비스 관련 속성의 목록을 문의한다.

또한, VTS 서비스 시스템은 자체적으로 VPEP와 VPDP를 가지고 있을 수 있다. 이 경우, VPDP는 VTS의 서비스 속성에 대한 조건부 작업을 첨부한 권한부여 결정을 반환한다. 이 때문에 VPEP는 권한부여 결정 요청을 외부 서비스에 전송한다. VPEP로부터 권한부여 결정 요청을 접수한 VTS 서비스는 속성 토큰을 반환하며, 이는 VTS 서비스 시스템의 VPEP에서 조건부 작업을 검증하는데 사용된다. 다음은 VTS 도메인간 상호 연동을 위한 조건부 사용자 접근제어 메커니즘의 절차이다.

(1) VTS 도메인 B는 VTS 서비스 시스템의 접근을 요청한다.

(2) VTS 서비스 시스템은 서비스에 권한부여 결정 요청을 전송한다. 이는 VTS 서비스 시스템 내의 VPEP 혹은 VTS 서비스 시스템 외부의 VPEP에 의해서 수행된다.

(3) VTS 서비스 시스템의 VPEP로부터 권한부여 결정 요청을 접수한 VTS 서비스는 PEP에 권한부여 결정 요청을 전달한다.

(4) VPEP는 VPDP에게 XAML 속성 결정 요청을 전송한다.

(5) VPDP는 VTS 도메인 B의 계정, 속성과 정책을 확인하여 권한부여 허가/거부 결정을 VPDP에게 전송한다.

(6) 권한부여가 허가된 경우에 VPDP는 SAML(Security Assertion Markup Language) 속성 토큰을 PEP에게 전송 한다.

(7) VPEP는 SAML 속성 토큰을 전달한다.

(8) VTS 서비스는 VTS 서비스 시스템에게 속성 토큰을 전달한다.

(9) VTS 서비스 시스템은 VTS 도메인 B에게 VTS 도메인 A의 서비스를 제공한다.

4. 보안의 중요성 및 적용

IVEF서비스는 보통 육상국(shore-based) e-Navigation 시스템내에 포함되며, 안전한 운송 서비스를 위하여 기본적인 IVEF 연동 보안 뿐만 아니라 물리적 보안을 위한 적절한 보안 수단이 시스템에서 제공되어야 한다(Daniel Z. 등 2007).

그리고 인증과 인가를 위해 선택된 단순한 클라이언트 서버 사이에 공유기밀(예:XML기반 보안구조 및 인증서 기반의 보안 체계 등)에 기초한 별도의 보안 구조가 정의되어야 한다.

여기서 클라이언트는 서버의 인증이 요구되며, 서버 또한 클라이언트를 위한 특정 인증 방법이 제공되어야 한다. 즉, 선박이 분포된 현재 시점의 트래픽이나, 선박의 정보를 단순한 인터넷 접속을 위한 패스워드와 같은 단순한 방법을 이용할 수는 없다. 이러한 방법은 클라이언트가 요구한 서비스에 대한 권한에 대한 내용을 검증할 방법이 없으며, 클라이언트가 요청한 서비스가 보안 속성을 요구하더라도 제공할 방법이 없기 때문이다.

또한 이러한 선박의 정보가 노출되는 경우, 국가적 테러위협에 노출되기 쉽고, 선박의 나포가 이루어지는 국제선박의 통항과정에서 해적선의 표적이 되기 쉽기 때문이다(국해부 등 2010)

과거의 해상교통관제(VTS)는 좁은 의미 또는 고전적 의미로는 레이더신호 관제 범위에 의한 통항선박 감시와 선박 통항의 조정으로 해당 구역의 관제 위주가 목적이었으나, 최근 IALA에서 추진되고 있는 VTS의 방향은 특정 관제구역에 대한 제한도 없으며, 정보공유의 확대를 위한 주무관청에 대한 제한도 두지 않는 것이다. 즉, 다양한 센싱 정보로부터 항행원조(Aids to Navigation)와 적시의 함축된 정보제공으로 선박운항의 개념에 대한 확장이 되고 있음을 의미한다(Carter B. 등 2008 ; Ornulf J. 2011).

그러나 이러한 국가간의 연동시 적절한 보안 메커니즘이 제시되지 않는 경우, 해적이나 테러 집단 등의 공격 목표가 될 수 있다. 따라서 이러한 정보 연동을 위한 관제 시스템은 수집 정보를 분석하여 현재 해상상황을 인지하고 해당 상황을 관제사에게 직관적으로 빠르게 전달하여야 하기 때문에 효율적인 보안 알고리즘과 보안 구조를 필요로 한다. 따라서 본 논문에서는 이러한 보안 요구사항을 만족시키기 위한 기본적인 보안 구조를 제안하였다.

5. 결 론

최근 전세계적 추세로 보면, 해상교통관제 및 해상컴퓨팅 환경은 급속하게 발전하고 있으며, e-Navigation기반의 지능형 항행지원 형태의 서비스가 중요한 요소가 되고 있다.

본 논문에서는 차세대 VTS를 위한 상호 네트워킹 기술을 기반으로한 VTS 시스템간 연동에 대한 보안 구조를 설계하고 상호 안전한 처리구조를 제안하는데 주안점을 두었으므로 다음 단계에서의 연구는 이러한 기술의 실제적 적용에 대한 성능분석과 서비스 플랫폼에 대한 구체적인 연구결과를 제시할 수 있을 것이다.

또한 본 연구는 최근 해양 산업발전의 새로운 패러다임으로 IMO에서 제시된 e-Navigation에 대한 연구와 국제적 표준화가 활발하게 진행되고 있으므로, 새로운 보안과 관련된 표준에 대한 제시가 가능할 것으로 본다. 또한, 이러한 표준화 활동과 더불어 보안 기능이 포함되어 e-Navigation을 실현하고, 안전한 상호 연동 서비스를 제공 할 수 있을 것이라 생각된다.

최근 국내에서도 e-Navigation의 육상국으로서 해상관제 시스템이 활발하게 연구되고 있어, 이러한 연구가 최신 IT기술과의 융합을 통한 새로운 해상교통관제시스템의 변화에 큰 역할을 할 것이라 판단된다.

후 기

본 연구는 2011년 국토해양부의 해양안전 및 해양교통사업 기술개발사업의 재원으로 수행된 연구임

참 고 문 헌

[1] 국토해양부/ETRI 지식정보보안연구부(2008), “신개념 통합전자 항법 시스템(e-Navigation) 국내 대응방안 보고서”

[2] 이병길, 한종욱, 조현숙(2010), "해양안전 실현을 위한 차세대 해상교통관제 시스템의 상황인지 및 항행지원 구조 설계", 한국통신학회 논문지 35권 제7호, pp. 1073-1080

[3] 장운재, 금종수(2007), “해상교통정보시스템의 정보제공에 대한 구조분석”, 해양환경안전학회, pp. 133-139

[4] Arifin B., Ross E., Brodsky Y.(2011), "Data security in a ship detection and Identification system", IEEE RAST2011, pp. 634-636

[5] Carter B., Green S., Leeman R., Chaulk N.(2008), "SmartBay:Better Information - Better Decisions", IEEE OCEANS 2008, pp 1-7

[6] Frejlichowski D., Lisaj A.(2008), "Analysis of lossless radar images compression for navigation in marine traffic and remote transmission", IEEE Radar Conference 2008, pp. 1-4

[7] Garnier B., Andritsos F.,(2010), “A Port Waterside Security Systemic Analysis”, IEEE WSS Conference2010, pp. 1-6

[8] IALA(2010), IALA Recommendation on the e-Navigation Architecture the Shore Perspective, IALA Recommendation eNAV-101

[9] IALA(2010), Generic e-Navigation Service Engineering Model Template, (draft) IALA Recommendation eNAV-210

[10] IALA(2010), IALA Recommendation on the Inter-VTS Exchange Format(IVEF) Service(draft), September

[11] Ornulf Jan Rodseth(2011), "A Maritime ITS Architecture for e-Navigation and e-Maritime: Supporting Environment Friendly Ship Transport", IEEE ITS Conference 2011, pp. 1156-1161

[12] TTA Journal(2008), "조선-IT융합기술 e-Navigation 동향” No. 119.

[13] Zeng D, Chawathe S. Hua H, Fei-Yue W.(2007), "Protecting Transportation Infrastructure", IEEE Intelligent Transportation Systems 2007, pp 8-11

원고접수일 : 2011년 11월 1일
심사완료일 : 2012년 2월 24일
원고채택일 : 2012년 2월 24일