The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 23, No. 5, pp.21-27, Oct. 31, 2023. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2023.23.5.21
JIIBC 2023-5-4

해상환경에서 안전한 통신을 위한 보안체계 연구

Research on Security System for Safe Communication in Maritime Environment

홍승표, 이훈재, 이영실*

Seoung-Pyo Hong, Hoon-Jae Lee, Young-Sil Lee*

요 약 선박이 안전한 항해를 하기 위해 도움을 주는 수단으로서 해상환경에서 운용 중인 항로표지는 주기적인 관리가 필요하며 환경 특성상 정확한 상태를 육안으로 확인하기는 어려움이 존재한다. 이에 따라 항로 안전 및 운항 효율성을 향상시키는 스마트 항로표지 시스템은 일반적인 항로표지와 다르게 센서, 통신 및 정보 기술을 포함한 전문적인 기술을 활용한다. 선박 안전과 선박을 운항하는 항해자들의 안전을 지키는 것이 목적인 스마트 항로표지 시스템의 통신 환경은 해상환경에 맞게 무선 통신 네트워크를 사용하게 된다. 선박은 육상에서 해상환경에 필요한 정보들을 수집하며 운항을 하게 되는데 이 과정에서 무선 통신 보안 지침에 대한 부분도 고려해야할 필요가 존재한다. 기본적으로 데이터 교환을 용이하게 하기 위한 표준 IHO S-100과 안전한 통신을 할 수 있는 인터페이스를 제공하는 SECOM을 기반으로 본 논문에서는 해상환경에서 안전한 통신을 위한 보안체계를 연구하였다. 문서에 기반한 기본적인 보안 체계를 제시하였으며 해상환경의 무선 통신 특성상 데이터 교환에 대한 취약점도 다소 존재하였으며 비인가된 사용자가 서비스에 접근할 수 있는 취약점을 고려하여 사용자 인증에 대한 부분을 추가하였다.

Abstract As a means of helping ships navigate safely, navigational aids in operation in the maritime envirionment require periodic management, and due to the nature of the environment, it is difficult to visually check the exact state. As a result, the smart navigation aid system, which improves route safety and operational efficiency, utillizes expertise including sensors, communications, and information technology, unlike general route markings. The communication environment of the smart navigation aid system, which aims to ensure the safety of the navigators operating the ship and the safety of the ship, uses a wireless communication network in accordance with the marine environment. The ship collects the information necessary for the maritime environment on the land and operates. In this process, there is a need to consider the wireless communication security guideline. Basically, based on IHO S-100 a standard for facilitating data exchange and SECOM, which provides an interface for safe communication. This paper research a security system for safe communication in a maritime environment. The security system for the basic interface based on the document was presented, and there were some vulnerabillties to data exchange due to the wireless communication characteristics of the maritime environment, and the user authetication part was added considering the vulnerability that unauthorized users can access the service.

Key Words : IHO S-100, Maritime, SECOM, Security System

*정회원, 동서대학교 컴퓨터공학과
접수일자 2023년 8월 30일, 수정완료 2023년 9월 30일
게재확정일자 2023년 10월 6일

Received: 30 August, 2023 / Revised: 30 September, 2023 / Accepted: 6 October, 2023
*Corresponding Author: debiii@naver.com
Dept. of Computer Engineering, Dongseo University, Korea

Ⅰ. 서 론

우리나라에서 항로표지는 다음과 같이 정의되고 있다. 항행하는 선박에 대해서 등광, 색체, 형상, 전파, 음향 등의 수단으로 항·만·해엽 등 대한민국의 영해, 내수 및 배타적 경제수역을 항행하는 선박의 지표로서 운영되는 등대, 선박의 위치·방향 및 위험 요소의 위치를 알려주는 항행보조시설인 광파표지, 음파표지, 형상표지 및 특수신호표지 등을 포함하는 것이다[1]. 선박이 안전한 항해를 하기 위해 도움을 주는 수단으로서 해상환경에서 운용중인 항로표지는 주기적인 관리가 필요하며 환경 특성상 정확한 상태를 육안으로 확인하기는 어려움이 있었다.

이에 따라 항로 안전 및 운항 효율성을 향상시키는 스마트 항로표지 시스템은 일반적인 항로표지와 다르게 센서, 통신 및 정보 기술을 포함한 전문적인 기술을 활용한다. 스마트 항로표지 시스템은 다양한 요소로 구성되어 있는데 예를 들어, 항로 주변에는 센서 네트워크가 설치되어 항로의 조건을 모니터링하고 실시간으로 데이터를 수집한다. 이 데이터는 해양 트래픽 관제 센터나 선박에 전송되어 항로의 안정성과 효율성을 평가하고 관리할 수 있다.

또한, 스마트 항로표지는 전자식 항로표지(Electronic Navigational Aids) 시스템과 통합될 수 있는데 이는 선박 운항에 필요한 정보를 전자적으로 제공하여 항로를 안내하고 위험을 경고하는 기능을 제공한다. 전자식 항로표지 시스템은 GPS, AIS(Automatic Identification System), 라이다(Lidar) 등의 기술과 연계하여 선박의 위치와 주변 환경을 모니터링하고 정보를 제공한다.

Ⅱ. 관련 연구

1. IEC 63173-2 SECOM 모델 분석

SECOM(Secure Communication between Ship and Shore)은 국제전기기술위원회(IEC: International Electrotechnical Commission)가 제정한 육·해상 간의 통신 표준이다. IEC 63173은 무선 통신 장비 및 해상 항법 시스템에 대한 데이터 인터페이스 표준이며, 2021년 IEC 63173-1(S-100 기반 S-421 항로 계획)을 제정하였고, 2022년 IEC 63173-2(선박과 해안간 보안 통신(SECOM))을 제정하였다. SECOM은 데이터 교환(정보 서비스)을 위한 인터페이스(API), 안전한 통신을 가능하게 하는 정보 보안 조치 및 서비스 검색 가능성을 위한 인터페이스가 포함된다. 온라인상에서 안전하게 정보를 교환하는 수준까지 운영 용도와 상관없이 동일한 서비스 인터페이스를 사용하여 정보를 교환하는 기술적 상호 운

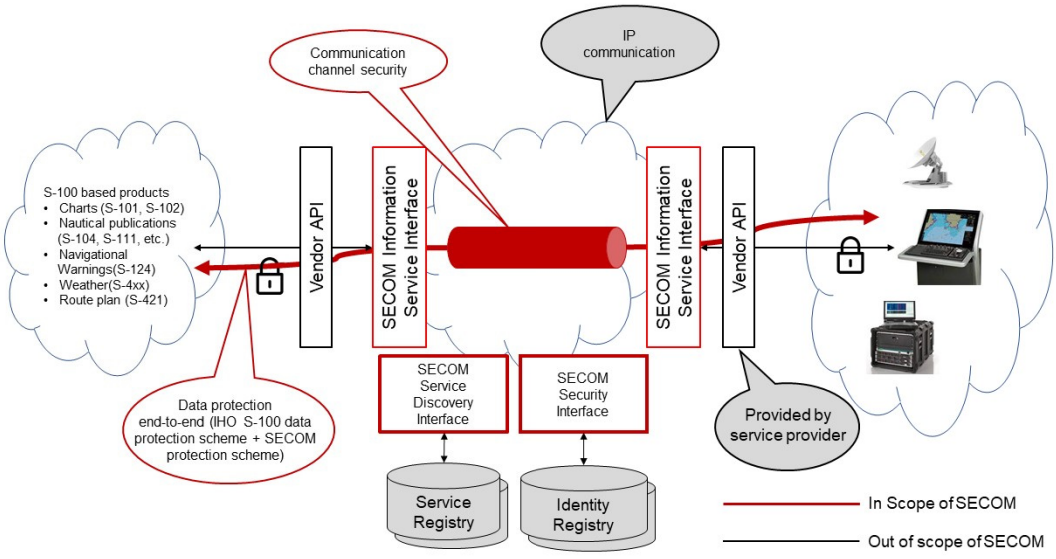

그림 1. IEC 63173-2 SECOM 개요
Fig. 1. Overview of IEC 63173-2 SECOM

용성을 제공한다. IHO S-100 기반 제품용으로 설계되었지만, SECOM은 기술적으로 페이로드에 구애받지 않으며 다른 유형의 데이터에도 적용할 수 있다. 데이터 교환을 위한 SECOM 정보 서비스 간의 통신은 IP 기반 웹 서비스에 의존하게 되며, 정보 서비스 간의 데이터 전송을 위한 물리적 계층 또는 링크 계층을 정의하지 않지만, 전송이 IP 통신을 지원하도록 요구한다. SECOM은 공공(정부) 및 민간(기업) 서비스 모두에 적용할 수 있으며 선박-육상 및 육상-선박 통신에 적용할 수 있으며 선박-선박 통신에 사용할 수 있다. 그림 1은 IEC 63173-2 SECOM의 개요이다. SECOM의 정보 보안에는 통신 채널 보안, PKI(공용 키 인프라)의 변형 및 IHO S-100을 완전히 또는 부분적으로 준수하는 정보 교환을 위한 데이터 보호 체계 대안이 포함된다[2].

2. IHO S-100 모델 분석

물리적인 해양 정보와 관련된 국제 해양 기구(International Hydrographic Organization, IHO)의 S-100(Universal Hydrographic Data Model)은 해양 공간 정보를 관리하고 교환하기 위한 표준을 정의하는 프레임워크다. S-100은 해양 정보를 다양한 형식으로 기술하고 교환하는 데 사용되는 표준화된 데이터 모델과 표현법을 포함한다. 다양한 해양 관련 조직과 기관 간에 데이터 교환을 용이하게 하고, 해양 정보를 보다 효율적으로 관리하고 활용하기 위해 개발되었다. 이러한 표준화된 데이터 모델과 표현법은 해양 산업 및 연구 분야에서 중요한 역할을 수행하며 해양 자원 보호, 해상 안전, 항해 효율성 향상 등에 기여한다. 데이터 제품 사양 목록은 각 정보의 특징에 따라 S-10x, S-20x, S-30x 등의 번호로 분류되고 있다. 표 1은 차세대 수로 표준 S-100 기반 데이터 제품 사양이다[3]. S-100 표준은 해양 정보를 관리하는데 있어서 중요한 이점을 제공하게 되는데 그 중 하나는 상호 운용성에 있다. 다양한 종류의 해양 정보를 하나의 통합된 데이터 모델로 표현한다. 이로 인해 서로 다른 해양 데이터 세트를 쉽게 통합하고 상호 운용성을 갖출 수 있다. 해양 데이터를 표준화하여 교환하면 다양한 해양 관련 조직과 기관 간의 협업과 정보 교류를 간소화하고 효율성을 높일 수 있다.

표 1. 차세대 수로 표준 S-100 기반 데이터 제품 사양
Table 1. S-100 based Data Product Specification

No.	Title
S-101	Electronic Navigational Chart(ENC)
S-102	Bathymetric Surface
S-103	Sub-Surface Navagation
S-104	Water Level Information for Surface Navigation
S-111	Surface Currents
S-121	Marine Limits and Boundaries
S-122	Marine Protected Areas
S-123	Marine Radio Services
S-124	Navigational Warnings
S-125	Marine Navigational Services
S-126	Marine Physical Environment
S-127	Marine Traffic Management
S-128	Catalogue of Nautical Products
S-129	Under Keel Clearance Management(UKCM)
S-130	Polygonal Demarcations of Global Sea Areas
S-131	Marine Harbour Infrastructure
S-164	IHO Test Data Sets for S-100 ECDIS

Ⅲ. 본 론

1. 한국형 e-Navigation

미래 해상환경의 변화와 정책 수요에 맞춰 항로표지의 스마트화를 위해 정보교환체계의 표준화, 정보의 디지털화, 정보수집의 다양화 및 정보의 통합DB 구축을 통해 해양 분야 ICT 기술개발이 필요하게 된다[4]. 기존 항로표지 고장 유무와 같은 상태정보는 선박에서 즉각 대응하기 어렵고, 사용하고 있던 전자해도는 해상환경에서 빈번하게 변경되는 항로표지 상태정보를 선박에서 실시간으로 확인하기에는 어려움이 존재하였다. 이에 대응하여 선박해양플랜트연구소(KRISO)에서는 항로표지 수집정보에 기반한 해양 정보 관리 서비스 기술을 연구중에 있다.

S.W. Oh 외 2명[5]은 항로표지 스마트화 전략의 핵심 목표인 항로표지 정보 표준에 기반한 체계 구축 등 스마트화 전략을 제시하고 있다.

항로표지 스마트화 전략에 관하여 여러 연구가 개발되고 있으며 대표적으로 한국형 e-Navigation이 있다. e-Navigation 사업은 차세대 해상항법체계로서 육상과 선박에서 통합, 수집, 교환, 표현에 대해 해상 관련 정보를 분석하는 전자 시스템이다. 해상에서의 안전을 보장하며 보안을 증진하게 되며 해상환경을 보호하는 것이 e-Navigation의 목적이다. 우리나라 해상환경에 특화되어 있는 한국형 e-Navigation은 어선, 소형선 등 대상으로 서비스를 제공하게 되며 최적화된 시스템을 구현한다[6]. 한국형 e-Navigation에는 항해 중인 선박에게 필

수적인 서비스들을 제공한다. 첫 번째, 해양안전정보 서비스다. 해상 환경은 위험 요소들이 많이 존재한다. 그런 위험 요소들을 피해 안전한 항해할 수 있게 정보를 제공하는 서비스이다. 두 번째, 대형 선박 뿐만 아니라 소형 선박용 전자해도 서비스를 제공한다. 대형 선박 같은 경우 그 목적에 따라 선원들의 연령대가 다양하다. 따라서 전자해도에 대한 업데이트 주기가 빠른편이며, 지속적으로 업데이트가 되는 전자해도를 소형 선박에서 업데이트를 하기에는 다소 어려움이 존재한다. 실제 소형 선박을 운항하는 어민들이 업데이트를 진행하는 사례는 다소 드물며 이 결과는 사고로 이어질 수 있다. 따라서 이러한 서비스를 e-Navigation에서 제공하고 있다[7].

2. 스마트 항로표지 시스템

ICT가 다양한 분야에서 접목되면서 스마트 사회로 점차 발전되어가고 있다. 해양 분야에서도 새로운 패러다임의 변화가 생겨나고 있다. 자율운항선박(MASS), 스마트 해운, 항만물류시스템 등 발전된 기술을 통해 고도화되고 있다. 해상 교통의 도움을 주는 항로표지도 단순한 항해에 도움을 주는 기능을 넘어서서 정보수집, 분석, 예측 등 강화된 모니터링 기술을 보여주고 있다. 넓은 범위에서 이러한 기술들을 활용하고 있는데, 작게는 소형 어선에서부터 넓게는 대형선박들이 이러한 스마트 항로표지 시스템을 생업에 중요하게 활용하고 있다. 해상에서의 선박 안전과 선박을 운항하는 항해자들의 안전을 지키는 것이 목적인 스마트 항로표지 시스템의 통신 환경은 해상 환경에 맞게 무선 네트워크를 사용하게 된다. 선박은 육상에서 해상환경에 필요한 정보들을 수집하며 운항을 하게 되는데 이 과정에서 무선통신 보안지침에 대한 부분도 고려해야할 필요가 존재한다. 기본적으로 데이터 교환을 용이하게 하기위한 표준 S-100과 안전한 통신을 할 수 있는 인터페이스를 제공하는 SECOM을 기반으로 선박과 육상 간의 서비스를 안전하게 데이터를 주고 받을 수 있는 인터페이스를 연구하였다.

3. 보안 인터페이스 - SECOM을 중심으로

IEC 63173-2 SECOM과 IHO S-100에 기반한 스마트 항로표지 보안 인터페이스 개요는 표 2와 같다.

데이터를 송수신하는 데 필요한 사용자 정의, 사용자 인증, 서비스 과정으로 구성되어 있으며 실제 해상환경에서 사용할 수 있는 서비스에 맞게 설계하였다. 또한, 데이터를 안전하게 통신하는데 필요한 통신 채널, 데이터 암호화, 전자서명으로 구성되어 있다. 현재 해상환경에 제공하고있는 서비스는 무선 통신을 운용중이며 사용자는 웹페이지를 통해 해양 서비스에 접근하게 된다. 서비스를 이용하기 전 사용자는 일련의 인증과정을 통해 진입하게 되고, 서비스 제공자는 사용자의 신원을 확인 후 서비스 제공을 하게 된다. 육상에서의 유선 네트워크는 사용자의 위치가 고정되어 있는 반면, 해상환경에서 무선 네트워크는 각 사용자의 위치가 언제든지 바뀔 수 있어 취약성에 대해 보안 체계의 연구가 필요해 보인다[8].

표 2. 보안 인터페이스 개요
Table 2. Overview of Security Interface

Title	Description
User-Defined	Define the users who use the service.
User-Authentication	Authenticates users who use the service. The authentication is session method.
Service Process	In the service process, there are methods of upload and get.
Community Chennel	The communication channel uses TLS Version 1.3 and is based on SECOM.
Data Encryption	The data encryption algorithm uses AES-256.
Digital Signature	Data digital signature algorithm uses SHA256

가. 사용자 정의 (User-Defined)

IHO S-100 표준에 따르면 각 객체의 특징은 표 3과 같다. 가장 상위기관인 스키마 관리자(Scheme Administrator, SA)와 도메인 코디네이터, 데이터 서버, 데이터 사용자, 제품 생산자(Original Equiment Manufacturer, OEM)이 있다. 스키마 관리자(SA)는 국제수로기구(IHO) 사무국이며 S-100 데이터 보안 체계 관리자이다. 도메인 코디네이터는 각국의 해양 기관에 속하며 하위 기관에게 고유 ID 혹은 인증서를 발급하는 역할을 한다. 데이터 서버는 해양 서비스 데이터베이스의 역할을 하고 있으며 사용자별 데이터를 암호화하게 된다. 데이터 사용자는 실제 서비스를 이용하는 위치로서 상위기관에게 고유 ID를 발급받고 서비스를 이용할 수 있다. 마지막으로, 제품 생산자(OEM)은 데이터 사용자가 이용하는 해양 전자 장비 생산자 역할을 한다. 도메인 코디네이터로부터 등록이 되며 장비별로 고유 ID를 발급한다.

본 논문에서 인터페이스상 서비스 과정의 사용자는 데이터 서버와 데이터 클라이언트를 기준으로 구성하였다. 데이터 서버는 육상에 있는 항만, VTS 등이며, 데이터 클라이언트는 선박 항해자, 선원 등이 있다.

표 3. IHO S-100 객체의 특징
Table 3. Features of the IHO S-100 Object

Role	Description
Scheme Administrator	The Scheme Administrator signs the public key of the data server to create a digital certificate to be used in the operation of the protection system, and directly distributes M_ID and M_KEY information to all data servers.
Domain Coordinator	The Domain Coordinator informs the Scheme Administrator of the Data Server identity and contact information.
Data Server	The Data Server uses the M_KEY and HW_ID information provided by the Scheme Administrator to issue an encrypted product key for each specific installation.
Data Client	The Data Client is end user of the data set and receive protected information from the Data Server to access and use the data set and services.
Original Equipment Manufacturer	Bulid software applications according to the specifications specified in the IHO S-100 document, and conduct self-verification and validation according to the conditions required by Scheme Administrator.

나. 사용자 인증 (User-Authentication)

데이터 사용자는 해양 서비스를 웹서비스를 통해 접근하게 된다. 서비스를 이용하기 전 일련의 인증 과정을 진행해야 하며 각 서비스별 사용자의 권한에 따라 달라지게 된다. 인증 절차는 세션 방식으로 진행이 되며 사용자는 고유 세션ID를 발급받게 되고 서비스를 이용할 때 데이터 서버에게 세션 ID를 전달하게 된다. 그림 2는 사용자 인증 방식에 대한 시퀀스 다이어그램이다.

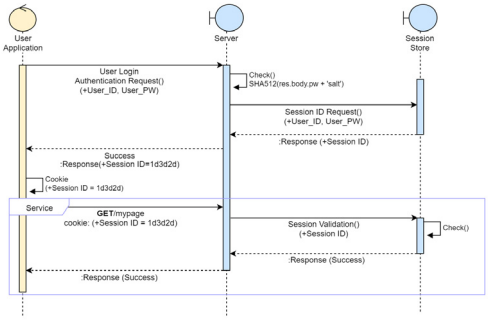

그림 2. 사용자 인증 절차 – 세션 방식
Fig. 2. User Authentication Procedure – Session Method

다. 서비스 과정 (Service Process)

서비스 과정은 S-100 표준에 기반하여 개발중인 서비스에 대해 작성했으며 각각 S-124(항행경보), S-125(항로표지 변경정보)다. S-124는 해사 안전 정보를 선박에게 전달해주는 서비스로서 안전 관련 긴급 정보로 구성되어 있으며, S-125는 항로표지 변경정보 서비스로서 항로표지가 변경된 사항이 있으면 선박에게 변경 정보를 전달해주는 서비스로 구성되어 있다. 그림 3은 해당 서비스 테스트 시나리오 중 S-124에 대한 시퀀스 다이어그램이다.

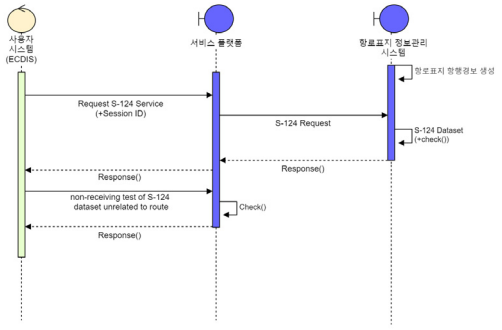

그림 3. S-124(항행경보 표준) 시나리오
Fig. 3. Navigational Warnings Scenario

라. 통신 채널 (Community Channel)

SECOM 문서에 따르면 서비스 인스턴스를 사용할 때 인터넷 전송은 SECOM 통신 채널 보안에 명시된 대로 신뢰할 수 있는 사용자의 TLS 및 유효한 인증서로 보호된다. 통신 채널 보호는 데이터 자체 보호를 보완하는 것이며 액세스 요청 및 알림과 같은 다른 서비스 요청도 보호하기 위해 포함되어야 한다. SECOM 통신 채널 보안은 ID 레지스트리에서 얻은 인증서의 사용을 설명하며 이를 통해 그림 4와 같이 서비스 상호 작용 자체에 대한 인증을 가능하게 한다. 또한, SECOM 공개 키 인프라(SECOM PKI) 또는 공개 키 인프라에 의존한다.

마. 데이터 암호화 (Data Encryption)

SECOM에서 사용되는 암호화 알고리즘은 IHO S-100 Part 15(Data Encryption)을 참고하고 있으며 기술된 내용은 다음과 같다. 데이터가 암호화 될 때 알고리즘은 암호 블록 체인(Cipher Block Chaining mode, CBC) 작동 모드에서 고급 암호화 표준(Advancded Encryption Standard, AES)이어야 하며, 항상 전체 데이터(페이로드) 암호화되어야 한다고 가정한다. AES 블록 암호 알고리즘은 대칭 키 알고리즘이며 이는 암호화와 복호화에 동일한 키가

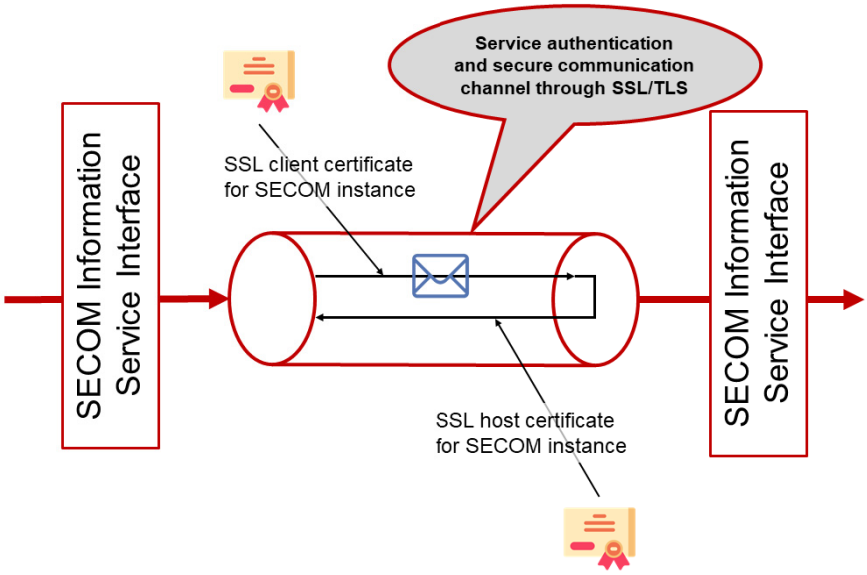

그림 4. 보안 통신 채널 개요도
Fig. 4. Overview of Secure Communication Channel

사용됨을 의미한다[9]. AES 알고리즘은 한 블록의 일반 텍스트가 한 블록의 암호 텍스트로 변환되는 방식과 그 반대로 변환되는 방식으로 정의하고 있다. AES의 블록 크기는 항상 16바이트(128비트)이며 키 길이는 128비트, 192비트 또는 256비트 중에서 선택할 수 있다. 해당 변형의 이름을 AES-128, AES-192, AES-256로 정의한다. 또한, SECOM 암호화 키 관리 체계에서는 데이터 암호화에 사용되는 대칭 키를 임시 키로 생성하여 보호된 전용 서비스 인터페이스를 통해 데이터 클라이언트로 보낸다. 대칭 키는 제한된 시간(세션)에만 사용된다. 그림 5는 암호화 키 관리에 대한 시퀀스 다이어그램이다.

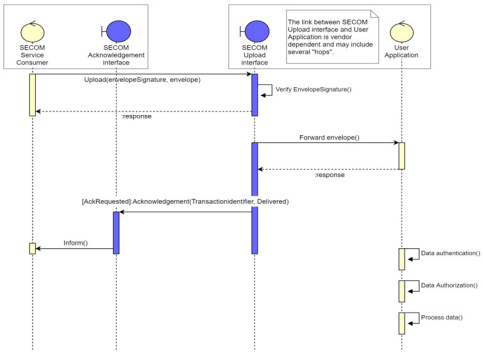

그림 5. 암호화 키 관리 시퀀스 다이어그램
Fig. 5. Sequence for Encryption Key Management

바. 전자 서명 (Digital Signature)

전자 서명에는 수신된 데이터의 무결성을 확인하는데 사용되는 체크섬과 데이터 인증을 위해 요구되는 ID가 포함되어 있다. 데이터가 교환될 때마다 디지털 서명은 항상 최종 사용자에게 첨부되고 확인되어야 한다. 이것은 기본 데이터에 대한 엔드 투 엔드 보호를 제공한다. 데이터 서명 알고리즘은 SHA256을 사용하며 SHA (Secure Hash Algorithm)의 하나의 종류다. 무작위 값을 입력하더라도 256비트의 고정된 결과값을 출력하며 서명은 HEX로 전송이 된다. 이때, 서명은 사용자의 신원 정보를 설명하는 구조화된 정보이다[10].

Ⅳ. 결 론

해상에서 사이버보안 위협은 인명 피해뿐만 아니라 국가적 재산 손실로 이어질 수 있다. ICT기술이 점차 고도화되어 가고 있는 시대에는 보안적인 요소는 필수적으로 자리매김을 하고 있다. 해상환경의 안전과 보안증진의 목적으로 개발하고있는 기술은 용도에 맞게 보안 지침이 설계가 되어야 한다. 선박 안전과 해상 사이버 보안 위협이라는 주제로 IMO(국제해사기구)에서는 최근 몇 년간 논의를 하고 있다.

본 논문에서는 해상환경에서 안전한 통신을 위한 보안

체계를 연구하였다. IEC 63173-2 SECOM과 IHO S-100모델을 분석하였으며, 문서에 기반한 기본적인 서비스 과정에 대한 보안체계를 제시하였다. 해상환경의 무선 통신 특성상 데이터 교환에 대한 취약점도 다소 존재하였으며 비인가된 사용자가 서비스에 접근할 수 있는 취약점을 고려하여 사용자 인증에 대한 부분을 추가하였다. 기존 해상환경에 관련되어 있는 전산 시스템들이 스마트화가 되고 있으며 통신 환경에서 보안적인 요소들에 대한 연구가 필요해보인다.

References

[1] In-Huhum BAEK, Mi-Ra YI, Jun-Mo PARK.(2023).A Study on the Conformity Verification Method for the Placement of the Aids to Navigation.THE JOURNAL OF FISHERIES AND MARINE SCIENCES EDUCATION, 35(1),22-32.
DOI : https://doi.org/10.13000/JFMSE.2023.2.35.1.22

[2] IEC 63173-2. Secure Communication between Ship and Shore(SECOM) Available : https://webstore.iec.ch/publication/64543

[3] Sang-Min Lee, Yun-Soo Choi, Jae-Myeong Kim, Byeong-Heon Min, Won-Jong Lee.(2021).Design of Data Model for Marine Information Industry based on S-100 Standard.Journal of Digital Contents Society, 22(8),1351-1357.
DOI: https://doi.org/10.9728/dcs.2021.22.8.1351

[4] Young-Jae Kim (2019). Smart Navigational Beacon Establishment and Promotion Plan. Korean Institute of Navigation and Port Research, 2019(3), 94-97

[5] Se-Woong Oh, Young-Jae Kim (2019). A Study on the Smartization Strategy of Navigation Aid Information, Korean Institute of Navigation and Port Research, 104-106

[6] KRISO, Korean e-Navigation Project Available : https://www.kriso.re.kr/menu.es?mid=a10209010000

[7] Dong-Woo Kang, Se-Woong Oh, Hyun-Soo Choi(2018). Development of Electronic Chart Service for Small Ships. Korean Institute of Navigation and Port Research. 358-359

[8] Eun-Sub Lee. Young-Kon Kim (2020). A Study on Wireless Network Management for Security sEnhancement. The Journal of the Institute of Internet, Broadcasting and Communication, 20(3), 195-200.
DOI : https://doi.org/10.7236/JIIBC.2020.20.3.195

[9] Chan-Il Woo. Eun-Hee Goo (2020). A Study on Image Integrity Verification Based on RSA and Hash Function. Journal of the Korea Academia-Industrial cooperation Society. 21(11), 878-883.
DOI : https://doi.org/10.5762/KAIS.2020.21.11.878

[10] Jung-Hwa Jo. Soo-Bin Yoo. Su-Min Yoo. Ae-Seon Son (2020). Contract Platform in a Blockchain-based Decentralized Identity Environment. The Journal of KIIT, Vol. 18. No. 12. 131-139
DOI : 10.14801/jkiit.2020.18.12.131

저 자 소 개

홍 승 표(정회원)

- 동서대학교 컴퓨터공학 석사
- 현재 : 동서대학교 컴퓨터공학 (박사과정)
- 주요 관심분야 : 디지털 포렌식, 정보보호

이 훈 재(정회원)

- 경북대학교 전기공학과 석사
- 경북대학교 전기공학과 박사
- 현재 : 동서대학교 컴퓨터공학과 (정교수)
- 주요 관심분야 : 보안 통신 시스템, 부채널 공격, USN 및 RFID 보안

이 영 실(정회원)

- 동서대학교 유비쿼터스IT학과 석사
- 동서대학교 유비쿼터스IT학과 박사
- 현재 : 동서대학교 International College Computer Science학과 부교수
- 주요 관심분야 : Computer Security, Maritime IT Convergence, Healthcare

※ 이 논문은 2023년도 해양수산부 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임 (20210650. 해양 디지털 항로표지 정보협력시스템 개발)