Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.447

자율 운항 선박의 인공지능: 잠재적 사이버 위협과 보안*

유 지 운,[1†] 조 용 현,[2] 차 영 균[3‡]
[1,2](주)디에스랩컴퍼니 (연구원, 대표이사), [3]고려대학교 (교수)

Artificial Intelligence for Autonomous Ship: Potential Cyber Threats and Security*

Ji-Woon Yoo,[1†] Yong-Hyun Jo,[2] Young-Kyun Cha[3‡]
[1,2]DSLABCOMPANY Inc. (Researcher, CEO), [3]Korea University (Professor)

요 약

인공 지능(AI) 기술은 해양 산업에서 스마트 선박을 자율 운항 선박으로 발전시키는 주요 기술이다. 자율 운항 선박은 사람의 의사 판단 없이 수집된 정보로 상황을 인식하며 스스로 판단하여 운항한다. 기존의 선박 시스템은 육상에서의 제어 시스템과 마찬가지로 사이버 공격에 대한 보안성을 고려하여 설계되지 않았다. 이로 인해 선박 내·외부에서 수집되는 수많은 데이터에 대한 침해와 선박에 적용될 인공지능 기술에 대한 잠재적 사이버 위협이 존재한다. 자율 운항 선박의 안전성을 위해서는 선박 시스템의 사이버 보안뿐만 아니라, 인공지능 기술에 대한 사이버 보안에도 초점을 맞춰야 한다. 본 논문에서는 기존 선박 시스템과 자율 운항 선박에 적용될 인공지능 기술에 발생할 수 있는 잠재적인 사이버 위협을 분석하고, 자율 운항 선박 보안 위험과 보안이 필요한 범주를 도출했다. 도출한 결과를 바탕으로 향후 자율 운항 선박 사이버 보안 연구 방향을 제시하고 사이버 보안 향상에 기여한다.

ABSTRACT

Artificial Intelligence (AI) technology is a major technology that develops smart ships into autonomous ships in the marine industry. Autonomous ships recognize a situation with the information collected without human judgment which allow them to operate on their own. Existing ship systems, like control systems on land, are not designed for security against cyberattacks. As a result, there are infringements on numerous data collected inside and outside the ship and potential cyber threats to AI technology to be applied to the ship. For the safety of autonomous ships, it is necessary to focus not only on the cybersecurity of the ship system, but also on the cybersecurity of AI technology. In this paper, we analyzed potential cyber threats that could arise in AI technologies to be applied to existing ship systems and autonomous ships, and derived categories that require security risks and the security of autonomous ships. Based on the derived results, it presents future directions for cybersecurity research on autonomous ships and contributes to improving cybersecurity.

Keywords: Autonomous Ship, Maritime Cyber Security, Cyber Threat, AI Security

Received(02. 10. 2022), Modified(03. 24. 2022), Accepted(03. 25. 2022)

* 이 논문은 2022년 해양수산부 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임(해양 사이버위협 인텔리전스 시스템 개발)

† 주저자, jw.yoo@dslabcompany.com
‡ 교신저자, ykcha@korea.ac.kr(Corresponding author)

I. 서 론

지난 몇 년 동안 우리는 다양한 유형의 사이버 물리 시스템(cyber-physical system)의 개발과 배치에서 기하급수적인 성장을 목격했다. 이러한 성장은 전력망, 운송 시스템, 의료 기기, 가전제품 등 일상생활의 거의 모든 측면에 영향을 끼쳤다[1]. 이러한 변화는 조선 해양 산업에도 많은 변화를 가져왔다. 선박 네트워크 연결성이 매우 높아지면서 스마트 선박이 등장했고, 해양 산업의 새로운 패러다임을 이끌 자율 운항 선박 기술 확보 경쟁이 치열해지고 있다. 자율 운항의 핵심 기술인 인공지능 기술은 데이터와 지식을 기반으로 인간의 인지, 학습, 추론 등과 같이 고차원적인 정보처리 능력을 구현한다[2]. 머신러닝, 딥러닝 등 인공지능 기술은 자율 운항 선박에서 발생하는 수많은 데이터를 처리하여 선박의 무인화·자율화를 지원할 것으로 기대한다.

자율 운항 선박은 인공지능, 빅데이터, 센서 등 많은 첨단 기술이 융합된 차세대 선박으로 운영비의 감축과 해양사고 감소라는 기대효과를 가지고 있지만[3], 육상에서의 운영, 관리 시스템과 연결되어야 하는 높은 연결성으로 인해 많은 사이버 위협에 노출될 것이다[4]. 이중화되지 않은 시스템의 고장이 선박의 운항 능력에 중대한 영향을 미치지 않도록 이중화 또는 백업 시스템을 고려해야 하며, 선박 항해 시스템은 고가용성을 염두에 두고 설계되어야 한다[5]. 따라서 자율 운항을 지원하는 통신 시스템은 안전 시스템의 필수적인 부분으로 간주되며 안전 인증이 필요하다[6]. 이러한 사이버 보안 문제를 해결하기 위해 선박의 시스템, 인공지능 기술의 취약점 등에 대한 여러 연구가 활발히 진행 중이다.

본 논문에서는 자율 운항 선박에서 어떠한 인공지능 기술이 사용되는지 알아보고, 인공지능 기술이 선박에 적용되면서 발생할 수 있는 사이버 위협을 알아본다. 기존에 연구되고 알려진 사이버 위협이 자율 운항 선박에 어떠한 영향을 줄 수 있는지 공격 시나리오를 예측하여 자율 운항 선박 보안에 필요한 연구 방향을 제시한다.

II. 관련 연구

2.1 인공지능(AI)

인공지능이란 인간의 학습능력, 추론능력, 지각능력, 자연어 처리 등을 인공적으로 구현하는 컴퓨터 공학의 세부분야 중 하나이다. 다시 말해 인간의 지능을 기계 등에 인공적으로 구현한 것 또는 구현하는 기술이다. 인공지능은 고전적 방법과 반응적 방법부터 머신러닝(machine learning)으로 발전했고, 고급 지능형 의사 결정 알고리즘인 딥러닝(deep learning)으로 더욱 발전했다. Table 1.은 인공지능 기술의 방법과 알고리즘 종류이다[7].

최근 인공지능 기술 개발 동향은 단순한 인지능력이 아닌 인지한 환경 속에서 최적의 답을 찾아내고 스스로 학습한 지식을 더해 추론 및 예측을 하며, 문제를 스스로 발견하고 해결하는 단계에 이르기까지 다양한 분야의 연구 진행되고 있다. 현재 인공지능은 국방, 의료, 교육, 게임, 보안 등 다양한 산업 분야에 적용되고 있다[8]. 또한, 빅데이터, 클라우드 컴퓨팅 등 다른 첨단 기술과의 융합으로 스마트 시티, 인공지능 로봇, 자율주행 등 자율적인 상황 판단과 능동적인 행동을 수행하는 응용 분야에도 적용되고 있다[2].

하지만 인공지능의 적용 분야가 확대됨에 따라 인공지능 기술의 보안 문제에 대한 관심도 증가하고 있

Table 1. Classification of artificial intelligence methods

Methods	Algorithm
Classical	• Road Map Building • Cell Decomposition • Artificial Potential Field
Reactive	• Fuzzy Logic Controller • Neural Network • Neuro - Fuzzy • Genetic Algorithm (GA) • Ant Colony Optimization • Particle Swarm Optimization • Artificial Immune Network
Machine Learning	• Transfer Learning • Artificial Neural Network • Active Learning • Extreme Learning Machine • Incremental learning • Feature Learning
Deep Learning	• Deep Neural Network • Convolutional Neural Network • Deep Convolutional Auto-Encoders

다. 인공지능 기술의 사용으로 인해 발생하는 잠재적 위협은 인공지능의 기능을 사이버 공격 도구로 사용하는 방법과 인공지능 시스템의 취약점을 악용하는 방법으로 분류할 수 있다. 사이버 공격자들은 기존의 사이버 공격 기술과 연계해 더 큰 피해를 입힐 수 있는 인공지능 기반 사이버 공격을 지속적으로 변화시키고 개선해나가고 있다. 따라서 인공지능 기술의 개발 및 적용에 있어 이러한 위험성에 대한 고려와 대비가 반드시 필요하다[9][10][11].

2.2 자율 운항 선박

자율 운항 선박은 인공지능, 사물인터넷, 빅데이터, 센서 등 모든 디지털 핵심 기술을 융합해 스스로 최적항로를 설정하고 항해할 수 있는 차세대 고부가가치 선박이다. 자율 운항 선박은 연료비를 절약하고 정비 및 고장시간을 단축시켜 운영비를 감축시키고, 인적 과실 감소와 사고대응시스템을 강화시켜 해양사고를 감소시키는 기대효과를 가지고 있다[3].

국제해사기구(IMO)에서는 자율 운항 선박을 MASS(Maritime Autonomous Surface Ship)라 명명하고, 사람의 개입 없이 또는 최소한의 개입으로 운항하는 선박으로 정의한다. IMO에서는 자율 운항 선박의 운항안전을 위한 법적 규정을 논의하고, 선박 운영과 규제 적용을 위해 선박의 자율화 정도에 따라 자율 운항 선박을 Fig.1.과 같이 4단계 등급으로 구분한다[12].

1단계는 부분적 자동화와 선원의 의사결정을 돕는다. 2단계는 선박이 원격으로 제어되지만 선원은 탑승하여 시스템과 기능을 제어하고, 시스템 고장 시 탑승한 선원이 직접 대응한다. 3단계는 선원이 탑승하지 않고 원격으로 제어하며, 시스템 고장에 대비하여 stand-by 시스템을 구축한다. 완전한 무인 자율 운항 선박은 4단계에 해당한다.

선박의 무인화를 위해서는 여러 선박을 동시에 조종할 수 있는 "가상 선장"이라고 할 수 있는 해안 통제 센터(shore control centre)와 원격 운영자가 필요하다. 자율 운항 선박은 선박의 단순한 무인화를 넘어서 사람의 개입 없이 선체의 안전성과 환경을 모니터링하고, 얻은 정보를 전달하고, 그에 기초한 결정을 내릴 수 있어야 한다[6][13].

Rolls-Royce의 백서[14]에 따르면 자율 운항 선박 개념의 중요한 구현 요소는 연결성이다. 이러한 연결성은 양방향성과 정확성을 지원하고 확장이 가능하므로 이중화를 생성하고 위험을 최소화할 수 있다. 또한 자율 운항 선박의 경우 운항 제어 알고리즘 및 충돌 회피가 특히 중요하다. 이를 위한 의사결정 알고리즘은 해양 규칙과 규정의 해석이 필요하다. 자율 운항 선박의 제어 알고리즘의 개발은 지속적인 개발을 통해 발전할 것이며, 광범위한 테스트와 시뮬레이션의 대상이 될 것이다.

2.3 자율 운항 선박의 구성 요소

자율 운항 선박의 핵심 기술은 Fig.2.와 같이 상황인식 및 탐지기술, 판단기술, 조치 및 제어 기술, 인프라 기술로 구분할 수 있다. 자율 운항 선박은 탐지, 판단, 조치를 모두 인공지능이 수행하며, 조치 결과만 선원 또는 해안 통제 센터에서 모니터링 한다[15].

상황인식과 탐지기술은 Radar, Lidar, CCTV, AIS(Automatic Identification System) 등의

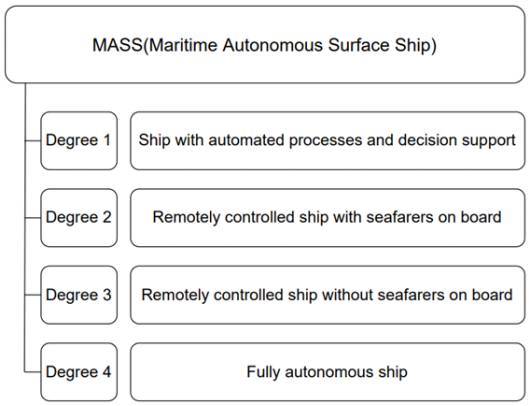

Fig. 1. The degrees of autonomy

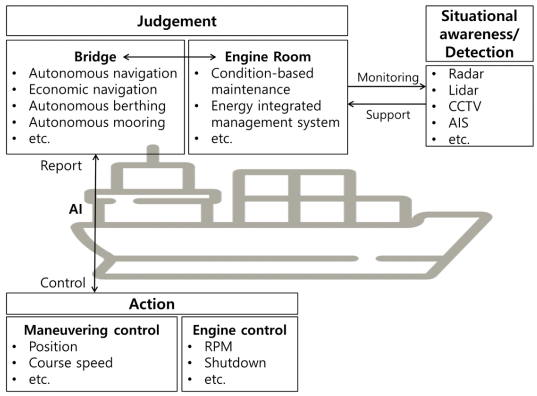

Fig. 2. Systems of autonomous ship

Table 2. Examples of autonomous ship components and functionalities description[15][16]

System	Component	Functions
Situational awareness/ Detection	Voyage Data Recorder (VDR)	▪ Principal alarms and sensors measurements recording
	Very High Frequency (VHF) radio	▪ Transmitting messages between vessels
	Automatic Identification System (AIS)	▪ Sending and receiving GPS positions, speed, heading, type of ship, next port and estimated time of arrival to and from surrounding ships
	Global Maritime Distress and Safety System (GMDSS)	▪ Sending and receiving critical safety alerts
	RAdio Detection And Ranging (RADAR)	▪ Detection and determination of the position and speed of the objects
	Light Detection And Ranging (LiDAR)/ Laser Detection And Ranging (LADAR)	▪ Detection and determination of the position and speed of the objects with greater accuracy
	Video cameras (CCTV)	▪ Objects detection and recognition
	Echo sounder	▪ Depth measurement
	Global Positioning System (GPS)	▪ Position measurement, and indirectly speed measurement
	Gyro compass	▪ Angular position and velocity measurement
	Speed log measurement	▪ Speed measurement
	Situation awareness system	▪ Picture compilations around the vessel
	Electronic Chart Display Information System (ECDIS)	▪ Detecting position of the ship on the map
	System Control And Data Acquisition(SCADA) server	▪ Machinery system sensors measurements and alarms data log
Judgement	Engine automation system	▪ Machinery components health monitoring
	Route planning system	▪ Selecting the route between departure and arrival point based on the traffic in area
	Navigation and collision avoidance system	▪ Navigating within ports and channels ▪ Position holding ▪ Avoiding collision with other vessels and objects
Action/ Control	Bow thruster controller	▪ Bow thruster speed control
	Main engine controller	▪ Control over engine speed ▪ Engine health status monitoring
	Generator controller	▪ Generator speed control ▪ Generator health status monitoring
	Azimuth controller	▪ Azimuth angle control ▪ Azimuth health monitoring
Infra structure	Shore control centre	▪ Monitoring of physical processes ▪ Navigation control ▪ Control over the ship in emergency/manoeuvring operating modes ▪ Implementation of software updates
	Connectivity manager	▪ Control over information flow between the vessel and the shore control centre
	Autonomous ship controller	▪ Monitoring of the processes safety and alarm generation ▪ Control over ship operating modes (emergency, sailing, autonomous, remotely controlled etc.)
	Ship control station	▪ Interface between crew on board and the vessel, allowing the crew to take control over the navigation systems and engine automation systems

비전 시스템으로 기상 상황, 해상의 물체 등을 정확하게 인식할 수 있는 기술이다.

판단 기술은 비전 시스템을 통해 수집 및 예측되는 데이터를 기반으로 자율 운항 선박이 자동으로 항해, 접안, 계류할 수 있는 기술이다. 해상 조건에 따라 경제적이고 안전하게 항해할 수 있는 경로를 자동으로 설정하고, 고장을 예측하여 사전에 조치를 취할 수 있다.

조치 및 제어 기술은 판단기술을 통해 선박의 위치, 속도, 엔진 제어 등을 인공지능을 통해 수행하며, 비상시 해안 통제 센터에서 선박을 원격으로 통제할 수 있는 기술이다.

인프라 기술은 자율 운항 선박을 운용할 수 있는 항만 자동화 기술 등을 의미하며 법률, 제도, 표준을 포함한다.

각 기술은 역할별로 분류되지만 자율 운항 선박에서 각 기술 및 시스템은 서로의 데이터를 기반으로 인식, 탐지, 판단, 제어되기 때문에 개별적인 시스템으로 볼 수 없다. 자율 운항 선박의 각 시스템별 구성 요소 예시는 Table 2.에 제시되어 있다.

III. 자율 운항 선박의 AI 기술

3.1 상황 인식 및 탐지

국제해사기구의 1974 SOLAS(1999/2000 개정사항 제5장 규칙19)에 따르면 선박 중 300톤 미만의 여객선을 제외한 대부분 선박에는 자동식별 시스템(AIS) 설치가 의무화되어 있다. AIS는 해상 교통 상황 인식에 필수적인 정적 및 동적 데이터를 보고한다. AIS 데이터를 다른 데이터와 결합할 때는 높은 수준의 인식과 상황 판단이 필요한데, 인식 방법에는 신경망(neural network), 베이지안 네트워크(bayesian network), 가우스 프로세스(gaussian process) 등이 있다[7]. 또한 AIS의 수많은 데이터를 이용하여 해양 영역에서 이상 징후를 탐지하는 VRNN(Variational Recurrent Neural Network), ANN(Artificial Neural Network) 등 딥러닝 기반 기법이 연구되고 있다[17][18]. 해상에서 물체를 탐지하기 위해 CNN(Convolutional Neural Networks)을 사용할 경우 방대한 계산 작업이 필요하다는 단점이 있다. 해상에서는 이미지에 포함된 개체의 크기가 거리에 따라 달라지기 때문에 이 작업이 항상 가능하지

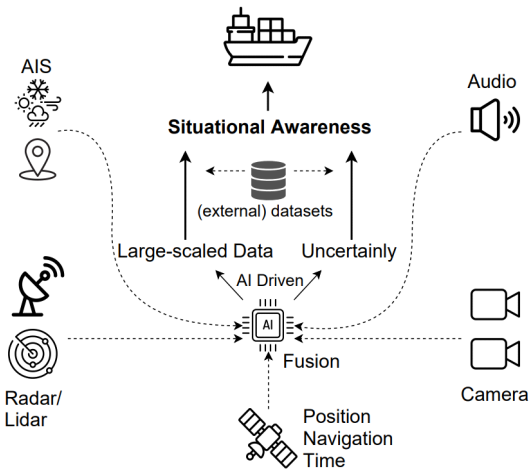

Fig. 3. An overall view of AI driven maritime situational awareness system[19]

않기 때문에 RPN(Region Proposal Network)은 이 문제를 해결하는 방법 중 하나로 제시된다. RPN은 작은 보트 등과 같이 픽셀 면적으로 볼 때 물체의 영역이 매우 작을 때 유용하다[19].

선박의 전체적인 상황 인식 주요 과제는 안전과 이상 징후를 탐지하는 것이다. Fig.3.와 같이 AIS, GNSS(Global Navigation Satellite System), 카메라 이미지, 오디오 신호, 센서 데이터 등을 융합하여 상황을 인식하고 이상 징후를 탐지할 수 있다. 예를 들어 탐지 및 분류된 결과가 AIS 메시지의 메타 데이터와 일치한다면 정상적인 상황 인식을 했다고 볼 수 있다. 이 과정은 다음 단계를 위한 기초가 되고, 식별된 주변의 물체를 인식하고 계획된 경로를 사용하여 충돌 확률을 계산한다.

3.2 자동 항해 시스템

선박의 자율 운항에는 다양한 인공지능 기술이 포함된다. Fig.4.는 자동 항해 시스템(autonomous navigation system)의 구조이다[20].

자동 항해 시스템 구조는 네 가지 기술 영역으로 구분할 수 있다. 사람의 의사결정 없이 자율적인 운항을 위해 센서 데이터 수집 및 분석을 통한 상황인식과 탐지기술과 자동 항해, 충돌 회피, 효율적인 경로 계획 등의 판단 기술, 판단 기술을 근거로 선박의 활동을 제어하고 상황에 대해 조치하는 기술, 그리고 선박 외적으로 자율 운항 선박을 운용하고 원격 모니터링 및 원격 제어하기 위한 인프라 기술 등이 있다.

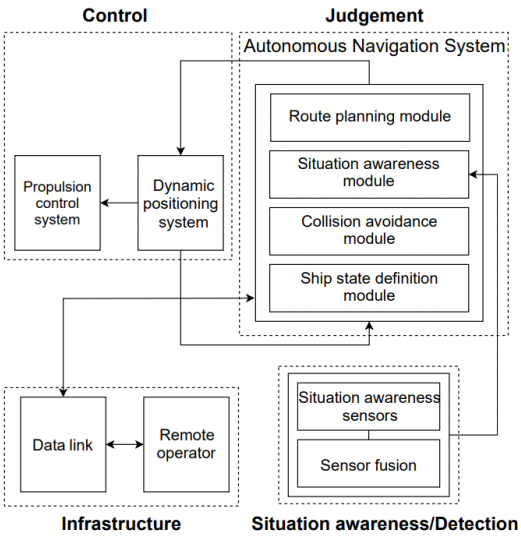

Fig. 4. ANS(Autonomous Navigation System) architecture

선박 충돌 사고 대부분은 인적 사고로 인해 발생하며 해양에서 큰 위협이 되고 있다[21]. 선박 충돌 회피는 1972년 국제 해상 충돌 방지 규정 협약(COLREGs)으로 규제하고 있다. 자율 운항 선박은 딥러닝의 발전으로 충돌 회피 문제를 해결할 수 있다. Fig.5.는 충돌 회피 절차를 설명하기 위한 도식적인 표현이다. 충돌 회피는 사전에 수집된 데이터와 실시간 센서 데이터를 분석하여 COLREG을 따를 수 있는 행동을 찾아낸다. 이 과정을 통해 학습하고

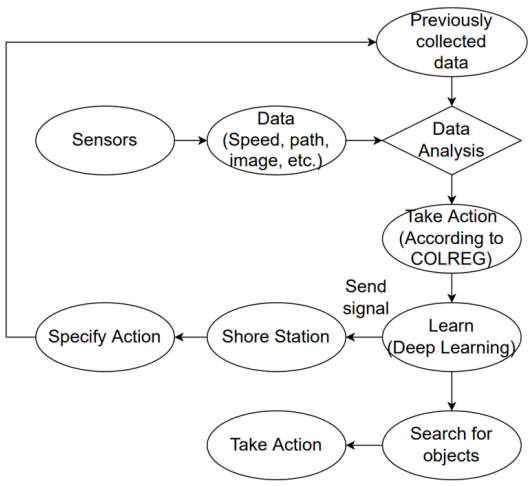

Fig. 5. Schematic representation for autonomous collision avoidance[7]

해안 통제 센터는 이 학습 데이터를 다시 분석 과정의 데이터로 사용한다. 인공지능은 이 반복 과정으로 물체를 탐지하여 충돌 회피 절차를 수행한다.

선박 간 상황 인식과 충돌 방지를 위해서는 추가적인 의사결정 지원도 가능해야 한다. 이러한 기술들을 적용하기 위한 딥러닝 프레임워크와 머신러닝 등에 필요한 선박 인텔리전스를 달성하기 위한 연구개발이 필요하다[22].

경로 계획은 선박 자율 시스템의 주요 매개 변수 중 하나이다. 경로 계획의 목적은 최적의 거리와 시간으로 목적지에 도착하는 것이다. 현재 무인자동차, 이동로봇, 드론 분야에서의 경로 계획에는 신경망, 퍼지, 유전 알고리즘 등의 기법이 연구되고 있다[7]. 기존 경로 계획 알고리즘은 과거 데이터를 재활용하여 알고리즘의 정확도가 떨어지고 실제 경로가 효율적이지 않다. 그로 인해 무인 자율 운항 선박 경로 계획 모델에 대한 연구가 진행되고 있고, 개선된 경로 계획 알고리즘 및 모델이 개발되고 있다[23][24].

3.3 자동 접안 시스템

접안은 선박이 항만에 정박하는 것을 의미한다. 기존 대형 선박이 접안하기 위해서는 예인선의 지원을 받는다. 예인선이란 크기에 비해 강한 추진력을 가지고서 다른 선박을 밀거나 당겨서 움직이는 것을 목적으로 하는 선박이다. 그렇기 때문에 이전에는 여러 예인선의 움직임을 동기화하는 방향으로 연구가 진행되었다. 하지만 최근에는 예인선과 같은 추가 지원 선박을 사용하지 않고 자동으로 접안하는 방안을 찾기 위한 연구로 방향이 바뀌었다.

접안 문제를 해결하는 접근법 중 하나는 인공신경망(ANN)의 사용이다. ANN은 머신러닝과 인지과학에서 생물학의 신경망에서 영감을 얻은 통계학적 학습 알고리즘이다. ANN을 이용한 선박 자동 접안 시스템은 신경망 훈련을 위한 학습 데이터를 생성하기 위해 선박을 수동으로 조종한다. 선박 조종 과정에서 기록되는 선박 좌표, 방향, 접안까지의 거리와 같은 선박 상태를 학습 데이터로 사용한다. 이 데이터로 학습한 신경망은 접안 시스템의 메인 컨트롤러로 사용된다. 기존 ANN 컨트롤러는 학습 데이터를 수집한 항만에서만 접안이 가능했지만, 최근 연구를 통해 ANN 컨트롤러를 다시 학습시키지 않고 새로운 항만에서도 자동으로 접안할 수 있는 컨트롤러가

제안되었다[25][26][27]. 접안 시스템은 복잡하기 때문에 입력과 출력의 관계를 글로벌하게 모델링할 수 있는 신경망을 선택하는 것이 필수적이다. 이를 위해 6개의 입력과 2개의 출력을 가진 교육 데이터를 학습하기 위해 다중 계층 인식을 사용한다[25]. 접안은 3단계로 이루어지는데, 배의 진로를 최적의 접안-접근 방향으로 변경하고, 배의 속도가 감소하다가 마지막으로 메인 엔진이 정지한다.

학습 기반 방법 중 보다 최근 방법은 딥러닝을 사용한다. ANN 기법의 모델 내 은닉 층을 많이 늘려서 학습의 결과를 향상시키는 DNN(Deep Neural Network) 기법 등 기존의 기법보다 향상된 기법들이 적용되고 있다[28][29]. 심지어 지도 학습, 강화 학습을 넘어 심층 강화 학습을 적용하여 더 높은 정확도와 효율성으로 우수한 성능을 보여주는 연구도 진행되고 있다[30].

IV. 자율 운항 선박 사이버 위협

4.1 선박 시스템의 사이버 위협

AIS는 선박 식별, 항해 상태, 방향, 위치 등을 통해 충돌을 방지하도록 설계되었다. 일반적으로 GPS와 VHF(Very High Frequency) 무선 통신의 조합을 활용한다. 이러한 기술은 사용되는 신호와 데이터 전송 프로토콜 모두에서 이미 알려진 취약점을 가지고 있다[31][32][33]. 이런 취약점을 감안하면 공격자가 데이터를 변조할 위험이 존재한다.

해양 산업에서 위치 데이터를 위해 많은 위성이 사용된다. GNSS는 상호 연결이 가장 많이 되는 시스템 중 하나이다. 위성 기반 통신에 의존하는 자율 운항 선박은 DoS(Denial of Service) 공격, 중간자(man-in-the-middle) 공격 등에 더욱 취약할 수 있다. GNSS에 대한 공격은 AIS 공격처럼 다른 선박 시스템의 장애를 일으킬 수 있다. 자율 운항 선박 시스템은 육상와의 통신을 원활하게 하기 위한 높은 연결성으로 인해 사이버 공격이 선박에 대한 완전한 통제를 제공할 가능성이 있다[34][35].

RADAR(RAdio Detection And Ranging)의 무선 신호는 위성보다 전파 Jamming이 더 어렵지만 불가능한 것은 아니다. 전통적으로 레이더 기반 공격은 레이더에서 정보를 얻는 선원이 탑승한 선박을 기반으로 하지만 자율 운항 선박이 항해 정보 침해에 더 취약할 수 있다. 무인 자율 운항 선박은 레이더, 빛, 적외선 등을 방출하는 기술을 포함한 센서에 의존하기 때문에 취약점을 악용할 가치가 증가할 수 있다[34].

Table 3. Cyber threat of system in ship

System	Threat(ICT)	ref
Automatic Identification System (AIS)	Spoofing Denial of Service	[31] [32] [33]
Global Navigation Satellite System (GNSS)	Jamming Spoofing	[34] [35]
RAdio Detection And Ranging (RADAR)	Jamming	[34]
Echo sounder / Light Detection And Ranging (LiDAR)	Denial of Service	[36]
Video camera (CCTV)	obfuscation, Covert Channels Attacks, Steganography, Denial of Service, Jamming Attacks	[37] [38] [39] [40]
Voyage Data Recorder (VDR)	Weak encryption Authentication Firmware update Data corruption	[41]

Echo Sounder, Lidar와 같이 신호를 보내고 받는 유사한 기술은 서비스 거부 공격과 같은 취약점을 공유한다. 미래의 자율 운항 선박은 유사한 취약점을 공유하고 동일한 시스템과 통신할 수 있기 때문에 몇 가지 단순한 사이버 공격으로 침해가 발생할 수 있다[36].

무인 자율 운항 선박에서 CCTV는 선박 내·외부를 촬영하며 선박 운영을 모니터링 한다. CCTV 기술은 사이버 공격자가 무인 선박에 대한 사이버-물리적 공격을 통해 CCTV 촬영 데이터를 난독화 하는 취약점이 알려져 있다[37][38]. 또한 은닉 채널과 스테가노그래피를 통한 데이터 유출, 서비스 거부 공격과 Jamming 공격으로 CCTV의 정상적인 동작을 방해하는 행위가 발생할 수 있다[39][40].

VDR은 사이버 공격자의 활동을 숨기기 위한 공격에 취약할 수 있다. VDR은 취약한 암호화, 인증, 펌웨어 업데이트 메커니즘, 데이터 손상 등의 취약점

에 대한 분석 결과가 있다. VDR은 블랙박스와 같은 역할을 수행하며 여러 해양 시스템에서 데이터를 수집한다. 컴퓨터의 로그를 지우거나 수정하여 악의적인 활동을 숨기는 것처럼 자율 운항 선박의 VDR을 표적으로 삼아 선박 시스템을 공격하는 공격자의 활동을 숨길 수 있다[41]. Table 2.는 선박 시스템에 존재하는 사이버 위협 분류이다.

또한 센서, 컨트롤러를 포함하는 선박 제어 시스템은 온도, 압력, 속도, 기기 상태 등을 모니터링하며 제어하면서 인적 오류를 줄이고, 자원 효율을 높이고, 기기의 수명을 연장시키며 경제적 이점을 보장하는데 큰 도움이 된다[42][43]. 다양한 디바이스와 프로토콜로 상호 운용성을 제공하기 위해 연결되지만 보안을 염두에 두지 않고 설계 및 개발되었으며 데이터는 일반 텍스트로 전송되기 때문에 공격자가 악용할 수 있는 많은 약점을 가지고 있다[44].

선박의 네트워크는 종종 육상의 시설과 연결되어 체계적이고 지속적인 위협에 대한 노출을 더욱 증가시킨다. 네트워크 간의 링크 설계 및 구성에서는 인증 및 암호화 방법을 거의 고려하지 않았기 때문에 잠재적으로 취약한 시스템이 인터넷에 노출될 수 있다[45]. 네트워크를 통해 IT 시스템에 광범위한 공격 표면과 많은 침입 지점을 제공할 수 있으므로 보안을 더욱 고려해야한다.

4.2 인공지능의 사이버 위협

사이버 보안을 위한 인공지능 기술 연구가 활발하게 진행되고 있다. 인공지능을 기반으로 시스템을 보호하고, 인공지능 또한 공격당하는 것을 예방하는 것이 주요 기술 동향이 되고 있다. 인공지능에 대한 사이버 공격은 머신러닝 알고리즘이 가지고 있는 취약점을 이용한다는 점에서 기존의 사이버 공격과 다른 점이 있다. 딥러닝 또한 머신러닝을 기반으로 하기 때문에 머신러닝 취약점에 영향을 받을 수 있다.

인공지능 사이버 위협에는 머신러닝 학습 과정에서 Poisoning Attack과 Backdoor Attack이 있다. Poisoning Attack은 잘못된 학습 데이터로 인공지능의 오동작을 유발하는 공격으로, 최소한의 데이터를 주입해 최대한 성능을 떨어뜨리는 것을 목표로 한다. Backdoor Attack은 Poisoning Attack에 연계된 공격이다. 어떠한 데이터가 학습 데이터로 활용될 때 공격자가 원하는 결과를 반환하게 하는 방식을 머신러닝 모델에서의 Backdoor라고 한다. Yao, Y 등[46]은 전이 학습 과정에서 Backdoor를 삽입하는 잠재적 Backdoor Attack 시나리오를 제안하였다. 전이 학습은 새로운 모델을 구축할 때 시간과 비용을 최소화하기 위해 학습 데이터가 부족한 사용자가 처음부터 전체 모델을 훈련할 수 있도록 설계되었다.

추론 과정에서는 Evasion Attack으로 인공지능의 오동작을 유발한다. 사람은 인식하지 못할 정도의 아주 작은 변조지만 인공지능은 전혀 다른 데이터로 인식할 수 있다. Fig.6.와 같이 사람의 눈으로는 분간하기 어려운 노이즈를 추가하면 머신러닝이 판다를 아에 다른 동물로 인식하도록 하는 것이 가능하다[47].

머신러닝은 입력에 대한 결과와 신뢰도를 출력한다. Inversion Attack 또는 학습 데이터 추출 공격은 수많은 입력에 대한 결과를 분석해 학습 데이터를 복원하는 공격이다. Fig.7.과 같이 Inversion Attack을 통해 안면 인식 머신러닝 모델의 학습 데이터를 복원할 수도 있다. 머신러닝 학습 데이터에 기밀정보나 개인정보 같은 주요 데이터가 포함되어 있는 경우 Inversion Attack을 통해 유출될 가능성이 존재한다[48].

Inversion Attack과 다르게 학습 데이터가 아닌 머신러닝 모델을 추출하는 공격을 Model Extraction Attack이라고 한다.

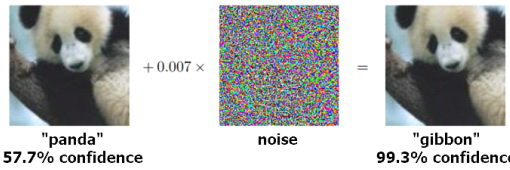

Fig. 6. Misclassification of the image after add noise[47]

Fig. 7. An image recovered using model inversion attack(left) and training set image of the victim(right)[48]

4.3 자율 운항 선박의 인공지능 기술 사이버 공격 시나리오

자율 운항 선박에 대한 기대효과와 추정치에는 사이버 및 사이버-물리적 공격과 관련된 잠재적인 위협을 고려하지 않았다. 그 이유는 기존의 해양 시스템과 새로운 자율 운항 기술의 검증되지 않은 조합으로 인해 위험과 취약점을 종합적으로 평가할 수 없기 때문이다. 선박과 선박, 선박과 육상 인프라 간의 상호 연결이 증가할수록 잠재적인 사이버 위협 또한 증가한다[49][50]. 자율 운항 선박은 AIS, GNSS, 센서, 카메라 등으로부터 데이터를 수집하고 분석한 결과를 근거로 적절한 판단을 통해 선박을 제어한다. 이 과정에서 선박 시스템과 인공지능 기술의 취약점을 이용한 공격 시나리오를 다음 세 가지로 제안한다.

4.3.1 Ship Dataset Poisoning Attack

자율 운항 선박이 해상에서 충돌을 피해 운항하기 위해서는 장애물을 식별해야한다. 많은 장애물 중 선박을 분류하기 위해서는 운항 전 선박을 분류하기 위해 Fig.8.과 같은 학습 데이터가 필요할 것이다. Fig.8.은 인공지능 모델에 선박 식별을 위해 학습시킬 학습 데이터의 예시를 나타낸 것이다.
공격자가 인공지능 학습 단계에서의 취약점으로 공격한다면 잘못된 학습으로 인해 잘못된 판단을 하도록 유도할 수 있다. 이러한 경우는 선박의 항해 중 위협요소를 안전한 요소로 오인하여 선박으로 접근을 허용하도록 유도하는 공격 시나리오를 예상할 수 있다. Wenbo Jiang 등[52]은 PAPSO(Poisoning Attack with Particle Swarm Optimization)

Fig. 8. Before & after preprocessing input data[51]

Fig. 9. Dataset sample for poisoning attack

기법을 통해 학습 데이터세트에 악의적 샘플을 일부 주입하여 최대 95%에서 33%로 성능을 저하시키는 연구 결과를 얻었다. 이와 같은 방법으로 Fig.9.와 같이 선박 식별 학습에 Poisoning Attack을 시도할 수 있다. (a)는 정상적인 선박 이미지이고, (b)는 기존 이미지에 노이즈를 추가한 이미지이다. 사람의 눈으로는 같은 선박으로 인식할 수 있지만, 인공지능 학습 데이터에 주입할 경우 분류 정확도가 크게 감소될 수 있다.

4.3.2 Situation Awareness/Detection Evasion Attack

Wenbo Jiang 등[52]은 PAPSO 기법과 동일하게 EAPSO(Evasion Attack with Particle Swarm Optimization) 기법으로 Evasion Attack을 시도했다. Poisoning Attack과 마찬가지로 여러 반복 후에 성능이 크게 감소하는 결론을 얻었다. Evasion Attack은 특히 자율 주행에서 치명적일 수 있다[53]. 자율 주행 차량의 경우도 마찬가지로 물체를 인식하고 차량을 제어하기 위해 인공지능을 활용한다. 교통 표지판 인식은 자율 주행 차량에서 중요한 응용 프로그램이다. 차량의 카메라 장치에서 교통 표지판을 캡처하여 이미지를 분류하고 분류 결과에 따라 차량을 제어한다. 하지만 Fig.10.과 같이 스티커 부착 등 간단한 방법만으로 표지판 인식 모듈을 교란시키는 실험이 시연된 사례가 있다[54].

Evasion Attack에는 카메라를 통해 촬영되는 물체를 변조시켜 악용하는 방법도 있지만, 선박 시스템 취약점을 이용하여 Spoofing, Jamming 등의 공격 가능성도 존재한다. 선박 시스템을 공격하여 데

Fig. 10. Misclassification sign by sticker attack[55]

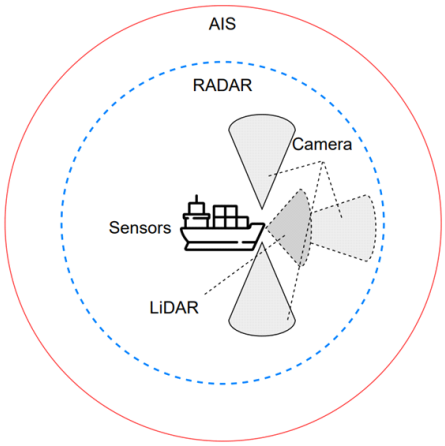

Fig. 11. Areal coverage of multi-sensors of ship[19][55]

이터 변조, 교란 등의 침해를 통해서도 인공지능의 오동작을 유발하는 공격이 가능하다. 선박은 Fig.11.과 같이 AIS, RADAR, Audio, Camera 등 여러 해양 센서 데이터를 통해 상황을 인식하고 물체를 탐지하여 경로 수정, 충돌 회피 등 적절한 판단을 수행한다.

4.3.3 Ship Sensor Data Attack

Fig.12.와 같이 인공지능의 입력 데이터로 활용되는 센서 데이터가 사이버 공격으로 데이터 침해를 받는다면 안전한 자율 운항을 보장할 수 없다. 대표적으로 AIS는 많은 대형 선박에서 의무적으로 사용하고 있지만, AIS 표준은 보안이 고려되지 않았다[56]. AIS 메시지는 암호화되지 않으므로 공격자가 쉽게 이용하고 조작할 수 있다. AIS 취약점을 이용한 공격은 기상 정보 조작, 거짓 충돌 경고, 서비스 거부 공격 등 여러 시나리오가 가능한 것으로 나타났다[31]. 데이터 변조 및 교란은 무인 자율 운항에

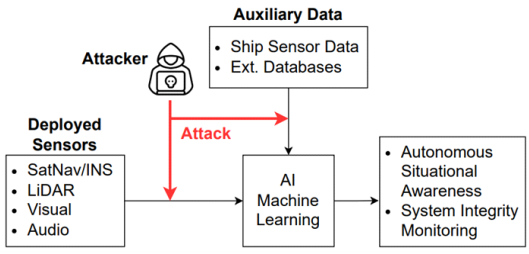

Fig. 12. Cyber attack scenario of identification data

상당히 많은 영향을 줄 것을 예상할 수 있다. 공격자가 센서 데이터를 공격하는 방법은 4.2절에 설명한 바와 같이 Spoofing, Jamming, DoS 등의 공격이 알려져 있다. 만약 Evasion Attack을 이용하여 자동 접안 시스템에서 카메라 또는 센서 데이터를 교란시켜 항만과의 거리를 잘못 판단한다면 선박이 항만에 충돌하는 사고가 발생할 가능성이 존재한다.

V. 자율 운항 선박 사이버 위협 대응 방안

Table 3.와 같이 AIS, GNSS 등 선박 주요 시스템 보안 문제에 대해 각각의 대책을 제시한 연구는 다수 발표되었다. 하지만 현재의 선박은 이미 배포된 시스템의 하드웨어를 변경해야 하는 등 고가의 비용 문제가 발생한다. 따라서 미래의 선박 보안은 하드웨어 교체가 필요하지 않은 방향을 목표로 해야 한다[57].

인공지능 기술의 사이버 위협 대응 방안으로 Levine 등[62]이 Poisoning Attack방어에 대해 기존의 기법과 달리 DNN을 사용하여 구현할 수 있는 새로운 접근법을 제안하여, 최신 공격 기술을 능가하고 일반적인 Posioning Attack에 대한 인증된 방어를 개발할 수 있다고 설명한다. Apruzzese 등[63]은 Evasion Attack에 대한 복원력을 개선하는 것을 목표로 하는 새로운 접근 방식인 AppCon을 제안했다. Gupta 등[64]은 적대적 공격에 대해

Table 4. Countermeasure for cyber threat of ship component

System	Countermeasure	ref
Automatic Identification System (AIS)	Software Security Framework, Authentication, Encryption	[57] [58]
Global Navigation Satellite System (GNSS)	Cross-Technology Location Estimation, Encryption, Drift Monitoring	[57] [59]
Echo sounder / Light Detection And Ranging (LiDAR)	Obfuscate signals, Randomly skipping pulses	[60] [61]
Video cameras (CCTV)	Standards compliance, (Remote) attestation	[37]

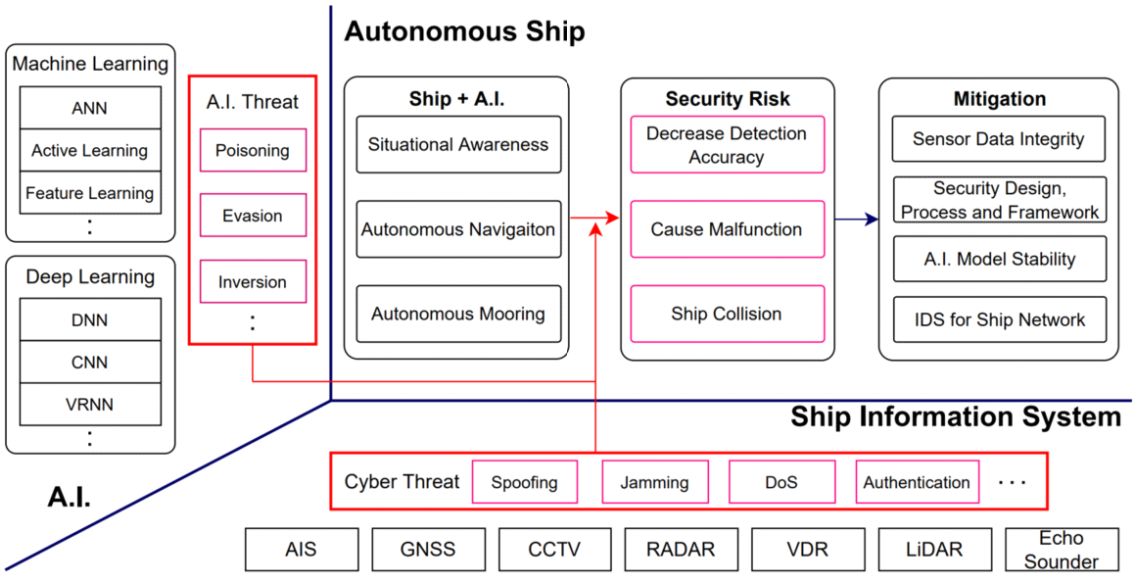

Fig. 13. Security risk and mitigation of autonomous ship

잘 확립된 방어 기술의 실행 가능성 문제를 연구하여 효과적인 해결책을 위한 지침을 제안했다.

본 논문에서는 선박 시스템과 자율 운항 선박에 적용될 인공지능 기술의 취약점에 대해 알아보고, 취약점을 이용한 사이버 위협을 통해 공격 시나리오를 도출했다. 선박 정보 시스템의 사이버 위협과 인공지능 위협은 어떤 것이 있는지와 선박 시스템과 인공지능 기술이 자율 운항 선박에서 어떠한 보안 위험이 되는지, 그 보안 위협을 완화하기 위한 방안을 Fig.13.에 도식화했다. 선박과 인공지능이 융합된 자율 운항 선박은 주변 상황을 인식하고 분석하여 운항과 접안을 사람의 개입 없이 수행한다. 자율 운항 과정에서 인공지능과 선박 시스템의 위협을 공격으로 이용한 보안 위험이 존재할 수 있다. 자율 운항이라는 핵심 기술에 존재하는 위험은 사이버 세계에 존재하는 위험이 아닌 사이버-물리적 위험이 된다. 자율 운항 선박에 존재하는 위험을 줄이고 보안을 향상시키기 위한 방법을 Fig.13과 같이 제안한다.

취약하다고 알려진 AIS, GNSS 등 선박 주요 시스템의 실시간 데이터는 인공지능의 상황 인식과 적절한 판단을 위해 보호되어야 한다. 센서 데이터와 외부와 상호 교환하는 선박 시스템 데이터는 자율 운항 중 인공지능의 인식, 판단에 기반이 되기 때문에 무결성과 신뢰성을 달성해야한다[65].

보안 설계는 센서 데이터 무결성과 신뢰성을 달성하기 위해 반드시 필요하다. 선박 시스템은 여전히 많은 취약점을 가지고 있고, 개선하기 위해서 높은 교체 비용을 부담해야한다. 자율 운항 선박에 탑재될 시스템은 기존에 존재하는 보안 문제를 해결하기 위해 설계 단계부터 보안을 고려해야 한다. 또한 운영 단계에서 안전한 자율 운항을 위해 보안 프로세스와 프레임워크가 필요하다. 보안 프로세스와 프레임워크가 정립되지 않으면 이상 행위가 발생했을 때 인공지능이 대처하기 어려운 상황이 발생할 수 있다. 지금까지 많은 선박 사고가 인적 과실로 인해 발생했다. 인공지능이 사람을 대신하여 승선하는 것과 동일한 자율 운항 선박은 보안 프로세스를 통해 기술만으로 해결하지 못하는 보안 틈새를 차단해야한다.

자율 주행 차량 보안은 2010년 중반부터 많은 연구 결과가 발표되었지만 자율 운항 선박 보안 분야는 아직 연구가 진행 중이다. 자율 운항 선박이 광범위한 테스트와 시뮬레이션 단계를 통해 안정성을 검증이 수행될 것이다. 이 과정에서 인공지능이 가지고 있는 사이버 위협에 대응하기 위한 연구가 함께 진행되어야 한다. 해상에서 선박 인공지능에 문제가 발생한다면 자율 운항 선박은 목적을 상실하게 된다. 인공지능 안정성이 검증되지 않으면 자율 운항 선박 또한 검증되지 않는다. 인공지능 또한 연구가 지속되고 있지만 선박에 적용될 인공지능에 필요한 보안 요구사항을 도출할 필요가 있다.

마지막으로 선박 내부 네트워크에 대한 침입 탐지 시스템(IDS)은 네트워크 내부 또는 외부에서 무단으로 접근하거나 악의적인 공격을 탐지하기 위해 필요하다. 특히 선박 시스템 간의 통신을 위해 사용되는 NMEA 프로토콜을 고려해야 한다. 자율 운항 선박의 높은 연결성으로 인해 발생할 수 있는 외부 공격자의 악의적인 접근과 이상 징후를 탐지하고, 선박 네트워크 특성을 고려한 네트워크 보안이 필요하다.

VI. 결 론

선박 센서 데이터는 인공지능의 인지, 판단, 제어에 영향을 주고 인공지능은 선박 제어에 영향을 준다. 자율 운항 선박은 개별 시스템이 독립적이지 않고 각 시스템이 자신의 역할을 수행하며 다른 시스템에 영향을 주는 데이터를 생성한다. 사이버 보안 위협 또한 하나의 시스템에만 영향을 주는 것이 아니라 자율 운항 선박 전체에 영향을 줄 수 있다. 자율 운항 선박은 운영비를 감축시키고 해양사고를 감소시키는 기대효과를 가지고 있는데, 자율 운항 선박이 사이버 공격으로 인한 사고가 발생한다면 그 목표를 달성하기 어려울 것이다. 따라서 사이버 공격을 예방하기 위해 각각의 시스템에 대한 사이버 침해가 다른 시스템에 영향을 주지 않도록 설계되어야 한다.

본 논문에서는 선박 시스템과 인공지능 기술의 취약점 및 위협을 조사하였고, 자율 운항 선박에서 사용될 수 있는 인공지능 기술에 대한 잠재적 사이버 위협과 대응 방안을 알아보았다. 자율 운항 선박은 아직 연구 단계이기 때문에 상용화 단계에서는 더욱 발전된 시스템이 적용될 것이다. 기존 해양 시스템과 인공지능 기술의 융합으로 알려지지 않은 새로운 위협이 발생할 가능성도 존재한다. 향후 연구에서는 해양 사이버 위험 환경에 대한 포괄적인 이해를 토대로 새롭게 적용될 인공지능 기술과 자율 운항 시스템에 대한 사이버 보안 연구가 필요할 것이다.

References

[1] A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-physical systems security—A survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802-1831, May. 2017.

[2] Sun-seon Kwon, "Technology Trends of AI and Big Data," TTA journal, 187(393), pp. 38-44, Jan. 2020.

[3] Korea Autonomous Surface Ship, "autonomous ship effect," https://kassproject.org/?menucode=10700&tmenu=content, Feb 3, 2022.

[4] J.E. Vinnem, and I.B. Utne, "Risk from cyberattacks on autonomous ships." Safety and Reliability - Safe Societies in a Changing World, CRC Press, pp. 1485-1492, June. 2018.

[5] Ø.J. Rødseth, B. Kvamstad, T. Porathe and H.C. Burmeister, "Communication architecture for an unmanned merchant ship," 2013 MTS/IEEE OCEANS-Bergen, pp. 1-9, June. 2013.

[6] M. Höyhtyä, J. Huusko, M. Kiviranta, K. Solberg, and J. Rokka, "Connectivity for autonomous ships: Architecture, use cases, and research challenges," 2017 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, pp. 345-350, Oct. 2017.

[7] A. Noel, K. Shreyanka, Kumar, K.G.S., Shameem, B.M. and B. Akshar, "Autonomous ship navigation methods: A review," Proc. Int. Conf. Marine Eng. Technol. Oman, pp. 161-174, Nov. 2019.

[8] K.W. Kug, "Case of application by artificial intelligence technology and industry field," ISSN 1225-6447. Weekly ICT Trends, IITP, pp. 15-27, Mar. 2019.

[9] S. Park and D. Choi, "Artificial intelligence security issues," Review of KIISC, 27(3), pp. 27-32, June. 2017.

[10] C. Benzaïd and T. Taleb, "AI for beyond 5G networks: a cyber-security defense or offense enabler?," IEEE

Network, vol. 34, no. 6, pp. 140-147, Sep. 2020.
[11] N. Kaloudi and J. Li, "The ai-based cyber threat landscape: A survey," ACM Computing Surveys (CSUR), vol. 53, no. 1, pp. 1-34, 2020.
[12] MSC. 1/Circ. 1638. "Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS)," IMO, June. 2021.
[13] S. Ahvenjärvi, "The human element and autonomous ships," TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, vol. 10 no. 3, pp. 517-521, Oct. 2016.
[14] R. Royce, "Autonomous ships: The next step," Marine Ship Intelligence. 2017.
[15] J. Kim and H.S. Jang, "Technology trends and preparations for autonomous ships," Bulletin of the Society of Naval Architects of Korea, 56(4), pp. 4-7, Dec. 2019.
[16] V. Bolbot, G. Theotokatos, E. Boulougouris and D. Vassalos, "Safety related cyber-attacks identification and assessment for autonomous inland ships," International Seminar on Safety and Security of Autonomous Vessels (ISSAV), Sep. 2019.
[17] D. Nguyen, R. Vadaine, G. Hajduch, R. Garello and R. Fablet, "A multi-task deep learning architecture for maritime surveillance using AIS data streams," 2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA), pp. 331-340, Oct. 2018.
[18] S.K. Singh and F. Heymann, "Machine learning-assisted anomaly detection in maritime navigation using AIS data," 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 832-838, Apr. 2020.
[19] S. Thombre, Z. Zhao, H. Ramm-Schmidt, J.M.V. García, T. Malkamäki, S. Nikolskiy and V.V. Lehtola, "Sensors and AI Techniques for Situational Awareness in Autonomous Ships: A Review," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 1, pp. 64-83, Jan. 2022.
[20] E. Jokioinen, "Redefining shipping: Remote and Autonomous Ship-The next steps," vol. 4, no. 5, AAWA whitepaper, Ship Intelligence Marine, June. 2016.
[21] L.P. Perera, V. Ferrari, F.P. Santos, M.A. Hinostroza and C.G. Soares, "Experimental evaluations on ship autonomous navigation and collision avoidance by intelligent guidance," IEEE Journal of Oceanic Engineering, vol. 40, no. 2, pp. 374-387, 2014.
[22] L.P. Perera, "Autonomous ship navigation under deep learning and the challenges in COLREGs," International Conference on Offshore Mechanics and Arctic Engineering, June. 2018.
[23] C. Wang, X. Zhang, R. Li and P. Dong, "Path planning of maritime autonomous surface ships in unknown environment with reinforcement learning," International Conference on Cognitive Systems and Signal Processing, Springer, Singapore, pp. 127-137, Nov. 2018.
[24] S. Guo, X. Zhang, Y. Zheng and Y. Du, "An autonomous path planning model for unmanned ships based on deep reinforcement learning," Sensors, vol. 20, no. 2: 426. Jan. 2020.
[25] N. Im, "A study on ship automatic berthing with assistance of auxiliary

devices," International Journal of Naval Architecture and Ocean Engineering, vol. 4, no. 3, pp. 199-210, Sep. 2012.
[26] V.S. Nguyen, V.C. Do and N.K. Im, "Development of automatic ship berthing system using artificial neural network and distance measurement system," International journal of Fuzzy logic and Intelligent systems, vol. 18, no. 1, pp. 41-49, Mar. 2018.
[27] N.K. Im and V.S. Nguyen, "Artificial neural network controller for automatic ship berthing using head-up coordinate system," International Journal of Naval Architecture and Ocean Engineering, vol. 10, no. 3, pp. 235-249, May. 2018.
[28] D. Lee, S.J. Lee and Y.J. Seo, "Application of recent developments in deep learning to ANN-based automatic berthing systems," International Journal of Engineering and Technology Innovation, vol. 10, no. 1, pp. 75-90, Jan. 2020.
[29] N. Mizuno and R. Kuboshima "Implementation and evaluation of non-linear optimal feedback control for ship's automatic berthing by recurrent neural network," IFAC-PapersOnLine, vol. 52, no. 21, pp. 91-96, Sep. 2019.
[30] E.L.H. Rørvik, "Automatic docking of an autonomous surface vessel," Master thesis. Norwegian University of Science and Technology (NTNU), Feb. 2020.
[31] CyberKeel, "Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas," NCC Group Publication, Oct. 2014.
[32] M. Guri, G. Kedma, A. Kachlon and Y. Elovici, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), pp. 58-67, Oct. 2014.
[33] J. Wagstaff, "All at sea: global shipping fleet exposed to hacking threat," Reuters, Apr. 24. 2014.
[34] J. Coffed, "The threat of gps jamming: The risk to an information utility," Report of EXELIS, Feb. 2014
[35] D. Schmidt, K. Radke, S. Camtepe, E. Foo and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," ACM Computing Surveys (CSUR), vol. 48, no. 4, pp. 1-31, May. 2016.
[36] K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, pp. 1-8, June. 2018.
[37] A. Costin, "Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations," Proceedings of the 6th international workshop on trustworthy embedded devices, pp. 45-54, Oct. 2016.
[38] C. Heffner, "Exploiting surveillance cameras like a hollywood hacker," Black Hat USA 2013, Aug. 2013.
[39] A. Costin, "Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations," Proceedings of the 6th international workshop on trustworthy embedded devices, pp. 45-54, Oct. 2016.
[40] B. Muthusenthil and H.S. Kim, "CCTV Surveillance System, attacks

and design goals," International Journal of Electrical and Computer Engineering (IJECE), vol. 8, no. 4, pp. 2072-2082, Aug. 2018.
[41] R. Santamarta, "Maritime security: Hacking into a voyage data recorder (VDR)," IOActive [Online], Dec. 2015.
[42] J. Wang and S.M. Zhang, "Management of human error in shipping operations," Professional safety, vol. 45, no. 10, pp. 23-28. Oct. 2000.
[43] M.S. Zaghloul, "Online ship control system using Supervisory Control and Data Acquisition (SCADA)," International Journal of Computer Science and Application, vol. 3, no. 1, pp. 6-10, Feb. 2014.
[44] R. Santamarta, "SATCOM terminals: Hacking by air, sea, and land," BlackHat USA 2014. Aug. 2014.
[45] BIMCO. The Guidelines on Cyber Security Onboard Ships, Version 4, BIMCO, Dec. 2020.
[46] Y. Yao, H. Li, H. Zheng and B.Y. Zhao, "Latent backdoor attacks on deep neural networks," Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 2041-2055, Nov. 2019.
[47] I.J. Goodfellow, J. Shlens and C. Szegedy, "Explaining and harnessing adversarial examples," arXiv preprint arXiv:1412.6572, Mar. 2015.
[48] M. Fredrikson, S. Jha and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, pp. 1322-1333, Oct. 2015.
[49] K.D. Jones, K. Tam and M. Papadaki, "Threats and impacts in maritime cyber security," Engineering & Technology Reference, Apr. 2016.
[50] K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, pp. 1-8, June. 2018.
[51] S.J. Lee, H.C. Lee, H.H. Song, H.S. Jeon and T.H. Im, "Comparative Analysis of CNN Deep Learning Model Performance Based on Quantification Application for High-Speed Marine Object Classification," Journal of Internet Computing and Services (JICS), 22(2), pp. 59-68, Feb. 2021.
[52] W. Jiang, H. Li, S. Liu, X. Luo and R. Lu, "Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles," IEEE transactions on vehicular technology, vol. 69 no. 4, pp. 4439-4449. Apr. 2020.
[53] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao and D. Song, "Robust physical-world attacks on deep learning visual classification," Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1625-1634, Dec. 2018.
[54] I. Evtimov, K. Eykholt, E. Fernandes, T. Kohno, B. Li, A. Prakash, and D. Song, "Robust physical-world attacks on machine learning models," arXiv preprint arXiv:1707.08945, vol. 2, no. 3:4, Apr. 2018.
[55] D. Qiao, G. Liu, T. Lv, W. Li and J. Zhang, "Marine vision-based situational awareness using discriminative deep learning: A survey," Journal of Marine Science and Engineering, vol. 9, no. 4:397, Apr. 2021.

[56] G. Kavallieratos, V. Diamantopoulou, and K. S. Katsikas, "Shipping 4.0: Security requirements for the cyber-enabled ship," IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6617-6625, Feb. 2020.

[57] M. Caprolu, R. Di Pietro, S. Raponi, S. Sciancalepore and P. Tedeschi, "Vessels cybersecurity: Issues, challenges, and the road ahead," IEEE Communications Magazine, vol. 58, no. 6, pp. 90-96, June. 2020.

[58] A. Goudosis and S. Katsikas, "Secure AIS with identity-based authentication and encryption," 2020

[59] Y. Takefuji, "Connected vehicle security vulnerabilities [commentary]," IEEE Technology and Society Magazine, vol. 37, no. 1, pp. 15-18. Mar. 2018.

[60] D.S. Fowler, A.T. Le and C. Maple, "LiDAR Sensor Security of a Driverless Pod," May. 2021.

[61] J. Petit, B. Stottelaar, M. Feiri and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," Black Hat Europe, Nov. 2015.

[62] A. Levine and S. Feizi, "Deep partition aggregation: Provable defense against general poisoning attacks," arXiv preprint arXiv:2006.14768. Mar. 2021.

[63] G. Apruzzese, M. Andreolini, M. Marchetti, V.G. Colacino and G. Russo, "AppCon: Mitigating evasion attacks to ML cyber detectors," Symmetry, vol. 12, no. 4, pp. 653, Apr. 2020.

[64] K.D. Gupta, D. Dasgupta and Z. Akhtar, "Applicability issues of evasion-based adversarial attacks and mitigation techniques," In 2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1506-1515, Dec. 2020.

[65] R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle," IEEE Access, vol. 7, pp. 138018-138031, Sep. 2019.

〈저자소개〉

유 지 운 (Ji-Woon Yoo) 정회원
2017년 2월: 안양대학교 컴퓨터공학과 졸업
2021년 3월~현재: 고려대학교 정보보호대학원 융합보안학과 석사과정
2018년 4월~현재: (주)디에스랩컴퍼니 연구원
〈관심분야〉 해양 사이버보안, IT융합, 시스템 및 네트워크 보안, AI보안

조 용 현(Yong-Hyun Jo) 종신회원
2004년 8월: 경희대학교 졸업
2007년 2월: 아주대학교 정보통신대학원 석사
2022년 2월: 고려대학교 정보보호대학원 박사
2002년~2007년: 육군중앙수사단 사이버범죄수사/디지털증거분석 수사관
2009년~2014년: 비씨카드 정보보안실, 신한카드 정보보호팀
〈관심분야〉 해양 사이버보안, 디지털 포렌식, 사고대응, 융합보안, 사이버범죄대응

차 영 균 (Young-Kyun Cha) 종신회원
1989년 2월: 고려대학교 수학과 졸업
1992년 6월: 고려대학교 대학원 석사
2012년 8월: 고려대학교 정보보호대학원 박사
2018년~현재: 고려대학교 정보보호대학원 연구교수
〈관심분야〉 융합보안, 암호학, 물리보안, 금융보안, 정보보호 정책