머신러닝 기반 선박 AIS IDS 설계 및 구현

양승권, 임성빈, 이병천, 최한림, 임정묵
중부대학교

Design and Implementation of Machine Learning-based AIS IDS for Maritime Vessels

Seungwon Yang, Sungbin Im, Byungchun Lee, Hanrim Choi, Jeongmook Im
Joongbu University

요약 : 본 연구는 AIS Spoofing 공격을 탐지하기 위한 머신러닝 기반 IDS를 설계 및 구현한다. OpenCPN 플러그인 환경에서 AIS AIVDM 메시지를 실시간 수집하고, 선박 시계열 데이터를 기반으로 이상 탐지를 수행한다. LSTM Autoencoder를 적용하여 정상 항적 패턴을 학습하고, 복원 오차(MSE)를 기준으로 이상 여부를 판단한다. Marine Cadastre AIS 데이터를 활용하여 비지도 학습 방식으로 모델을 구성하였으며, 다양한 항적 기반 공격 시나리오를 통해 성능을 검증하였다. 실험 결과, 속도 이상 및 위치 점프 기반 spoofing 시나리오에서 높은 이상 탐지 성능을 확인하였다.

Key Words : AIS Spoofing, AIS IDS, Maritime Cybersecurity, LSTM Autoencoder

1. 서 론

현대 선박은 GPS, AIS, ECDIS 등 다양한 디지털 항해 장비를 탑재하고 있으며, IT/OT 융합에 따라 외부 신호 의존도가 지속적으로 증가하고 있다. 특히 선박 내 항법 시스템은 NMEA 기반 네트워크로 확장되면서 외부 신호 위·변조에 대한 보안 위협이 증가하고 있다.

최근 중동 및 동유럽 해역을 중심으로 GNSS Jamming 및 AIS Spoofing 사례가 지속적으로 발생하고 있으며, 이는 항로 왜곡, 위치 오인, 충돌 사고 등 심각한 항해 안전 문제를 야기한다. 대표적으로 중동 해역에서는 GNSS 교란으로 인해 선박 위치 정보 이상 현상이 지속적으로 보고되고 있다.

또한 IMO의 MSC.428(98)과 IACS UR E26/E27 등 국제 규정이 강화되며 선박 사이버보안 관리가 의무화되고 있다. 이에 따라 AIS 신호 기반 이상 탐지 시스템의 필요성이 증대되고 있다.

본 연구에서는 AIS Spoofing 공격을 탐지하기 위한 머신러닝 기반 AIS IDS(Intrusion Detection System)를 설계 및 구현하였다. 본 시스템은 OpenCPN 플러그인 형태로 개발되어 실제 항해 환경과 유사한 GUI 환경에서 이상 신호를 시각적으로 탐지할 수 있도록 구성하였다.

2. 관련 연구 및 산업 동향

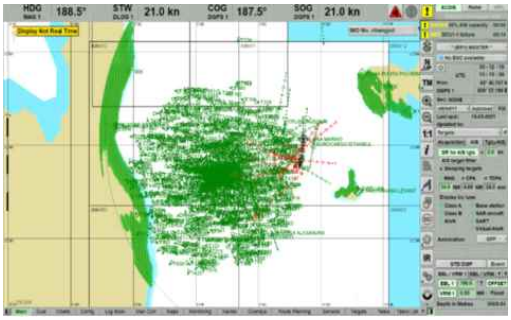
최근 해사 분야에서는 자율운항선박(MASS, Maritime Autonomous Surface Ship)과 스마트 선박 기술 발전에 따라 AIS 및 항법 시스템 보안 연구가 활발히 진행되고 있다. 특히 AIS spoofing, GNSS jamming, 항적 변조 등 항법 데이터 신뢰성 문제에 대한 연구가 증가하는 추세이다.

국내에서는 한국인터넷진흥원(KISA), 한국선급(KR) 등을 중심으로 IMO MSC.428(98), IACS UR E26/E27 대응을 위한 선박 사이버보안 연구가 진행되고 있다. 주요 연구 방향은 선박 네트워크 분리, 로그 기반 이상행위 분석, ECDIS 보안 강화, 보안 관제 체계 구축 등이다.

해외에서는 AIS 데이터와 위성 이미지, 레이더, GNSS 정보를 함께 분석하는 다중 센서 기반 연구가 활발히 수행되고 있다. 또한 머신러닝 기반 항적 분석을 통해 비정상 선박 이동 패턴을 탐지하거나, 항로 예측 기반 이상 탐지 모델을 적용하는 연구도 증가하고 있다.

3. 본 론

3.1 AIS Spoofing 공격 및 보안 문제



(그림 1) AIS Spoofing 피해 선박 화면

AIS는 선박의 위치, 속도, 식별 정보를 브로드캐스트 방식으로 송수신하는 시스템으로, AIVDM 규격 기반 평문 메시지를 사용한다. 이러한 구조는 인증 및 무결성 검증 기능이 부족하여 허위 위치·속도·식별 정보가 삽입된 가짜 신호를 무방비하게 수신할 수 있는 문제가 존재한다.

AIS Spoofing은 허위 정보를 삽입하여 주변 선박 및 항해 시스템의 상황 인식을 왜곡하는 공격이다. 이는 운항 중단, 경제적 손실, 심각한 경우 선박 간 충돌 사고를 초래할 수 있다.

3.2 시스템 설계

본 연구의 전체 시스템은 크게 OpenCPN 기반 IDS 플러그인과 머신러닝 기반 이상 탐지 모듈로 구성된다.

3.2.1 OpenCPN AIS IDS 플러그인

OpenCPN은 오픈소스 ECS(Electronic Chart System) 소프트웨어로, 다양한 운영체제를 지원하며 플러그인 기능을 제공한다. 본 연구에서는 OpenCPN 플러그인 API를 활용하여 다음 기능을 구현하였다.

- AIVDM 메시지 수신
- MMSI별 시퀀스 데이터 저장
- 이상 탐지 결과 GUI 시각화
- 이상 탐지 로그 출력

이상 신호로 탐지된 객체는 GUI 상에서 시각적으로 구분되도록 표시되며, 로그 창에 MMSI가 출력된다.

3.2.2 머신러닝 기반 이상 탐지

학습 데이터는 Marine Cadastre에서 제공하는 AIS 데이터를 활용하였다. 해당 데이터셋은 별도의 레이블이 존재하지 않으므로 비지도 학습 기반 접근 방식을 적용하였다.

AIS 스푸핑 데이터는 실제 공격 사례 수집이 제한적이며, 정상·비정상 데이터를 명확히 구분한 공개 데이터셋이 부족하다. 따라서 정상 패턴을 학습하고 이로부터의 이탈 정도를 기준으로 이상 여부를 판단하는 비지도 학습 방식이 적합하다.

본 연구에서는 시계열 데이터 기반 이상 탐지를 위해 DCdetector와 TranAD 두 모델의 가중 앙상블을 적용하였다. DCdetector는 Transformer 기반 이중 어텐션 구조를 활용하여 정상 패턴과의 연관성 차이를 학습하며, TranAD는 Transformer 기반 오토인코더로 Self-Attention 메커니즘을 통해 시퀀스 내 장거리 의존성을 학습한다. 두 모델은 AIS 항적의 단기적 변화와 전역적 패턴을 상호 보완적으로 포착한다.

각 모델은 입력 시퀀스(길이 10, 피처 12개)를 인코딩한 후 동일한 shape로 재구성하며, 원본과 복원값 간의 평균 제곱 오차(MSE)를 이상 점수로 사용한다. 최종 이상 점수는 두 모델의 MSE를 가중 평균하여 산출하며, 사전에 정의된 임계값을 초과할 경우 해당 선박을 이상으로 판정한다.

$$score = 0.7 \times MSE_{DCdetector} + 0.3 \times MSE_{TranAD}$$

임계값은 정상 데이터 5,000개 시퀀스를 기준으로 오탐율 5%에 해당하는 재구성 오차로 자동 산출하였으며, 설정된 임계값은 0.000020이다.

3.3 실험 환경 구성

(Table 1) 환경 구성 표

항목	구성
HW	Linux 24.04 VM
SW	OpenCPN, Python 3.x

가상 시리얼 포트를 통해 OpenCPN에 위조

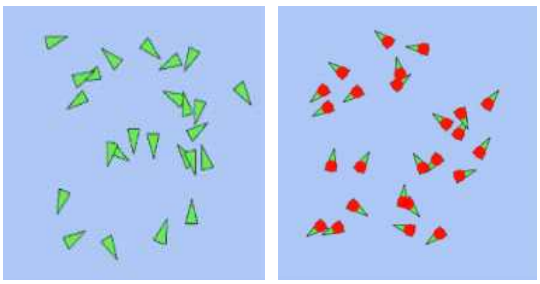
AIS 데이터를 입력하도록 구성하였다.

3.4 실험 수행 및 결과

(Table 2) 테스트 공격 종류

패턴	정의
A1	순간/주기적 속도 급증
A2	정박 상태 이동 이상
A3	COG/HDG 불일치
A4	위치 점프
B1	원형 정지 선박
B2	원형 순찰 선박
B3	직선 왕복 이동
B4	유사 실제 항로 + 속도 이상

공격 시나리오는 다음과 같이 구성하였다.



(그림 2,3) 공격 신호 화면 탐지 전/후

(Table 3) 실험 통계

Metric	Value
Average Reconstruction Error	0.000008
Normal Sequence MSE	0.000019
Attack Sequence MSE	0.000021
Average Detection Time	239 ms
Memory Usage	10.3 %

실험 결과, 정상 시퀀스(MSE: 0.000019)와 공격 시퀀스(MSE: 0.000021) 간 재구성 오차 차이가 확인되었으며, 설정된 임계값(0.000020)을 기준으로 이상 여부를 탐지할 수 있음을 검증하였다. 특히 위치 점프(탐지율 100%)와 속도 이상(탐지율 99.8%) 시나리오에서 높은 탐지 성능이 관측되었으며, DCdetector와 TranAD의 앙상블 적용을 통해 단일 모델 대비 보완적인 탐지가 가능함을 확인하였다.

평균 탐지 시간은 약 239ms 수준으로 측정되어 실시간 탐지 가능성을 확인하였다. 단, D1-LowSlow(저속 이동 위장) 시나리오의 경우 정상 패턴과의 구별이 어려워 탐지율 0%로 나타났으며, 이는 향후 개선이 필요한 한계점으로 분석된다.

4. 결론

본 연구에서는 AIS spoofing 공격에 대응하기 위한 머신러닝 기반 AIS IDS를 제안하였다. AIS 데이터의 시계열 특성을 고려하여 비지도 학습 기반 이상 탐지 모델을 적용하였으며, 실제 ECDIS 환경과 유사한 OpenCPN 플러그인 구조를 통해 실환경 적용 가능성을 검증하였다.

또한 속도 이상, 위치 점프, COG/Heading 불일치 등 다양한 공격 시나리오를 구성하여 이상 탐지 성능을 분석하였으며, AIS spoofing 공격에 대해 시계열 기반 이상 탐지 접근이 효과적으로 적용 가능함을 확인하였다.

본 연구는 기존 오프라인 분석 중심 AIS 보안 연구와 달리 실제 항해 시스템 환경과 연계 가능한 IDS 구조를 제시하였다는 점에서 의의를 가진다. 다만 실제 선박 환경에서는 해역, 선종, 통신 환경 등에 따라 데이터 특성이 달라질 수 있으므로, 다양한 환경 기반 추가 학습 및 검증이 필요하다.

향후 연구에서는 피처 최적화 및 앙상블 구조 고도화를 통해 탐지 성능을 개선하고, 서버-클라이언트 기반 실시간 분석 구조 및 다중 센서 연계 탐지 체계로 확장할 예정이다.

참고문헌

[1] IMO, “MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems,” 2017.

[2] IACS, “UR E26 Cyber Resilience of Ships,” 2022.

[3] IACS, “UR E27 Cyber Resilience of On-board Systems and Equipment,” 2022.

[4] Marine Cadastre, “Vessel Traffic Data,” 2025.

[5] Malhotra, P., et al., “LSTM-based Encoder-Decoder for Multi-sensor Anomaly Detection,” ICML Workshop, 2016.