군집 무인수상정 실시간 보안을 위한 DDS 및 GNN 기반 협력 침입 탐지 시스템 설계

백준혜[1], 이재민[2], 김동성*

금오공과대학교 IT융복합공학과[1,2,*]

{backjun03[1], ljmpaul[2], dskim*}@kumoh.ac.kr

Design of a Collaborative Intrusion Detection System Based on DDS and GNN for Real-Time Security in Swarm USVs

Jun-Hye Baek[1], Jae-Min Lee[2], and Dong-Seong Kim*

Kumoh National Institute of Technology Dept. of IT Convergence Eng.[1,2,*]

요 약

본 논문은 다수의 무인수상정(USV)이 협력하여 실시간으로 침입을 탐지하고 대응할 수 있는 분산형 협력 침입 탐지 시스템을 제안하였다. 각 USV는 실시간으로 데이터를 수집·분석하여 이상 행위를 탐지하고, 그 결과를 DDS 미들웨어를 통해 중앙 통제소 및 인접 USV들과 신속히 공유한다. 중앙 통제소는 다수의 USV로부터 수집된 탐지 결과를 통합 분석하여 판단 정확도를 향상시키며, 상황에 따라 대응 명령을 실시간으로 전파함으로써 신속한 군집 대응이 가능하도록 설계되었다. 본 시스템은 분산 탐지와 중앙 대응의 조화를 통해 해양 내 다양한 사이버 위협에 효과적으로 대응하며, 신뢰성과 확장성도 확보할 수 있다.

Ⅰ. 서 론

최근 해양 작전 및 경계 임무에 있어 군집 무인수상정(Unmanned Surface Vehicle, USV)의 활용 가능성이 크게 주목받고 있다. 이들은 자율 항해, 분산 경계, 원격 제어 등을 통해 유인 수상정 대비 작전 효율성과 안전성을 동시에 확보할 수 있다는 장점을 가진다. 특히 복수의 USV가 협력하여 해역을 감시하는 군집 시스템은 넓은 영역을 빠르게 커버할 수 있어 미래 해양 무인체계의 핵심으로 여겨진다[1]. 하지만 이러한 군집 USV는 대부분 실시간 네트워크 통신, 원격 명령 수신, onboard 자율 판단 등에 의존하기 때문에 사이버 공격에 매우 민감하다. 실제로 GPS 스푸핑, 악의적인 제어 명령 주입, 통신 재밍 등의 공격은 단일 USV뿐만 아니라 군집 전체의 임무 실패로 이어질 수 있다[2]. 따라서 군집 USV 운용 시 실시간 침입 탐지 기능은 필수적이며, 단순 중앙 집중형 보안 감시가 아닌 각 USV가 독립적으로 침입을 감지하고 협력하여 대응할 수 있는 구조가 요구된다. 최근에는 대규모 실시간 데이터 처리에 적합한 Kafka-Spark 기반의 분산 침입 탐지 구조가 주목받고 있으나, 이는 연산 자원이 제한된 군집형 USV 환경에서는 적용이 어려운 한계가 있다[3]. 반면, DDS(Data Distribution Service) 기반 통신은 중앙 중계 서버 없이도 노드 간 직접 메시지 전파를 지원하며, 고신뢰·저지연 특성 덕분에 군집 USV 간의 실시간 협력 보안 체계에 적합한 기술로 평가받고 있다[4][5].

이러한 기술적 흐름을 바탕으로 본 연구에서는 GNN(Graph Neural Network) 기반의 이상 탐지 모델과 DDS(Data Distribution Service) 기반의 경량 메시지 전파 체계를 결합하여, 각 USV가 로컬 데이터를 통해 침입을 판단하고, 이를 군집 전체 및 중앙 통제소와 실시간으로 공유할 수 있는 분산 침입 탐지 시스템을 제안한다.

Ⅱ. 기존 연구 분석 및 협력적 침입 탐지 시스템의 필요성

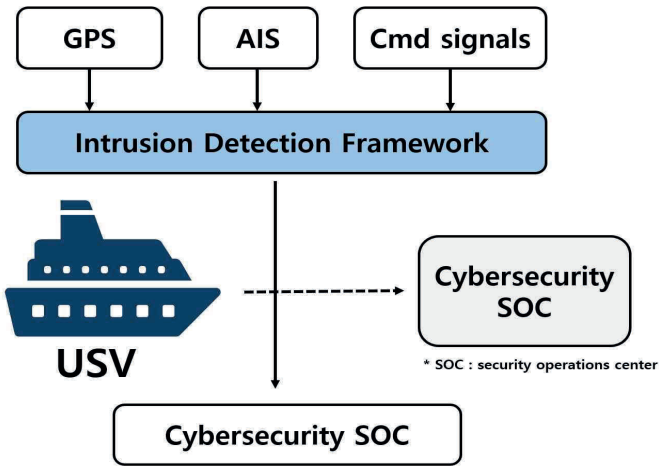

그림 1. 기존 중앙 집중형 침입 탐지 시스템

해양 자율 시스템의 사이버 위협에 대한 관심이 높아짐에 따라, 이를 방지하기 위한 다양한 침입 탐지 구조가 연구되고 있다. 기존 연구에서는 센서 및 항법 데이터 위변조, 원격 명령 탈취와 같은 공격 유형에 대응하기 위한 보안 프레임워크 설계와 보안 정책 제안이 이루어졌다. 일부 연구는 해상 사이버 보안 운영 센터(SOC)를 통해 중앙에서 데이터를 수집하고 판단하는 구조를 제시하였으나, 이는 군집 운용 상황처럼 각 노드의 실시간 협력과 자율적 대응이 요구되는 환경에서는 지연, 통신 의존도, 단일 장애점(Single Point of Failure)과 같은 구조적 한계를 가진다. 이러한 구조는 센서 데이터를 수집한 USV가 침입 여부를 스스로 판단하지 않고, 중앙 프레임워크에 탐지를 위임하며, 그 결과는 SOC를 통해 대응까지 일

괄 처리되는 중앙 집중형 방식이다. 그림 1은 이러한 탐지 흐름을 도식화한 것으로, USV는 데이터 수집만 수행하고, 모든 분석과 판단은 중앙에서 이루어지는 구조를 보여준다. 이러한 중앙 집중형 구조의 한계를 보완하고, 실시간 협력 및 자율적 판단이 가능한 군집 보안 체계를 구현하기 위해, 본 연구에서는 각 USV가 로컬 데이터를 기반으로 침입을 감지하고, 이를 DDS를 통해 군집 전체와 공유하는 GNN 기반 분산 침입 탐지 시스템을 제안한다.

Ⅲ. 제안하는 DDS 기반 무인수상정 협력 침입 탐지 및 대응 시스템

본 연구에서는 군집 무인수상정 환경에서의 실시간 협력 기반 보안을 실현하기 위해, 각 USV가 독립적으로 침입을 탐지하고, 탐지 결과를 군집 전체 및 중앙 통제소와 공유할 수 있는 경량 분산 침입 탐지 시스템을 제안한다. 제안 시스템은 USV 로컬 침입 탐지기, DDS 기반 메시지 전파 체계, 협력 기반 대응 구조 크게 세 가지 핵심 구성 요소로 이루어진다.

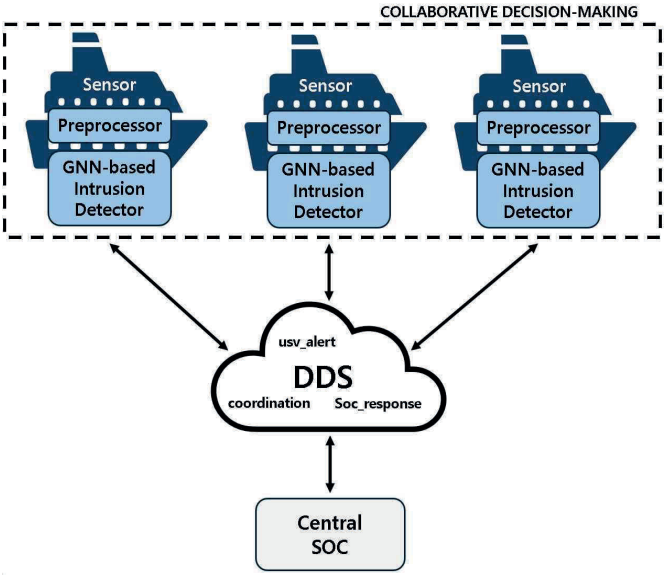

그림 2. DDS 및 GNN 기반 협력 침입 탐지 시스템

그림 2는 제안하는 시스템의 전체 구조를 나타낸다. 각 USV는 GPS, AIS, 명령 신호 등 자체 센서를 통해 외부 객체 및 통신 데이터를 수집한다. 수집된 원시 데이터는 전처리 모듈에서 정규화, 시간 정렬, 노이즈 제거 등의 처리를 거친다. 이후 각 객체의 궤적, 속도, 방향 변화 등의 정보가 벡터 형태의 노드 특성으로 변환되며, 객체 간 거리 및 행동 유사성 등을 기준으로 관계(엣지)가 설정된다. 이렇게 구성된 그래프 데이터는 GNN 기반 이상 탐지기로 입력되어, 각 객체의 상태뿐만 아니라 주변 객체들과의 관계 구조를 종합적으로 분석하여 이상 행동 여부를 판단한다. 이상 행동이 감지되면, 탐지기는 anomaly score 및 침입 유형 정보를 포함한 탐지 결과를 DDS 모듈로 전달한다. 그림 3은 제안 시스템에서 사용되는 DDS 토픽 및 토픽의 QoS 설정을 나타낸다.

Topic Name	Purpose	QoS Profile
usv_alert	침입 발생 시 군집 및 SOC에 경고 전파	Reliable, Low Latency
usv_status	현재 USV의 속도, 방향, 모드 등 상태 공유	Best Effort, Volatile
coordination	회피 기동, 리더 변경 등 협력 명령 공유	Reliable, History:1
soc_response	중앙 통제소의 대응 명령 전파	Reliable, Transient Local

그림 3. 제안 시스템의 DDS 토픽 정의 및 QoS 설정

각 USV는 usv_alert를 수신하면, 해당 객체에 대한 자율적 데이터 분석을 수행하여 본인 기준에서도 이상 징후가 감지되는지 확인한다. 일정 수 이상의 USV가 동일한 침입 판단을 내릴 경우, 해당 객체는 공동으로 침입자로 확정되며, 군집 내 coordination 토픽을 통해 즉각적인 대응이 전개된다. 예를 들어, 특정 객체가 비정상적인 궤적으로 침입하거나 명령 신호 위조가 의심될 경우, 해당 USV를 격리하거나 경로를 회피하고, 동시에 SOC에 경고가 전송되어 추가 대응이 가능해진다. 이러한 구조는 로컬 판단, 분산 공유, 중앙 통제가 유기적으로 연결된 구조로, 군집형 자율 시스템에 최적화된 침입 탐지 및 대응 체계를 제공한다.

Ⅴ. 결론 및 향후 계획

본 논문은 USV 기반 분산형 협력 침입 탐지 시스템 아키텍처를 제안하였으며, 실시간 이상 탐지와 대응 효율성 향상에 기여한다. 기존 단일 IDS 한계점을 극복하고, DDS 미들웨어와 Self-Learning IDS를 통합하여 보안성과 실시간성을 동시에 만족하는 시스템을 설계하였다.

향후 연구에서는 제안 시스템의 실현 가능성 검증을 위한 시뮬레이션 및 실제 적용 연구를 진행할 예정이며, 탐지 알고리즘의 고도화, 통신 네트워크 보안 강화 방안을 모색할 것이다.

ACKNOWLEDGMENT

본 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-학·석사연계ICT핵심인재양성 지원을 받아 수행된 연구(IITP-2025-RS-2022-00156394, 25%)와 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 지역지능화혁신인재양성사업(IITP-2025-RS-2020-II201612, 25%)과 2025년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(2018R1A6A1A03024003, 25%)과 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터사업의 연구결과로 수행되었음 (IITP-2025-RS-2024-00438430, 25%)

참 고 문 헌

[1] D.-H. Choi, D.-H. Kim, M.-S. Kim, B.-W. Choi, M.-C. Jung, and Y.-D. Choi, “Design and Implementation of Wireless Communication Topology for Swarm Unmanned Surface Vehicle(USV) Operation,” Journal of KIIT, Vol. 20, pp. 79 - 89, Aug. 2022.

[2] N. Tabish and C.-L. Tsai, “Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives,” IEEE Access, Vol. 12, pp. 17114 - 17131, Feb. 2024.

[3] K. M. K. Kumar, M. V. S. Reddy, K. Ullas, and S. M., “Distributed Intrusion Detection System using Kafka and Spark Streaming,” in Proceedings of the International Conference on Visual Analytics and Data Visualization (ICVADV-2025), pp. 302 - 307, May. 2025.

[4] S. El-Ferik, B. Almadani, and S. M. Elkhider, “Formation Control of Multi Unmanned Aerial Vehicle Systems Based on DDS Middleware,” IEEE Access, Vol. 8, pp. 44211 - 44218, Mar. 2020.

[5] W.-P. Nwadiugwu, D.-S. Kim, W. Ejaz, and A. Anpalagan, “MAD-DDS: Memory-efficient Automatic Discovery Data Distribution Service for Large-Scale Distributed Control Network,” IET Communications, pp. 1 - 15, Jun. 2023.