A Methodological Review of Anomaly Detection Methods for Maritime Hybrid Warfare Analysis

Julius Venskus [1,3], Robertas Jurkus [2,3], Povilas Treigys [2], Darius Drungilas[3]
1 Institute of Applied Mathematics, Vilnius University
2 Institute of Data Science and Digital Technologies, Vilnius University
3 Klaipeda University

Vital subsea infrastructure faces increasing threats from hybrid warfare. This paper reviews anomaly detection methods to distinguish between legitimate vessel activity and potential sabotage. We find that standard kinematic analysis generates unacceptably high false positive rates because raw data is often ambiguous. To be effective, detection methodologies must fuse vessel behavior with geospatial and economic context—specifically determining if an action is normal for a precise location. This review provides a roadmap for developing surveillance tools capable of protecting critical undersea assets by moving beyond simple motion tracking to contextual awareness.

Acknowledgements: This project has received funding from the Research Council of Lithuania (LMTLT), agreement No S-MIP-24-117.

Introduction and Context

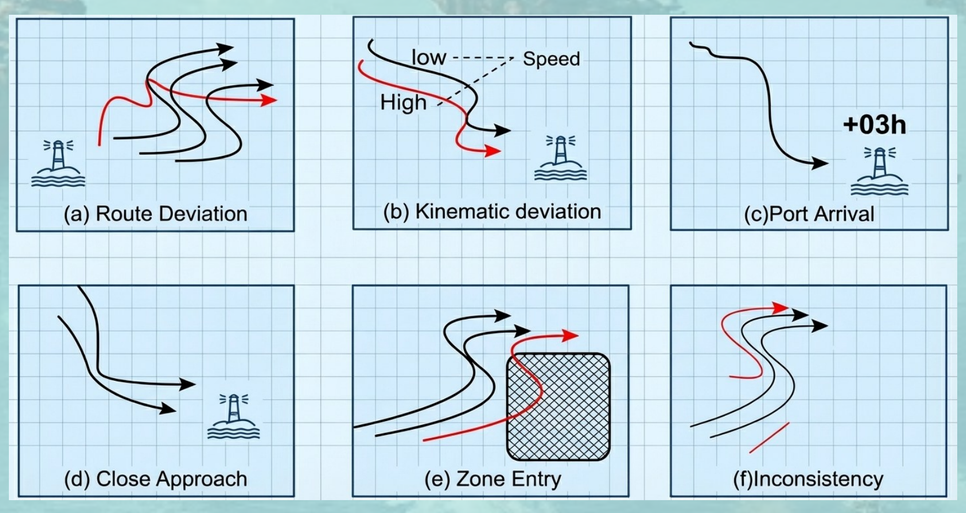
The Vulnerability of Subsea Assets

- The seabed hosts the "arteries" of the global economy: gas pipes, electrical interconnectors, and fiber-optic cables.
- Hybrid Warfare Threat: State-sponsored actors use "shadow fleets" (commercially flagged vessels) to conduct covert operations against these assets.
- The Sabotage Mechanism: Recent incidents involve vessels intentionally damaging infrastructure by dropping anchors or trawling gear.

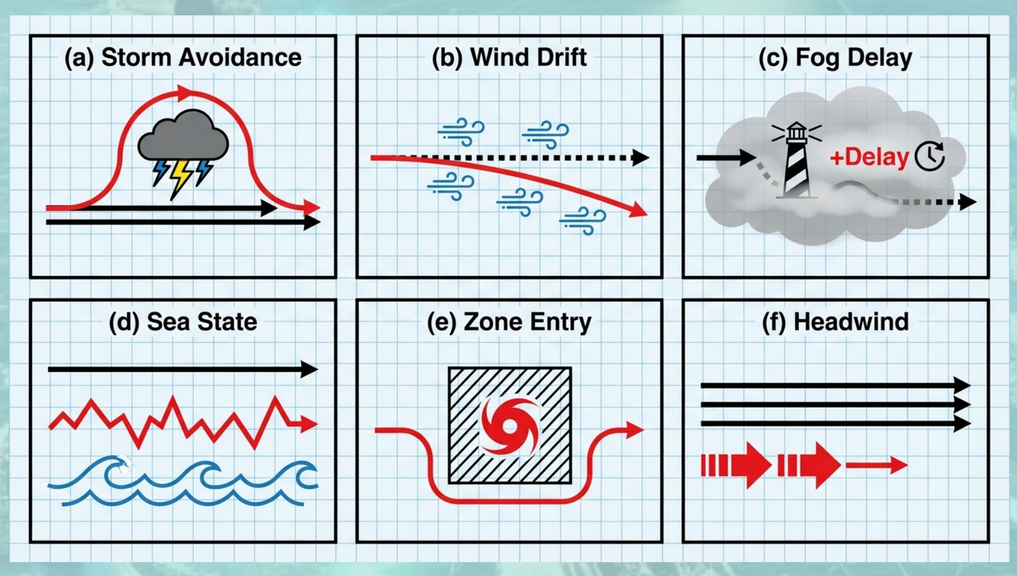
The Detection Challenge

- Ambiguity: Legitimate maritime behaviors (slowing down, loitering) look identical to preparation for sabotage in raw data.
- Goal: This paper reviews anomaly detection methods to distinguish between benign activity and hostile intent.

Anomaly types



Weather influence



The Analytical Challenge

- Kinematics are Insufficient: Standard algorithms analyzing speed and trajectory generate high rates of False Positives.
- The Context Gap: A ship stopping in a designated anchorage is normal; a ship stopping over a data cable is a threat.
- Requirement: Analysis must move from Simplistic Kinematics to Context-Aware.

A Multi-Domain Approach Methodology

Synthesizes methods that fuse data from three distinct scientific domains to achieve contextual awareness:

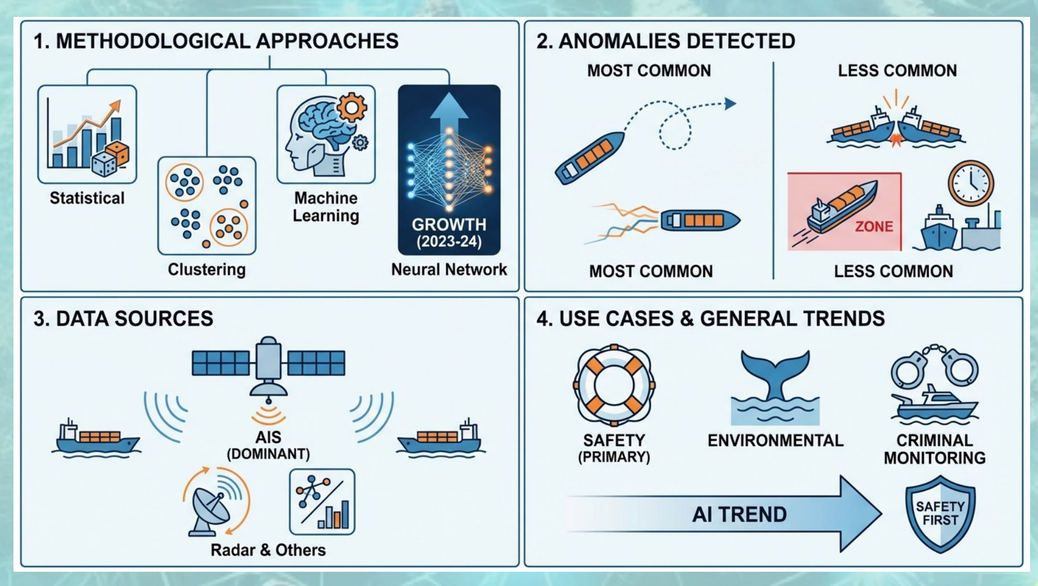
Geospatial & Oceanographic Models

- Map seabed topography and precise coordinates of critical infrastructure (CI).
- Determine physical proximity of vessels to vulnerable assets.

Behavioral & Economic Baselines

- Define "normative" activity for specific zones (e.g., fishing patterns, shipping lanes, designated anchorage).
- Filters out behavior that is economically or operationally logical, isolating outliers.
- C. Advanced Kinematic Analysis
- Detect subtle deviations in a vessel’s dynamic signature.
- Identifies non-standard maneuvering (e.g., drifting with intent vs. mechanical failure).

Anomaly Detection Methods



Conclusion & Roadmap

- Standard anomaly detection is inadequate for protecting subsea infrastructure against hybrid threats.
- This review provides a structured roadmap for developing Next-Generation Surveillance Tools.
- Future systems must integrate economic baselines and bathymetric data to reduce false alarms and identify true threats.