# Maritime Cybersecurity: Fusing Deep Learning and Kinematics to Detect Stealthy GPS Attacks

## Problem Statement and Goals

**The Problem:** Modern vessels rely on fragmented systems like GPS, AIS, and Internal Networks that operate in silos. Sophisticated cyberattacks, such as GPS spoofing, replay attacks, and meaconing, can exploit these "blind spots" by altering data in one system while appearing normal in another.

**The Gap:** Current detectors often fail because they lack context and integrated high-fidelity datasets. A physics detector might miss a subtle signal spoof, while a network detector might miss a physically impossible maneuver. Research is currently stalled by the lack of datasets that capture both the cyber signal and the physical reaction simultaneously.

**The Challenge:** Finding and integrating data sources was non-trivial due to Time-Domain Incompatibility. Internal NMEA logs update at 1Hz, while external AIS data arrives irregularly (15s to 5 mins). We overcame this by developing a custom kinematic upsampling algorithm. This allowed us to synthesize a hybrid dataset that is both physically plausible and synchronized across time domains.

**The Goal:** To develop an architecture that fuses internal network integrity using NMEA logs with external physical verification via Kinematics. We aim to eliminate blind spots by synthesizing a high-fidelity dataset that allows us to cross-reference cyber signals with physical reality.

## Approach

**Data Synthesis:**

- Because real-world attack data is scarce, we created a Hybrid Dataset.
- We took real Sea Trials data sampled at 15s intervals and upsampled it to the baseline of 1 Hz using a Dubins Path Kinematic Model to create a smooth, physically realistic "Ground Truth" trajectory. Repeated this with different data that we found.
- We then overlaid realistic sensor noise and attack signatures from the MARSIM simulation to train our models.

**Two-Layer Detection System:**

- **Layer 1 (Internal, LSTM Autoencoder):** A Deep Learning model analyzes internal network traffic from NMEA data. It learns "normal" patterns, such as timestamps and signal strength, and flags high reconstruction errors as anomalies.
- **Layer 2 (External, Physics Cross-Check):** A Kinematic Forecaster predicts where the ship should be based on its last known speed and heading. If the reported GPS position deviates significantly from the physics-based prediction, it flags a kinematic anomaly

## Results

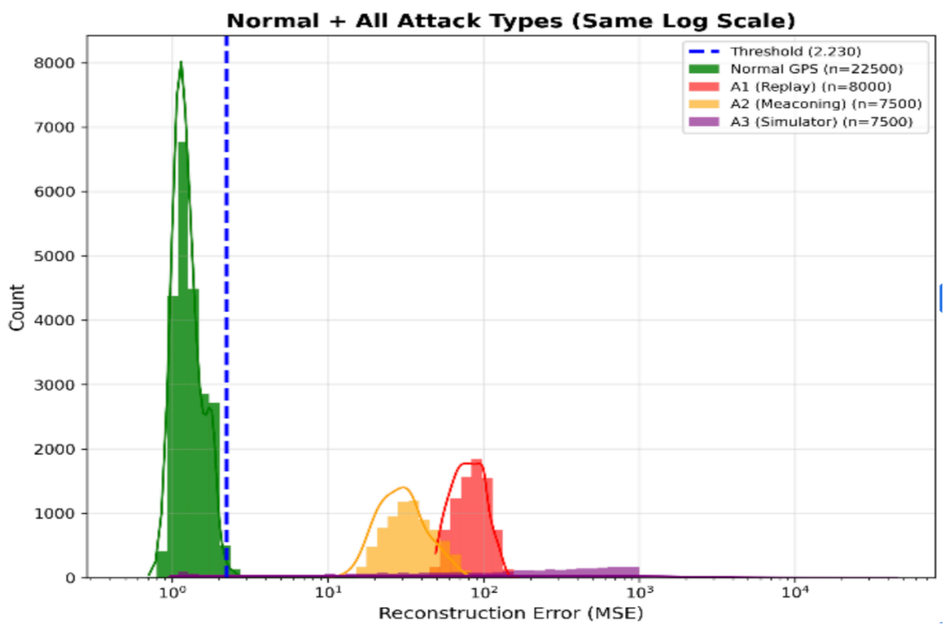



**Figure 1: LSTM Reconstruction Error Separation**

**The LSTM Autoencoder successfully distinguishes between benign voyages and cyberattacks. As shown in the histogram, "Normal" GPS data clusters with low reconstruction error (MSE), while attacks like Replay and Meaconing result in significantly higher error rates, allowing for a clear detection threshold.**

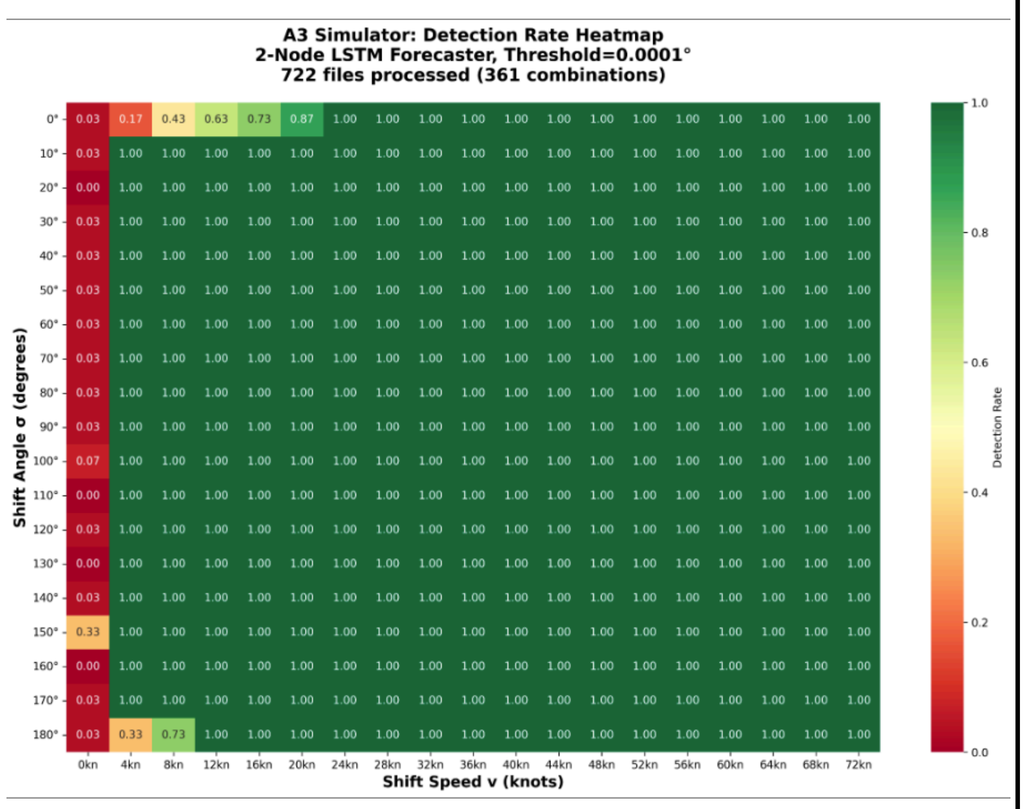



**Figure 2: Physics-Based Detection Heatmap**

**The Physics-based detector provides a robust second layer of defense. The heatmap demonstrates high detection rates for attacks that force the vessel into physically impossible maneuvers, such as high shift speeds or sharp turn angles. It identifies the specific "safe" zones where deviations are too small to impact navigation, proving the system effectively filters out noise while catching dangerous spoofing attempts.**

**By combining these two modalities, we achieve Asymmetric Resilience. Attackers must now perfectly spoof both the electromagnetic signal and the physical trajectory of the vessel simultaneously to remain undetected.**

**Future Work:** To tackle these remaining stealthy attacks, future work will expand the "Defense in Depth" architecture to include Optical and Radar data layers. This would cross-verify GPS inputs against visual landmarks, closing the loop on "Zero Trust" navigation. Distinguish from natural environmental factors like rough sea states.

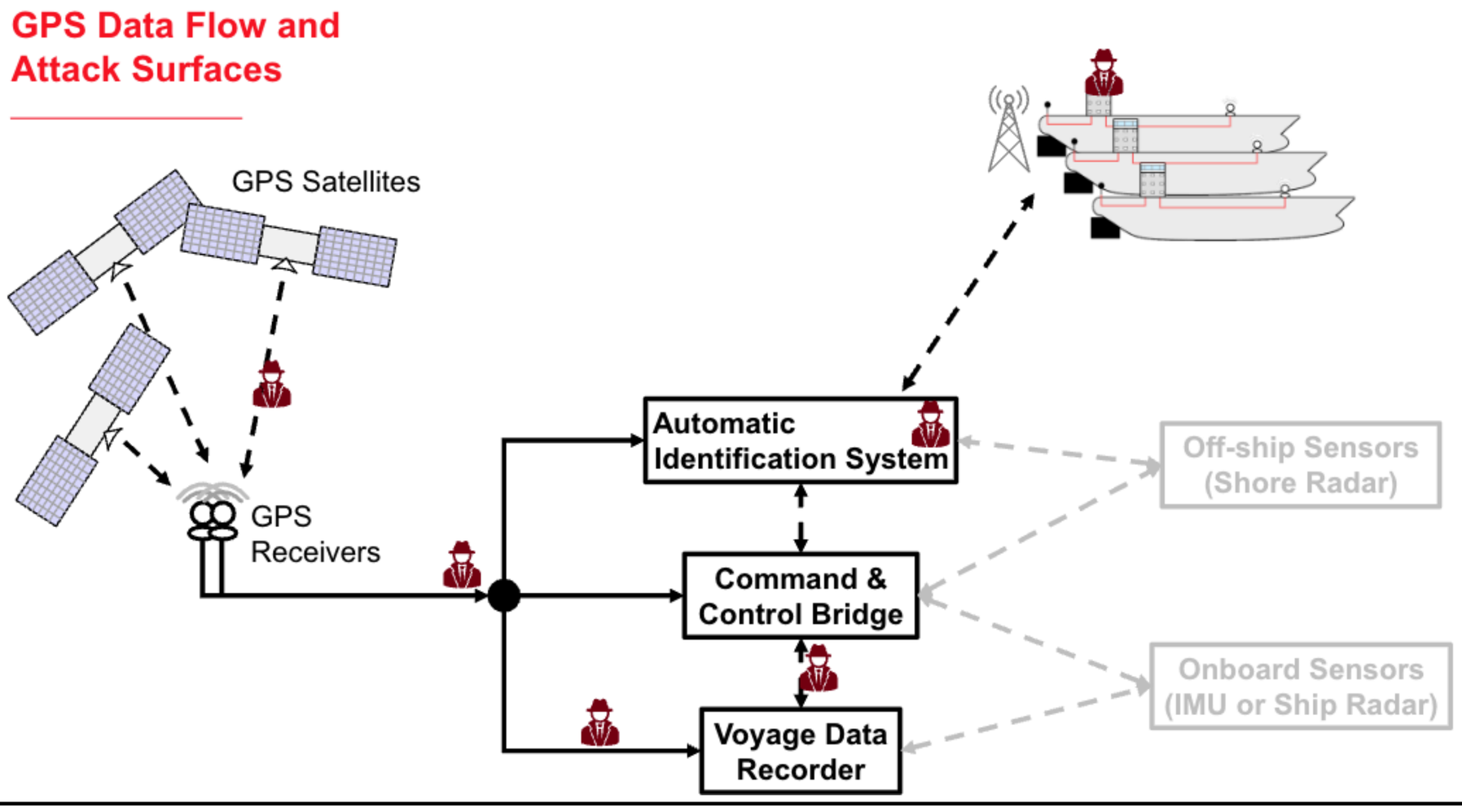
**Strahinja Janjusevic**
Massachusetts Institute of Technology

# Maritime Cybersecurity: Fusing Deep Learning and Kinematics to Detect Stealthy GPS Attacks

## Abstract

Global maritime logistics rely on commercial vessels using unauthenticated GPS and AIS signals, creating a critical vulnerability in strategic choke points where a spoofing attack could trigger catastrophic blockages. Current security systems fail to mitigate this risk because they operate in silos, creating blind spots where sophisticated attacks appear benign in one domain while violating constraints in another. Furthermore, the field is hindered by the lack of integrated datasets that capture both cyber signals and physical vessel responses simultaneously.

To bridge this gap, this research introduces a "Defense-in-Depth" architecture that fuses internal network integrity monitoring with external physical verification. We synthesized a high-fidelity hybrid dataset combining real-world commercial sea trials with a comprehensive suite of attack signatures, including signal replay, meaconing, and generated simulator spoofing. By combining an LSTM Autoencoder to detect anomalies in network parameters with a Physics-Based Kinematic Forecaster for trajectory validation, our multi-modal system successfully identifies stealthy threats that evade single-layer detectors. This approach correlates physical vessel dynamics with cyber signals to create an asymmetric disadvantage for adversaries, requiring them to perfectly falsify both digital signatures and physical reality to remain undetected.




**Strahinja Janjusevic**
Massachusetts Institute of Technology