Detecting Illegal, Unreported, and Unregulated Fishing through AIS Data and Machine Learning Approaches

Samuel Brown*, Danielle Katz†, Dana Korotovskikh‡, and Stephen Kullman§
*School of Data Science
University of Virginia, Charlottesville, VA
Email: sab3hzc@virginia.edu
†School of Data Science
University of Virginia, Charlottesville, VA
Email: ujj2wd@virginia.edu
‡School of Data Science
University of Virginia, Charlottesville, VA
Email: dk9nt@virginia.edu
§School of Data Science
University of Virginia, Charlottesville, VA
Email: sjk5cu@virginia.edu

***Abstract*—Illegal, unreported, and unregulated (IUU) fishing is a critical issue impacting the health of the marine ecosystem and global security. It is linked to crimes such as human trafficking and destroys local economies through over-fishing, collapsing species populations and throwing the ecosystem out of balance. A major contributor to this is the deceptive use of Automatic Identification System (AIS) beacons on fishing nets, buoys, or lines, to conceal illegal fishing hauls from local vessels and enforcement authorities. Enhancing the capacity to recognize fraudulent AIS devices, and predicting their operational areas of activity, is crucial for regulatory agencies aiming to reform the current state of fishing practices. This paper focuses on analyzing geospatial AIS data from Southeast Asia and provides three machine learning modelling approaches to aid in the detection of IUU fishing occurrences. We utilize semi-supervised classification, unsupervised clustering, and standard neural network models as approaches to identify irregular AIS beacons, suspected to be IUU fishing instances, based on device patterns and characteristics. For further exploration, we also conducted regional analysis of IUU fishing features to identify areas of suspected heightened illegal activity. Our results show that movement and positional features of AIS devices can serve as successful indicators, alongside machine learning techniques, for IUU detection. This research serves as foundational analysis to improve the field of IUU fishing using modelling techniques.**

***Index Terms*—IUU Fishing, Geospatial Data, Machine Learning, Clustering, ANN**

I. Introduction

Illegal, unreported, and unregulated (IUU) fishing is the activity of fishing outside of local and international rules and regulations. It is a widely defined term that includes activities such as contravening local fishery laws, falsifying reports to authorities, or fishing in protected waters outside a country's Economic Zone. With minimal barriers to entry and a profitable market, IUU fishing has grown to become a serious threat to the environment as well as economic security. Nearly half of the world's population relies on fish for a portion of their protein intake. Over-fishing affects every country, but especially those nations who are more reliant on the sea for resources. IUU fishing has been estimated to make up 15-30 percent of global annual catches, demonstrating its extreme prevalence [1].

It is not only an environmental problem but an economic one as well. IUU fishing is estimated to cost global economies anywhere from 10 to 23 billion dollars annually [2]. More troubling, IUU fishing is linked to global crimes such as drug and human trafficking. Poor and illiterate workers, promised with steady wages and work, find themselves trapped aboard these illegal vessels with little food, poor sanitation, and long, unpaid workdays. With both economic and ecological impacts, the need for improved IUU management is vital.

The problem is complex, spanning multiple jurisdictions with patchwork laws, if the laws are enforced to begin with. Solutions require cooperation between nations that may have opposing geopolitical goals. The emergence of Big Data has given nations tools to fight back. Fish, fresh or frozen, legally caught or otherwise, lose value as they age. Machine learning that can help predict suspected illegal activity can give port authorities motive to delay fish sales, eating away at profit margins.

This paper will focus on the characteristics of IUU fish-

ing that can be observed through Automatic Identification Systems (AIS) readings. This research began with exploring the relationships between AIS user data and illegal buoys or nets. We then attempted several machine learning models in an attempt to classify the AIS observations as legal or illegal. These results, in conjunction with regional analysis, serve as baseline methodologies to assist with IUU detection and regulation in Southeast Asia.

II. Background and Motivation

A. Automatic Identification Systems

Automatic Identification Systems are customary maritime monitoring systems that provide vessel information such as identity, position, and course data. These systems serve primarily for identification and collision avoidance purposes, but also supplement various regulatory work by maritime authorities. AIS devices are outfitted on both commercial vessels and small recreational vessels. These devices continuously transmit user data over routine intervals via ground-based or satellite systems. AIS data follows a standardized format which combines the unit's position and movement with user-defined programmable information. This programmable information includes sections such as Maritime Mobile Service Identity (MMSI) number, vessel name, destination, and cargo type [3].

B. IUU Activity with Nets and Buoys

IUU activity is known to be linked to the misuse of AIS devices in recent years. Although designed for regulation, fishermen are able to purchase these relatively inexpensive transponders and attach them to their fishing nets, buoys, and lines. In doing so, fishermen are able to disguise their fishing hauls as vessels, protecting them from maritime traffic that may disrupt them, and conceal them from ordinary detection. It also allows fisherman to conveniently drop their fishing nets and use AIS tracking information to return, and easily collect their protected hauls. These nefarious activities help facilitate over-fishing and provide easy workarounds for fisherman to avoid regulatory authorities.

C. Data Overview

The dataset for this research consisted of AIS transmissions recorded from September 2023 to November 2023. This data collection was restricted to only focus on the Southeast Asia region, specifically in the South China Sea and Sea of Japan. It consists of spatial, temporal, and user inputted data regarding a specific AIS device. Figure 1 provides an overview of the region of AIS transmissions that were used to conduct this research analysis.

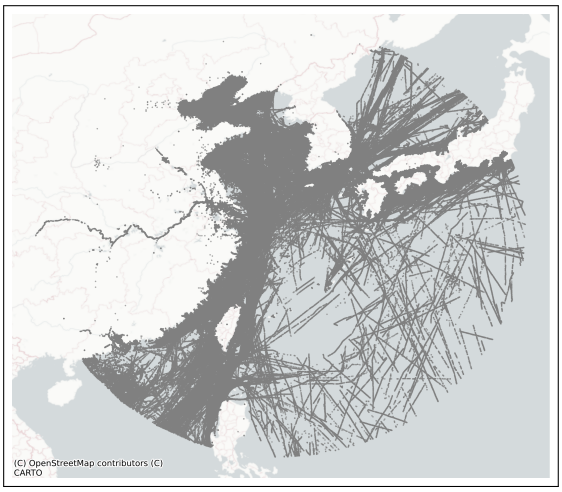

Fig. 1: Dataset Region of Interest

III. Pre-Processing and Approach

A. Net and Buoy Characteristics

In an effort to recognize suspicious AIS transponders resembling net or buoy use, we analyzed the devices' user-inputted data as well as positional information for identifying features. Suspicious user-inputted data can be reflected via the vessel name or MMSI value. We considered unconventional inputs to be flagged features for IUU fishing. These features adhere to the following assumptions:

- Vessel names including a battery percentage (digit followed by percent sign), or the phrases 'buoy' or 'net'
- MMSI values unequal to 9 digits

In addition to naming conventions, an AIS beacon's movement over time can also display characteristics of a fishing buoy or net. Similarly, if a device displayed these movement patterns, they were flagged for suspicious activity. In this process, the following assumptions are made:

- Devices which suddenly 'spawn' and whose first transmission is offshore (1 nautical mile off the coastline)
- Devices with unreasonably high calculated speeds (greater than 150 knots) are assumed to 'spoof' their data

The suspicious naming conventions listed are commonly recognized as indicators for illegal AIS use in this field of work. In this paper, naming convention indicators are aggregated with the aforementioned positional characteristics and categorized as red_flags for an AIS observation. Each unique AIS correspondence is designated with a red flag score ranging from 0 to 4. The red_flags scoring feature is used throughout this paper for model analysis.

Additionally, for the purpose of this research, the indicator for a bad AIS vessel name, net_name, is also used for model analysis, as it is commonly understood to be synonymous with illegal devices in the field of IUU fishing, and is seen as the 'strongest' of our red flag components.

B. Pseudo-Labels

Although the AIS dataset is unlabelled, for certain model approaches, pseudo-labels were developed in order to train our supervised and semi-supervised models. In these instances, a select set of the AIS observations that were

confident examples of illegal vessels or legal vessels were manually labelled based on specific red_flag criteria. Observations with a bad AIS vessel name indicator and a red_flag score of 3 or more, were labelled as 'illegal'. Observations with 0 red flags were labelled as 'legal'. The resulting pseudo-labels were applied to develop a subset of labelled data observations, which reflected a realistic spread. This dataset was then used to train the applicable models discussed.

C. Feature Development

In order to analyze each AIS beacon appropriately in all of our models, the data features were aggregated by trip of a unique device. In this instance, a trip represents the continuous period during which the AIS device is transmitting. Since AIS devices are mandated to be turned on during vessel use and traditionally turned off when in port or not in use, a trip is assumed to accurately reflect a devices activity over time. Additionally, if a device is turned off for over 4 hours, its subsequent data collection is then considered a separate trip.

After aggregating by trip, we processed the dataset to calculate scaled parameters for speed, heading, and spatial positioning. In order to observe the activity over a device's trip, these features were broken down to reflect the initial, median, maximum, and standard deviation values for each [4].

Due to computational limitations, the modeling considered a subset region of focus (between latitudes of 25° and 35° and longitudes of 120° and 130°) and trained on a primary dataset covering a continuous time period of approximately four days in September. In sections where a test set was required for analysis, a separate time period in October of approximately four days of data collection was utilized.

IV. Supervised Approaches

A. Semi-Supervised XGBoost

For this research, the dataset did not contain labelling that classifies a signal as a valid vessel or illegal net. However, the previously mentioned 'red flags' are considered to be very strong indicators of nets or buoys and can be synonymous with ground truth data. Using this principle, with a small sample of pseudo-labels and a majority unlabelled data, a semi-supervised modeling approach was considered. A semi-supervised model is unique in that it can handle both labelled and unlabelled data, and trains its respective model based on confident observations.

This approach uses a classifier to train on the small labelled dataset. Here, we use XGBoost as the selected classifier. XGBoost is a form of Gradient-Boosted Decision Trees known for its speed and accuracy. The XGBoost model receives the pre-processed training data, described in Section III, where a vessel's trip was described using several engineered features. Once processed, this trained model then ingests the remaining unlabelled data and produces new classification predictions. From these probabilities the model takes the most confident observations on either end and reclassifies them as a legal or illegal vessel, and appends them to the labelled dataset. This classification is based on set thresholds. A prediction with $p \leq 0.015$ is labelled as legal and $p \geq 0.985$ is labelled as illegal. This process is iterated five times until there are no remaining confident unlabelled observations to be classified.

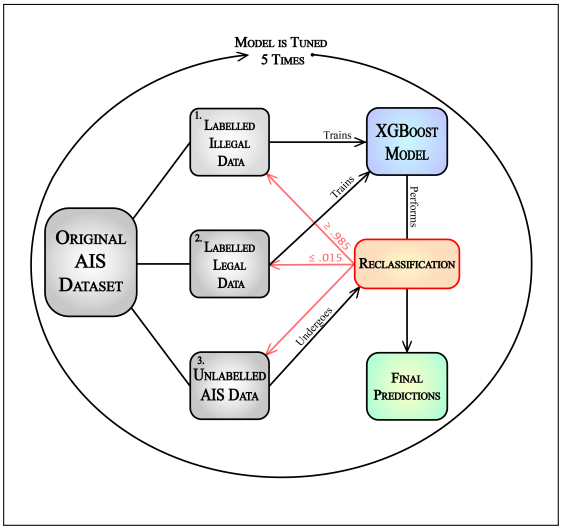

Fig. 2: Semi-Supervised Model Workflow

B. Artificial Neural Network

An artificial neural network (ANN) offered us an alternative and very simple way of modeling the pre-processed data. In this fully supervised model approach we manually labelled all observations in the dataset based on its red_flag scoring. Using these labels to train on, the model outputs a binary prediction. Our ANN framework consisted of two linear layers with a Parametric Rectified Linear Unit (PReLU) activation function in the hidden layer, and a final sigmoid activation function as the output layer. We tested several combinations of learning rates and hidden node parameters to optimize learning.

C. Semi-Supervised Artificial Neural Network

The semi-supervised ANN approach followed the same framework and parameters described previously. However, in this iteration, it followed the same methodology as the XGBoost model. The semi-supervised model trains on a small subset of confidently labelled observations and iteratively, the model classifies the remaining unlabelled observations based on the set classification thresholds.

D. Model Results

Both ANN models were tested with learning rates of [0.005, 0.001, 0.0001, 0.00005] and [10, 15, 20] hidden nodes. The best results were achieved with a learning rate of 0.005 and 15 nodes. These parameters were specified to build the final test models for each.

TABLE I: Final Model Parameters

Model	Learning Rate	Hidden Nodes
Semi-supervised XGBoost	0.03	NA
Semi-supervised ANN	0.005	15
ANN	0.005	15

For the semi-supervised models, each utilized the same classification thresholds mentioned previously. Both iterated through this reclassification process five times for standardization.

The models were tested on the pseudo-labeled observations within our test set. Amongst all final classification models, the semi-supervised XGBoost achieved the overall top performance. With superior test accuracy and specificity, and high test sensitivity, the XGBoost model appeared to classify the AIS dataset best. To further explore its methodology, we analyzed the XGBoost feature importance scores. The longitude, latitude, and average speed parameters received the highest feature importance scores, indicating they had the largest impact on the model.

TABLE II: Model Performance Results

Model	Test Accuracy	TPR	TNR
Semi-supervised XGBoost	0.891	0.915	0.848
Semi-supervised ANN	0.879	0.900	0.842
ANN	0.867	0.907	0.801

The resulting predictions of the semi-supervised XGBoost model on our test set can be seen in Figure 3. The predicted probability of each observation was mapped onto the region of interest. Orange and red sections indicated areas in which the model observed higher averages of illegal net activity during the tested time period.

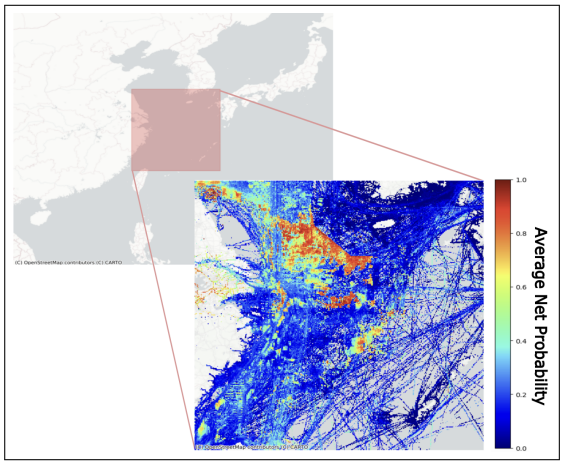

Fig. 3: Semi-Supervised XGBoost Prediction Results

V. Unsupervised Approach

In an alternative approach, we treated the dataset as truly unlabelled. We applied an unsupervised clustering model in this instance to identify groups of AIS observations with common patterns of performance in an effort to recognize true vessels from nets or buoys. For the purpose of this exploration, we used Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN). While traditional clustering methods such as K-means were utilized for baseline analysis, HDBSCAN provided a more powerful, tailored clustering approach for the dataset. Unlike other methods, HDBSCAN has the ability to handle both dense and sparse clusters. This was necessary for the large AIS dataset with varying densities of true vessels, nets, and buoys throughout. Another key aspect of HDBSCAN is that it handles noisy observations well, designating them in their own cluster '-1'. For these reasons, HDBSCAN served as the most appropriate clustering method for this research.

Similar to the other model instances, the HDBSCAN assessed the pre-processed AIS data including positional, speed, distance travelled, and trip elements.

A. HDBSCAN

The HDBSCAN model was designed knowing that true vessels significantly outnumber illegal AIS observations. HDBSCAN uniquely allows users to intuitively design the model. Specifically, for this model we chose to develop clusters with the smallest group size to be 5 points. This parameter, the $min\_cluster\_size$, we felt was representative of the resulting groupings we desired and served as a realistic benchmark for illegal net identification. Additionally, since we knew that some groups with fewer observations would still be valuable for analysis, we utilized the $cluster\_selection\_epsilon$ parameter. This parameter helped to avoid a significant amount of micro-clusters. Having this value set to 0.5 initiated DBSCAN's epsilon feature, which allowed us to avoid breaking up clusters that were less than 0.5 units apart. Lastly, we chose to not apply a hard computation for $min\_samples$ and allowed the HDBSCAN to use its default settings.

With these parameters, we ran our first HDBSCAN model with the scaled features previously mentioned. We analyzed the resulting model cluster assignments by the distribution of 'red flag' scores in each group. Using a similar iterative technique conducted in previous research on illegal vessel interactions, we calculated the average red flag score per cluster [5]. These averages were then added to each respective red flag score in the original pre-processed dataset, based on the cluster in which the observation fell. The model data was again scaled and rerun with HDBSCAN a second time. In this iteration, we included the updated red flag score feature and specified a minimum cluster size of 100 points, in an attempt to improve the model's ability to cluster illegal devices.

B. Clustering Results

The resulting model developed 10 cluster groups of varying densities. To analyze the results, we cross referenced the bad AIS name feature, net_name, and assessed its distribution throughout each cluster. As seen in Figure 4, the resulting clusters identified three groups primarily containing bad AIS names. These results suggest that the three clusters best capture the suspected illegal vessels.

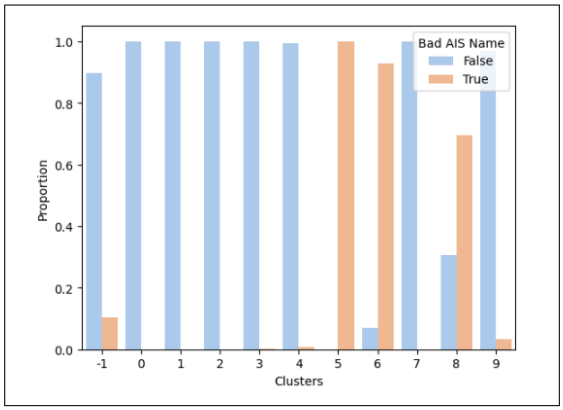

Fig. 4: HDBSCAN Cluster Analysis Using Bad AIS Names

Figure 4 displays the proportion of each cluster based on their designation. Of note, the collection of illegal observations grouped in clusters 5, 6, and 8 captured ∼95% of all trips with bad AIS names and made up approximately 36.2% of the total trips within the pre-processed dataset.

These clustering results show that AIS positional features can also serve as potentially strong indicators of IUU net or buoy activity. Additionally, the three clusters also captured approximately 1% of the dataset with valid AIS names. This may suggest that the developed features, such as $spawn\_offshore$ and $spoof$, can serve as valid indicators of IUU activity that cannot be detected with naming conventions alone.

VI. Regional Analysis

For our regional analysis, we leveraged the pre-existing flagging features to examine areas of elevated illegal AIS activity. By overlaying a grid over our area of focus and using data manipulation techniques, we color-coded cells based on 'hotspot' activity [6]. The map visual allowed us to discern areas of heightened illegal activity and track their development over time.

A. Data Preparation

To begin, we processed our data in a similar way to our previous models; we generated the same four flagging variables for each AIS signal. These 'red flags' include: net_name, $mmsi\_length$, $spawn\_offshore$, and $spoof$. Each AIS signal was assigned a total count of red_flags ranging from 0 to 4. A value of 4 indicated a high likelihood that the AIS signal belongs to an illegal device.

B. GeoPandas and Grid Work

By transforming our data-frame into a GeoDataFrame, we generated a geometry column that mapped each AIS signal's latitude and longitude coordinates to the geographic coordinate system ESPG:4326 [7]. Our AIS signals were geographically confined between $107°$ to $142°$ longitude, and $14°$ to $44°$ latitude. Using these boundaries, we created a grid composed of $0.1°$ by $0.1°$ cells, roughly equivalent to 6x6 miles [8]. Through merging this grid with our AIS data, we positioned each AIS signal within its corresponding grid cell location within Southeast Asia.

C. Plotting

A hot_score was calculated for each grid cell derived from the total number of red_flags (per unique vessel), divided by the total count of unique vessels (based on MMSIs). Elevated hot_score values indicate a higher concentration of red flags relative to the number of unique vessels, whereas lower scores signify fewer red flags in relation to unique vessels. Using these scores, we assigned a color gradient to each grid cell [7]; this allowed us to visualize the distribution of hotspots on a map of Southeast Asia for a specific hour:

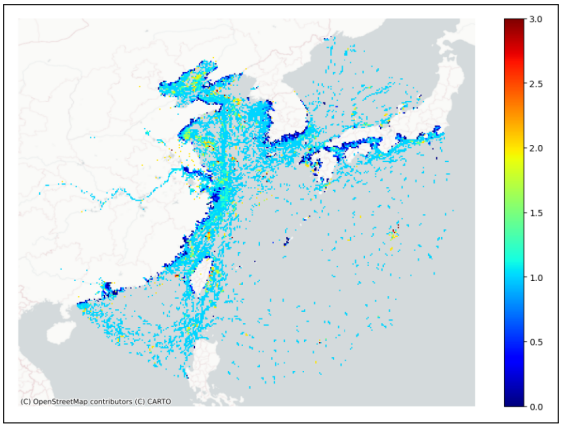

Fig. 5: Visualization of Hotspots: September 1st, Hour 1

Condensing our code into functions, we were able to speed up the process of analyzing multiple datasets to identify unique hotspot scores for each grid cell–on an hourly basis. These scores were aggregated to obtain a total hotspot score, allowing us to see which locations had the highest frequency of illegal devices over the course of a full day. The aggregated hotspot scores for September 1st–all 24 hours–is shown in Figure 6.

D. Results

Using this grid-based analysis, we were able to pinpoint distinct areas around Southeast Asia showing a higher frequency of suspicious vessel activity while being much more computationally efficient than any of the models specified above. These flagged occurrences serve as strong indicators of illegal activity. Through the specificity of 6x6 mile cells,

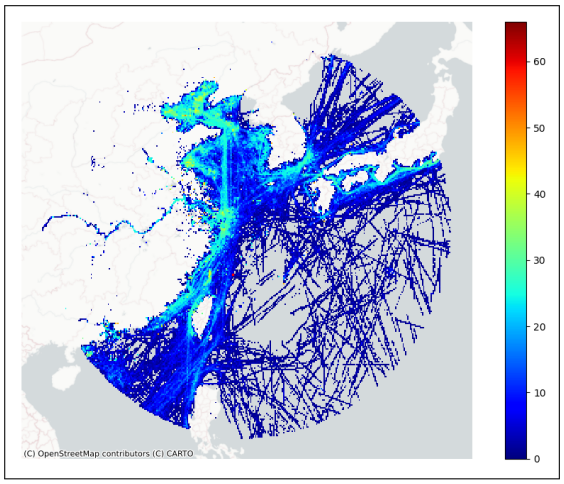

Fig. 6: Visualization of Hotspots: September 1st, Day 1

we identified significant spots of illicit activity that may warrant targeted intervention.

VII. Future Work

While our models were able to successfully detect suggestive patterns of IUU nets and buoys, this research had notable limitations. Our data and modelling was only applied to a specific area of interest in Southeast Asia. In other regions, IUU fishing may behave differently, with unique movement or user characteristics, leaving our engineered features for red flags insignificant and inapplicable. To supplement, this research relies heavily on the assumption that nonstandard naming conventions are directly indicative of nefarious AIS devices. Those assumptions may not always hold true. This lack of validated identifiers may have the potential for misrepresentation. In turn, we propose several opportunities for future work. We suggest this research be extended to process a longer duration of AIS data, as well as expanded to alternative, larger regions of interest. Additionally, we recommend further development of the neural network approaches; specifically, to approach the research with more complex neural network architectures, with supplemental layers and hidden nodes to optimize learning performance. Alternatively, we suggest further exploration into a recurrent neural network (RNN) which uses the AIS temporal data, then processes with positional features. Lastly, pending the research application, we suggest exploring a case study with true labelled AIS observations in conjunction with these approaches.

Acknowledgments

We would like to express our thanks to GA-CCRi, specifically, Tara Valladares and Rebecca DeSipio, for providing the dataset for this research as well as their subject matter expertise throughout. We would also like to extend our gratitude to the School of Data Science and our mentor, Heman Shakeri, for giving us the opportunity and tools to explore this research.

References

[1] "Global Implications of Illegal, Unreported, and Unregulated (IUU) Fishing," Sep. 2016. [Online]. Available: https://irp.fas.org/nic/fishing.pdf

[2] U. Nations, "International day against illegal fishing." [Online]. Available: https://www.un.org/en/observances/end-illegal-fishing-day

[3] "AIS (Automatic Identification System) Overview." [Online]. Available: https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview.aspx

[4] Z. Yan, X. Song, H. Zhong, L. Yang, and Y. Wang, "Ship Classification and Anomaly Detection Based on Spaceborne AIS Data Considering Behavior Characteristics," *Sensors*, vol. 22, no. 20, p. 7713, Oct. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/20/7713

[5] N. Kalinowski, J. Kimbrell, C. Longchamp, and A. L. Seekford, "Exploration of Illegal, Unreported, Unregulated Fishing and Vessel Relationships using AIS Data and Machine Learning," Jun. 2023. [Online]. Available: https://zenodo.org/record/8008295

[6] "The Use of AIS Data to Identify Dark Activity for Marine Auditing Purposes," Feb. 2020. [Online]. Available: https://mismarine.com/wp-content/uploads/2020/02/The-Use-of-AIS-Data-to-Identify-Dark-Activity-for-Marine-Auditing-Purposes-v3.pdf

[7] "Fast and easy gridding of point data with geopandas," Mar. 2020. [Online]. Available: https://james-brennan.github.io/posts/fast_gridding_geopandas/

[8] J. P. Rodríguez, X. Irigoien, C. M. Duarte, and V. M. Eguíluz, "Identification of suspicious behavior through anomalies in the tracking data of fishing vessels," *EPJ Data Science*, vol. 13, no. 1, p. 23, Mar. 2024. [Online]. Available: https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-024-00459-0