Social Network Analysis of Global Transshipment: A Framework for Discovering Illegal Fishing Networks

Andrew J. Park
Department of Computing Science
Thompson Rivers University
Kamloops, BC, Canada
apark@tru.ca

Stefano Z. Stamato
Department of Computing Science
Thompson Rivers University
Kamloops, BC, Canada
stamatos17@mytru.ca

***Abstract*—Illegal, Unreported and Unregulated fishing activities contribute to economic and environmental issues across the world. Research has been done to leverage technology in the combat against illegal fishing, and methods have been published to enable the use of technology-driven tactics by authorities in charge of maritime monitoring. A challenge in continuing to combat these activities is transshipment, a practice in which transport vessels are used to mask the origins of marine products. This paper proposes a framework to use transshipment encounters as a basis for understanding the criminal networks profiting from illegal fishing by generating a global network of transshipment. The use of a network structure to represent vessels and their relationships enables the use of formal methods derived from social network analysis to interpret the structures of the criminal organizations engaging in criminal fishing activities worldwide. A framework for generating and visualizing this global network is discussed, and strategies to detect criminal activity are proposed, such as the calculation of the criminal centrality metric. This framework utilizes social network analysis techniques on the domain of illegal fishing and can empower law enforcement agencies to investigate criminal fishing operations on a global scale.**

***Index Terms*—social network analysis and visualization, illegal fishing, transshipment, criminal networks**

I. Introduction

The problem space of Illegal, Unreported, or Unregulated (IUU) fishing impacts society on numerous levels. Estimated to cause losses of up to $23.5 billion annually [1], the impacts of IUU fishing activities expand beyond fishing communities and law enforcement. Combined with the economical impact of these activities, their effects on the environment are known to contribute to issues such as the collapse of ecosystems due to the excessive and systematic exploitation of certain species.

A challenge in combating illegal fishing activities on a global scale is the criminal organizations' use of transshipment vessels, which enables them to mask the illegal origins of their products. In an attempt to camouflage criminal activity, reefers (large, refrigerated vessels) collect catch from several fishing vessels, some operating legally and some illegally. Reefers are equipped to travel long distances without damaging the marine products they transport, which enables criminals to offload their catch in ports where the risk of being caught is known to be lower (ports-of-convenience).

IEEE/ACM ASONAM 2020, December 7-10, 2020
978-1-7281-1056-1/20/$31.00 © 2020 IEEE

Efforts in monitoring the marine environment via the Automatic Identification System (AIS) have provided stakeholders and researchers with volumes of data on vessels at sea. Through the positional information that is provided periodically by vessels in the AIS, researchers and stakeholders are able to obtain near real time information on vessels' voyages. The ability to analyze AIS data to determine instances where transshipment is potentially occurring - and which vessels are participating in the encounter - is the facet of AIS research on which our framework is based.

This paper explores using transshipment events as an avenue to discover more about the organizations that profit from IUU fishing activities. Because transshipping goods at sea involves coordinating multiple vessels, there must be some underlying structure to IUU fishing operations in terms of how transshipment occurs. Understanding the relationships between IUU fishing and transshipment vessels can provide enforcers with intelligence on IUU fishing operations. This intelligence creates an opportunity to conduct more efficient inspections and apprehensions, as vessel relationships contain information on the behaviour of the entire transshipment networks that enable criminals to successfully catch and sell marine products illegally.

The paper is organized as follows: A background context is presented, including previous research using AIS data and an overview of social network analysis methods. The framework for extracting the transshipment network from AIS data is then presented, and techniques for determining illegal activity within the network are discussed. To illustrate the framework in practice, a case study of a criminal transshipment network is discovered and analyzed. The paper concludes with a discussion of the social network analysis of global transshipment encounters and the value it aggregates to law enforcers in combating illegal fishing around the world.

II. Background

The strategies currently used in combating IUU fishing are diverse, and a popular trend amongst regions that were able to mitigate this issue is to leverage technology to aid in the detection and prediction of criminal fishing activities.

A. Previous Research using AIS Data

AIS is a technology that monitors information about vessels and their voyages. Originally introduced to aid in collision prevention in the late 1980's, it allows researchers access to both static and positional data on vessels at sea [2]. Due to the large volume of the data sets associated with AIS, a popular trend in researching vessels at sea is the use of artificial intelligence techniques to extract knowledge from the large data sets containing records of their activities [3][4][5][6][7]. Research efforts surrounding the extraction of knowledge from all available data sources have been instrumental in combating IUU fishing activities, where some of the reliability problems of AIS data - a consequence of the manual-entry nature of vessel information in the system - are tackled via cross-referencing with satellite imagery (such as imagery from Synthetic Aperture Radars). This is done in an attempt to identify potential criminal activity by monitoring non-cooperative vessels: if a vessel shows up in the satellite images, but the data from AIS does not report a vessel in that position, the vessel is deemed non-compliant. Although this is not direct evidence of criminal activity, monitoring vessels in this manner shows promise in increasing the effectiveness of inspections.

Positive impacts of techniques such as the one above described were observed in a case study conducted in Ghana, where researchers observed a decline in local IUU fishing activities following the implementation of a model that combines AIS data with satellite imagery for illegal fishing detection [8]. This study showed that using technology to aid law enforcement in combating illegal fishing can be effective and, if implemented in a large scale, could empower law enforcers around the world to mitigate IUU fishing activities. However, because methods such as the ones described in the Ghana case study are only implemented in select locations, criminal activity can easily be displaced by simply fishing in areas where this level of monitoring is not in place.

A challenge in detecting criminal fishing activities is a strategy known as transshipment. This strategy involves collecting catch from fishing boats using large, refrigerated transport vessels - known as reefers. Reefers collect catch from several sources, which can operate either legally or illegally. These transport vessels are able to avoid detection by offloading their cargo in ports known to have more lax regulations (ports-of-convenience), where they can offload marine products of questionable origins into mainstream markets [9]. Since reefers used to mask IUU fishing have to appear to be compliant with norms in order to successfully hide criminal activities, their positions are often recorded by the AIS. Research on detecting transshipment in AIS has been conducted and conveniently summarized by Global Fishing Watch (GFW) - an organization concerned with providing open, centralized resources on marine monitoring globally. GFW communicates their findings in the form of reports and open data sets pertaining to each of their research fronts. A recent publication by the organization presented a data set of numerous potential transshipment encounters, alongside a report on some of the patterns in the data [10].

B. Social Network Analysis

Social network analyisis (SNA) is a tool with origins in classical sociology that aggregates concepts from social science into a mathematical formulation, allowing researchers to quantify social aspects of a group of individuals [11]. The use of a network paradigm to represent groups enables their analysis via numerous formal methods developed in the field of SNA.

The field of SNA has evolved steadily throughout the years, as an increasingly wide array of parameters were introduced to different types of analyses. Because SNA can be used to represent networks of all sizes, these flexible analysis techniques have been leveraged in different domains. An example of the flexibility of SNA techniques is provided in a study that discussed strategies to validate the analyses of small social networks in the healthcare sector [12]. In the study, SNA is used to understand social aspects of communication in networks varying both in size and density.

With the increase in popularity of social media platforms that largely took place in the 2010's, SNA became an even more popular research front. Due to the unprecedented volume of data compiled by social media platforms, blogs, customer feedback platforms and others alike, researchers had access to large amounts of data on individuals and their interactions. Research using data from social media platforms was presented in a study focused on outlining methods for the use of SNA in determining metrics related to influence and trust among individuals in social networking platforms, specifically focusing on the impact of influence and trust on the propagation of information in the online environment [13].

SNA techniques have been a powerful tool in the field of criminology, as they enable the verification of hypotheses based on analyses of real world data. An example of the power of SNA in verifying hypotheses is discussed in an article studying phenomena related to self-control, homophily and adolescent relationships [14]. Prior to this study, a widely accepted hypothesis in criminology was individuals with low levels of self-control tended to form relationships between each other and tend to commit crimes together resulting in the formation of criminal networks. By applying SNA techniques to a sample of respondents from 15 different schools, researchers in the study were able to determine that there is little evidence to correlate self-control with friendship selection. Therefore, by applying SNA methods in an analysis of real world data, researchers found that assumption to be less accurate than it was believed to be. The findings in this study further establish the SNA of real world data as an avenue to test hypotheses on the interactions between individuals.

Even though SNA has been extensively utilized in criminology studies, and ample research has been conducted using data from the AIS system, there have not been many studies intersecting these two research fronts. For that reason, this paper presents a framework for generating the social network of transshipment at sea on a global scale and provides insights into the analysis of criminal networks within the IUU fishing industry. As the effectiveness of SNA methods has been capitalized upon in several other areas within criminology studies, the intent of this paper is to enable further research to be done on the global network of transshipment and to leverage findings from the SNA of transshipment in the combat against criminal activity at sea.

III. Data

This study is primarily based on the Global Fishing Watch (GFW) data set of potential transshipment encounters [1]. It was retrieved from the GFW Transshipment GitHub repository [15], which is periodically updated to reflect suggestions made by peer-reviewers of the data set. These data compile numerous encounters between fishing vessels with vessels capable of transshipping fish at sea. Entries in the data set provide information on over 10,000 potential transshipment events, which are defined as a fishing vessel being in close proximity to a vessel capable of transshipment for an extended period of time. Maritime Mobile Service Identity (MMSI) numbers, which are unique 9-digit numbers used to identify vessels in the AIS, can be extracted from this data set and are used to identify nodes in the network. With each entry representing an encounter between two vessels (identified by their MMSIs), the relationships between nodes (and edges connecting them) can also be defined.

This study also references a list of known offender vessels, curated and made publicly available by Trygg Mat Tracking [16], a not-for-profit organization serving researchers and stakeholders with information on vessels that are currently wanted by maritime authorities. This known offender list represents an updated, centralized resource of all the main IUU vessel lists, including those in the INTERPOL Purple Notices - a set of vessels wanted for crimes related to illegal fishing. A compiled list of these vessels provides information on vessels that are known to be involved in IUU fishing, which will often be referred to as known offenders throughout this paper. Knowledge about vessels in this list can be correlated with the transshipment network, in an attempt to identify potential transshipment events in which known offenders were present.

The intent behind this known offender list is to share information between law enforcement agencies across the globe, therefore the list is organized to supply information to human stakeholders. Information on the list is often incomplete, as different vessel identifiers are used by different enforcement agencies. To properly identify known offenders in the network, a standardized list of known offenders must be generated to identify all known offenders by their MMSI numbers.

Vessels in the list of known offenders that are not identified by their MMSI numbers are generally identified by their International Maritime Organization (IMO) numbers. IMO numbers are another unique identifier assigned to vessels by the International Maritime Organization. Hence, the preprocessing of known offenders is done to obtain the corresponding MMSI numbers of vessels identified by their IMO numbers in the data set.

The generation of the standardized known offender list is started by adding all of the MMSI numbers in the IUU list to the standardized known offender list. Since the nodes in the transshipment network are identified by their MMSI numbers, known offender MMSIs can be directly correlated to their corresponding nodes in the network, and therefore no additional processing is required. Then, the remaining vessels (identified by IMO numbers) are selected, and the Fleetmon API [17], an online service providing information about vessels in the AIS, is used to correlate each known offender's IMO number to its corresponding MMSI number. The MMSIs discovered from the API queries are also added to the standardized known offenders list. The resulting information from these steps is then written to a csv file, so that this information is available offline - without requiring access to external databases at each iteration of development.

IV. Methods

The methods upon which the analyses in this paper were based come from the field of SNA [18][19]. SNA techniques aim to visually represent a set of individuals and their relationships by modelling data on individuals and relationships as a graph. In a social network graph, nodes represent individuals, and an edge connecting two nodes denotes a connection between the two individuals represented by those nodes. Each edge connecting two nodes can also be assigned a weight, allowing researchers to distinguish between stronger and weaker connections.

SNA uses methods derived from graph theory to make inferences about individuals and their relationships. For example, centrality metrics can be utilized to describe the importance of each node to the network. Different centrality metrics can be used for different interpretations of the meaning of importance. Degree centrality is the simplest of centrality metrics and comprehends a node's importance as the number of edges to and from its neighbors. Eigenvector centrality [20] expands upon the concept of importance, and takes into account the centrality of a node's neighbors in the calculation of its own centrality. Betweenness centrality measures [21] the degree to which nodes stand between each other.

To conduct the visualization and analysis of the network, Gephi is used in our study. Gephi is an open source SNA platform, which provides features used to visualize and analyze the global network of transshipment. Due to its open source nature, Gephi also offers plugins developed by the community of social network researchers to expand upon the features included in the platform. Gephi is able to efficiently visualize and analyze very large networks, which makes it the ideal tool for implementing the framework described in this paper.

V. Framework for visualizing and analyzing the global transshipment network

The analysis of the data is done by correlating all of the necessary information on vessels and their connections and parsing it into a network format. The framework proposed to generate, visualize, analyze, and discover criminal activity within the global transshipment network encompasses the following activities:

- Modelling transshipment encounters as a network
- Visualizing and analyzing the network
- Discovering criminal activity
- Conducting a case study

A. Modelling Transshipment Encounters as a Network

The network generation process begins by extracting the following information from the data set:

- Unique vessel's MMSI number
- Type (fishing or transport)
- Boolean property (known offender or not)
- Number of times that connection appears in the data

Because the same two vessels may have multiple transshipment encounters, the number of encounters between the same two vessels can later be utilized to define the edge weights in the network.

The data in the potential transshipment encounters data set are then iterated through, and each new vessel that appears is recorded. Since each entry in the data set represents an encounter between a fishing vessel and a transshipment vessel, encounter objects are created for each entry. As the study's intention is to interpret recurring encounters between two vessels as an increase in the weight of the edge connecting them, unique encounter keys are defined based on both vessels' MMSI numbers. If an encounter with that key has not been recorded yet, it is then recorded. If the key has already been seen in the data, then the encounter representing that connection is accessed, and its associated frequency is increased by 1.

All these captured data are then passed to a function responsible for parsing that information into a .gexf file. This file contains information about our vessels (represented as nodes) and the encounters between them (represented as edges). With the network file prepared, the analysis proceeds using the Gephi platform.

B. Visualizing and Analyzing the Network

The OpenOrd [22] layout algorithm is applied to highlight some of the clusters in the network and position nodes in a way that facilitates the visual analysis of the connections between fishing and transshipment vessels at sea. OpenOrd is a force-directed layout algorithm focused on identifying clusters and components that can be scaled to networks with upwards of one million nodes, making it ideal for the analysis of large networks.

The simple visualization in Figure 1 outlines some of the clusters in the global network of transshipment and denotes the existence of disconnected components. These disconnected components are then displaced by the OpenOrd algorithm and tend to end up on the outer perimeter of the network. A closer inspection of these components shows the underlying structures of small transshipment networks, where vessel types can be visualized with different node colours (Figure 2).

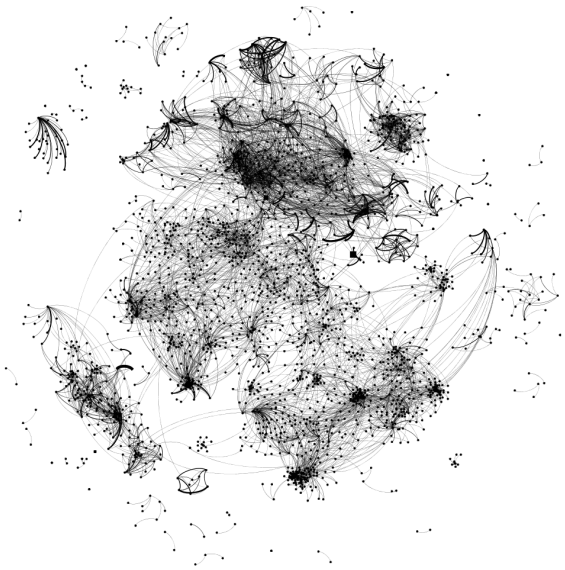

Fig. 1. OpenOrd layout

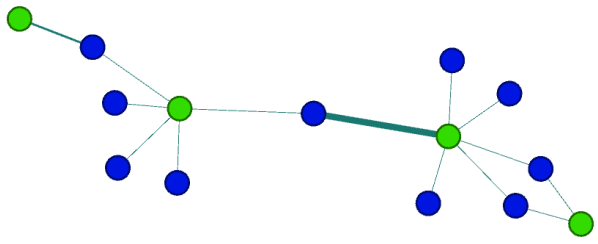

Fig. 2. A disconnected component, with green transshipment nodes and blue fishing nodes

The global network of transshipment is comprehended in terms of its communities. Communities are detected directly through Gephi's implementation of the Louvain Modularity method [23], which evaluates how densely connected nodes in a community are when compared to their connections in a random network. The results obtained from this analysis show a total of 68 detected communities, some containing significantly more nodes than others. Figures 3 - 4 show both the visualization of the largest communities in the network, as well as a distribution correlating the modularity classes with their size (number of nodes). The nodes shown in grey in Figure 3 belong to communities that each amount to 3.06% or less of all of the nodes in the network. The discoloration of smaller communities is done to visually highlight larger groups of nodes with the use of more vivid colours.

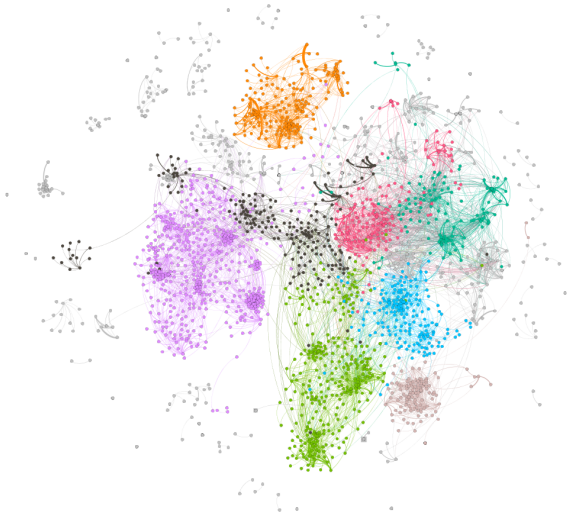

Fig. 3. Visualization of communities in the global transshipment network

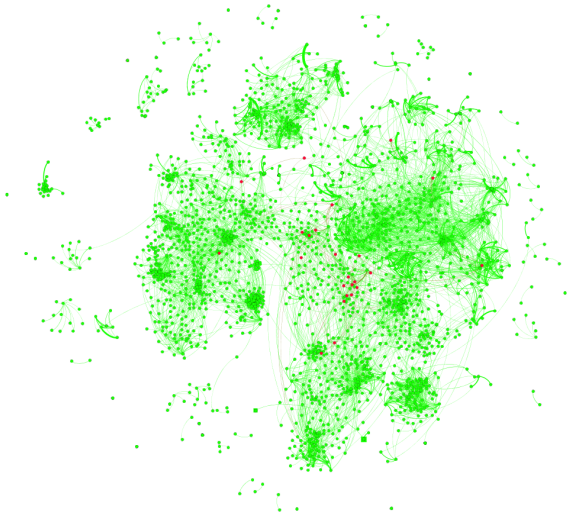

Fig. 5. Visualization of known offenders

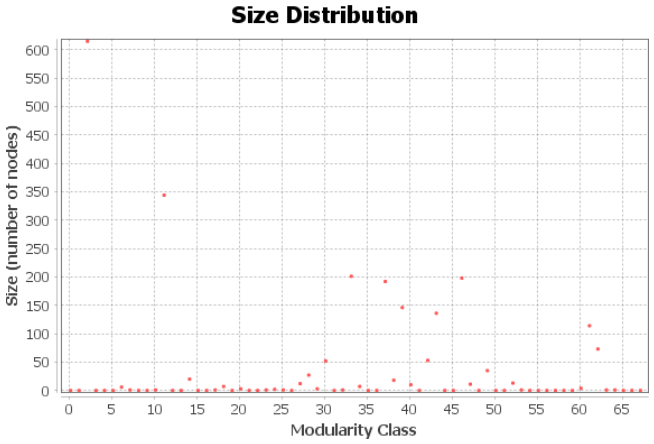

Fig. 4. Modularity class size distribution

The next step in analyzing this network is visualizing known offenders. This is done by using boolean node properties representing whether or not that vessel is in the standardized known offenders list. Using this property as the parameter, node colours are assigned to represent whether each vessel is known to engage in criminal activity. Figure 5 visualizes known criminals by colouring known offender nodes in red, and colouring the remaining vessels (which may or may not be involved in IUU fishing activities) in green.

Visually identifying known offenders in this manner allows for a clear way to understand their connections. Observing the positions of the red nodes in the network shows that a significant portion of red nodes appear to be close to each other. The existence of these criminal clusters suggests common connections between known offenders.

C. Discovering Criminal Activity

The analysis of transshipment events shows underlying patterns in connections between fishing and transshipment vessels. Furthermore, the integration of knowledge on vessels known to engage in criminal activity enables a closer analysis of the connections between criminal and non-criminal nodes in the network. It is important to note that a connection between a vessel and a known offender is not direct evidence that the vessel is involved in criminal activity. However, suspicions towards vessels' involvement in criminal activities increase as those vessels show more connections to known offenders.

In order to discover nodes that are central to the success of IUU fishing activities, the suspicion of each node's involvement in criminal activity must be quantified. To accomplish this quantification, the nodes are ranked based on a network analysis metric defined by this study: criminal centrality. This is an extension of the metric of degree centrality, where a node's importance is represented as the number of edges connecting it to its neighbors. In the calculation of a node's criminal centrality, the only edges taken into account are the ones leading to known offenders. Calculating each node's criminal centrality is done using the following equation:

$$CC(n) = DC(n) * \frac{CN(n)}{TN(n)} \quad (1)$$

Where $CC(n)$ is the criminal centrality of node n, $DC(n)$ is the degree centrality of node n, $CN(n)$ is the number of criminal neighbors of node n, and $TN(n)$ is the total number of neighbors of node n. Because the total number of neighbors of node n is the same as the degree centrality of node n, those two factors are cancelled out. That means that the criminal centrality of node n is equivalent to the number of criminal neighbors of node n.

To calculate this, a new data column is introduced in Gephi's Data Laboratory (a feature of Gephi that allows real time editing of data on nodes and edges). The column is named criminal centrality and is initialized as 0 for every node in the graph. Then, Gephi's scripting plugin is utilized to run an algorithm that calculates the number of edges leading to known offenders for every node in the graph. These values are stored in the criminal centrality column, and this parameter can now be utilized to determine the nodes most likely to be involved in IUU fishing activities.

Based on the calculated data, node sizes are reassigned to be proportional to each node's criminal centrality. Figure 6 expands upon the known offender visualization and shows a closer look at the nodes that are more heavily connected to known criminals.

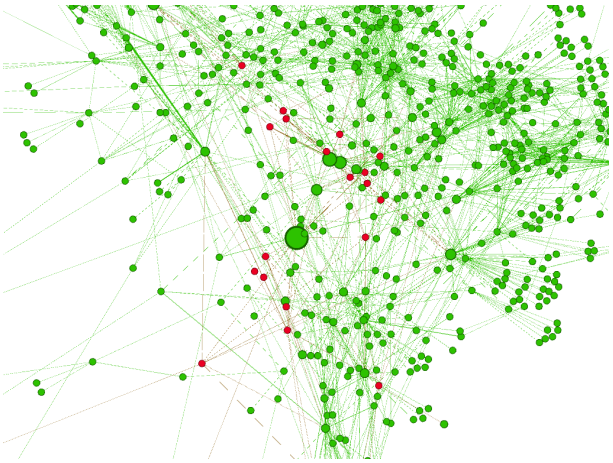

Fig. 6. Visualization of Criminally Central nodes

From this analysis, it becomes clear that the nodes with the highest criminal centrality (shown in a larger size) do not necessarily appear in the standardized known offenders list. This shows that quantifying the node's connections to known offenders can discover vessels likely to be involved in IUU fishing activities even if they are not officially reported as known offenders.

The criminal centrality metric also allows for the identification of potential offenders, and hence Gephi's Data Laboratory is used to sort the nodes in descending order of criminal centrality. This step in the analysis identified the nodes that appear larger in Figure 6, and enabled the study to identify a transshipment vessel not reported as a known offender - but heavily connected with other known offenders. The connections of this vessel are then further inspected.

D. Conducting a Case Study

By simply sorting the nodes in descending order of criminal centrality, the entire network can be leveraged to identify some of the more criminally connected vessels. After sorting the nodes in this manner, the node with the highest criminal centrality score is selected for a case study. To better comprehend the node's connections, a sub network is extracted using Gephi's built in ego network algorithm. The most criminally central node is selected based on its ID (MMSI number). This process results in a visualization that outlines the network as seen from this vessel's point of view. In this case, the ego node is a transshipment vessel. The ego network is generated with a maximum depth of 2, which limits the network to the Ego node, it's immediate neighbors, and the neighbors' neighbors. This visualization enables the inspection of the specific set of vessels closely connected to the Ego node, including the fishing vessels it served as well as other transshipment vessels connected to the known offenders. These other transshipment vessels are important to this analysis as they could potentially be utilized in the event of the apprehension of the central transshipment vessel (Ego node). This visualization is depicted in Figure 7, where known offenders are red and the other nodes are grey, and node sizes are still proportional to their criminal centrality. The ego is the large grey node at the center of the figure.

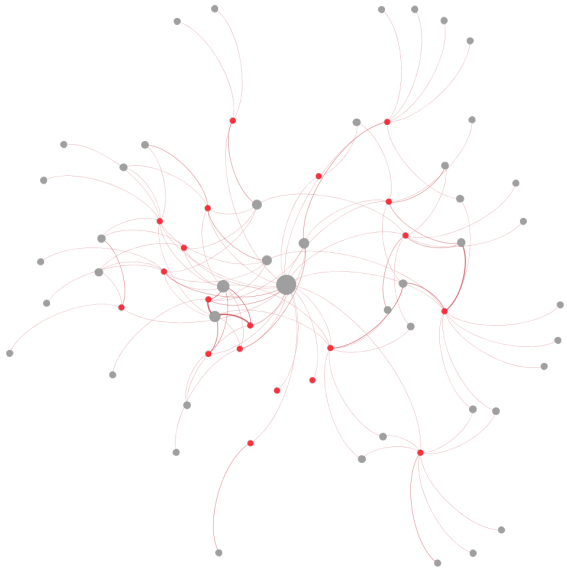

Fig. 7. Ego network visualization

This visualization clearly shows the connections between the nodes in this criminal network, where the central transshipment vessel is connected to 20 fishing vessels - all of which appear in the standardized known offender list. Based on this information, despite not a known offender itself, the central transshipment vessel is shown to likely be a part of an IUU fishing network.

VI. Discussion

The framework presented in this paper is able to generate a visual representation of the global transshipment network, with integrated information on vessels known to engage in criminal activities via the use of a standardized known offender list. The integration of information on vessel encounters combined with data on known offenders enables the discovery and inspection

of criminal networks in the domain of IUU fishing activities. Moreover, the expansion of an Ego network from the most criminally central nodes permits the identification of other transshipment vessels utilized by criminals. These alternative transshipment vessels are potential candidates for displacing criminal activities in the event of the apprehension of the vessel represented by the Ego node.

Another avenue is created by this analysis related to the understanding of patterns in the characteristics of the vessels that belong to criminal networks. For example, data can be compiled on the reported flags of these vessels as well as their last reported locations, as depicted on figures 8 and 9.

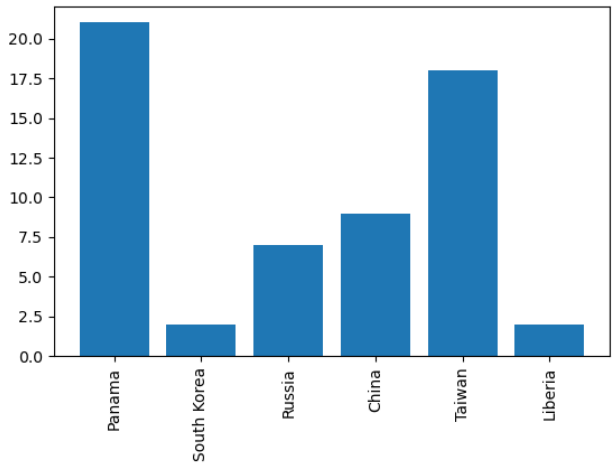

Fig. 8. Distribution of vessel flags in the case study network

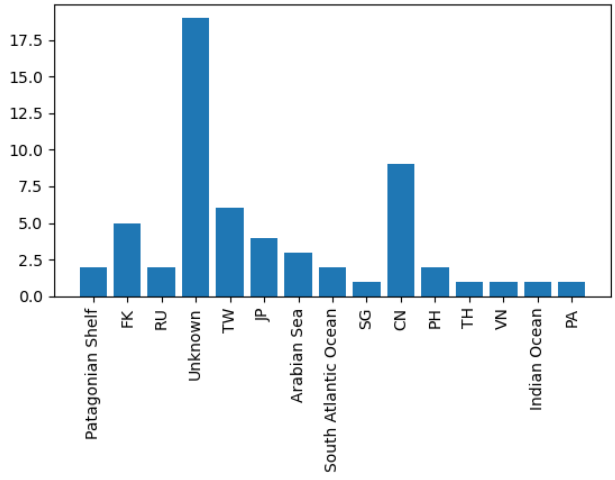

Fig. 9. Distribution of last reported vessel locations for the case study network

These data show that the most common flag reported among these vessels is Panama, which happens to be a known flag-of-convenience. By selecting a flag, vessels also select which laws they must respect when operating in international waters. Choosing to declare a flag-of-convenience is a common practice between vessels involved in IUU fishing activities as it helps illegal vessels avoid sanctions against their crimes.

When contrasting the flag information with the last reported locations of these vessels, some discrepancies are discovered: only two vessels are reported to be in Panama, and most locations appear to be in completely different areas of the world, mainly Asia. This analysis shows that the reported vessel flags are consistent with the practice of transshipment to mask IUU fishing activity. Though not direct evidence of criminality, these patterns corroborate the understanding that this may be a criminal fishing network, which was discovered through the framework described in this study.

VII. Conclusion

This study presents a framework for the generation of a social network graph from global transshipment encounters. Though both SNA and AIS data are well established research domains, this paper presents a novel framework to utilize SNA techniques on the analysis and visualization of AIS data.

The SNA of global transshipment events provides insight on how transshipment networks behave, and the integration of information on known offenders enables the discovery of criminal activity within the global transshipment network.

Continuing to utilize SNA techniques to extract knowledge about the connections of vessels known to engage in criminal activity allows for the study of behaviours and patterns within the discovered criminal networks. This analysis permits the identification of vessels in these networks, which can then be identified and queried on AIS databases to obtain aggregate information on IUU fishing networks.

The use of the framework outlined in this study can help law enforcement agencies understand more about the criminal networks they face on a daily basis. By producing information on criminal network members and how they are organized, enforcers can develop a more holistic strategy in combating IUU fishing activities. Understanding illegal fishing vessels and their relationships enables the direction of enforcement efforts toward vessels more likely to be involved in criminal activity. By apprehending more criminally central vessels and observing shifts in the network structure, enforcers can also understand how crime is displaced in response to their sanctions.

This understanding of IUU fishing activities under the scope of SNA also entails a practical approach in managing fisheries more effectively. By directing inspection efforts toward the most criminally central vessels, the enforcement resources currently available can be leveraged to their full potential in terms of significantly hindering the operations of criminal organizations profiting from the devastation of oceanic ecosystems.

VIII. Future Plan

In the future, an analysis of the transshipment network taking into account the timeline of encounter events in conjunction with time-bound reports of criminal activity could provide direct evidence of criminal interactions between fishing and transshipment vessels.

In a similar fashion, incorporating different sources of data on criminal fishing operations into the analyses enabled by the framework outlined in this study could help correlate criminal activity to traceable entities on land. Intelligence on how illegal fishing operations function can help coordinate law enforcement efforts globally, culminating in a data-driven, interconnected approach to combating crime at sea.

The same framework proposed to generate a transshipment network in the domain of IUU fishing could also be employed in the analysis of other illegal activities that are able to mask their crimes via transshipment at sea, such as human trafficking and drug smuggling.

IX. Acknowledgements

The authors would like to acknowledge the Software Technology Lab at Simon Fraser University for their relentless support for our research study. The authors would also like to thank the Department of Computing Science of Thompson Rivers University for their generous support.

References

[1] D. J. Agnew *et al.*, "Estimating the worldwide extent of illegal fishing," *PLoS ONE*, vol. 4, no. 2, 2009.

[2] J. H. Oltmann and S. Bober, *The shipborne automatic identification system (ais) - its idea, its technology, and its applications in maritime and inland shipping*, Jul. 1999.

[3] M. Gao and G.-Y. Shi, "Ship-handling behavior pattern recognition using ais sub-trajectory clustering analysis based on the t-sne and spectral clustering algorithms," *Ocean Engineering*, vol. 205, p. 106 919, 2020.

[4] J. Coleman, F. Kandah, and B. Huber, "Behavioral model anomaly detection in automatic identification systems (ais)," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 0481–0487.

[5] S. Mao, E. Tu, G. Zhang, L. Rachmawati, E. Rajabally, and G.-B. Huang, "An automatic identification system (ais) database for maritime trajectory prediction and data mining," in *Proceedings of ELM-2016*, J. Cao, E. Cambria, A. Lendasse, Y. Miche, and C. M. Vong, Eds., Cham: Springer International Publishing, 2018, pp. 241–257.

[6] W. Kazimierski, "Proposal of neural approach to maritime radar and automatic identification system tracks association," English, *IET Radar, Sonar & Navigation*, vol. 11, 729–735(6), 5 May 2017, ISSN: 1751-8784.

[7] F. Ma, X. Chu, and C. Liu, "The error distinguishing of automatic identification system based on improved evidence similarity," in *ICTIS 2013*, pp. 715–722.

[8] A. Kurekin *et al.*, "Operational monitoring of illegal fishing in ghana through exploitation of satellite earth observation and ais data," *Remote Sensing*, vol. 11, no. 3, p. 293, Feb. 2019.

[9] A. Telesetsky, "Laundering fish in the global undercurrents: Illegal, unreported, and unregulated fishing and transnational organized crime," *Ecology law quarterly*, vol. 41, pp. 939–997, Jan. 2014.

[10] N. A. Miller, A. Roan, T. Hochberg, J. Amos, and D. A. Kroodsma, "Identifying global patterns of transshipment behavior," *Frontiers in Marine Science*, vol. 5, p. 240, 2018.

[11] S. Wasserman, K. Faust, *et al.*, *Social network analysis: Methods and applications*. Cambridge university press, 1994, vol. 8.

[12] A. G. Dunn and J. I. Westbrook, "Interpreting social network metrics in healthcare organisations: A review and guide to validating small networks," *Social Science & Medicine*, vol. 72, no. 7, pp. 1064–1068, 2011.

[13] I. Varlamis, M. Eirinaki, and M. Louta, "A study on social network metrics and their application in trust networks," in *2010 International Conference on Advances in Social Networks Analysis and Mining*, 2010, pp. 168–175.

[14] J. T. N. Young, "How do they 'end up together'? a social network analysis of self-control, homophily, and adolescent relationships," *Journal of Quantitative Criminology*, vol. 27, no. 3, pp. 251–273, 2010.

[15] GlobalFishingWatch, *Global fishing watch transshipment github repository*. [Online]. Available: https://github.com/GlobalFishingWatch/paper-identifying-global-patterns-of-transshipment.

[16] *Combined IUU Vessel List*. [Online]. Available: https://www.iuu-vessels.org/.

[17] *Live AIS Vessel Tracker with Ship and Port Database*. [Online]. Available: https://www.fleetmon.com/.

[18] J. Scott, "Social network analysis," *Sociology*, vol. 22, no. 1, pp. 109–127, 1988.

[19] P. J. Carrington and J. Scott, *The SAGE handbook of social network analysis*. SAGE Publications, 2014.

[20] P. Bonacich, "Some unique properties of eigenvector centrality," *Social Networks*, vol. 29, no. 4, pp. 555–564, 2007, ISSN: 0378-8733.

[21] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, 1977.

[22] S. Martin, W. M. Brown, R. Klavans, and K. W. Boyack, "OpenOrd: an open-source toolbox for large graph layout," in *Visualization and Data Analysis 2011*, P. C. Wong, J. Park, M. C. Hao, C. Chen, K. Börner, D. L. Kao, and J. C. Roberts, Eds., International Society for Optics and Photonics, vol. 7868, SPIE, 2011, pp. 45–55.

[23] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2008, no. 10, P10008, Oct. 2008.