Journal of
Marine Science and Engineering

MDPI

Review

Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches

Konrad Wolsing [1,2,*], Linus Roepert [2], Jan Bauer [1] and Klaus Wehrle [2]

[1] Cyber Analysis & Defense, Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, Fraunhoferstraße 20, 53343 Wachtberg, Germany; jan.bauer@fkie.fraunhofer.de
[2] Communication and Distributed Systems, RWTH Aachen University, Ahornstraße 55, 52074 Aachen, Germany; linus.roepert@rwth-aachen.de (L.R.); wehrle@comsys.rwth-aachen.de (K.W.)
* Correspondence: konrad.wolsing@fkie.fraunhofer.de; Tel.: +49-241-8021465

Abstract: The automatic identification system (AIS) was introduced in the maritime domain to increase the safety of sea traffic. AIS messages are transmitted as broadcasts to nearby ships and contain, among others, information about the identification, position, speed, and course of the sending vessels. AIS can thus serve as a tool to avoid collisions and increase onboard situational awareness. In recent years, AIS has been utilized in more and more applications since it enables worldwide surveillance of virtually any larger vessel and has the potential to greatly support vessel traffic services and collision risk assessment. Anomalies in AIS tracks can indicate events that are relevant in terms of safety and also security. With a plethora of accessible AIS data nowadays, there is a growing need for the automatic detection of anomalous AIS data. In this paper, we survey 44 research articles on anomaly detection of maritime AIS tracks. We identify the tackled AIS anomaly types, assess their potential use cases, and closely examine the landscape of recent AIS anomaly research as well as their limitations.

Keywords: automatic identification system; AIS; anomaly detection; maritime safety; maritime security; maritime surveillance

Citation: Wolsing, K.; Roepert, L.; Bauer, J.; Wehrle, K. Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches. *J. Mar. Sci. Eng.* **2022**, *10*, 112. https://doi.org/10.3390/jmse10010112

Academic Editors: Juan-Chen Huang and Shuen-Tai Ung

Received: 14 December 2021
Accepted: 8 January 2022
Published: 14 January 2022

1. Introduction

Freight transport via sea is one of the major backbones of our highly connected global economy today. Global demand for freight transportation is expected to more than double by 2050, with over 70% of goods shipped by sea [1]. In addition to commercial transport vessels, the world's oceans are traveled by a wide range of other ships, such as passenger ships, ferries, fishing vessels, or recreational crafts. Therefore, ensuring the safety and security of diverse maritime traffic is necessary for the continued functioning of the increasingly globalized market economy and the well-being of passengers and marine ecosystems.

To augment safety and security at seas, the International Maritime Organization (IMO) designed the Automatic identification system (AIS) [2] in the 1990s, providing a complementary system to high-frequency radar. Ships equipped with AIS transceivers broadcast their positions derived from the Global navigation satellite system (GNSS) periodically to vessels and authorities in their vicinity. While neighboring vessels may utilize positional data for collision avoidance, on-shore Vessel traffic services (VTSs) leverage AIS for traffic planning and guidance. According to the SOLAS (Safety of life at sea) agreement from 2002 [3,4], it is mandatory for ships above a certain size to be equipped with AIS. Together with this agreement, the use of satellite-mounted AIS receivers for increased reception coverage led to an abundance of AIS data today [5]. Thus, AIS has become a valuable system for maritime collision risk assessment [6,7] and surveillance, such as anti-piracy operations or the prevention of illegal fishing [8].

With over 1,490,776 ships tracked worldwide [9], a manual unveiling of suspicious ship activities is infeasible. Hence, in recent years, many different approaches for automated anomaly detection of maritime AIS tracks have been proposed [10–15]. These anomaly detectors utilize the fact that vessel traffic is to some extent predictable, especially within confined local regions, and that vessels cannot behave arbitrarily due to physical constraints or mandatory sea routes. Thus, such detectors often train a model of normal vessel traffic patterns. They mark outliers or violations as anomalies potentially indicating, e.g., accidents or criminal activities.

To provide a concise overview on this research field, existing methodologies and their applications, we review and compare recent approaches in this paper. Therefore, we first summarize the anomaly types that can be revealed by suspicious AIS activity and map these anomalies to their common use cases. Then, we present our literature survey on anomaly detection of maritime AIS track covering 44 publications. We find that most proposals focus on the detection of route deviation anomalies and are limited to a confined geographical region their models were trained on. While there are many AIS datasets and databases of real traffic freely available [14], one observation is that authors oftentimes evaluate against self-recorded, inaccessible, or private AIS samples. In particular, it is notable that there is no established dataset that also includes labeled anomalies as ground truth. Finally, we highlight emerging privacy concerns related to AIS in general and its implications for maritime AIS anomaly detection.

The paper is structured as follows: In Section 2, we provide an overview of AIS, including a brief technical background, its history, initial purpose, and today's applications. Afterward, we elaborate on the concept of anomalies in AIS tracks and provide the rationale for anomaly detection in Section 3. Section 4 presents our survey of recent research in detail. We discuss limitations and emerging privacy concerns regarding AIS in Section 5 and conclude the paper in Section 6.

2. The Automatic Identification System

2.1. Background, Regulations, and Requirements

AIS is an identification and localization system that is mainly used in the maritime domain. The development of AIS began in the early 1990s to provide an additional ship-to-ship awareness system to supplement radar and visual observation [16]. AIS was designed for three primary purposes as specified by the IMO [2]: The first and foremost purpose is collision avoidance enabled by exchanging AIS messages between all vessels in a certain vicinity. These messages contain the vessels' identities, precise locations, and further relevant information to increase situational awareness and assist navigation. The second purpose is to support on-shore VTS for improved guidance and assistance through heavily trafficked areas or particularly dangerous passages, such as ports or sea routes [17]. Furthermore, traffic services can use special AIS messages to inform vessels about those areas. For this purpose, specific stationary Aids to navigation (AtoN) transceivers are used, e.g., installed on buoys. Similarly, AIS transceivers attached to survival crafts or even life jackets greatly enhance Search and rescue (SAR) operations. Finally, littoral states have the ability to identify ships and their cargo that are traveling in their territorial waters. As an amendment to the SOLAS agreement of 1974, the IMO mandated that all ships on international voyages above 300 gross tonnages must use AIS [3,4]. Many countries have specified stricter rules, such as the United States (vessels above 65 feet) or the European Union (fishing vessels above 15 m).

AIS messages are periodically broadcasted by transceivers onboard vessels and received by nearby ship- or land-based receivers. The system uses two VHF radio bands around 162 MHz and is based on Time-division multiple access (TDMA), allowing it to be used simultaneously by multiple participants [4,18,19]. In the horizontal direction, AIS has an effective communication range up to 50 km, which is limited by the geodetic visibility, i.e., the fact that communication entities will be hidden by the horizon due to the earth's curvature. The effects on the reception range are evaluated in great detail by the

work of Mazzarella et al. [20]. In line-of-sight, AIS signals can however travel hundreds of kilometers [21] mostly affected by radio interference and attenuation only. This is leveraged by satellite-mounted receivers that nowadays provide Satellite-based AIS (S-AIS), enabling global monitoring and a tracking extension addressing the gaps of terrestrial AIS in ocean observations [22,23].

The actual reporting interval of AIS messages lies in the range of 2–12 s (3 min for ships at anchor) and depends on the vessel's velocity as specified in the IMO Resolution 74(69) [2]. According to this resolution, the reporting frequencies allow for accurate tracking of positions and maneuvers by maritime authorities and other vessels. Moreover, further AIS requirements are specified: AIS electronics onboard vessels must automatically transmit information. On the other hand, they must be able to receive and process corresponding information automatically. Furthermore, high-priority and safety-related calls must be answered with a minimum delay. There should be a separate system with a user interface for displaying, accessing, and selecting information for human operators. Positional data of ships is generally obtained via one of the available GNSSs, such as GPS or Galileo [24].

While the AIS requirements in Resolution 74(69) state that cyber security mechanisms should be implemented, it is important to note that the AIS protocol itself is not secured and publicly accessible. In particular, neither authentication, encryption, nor integrity protection is considered. Hence, AIS is highly vulnerable to a wide range of different cyber attacks [25,26], e.g., false AIS message injection [27]. Unfortunately, the privacy issues of ship crews, passengers, owners, and other associated persons are not addressed at all. This has severe consequences, which will be considered in Section 5.2.

2.2. Data Format of AIS Messages

Information announced by AIS consists of so-called static, dynamic, voyage-, and safety-related data [2]. All required information to be transmitted via AIS is shown in Table 1. Besides the call name, call sign, and general information about the ship type, the static information consists most importantly of the Maritime mobile service identity (MMSI) number. The MMSI is uniquely assigned to each vessel and serves as the primary identifier for ships in AIS [27].

Table 1. Information announced via AIS messages. Content of the table adapted and slightly modified from IMO Resolution MSC. 74 (69) [2].

Type	Data
Static	• MMSI number • Call sign & call name • Length & beam • Ship type • Antenna location (aft/bow; port/starboard)
Dynamic	• Ship position (PO), accuracy, and integrity • Time in UTC • Course over ground (COG) • Speed over ground (SOG) • Heading (HE) • Rate of turn (ROT) • Navigational status, e.g., at anchor (STA)
Voyage related	• Draught • Hazardous cargo (type) • Destination (DST), and estimated time of arrival
Safety related	• Text messages

Since this paper is focussed on anomaly detection of AIS tracks, the dynamic part of the AIS record is of most interest. Foremost, it includes the vessel's position (latitude and longitude), its course (COG), speed (SOG), heading (HE), and rate of turn (ROT) along with

a timestamp. Voyage-related information, such as the destination port with the expected time of arrival, or in rare cases, specific information about vessels' draught or possible hazardous cargo, may be suitable for anomaly detection as well.

2.3. AIS-Based Surveillance

The use of AIS as a surveillance tool for authorities has steadily increased since its introduction, especially with the advent of satellite-based AIS that enabled an effective global tracking of vessels [5]. With the increased desire by authorities to enhance maritime security after the September 11 attacks, AIS has been recognized as a valuable tool for identifying vessels approaching coasts and ports and, thus, for preventing possible terrorist attacks [28]. Both civil and military research that focus on ship surveillance have been steadily increased with surveillance approaches developed for a wide variety of different domains [29]. They can be used, e.g., to investigate criminal activities [30], to monitor fishing activities [8], or to optimize maritime logistics and supply chains [29].

2.4. Available Datasets

By design, AIS is an entirely open protocol. Since its communication is done by radio broadcast, anyone in range can record and interpret AIS data with a suited receiver. Nowadays, AIS equipment has become steadily more affordable [27] and viable for private entities, research institutes, or companies to place AIS receivers along coastlines. Even the costs of satellite-based receivers that enable tracking of vessels around the globe have been significantly reduced and commercialized [5], which leads to a plurality of available AIS datasets. In this context, Tu et al. [14] explored different AIS data sources and assessed the data quality among different providers.

There is also a wide range of commercial providers that readily provide AIS data to paying customers via publicly available websites. Other providers can be considered non-commercial offering available data free of charge. Generally, large differences between the providers exist in terms of pricing, data availability, and data quality. According to [31], most providers generally do not fully provide all information carried via AIS (cf. Table 1). Whereas AIS's static information is never available in full detail, the available content of dynamic or voyage-related data depends on the individual provider. In addition, shipping tracks that can only be recorded by satellites, e.g., away from coasts on open oceans, may be excluded by non-commercial providers. Furthermore, data validity, such as the accuracy of ships' heading information, is severely limited for most providers. Some providers sell only live data but do not offer historical data, and vice versa. For scientific purposes, it is also possible to directly request AIS data from maritime authorities like the European Maritime Safety Authority (EMSA) [31].

3. AIS Anomaly Detection

In this section, we first elaborate on the possible types of anomalies in AIS tracks to classify current research in the later sections. We will then focus on applications of anomaly detection methods in the maritime domain, which aim to increase safety and security at sea.

3.1. Anomalous AIS Behaviors

The concept of anomalies in AIS tracks can be described as a behavior that is not "normal" or, more specifically, not expected to occur during regular operation [32]. For example, in the field of vessel traffic, it is expected that the velocity of ships does not change too rapidly or that they usually travel along common sea routes. The latter can be observed in visualizations of historical AIS tracks, as depicted in Figure 1.

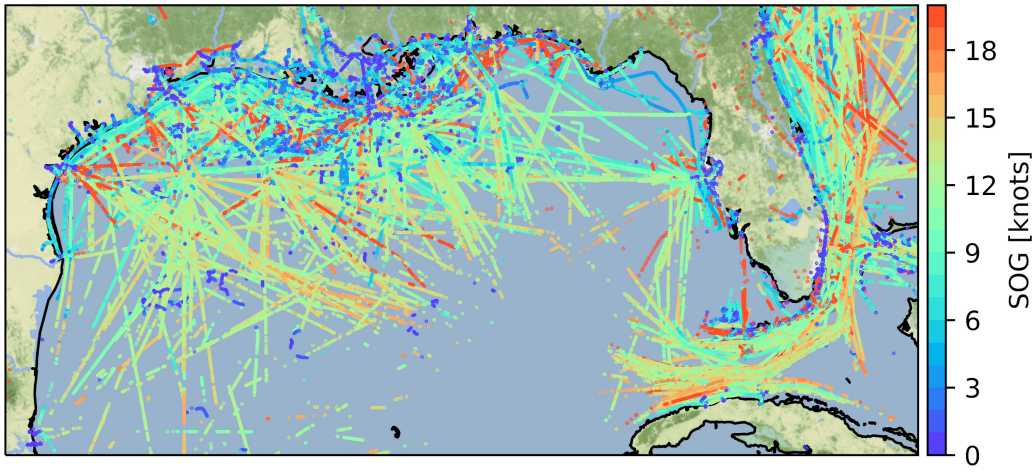

Figure 1. The usual shipping lanes and common patterns are directly accessible in the visualization of AIS messages, exemplarily shown for the Gulf of Mexico (first four days of June 2020). The historic AIS data is made publicly available by the NOAA Office for Costal Management (AIS data was obtained by https://coast.noaa.gov/htdata/CMSP/AISDataHandler/2020/index.html, accessed on 3 December 2021. Note that the central area with sparse AIS data might be explainable by the range of AIS transceivers and the providers' reception capabilities).

Regarding different anomaly types, Lane et al. [33] defined five general anomalous behaviors derived from AIS ship tracks. In this paper, we will use these anomaly types to classify recent research. Examples for each of the five categories are sketched in Figure 2 including (a) deviation from standard route, (b) unexpected AIS activity, (c) unexpected port arrival, (d) close approach, and (e) zone entry.

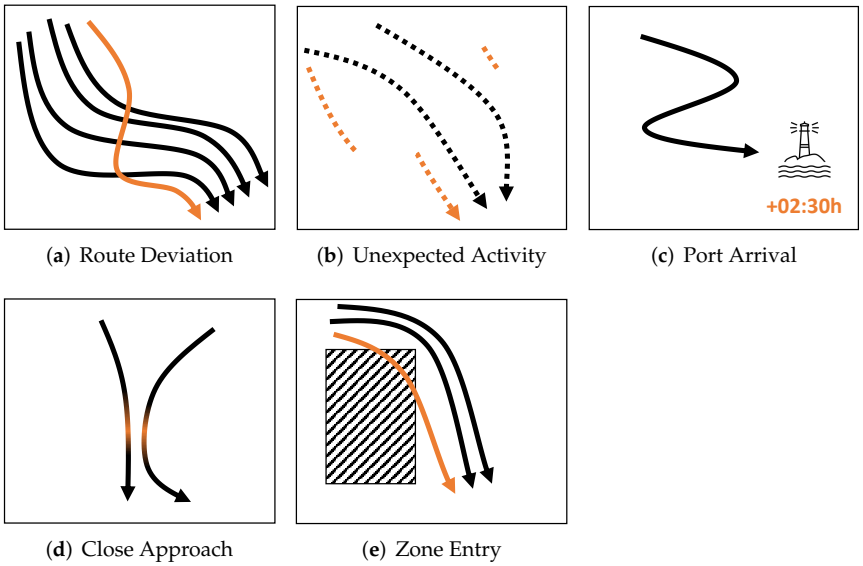

Figure 2. These general five AIS anomaly types, derived by Lane et al. [33], are used in the survey to classify the capabilities of published anomaly detectors. The arrows and data marked in orange in each figure indicate a potential deviation from the normally expected patterns.

Deviation from standard routecan be considered the most elementary anomaly. Ships, especially cargo or passenger ships on repetitive routes, generally take the most direct path possible between the origin and the destination during travel (cf. Figure 1), with the origin and destination usually being seaports. In open waters, a deviation from a straight route may then indicate an anomaly. In areas where landmasses or narrow sea lanes restrict traffic, ships can be expected to travel in relatively straight paths between common

waypoints. At the entrance of seaports or in canals, ships should be expected to take very similar routes, particularly when guided by VTS. Unexpected AIS activity encompasses two types. The first type is AIS signal loss in areas where reception is usually adequate. Such outages may indicate intentional on–off switching of AIS equipment. Unexpected continuations of routes after an AIS outage represent the second type and might obfuscate malicious actions. Unexpected port arrival can be investigated using the voyage-related data of the AIS tracks, i.e., information about the destination port and waypoints. This anomaly could occur, for example, when an illegal fishing catch is offloaded at different ports. Long-lasting close approaches between vessels should generally be rare, except, e.g., in case of emergencies. Otherwise, they might be an indication of illegal activity such as the exchange of contraband and/or drugs. Finally, zone entry anomalies can be defined as vessels entering an area for a significant amount of time they are not expected or allowed to be in, such as marine protected areas or other exclusion zones.

One of the main drawbacks of AIS is its inherent unreliability, i.e., AIS tracks of ships often show large blank spots [20]. This may be due to unintentional technical problems, radio interference, attenuation, or actual tampering with equipment, such as intentionally turning off AIS transceivers [34]. Moreover, as mentioned before, AIS signals can be easily spoofed and manipulated by attackers or parties willing to obscure their locations [27], which has been reported in practice [35]. Even if AIS tracks are complete, the detection of vessel movements, which indicate emergencies, dangerous or illegal behaviors, is often not feasible to be performed manually because the total number of ships to consider is simply too large. For this purpose, a lot of research effort has been put into so-called automated anomaly detection, which autonomously identifies anomalous behaviors, possibly acting on the knowledge of data that represents the norm [32].

3.2. Applications of AIS-Based Anomaly Detection

Initially developed for safety purposes, the focus of AIS has shifted towards a surveillance and security tool for maritime authorities AIS [5,16,28]. In this context, anomaly detection can be an efficient tool for identifying conspicuous, dangerous, or even illegal behavior at sea across a wide range of applications that are summarized in Table 2. These use cases can be broadly categorized in monitoring criminal activities, supporting safety activities, and environmental monitoring, which we explain in the following.

A lot of anomaly detection research focuses on monitoring criminal activities, such as drug smuggling or piracy. Similar efforts are likely pursued in the military domain. For instance, AIS transceivers of Iranian-flagged tankers were tampered with to disguise the identity of the vessels in order to evade sanctions on oil exports [27]. Some of the proposed anomaly detection methods have focused on concrete activities, such as the rendezvous of ships (close approach) on the open ocean for the purpose of smuggling or drug trade [36]. Others have focused on more general anomalies, such as on–off switching of AIS transceivers [37] (unexpected activities) or route deviations [38], which are used to detect pirate attacks, for example.

The majority of anomaly detection research considered in this review confirms the use of the proposed methods with respect to safety activities. In the context of safety, AIS anomaly detection may identify zone entering, where travel is considered dangerous [39]. It can also be effectively utilized to evaluate the vessel's collision risks (close approach) [40] and, thus, supports traffic surveillance [7] and also collision risk prediction [6]. It may even be possible to decrease the coast guards' or other responders' rescue times by identifying when and where SAR missions are occurring from the anomalous AIS tracks (route deviation) of the involved vessels [41]. AIS anomaly detection can further increase the efficiency of marine traffic management and planning [42]. Deploying these methods could reduce the environmental impact and overall costs of shipping due to a lowered risk of accidents or a decreased fuel consumption. Similarly, the identification of sea routes where many close approach anomalies occur could provide engineers with insights to improve the design of canals and traffic lanes.

Table 2. Use cases supported by AIS anomaly detection methods presented in Figure 2. References given in the Applications column address the individual use case.

		Route Deviation	Unexpected	Port Arrival	Close Approach	Zone Entry
Applications	**Monitoring criminal activities**					
	• drug trade/smuggling [27,36]	✓	✓	✓	✓	
	• piracy [38]	✓	✓	✓	✓	
	• cloak the vessels' identities [27]	✓	✓	✓		
	Support for safety activities					
	• collision risks [39,40]	✓			✓	✓
	• Search and rescue (SAR) [41]	✓			✓	✓
	• traffic monitoring [42]	✓			✓	
	Environmental monitoring					
	• (over)fishing [8]	✓	✓			✓
	• illegal fishing [37,43]	✓				

Finally, AIS anomaly detection can be beneficial for *environmental monitoring* to prevent or reduce the degradation of the marine environment. The depletion of the oceans' fish populations due to overfishing poses an immense risk to a large part of humanity that relies on seafood consumption. Pauly and Zeller [44] report that catch estimates have been severely under-approximated for many years and that decreasing catch volumes already indicate the decimation of fish populations. This disruption of the fragile remaining ecosystems endangers all other marine wildlife. Data analyses of AIS tracks have already helped to map fishing efforts in Europe [8]. AIS anomaly detection could supplement existing methods, identifying illegal fishing and, thus, properly managing resources and preventing overfishing. Interesting approaches have been suggested to identify illegal fishing operations, such as the ability to detect intentional off switching of AIS on fishing boats [43]. Other risks could also be reduced and the location of potential environmental incidents identified.

In summary, AIS anomaly detection enables a variety of applications across the maritime domain. In the future, there will likely be more applications in the field of AIS that can undoubtedly increase the effectiveness of AIS data utilization.

4. Classification of AIS Track Anomaly Detection Approaches

With the advent of increasing demand for freight transportation in the following years [1] and millions of vessels tracked worldwide [9], methods to automatically unveil anomalous ship behaviors become increasingly necessary, e.g., to assist VTSs. To provide a comprehensive overview of existing techniques, we present the results of our literature survey regarding approaches for automated AIS anomaly detection in this section. We begin by consulting related work (Section 4.1) and deriving the methodology of the survey (Section 4.2). Afterward, we classify the examined literature and successively discuss them along their properties (Sections 4.3–4.7). Table 3 summarizes the results of the survey.

Table 3. Summarized survey results of the 44 anomaly detection approaches for maritime AIS tracks. While the methodologies are quite diverge, we observe large commonalities regarding the anomaly type with route deviation being the most prominent one. Furthermore, the majority of detectors focus on a specific region and thus require re-training in order to be applied in other regions. Moreover, most publications refer to private datasets and struggle to find ground truth of known anomalies for their evaluation.

Method (Section 4.3)	Publication Authors	Year	Anomaly (Section 4.4)	Features (Section 4.5) PO	COG	SOG	HE	DST	Type	STA	EXT	Scope (Section 4.6) Region	Vessel	Time	Dataset (Section 4.7) Type	Ground Truth
DBSCAN	Guillarme and Lerouvreur [45]	2013	R	●	●	●	○	○	○	○	○	●	○	●	priv	○
	Wang et al. [46]	2014	R	●	○	●	●	○	○	○	○	●	○	○	–	●
	Liu et al. [47]	2014	R	●	●	●	○	○	○	○	●	●	○	●	priv	○
	Radon et al. [48]	2015	R	●	●	●	○	●	○	○	○	●	○	●	pub	●
	Fu et al. [49]	2017	R	●	●	●	○	●	●	○	○	●	○	●	priv	○
	Goodarzi and Shaabani [50]	2019	R	●	●	●	○	○	○	○	○	●	○	○	priv	○
Gaussian Mixture Model and Kernel Density Estimation	Riveiro et al. [51]	2008	R	●	○	●	●	○	○	○	○	●	●	●	synth	◐
	Laxhammar [32]	2008	R	●	○	●	○	○	○	○	○	●	○	○	priv	○
	Ristic et al. [52]	2008	R	●	○	●	○	○	○	○	○	●	○	●	self	○
	Laxhammer et al. [53,54]	2010	R	●	○	●	○	○	●	○	○	●	○	○	pub	◐
	Smith et al. [55]	2014	R	●	○	●	○	○	○	○	○	●	●	●	self	○
	Anneken et al. [56]	2015	U	●	○	●	●	○	○	○	○	●	●	●	self	●
Neural Network	Rhodes et al. [57]	2009	R	●	●	●	○	○	○	○	○	●	○	○	priv	○
	Nguyen et al. [24]	2018	R	●	●	●	○	○	○	○	○	●	○	●	pub	◐
	Venskus et al. [58]	2019	R	●	○	●	●	○	○	○	●	●	●	○	priv	○
	Singh and Heymann [37]	2020	U	●	●	●	○	○	○	○	○	○	●	●	self	●
	Nguyen et al. [59]	2021	R	●	●	●	○	○	○	○	○	●	●	●	priv	◐
Geometry	Osekowska et al. [60]	2014	U	●	○	○	○	○	○	○	○	●	○	●	-	-
	Soleimani et al. [61]	2015	R	●	○	○	○	○	○	○	○	○	●	○	priv	●
	Venskus et al. [62]	2015	R	●	○	○	○	○	○	○	●	○	●	●	priv	○
	Zissis et al. [15]	2020	R	●	○	○	○	●	○	○	○	●	●	○	priv	●
	Guo et al. [63]	2021	R	●	●	●	●	○	○	○	○	○	●	●	pub	○
Stochastic	Katsilieris et al. [64]	2013	R Z	●	○	○	○	○	○	○	●	○	○	○	priv	○
	Keane [65]	2017	R	●	○	○	○	○	○	○	○	●	○	○	priv	○
	Ford et al. [43]	2018	U	●	○	○	○	○	○	○	○	●	○	●	priv	◐
	d'Afflisio et al. [66]	2018	U	●	○	●	○	○	○	○	○	○	●	●	–	●
	Rong et al. [38]	2020	R	●	○	●	●	●	●	○	○	●	○	●	–	○
Machine-Learning & Clustering	Vespe et al. [39]	2012	R Z	●	●	●	○	○	○	○	○	●	○	●	priv	○
	de Vries and van Someren [67]	2012	R	●	○	○	○	○	○	○	●	●	○	●	self	○
	Handayani et al. [68]	2013	R	●	●	●	●	○	○	●	○	●	○	●	pub	○
	Zhen et al. [69]	2017	R	●	●	●	○	○	○	○	○	●	○	●	priv	○
Frameworks	Pallota et al. [70,71]	2013	R	●	●	●	○	○	○	●	○	●	○	●	priv	○
	Kazemi et al. [72]	2013	P	●	○	●	●	●	●	●	●	●	●	●	pub	●
	Lei [73]	2016	R	●	○	○	○	○	○	○	○	●	○	●	self	◐
	Lane et al. [33]	2010	R U P C Z	●	○	●	●	●	○	○	○	●	●	○	–	–
Bayesian Network	Johansson and Falkman [74]	2007	R	●	○	●	●	○	●	○	○	●	●	○	synth	○
	Mascaro et al. [75]	2010	R	●	●	●	●	○	●	○	●	●	○	●	priv	◐
	Mascaro et al. [76]	2014	R C	●	●	●	●	○	●	○	●	●	○	●	priv	◐
Gaussian Process	Kowalska and Peel [36]	2012	R C	●	○	●	●	○	●	○	○	●	○	●	priv	◐
	Zor and Kittler [77]	2017	R P	●	○	●	●	●	○	○	○	●	●	●	priv	○
Miscellaneous	McAbee et al. [78]	2014	R	●	○	○	○	○	○	○	○	●	○	○	self	◐
	Wu et al. [79]	2014	U	●	○	●	○	○	○	○	○	●	○	●	self	○
	Terroso-Saenz et al. [80]	2016	R C	●	○	●	○	○	○	○	●	●	●	●	pub	◐
	Kong et al. [81]	2017	R	●	○	○	○	○	○	○	○	●	○	●	priv	○

Anomaly types: Route Deviation (R) Unexpected Activity (U) Port Arrival (P) Close Approach (C) Zone Entry (Z)
Dataset availability: Public (pub) Private/Closed (priv) Self-recorded (self) Synthetic (synth) ●: A feature is used or a method is restricted to a scope ○: otherwise ◐: For synthetic/simulated ground truth.

4.1. Related Work

The interest in anomaly detection in the maritime domain experienced steady attention over the past years and resulted in several scientific publications in this field. Related to our work, there are surveys with similar intentions, which we discuss briefly. The first publication from 2008 [82] derived a taxonomy for the term anomaly within the maritime domain. It is followed by a summary of a few selected approaches in 2011 [11]. Sidibé and Shu [13] conducted the first systematic review covering literature published from 2011 until 2016. Their review focuses on the individual detection methodology, approach type, AIS attributes, and used dataset. Another extensive literature survey was conducted by Riveiro et al. [12], yet many of the considered approaches are either very generic or focus on other technologies besides AIS. The survey of Tu et al. [14] paid special attention to differentiating between approaches that are geographically confined (map dependent) or universally applicable (map-independent). The most recent study [10] covers only 18 publications found in a systematic literature review and discusses high-level research questions. Finally, Zissis et al. [15] developing methods for modeling maritime routes also performed an extensive literature review.

However, while there have been extensive studies in that area, most of them lack a clear differentiation between methods developed primarily for detecting anomalies of AIS tracks and those originally addressing related problems. Some approaches, for instance, predict vessel trajectories [83] or their time of arrival [84]. Although deviations from these predictions might indicate anomalies, the authors evaluated their approaches only in terms of predictive quality and not its anomaly detection capabilities, as the papers in our review do. Similar reasons for exclusion hold for related methods that investigate the signal strengths of AIS [20] or optimize visualizations in human–machine interfaces [85], which both can contribute to anomaly detection as well, but only as a secondary use case. Thus, in our literature survey, we focus on publications specifically designed for anomaly detection in AIS tracks, which allows, among others, to assess and compare their evaluation methodologies qualitatively.

4.2. Survey Methodology

To identify publications that are explicitly concerned with the detection of anomaly in AIS tracks, we conducted a literature review. We considered papers found according to the keywords “AIS”, “anomaly detection”, “maritime”, and “tracks”. In addition, we also considered publications covered by previous reviews [10–15]. The main reason for excluding papers was that they do not fit the topic or do not focus exclusively on anomalies in AIS tracks. This way, we obtained a selection of 44 papers, which encompass the years 2007 until 2021, cf. Table 3 summarizing our selection.

For each publication, similar to related work [13,14], we extracted the following properties of the detectors: First, the underlying detection method is highlighted, which groups similar detection methods. Furthermore, we list the anomaly types each method addresses (cf. Figure 2), the used AIS features (cf. Table 1), or whether these use external non-AIS features (referred to as EXT in Table 3). We display the scope of each approach with respect to a fixed region or scaling independently of a trained region, following to the notion of map-dependency used by Tu et al. [14] (cf. Section 4.1). Similarly, the vessel scope indicates whether the approach distinguishes between different vessel types announced via AIS (cf. static in Table 1), and the time scope whether temporal relationships are incorporated. Finally, the survey lists the dataset type, e.g., public or private, and whether the evaluation compares to a ground truth of known anomalies.

4.3. Methods for AIS Anomaly Detection

Regardless of the specific method, what most AIS anomaly detectors have in common is that they require learning an underlying model by using normal and sometimes anomalous AIS training data. Based on this model, detectors can decide whether new data classifies as normal or anomalous behavior. Among the considered research, only

a few approaches are model-free, e.g., the approach by d'Afflisio et al. [66]. The authors deterministically verify if trajectories could have occurred during an (intentional) AIS outage, considering data before the individual outage. The scope of the models is discussed in the later Section 4.6.

Our survey identified ten groups of utilized detection methods, which are further categorized in Figure 3. One major group accounts for machine learning, either with neural networks or clustering. In particular, DBSCAN is the primary method for the latter. It finds wide use across the domain of AIS anomaly detection because it is an algorithm that appropriately clusters similar regions such as maritime vessel tracks well and can incorporate course (COG) or speed (SOG) as additional features in addition to the position (cf. Section 4.5). Tracks outside of the clustered regions then indicate anomalies. Another large group of works accounts for stochastic methods such as gaussian mixture models, which assume that the properties of AIS tracks underlay probabilistic variations. Complementing these fundamental methodologies, which are applied in other domains of intrusion detection as well [86], further specialized approaches utilizing geometric properties exist. Such approaches, for instance, calculate the convex hull of tracks in a certain region [15] or model each AIS message as a potential electrical charge decaying over a larger distance [60]. Finally, there are approaches that do not rely on a single anomaly detection method but rather incorporate multiple methods into a comprehensive framework. We therefore assigned them to a separate category (framework) in our survey.

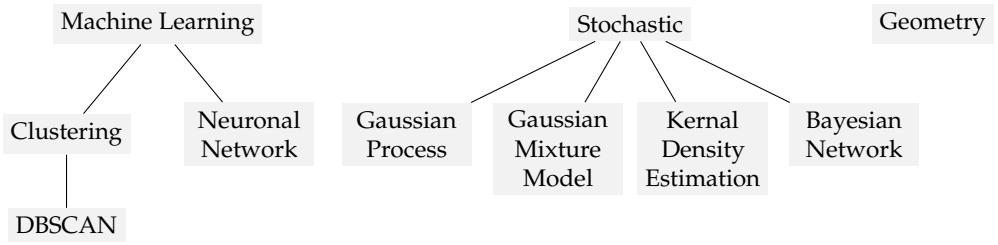

Figure 3. Classification of the underlying anomaly detection methods. Besides frameworks or miscellaneous approaches, most works can be grouped into one of the the major groups: machine-learning, stochastic, or geometry approaches.

4.4. Anomaly Types Addressed by Research

In this paper, research is classified according to the five categories proposed by Lane et al. [33] as introduced in Section 3.1 (cf. also Figure 2). Current research on AIS track anomaly detection considers all five types of anomalies. Yet, the proposed methods often identify a single anomaly type only.

The deviation from a standard route is the most prominent anomaly type that research addresses in 37 out of 44 publications. Many approaches extract frequently traveled sea routes from historical AIS data, e.g., via clustering. Unknown AIS tracks can then be compared in order to investigate whether they are similar enough to the extracted routes, or in the case of clustering, belong to one of the identified route clusters. These approaches work very well in areas where many ships take similar routes, which has been demonstrated by Wang et al. [46] and Zhen et al. [69] for bay areas and port entrances. The deviations from a standard route can also be used without a priori knowledge of common routes [64,66].

Seven approaches in our survey particularly consider unexpected AIS activity. The work of d'Afflisio et al. [66] aims to identify velocity changes occurring during AIS outages assuming that ships travel with similar velocity most of the time. They argue that intentional on–off switching is generally used to hide changes in the nominal velocity of vessels, which may occur when vessels change their course, for instance. The methodology suggested by Singh and Heymann [37] relies on known AIS tracks from other vessels and also addresses the detection of intentional on–off switching of the AIS equipment. It should be noted at this point that a plurality of other methods in the context of unexpected AIS activity aims to detect anomalies by monitoring radio signal strengths or outages occurring

in specific areas. Suchlike approaches, most notably the work of Mazzarella et al. [20], are excluded from this paper due to its clear focus on AIS tracks. However, they represent promising complementary approaches that can be used alongside pure AIS-based methods to improve the detection capability.

We found three publications that explicitly consider anomalous port arrival. Zor and Kittler [77], for instance, look at ferries that run regular routes according to a fixed schedule. However, only a single ship is considered separately at a time. Hence, it is known a priori from where the vessel will (always) depart and where it is (always) expected to arrive. In general, the destination port is transmitted via AIS. As a result, it can simply be checked if the vessel's AIS track violates the port order.

Similarly, close approach anomalies can only be found in a few publications, namely in [33,36,76,80]. Mascaro et al. [76] consider the number of close interactions between ships, which may be used to indicate cargo handover, for example. In contrast, Terroso-Saenz et al. [80] forecast the closest point of arrival between two vessels. This approach could be beneficial for VTSs and enable safer and more effective navigational guidance.

Zone entry as an anomaly type is considered only marginally in the methods developed by Vespe et al. [39], Katsilieris et al. [64], and Lane et al. [33]. Restricted zones, which should not be entered, are learned implicitly as part of the general shipping routes and trajectories [39]. Zone entry in isolation may not be considered because it may be deemed too trivial to implement, i.e., the vessel's position being inside the zone constitutes an anomaly. However, one could imagine other, more elaborate methods such as predicting whether a zone entry is likely to occur soon [33].

4.5. Detection Features

As outlined in Section 2.2, AIS messages carry a wide range of different data (cf. Table 1). All anomaly detection methods generally only use a limited subset of the available features. Furthermore, they implicitly require the MMSI number to recover ship tracks from individual AIS data points. Thus, the MMSI is not explicitly listed in Table 3.

Because approaches based on AIS tracks are considered, it is not surprising that all methods use vessels' positions (PO). Whereas the speed over ground (SOG), heading (HE), or course over ground (COG) are often analyzed additionally, there exist approaches that utilize a minimum of different features only [60,61,73,78,81]. In contrast, others have seemingly adopted a maximalist approach [72,76]. Mascaro et al. [76], for instance, included most of the dynamic AIS information (cf. Table 1), as well as a vast range of external non-AIS features, such as information about weather or daytime. Similarly, although not including external features, Handayani et al. [68] argue that the usage of a wider range of features has the potential to further increase the precision. Only a few approaches use the port destinations (DST), vessel types (Vessel), or status information (STA) features. Sometimes, however, it remains unclear whether the authors obtain information about the destinations from the actual AIS data or other sources. Note that some approaches utilize the vessel type as a dedicated feature, whereas others already focus their scope on a specific vessel type beforehand (cf. Section 4.6).

4.6. Scope of Detection Methods

Besides the detected anomaly types and utilized AIS features, the scope of the detectors may differ largely regarding regions, vessel types, and time. Table 4 summarizes the regional and vessel type scopes, which are discussed in more detail in the following. Regarding the time scope, 31 publications incorporate temporal relationships. The remaining 13 publications operate time-independently and solely test, e.g., whether new AIS messages' speed vectors are similar to adjacent historic ones [32].

The survey assesses the regional scope, meaning whether the learned model is valid only in the confined region of the training data or whether it generalizes to unknown, not yet trained areas. As shown in Table 4, the majority of approaches (38) are region centric. Only six can be applied on a global scale. The geographical size the regional

methods are constrained and can vary significantly from approaches focusing on bays and port entrances [46,69] to areas of continental scale [45]. A major disadvantage of local approaches is, however, that they strongly rely on historical AIS data of the region. Thus, they cannot be applied to regions from which there exists no or sparse information.

Table 4. Overall, the majority of publications (38 out of the total 44 from the review) consider a given constrained region, as show in the table below. Only a few (6) are region independent and generally applicable, i.e., worldwide. Furthermore, the minority (16) differentiate between vessel-specific types prior to training. Overall, most approaches (27) are vessel type independent and region constrained.

		Vessel Type	
		Specific (●)	**Independent (○)**
Region	constrained (●)	11	27
	independent (○)	5	1

Approaches also differ in the way vessel types are considered for detection. The distinction made in this work is whether the methods aim to detect anomalies from one specific vessel type or if anomalies can be detected for any other (unknown) vessel types. It is apparent that many of the methodologies developed (28 papers) generalize to all other vessels. Yet, not insignificantly few work (16 papers) focuses on unique vessels and anomalies, such as Zor and Kittler [77] who consider route anomalies of ferries oscillating between two fixed ports. The method exploits the characteristics of ferry traffic, which always follows very similar and known paths. The models are then built from the individual routes of specific ferries. Present behavior can then be analyzed with respect to anomalies, but it remains questionable whether their approach can be applied to other ships traveling a similar route. A limitation when considering approaches specific for single vessels is that vessels involved in anomalous behavior have to be known in advance. Furthermore, a sufficient amount of regular non-anomalous AIS data would have to be recorded before anomaly detection could take place. While such approaches may be suitable for detecting anomalies of ferries, it seems too specific for most scenarios beyond that context. In security- and safety-related scenarios, such as terrorist attacks or emergencies, a meaningful selection of ships for which to train a vessel-specific detection model is challenging because it is not known in advance which ships are likely to be involved in an upcoming incident or illicit activities (cf. Table 2).

4.7. Evaluation Datasets and Ground Truth

Besides proposing new anomaly detectors, evaluating their effectiveness and comparing them to existing state of the art is essential in scientific research. The usual procedure involves splitting a given dataset into training and test data containing (known) anomalies that are expected to be found.

Regarding dataset types, we differentiate between publicly available, self-recorded, private/closed, and synthetic AIS data. As shown in Table 3, the data sources vary widely between the different research approaches. While 7 publications revealed their data sources, unfortunately, 32 approaches are evaluated on closed data sets and 5 with unknown sources. As our survey shows, 22 of the 32 approaches are evaluated on private datasets, whereas eight publications are based on self-recorded and two are based on synthetic datasets. Many authors obtained data from (military) authorities or defense contractors, e.g., the Swedish navy [32] or BAE Systems [36], while others relied on commercial platforms, such as MarineTraffic [66,68]. Since inexpensive Commercial off-the-shelf (COTS) AIS equipment is available today, it is reasonable that some research groups self-recorded the needed AIS data [37,52,55,56,67,73,78,79]. However, not all researchers used real-world AIS data. Kong et al. [81], for instance, artificially generated a set of short AIS tracks that are claimed to be consistent with real-world AIS traffic and terrorist behavior.

Moreover, we observe that the lack of ground truth is a common challenge in this area of research. When using real-world data, many researchers struggle to find a valid ground truth [32,59,76] and resort to the artificial generation of AIS anomalies [55,66]. Besides the 8 publications with a decent ground truth derived, e.g., from real reported incidents in Europe [15] or suspected illegal fishing rendezvous [66], tracks labeled by domain experts [61], or situations with severe weather conditions [78], there are also 11 publications with makeshift ground truth (marked with ◐ in Table 3). These include drawing anomalies by hand [75], introducing random data, or adding synthetic anomalies, among others. Validation of methods with exclusively self-generated anomalies might limit the reliability of the developed methods in real-world scenarios, the credibility of the approaches, and hinders comparison in the research community.

Overall, this heterogeneous landscape of AIS data sources constraints science. A dedicated scientific database for regular AIS data might not necessarily be of much additional value because there is already a large number of sources available (cf. Section 2.4) [14]. However, having such a database including known and confirmed anomalous AIS tracks would be of great value. From a scientific view, there are three general requirements for such a dataset. First, it should be representative in terms of relevance and coverage. Second, accessibility is crucial, meaning the data must be made available and easily accessible. Most important, in the context of AIS anomaly detection, anomalous traces must be marked with an appropriate label. It should be noted that Mao et al. [87] have already laid the foundation for a scientific AIS database, but for evaluating trajectory prediction methods rather than anomaly detection.

5. Discussion

This section discusses the results of our review and classification of research approaches for anomaly detection in AIS tracks. First, limitations arising from the homogeneity of methods are mentioned (Section 5.1). We then outline the critical challenges related to privacy implications of AIS surveillance and anomaly detection (Section 5.2).

5.1. Limitations of Recent Approaches

The literature review reveals that research on anomaly detection in AIS tracks follows a relatively homogeneous path. Firstly, the bulk of research is aimed at detecting route anomalies (cf. Table 3), and thus, lacking diversity. Detection methods for zone entry and unexpected port arrival could be effortlessly implemented and successfully complement route deviation detection. Close approach anomalies may be more challenging to detect reliably, especially in high-trafficked areas, because they simultaneously require position, course, and speed information of multiple ships. Nevertheless, it is surprising, in particular with respect to the original safety goal of AIS (see Section 2.1), that there is not more research focused on the detection of close approaches. However, simple collision avoidance mechanisms are already built into existing AIS equipment [2] and are likely to be not covered by our survey due to their design (cf. Section 4.1).

The majority of research is concerned with modeling "normal" behavior specific to a geographically confined region (cf. Table 4). While these approaches seem to work very well, they may suffer from the following disadvantages: In areas where not sufficient data is available or it is not plentiful enough, these approaches can hardly be used. In addition, when entering AIS data or configuring AIS equipment, mistakes are often introduced [88] that can be unintentionally and wrongly incorporated as normal into the learned detection model. Finally, with the advent of upcoming autonomous vessels and ships [89–91], implementing AIS track anomaly detectors directly into moving vessels may be beneficial to enhance safe automated navigation. Again, region-specific approaches may not be fully applicable here because they require re-training for each region the vessel moves to. Thus, we deduce that these region-specific approaches are mostly only suitable for static use cases and stationary AIS receivers.

With respect to datasets that are used for the evaluation of proposed approaches, it turns out that in many cases AIS anomaly detection is funded or performed by researchers associated with maritime authorities or defense contractors. Thus, it is not surprising that these entities often also supply their datasets. Nevertheless, some researchers (8 papers) also recorded their own datasets, while only a few (seven papers) use publicly available sources. Unfortunately, there is a lack of known anomalous AIS situations that represent reliable ground truth. Hence, many researchers resort to simulating their own anomalies as substituted ground truth. Existing approaches range from manually drawing AIS tracks [75] to simulating data with rigid-hulled inflatable vehicles [36]. Overall, the lack of a common dataset heavily reduces transparency, hinders a replication of results, and makes it particularly impossible to evaluate and compare the effectiveness of different approaches in a sound and scientific manner. The development of an established and freely available AIS database, such as suggested by Mao et al. [87], is thus urgently necessary in order to advance science in this domain.

Still, as found out recently by Serra-Sogas et al. [92], only a minority of the total vessels contribute to AIS, and about 70% remain invisible. This severely limits the applicability of detection methods, especially to small recreational vessels, which account for 53% of the non-AIS-equipped vessels [92]. Thus, supplementary methods that can track vessels regardless of their AIS equipment, such as those based on radar, may be beneficial in the future in addition to AIS-based anomaly detection.

5.2. Privacy Considerations

With respect to information security, a problem already mentioned in Section 2.1 is the general openness of the AIS protocol because AIS information can be accessed by anyone at any time. The trade-off between the gain in security and safety through AIS and the loss of privacy for those traveling on vessels may be skewed in favor of the former. With AIS data readily available for anyone willing to pay (cf. Section 2.4), the location of known crews and passengers can be revealed in real time. In addition, AIS receivers placed around the globe are connected to the Internet, sometimes without any security mechanisms in place [93].

The IMO noted already in 2004 that freely available AIS data may undermine the initial safety and security goals [94]. The situation is so serious that the European Data Protection Supervisor has acknowledged that AIS may have infringed the EU's data protection regulation since its inception [95]. Similar considerations that AIS may violate the freedom of information act are made in the United States [96].

To the best of our knowledge, none of the anomaly detection research considers privacy issues. Existing work may be used to identify and track individuals involved in (suspected) illicit activities by anyone having the ability to obtain AIS data. However, this also means that these methods can be used by authorities and governments that violate basic human rights to, e.g., actively prohibit identified SAR missions and persecute individuals involved in such missions. These issues may be partially remedied by extending confidentiality and authentication protection to AIS as suggested by Goudossis and Katsikas [25], Aziz et al. [97], and Kessler [26].

6. Conclusions

To increase the safety and security of a globally growing maritime traffic, AIS was introduced by fitting transceivers to each vessel, primarily to suit as a digitized ship-to-ship collision avoidance system. With the ability to overhear AIS position broadcasts from ships worldwide, e.g., via satellite-based receivers, AIS became the leading tool to enable surveillance of the entire maritime domain. With plenty of available AIS datasets and vessels following predictable routes and maneuvers, automated anomaly detection promises to detect unintended or even malicious behavior, e.g., by learning frequent shipping routes.

In this paper, we performed a literature survey to classify academic anomaly detection approaches utilizing AIS tracks. Based on a detailed assessment of 44 publications, it

reveals that most research tackles deviations from the expected or well-known shipping routes by focusing on confined regions rather than training universally applicable models. This may be suitable for stationary VTSs or vessels on repetitive routes, but hinders the adoption of new use cases such as future autonomous vessels operating on worldwide cargo routes. Moreover, an objective and sound comparison between approaches is hardly possible due to closed evaluation datasets and missing ground truth for anomalies.

With AIS being a powerful tool for worldwide surveillance, it contradicts the individual's rights to privacy, as already recognized by the IMO and also at state level [94–96]. Hence, we believe that awareness should be raised, especially for AIS tracking and automatic anomaly detection in the future. Extensions to AIS that provide both pseudonymity and confidentiality to vessels are needed to protect the privacy and data sovereignty of individuals at sea.

Author Contributions: Conceptualization, K.W. (Konrad Wolsing), L.R. and J.B.; methodology, K.W. (Konrad Wolsing) and J.B.; validation, K.W. (Konrad Wolsing); writing—original draft preparation, L.R.; writing—review and editing, K.W. (Konrad Wolsing) and J.B. visualization, K.W. (Konrad Wolsing); supervision, K.W. (Klaus Wehrle). All authors have read and agreed to the published version of the manuscript.

Funding: This work is part of the project MUM2 (https://www.mum-project.com). It was partially funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK) within the "Maritime Research Programme" with contract number 03SX543B managed by the Project Management Jülich (PTJ). The authors are responsible for the contents of this publication.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic identification system
AtoN	Aids to navigation
COG	Course over ground
COTS	Commercial off-the-shelf
DST	Destination
EMSA	European Maritime Safety Authority
GNSS	Global navigation satellite system
GPS	Global positioning system
HE	Heading
IMO	International Maritime Organization
MMSI	Maritime mobile service identity
PO	Position
ROT	Rate of turn
S-AIS	Satellite-based AIS
SAR	Search and rescue
SOG	Speed over ground
SOLAS	Safety of life at sea
STA	Status
TDMA	Time-division multiple access
VHF	Very high frequency
VTS	Vessel traffic service

References

1. International Transport Forum. *ITF Transport Outlook 2021*; Economic Cooperation and Development (OECD) Publishing: Paris, France, 2021. [CrossRef]
2. International Maritime Organization (IMO). *Resolution MSC. 74 (69) Adoption of New and Amended Performance Standards*; IMO: London, UK, 1998.
3. International Maritime Organization (IMO). *SOLAS Chapter V—1/7/02 Safety of Navigation*; IMO: London, UK, 2002.
4. International Maritime Organization (IMO). *Resolution A.1106(29) Revised Guidelines for the Onboard Operational Use of Shipborn Automatic Identification Systems (AIS)*; IMO: London, UK, 2015.
5. Fournier, M.; Casey Hilliard, R.; Rezaee, S.; Pelot, R. Past, present, and future of the satellite-based automatic identification system: Areas of applications (2004–2016). *WMU J. Marit. Aff.* **2018**, *17*, 311–345. [CrossRef]
6. Liu, D.; Wang, X.; Cai, Y.; Liu, Z.; Liu, Z.J. A Novel Framework of Real-Time Regional Collision Risk Prediction Based on the RNN Approach. *J. Mar. Sci. Eng.* **2020**, *8*, 224. [CrossRef]
7. Zhen, R.; Riveiro, M.; Jin, Y. A novel analytic framework of real-time multi-vessel collision risk assessment for maritime traffic surveillance. *Ocean Eng.* **2017**, *145*, 492–501. [CrossRef]
8. Natale, F.; Gibin, M.; Alessandrini, A.; Vespe, M.; Paulrud, A. Mapping Fishing Effort through AIS Data. *PLoS ONE* **2015**, *10*, e0130746. [CrossRef] [PubMed]
9. MarineTraffic. Vessels Database. 2021. Available online: https://www.marinetraffic.com/en/data (accessed on 29 December 2021).
10. Ferlansyah, N.; Suharjito, S. A Systematic Literature Review of Vessel Anomaly Behavior Detection Methods Based on Automatic Identification System (AIS) and another Sensor Fusion. *Adv. Sci. Technol. Eng. Syst. J.* **2020**, *5*, 287–292. [CrossRef]
11. Martineau, E.; Roy, J. *Maritime Anomaly Detection: Domain Introduction and Review of Selected Literature*; Technical Report; Defence Research and Development Canada—Valcartier, Technical Memorandum TM2010-460; Defence Research and Development Canada: Ottawa, ON, Canada, 2011.
12. Riveiro, M.; Pallotta, G.; Vespe, M. Maritime anomaly detection: A review. *WIREs Data Min. Knowl. Discov.* **2018**, *8*, e1266. [CrossRef]
13. Sidibé, A.; Shu, G. Study of Automatic Anomalous Behaviour Detection Techniques for Maritime Vessels. *J. Navig.* **2017**, *70*, 847–858. [CrossRef]
14. Tu, E.; Zhang, G.; Rachmawati, L.; Rajabally, E.; Huang, G.B. Exploiting AIS Data for Intelligent Maritime Navigation: A Comprehensive Survey From Data to Methodology. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 1559–1582. [CrossRef]
15. Zissis, D.; Chatzikokolakis, K.; Spiliopoulos, G.; Vodas, M. A Distributed Spatial Method for Modeling Maritime Routes. *IEEE Access* **2020**, *8*, 47556–47568. [CrossRef]
16. Cutlip, K. AIS for Safety and Tracking: A Brief History. 2017. Available online: https://globalfishingwatch.org/data/ais-for-safety-and-tracking-a-brief-history/ (accessed on 29 December 2021).
17. Committee on Maritime Advanced Information Systems. *Vessel Navigation and Traffic Services for Safe and Efficient Ports and Waterways: Interim Report*; National Academies Press: Washington, DC, USA, 1996. [CrossRef]
18. ITU-R. Recommendation M.1371-5 (02/2014)—Technical Characteristics for a Universal Shipborne Automatic Identification System Using Time Division Multiple Access in the VHF Maritime Mobile Band—M Series Mobile, Radiodetermination, Amateur and Related Satellite Services. Technical Report, International Telecommunication Union (ITU). 2014. Available online: https://www.itu.int/rec/R-REC-M.1371-5-201402-I/en (accessed on 29 December 2021).
19. Harchowdhury, A.; Sarkar, B.K.; Bandyopadhyay, K.; Bhattacharya, A. Generalized mechanism of SOTDMA and probability of reception for satellite-based AIS. In Proceedings of the 2012 5th International Conference on Computers and Devices for Communication (CODEC), Kolkata, India, 17–19 December 2012; pp. 1–4. [CrossRef]
20. Mazzarella, F.; Vespe, M.; Alessandrini, A.; Tarchi, D.; Aulicino, G.; Vollero, A. A novel anomaly detection approach to identify intentional AIS on-off switching. *Expert Syst. Appl.* **2017**, *78*, 110–123. [CrossRef]
21. Vesecky, J.F.; Laws, K.E.; Paduan, J.D. Using HF surface wave radar and the ship Automatic Identification System (AIS) to monitor coastal vessels. In Proceedings of the IEEE 2009 IEEE International Geoscience and Remote Sensing Symposium, Cape Town, South Africa, 12–17 July 2009; Volume 3, pp. 761–764. [CrossRef]
22. Cervera, M.A.; Ginesi, A. On the performance analysis of a satellite-based AIS system. In Proceedings of the 2008 10th International Workshop on Signal Processing for Space Communications (SPSC), Rhodes, Greece, 6–8 October 2008; pp. 1–8. [CrossRef]
23. Metcalfe, K.; Bréheret, N.; Chauvet, E.; Collins, T.; Curran, B.K.; Parnell, R.J.; Turner, R.A.; Witt, M.J.; Godley, B.J. Using satellite AIS to improve our understanding of shipping and fill gaps in ocean observation data to support marine spatial planning. *J. Appl. Ecol.* **2018**, *55*, 1834–1845. [CrossRef]
24. Nguyen, D.; Vadaine, R.; Hajduch, G.; Garello, R.; Fablet, R. A Multi-Task Deep Learning Architecture for Maritime Surveillance Using AIS Data Streams. In Proceedings of the 2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA), Turin, Italy, 1–3 October 2018; pp. 331–340. [CrossRef]
25. Goudossis, A.; Katsikas, S.K. Towards a secure automatic identification system (AIS). *J. Mar. Sci. Technol.* **2019**, *24*, 410–423. [CrossRef]
26. Kessler, G.C. Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity. *Trans. Nav. Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 279–286. [CrossRef]

27. Balduzzi, M.; Pasta, A.; Wilhoit, K. A security evaluation of AIS automated identification system. In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC), New Orleans, LA, USA, 8–12 December 2014; pp. 436–445. [CrossRef]
28. Department of Homeland Security. Small Vessel Security Strategy. 2008. Available online: https://www.dhs.gov/sites/default/files/publications/small-vessel-security-strategy.pdf (accessed on 29 December 2021).
29. Yang, D.; Wu, L.; Wang, S.; Jia, H.; Li, K.X. How big data enriches maritime research—A critical review of Automatic Identification System (AIS) data applications. *Transp. Rev.* **2019**, *39*, 755–773. [CrossRef]
30. Schwehr, K.D.; McGillivary, P.A. Marine Ship Automatic Identification System (AIS) for Enhanced Coastal Security Capabilities: An Oil Spill Tracking Application. In Proceedings of the OCEANS 2007, Vancouver, BC, Canada, 29 September–4 October 2007; pp. 1–9. [CrossRef]
31. European Maritime Safety Agency (EMSA). Procedures for requesting EMSA data from maritime applications. *Marit. Data Req. Proced.* **2018**. Available online: http://www.emsa.europa.eu/publications/data-request-procedure/download/5120/2076/23.html (accessed on 29 December 2021).
32. Laxhammar, R. Anomaly detection for sea surveillance. In Proceedings of the 2008 11th International Conference on Information Fusion Fusion, Cologne, Germany, 30 June–3 July 2008; pp. 1–8.
33. Lane, R.O.; Nevell, D.A.; Hayward, S.D.; Beaney, T.W. Maritime anomaly detection and threat assessment. In Proceedings of the 2010 13th International Conference on Information Fusion, Edinburgh, UK, 26–29 July 2010; pp. 1–8. [CrossRef]
34. Iphar, C.; Ray, C.; Napoli, A. Uses and Misuses of the Automatic Identification System. In Proceedings of the OCEANS 2019, Marseille, France, 17–20 June 2019; pp. 1–10. [CrossRef]
35. Androjna, A.; Perkovič, M.; Pavic, I.; Mišković, J. AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Appl. Sci.* **2021**, *11*, 5015. [CrossRef]
36. Kowalska, K.; Peel, L. Maritime anomaly detection using Gaussian Process active learning. In Proceedings of the 2012 15th International Conference on Information Fusion, Singapore, 9–12 July 2012; pp. 1164–1171.
37. Singh, S.K.; Heymann, F. Machine Learning-Assisted Anomaly Detection in Maritime Navigation using AIS Data. In Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020; pp. 832–838. [CrossRef]
38. Rong, H.; Teixeira, A.P.; Guedes Soares, C. Data mining approach to shipping route characterization and anomaly detection based on AIS data. *Ocean Eng.* **2020**, *198*, 106936. [CrossRef]
39. Vespe, M.; Visentini, I.; Bryan, K.; Braca, P. Unsupervised learning of maritime traffic patterns for anomaly detection. In Proceedings of the 9th IET Data Fusion Target Tracking Conference (DF&TT): Algorithms Applications, London, UK, 16–17 May 2012; pp. 1–5. [CrossRef]
40. Fang, Z.; Yu, H.; Ke, R.; Shaw, S.L.; Peng, G. Automatic Identification System-Based Approach for Assessing the Near-Miss Collision Risk Dynamics of Ships in Ports. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 534–543. [CrossRef]
41. Varlamis, I.; Tserpes, K.; Sardianos, C. Detecting Search and Rescue Missions from AIS Data. In Proceedings of the 2018 IEEE 34th International Conference on Data Engineering Workshops (ICDEW), Paris, France, 16–20 2018; pp. 60–65. ISSN: 2473-3490. [CrossRef]
42. Gao, M.; Shi, G.; Li, S. Online Prediction of Ship Behavior with Automatic Identification System Sensor Data Using Bidirectional Long Short-Term Memory Recurrent Neural Network. *Sensors* **2018**, *18*, 4211. [CrossRef]
43. Ford, J.H.; Peel, D.; Kroodsma, D.; Hardesty, B.D.; Rosebrock, U.; Wilcox, C. Detecting suspicious activities at sea based on anomalies in Automatic Identification Systems transmissions. *PLoS ONE* **2018**, *13*, e0201640. [CrossRef]
44. Pauly, D.; Zeller, D. Catch reconstructions reveal that global marine fisheries catches are higher than reported and declining. *Nat. Commun.* **2016**, *7*, 10244. [CrossRef]
45. Guillarme, N.L.; Lerouvreur, X. Unsupervised extraction of knowledge from S-AIS data for maritime situational awareness. In Proceedings of the 16th International Conference on Information Fusion, Istanbul, Turkey, 9–12 July 2013; pp. 2025–2032.
46. Wang, X.; Liu, X.; Liu, B.; de Souza, E.N.; Matwin, S. Vessel route anomaly detection with Hadoop MapReduce. In Proceedings of the IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 27–30 October 2014; pp. 25–30. [CrossRef]
47. Liu, B.; Souza, E.N.d.; Matwin, S.; Sydow, M. Knowledge-based clustering of ship trajectories using density-based approach. In Proceedings of the IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 27–30 October 2014; pp. 603–608. [CrossRef]
48. Radon, A.N.; Wang, K.; Glässer, U.; Wehn, H.; Westwell-Roper, A. Contextual verification for false alarm reduction in maritime anomaly detection. In Proceedings of the IEEE International Conference on Big Data (Big Data), Santa Clara, CA, USA, 29 October–1 November 2015; pp. 1123–1133. [CrossRef]
49. Fu, P.; Wang, H.; Liu, K.; Hu, X.; Zhang, H. Finding Abnormal Vessel Trajectories Using Feature Learning. *IEEE Access* **2017**, *5*, 7898–7909. [CrossRef]
50. Goodarzi, M.; Shaabani, M. Maritime Traffic Anomaly Detection from Spatio-Temporal AIS Data. In Proceedings of the 2nd of International Conference on Management and Fuzzy Systems (ICMFS Series), Eyvanekey, Iran, 29 November 2018; pp. 1–9.
51. Riveiro, M.; Johansson, F.; Falkman, G.; Ziemke, T. Supporting maritime situation awareness using self organizing maps and gaussian mixture models. *Front. Artif. Intell. Appl.* **2008**, *173*, 84.

52. Ristic, B.; La Scala, B.; Morelande, M.; Gordon, N. Statistical analysis of motion patterns in AIS Data: Anomaly detection and motion prediction. In Proceedings of the 11th International Conference on Information Fusion (FUSION), Cologne, Germany, 30 June–3 July 2008; pp. 1–7.
53. Laxhammar, R.; Falkman, G. Conformal Prediction for Distribution-Independent Anomaly Detection in Streaming Vessel Data. In Proceedings of the 1st International Workshop on Novel Data Stream Pattern Mining Techniques (StreamKDD), Washington, DC, USA, 25 July 2010; pp. 47–55. [CrossRef]
54. Laxhammar, R.; Falkman, G.; Sviestins, E. Anomaly detection in sea traffic - A comparison of the Gaussian Mixture Model and the Kernel Density Estimator. In Proceedings of the 12th International Conference on Information Fusion (FUSION), Seattle, WA, USA, 6–9 July 2009; pp. 756–763.
55. Smith, J.; Nouretdinov, I.; Craddock, R.; Offer, C.; Gammerman, A. Anomaly Detection of Trajectories with Kernel Density Estimation by Conformal Prediction. In *Artificial Intelligence Applications and Innovations (AIAI)*; Springer: Heidelberg, Germany, 2014; pp. 271–280. [CrossRef]
56. Anneken, M.; Fischer, Y.; Beyerer, J. Evaluation and comparison of anomaly detection algorithms in annotated datasets from the maritime domain. In Proceedings of the SAI Intelligent Systems Conference (IntelliSys), London, UK, 10–11 November 2015; pp. 169–178. [CrossRef]
57. Rhodes, B.J.; Garagic, D.; Dankert, J.R.; Stolzar, L.H.; Zandipour, M.; Seibert, M.; Bomberger, N.A. *Anomaly Detection & Behavior Prediction: Higher-Level Fusion Based on Computational Neuroscientific Principles*; IntechOpen Limited: London, UK, 2009.
58. Venskus, J.; Treigys, P.; Bernatavičienė, J.; Tamulevičius, G.; Medvedev, V. Real-Time Maritime Traffic Anomaly Detection Based on Sensors and History Data Embedding. *Sensors* **2019**, *19*, 3782. [CrossRef]
59. Nguyen, D.; Vadaine, R.; Hajduch, G.; Garello, R.; Fablet, R. GeoTrackNet–A Maritime Anomaly Detector Using Probabilistic Neural Network Representation of AIS Tracks and A Contrario Detection. *IEEE Trans. Intell. Transp. Syst.* **2021**, 1–13. [CrossRef]
60. Osekowska, E.; Johnson, H.; Carlsson, B. Grid Size Optimization for Potential Field based Maritime Anomaly Detection. *Transp. Res. Procedia* **2014**, *3*, 720–729. [CrossRef]
61. Soleimani, B.H.; Souza, E.N.D.; Hilliard, C.; Matwin, S. Anomaly detection in maritime data based on geometrical analysis of trajectories. In Proceedings of the 18th International Conference on Information Fusion (FUSION), Washington, DC, USA, 6–9 July 2015; pp. 1100–1105.
62. Venskus, J.; Kurmis, M.; Andziulis, A.; Lukošius, Z.; Voznak, M.; Bykovas, D. Self-learning adaptive algorithm for maritime traffic abnormal movement detection based on virtual pheromone method. In Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), Chicago, IL, USA, 26–29 July 2015; pp. 1–6. [CrossRef]
63. Guo, S.; Mou, J.; Chen, L.; Chen, P. An Anomaly Detection Method for AIS Trajectory Based on Kinematic Interpolation. *J. Mar. Sci. Eng.* **2021**, *9*, 609. [CrossRef]
64. Katsilieris, F.; Braca, P.; Coraluppi, S. Detection of malicious AIS position spoofing by exploiting radar information. In Proceedings of the 16th International Conference on Information Fusion (FUSION), Istanbul, Turkey, 9–12 July 2013; pp. 1196–1203.
65. Keane, K.R. Detecting Motion Anomalies. In Proceedings of the 8th ACM SIGSPATIAL Workshop on GeoStreaming (IWGS), Redondo Beach, CA, USA, 7 November 2017; pp. 21–28. [CrossRef]
66. d'Afflisio, E.; Braca, P.; Millefiori, L.M.; Willett, P. Maritime Anomaly Detection Based on Mean-Reverting Stochastic Processes Applied to a Real-World Scenario. In Proceedings of the 21st International Conference on Information Fusion (FUSION), Cambridge, UK, 10–13 July 2018; pp. 1171–1177. [CrossRef]
67. de Vries, G.K.D.; van Someren, M. Machine learning for vessel trajectories using compression, alignments and domain knowledge. *Expert Syst. Appl.* **2012**, *39*, 13426–13439. [CrossRef]
68. Handayani, D.O.D.; Sediono, W.; Shah, A. Anomaly Detection in Vessel Tracking Using Support Vector Machines (SVMs). In Proceedings of the International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuching, Malaysia, 22–24 December 2013; pp. 213–217. [CrossRef]
69. Zhen, R.; Jin, Y.; Hu, Q.; Shao, Z.; Nikitakos, N. Maritime Anomaly Detection within Coastal Waters Based on Vessel Trajectory Clustering and Naïve Bayes Classifier. *J. Navig.* **2017**, *70*, 648–670. [CrossRef]
70. Pallotta, G.; Vespe, M.; Bryan, K. Vessel Pattern Knowledge Discovery from AIS Data: A Framework for Anomaly Detection and Route Prediction. *Entropy* **2013**, *15*, 2218–2245. [CrossRef]
71. Pallotta, G.; Vespe, M.; Bryan, K. Traffic knowledge discovery from AIS data. In Proceedings of the 16th International Conference on Information Fusion (FUSION), Istanbul, Turkey, 9–12 July 2013; pp. 1996–2003.
72. Kazemi, S.; Abghari, S.; Lavesson, N.; Johnson, H.; Ryman, P. Open data for anomaly detection in maritime surveillance. *Expert Syst. Appl.* **2013**, *40*, 5719–5729. [CrossRef]
73. Lei, P.R. A framework for anomaly detection in maritime trajectory behavior. *Knowl. Inf. Syst. Vol.* **2016**, *47*, 189–214. [CrossRef]
74. Johansson, F.; Falkman, G. Detection of vessel anomalies—A Bayesian network approach. In Proceedings of the 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP), Melbourne, VIC, Australia, 3–6 December 2007; pp. 395–400. [CrossRef]
75. Mascaro, S.; Korb, K.B.; Nicholson, A.E. Learning Abnormal Vessel Behaviour from AIS Data with Bayesian Networks at Two Time Scales. Technical Report, 2010/4, Bayesian Intelligence. 2010. Available online: https://bayesian-intelligence.com/publications/TR2010_4_AbnormalVesselBehaviour.pdf (accessed on 29 December 2021).

76. Mascaro, S.; Nicholso, A.E.; Korb, K.B. Anomaly detection in vessel tracks using Bayesian networks. *Int. J. Approx. Reason.* **2014**, *55*, 84–98. [CrossRef]
77. Zor, C.; Kittler, J. Maritime anomaly detection in ferry tracks. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017; pp. 2647–2651. [CrossRef]
78. McAbee, A.; Scrofani, J.; Tummala, M.; Garren, D.; McEachen, J. Traffic pattern detection using the Hough transformation for anomaly detection to improve maritime domain awareness. In Proceedings of the 17th International Conference on Information Fusion (FUSION), Salamanca, Spain, 7–10 July 2014; pp. 1–6.
79. Wu, Y.; Patterson, A.; Santos, R.; Vijaykumar, N. Topology Preserving Mapping for Maritime Anomaly Detection. In Proceedings of the International Conference on Computational Science and Its Applications (ICCSA), Guimarães, Portugal, 30 June–3 July 2014. [CrossRef]
80. Terroso-Saenz, F.; Valdes-Vela, M.; Skarmeta-Gomez, A.F. A complex event processing approach to detect abnormal behaviours in the marine environment. *Inf. Syst. Front.* **2016**, *18*, 765–780. [CrossRef]
81. Kong, Z.; Jones, A.; Belta, C. Temporal Logics for Learning and Detection of Anomalous Behavior. *IEEE Trans. Autom. Control* **2017**, *62*, 1210–1222. [CrossRef]
82. Roy, J. Anomaly detection in the maritime domain. In *Optics and Photonics in Global Homeland Security IV*; Halvorson, C.S., Lehrfeld, D., Saito, T.T., Eds.; International Society for Optics and Photonics, SPIE Defense and Security Symposium: Orlando, FL, USA: 2008; Volume 6945, pp. 180–193. [CrossRef]
83. Alessandrini, A.; Mazzarella, F.; Vespe, M. Estimated Time of Arrival Using Historical Vessel Tracking Data. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 7–15. [CrossRef]
84. Chen, X.; Ling, J.; Yang, Y.; Zheng, H.; Xiong, P.; Postolache, O.; Xiong, Y. Ship trajectory reconstruction from AIS sensory data via data quality control and prediction. *Math. Probl. Eng.* **2020**, *2020*, 7191296. [CrossRef]
85. Willems, N.; Van De Wetering, H.; Van Wijk, J.J. Visualization of vessel movements. *Comput. Graph. Forum* **2009**, *28*, 959–966. [CrossRef]
86. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 1–22. [CrossRef]
87. Mao, S.; Tu, E.; Zhang, G.; Rachmawati, L.; Rajabally, E.; Huang, G.B. An Automatic Identification System (AIS) Database for Maritime Trajectory Prediction and Data Mining. In Proceedings of the International Conference of Extreme Learning Machine (ELM), Singapore, Yatai, China, 4–7 October 2017; pp. 241–257. [CrossRef]
88. Harati-Mokhtari, A.; Wall, A.; Brookes, P.; Wang, J. Automatic Identification System (AIS): A human factors approach. *J. Navig.* **2007**, *60*, 373–389. [CrossRef]
89. Mondal, K.; Banerjee, T.; Panja, A. Autonomous Underwater Vehicles: Recent Developments and Future Prospects. *Int. J. Res. Appl. Sci. Eng. Technol.* **2019**, *7*, 215–222. [CrossRef]
90. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Modelling Shipping 4.0: A Reference Architecture for the Cyber-Enabled Ship. In Proceedings of the Asian Conference on Intelligent Information and Database Systems (ACIIDS), Phuket, Thailand, 23–26 March 2020; pp. 202–217. [CrossRef]
91. Golz, M.; Boeck, F.; Ritz, S.; Holbach, G.; Richter, N.; Haselberger, P.; Wehner, W.; Schiemann, M.; Rentzow, E.; Müller, T.; et al. MUM - Large Modifiable Underwater Mother Ship: Requirements and Application Scenarios. In Proceedings of the 2018 OCEANS - MTS/IEEE Kobe Techno-Oceans (OTO), Kobe, Japan, 28–31 May 2018; pp. 1–9. [CrossRef]
92. Serra-Sogas, N.; O'Hara, P.D.; Pearce, K.; Smallshaw, L.; Canessa, R. Using aerial surveys to fill gaps in AIS vessel traffic data to inform threat assessments, vessel management and planning. *Mar. Policy* **2021**, *133*, 104765. [CrossRef]
93. nex. Spying on the Seven Seas with AIS. 2013. Available online: https://blog.rapid7.com/2013/04/29/spying-on-the-seven-seas-with-ais/ (accessed on 29 December 2021).
94. International Maritime Organization (IMO). *Report Of The Maritime Safety Committee On Its Seventy-Ninth Session, Agenda item 23 (15 December 2004). MSC 79/23*; IMO: London, UK, 2004.
95. European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the Commission Implementing Regulation (EU) No 404/2011. *Off. J. Eur. Union* **2012**, *C 37/1*, 5.
96. epic.org. EPIC v. USCG – Nationwide Automatic Identification System. Available online: https://epic.org/documents/epic-v-uscg-nationwide-automatic-identification-system/ (accessed on 29 December 2021).
97. Aziz, A.; Tedeschi, P.; Sciancalepore, S.; Pietro, R.D. SecureAIS - Securing Pairwise Vessels Communications. In Proceedings of the IEEE Conf. on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020; pp. 1–9. [CrossRef]