AIS Spoofing: A Tutorial for Researchers

Gary C. Kessler
Gary Kessler Associates
Ormond Beach, Florida, USA
gck@garykessler.net

Diane M. Zorri
Equis Group
Rome, Italy
diane.zorri@blackeagleholding.com

***Abstract*—Spoofing of Automatic Identification System (AIS) messages has evolved over the last decade from demonstrations of capability showing protocol vulnerabilities to performance art for researchers for showcasing various maritime scenarios to what is now a formidable maritime threat. This paper will provide an overview of the purpose of AIS, the protocol weaknesses, why signals are spoofed, and offer a detailed description of a specific spoofing example. Proposals for future research about AIS spoofing, how it can be detected, and the potential roles for machine learning and artificial intelligence are also presented.**

Keywords—Automatic Identification System (AIS), ITU Rec. M.1371, artificial intelligence, machine learning, protocol vulnerabilities, spoofing

I. Introduction

The Automatic Identification System (AIS) is the primary way to achieve situational awareness in the maritime domain. Designed in the 1990s in the aftermath of the 1999 grounding of oil tanker EXXON VALDEZ that caused an environmental disaster in Prince Edward Sound off the Gulf of Alaska, it became required equipment on board most commercial and merchant vessels when it was adopted in the 2002 International Convention for the Safety of Life at Sea (SOLAS) [1, 2]. A decade later, researchers demonstrated protocol vulnerabilities that make AIS spoofing possible amid the observations of actual spoofing events [3, 4, 5].

In order to help create an AIS research agenda, this paper will discuss details of how bogus AIS tracks can be created, how AIS spoofing has escalated over the years, and today's research challenges. To that end, Section II will describe the basics of the AIS protocol and the mechanics of spoofing an AIS route, and reasons for spoofing AIS in the first place. Section III will provide a specific AIS spoofing demonstration of capability, while Section IV will describe how spoofed routes can be detected, counter-detection measures, and areas for future research. Section V offers a summary and conclusions.

II. Background

This section will provide a description of the purpose of AIS, protocol weaknesses, and why spoofing activities are taking place.

A. AIS Defined

AIS is a maritime situational awareness system that allows vessels at sea to be aware of each other's presence (within approximately 20-30 nautical miles [nm]), maritime authorities to identify and monitor vessels in their area of responsibility, and ships and shore stations to exchange navigation, meteorological, safety, and other information. It is employed primarily for situational awareness and collision avoidance, vessel traffic management, search-and-rescue (SAR) operations, and coastal surveillance [1, 6].

The 2002 SOLAS Convention mandates that AIS transceivers be carried on ships of a certain size and/or function, such as ships of 300 or more gross tons operating internationally, cargo ships of 500 or more gross tons not operating internationally, and passenger vessels [2]. In the U.S., commercial power vessels 65 feet or more in length, power vessels certified to carry more than 150 passengers, and other specified ships must also carry AIS; warships are specifically exempted from the requirement to broadcast AIS information, although all modern warships do have AIS capability [6, 7]. Class A shipborne AIS devices comply with all AIS protocol requirements and are carried on vessels required to do so per SOLAS. Class B AIS devices—which might not be as fully featured as Class A equipment—may be carried on non-SOLAS vessels [1, 2, 6, 8].

The AIS network is composed of mobile stations (e.g., ships, Emergency Position Indicating Radio Beacons [EPIRBs], and AIS-equipped satellites and aircraft) and fixed stations (e.g., shore stations, repeaters, and specially equipped aids to navigation [ATONs]) [6]. The Global Positioning System (GPS) is integral to providing essential geographic positioning information to mobile AIS components, and most AIS transceivers have an integrated GPS receiver (as well as a port with which to receive information from external GPS devices).

Every AIS transceiver is assigned a unique, nine-digit Maritime Mobile Service Identity (MMSI). MMSIs generally includes a three-digit Maritime Identification Digit (MID), which is a country or region code that indicates the country where the device has been registered (e.g., 226-228 represents France, 247 represents Italy, and 366-369 represent the U.S. [9]).

MMSIs associated with ships are formatted as a MID followed by a six-digit serial number; the country identified in the MID is independent of the vessel's flag state. MMSIs indicating ATONs are of the form "99" followed by the MID followed by a four-digit serial number [9]. (ATONs can also be spoofed, although that is not the subject of this paper.)

B. AIS Protocol Vulnerabilities

The National Marine Electronics Association (NMEA) 0183 standard was first released in 1983 and defines data communication between maritime devices on board a ship. International Telecommunication Union (ITU) Recommendation M.1371, designed during the 1990s, adapted the NMEA 0183 AIS messages for broadcast over very high

frequency (VHF) radio between mobile and fixed AIS stations [8]. AIS transceivers share bandwidth using one of several different forms of time-division multiple-access (TDMA) [8].

Security was not a major priority in the pre-Internet era, even for a safety-oriented protocol. References [4, 5] were the first to clearly describe the security vulnerabilities in the AIS protocol:

- *Lack of validity checks:* AIS messages do not include any geographic validation information; a message's latitude and longitude, and other information, are assumed to be correct.
- *Lack of timing checks:* AIS messages do not contain any timestamp information indicating the point in time that the messages were transmitted.
- *Lack of authentication:* The AIS protocol provides no mechanism to authenticate the sender, thus anyone with the ability to craft or otherwise transmit an AIS packet can impersonate any other AIS device.
- *Lack of integrity checks:* AIS messages are broadcast in an unencrypted and unsigned form, thus providing everyone within range with the ability to intercept a message and allowing an interloper to modify transmissions.

C. The Purpose of Spoofing AIS

A history of the evolution of AIS spoofing is beyond the scope of this paper but has been addressed in other forums [3, 10, 11, 12, 13]. Of more pertinence to this paper are the reasons that AIS messages are being spoofed. The most innocuous reasons to spoof AIS include:

- demonstrations of capability, particularly related to the relative ease of spoofing;
- education related to understanding the AIS protocols and vessel interactions;
- research, including analysis of vessel routing under various conditions at sea; and
- simulation and training.

After the initial demonstration of capability and development of sample AIS spoofing tools more than 10 years ago [4, 5], spoofing of AIS moved quickly from an interesting academic exercise to much darker overtones. In recent years, AIS spoofing, reported by organizations such as the Center for Advanced Defense Studies (C4ADS) [14], Global Fishing Watch (GFW) [10], PoleStar [15], and Windward [16], has been used for many reasons:

- Illegal, unreported, and unregulated (IUU) fishing, a threat to fragile marine ecosystems, sustainable fisheries, economic security, and other natural resources and national assets. There have reported many cases of AIS spoofing to mask IUU fishing over the years [3, 17, 18].
- Smuggling or masking of actions in violation of international sanctions impacting some nation's maritime trade (Fig. 1). These actions have been particularly pervasive in the illegal oil trade, particularly by Iran, North Korea, and Russia, smuggling grain, oil, weapons, and other cargo, and masking the true location of more than a half dozen superyachts owned by Russian oligarchs after the 2022 invasion of Ukraine and subsequent sanctions [19, 20, 21, 22, 23, 24].
- Identity laundering, where a vessel with a criminal or suspicious past takes on the identity of a "clean" vessel in order to avoid detection or inspection by maritime authorities, or to defraud regulators, maritime insurance companies, or other commercial entities [19, 20, 24].
- Military offensive or defensive maneuvers, e.g., turning AIS off in order to mask the presence of military vessels or spoofing to falsely show the presence of warships for deterrence [10, 13, 25].
- An irregular form of warfare by which the spoofer manufactures a pretext in order to set a political stage. Consider the spoofing of HMS DEFENDER and HNLMS EVERTSEN in the Black Sea in mid-June, 2021 (Fig. 2), followed by spoofing of USS ROSS later that month. These bogus AIS tracks in close proximity to a Russian naval base in Crimea could have been anything from an information warfare operation in order to put pressure on the nations of the North Atlantic Treaty Organization (NATO) or part of a disinformation campaign offered as "proof" to the Russian people of NATO's aggressive policies towards that nation. If the latter, it could have been a pretext or precursor to the invasion of Ukraine some eight months later [10, 12, 26].
- Other nefarious acts such as the denial-of-service attacks on AIS in order to blind or confuse vessels; the broadcast of bogus weather, SAR, or closest point-of-approach messages; or the broadcast of fake virtual ATONs, all in order to advance piracy or other criminal activities [4, 5, 10, 12].

III. AIS Protocol Fundamentals

This section will describe the elements of the AIS protocol that are specific to a detailed description of the process of designing and developing an AIS spoof. The intent is to demonstrate the relative ease with which such an activity can be carried out.

Fig. 1. Movement of oil tanker TULIP, 9-13 December 2021. The blue dots represent the AIS track that was broadcast and the red dots represent the actual route according to satellite imagery [21].

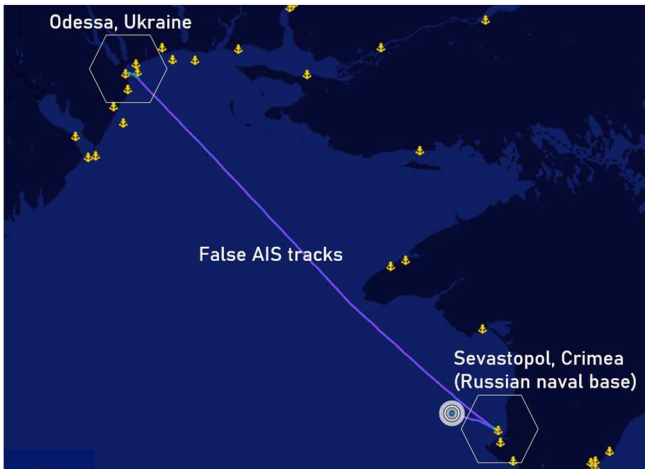

Fig. 2. False AIS track showing the movement of HMS DEFENDER and NHLMS EVERTSEN from Odessa to Sevastopol, 19-20 June 2021 [26].

The AIS protocol supports 27 message types [8, 27]. It is necessary to employ only a few types of messages in order to spoof a vessel and its track:

- Type 1 (Position Report Class A) messages transmit a vessel's current position and include such information as the latitude, longitude, course, heading, speed, and rate-of-turn, and whether the vessel is underway or moored.
- Type 5 (Static and Voyage Related Data) messages contain vessel identification information (e.g., vessel name, radio call sign, International Maritime Organization [IMO] number, ship type and dimensions) and voyage-specific information (e.g., ship's draft, destination, and estimated time of arrival [ETA]).
- Type 27 (Long Range AIS Broadcast) messages are similar in content to Type 1 messages, but are shorter and intended for long-range detection of the transmissions (e.g., by satellites).

Other messages might also be used but they are largely unnecessary for our purposes; a simple, effective spoof can be managed with just these messages.

A Bad Actor engaged in sending spoofed messages would likely start with a Type 5 message to identify the vessel. This would be followed by a series of Type 1 messages that identify the bogus positions of the vessel. For an effective spoof, the Type 1 messages need to be transmitted at the same real time rate as a real vessel would transmit; e.g., a vessel not turning would transmit a Type 1 message every 10 sec. if the speed is less than 14 knots (kn), every six sec. at speeds from 14-23 kn, and every two sec. at speeds greater than 23 kn [6, 8]. Type 5 messages should be repeated every 360 seconds [8].

Each message is associated with a MMSI. It is a misnomer to refer to a "ship's MMSI" when, in fact, MMSIs are assigned to maritime transmitters rather than vessels, but that is a common reference. A spoofer could, in fact, produce a bogus track with just Type 1 messages, but the lack of any vessel identifying data would immediately appear suspicious or, at least, odd to anyone seeing the sequence of messages.

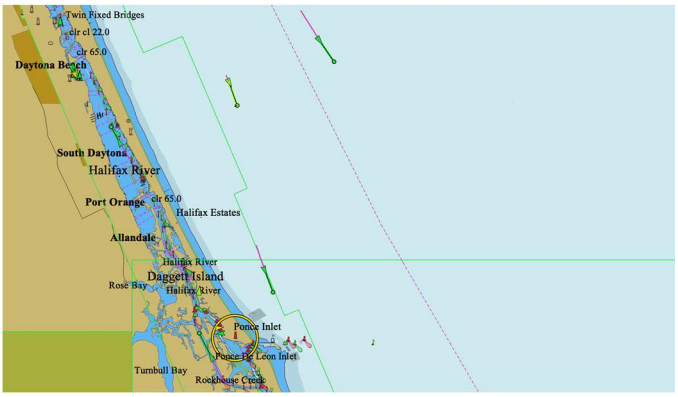

Fig. 3. AIS tracks observed on an OpenCPN chart display. Two of the vessels shown here are ghost vessels from tracks that are at least two years old. It is impossible to determine real vessels from ghost vessels from the chart display alone *(Source: Kessler)*.

The bogus messages then need to be transmitted over the air using any number of hardware and software VHF radio technologies. The signals should be seen by vessels and shore stations over at least a 20-30 nautical mile (nm) range and, quite probably, by satellites listening for AIS messages. This is how bogus AIS traffic ends up in the historical record.

A spoofed vessel that appears on an Electronic Chart Display and Information System (ECDIS) is indistinguishable from a real vessel. Figure 3 shows approximately a dozen AIS targets in the vicinity of Daytona Beach and Ponce de Leon Inlet on the east coast of Florida in April 2024. Two of the tracks are actually replays of vessels that were in the area in early 2021 [28, 29].

AIS Spoofing Demonstation Detail

This section will describe the process of designing and producing an AIS spoofed route, with the intent of demonstrating the relative ease with which such an activity can be carried out.

A. Choosing the Vessel

The purpose of creating a spoofed AIS track will drive the selection of a vessel and route. The spoof might involve a real ship, for example, if the purpose is identity laundering or pretext setting. A Bad Actor might spoof their own vessel for purposes of IUU fishing or sanction avoidance. Alternatively, someone might just make up a vessel for purposes of a demonstration or to generate random marine traffic.

For spoofing or research purposes, information about real vessels can be found by examining vessel tracking sources (e.g., Equasis or Vessel Finder), Wikipedia, or any other myriad open source intelligence (OSINT) sites. Military vessels are often attractive because they generally do not transmit AIS messages and that silence makes it easy to impersonate them.

For purposes of our demonstration, USS LAKE CHAMPLAIN, a U.S. Navy guided missile cruiser (MMSI 338951000) will be spoofed [30]. This vessel was selected because the first author lived on Lake Champlain (Vermont, US) for several decades. She was decommissioned in 2023.

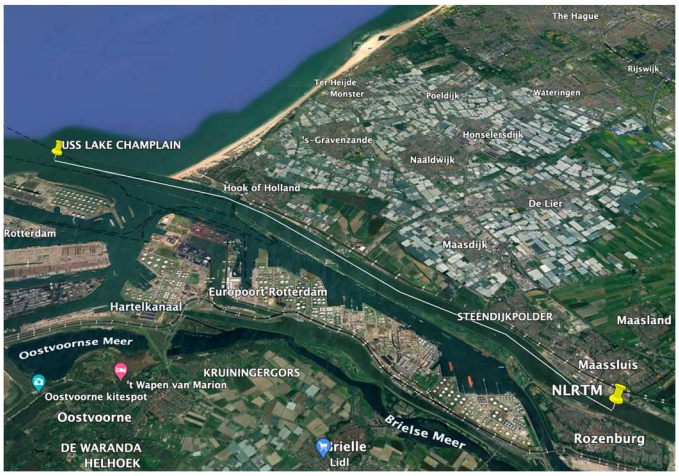

Fig. 4. An overview of the spoofed route of USS LAKE CHAMPLAIN in the Port of Rotterdam *(Source: Kessler)*.

B. *Choose the Location and Build the Route*

There are a variety of ways with which to build a spoofed route; manually with a chart, using a software simulator (e.g., NMEASimulator), or with charting software (e.g., OpenCPN). The route requires a starting point and some number of legs, which can be defined in terms of speed, course, and distance or speed and ending position.

The speed of the vessel during each leg and the distance covered will determine the number of AIS Type 1 messages that need to be created. As an example, a vessel sailing at 6 kn is moving 3.1 meters per second. At that speed, a Type 1 message needs to be sent every 10 sec., during which time the ship will have advanced 31 m.

In the example here, USS LAKE CHAMPLAIN will be shown entering and moving 9.28 nm in the Port of Rotterdam, commencing at position 51.991808°N, 004.042953°E (Fig. 4). This route is composed of nine separate legs. At an average speed of 6.2 kn, it will take 89.8 minutes to traverse this route. The course (true), distance, and endpoint of each leg is shown in Table 1.

TABLE I. PER-LEG DESCRIPTION OF THE ROUTE

Leg	Course	Distance	End. Lat.	End Long.
1	108°	2.94 nm	51.976642°N	004.118607°E
2	122°	0.74 nm	51.970105°N	004.135585°E
3	130°	1.23 nm	51.956925°N	004.161068°E
4	131°	1.24 nm	51.943364°N	004.186370°E
5	120°	1.51 nm	51.930775°N	004.221716°E
6	140°	0.89 nm	51.919411°N	004.237175°E
7	145°	0.32 nm	51.915042°N	004.242135°E
8	130°	0.41 nm	51.910650°N	004.250620°E

C. *Create the Set of AIS Messages*

The first message to create is an AIS Type 5 message, which will contain such information as the vessel name, type and size of the vessel, destination, etc.; these static vessel- and voyage-related messages are sent every six minutes or upon request. The specifications of USS LAKE CHAMPLAIN necessary to prepare a Type 5 message can be found in a variety of sites online; one plausible Type 5 message requires two separate transmissions (called "sentences") and looks like this:

```
!AIVDM,2,1,2,A,553?sF800000p=0p001E=>0h4dF0<P4m
     0h4Tp00S6ab9936hNISS4U3@0000,0*41
!AIVDM,2,2,2,A,00000000008,2*2E
```

The next messages are AIS Type 1 position information. At a speed of 6.2 kn, we need to produce one message every 10 sec.; thus, this route will require approximately 5,350 messages. The first few Type 1 messages of this route are:

```
!AIVDM,1,1,,A,153?sF000v0BPMFMgwk4>3J00000,0*01
!AIVDM,1,1,,A,153?sF000v0BPUdMgwUl>3FD0000,0*25
!AIVDM,1,1,,A,153?sF000v0BPf4MgwHD>3H`0000,0*59
```

D. *A Diversion on Great Circle Calculations*

Determining the next position on the leg employs great circle calculations in order to find the shortest distance (Fig. 5). A ship does not move in two dimensions as it appears on a Mercator projector chart, but along the curved surface of a sphere [31, 32]. Equations (1) and (2) show how to compute a new position given a current latitude and longitude, distance navigated (d, in nm), course (θ, in radians), and radius of the Earth (r = 3,444 nm). (Nautical miles are the units for d and r if speed is in kn; if speed is given in miles per hour or km per hour, d and r unit will be miles or km, respectively.)

$$\text{new\_lat} = \text{lat} + d * \sin(\theta) / r \quad (1)$$

$$\text{new\_long} = \text{long} + d * \cos(\theta) / (r * \cos(\text{lat})) \quad (2)$$

Note that one degree of latitude (which measures the north-south position) and one degree of longitude (which measures the east-west position) do not represent the same linear distance. One degree of latitude is 60 nm. One degree of longitude is 60 nm only at the Equator and then decreases to zero as the position approaches the poles (i.e., a latitude of ±90°). Therefore, to calculate the distance of changes in longitude, you must know the latitude. Fortunately, nearly all programming languages include geometry libraries that can perform great circle calculations (e.g., [33]).

E. *Play the Messages*

For the spoof to be plausible, the AIS messages must be transmitted in relative real time; i.e., this 89.8 min. route needs to be played back in 89.8 min. For demonstration purposes, the messages can be played to ECDIS software, such as OpenCPN (Fig. 6).

Fig. 5. The great circle path is generally shorter than the direct, or rhumb line, path [31].

Fig. 6. The USS LAKE CHAMPLAIN appearing to be in the Port of Rotterdam, displayed on OpenCPN *(Source: Kessler)*.

A real spoof, of course, would be transmitted over the air where it could be picked up by any AIS receiver within range, including satellites, per ITU Rec. M.1371. AIS messages are transmitted over maritime VHF radio channels 87B (161.975 MHz) and 88B (162.025 MHz), aka AIS channels 1 and 2, respectively. This is referred to as terrestrial AIS (T-AIS). Class A transponders also broadcast Type 27 messages on VHF channels 75 (156.775 MHz) and 76 (156.825 MHz), aka AIS channels 3 and 4, respectively. These messages are intended to support satellite-based AIS (S-AIS) [6, 8].

The AIVDM messages shown here are at the top layer of the AIS protocol stack; ITU Rec. M.1351 also describes the data link layer bit stream and radio signal characteristics of the transmission. Software-defined radio (SDR), coupled with a hardware transmitter, provides a low-cost mechanism with which to transmit the messages [34, 35]. A spoofing agent can appear to other receivers exactly like any other AIS transponder [36]. (Researchers should be aware that such over-the-air transmissions violates the SOLAS Convention, as well as the laws of most countries [36].)

After spoofing a single vessel on a route, it is simple to build similar routes for other vessels as a way to spoof a fleet of anything from fishing vessels to warships.

IV. Detection, Research, and Countermeasures

It is sometimes easy to detect a bogus AIS track by simply observing the advertised position and route information. It is a red flag, for example, if the speed never changes; while an ETA can be calculated based on the average speed of the route, a vessel at sea cannot maintain the exact same speed over any sort of distance. Similarly, while the course might remain unchanged over large distances, a vessel's heading is constantly changing. Observe that HMS DEFENDER and NHLMS EVERTSEN appear to have taken a remarkably straight path from Odessa to Sevastopol (Fig. 2).

It is easy to avoid these obvious clues when creating a false track by randomly adding or subtracting some small value from the heading and speed parameters in the Type 1 message. This will not protect the bogus route from being detected upon being deeply scrutinized but will eliminate the obvious.

There are, in fact, several ways to detect spoofing, determine a vessel's actual route and position, and corroborate the true activities of a vessel. In the case of DEFENDER and EVERTSEN, contemporaneous photographs and other evidence showed the vessels moored at their dock in Odessa during the time that the AIS track purported that they were at sea [26].

Satellite imagery can also be employed to demonstrate the true position of a ship [37, 38, 39]. In one early example of spoofing of multiple warships, false AIS tracks showed HMS QUEEN ELIZABETH and five other warships from Belgium, the Netherlands, and the U.K. steaming in St. George's Channel towards the Irish Sea. Analysts at Global Fishing Watch and SkyTruth examined satellite imagery to determine that none of the vessels were in the area at the time of the purported track [40].

There is a concept in physical and cyber security that suggests that a defensive system—everything from a lock or safe to a firewall or encryption scheme—does not need to provide absolute protection forever, but simply needs to slow down an adversary long enough for an attack on the system to be detected and a response mounted. Similarly, a Bad Actor does not need to keep its nefarious behavior a secret forever, but just long enough to do the damage that they intend or spread the fog of confusion.

This suggests that not all spoofed tracks need to be perfect or hardened against detection. A poorly designed spoofed AIS track might be detected days or weeks later upon close analysis but be sufficient in the short-term for the purpose of causing momentary uncertainty in a local area. The flaws and trickery might be obvious in the long-term upon examination but can still be quite effective in the near-term.

For this reason, analytic methods need to be designed that can detect bogus AIS tracks in as near-real-time as possible. The problem of real-time analysis is made more difficult by the fact that there are probably more than 100,000 merchant ships at sea at any given time [41] and public AIS aggregation sites report tracking more than 740,000 AIS-equipped vessels [42].

The complexity and intricacy of AIS data presents an ideal opportunity for machine learning and artificial intelligence (AI) systems [37, 43, 44]. As an example, AI could be used to analyze an AIS track's reported MMSI and determine whether the MMSI is bogus (i.e., unassigned), if it belongs to a vessel that is currently transmitting 20,000 km away on the other side of the world, or if it appears to be legitimate.

Another example would be the creation of near-real-time AIS track analysis. Using the enormous databases of existing AIS information, AI could compare real tracks with bogus tracks in order to better understand syndromes that might indicate a spoofed route in real-time.

Routes used for AI learning and modeling must be valid, of course, or else researchers might inadvertently poison the machine learning models by using flawed data. In fact, adversarial AI could deliberately taint the learning conditions with false AIS data [45].

Once such track syndrome models are created, defensive AI processes could check real-time AIS broadcasts to detect possible spoofing. Naturally, offensive AI processes could be

utilized as a countermeasure by using the same models to build bigger and better bogus tracks that appear to be real and slow-down detection [45].

But even checking the veracity of an AIS route in real-time would have limited use in detecting a replay attack because the visual display and messages, in such a case, are simply retransmissions of an actual route and legitimate AIS messages. Detection of a replay would require some form of supplementary information such as examining the historical record to see if the route was an exact duplicate of a previous route or, in the longer term, integration of satellite imagery or VHF radio traffic analysis.

V. Summary and Conclusion

The AIS protocols are known to have several weaknesses. A competent programmer with knowledge of AIS protocols, RF transmission, or a software-defined radio can exploit these weaknesses to spoof the route of nearly any vessel. Moreover, AIS spoofing is a low-cost, low-risk, and high-gain attack vector. While there are efforts currently in play to provide a more secure transmission channel for AIS employing the VHF Data Exchange System (VDES), it is unlikely to help the situation for several years [46].

Even military vessels are not immune from AIS spoofing. All global navigation satellite systems (GNSS) employ encrypted channels for military applications, thus making spoofing military GNSS signals extraordinarily difficult. This is not true with AIS, where all vessels use the same protocols and VHF channels for public situational awareness. In fact, since military vessels are generally not transmitting AIS messages, it might be more difficult to detect a spoof of one in real-time [47]. Although NATO has adopted warship-specific guidelines for the use of AIS on warships, including the use of encryption [48, 49], these do not obviate the possibility of NATO warships being spoofed, as has been seen on multiple occasions [26, 40].

The primary goal of this paper is to advance the academic and scientific research in this area where vessels are broadcasting safety-related information under adversarial conditions. The authors are mindful that disclosure of such information can make it easier for Bad Actors to engage in nefarious activities. This is a debate that has been going on in the information security field since at least the 1980s. We recognize the potential for the information presented here to be repurposed and utilized for malign purposes by malicious actors. However, we believe that the most egregious offenders among such actors are already adept at engaging in these behaviors and are actively doing so. The primary beneficiaries of this information are individuals and entities with noble intentions, including researchers who require a structured agenda. With this objective in mind, we present this report.

Acknowledgments

Thanks are given to Alessio Armenzoni (U.S. Geospatial Intelligence Foundation), Giangiuseppe Pili (James Madison University), and other, anonymous reviewers for their comments and suggestions.

Additional Information

The authors recognize that the image detail might be difficult to discern because of their small size. Larger-sized images can be downloaded from *https://www.garykessler.net/gck/MarCaS_2024.pdf*.

Some tools that will create and interpret AIS messages can be found at [28]. If interested in source code for route spoofing research, contact the first author directly.

References

[1] K. Cutlip, "AIS for safety and tracking: a brief history," Global Fishing Watch, March 2017, https://globalfishingwatch.org/data/ais-brief-history, Accessed: July 9, 2024.

[2] International Convention for the Safety of Life at Sea (SOLAS), Chap. V, Safety of navigation, https://assets.publishing.service.gov.uk/media/5a7f0081ed915d74e33f3c6e/solas_v_on_safety_of_navigation.pdf, Accessed: July 9, 2024.

[3] A. Androjna, M. Perkovič, I. Pavic, and J. Mišković, "AIS data vulnerability indicated by a spoofing case-study," Appl. Sci., vol. 11, iss. 11, art. 5015, May 2021, DOI: 10.3390/app11115015.

[4] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of AIS automated identification system," Proc. 30th Annual Computer Security Applications Conference (ACSAC '14), pp. 436-445, December 8-12, 2014, DOI: 10.1145/2664243.2664257.

[5] M. Balduzzi, K. Wilhoit, and A. Pasta, "A security evaluation of AIS," Trend Micro Research Paper, December 2014, https://documents.trendmicro.com/assets/white_papers/wp-a-security-evaluation-of-ais.pdf, Accessed: July 9, 2024.

[6] International Association of Marine Aids to Navigation and Lighthouse Authoprities (IALA), "An overview of AIS," 2nd ed., IALA Guideline 1082, June 2016, https://www.navcen.uscg.gov/sites/default/files/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf, Accessed: July 9, 2024.

[7] Title 33, Code of Federal Regulations (CFR), §164.46, Automatic Identification System, https://www.navcen.uscg.gov/ais-requirements, Accessed: July 9, 2024.

[8] International Telecommunication Union Radiocommunication Sector (ITU-R), Recommendation M.1371-5, "Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band," February 2014, https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1371-5-201402-I!!PDF-E.pdf, Accessed: July 9, 2024.

[9] International Telecommunication Union (ITU), Table of Maritime Identification Digits [website], https://www.itu.int/en/ITU-R/terrestrial/fmd/Pages/mid.aspx, Accessed: July 9, 2024.

[10] B. Bergman, "Systematic data analysis reveals false vessel tracks," Global Fishing Watch, July 21, 2021, https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/, Accessed: July 9, 2024.

[11] G.C. Kessler, "GPS:AIS spoofing attacks and some tools," DEF CON 28 Hack the Sea Village [video], August 2020, https://www.youtube.com/watch?v=9xBze1hZVgk, Accessed: July 9, 2024.

[12] G.C. Kessler and S.D. Shepard, Maritime Cybersecuity: A Guide for Leaders and Managers, 2nd ed. Kindle Direct Publishing, 2024, https://www.maritimecybersecuritybook.com/, Accessed: July 9, 2024.

[13] G.C. Kessler and D.M. Zorri, "Cross domain IW threats to SOF maritime missions: implications for U.S. SOF," Joint Special Operations University (JSOU) Report 21-4, May 15, 2021, https://jsouapplicationstorage.blob.core.windows.net/press/12/21-4.pdf, Accessed: July 9, 2024.

[14] Center for Advanced Defense Studies (C4ADS), "Above us only stars," March 26, 2019, https://c4ads.org/reports/above-us-only-stars/, Accessed: July 9, 2024.

[15] Courtnell, "What is spoofing? Your complete guide (+4 key AIS spoofing typologies)," Pole Star Space Applications, February 10, 2023, https://www.polestarglobal.com/resources/what-is-spoofing-your-complete-guide-4-key-ais-spoofing-typologies, Accessed: July 9, 2024.

[16] Windward, "AIS spoofing: New technologies for new threats," December 4, 2022, https://windward.ai/blog/ais-spoofing-new-technologies-for-new-threats/, Accessed: July 9, 2024.

[17] Oceana, "Now you see me, now you don't: vanishing vessels along Argentina's waters," June 2021, https://usa.oceana.org/wp-content /uploads/sites/4/2021/06/oceana_argentina_mini_report_finalupdated .pdf, Accessed: July 9, 2024.

[18] Oceana, "Oceana finds 300 Chinese vessels pillaging the Galapagos for squid," September 2020, https://usa.oceana.org/reports/oceana-finds-300-chinese-vessels-pillaging-galapagos-squid/, Accessed: July 9, 2024.

[19] A. Androjna, I. Pavić, L. Gucma, P. Vidmar, M. Perkovič, "AIS data manipulation in the illicit global oil trade," J. Marine Sci. & Eng, vol. 12, December 2023, DOI: 10.3390/jmse12010006.

[20] A. Boling, L. Kuo, L. Snyder, and L. Sung, "UNMASKED: vessel identity laundering and North Korea's maritime sanctions evasion," Center for Advanced Defense Studies (C4ADS), September 9, 2021, https://c4ads.org/wp-content/uploads/2021/09/Unmasked-Brief.pdf, Accessed: July 9, 2024.

[21] J. Goodman, "Digital warfare tech at sea helping US foes evade sanctions," AP News, February 3, 2022, https://apnews.com/article /technology-business-middle-east-iran-shipping-44d5cdc52e589c44a7bb 0fc5be59d156, Accssed: July 9, 2024.

[22] G. Pili, J. Crawford, and N. Loxton, "Greyzone lawfare: Russia and the voyages of the SPARTA IV," Royal United Services Institute for Defence and Security Studies, September 13, 2023, https://www.rusi.org/explore-our-research/publications/commentary/greyzone-lawfare-russia-and-voyages-sparta-iv, Accessed: July 9, 2024.

[23] M. Schuler, "Windward flags dark activity and ship-to-ship transfers to launder Ukrainian grain," gCaptain, July 20, 2022, https://gcaptain.com/windward-flags-dark-activity-and-ship-to-ship-transfers-to-launder-ukrainian-grain/, Accessed: July 9, 2024.

[24] United Nations, Security Council, Final Report of the Panel of Experts Submitted Pursuant to Resolution 2680, S/2024/215, March 7, 2024, https://daccess-ods.un.org/*acc*ess.nsf/Get?OpenAgent&DS=S/2024/215 &Lang=E, Accessed: July 9, 2024.

[25] D.M. Zorri and G.C. Kessler, "Position, navigation, and timing: weaponization in the maritime domain orientation in the era of great systems conflict," Joint Forces Quarterly, vol. 112, pp. 12-21, 1st Quarter 2024, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-112/Article /Article/3678180/position-navigation-and-timing-weaponization-in-the-maritime-domain-orientation/, Accessed: July 9, 2024.

[26] H.I. Sutton, "Positions of two NATO ships were falsified near Russian Black Sea naval base," USNI News, June 21, 2021, https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base, Accessed: July 9, 2024.

[27] E.S. Raymond, "AIVDM.AIVDO protocol decoding" [website], June 2023, https://gpsd.gitlab.io/gpsd/AIVDM.html, Accessed; July 9 2024.

[28] G.C. Kessler, "AIS related-tools" [website], March 25, 2024, https://www.garykessler.net/software/index.html#ais, Accessed; July 9 2024.

[29] G.C. Kessler, "AIS tools demo," DEF CON 29 Hack the Sea Village [video], August 2021, https://www.youtube.com/watch ?v=TL9Inu2NqVY, Accessed; July 9 2024.

[30] https://www.vesseltracker.com/en/Ships/Uss-Lake-Champlain-I380585 .html, Accessed; July 9 2024.

[31] R. Shrubb, "Great circles - the shortest distance between two points," Kavas Blog, no date, https://www.kavas.com/blog/great-circle-and-rhumbline.html, Accessed: July 9, 2024.

[32] T.J. Cutler, Dutton's Nautical Navigation, 15th ed. Annapolis: Naval Institute Press, 2004.

[33] PerlDoc Browser, v5.40.0, Math::Trig, Great circle distances and directions, no date, https://perldoc.perl.org/Math::Trig#GREAT-CIRCLE-DISTANCES-AND-DIRECTIONS, Accessed: July 9, 2024.

[34] F. R. G. Cruz, R. C. M. Gania, B. W. C. Garcia and J. C. R. Nob, "Implementing Automatic Identification System transmitter on Software Defined Radio," 2018 IEEE 10th Int. Conf. on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM), Baguio City, Philippines, 2018, pp. 1-4, DOI: 10.1109/HNICEM.2018.8666288.

[35] M. M. Marques, D. Teles, V. Lobo, and G. Capela, "Low-cost AIS transponder using an SDR device," OCEANS 2019 MTS/IEEE SEATTLE, Seattle, WA, USA, 2019, pp. 1-4, DOI: 10.23919 /OCEANS40490 .2019.8962863.

[36] M. Louart, J.-J. Szkolnik, A.-O. Boudraa, J.-C. Le Lann, and F. Le Roy, "Detection of AIS messages falsifications and spoofing by checking messages compliance with TDMA protocol," Dig. Sig. Proc., vol. 136, March 28, 2023, DOI: 10.1016/j.dsp.2023.103983.

[37] O. Ballinger, "Automatic detection of dark ship-to-ship transfers using deep learning and satellite imagery," arXiv, April 11, 2024, DOI: 10.48550/arXiv.2404.07607.

[38] P. Heiselberg, H.B. Pedersen, K.A. Sørensen, and H. Heiselberg, "Identification of ships in satellite images," IEEE J. Sel. Top. App. Earth Observations and Remote Sensing, vol. 17, pp. 6045-6054, February 22, 2024, DOI: 10.1109/JSTARS.2024.3368508.

[39] U. Kanjir, H. Greidanus, and K. Oštir, "Vessel detection and classification from spaceborne optical images: A literature survey," Remote Sensing of Env., Vol. 207, pp. 1-26, March 15, 2018, DOI: 10.1016 /j.rse.2017.12.033.

[40] M. Harris, "Phantom warships are courting chaos in conflict zones," WIRED, July 29, 2021, https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/, Accessed: July 9, 2024.

[41] Electronic Quality Shipping Information System (Equasis), "The 2022 world merchant fleet," December 2023, https://www.equasis.org/Fichiers /Statistique/MOA/Documents%2520availables%2520on%2520statistics %2520of%2520Equasis/Equasis%2520Statistics%2520-%2520The %2520world%2520fleet%25202022.pdf, Accessed: July 9, 2024.

[42] Vessels database/AIS ship positions [website], July 8, 2024, https://www.vesselfinder.com /vessels; Accessed: July 9, 2024.

[43] J.N.A. Campbell, A.W. Isenor, and M. Dais Ferreira, "Detection of invalid AIS messages using machine learning techniques," Procedia Computer Science, Vol. 205, pp. 229-238, September 22, 2022, DOI: 10.1016/j.procs.2022.09.024.

[44] C. Gamage, R. Dinalankara, J. Samarabandu, and A. Subasinghe, "A comprehensive survey on the applications of machine learning techniques on maritime surveillance to detect abnormal maritime vessel behaviors," WMU J Marit Affairs, Vol. 22, pp. 447–477, December 2023, DOI: 10.1007/s13437-023-00312-7.

[45] M.J. Walter, A. Barrett, D.J. Walker, and K. Tam, "Adversarial AI testcases for maritime autonomous systems." AI, Comp. Sci. and Robotics Tech., Vol. 2023, Iss. 2, pp. 1-29, April 2023, DOI: 10.5772/acrt.15.

[46] I. Gonin, G. Johnson, J. Spilsbury, S. Ordell, and M. Wurl, "Very High Frequency Data Exchange System (VDES) technology roadmap," Report CG-D-02-21, U.S. Coast Guard Research and Development Center, January 2021, https://apps.dtic.mil/sti/trecms/pdf/AD1135170.pdf, Access: July 9, 2024.

[47] G.C. Kessler, "AIS spoof of a warship," DEF CON 28 Hack the Sea Village [video], August 2021, https://www.garykessler.net/gck /202108_MOSKVA_spoof.mp4, Accessed: July 9, 2024.

[48] North Atlantic Treaty Organization (NATO) Standardization Agency, "Warship - Automatic Identification System (W-AIS)," Technical Report STANAG 4668 (Edition 2), March 25, 2010, https://nso.nato.int/nso/nsdd /main/standards/stanag-details/7713/EN, Accessed: July 9, 2024.

[49] North Atlantic Treaty Organization (NATO) Standardization Agency, "Automatic Identification System (AIS) on warships," Technical Report STANAG 4669 (Edition 2), March 25, 2010, https://nso.nato.int/nso/nsdd /main/standards/stanag-details/7714/EN, Accessed: July 9, 2024, Accessed: July 9, 2024.