Use of Legacy Maritime Protocols Increases Exploitability of Virtual Aids to Navigation

May 2024

INL Cybercore Analyst Team
DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.
Use of Legacy Maritime Protocols Increases Exploitability of Virtual Aids to Navigation

INL Cybercore Analyst Team

May 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517
Use of Legacy Maritime Protocols Increases Exploitability of Virtual Aids to Navigation

Analytic Summary
With increased reliance on Virtual Aid(s) to Navigation (VAtoN) - also known as electronic Aid(s) to Navigation (eAtoN), or virtual buoys - a cyber event is likely to cause disruption to international maritime shipping. VAtoN has no physical hardware for visual reference and displays only on a vessel’s Electronic Chart Display Information System (ECDIS) and Automatic Radar Plotting Aid (ARPA); therefore, mariners must rely on the accuracy of the information provided. As VAtoN uses the National Maritime Electronics Association (NMEA) 0183 protocol for both Global Navigation Satellite System (GNSS) and Automatic Identification System (AIS), an insecure protocol that has been proven susceptible to spoofing, denial, and manipulation, the likelihood of a cyber-related event increases substantially.

Background
Aid(s) to Navigation (AtoN) assist in the safe navigation of maritime vessels through constricted, shallow, or otherwise challenging waterways. The three types of AtoN include: real, synthetic, and virtual. All three types of AtoN use AIS, which relies on GNSS to provide vessels early awareness of navigational situations.1,2,3,4,5,6

- **Real AtoN** use physical equipment mariners can see in the water, such as a buoy with an AIS transmitter attached to transmit to all vessels in the vicinity.8,9,10
- **Synthetic AtoN** also use physical equipment mariners can see in the water but may or may not feature an attached AIS transmitter. If the marker does not feature an attached AIS transmitter, an AIS signal is transmitted from another location (typically on land) to denote the AtoN’s location.11,12,13
- **Virtual AtoNs** have no physical structure and are solely an AIS signal transmitted to mark an area for navigational awareness. The virtual AtoN can only be seen on the vessel by equipment that can interpret AIS signals, such as an ECDIS or ARPA.14,15,16,17,18
Virtual Aids to Navigation (VAtoN) Usage

VAtoNs have become increasingly valuable in ensuring safety of navigation.²⁰,²¹,²²,²³ They use AIS, which is mandated to be onboard all vessels 300 gross tons or greater and engaged in international voyages, 500 gross tons or greater and not engaged in international voyages, and all passenger ships regardless of size.²⁴,²⁵ VAtoN are placed via the transmission of AIS message 21 from a AIS transmission station to pinpoint the location of the AtoN (see Figure 2).²⁶,²⁷

**Figure 1: Visual and Chart symbols for different aid(s) to Navigation²⁹**

<table>
<thead>
<tr>
<th>Paper Chart Symbol</th>
<th>Type</th>
<th>What they look like out the window of a ship’s bridge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green Lateral Buoy</td>
<td>Real non-AIS aid</td>
<td><img src="image1" alt="Image of Real non-AIS aid" /></td>
</tr>
<tr>
<td>Red Lateral Buoy</td>
<td>Real AIS aid and Synthetic AIS aid</td>
<td><img src="image2" alt="Image of Real AIS aid and Synthetic AIS aid" /></td>
</tr>
<tr>
<td>Safe Water Mark</td>
<td>Virtual AIS aid</td>
<td><img src="image3" alt="Image of Virtual AIS aid" /></td>
</tr>
</tbody>
</table>

* These examples are based on the IALA-B buoyage system that is used in North and South America. In the IALA-A system, used in U.S. territories in the South Pacific, the square and triangle top marks shown on V-AIS aids are switched with each other. Refer to the graphic at Q 130.1 in U.S. Chart No. 1 for more information about IALA buoyage regions.

**Figure 2: AIS message 21 showing the Virtual AtoN flag setting²⁷**

According to the International Maritime Organization (IMO), a VAtoN should not be used as a permanent marker where physical markers are able to be used. They may be “considered for marking an object or feature where it is difficult or economically unreasonable to establish a physical AtoN due to
environmental constraints." This could include situations when a marker needs to be in deep water, harsh sea conditions, or places such as shoals that change with time due to current or weather effects and where the object or feature is impossible to maintain as charted because of changes occurring over time.

Accepted usage from industry and organizations are as follows:

- Temporarily marking a recent wreck or danger.
- Temporarily marking locations where buoys are removed seasonally due to ice.
- Temporarily marking locations where buoys are removed due to maintenance, storms, or natural disasters.
- Permanently marking areas where a physical AtoN cannot be placed.
- Permanently marking locations where a physical AtoN could, itself, cause a navigation hazard or conflict with navigational requirements.

Since initial introduction and testing in 2007, the use of VAtoNs has increased around the world. Cases such as the MV Ice Prince foundering 26 miles off Portland Bill in the English Channel at the entrance to the Traffic Separation Scheme (TSS) required the use of VAtoN to mark the wreck. As the TSS area is controlled by France, the use of VAtoN allowed vessels to gain early warning and navigate around the wreck while overcoming the potential language barrier of the controlling country. VAtoN are also currently used to mark restricted or anchorage areas in the Great Lakes region as well as rivers and other areas. Although use of VAtoN can be seen as cost effective and easier to maintain, the communication protocols VAtoN use are insecure leading to inherent vulnerabilities.

Virtual Aids to Navigation Vulnerabilities and Threats

VAtoN requires the use of AIS to be effectively seen on vessels. The AIS also requires use of the GNSS for location and timing. The GNSS is comprised of several satellite constellations, including the American Global Positioning System (GPS) constellation, the European Galileo constellation, the Chinese BeiDou constellation, and the Russian Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS) constellation.

Both AIS and GNSS use the NMEA protocol to be compatible with vessel navigation systems. The primary protocol used is known as NMEA-0183. This protocol is an American Standard Code for Information Interchange (ASCII)-based protocol that is defined in the International Electrotechnical Commission (IEC) standards 61162 and was first adopted in 1995. Older protocols, such as NMEA-0183, were not designed to be secure and has contributed to a reported rise in the cases of GNSS and AIS spoofing, denial, and manipulation. As the primary systems used in VAtoN, the inherent vulnerabilities within AIS and GNSS can be used to manipulate, disable, or otherwise impact VAtoNs.

---

1. ASCII (American Standard Code for Information Interchange) is a common character encoding format for text data. ASCII data has unique values for 128 alphanumeric or special characters.
Automatic Identification System

The AIS uses NMEA protocol in a self-reporting, self-negotiated network. In this network, ships and stations transmit and receive vessel and station information in designated time slots. This Radio Frequency (RF) traffic is unencrypted and sent via Very High Frequency (VHF) with an approximate range of 25-30 nautical miles. AIS Message 21 is used to transmit VAlOn. The format of this message is openly available, and the transmission frequency of AIS is publicly known, leaving these AIS messages susceptible to spoofing, hijacking, data manipulation, and denial of service.

Instances of AIS manipulation to show false vessel locations include:

- In 2019, what was initially a few ships became more than one thousand as AIS streams appeared off the coast of Elba in Corsica and were recognized as Dutch-flagged naval vessels.
- In 2021, naval vessels from the U.S., U.K., and Netherlands were shown at different times steaming off the coast of Crimea, causing the Russian government to protest, as they had claimed Crimea back in 2014. Despite the AIS tracks, live camera feeds from the port of Odessa, Ukraine showed all three ships were pier side at the time of the alleged event.
- In 2023, AIS was spoofed to form a “Z”, the symbol used by Russia during the ongoing conflict in Ukraine.

Global Navigation Satellite System

The primary satellite navigation constellation used in GNSS is GPS. The GNSS constellation is used to provide timing, location, speed, and other information to systems on both land and sea. As with AIS,
GNSS uses NMEA messages to ensure compatibility with navigation equipment, making GPS susceptible to nefarious effects such as spoofing, Denial-of-Service (DoS), hijacking, and manipulation.\textsuperscript{64,65,66,67} Known instances of GPS interference in the Black Sea and Strait of Hormuz include:\textsuperscript{68}

- In 2017, more than 20 vessels in the Black Sea reported their GPS positions had moved their locations more than 25 nautical miles inland and placed them at a nearby airport.\textsuperscript{69} Moreover, between 2017 and 2019, approximately 10,000 similar incidents affected nearly 1,300 vessels.\textsuperscript{70}
- In 2019, the British tanker Stena Impero’s GPS was spoofed while transiting the Strait of Hormuz, causing her AIS and ECDIS to malfunction and forcing her to change course into Iranian waters (see Figure 4). Ultimately this resulted in the ship being seized by the Iranian military.\textsuperscript{71}

![Figure 4: Track of Stena Impero showing route deviation into Iranian waters\textsuperscript{72}](image)

**Known and Potential Attacks to Virtual Aids to Navigation**

Given the vulnerabilities inherent within protocols used in VAtoN, malicious actors would likely be able to manipulate VAtoN in areas such as dense fog and shifting shoals.\textsuperscript{73,74,75,76,77} In Ponce De Leon Inlet, Florida, four VAtoNs appeared on systems to show a safe approach passage when in fact the water depth was only 1 meter. Every vessel’s draft, depth below the waterline, varies based on the vessel. However, vessels used for international shipping will draft more than 1 meter (3.2 feet). The cause of this incident remains unsolved but represents the type of activity a malicious actor could engage in to
cause a maritime accident. Since VAtON relies upon AIS messages to place virtual buoys along the water way, it is critical to understand the risks associated with AIS spoofing incidents. For example, in 2019, the Italian Coast Guard detected more than 3,700 ghost ships which were falsely created by an AIS generator in a span of 17 minutes.

Additionally, in areas such as North Carolina, where tides cause shoals to shift, or San Francisco, where fog can become too thick for visual navigation, distrust in VAtONs and the inability to reliably use VAtONs on short notice is likely to lead to closures of major maritime traffic routes, thereby congesting maritime logistics worldwide for a significant amount of time.

Conclusion

An accident or incident caused by the manipulation of VAtONs is likely to lead to a global logistical problem if the cybersecurity challenges associated with this technology are not addressed. VAtON is an asset to navigation safety; however, due to unencrypted protocols and the ease with which these RF based messages can be sent, these aids also pose an inherent risk to safe marine navigation. Instances of AIS and GNSS spoofing, as well as the placement of random ships and virtual buoys, have demonstrated vulnerabilities associated with VAtON. It is plausible for nefarious actors to compromise VAtON leaving vessels, their cargo, and their crew at risk.

Given the maritime community’s reliance on older standards, independent investment in equipment with secure protocols is unlikely. A concerted effort by governments to implement administrative changes to both local and IMO policies is likely to improve reliability and security, however. Ensuring a check-and-balance procedure is in place for the use of VAtONs, such as sending out Notice to Mariners (NtM) messages or shipping notices with coordinates and start and stop times of the placement of VAtONs, would back up the placement of the virtual buoys with authenticated message traffic. Certain maritime administrative organizations have already taken this approach, such as a 2014 Indian Register of Shipping notice to Indian-flagged vessels when the United States Coast Guard (USCG) began testing VAtONs in U.S. ports. Training for new mariners and refresher training for qualified mariners to notice and seek authentic verification of VAtON placement is crucial.

---

35 Technical Circular | Indian Register of Shipping | USCG Testing of Virtual ATON or eATON | No. 013/2014 | https://www.irclass.org/media/1597/uscg-testing-of-virtual-aton-or-eaton.pdf | Accessed August 17, 2023