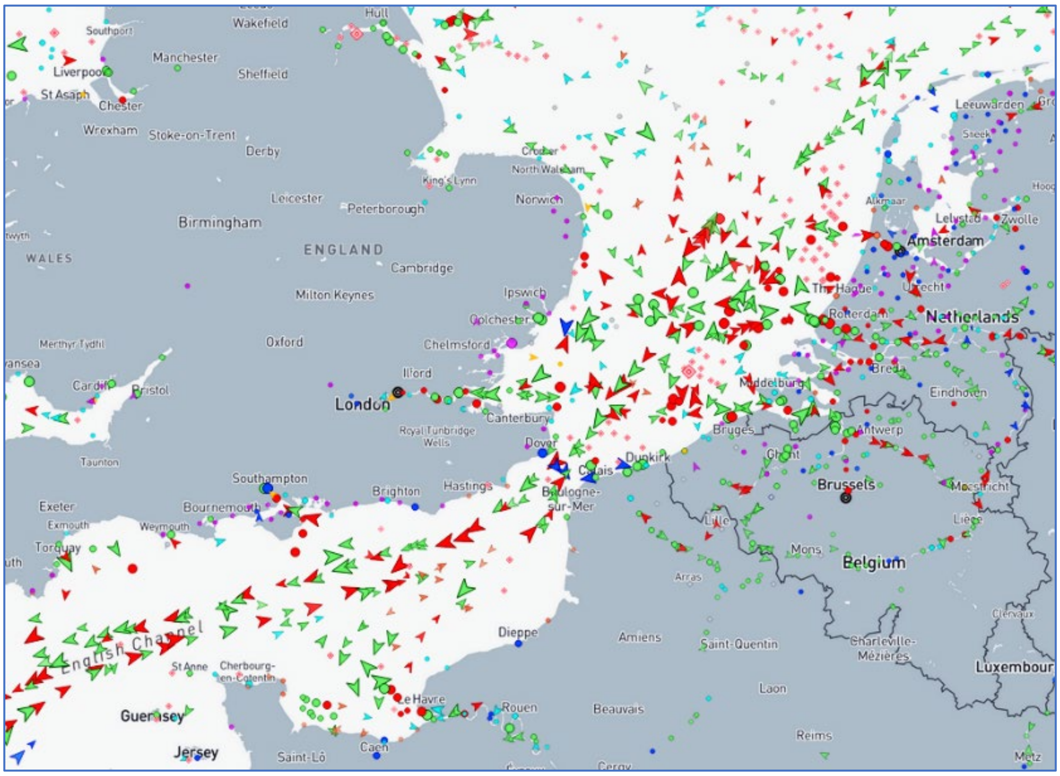
Type: Technical note
Title: Solutions to security problems in AIS and NAVTEX
Author(s): Lars Moltsen, Stefan Pielmeier
Date: 04 April, 2024

Solutions to security problems in AIS and NAVTEX

The maritime industry depends heavily on AIS

The AIS technology – a well-known ITU standard [itu.int/rec/R-REC-M.1371] – is used globally for vessel tracking in a number of commercial and maritime authority surveyance systems. The figure below shows a good example in the form of the popular MarineTraffic.com online service, which monitors vessels on a global scale, here in the busy English Channel.

Today, the maritime industry and maritime authorities are **heavily dependent** on the AIS technology.



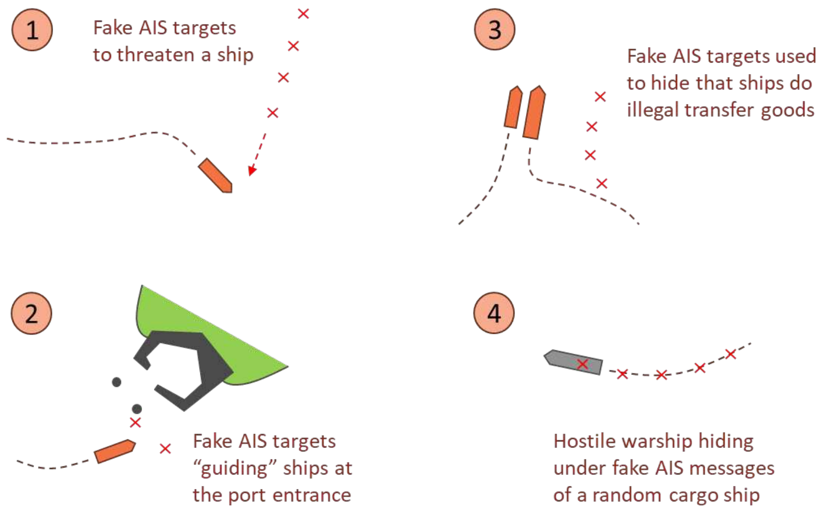
AIS has critical security flaws

The AIS technology was developed more than 20 years ago, and it has a number of security flaws. In particular, the sender of AIS messages is anonymous since there is no cyber secure mechanism in AIS for verifying identities. This means that anyone with basic software and radio skills can manufacture a simple AIS transmitter, take it to the beach, and start transmitting AIS data with non-verifiable identities, modified positions, and even AIS base station commands to be picked up by nearby ships, AIS coast stations, and AIS-receiving satellites.

These security flaws are already being exploited, from the simple action of powering off the AIS unit (dark ships), fake AIS data to hide organized crime (illegal transfer of goods at sea), to enemy state actors who want to cause confusion, accidents, and chaos. This is very problematic for vessels who rely on e.g. virtual Aids-to-Navigation (AtoNs) for navigation. It is also problematic for nations, authorities, ports, and commercial logistics operators, who depend on the data in daily operations.

Four examples of observed/possible misuse of AIS are illustrated below:

1. Fake AIS targets for a “virtual” ship (which may be a real ship not involved in the scam), transmitted to confuse another ship to make a turn (to ground it or just to confuse).
2. Fake AIS targets transmitted for port entry AtoNs (buoys) to confuse a ship to ground.
3. Fake AIS targets of a vessel for transmitted to hide that illegal transfer of goods is taking place. Typically, the vessel turns of its onboard AIS transmitter, while someone else starts transmitting the fake AIS data.
4. An enemy warship hiding its true identity by transmitting fake AIS targets of a cargo vessel. Since there is a match of radar and AIS targets, surveyance systems may not detect the warship.



The amount of AIS spoofing is currently on the rise. Over the past two years, different types of spoofing has increased by 82% [cnbc.com/2023/09/26/russian-dark-ships-vessels-fake-their-locations-to-move-oil-around-the-world.html]. We should expect this problem to grow in the coming years – potentially to a level which makes the AIS technology **useless**.

NAVTEX is also vulnerable

The NAVTEX system used for the transmission of Maritime Safety Information to ships suffers from the same vulnerabilities as AIS, since there is also no sender identity verification. Basic software/radio skills are enough to set up a NAVTEX transmitter to confuse or mislead marine traffic with false navigational warnings that ships have to take into account according to SOLAS.

Solution?: VDES, MCP/MMS, and S-100

The security flaws in AIS and NAVTEX must be solved! The obvious solution to the problem is to add digital signatures to AIS messages, such that the true sender can be verified, since we can assume that fake data will never be sent from a verified source.

Unfortunately, there is no available space in AIS messages for digital signatures, but the new **VDES** standard [itu.int/rec/R-REC-M.2092] (sometimes referred to as **AIS 2.0**), which is an extension of AIS, and which is supported by new AIS transceivers (ship and coast stations), adds new data channels that can be used also to authenticate AIS messages by using digital signatures.

The VDES technology does not itself include any concept for the protection of the transported service data using digital signatures. In fact, IALA has a new guideline, G1181 [www.iala-aism.org/product/g1181-vdes-vdl-integrity-monitoring], to partly mitigate integrity problems in VDES (including AIS and ASM).

However, the supplementary Maritime Connectivity Platform (**MCP**) standard and its Maritime Messaging Service (**MMS**) element contains the necessary features to provide such sender authentication and the necessary Private Key Infrastructure (PKI) for all marine services [maritimeconnectivity.net/mcp-documents]. The use of VDES and MCP/MMS in combination is recommended by IALA in the most recent version of its guidelines, G1117 [www.iala-aism.org/product/g1117]. Details about the system architecture can be found in Annex C of that document.

The old AIS standard includes so-called ASM (Application-Specific Messages), which defines a number of data formats (without digital signatures) for various use cases, e.g. virtual AtoNs. In the VDES/MCP-based framework, the data from maritime authority use cases should be encoded in **S-100 data formats** [iho.int/en/s100-project] as future ship equipment according to IMO has to be compatible with S-100 data formats from 2029. S-100 allows for digital signing of the data by the service provider, and thus, a proper end-to-end verifiability of identities and data integrity by the ship application. S-100 data formats cover a wide range of use cases, including AtoNs, Maritime Safety Information, weather and ice information, digital routes, etc.

The PKI in MCP/MMS is the key!

The necessary Private Key Infrastructure (PKI) to enable trust between service users and service providers, which comes with MCP, has to be established in a cyber secure way by either private, governmental or intergovernmental organizations. The MCC and IALA work on guidelines for authorities, service providers and service users. Trust is mainly enabled by proper establishment and regular check of identities, followed by the issuing of digital certificates, and the ability to revoke certificates in case of identity theft.

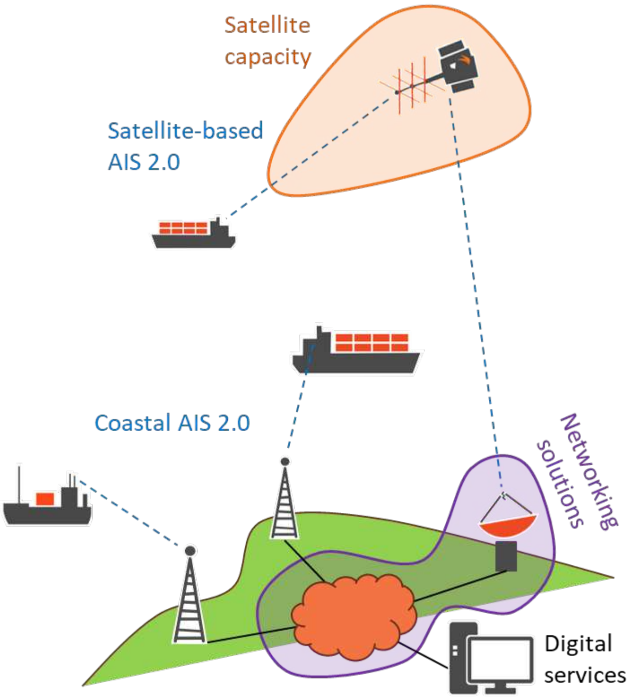
The establishment of a PKI and the use of certificates is the only way to secure all maritime services against simple fake identities or changed data content for all services, and it must be independent of the transport technology in use, be that Internet, VDES, or NAVTEX/NAVDAT.

Sternula provides satellite-based AIS 2.0 and MMS networking.

Sternula is a new satellite operator and the world’s first to offer **AIS 2.0 (VDES) satellite connectivity** on commercial terms as a supplement to coastal AIS 2.0 connectivity (see illustration below).

Sternula also offers **MMS-based networking** for coastal AIS 2.0 networks, including the support for extended coverage via satellite (see illustration below).

Finally, Sternula offers to **deploy and operate AIS 2.0 satellite constellations**, typically national projects. An example is the Nigerian AIS 2.0 project recently announced by NIMASA and Sternula [nimasa.gov.ng/nimasa-sternula-sign-mou-on-vhf-data-exchange-system].


Satellite capacity
Satellite-based AIS 2.0
Coastal AIS 2.0
Networking solutions
Digital services