AIS Spoofing

R. Ben Voth, Joey Simone

California State University Maritime Academy

Capstone: Maritime Profession People and Planet

Dr. Bets McNie

8 APR 2024

Approaches to Prevention and Detection of Malicious AIS Data

The modernization of the Maritime Industry has included many lifesaving improvements to our navigation and communication equipment and protocols. The *Automatic Identification System (AIS)* has decades of service facilitating vessel communication and preventing collisions; the use of AIS Aids to Navigation (AIS AToNS) is very useful for establishing marks where it is impossible to rig a traditional buoy, or to temporarily mark a dangerous position while traditional marks are installed. The AIS, when given true information and interpreted by competent officers, has saved lives, and will save countless more. However, the advent of cyberwarfare jeopardizes the safety of mariners like us, and AIS has minimal security features for preventing attacks. A solution must be adopted which verifies a message’s sender’s identity, that the message has not been tampered with, and that the content of the message is genuine.

# What is AIS Spoofing?

## Key definitions

## Regulations pertaining to AIS

## Signs of spoofed data

# Who are the Major Actors?

## China

## Russia

## Criminals

# What are the Major Issues?

## Cyber Terrorism

Mariners, particularly the watchstanding bridge officers, rely on AIS data to make safe navigation decisions; false AIS data necessarily decreases the safety of those navigation decisions. AIS messages are entirely insecure, so malicious actors can perpetrate attacks with effects ranging from confusion and delay to grounding and collisions. Wimpenny Et Al. provide a brief list of possible attacks from spoofed AIS messages:

“• Driving a vessel off course or re-routing it by spoofing the presence of virtual aids to navigation (VAtoN) via a spoofed ‘AIS Message 21’. VAtoN have no physical presence, but instead provide data via an AIS message which is used to display the presence of AtoN electronically on an ECDIS. Legitimate uses for VAtoN include the marking of new hazards (such as a dangerous wreck) whilst authorities arrange for a physical AtoN, or in instances where a physical AtoN is not appropriate.

• Spoofing a vessel’s reported position by providing it with false DGNSS corrections via a spoofed ‘AIS Message 17’. Such an attack could interfere with a vessel’s ability to navigate safely and has the potential to lead a vessel into harm (depending on how this data is used on the bridge).

• Performing denial of service attacks by misusing AIS channel management broadcasts via spoofing ‘AIS Message 22’. Such broadcasts could be used to instruct all AIS transceivers within range to cease operation or switch their AIS broadcasting onto an inappropriate maritime VHF channel, thereby interfering with other maritime communications.

The above are all particularly nefarious forms of attack as, unlike spoofing the presence of a physical AtoN or vessel, these spoofing attacks cannot be verified visually or against data from another system, such as radar, and the mariner is reliant solely on AIS data.” (2022, p. 334).

Such attacks are difficult to prevent or detect because the AIS does not verify senders or content, and the bridge has no way of knowing whether the received information can be trusted or not. A ship falling for the attack and being rerouted into a dangerous location is the worst-case scenario, but even the news or threat that such attacks occur may cause bridge teams to overreact and to disregard all AIS data in the future. In either situation, the functional utility of the AIS is diminished, again preventing its use in aiding safe navigation.

## Disguising illegal activity

As discussed in the subsection on criminals in the Major Actors section, AIS spoofing can be used to conceal evidence of crime at sea. Criminals can use false AIS data to hide their ship’s location, route, and their business. One such case is the Russian “shadow tanker” fleet, a group of smugglers who transmit false location data to conceal their route, their origin, and the transfer of their cargo. In September of 2023, Alaric Nightingale reported on the tanker *Turba* lightering oil from her own hold to another tanker, *Simba*, while falsely reporting that their own position was in a place miles away from her. “The precise reasons for any individual transfer are never clear, but the moves add a degree of separation and obfuscation for those ultimately purchasing the consignments.” (Nightingale, 2023). This is just one part of the shell game by which a sanctioned and cash strapped country like Russia can achieve their strategic goals. Oil can be loaded secretly onto a vessel transmitting a false name, travel to a country different from what the AIS says is the case, rendezvous with a clean vessel, and sell the oil. The more ubiquitous case is *IUUF: Illegal/Unreported/Unregulated Fishing*. Max Krüger’s 2019 presentation discussed how illegal fishers could use fraudulent data to claim that they are not fishing vessels, that they aren’t engaged in fishing, or to not appear to be fishing in an unauthorized zone. “Accordingly, for a fishing vessel, performing illegal activities creates some incentive to cover its own identity and/or activity by AIS type spoofing.” (Krüger, 2019). This, of course, is a financial motivation. To sell illegal species to rich epicures, to fish a greater quantity than authorized, or in the waters of a country where certain fish are more populous could be lucrative enough to risk punishment for being caught.

## Impersonation

Impersonation describes falsifying the AIS data of a vessel so that a vessel may pretend to be another, or that land stations can lie about the whereabouts of a vessel. One particularly worrying case is the incident with the HMS Defender in the early weeks of the Russia-Ukraine war in 2021.

“In the early hours of June 19, the site's tracking data showed the HMS Defender and a Dutch frigate, HNLMS Evertsen, approaching the port of Sevastopol in Crimea. The strange thing is, they weren't there.” (Bateman, 2021).

This constitutes a cyber attack perpetrated presumably by the Russian Military to create misleading AIS data to be uploaded to the website *Marine Traffic*, a platform which makes available up to date ship position info of ships globally. This was part of a misinformation campaign where “Russia's Defence Ministry claimed it fired warning shots and dropped bombs to deter the Royal Navy vessel.” (Bateman, 2021). The simulated data was used to skew public perception of the nature of the conflict in the water, and the political ramifications if the spoofing was not detected could have included a shooting war between the Russian Federation and the United Kingdom. Although this is the most extreme and high-profile example to date, this should illustrate the need to verify that the position information in AIS reports is true, and that the sender is the vessel.

## Obfuscation

# What solutions have been proposed?

## Sensor based detection technologies

## AI and Blockchain solutions

## Public Key Cryptography

# Drawbacks of this Solution

# Positive Outcomes of this Solution

# Conclusion

It is obvious that a solution is necessary to upgrade the AIS to a modern standard of cybersecurity to secure the safety of global trade and the environment from those who wish harm on them. For the people in this room, this means that you have a choice between having stricter controls on the AIS data you receive and being able to trust the validity of the ship reports and the ATS AToNs placed by local authorities, or constantly worrying that cyber-attacks are feeding you false data. The solution outlined herein can only be successfully implemented with development from the private sector, regulation from the public sector, and the welcome of the maritime industry. Invest in the technology, lobby for legislation, and be willing to learn the new system when it is developed. The consequences for failing are grim.

References

Androjna, A., Pavić, I., Gucma, L., Vidmar, P., & Perkovič, M. (2024). AIS data manipulation in the illicit global oil trade. *Journal of Marine Science and Engineering*, *12*(1), 6-. https://doi.org/10.3390/jmse12010006

Androjna, A., & Perkovič, M. (2021). Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. *Transactions on Maritime Science*, *10*(2), Article 2. https://doi.org/10.7225/toms.v10.n02.w08

Androjna, A., Perkovič, M., Pavic, I., & Mišković, J. (2021). AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences*, *11*(11), Article 11. https://doi.org/10.3390/app11115015

Bateman, T. (2021, June 28). *HMS Defender: AIS spoofing is opening up a new front in the war on reality*. Euronews. https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality

Bloomberg. (2023, September 27). *Fake coordinates and tanker tricks expose shadowy russian oil trade*. gCaptain. https://gcaptain.com/fake-coordinates-and-tanker-tricks-expose-shadowy-russian-oil-trade/

Boudehenn, C., Cexus, J.-C., Abdelkader, R., Lannuzel, M., Jacq, O., Brosset, D., & Boudraa, A. (2023). Holistic Approach of Integrated Navigation Equipment for Cybersecurity at Sea. In C. Onwubiko, P. Rosati, A. Rege, A. Erola, X. Bellekens, H. Hindy, & M. G. Jaatun (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media* (pp. 75–86). Springer Nature. https://doi.org/10.1007/978-981-19-6414-5\_5

Courtnell, J. (2023, February 10). *What is spoofing? Your complete guide (+ 4 key AIS spoofing typologies)*. Pole Star. https://www.polestarglobal.com/resources/what-is-spoofing-your-complete-guide-4-key-ais-spoofing-typologies

d’Afflisio, E., Braca, P., & Willett, P. (2021). Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection. *IEEE Transactions on Aerospace and Electronic Systems*, *57*(4), 2093–2108. https://doi.org/10.1109/TAES.2021.3083466

Diakun, B., & Meade, R. (2024, March 8). *Black Sea shipping hit by rising Russian GPS jamming*. https://www.lloydslist.com/LL1148493/Black-Sea-shipping-hit-by-rising-Russian-GPS-jamming

Duan, Y., Huang, J., Lei, J., Kong, L., Lv, Y., Lin, Z., Chen, G., & Khan, M. K. (2023). AISChain: Blockchain-based AIS data platform with dynamic bloom filter tree. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2332–2343. https://doi.org/10.1109/TITS.2022.3188691

Goudosis, A., & Katsikas, S. (2020). Secure AIS with identity-based authentication and encryption. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *14*(2), 287–298. https://doi.org/10.12716/1001.14.02.03

Goudossis, A., & Katsikas, S. K. (2019). Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology*, *24*(2), 410–423. https://doi.org/10.1007/s00773-018-0561-3

Guo, S. (2014). *Space-based detection of spoofing AIS signals using doppler frequency*. *9121*, 912108-912108–6. https://doi.org/10.1117/12.2050448

Harris, M. (2024, March 7). *How illegal fishing ships hide*. https://nautil.us/how-illegal-fishing-ships-hide-526064/

Iphar, C., Napoli, A., & Ray, C. (2015). *Detection of false AIS messages for the improvement of maritime situational awareness*. 1–7. https://doi.org/10.23919/OCEANS.2015.7401841

Iphar, C., Ray, C., & Napoli, A. (2020). Data integrity assessment for maritime anomaly detection. *Expert Systems with Applications*, *147*, 113219-. https://doi.org/10.1016/j.eswa.2020.113219

Jones, A., Koehler, S., Jerge, M., Graves, M., King, B., Dalrymple, R., Freese, C., & Von Albade, J. (2023). BATMAN: A brain-like approach for tracking maritime activity and nuance. *Sensors (Basel, Switzerland)*, *23*(5), 2424-. https://doi.org/10.3390/s23052424

Katsilieris, F., Braca, P., & Coraluppi, S. (2013). *Detection of malicious AIS position spoofing by exploiting radar information*. 1196–1203. https://ieeexplore.ieee.org/document/6641132

Kelly, P. (2022). A novel technique to identify AIS transmissions from vessels which attempt to obscure their position by switching their AIS transponder from normal transmit power mode to low transmit power mode. *Expert Systems with Applications*, *202*, 117205-. https://doi.org/10.1016/j.eswa.2022.117205

Kessler, G. C. (2020). Protected AIS: A demonstration of capability scheme to provide authentication and message integrity. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *14*(2), 279–286. https://doi.org/10.12716/1001.14.02.02

Krüger, M. (2019). Detection of AIS spoofing in fishery scenarios. *2019 22th International Conference on Information Fusion (FUSION)*, 1–7. https://doi.org/10.23919/FUSION43075.2019.9011328

Louart, M., Szkolnik, J.-J., Boudraa, A.-O., Le Lann, J.-C., & Le Roy, F. (2023). Detection of AIS messages falsifications and spoofing by checking messages compliance with TDMA protocol. *Digital Signal Processing*, *136*, 103983-. https://doi.org/10.1016/j.dsp.2023.103983

Ray, C., Gallen, R., Iphar, C., Napoli, A., & Bouju, A. (n.d.). *DeAIS project: Detection of AIS spoofing and resulting risks | ieee conference publication | ieee xplore*. Retrieved March 21, 2024, from https://ieeexplore.ieee.org/abstract/document/7271729

Sasson, H. (2021, September 13). *What is vessel identity laundering and why does it matter?* Windward. https://windward.ai/blog/north-korean-sanctions-evasion-identity-laundering-explained/

Schuler, M. (2024, March 5). *Planet Labs secures major U.S. Navy contract for advanced maritime monitoring*. gCaptain. https://gcaptain.com/planet-labs-secures-major-niwc-pacific-contract/

Wimpenny, G., Šafář, J., Grant, A., & Bransby, M. (2022). Securing the automatic identification system (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. *The Journal of Navigation*, *75*(2), 333–345. https://doi.org/10.1017/S0373463321000837