News Articles

<https://www.polestarglobal.com/resources/what-is-spoofing-your-complete-guide-4-key-ais-spoofing-typologies>

<https://gcaptain.com/planet-labs-secures-major-niwc-pacific-contract/>

<https://gcaptain.com/fake-coordinates-and-tanker-tricks-expose-shadowy-russian-oil-trade/>

<https://www.lloydslist.com/LL1148493/Black-Sea-shipping-hit-by-rising-Russian-GPS-jamming>

<https://windward.ai/blog/north-korean-sanctions-evasion-identity-laundering-explained/>

<https://www.mdpi.com/2076-3417/11/11/5015>

<https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality>

<https://nautil.us/how-illegal-fishing-ships-hide-526064/>

I’ve popped all of these into Zotero.

Explain the problem. Define the different ways AIS spoofing can be exploited; the ones that come to mind before conducting any reading are concealment, impersonation, and obfuscation. Concealment: Alice is doing some illegal economic exploitation, and doesn’t want Bob, in the Coast Guard for that region, to know where she is, who she is, or what she is doing, so she may disable the AIS, reduce the power to limit range, or transmit false information with regards to her business and whereabouts. Impersonation: Alice is a warship transiting in international waters where it is legal for her to do so, but Charlie sends false messages claiming to be Alice and their position information in the false messages shows Alice within the territorial waters monitored by Bob, which could constitute Casus Belli. Obfuscation: Alice, Bob, etc through Henry are merchant ships transiting a congested waterway, but Gary is a terrorist, who intercepts messages and modifies them slightly before passing them on to others, causing Alice to think that Dave is on a collision course when he’s not, or that Edward is not on a collision course when he really is, and the resulting confusion results in inefficiency at best or fatalities at worst.

The solution to be fashioned is that some protocol must be installed on AIS transponders that conform to the following rules. Information must be transmitted all the time, so vessels cannot hide. The information transmitted must be true, so vessels cannot lie. When a vessel receives this information, there must be a protocol by which the recipient can be satisfied as to the true sender of the message, and that the contents of the message have not been corrupted or tampered with. Propose to use something like PGP cryptography and signatures, which have been doing the job in email for decades.

Composed a first pass into the sources we’ve already pulled, just a skimming of the abstracts. The solutions available in the papers I’ve read so far include using external sensors such as Satellite and Radar to verify AIS data of vessels, using AI and Blockchain (see BATMAN and AISChain), a way of detecting low power transmission from a base station (somehow), and the method I first thought would be the most effective with public key encryption (Wimpenny).

I’ve made chatgpt cough up a draft based on the outline.

**Abstract:**

As maritime activities continue to expand globally, the threat of AIS (Automatic Identification System) spoofing emerges as a significant concern, jeopardizing vessel safety, national security, and marine environmental integrity. This paper provides an in-depth analysis of AIS spoofing, encompassing its various forms, actors involved, implications, and proposed solutions. By examining existing literature, expert opinions, and potential drawbacks, the paper advocates for a comprehensive approach combining technological advancements and regulatory measures to effectively combat AIS spoofing and ensure the integrity of maritime operations.

**1. Introduction**

The widespread adoption of AIS technology has revolutionized maritime navigation and communication. However, with its benefits come inherent vulnerabilities, particularly concerning AIS spoofing. This paper aims to explore the multifaceted nature of AIS spoofing, its implications for maritime security, and the imperative need for robust countermeasures.

**2. Understanding AIS Spoofing**

AIS spoofing refers to the deliberate manipulation of vessel identification, positional, navigational, and speed data to deceive maritime authorities, neighboring vessels, or satellite monitoring systems. This deceptive practice can take various forms, including altering vessel identities, falsifying positions, and fabricating navigational data. Despite mandates requiring AIS usage for vessels exceeding 300 gross tonnage and all passenger ships, the prevalence of AIS spoofing remains a significant challenge in maritime security.

**3. Major Actors in AIS Spoofing**

The motivations behind AIS spoofing are diverse and often driven by illicit activities. Major actors include illegal, unreported, and unregulated fishing (IUUF) operations seeking to evade detection, geopolitical actors aiming to provoke diplomatic tensions or conceal military activities, and entities attempting to circumvent sanctions or engage in illicit trade. These actors employ sophisticated tactics to exploit vulnerabilities in the AIS system, posing significant risks to maritime safety and security.

**4. Implications of AIS Spoofing**

AIS spoofing poses a range of implications for maritime operations, including concealment of vessel movements, provocation of diplomatic incidents through impersonation, disruption of navigation systems through obfuscation, and facilitation of illegal activities such as smuggling and sanctions evasion. These consequences not only undermine maritime security but also compromise environmental integrity and economic stability in maritime regions.

**5. Proposed Solutions**

Addressing AIS spoofing requires a multifaceted approach encompassing technological innovations, regulatory measures, and international cooperation. Proposed solutions include leveraging RADAR and satellite technologies for enhanced monitoring, implementing AI-based detection systems to identify suspicious activities, and adopting public key cryptography (PKC) solutions to ensure the authenticity and integrity of AIS data transmissions.

**6. Evaluating Solution Impacts**

While proposed solutions offer promising avenues for combating AIS spoofing, they also present challenges and potential drawbacks. Negative implications include technological and financial burdens, environmental concerns related to increased energy consumption, ethical dilemmas surrounding surveillance practices, and professional challenges concerning trust and reliability of cryptographic systems. However, the positive impacts of these solutions, such as improved industry transparency, enhanced environmental protection, and mitigation of cyber-terrorism threats, outweigh these drawbacks.

**7. Conclusion**

In conclusion, AIS spoofing represents a formidable challenge to maritime security and integrity. Addressing this threat requires collaborative efforts from stakeholders across the maritime industry, regulatory bodies, and international organizations. By implementing comprehensive solutions that combine technological innovations with regulatory frameworks, the maritime community can effectively combat AIS spoofing and safeguard the integrity of maritime operations for generations to come.

This is some hot garbage. We gotta do at least better than this.