GPS spoofing: what’s the risk for ship navigation?

By Chris Lo
Share

GPS spoofing – or GNSS spoofing more accurately – is a much-discussed cyber-threat to ship navigation systems. With the potential for paralysed shipping lanes, collisions and even untraceable piracy incidents, what is the current state of play between the shipping industry’s cyber-defences and the malicious actors who aim to cause chaos through GPS spoofing?

The shipping industry has been aware of the threat of GPS spoofing for years, but one incident in 2017 pushed the issue higher up the global news agenda. In June of that year, at least 20 vessels in the Black Sea, in the vicinity of Novorossiysk Commercial Sea Port, reported that their automatic identification system (AIS) traces erroneously showed their position as Gelendzhik Airport, around 32km inland.

The large number of vessels involved and the fact that all of the ships’ tracking systems placed them in the same nonsensical location, led to informed speculation – still unconfirmed officially – that the incident could be attributed to Russian testing of satellite navigation spoofing technology as part of its electronic warfare arsenal.

“My gut feeling is that this is a test of a system which will be used in anger at some other time,” the UK Royal Institute of Navigation’s former president David Last told New Scientist in 2017.

Since then, there have been persistent concerns that the shipping industry may be vulnerable to GPS spoofing, raising the risk of keeping ships at sea longer than necessary to clear the confusion, as occurred in the Black Sea, or even dangerous scenarios such as ship collisions, either with other ships or with land.

Earlier this year, UK-based cyber vulnerability testing firm Pen Test Partners released information from a demonstration at the Infosecurity Europe conference, where the company’s researchers showed how electronic chart systems could be hacked to spoof the size and location of vessels. This, they argued, could cause chaos in a busy shipping lane such as the English Channel.

So what exactly is GPS spoofing, what threat does it pose to shipping, and what action should the industry be taking to reduce the risk?

GPS spoofing: from military to civilian

https://www.ship-technology.com/features/ship-navigation-risks/
GPS spoofing could be described more specifically as Global Navigation Satellite System (GNSS) spoofing, as this is the generic term for satellite navigation systems with global coverage, including GPS (US), GLONASS (Russia), BeiDou (China) and Galileo (Europe), all of which are used in the shipping industry. To clarify, this article will use the two terms interchangeably.

The fundamentals of GNSS spoofing involve an actor replicating satellite navigation signals with an identical signal that is strong enough to force out the original transmission, as GNSS receivers lock on to the strongest available signal. Once the spoof signal is in place, rogue transmissions can mislead onboard navigation systems about fundamental calculations such as location, velocity and heading.

Up until the last few years, there was a wide gulf in the knowledge and equipment required for a user to carry out a full GNSS spoofing attack, rather than a jamming hack, which simply blocks the satellite signal and is much easier to detect. More recently, however, the commercial availability of radio hardware and downloadable software has brought GNSS spoofing from the military into the civilian realm, according to Roi Mit, chief marketing officer at Israel-based cybersecurity firm Regulus Cyber. Software-defined radios (SDRs) are cheaply available online, and, with the right software can be used to mimic satellite signals and transmit fake ones.

“We’ve done some testing at our lab at Regulus, where we purchased an SDR from Amazon, and without any technical knowledge we could easily, in a matter of a few days, completely replicate the entire GNSS satellite system transmission,” says Mit. “I even had a talk with one of the largest vendors for SDRs online; he said there was a big surge in the amount of systems he was selling because of games like Pokemon Go, which are based on GPS position. These kids don’t want to leave their home and walk around outside with their phone – they just buy this device, transmit their location and they trick their own phones’ GPS. But that exact same device can actually trick an entire ship.”

The spoofing threat

Given that GPS spoofing exists in the shadowy world of cybercrime and electronic warfare, with few publicly acknowledged cases to analyse, it’s difficult to get a handle on the exact risks that spoofing realistically poses to commercial ships.

As well as the aforementioned issues around ships unnecessarily idling at sea – which can cost shipowners millions in extra fuel and operational expenses – ship-to-ship and ship-to-land collisions are a possibility. A 2017 study, published by University of Texas at Austin researchers Jahshan Bhatti and Todd E. Humphreys, cites a field test showing how a 65m yacht was successfully hacked and supplied with fake positioning data, creating an obvious collision risk.

Mit raises another disturbing possibility: that the ease with which malicious actors can access GNSS spoofing tech could turn protecting commercial vessels against pirate raids from tricky to near-impossible.
“There is evidence that Somali pirates, for example, can acquire such technology,” he says. “It can be transmitted over a very long range, and the thing is, once the ship goes off-course close the coast of Somalia, it’s not only at risk of being raided, but also when they call for help from the international force there meant to protect them, the location they will transmit won’t be real. So the intervention force will actually reach a location when there’s nobody there.”

### Spoofing countermeasures

In terms of countermeasures, back-up navigation methods obviously exist from the centuries before the 1980s, when ships didn’t rely on satellite navigation – but the main issue is being able to detect when a hack is occurring, and when GNSS signals can and can’t be trusted.

Spoofing detection technologies originating from the defence industry are now coming on to the civilian market, while more advanced add-on systems offer a mitigation capability to ensure that connection to the satellite signal can always be maintained. But Mit argues that more pressure must be applied on GNSS hardware manufacturers to offer systems that are tested against jamming and spoofing.

“If the industry, the customers themselves, set a standard for the GNSS receiver manufacturers and tell them, ‘we will only acquire your antenna and your receiver if it is un-jammable and un-spoofable,’ they will motivate the manufacturers to start investing in protecting their own devices,” Mit says. “I don’t think maritime customers should compromise on buying a GNSS receiver that is not protected, and then having to deal with the right add-ons, like the Regulus technology, to equip on it.”

As fleet management software incorporating big data innovations mature, centralised state monitoring agencies could play a central role in flagging suspicious activity in shipping lanes, as University of Plymouth navigation expert Dr Tom Crichton (erroneously credited as Tim Crichton in this BBC news article) pointed out in response to Pen Test Partners’ spoofing demonstration. But the preferred solution will always be that the bridge officers onboard a ship are able to detect and thwart an attack themselves.

The International Maritime Organization (IMO) has given shipowners until January 2021 to incorporate cyber risk management into ship safety protocols, and as navigational security is likely to play a central role in these measures, so in the coming years protection against spoofing is likely to become a matter of regulatory compliance, rather than simply operational risk management.

### Working together to tackle the GPS spoofing threat

The human element is obviously a vital component of any cybersecurity strategy, and onboard a ship this factor is particularly pronounced. While technology can do much of the heavy lifting, without cyber-savvy humans at the helm, basic vulnerabilities will remain. Pen Test Partners noted in its investigation that the passwords of some vessel satellite communication terminals were still using default username and password credentials.

https://www.ship-technology.com/features/ship-navigation-risks/
Training courses on maritime cybersecurity are increasingly prevalent in the industry, and can simulate cases of spoofing to run through the recommended actions to take. Best-practice guides are also becoming more common; the UK National Cyber Security Centre published a code of practice for ship cybersecurity in 2017.

One potential barrier to the shipping industry dealing effectively with the spoofing threat is the general veil of secrecy that hangs over the risk.

“It usually doesn’t get published if a shipping company has been spoofed,” say Mit. “It’s bad branding for the company and it’s something they want to keep under cover. They can tell us this in closed calls, but usually it’s not something you go public with. In the maritime industry the competitiveness creates a situation in which they don’t share. By not sharing, they’re actually slowing down the entire industry in being prepared for such risks. If there was some kind of panel or committee, with closed doors, where all those companies could really discuss the types of threats they’re dealing with without risking their brand image, that would be ideal.”

The approaching prospect of autonomous and semi-autonomous ship technology raises the stakes in terms of cyber security, especially with regards to onboard navigation systems. One way or another, the spoofing threat will have to be dealt with definitively before the industry entrusts ship navigation to automated systems or remote operators.

“We should really keep a close eye on the maritime industry in 2019,” concludes Mit. “It’s a monumental year, because right now it seems like all the major players are pursuing semi-autonomous and autonomous ships. Since GNSS is a core technology in every single autonomous ship that I’ve read about or have been told about, we should all wait and think about if this is something we’re really ready to release into the ocean. You cannot save an autonomous ship if it’s completely controlled by a malicious actor. It should be a very slow process and it should only be done when we’re almost 100% sure it’s cyber-secure.”