ROYAL HOLLOWAY UNIVERSITY OF LONDON

Overcoming GNSS Dependency in Autonomous Ships

James Nicholls - Supervised by: Raja Naeem Akram
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Objectives

Survey the maritime environment to gain a greater understanding of its cyber-security landscape so that I can provide recommendations to existing problems and vulnerabilities.

This includes:
- Quantifying the importance of the maritime sector on a global scale
- Identify the most dangerous vulnerabilities and assess their exploitability
- Discuss potential solutions and assess their practicality
- Create custom systems to test the viability of theses solutions, and to analyse data to understand the effectiveness of these solutions.

Introduction

The maritime shipping industry is the giant behind the mass transportation of goods around the globe. A 2011 report by the European Network and Information Security Agency (ENISA) [1] outlined the following statistics:

- Around 90% of external EU trade and 43% of internal trade takes place through maritime routes
- Maritime industry makes up 3-5% of EU GDP, and 40% of EU GDP is contributed by maritime regions
- Three major EU seaports alone accounted for 8% of overall world goods traffic volume.
- A 7% increase in goods traffic through maritime routes over a decade.

These facts illustrate the importance of the sector on Europe, and hint at its importance globally. A cyber-attack on one of these ports alone could have a catastrophic rippling effect on the health of the public and the economy. Therefore, it is paramount that the cyber security of the maritime environment be bolstered against potential attacks.

Even though efforts are being made now to develop solutions, many exploitable vulnerabilities still exist, and new developments in the industry open up greater opportunities for attacks. Therefore, a proactive approach needs to be adopted to prevent this.

GNSS Vulnerabilties

One key vulnerability in the maritime sector is the dependency on Global Navigation Satellite System (GNSS) to determine location on ships.

Using GNSS location systems opens up a vessel to two main types of attacks – GNSS Spoofing and GNSS Jamming.

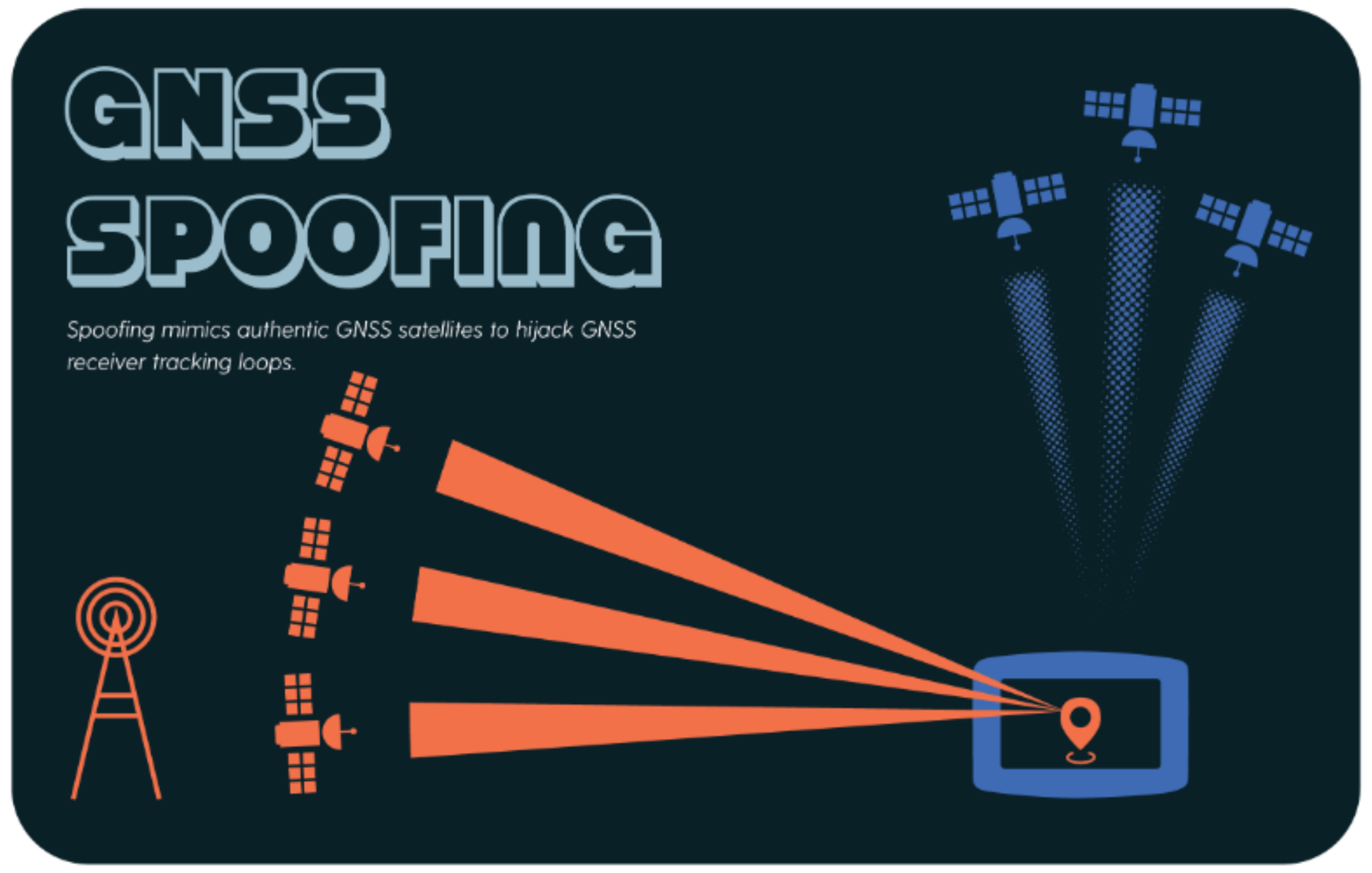
GNSS Spoofing occurs when the ships systems are fooled into reporting an incorrect position as a result of receiving faked GNSS signals from an attacker.

GNSS Jamming is where an attacker creates interference on the GNSS signal frequencies, preventing any signals being received by the ship so location cannot be determined

1.

GNSS
Jamming
Jamming creates noise which prevents GNSS receivers from locking on to authentic GNSS satellites.

2.


GNSS
Spoofing
Spoofing mimics authentic GNSS satellites to hijack GNSS receiver tracking loops.

Figures 1 & 2 show visual representations of jamming and spoofing attacks respectively. [2]

Autonomous Ships

Autonomous ships bring a unique challenge to the maritime environment, as any challenges which would usually be overcome by the onboard crew have to be solved by the ships systems since future autonomous ships are designed to be used with no crew at all.

Assuming a GNSS attack has taken place and the location of the ship cannot be found, the crew would be able to identify the attack from discrepancies in the systems and be able to estimate the ships location using celestial navigation.

Therefore, solutions must be established to enable autonomous ships to detect the presence of a GNSS attack without crew, and be able to determine their location using methods other than GNSS signals.

Detecting GNSS Attacks

Autonomous ships do not possess the human intuition to detect an attack, so systems must be developed to raise alarms when they may be a victim of one.

My solution to this problem is to develop an android app which uses the available sensors, such as accelerometer, step counter, and gyroscope, to track movement without using GNSS technology.

The purpose of the app is to calculate the position of the phone relative to a specific starting position using the data retrieved from the onboard sensors. This position is then continuously compared to GNSS positional data. If the tracking app and the GNSS have a substantial difference, then it is possible that the GNSS position is untrustworthy.

A system like this can be implemented on ships with the addition of extra sensors, such as those to measure the effects of waves when calculating speed. When the difference between the system's calculated position and the GNSS position is too great, it could be an indication that somebody is trying to direct the ship into danger.

Location Finding without GNSS

Once the attack has been detected, the location of the ship must be found without using GNSS technology.

The core of my potential solution to this problem involves peer-to-peer mechanisms to determine a ships location. However, due to the sparsity of ships in deep sea, the solutions would only be effective close to ports or highly populated channels.

Underwater acoustic signals were also an element of my solution, but limitations on their range and ability to determine direction means they were deemed ineffective.

As I did not have access to equipment to create and test my concepts, I do not know the extent to which these problems would limit the success of a potential solution.

Conclusion

Although autonomous ships are not fully implemented, development initiatives are cropping up around the globe. The industry should look into the future beyond the creation of autonomous ships, and begin to create solutions for inevitable vulnerabilities before they are exploited with dire consequences.

References

[1] ENISA, Analysis of Cyber Security Aspects in the Maritime Sector (2011)

[2] C4ADS, Above Us Only Stars – Exposing GNSS Spoofing in Russia and Syria (2019)

Acknowledgements

Thank you to Raja Naeem Akram and the other UROP Internship students for their continued support

Contact Information

- Email: James.Nicholls.2018@rhul.ac.uk
- Phone: +44 (0)7415 308 962