ASGARD – an EU project aimed at developing an anti-spoofing weapon

Saab and GMV are collaborating in ASGARD, an EU-funded project that aims to improve maritime security when using GNSS and OSNMA. The project addresses the growing threat of GNSS spoofing and other cyberattacks on navigation systems used in the maritime industry.

The ASGARD project, run by Saab and GMV, is an ambitious European Union (EU) initiative that aims to develop advanced technologies to improve Global Navigation Satellite System (GNSS) and Open Service Navigation Message Authentication (OSNMA) security in maritime environments. The project is a direct response to the growing threat of GNSS spoofing and other cyberattacks on navigation systems used in the maritime industry. By leveraging cutting-edge technology and expertise, the ASGARD project aims to address these challenges and improve the safety and security of maritime navigation systems across Europe and beyond.

GNSS is a critical technology used in maritime navigation systems. It enables vessels to determine their position, speed, and time by receiving signals from satellites orbiting the Earth. However, GNSS signals are vulnerable to interference and spoofing, which can cause navigation systems to provide incorrect information. This can lead to accidents and other safety hazards, as well as potential threats to national security.

The ASGARD project seeks to develop advanced technologies to detect and mitigate GNSS spoofing attacks in maritime environments. One of the key technologies being developed is OSNMA, which provides a means of authenticating GNSS signals to ensure that they are genuine and have not been tampered with. By implementing OSNMA, navigation systems can provide more reliable and trusted positioning information to vessels, which improves safety and efficiency in the maritime industry.

E-warfare at sea

In the late 1990s, the maritime industry stakeholders constructed the main Navigator, ECDIS, and AIS systems to improve maritime safety and security. While the development and deployment of AIS in the last decade have significantly contributed to increased navigational safety, it has also led to several safety and security concerns. One of the major issues is spoofing, where the vessel's AIS data is manipulated.

According to a report by the Center for Advanced Defense Studies (C4ADS), Russia has been manipulating GNSS signals since at least 2016. The report, based on satellite data collected by the International Space Station (ISS), identified 9,883 suspected spoofing incidents in ten global locations connected to the Russian military (Gary C. Kessler, CISSP DEFCON, 04/2019). The targeted regions include the Black Sea, Crimea, the Russian Federation, and Syria. The study discovered that 1,311 civilian ships were provided incorrect position coordinates from a variety of civilian satellite networks, including an incident in the Black Sea in 2017.

A new and inexpensive electronic device has emerged in Asia that is capable of spoofing AIS signals in ways that experts have not seen before. This has resulted in multiple spoofing incidents being reported in over 20 coastal areas and ports, including Shanghai, Fuzhou (Huilutou), Qingdao, Quanzhou (Shiyucun), Dalian, and Tianjin, which have been ongoing for months. Unlike traditional spoofing, the GNSS signals were gathered into large circles, which were later dubbed "crop circles." The moving signals were then shifted to the same position, creating a confusing traffic situation for ship pilots. Due to the low cost of GNSS spoofing technology, these attacks are likely to spread to other countries, terrorist groups, criminals, and even individual operators, posing a serious threat to maritime safety.

Existing countermeasures

What measures can be taken to detect GPS/GNSS spoofing? One method is to detect signal distortion at the point when the fake signal overrides the legitimate one. Another approach is to determine that the fake signal is originating from a different direction than the legitimate signal. Additionally, encrypted signals can be correlated to verify their authenticity, even if the civilian unit cannot interpret the encrypted signal. Employing a GNSS receiver that monitors multiple constellations and frequencies with security capabilities is also an option. Also, it is possible to authenticate the Open Service Navigation Message through OSNMA functionality.

Ultimately, enhanced cybersecurity is crucial. GNSS spoofing has been a security concern for many years, and it is now beginning to significantly impact shipping. As more devices and autonomous systems depend on GNSS, a greater number of systems could be susceptible to spoofing attacks. With hackers continually searching for new ways to exploit AIS vulnerabilities and spoofing, there will be numerous new cybersecurity vulnerabilities in the future, and systems that are not adequately secured will be at risk of attack.

Example attacks

On the other hand, AIS, as it currently exists, has several vulnerabilities that have emerged, largely as a result of being based on an open-source system that operates on specific VHF frequencies. The four main weaknesses are the absence of message integrity, timing, authentication, and validity. If compromised, AIS communications can be intercepted to create fictitious vessels or generate false collision or SOS alerts, events that could have serious implications at sea. The vulnerabilities in GNSS systems also open the possibility of attacks that could impact navigation and AIS-dependent technologies. Below are some examples of GPS spoofing attacks that have been documented by authorities:

In June 2017, there was a widespread GPS spoofing incident in the Black Sea. The captain of the 37,500-ton tanker ATRIA, located off the Russian port of Novorossiysk, reported that his GPS indicated he was at Gelendzhik Airport, which was 20 nautical miles (37 kilometers) away. AIS data from at least 20 nearby ships showed that they were in the same location as well.

In July 2019, a UK-flagged oil tanker was seized by Iran in the Strait of Hormuz. Iran claimed that the Stena IMPERO had violated international law. Analysis of AIS data suggested that GPS spoofing was involved.

In July 2017, the GPS units and AIS transponder on the 700-foot MANUKAI vessel failed as it approached its own berth. According to the Center for Advanced Defense Studies (C4ADS), spoofing had been ongoing since 2018, with 300 such incidents recorded on July 17, 2019, alone. Data from Shanghai indicated that spoofed signals were causing ships to appear to move around the eastern bank of the Huangpu River every few minutes in ring-like patterns.

Hacking scenarios

The vulnerabilities of systems as AIS can be exploited in different ways, depending on the type of hack scenario. For instance, in the closest point of approach (CPA) spoofing, the attacker creates a false impression of a possible collision with another ship, causing a CPA alert that could lead the victim vessel off-course and into danger. Another hack scenario is AIS Search and Rescue Transmitter (AIS-SART) spoofing, where the attacker sends a fake distress beacon to lure the victim vessel into an attacker-controlled area. A third type of spoofing attack is weather forecast spoofing, where the attacker sends false dynamic weather information via AIS, making the victim ship alter its course.

Denial-of-Service (DoS) attacks are another form of AIS spoofing that aims to overflow vessels' AIS updates, flooding adjacent shore facilities and vessels with excessive data. There is also the frequency hopper attack, where the attacker sends commands to shift the victim vessel's AIS to transmit on a specific frequency, making them "invisible" to all but the attacker.

Ghost vessels and data diddling are two other attack scenarios. In the former, the attacker creates fake vessels, while in the latter, the attacker modifies ship information such as name, location, course, cargo, type of ship, and speed. These attacks can be executed via software onshore or inland, or through radio frequency (RF) offshore or at sea.

One major security concern is the availability of AIS data online through various publicly accessible platforms. The IMO committee strongly recommends that nations take legal measures to protect data from being published, as such exposure could severely compromise safety at sea.

Acquiring the equipment required to spoof GNSS signals is both cheap and uncomplicated. In the instance of GPS, civilian signals are not encrypted (L1C, L2C, L5). All that is needed is a Software-defined radio (SDR) capable of transmitting on L1 frequency (1575.42 MHz). With the aid of open-source tools, it is easy to write a program that can generate GPS NMEA sentences and transmit them through SDR for GPS spoofing purposes.

ASGARD – Protection by Detection

Saab and GMV have collaborated to develop ASGARD, a technology to counter ongoing GNSS spoofing activities. This joint effort combines capabilities into an effective solution able to detect spoofing attacks and alert the crew, allowing them to take necessary actions to validate their position. ASGARD, an acronym for Advanced Shipborne Galileo Receiver Double Frequency, is an antispoofing GNSS receiver that is based on the open service of Europe's Galileo satellite navigation system. This receiver is designed to receive signals from multiple constellations, and it complies with European and international legislation. ASGARD uses Galileo's Open Service Navigation Message Authentication (OSNMA) mechanism to authenticate the navigation message, and it has been co-funded by the European Union Agency for the Space Programme (EUSPA). The aim of this project is to increase the adoption of Galileo in maritime transport by developing shipborne EGNSS data-processing receivers that can detect and alert vessels that are under spoofing attacks.

Galileo's Open Service Navigation Message Authentication (OSNMA) is a component of the end-to-end authentication system for Galileo's civilian navigation signals. This feature allows Galileo satellites to send a key and digital signature that the ASGARD receiver can use to verify the authenticity of the signal using its own public key. If the ASGARD receiver detects a signal that can’t be authenticated, it will alert the operator of a potential spoofing attack and prompt them to take alternative measures to validate the vessel's position.

ASGARD also offers an innovative integrity solution, ensuring the reliability and safety of the system. The use of OSNMA in combination with this advanced integrity solution makes ASGARD the first certified security and safety approach, compliant with SOLAS and IEC regulations for maritime safety.

According to Ana Cezón, Head of Advance Navigation Division at GMV, ASGARD operates by using a protection by detection strategy. It is a one-of-a-kind safety system that augments the security element of current Navigation and AIS solutions. Using Galileo’s OSNMA, the system provides an essential validation and authentication of message integrity for safe maritime navigation. ASGARD's innovative integrity feature enhances the safety of maritime users and sets the stage for the future approach to maritime safety. It is simply a very robust and reliable navigation solution, concludes Ana Cezón.

ASGARD is a multi-feature technology including the following functionalities:

Multi-GNSS receiver: ASGARD uses multiple GNSS constellations, such as GALILEO and GPS, to provide redundant positioning options. This feature improves navigation performance, and if one constellation is jammed, spoofed, or not usable, the receiver can switch to another.

Spoofing alert: ASGARD integrates the OSNMA functionality, which allows the receiver to detect a spoofing attack on the GALILEO constellation. This feature provides an initial countermeasure to enhance maritime security.

Multi-frequency: ASGARD utilizes double-frequency capabilities to reduce the ionospheric effect, resulting in better performance in terms of accuracy, availability, and integrity.

Reliable: ASGARD is a combination of two established technologies produced by Saab and GMV, both companies with a strong history in the field of maritime communication and navigation.

Integrity: ASGARD includes an innovative integrity solution that leverages the multi-GNSS and multi-frequency capabilities to enhance safety and alert the crew when the receiver is not working on the desired performance operation levels. Digital signatures through OSNMA provides an additional layer of system security for improved safety.

The accelerated use of digital technologies poses a significant threat to safety and security at sea. As highlighted in this article there are an immense number of vectors for attack. To maintain the integrity of vessels, it is critical to implement strong cyber security systems such as ASGARD, which provides active defense against spoofing.

Combined capabilities

ASGARD is the result of a collaboration between GMV and Saab, two leading companies with a long-standing reputation in the field of maritime communication and navigation. By combining GMV's latest generation Galileo receiver and Saab's well-proven navigation system, ASGARD offers a robust defense against cyber-attacks that aim to interfere with the navigation systems of vessels. Spoofing is a serious threat to vessel integrity and can have severe consequences, such as collisions and groundings. ASGARD provides an effective response to these attacks by ensuring that vessels stay on course and are not lured off by attackers. With ASGARD, vessel owners and operators can have peace of mind knowing that their vessels are equipped with cutting-edge technology that provides protection against cyber-attacks and helps ensure the safety and security of the crew and cargo.

Peter Bergljung, Head of Strategy at Saab AB (publ) TransponderTech, underscores Saab's commitment to ensuring the safety of everyone, including seafarers, who must feel safe and secure at sea. He affirms that the development of ASGARD is a dedicated effort by Saab and GMV, and the system is fully compliant with IMO, IEC, and MED standards.

Real-time testing will be a critical step in the development of ASGARD, where the system will be put through a series of spoofing attacks to ensure it delivers within set specifications. This testing is important to ensure that ASGARD can provide reliable and effective protection against the latest spoofing techniques that may be used by cyber attackers.

The ASGARD project is an important step forward in the development of robust and reliable cyber security systems for the maritime industry. Once released, ASGARD is expected to have a significant impact on the maritime industry, improving safety and security for vessels and crews. It is also expected to boost the uptake of Galileo in the maritime sector, when ASGARD is certified according to maritime safety regulations (SOLAS) and maritime standards (IEC).

For more information about ASGARD and the ongoing development, interested parties can visit the project's website, https://asgard.gmv.com/about-asgard/