OSNMA Implementation on Maritime GNSS Receiver

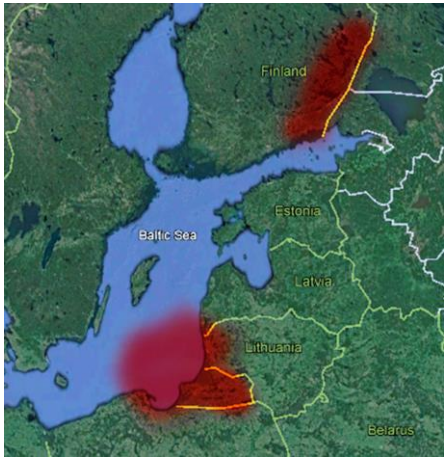
Marcos López
Héctor Llorca
Antonio R. Martín
Philipp Scheidemann

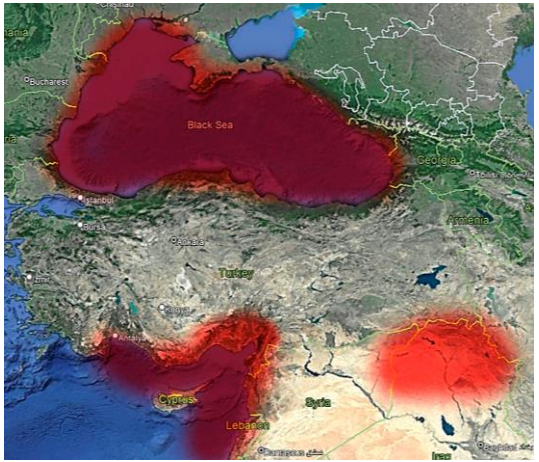
October 19th, 2022

Introduction & Motivation

GNSS systems are widely used in the maritime sector, leading to be the preferred one for navigation and positioning applications in this domain.

- **GNSS signal** is very **sensitive** to **interferences**.
- **Spoofing** is a malicious interference that aims to generate signals that mimic GNSS signals with the intention of **pretending** them **to be genuine** signals.
  - Some **real spoofing events** have been reported in recent years around the world.
  - These attacks have increased near the conflict zones.
- One of the forms of defensing against these attacks is through cybersecurity. The Open Service Navigation Message Authentication (**OSNMA**) in the **Galileo Open Service** has been developed for users around the world to validate information coming from the satellite





Images based on description provided in EASA, "Safety Information Bulletin - Global Navigation Satellite System Outage Leading to Navigation / Surveillance Degradation,". 2022

OSNMA Fundamentals

- **GNSS satellites** continuously transmit a Navigation Data to compute the PVT solution.

- **Inside** the **Galileo services**, the Galileo **Open Service** (OS) is providing a **Navigation Message Authentication** (NMA) capability.
  - **Confirms** that received **Galileo Open Navigation Data** was originated **from** the **Galileo** system **and has not been modified** by any other source.
  - **Galileo** is the **first GNSS system** to **provide this service**, which is currently in the **public test phase**, **free of charge** for users worldwide.
  - provides the possibility to authenticate satellites which do not transmit OSNMA data with the data retrieved from satellites transmitting OSNMA (**cross-authentication**)

OSNMA Solution - ASGARD context

- Within **ASGARD project**, funded by the **EUSPA:**
  - A **multi-constellation, multi-frequency maritime receiver** capable of **processing OSNMA information** is being developed at its **last stages**
  - At the date of today, the **OSNMA service** is **still in test phase with** already **Signal-In-Space** (SIS)
  - In this context, as a **future characteristic** the intention is to be able to **perform even cross-check** within **other constellations**.
  - However, **during** the **current test phase** it is **not possible** to use the **multi-constellation mode** while **using OSNMA** service.

Maritime OSNMA/Spoofing Testbed

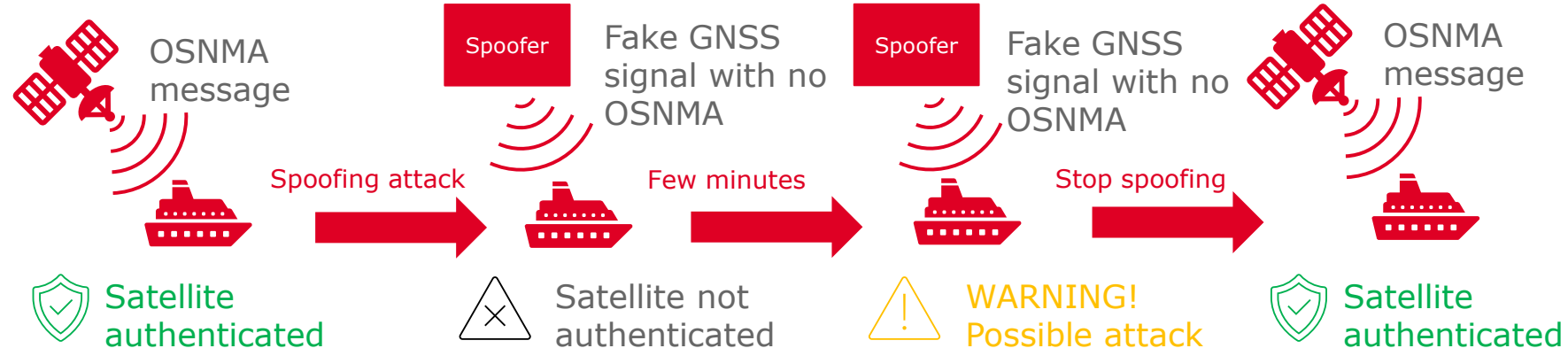
- Some European funded projects analyzed situations where **OSNMA and Spoofing** are being tested.
  - **EUSPA**: the ASGARD project is performing, for maritime domain, tests using both lab testing and on field tests.
  - **ESA:** In RIPTIDE project, field trials in maritime environment have been performed to collect data checking for existing GNSS attack situations, including OSNMA as one of the technological pillars
  - **EC**: The AIRING project addressed resilience tests for aviation operations to GNSS frequency jamming and cyber threats, considering to extend also to maritime domain.

- For stakeholders interested in testing OSNMA services, some agencies are allowing to **perform real spoofing testing campaigns outdoors**

Maritime OSNMA/Spoofing Testbed

- Receiver approach (ASGARD):
  - Test vectors
  - Spoofing attacks
    - Simple as "record and replay" (meaconing)
    - "Sophisticated" (modification of navigation data into the messages)
  - More successful attacks -> Jamming added before and into the spoofing attack

"Sophisticated" attack example:



Summary & Conclusions

- **OSNMA** is a good option to **improve safety** in maritime navigation.
  - NAV message authentication allows confidence in the genuineness of the processed signal. This allows knowing if there is a **possibility of being subjected to a spoofing attack**.
- Key aspects:
  - The IMO standard establishes a **maximum of 10 s** (Time to Alarm)
  - Internal clock (RTC) -> 15 seconds thresholds for an immediate alarm (within IMO 10 s requirement).
  - Re-start of the receiver vs maintain already tracked satellites (only received spoofing? attack)
  - Detection of no authenticate received navigation data -> delay of just? few minutes to alarm. (outside IMO 10 s requirement).
- OSNMA functionality should be understood, for now, as an **extra support** for navigation.

Thank you

Marcos López Cabeceira
malopez@gmv.com

Héctor Llorca
hector.llorca@gmv.com

ASGARD Project

https://asgard.gmv.com/

@AsgardGnss

ASGARD GNSS project