GNSS jamming and spoofing, risks and mitigation for maritime users

Aleksander Hammernes
Technical Advisor
Overview

- The economy of GNSS
- Jamming and interference
- Spoofing introduction
- Mitigation of threats in the maritime domain
The economy of GNSS
The economy of GNSS

• The global GNSS market:
  • 2017: 5.8 billion devices
  • 2020: 8 billion (estimated values)

• expected to produce over €70 billion in revenue annually in 2025
  • Expected to double with added-value services
The economy of GNSS

- The most critical mass users of GNSS technology account for less than 2.1% of the market (estimated 2015 values)
- 90% of global trade is carried by merchant vessels
- 50,000 merchant vessels generate an approximate USD 500 billions
- Values do not account for offshore related vessels and service, and revenues generated by the services made possible by this vessels.

Source: European Global Navigation Satellite Systems Agency (GSA)
GPS SATELLITE STATUS AND PLANS

- **Block IIA**
  - Last satellite decommissioned in 2016

- **Block IIR**
  - 12 operational
  - On-board clock monitoring

- **Block IIR(M)**
  - 7 operational
  - 2nd civil signal (L2C)

- **Block IIF**
  - 12 operational
  - 3rd civil signal (L5)

- **Block III**
  - In production
  - Ready for launch in 2018
  - 4th civil signal (L1C)
  - No Selective Availability

**GPS: 31 operational satellites**
GLONASS SATELLITE STATUS AND PLANS

GLONASS
- Launched: from 1982
- 81 launched
- Out of service

GLONASS-M
- Launched: from 2003
- 23 operational
- 8 stored and launch ready
- Improved clock and lifetime

GLONASS-K1
- 2 launched, 2011 & 2014 (delayed)
- Improved clock & lifetime

GLONASS-K2
Planned launched: from 2018
New radiation hardened electronics under development
L1, L2 & L3 CDMA

GLONASS-KM
Under development
Launched: unknown
4th civil signal

GLONASS:
- 24 operational satellites
- 1 in flight test phase
BEIDOU SATELLITE CONSTELLATION STATUS AND PLANS

- BeiDou Satellite Constellation
  - 6 MEO (Medium Earth Orbit)
  - 8 IGSO (Inclined Geosynchronous Orbit)
  - 6 GEO (Geostationary Orbit)

- Regional system declared operational in 2011

- 8 more MEO satellites launched and in commissioning

- Beidou services to cover most countries in the Silk Road Economic Belt initiative by 2018

- Expected system to be completed by 2020

BeiDou: 15 operational satellites
GALILEO SATELLITE CONSTELLATION STATUS AND PLANS

- Galileo Satellite Constellation
  - 2 GIOVE test satellites retired
  - 14 FOC (Full Operational Capability)

- 4 Galileo satellites successfully launched 2017-12-12 (under commissioning)

- Plan for further launch of 4 Galileo satellites Summer 2018

- January 2018: Member States approving provision of Commercial Service high accuracy for free
Jamming and interference
EXISTING CHALLENGES NOT BE UNDERESTIMATED

- From 2000 until end 2013 high focus on scintillation

- Creates large disturbance for GNSS reception
  - Equatorial belt highly exposed
  - Brazil
  - Northern areas

- Scintillation will have many of the same trade marks as a jamming and interference
  - Disturbance in Signal to Noise (SN) levels
  - Loss of satellite tracking

- Solar Cycle 24 ends 2020 with an predicted all time low cycle 25
GNSS INTERFERENCE (DOS)

- Interference is usually non-intentional

- Interference might be caused by radars or communication equipment

- A usual cause of interference is faulty GNSS antennas starting to transmit (might be a consequence of water intrusion causing the LNA to oscillate)

- It is usually a good protection to use multiple GNSS systems with a reasonable distance between antennas (>30m if possible).

- Monitoring the signal levels (SNR) gives an indication of interference problems

Are any of these antennas an occasional transmitter?
GNSS JAMMING (DoS)

• Jamming is intentional transmission in the GNSS frequency bands aiming to block the satellite signals at the user antenna

• GNSS jamming over short distances can easily be done by using low-cost jammers available on the Internet for just a few dollars and is hard to detect

• GNSS jamming over larger distances (> line-of-sight) requires more effort and is easier to detect

• Using CRPA (Controlled Radiated Pattern Antennas) will reduce the risk
GNSS JAMMING (DoS)

• Jammers are becoming smaller and cheaper

• A increase in the use of jammers in the civilian market has been observed by authorities
  – Introduction of GNSS based drivers logbooks are often seen as a root cause
Spoofing - introduction
GNSS SPOOFING

• GNSS spoofing is done by transmitting a fake GNSS signal to fool the reference system to believe it is in a different position

• Spoofing requires high skills and large resources to be a significant threat to a DP operation

• The spoofer needs to be located vicinity of the GNSS antennas to be effective

• RAIM algorithms can be used to check inconsistencies between measurements

• INS/IMU integration can be used to detect spoofers since there will be inconsistencies between real movement and GNSS measurements

• A dual antenna GNSS solution will provide additional protection against spoofing since it is very difficult to spoof such a solution with different signals

• Authentication methods can be used to verify the source of GNSS navigation message data
GNSS MEACONING

• A simpler way of spoofing

• Receive GNSS signals by an ordinary antenna, manipulate the signal in real-time (or not) and re-transmit the signal by an antenna with signal adjusted to an adequate level

• In the simplest form retransmission of GNSS signals can be considered as meaconing

• The user will measure the same position as the antenna used by the retransmitted signal

• A retransmitter can be located at a moving platform e.g. a high speed craft or a drone
GNSS MEACONING

- 2013: university of Austin Texas spoofs mega yacht
- 80 million $ yacht
- 2000 $ GNSS unit
  - RAIM capability’s
- Yacht and crew where not alerted about any error
- Home built hardware and software

$80 million yacht hijacked by students spoofing GPS signals
GNSS MEACONING

- With the introduction of Pokémon GO, GNSS Spoofing has changed

- Available spoofing (meaconing apps) for all Android phones
  - Fake GPS
  - Fly GPS
  - GPS Joystick
GNSS BEHAVIOUR DURING JAMMING AND SPOOFING

• Jamming and interference will typically look similar and the GNSS receiver may indicate low signal-to-noise levels and typically lose track of low-elevation satellites

• During low-level jamming attacks misleading position usually will show a random pattern

• Several vessels affected at the same time indicates an external event (like in the Black Sea, June 22 – 24)

• Several vessels reporting identical or close locations indicates a large-scale spoofing attack

• If the false position indicates a highly unlikely location it might be the position of a retransmitter

• Positions periodically “jumps” from true to incorrect locations are typical behavior during spoofing experiments because GNSS receivers may temporarily lose lock on the spoofing signal and reacquire the real GNSS signal
A LOW-LEVEL SPOOFING ATTACK SCENARIO
CHANGING SCENARIOS?
The challenges summarized

GNSS Jamming (interference)

GNSS Spoofing
Mitigation of threats in the maritime domain
Building the fence

RAIM

Safe Position & Timing
GNSS INTERFERENCE (DOS)
USER CASE: OFFSHORE SUPPORT VESSEL

• During commissioning phase of a offshore support vessel claims were made to the GNSS installation

• Intermittent loss of both GNSS systems

• Unpredictable pattern

• No correlation between vessel motion or heading

• Coaxial cables confirmed to be good and not damaged

• Ship yard confirmed installation of antennas according to makers instructions
GNSS INTERFERENCE (DOS) USER CASE: OFFSHORE SUPPORT VESSEL
GNSS INTERFERENCE (DOS)
USER CASE: OFFSHORE SUPPORT VESSEL
GNSS INTERFERENCE (DOS)
USER CASE: OFFSHORE SUPPORT VESSEL
GNSS INTERFERENCE (DOS)
USER CASE: OFFSHORE STANDBY VESSEL

• Reports of intermittent loss of GNSS
• No observable pattern
• No changes to existing equipment
GNSS INTERFERENCE (DOS)  
USER CASE: OFFSHORE STANDBY VESSEL

- Reports of intermittent loss of GNSS
- No observable pattern
- No changes to existing equipment
- LRIT (Long Range Identification and Tracking) enabled!
GNSS INTERFERENCE (DOS)
USER CASE: OFFSHORE STANDBY VESSEL

• Reports of intermittent loss of GNSS
• No observable pattern
• No changes to existing equipment
• LRIT (Long Range Identification and Tracking) enabled!

GNSS antenna
GNSS INTERFERENCE (DOS)
USER CASE: DRILL SHIP

- New INS system
- Worked perfect with corrections
- 10 Meter + drift without corrections
- Local interference suspected
- Denied by crew
Building the fence

RAIM

Safe Position & Timing

IMU integration

System installation
GNSS JAMMING (DoS)  
USER CASE: DRILL SHIP

- Current high reporting of Jamming events in eastern Mediterranean
- 5+ vessel reports daily interruptions to GNSS systems
- Airplanes affected
- Source and root cause not yet found
- Exact area affected not fully determined
GNSS JAMMING (DoS)
USER CASE: DRILL SHIP

• Ships in affected area reports:
  • Intermittent loss of GNSS
  • None even outages (variable outage length)
  • Increasing number of outages pr day
GNSS JAMMING (DoS)
USER CASE: DRILL SHIP

- Data shows that GNSS DoS is dependent on:
  - Height above sea level
  - Direction of vessel

- Antenna separation matters

- INS integration Matters
Building the fence

RAIM

Safe Position & Timing

IMU integration

System installation

Dual antenna integration
GNSS SPOOFING (MEACONING)

- April 2018 spoofing of vessels position reported by the captain of the vessel
- Position reported to be within the same area as large spoofing attack of June 22-24 2017 (Black Sea)
- Investigation launched (not yet concluded)
- Shows clear signs of jamming
- Loss of position confirmed
- No faulty or misleading position found in logged data.
GNSS SPOOFING (MEACONING)

- Extended RAIM allows for correct handling of position
- Dual antenna integration allows for improved integration checks.
Building the fence

RAIM
IMU integration

Safe Position & Timing

Anti jamming Antenna NovaTel (GAJT®)

Dual antenna integration

System installation
GNSS JAMMING EXPERIMENT, NOVEMBER 2017

- Jamming experiment with FFI

- Equipment
  - Seapath
  - DPS 5D
  - SeaNav
  - CRPA antenna
  - 3rd party receiver

- Jamming GPS, Glonass, Galileo, Beidou

- Good cooperation with on-board crew
GNSS JAMMING EXPERIMENT, NOVEMBER 2017

- Blue line shows SN (Signal to Noise) for Novatel Gajt antenna
- Orange show SN (Signal to Noise) for standard Novatel 713 GGG antenna
- Operation up-time significantly increased with Novatel Gajt antenna.
  - Antenna is only GPS compatible.
Building the fence

RAIM
IMU integration
Safe Position & Timing
System installation

Anti jamming Antenna NovaTel (GAJT®)

Dual antenna integration
Conclusion
CONCLUSION

• No single system can be trusted 100% at all times

• Poor installations and unintentional interference are still the most common causes for unstable GNSS signal tracking

• There are several protective means available to reduce the risk related to potential jamming and spoofing scenarios also for non-military users
  – BUILD YOUR FENCE

• Train for the unexpected
WORLD CLASS
THROUGH PEOPLE, TECHNOLOGY AND DEDICATION