Resilience and Security of Geospatial Data for Critical Infrastructures

Session 6: Resilient Position, Navigation and Timing (PNT)
United Nations/Finland Workshop on the Applications of GNSS
October 24, 2023
Helsinki, Finland

Prof. Zahidul Bhuiyan
Finnish Geospatial Research Institute
Agenda

1. Background
2. Actual impact
3. Resilient PNT Actions at FGI
4. Recommendations
Background

- GNSS, being the backbone of any global scale navigation system, offers accurate PNT in good signal conditions but is vulnerable to jamming/spoofing
  => due to weak signal reception and open unprotected signal authentication provision

- Heavy dependence on GNSS-based PNT systems has made jamming/spoofing a growing threat

- There has been a considerable upsurge in GNSS vulnerability incidents due to the advancement of affordable software-defined radios, signal simulators, cheap availability of jammers, and a broader understanding of spoofing as an effective disruption strategy against GNSS-based applications.
Radio Frequency interference

In short: unwanted signal at GNSS frequencies

- Unintentional interference
  - Natural causes, e.g. ionospheric effects
  - Man made, e.g. faulty electronic equipment

- Intentional interference
  - Personal privacy devices
  - Criminal intent
  - State level electronic warfare

- Mitigation techniques
  - Receiver algorithms, Antenna design, Monitoring...
GNSS Spoofing

In short: Trick the receiver to use wrong position and/or time

- Can be either:
  - Targeted: time and/or location synchronised with target receiver
  - Untargeted, time and/or location are completely off
  - Meaconing, real GNSS signal repeated (with delay)

- Mitigation techniques
  - Navigation message authentication (Galileo OSNMA, ACAS and/or PRS), signal methods in the receiver
Importance of PNT as perceived by Finnish GNSS stakeholders

Agenda

1. Background

2. Actual impact

3. Resilient PNT Actions at FGI

4. Recommendations
Impact of spoofing on different COTS GNSS receivers

- 5 different receivers were tested under different types of spoofing attacks

### Table VI. Overview of spoofing impacts on DUTs

<table>
<thead>
<tr>
<th>DUT</th>
<th>Targeted spoofing</th>
<th>Untargeted spoofing</th>
<th>Meaconing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Spoofed?</td>
<td>Spoofed?</td>
<td>Spoofed?</td>
</tr>
<tr>
<td>M8T</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>F9P</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>X5</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Delta-3</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>FGI-GSRx</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
</tbody>
</table>

### Table VII. Summary of spoofing impact on positioning accuracy for live-sky spoofing attack

<table>
<thead>
<tr>
<th>DUT</th>
<th>$\varepsilon_{3D}$</th>
<th>$\varepsilon_H$</th>
<th>$\sigma_H$</th>
<th>$\varepsilon_V$</th>
<th>$\sigma_V$</th>
<th>Availability (%)</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>M8T</td>
<td>29.2</td>
<td>17.3</td>
<td>10.7</td>
<td>23.5</td>
<td>16.2</td>
<td>100</td>
<td>High</td>
</tr>
<tr>
<td>F9P</td>
<td>37.1</td>
<td>12.8</td>
<td>7.7</td>
<td>34.9</td>
<td>21.4</td>
<td>100</td>
<td>High</td>
</tr>
<tr>
<td>X5</td>
<td>21.6</td>
<td>12.1</td>
<td>8.2</td>
<td>17.8</td>
<td>12.3</td>
<td>100</td>
<td>High</td>
</tr>
<tr>
<td>Delta-3</td>
<td>34.8</td>
<td>15.9</td>
<td>8.7</td>
<td>31.0</td>
<td>17.0</td>
<td>89.6</td>
<td>High</td>
</tr>
<tr>
<td>FGI-GSRx</td>
<td>74.0</td>
<td>49.3</td>
<td>29.4</td>
<td>55.1</td>
<td>33.1</td>
<td>100</td>
<td>High</td>
</tr>
</tbody>
</table>

Varying spoofing impact on different GNSS receivers

Impact of high-power jamming on L1/E1 in terms of positioning accuracy

### Table: Scenario ID, GNSS Constellation, DUT scope, Comments

<table>
<thead>
<tr>
<th>Scenario ID</th>
<th>GNSS Constellation</th>
<th>DUT scope</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAM-CH-S-02: Static, Chirp wide (fast) in-band - L1/E1</td>
<td>GPS L1 C/A, Galileo E1, GPS L5, Galileo E5a</td>
<td>Mitigation: Interference detected on L1/E1 - MFMC based mitigation</td>
<td>MFMC diversity is applied on-the-fly based on the detection of interference at signal level for each frequency</td>
</tr>
</tbody>
</table>

### Figure 1: No Mitigation Applied

- Coordinate variation, 3D RMS: 68.667
- GPS L1, Gal E1, GPS L5, Gal E5a
- Variations (w.r.t. true position) [meters]
- UTC Time [hh:mm:ss]

### Figure 2: Mitigation Applied with AGC/IQ-based detection followed by MFMC mitigation

- Coordinate variation, 3D RMS: 2.3348
- GPS L1, Gal E1, Gal E5a
- Variations (w.r.t. true position) [meters]
- UTC Time [hh:mm:ss]
STRIKE3 International Monitoring Network

Across the globe
- United Kingdom
- Sweden
- Finland
- Germany
- France
- Poland
- Czech Republic
- Spain
- Slovakia
- Slovenia
- Netherlands
- Belgium
- Croatia
- Latvia
- New Zealand
- Canada
- India
- Vietnam
- Thailand
- Malaysia
- Japan

STRIKE3 participant countries each have 3+ sites. STRIKE3 Partnering countries have had 1 or 2 sensors. Some countries have moved a sensor to multiple locations to try to build up a bigger picture. Typical duration of a monitoring campaign at a site has been between 3 – 24 months.
STRIKE3 Master Database (1/2/2016 – 31/01/2019)

STRIKE3 master database currently has 556,198 entries covering all interferences, all powers and all durations.
STRIKE3 Breakdown of 556,198 Events

1. Unintentional interferences that have no impact at the DETECTOR Receiver
   - Total: 491,791

2. DETECTOR receivers impacted by Unintentional interferences
   - Total: 21,752

3. DETECTOR receivers impacted by deliberate jamming
   - Total: 7,326

4. Deliberate jamming that has no impact at the DETECTOR Receiver
   - Total: 57,081

Unintentional interferences (87%)

Receiver impact* (5%)

Deliberate Jammers (12%)
7,326 “jammers” that denied GNSS
Agenda

1. Background
2. Actual impact
3. Resilient PNT Actions at FGI
4. Recommendations
Finnish National Reference Network (FinnRef)

- **47 CORS** → Basis for the national reference frame, EUREF-FIN, few stations also serve as IGS stations, and also co-located with EGNOS RIMS
- All GNSS and multiple frequencies are observed
- Real-time positioning service ‘FINPOS’ uses FinnRef data to provide DGNSS, Network RTK measurement data
- Data format available in RINEX and real-time streams (RTCM MSM (GPS+GLO+GAL+BDS))
GNSS-Finland Service: Monitoring GNSS signal quality on all global constellations in multiple frequencies in 47 FinnRef stations

Per-station average CNR for last 60 minutes for signals:

- GPS L1
- GPS L5
- Galileo E1
- Galileo E5a
- Galileo E5b
- BeiDou B1
- BeiDou B3
- BeiDou B2a

Signal strength of:
GPS, Galileo, GLONASS, BeiDou

FinnRef network

Position monitoring

Signal deviation (m) for last 30 minutes

Position monitoring

Link to the service: https://gnss-finland.nls.fi

17.2.2023
Detected Jamming Incident in Pasila, Helsinki

Galileo E1

BeiDou B1

GPS L1

GLONASS G1
GNSS-Finland Service: Observed Event, Example 2

Metsähovi, GLONASS G1, C/N₀ drop

20. Jan 2021

Gyltö, position bias

+ Kevo, Tornio, Romuvaara
GNSS-Finland Service: Navigation Message
Authentication status of monitored Galileo satellites

- Galileo satellites’ NMA monitoring status in GNSS-Finland Service
- Notification to subscribed users for a spoofing event detection

- The purpose of FGI-OSNMA is OSNMA processing
  - Decode OSNMA related information from a data stream
  - Authenticate navigation messages based on this information
  - Report the results, or pass them forward
  - Notification to subscribed users for a spoofing event detection

https://github.com/nlsfi/fgi-osnma

Regular vs authenticated position using FGI-OSNMA
Mitigation via exploiting multi-constellation and multi-frequency diversity

- **Resilient FGI-GSRx MFMC receiver**: Intelligent signal selection based on key vulnerability matrix.

<table>
<thead>
<tr>
<th>DUT</th>
<th>$\varepsilon_{3D}$</th>
<th>$\varepsilon_{H}$</th>
<th>$\sigma_{H}$</th>
<th>$\varepsilon_{V}$</th>
<th>$\sigma_{V}$</th>
<th>Availability (%)</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGI-GSRx (L1 only)</td>
<td>194.8</td>
<td>190.6</td>
<td>98.7</td>
<td>40.2</td>
<td>18.0</td>
<td>100</td>
<td>High</td>
</tr>
<tr>
<td>FGI-GSRx (L1+E1)</td>
<td>80.2</td>
<td>74.9</td>
<td>37.7</td>
<td>28.6</td>
<td>14.8</td>
<td>100</td>
<td>High</td>
</tr>
<tr>
<td>FGI-GSRx (L1+E1+L5+E5a)</td>
<td>39.8</td>
<td>37.8</td>
<td>18.6</td>
<td>12.4</td>
<td>6.1</td>
<td>100</td>
<td>High</td>
</tr>
<tr>
<td>FGI-GSRx (E1+L5+E5a)</td>
<td>4.5</td>
<td>1.5</td>
<td>0.4</td>
<td>4.2</td>
<td>0.9</td>
<td>100</td>
<td>Low</td>
</tr>
<tr>
<td>MST</td>
<td>158.4</td>
<td>100.5</td>
<td>62.0</td>
<td>122.4</td>
<td>77.2</td>
<td>98.1</td>
<td>High</td>
</tr>
<tr>
<td>F9P</td>
<td>117.3</td>
<td>117.1</td>
<td>68.4</td>
<td>9.6</td>
<td>6.1</td>
<td>100</td>
<td>High</td>
</tr>
<tr>
<td>XS</td>
<td>12.9</td>
<td>11.4</td>
<td>7.4</td>
<td>6.1</td>
<td>4.1</td>
<td>78.1</td>
<td>High</td>
</tr>
<tr>
<td>Delta-3</td>
<td>86.7</td>
<td>63.4</td>
<td>57.3</td>
<td>59.1</td>
<td>53.6</td>
<td>100</td>
<td>High</td>
</tr>
</tbody>
</table>

(Left): Position solution with all available constellations, (Right): Spoofing detection-based constellation selection for position solution with FGI-GSRx


https://github.com/nlsfi/FGI-GSRx
https://doi.org/10.1017/9781108934176
GNSS-Finland Service: Ongoing Activities

- Utilise machine learning methods for event identification
- Automatic classification of events
- Theoretical 'area-of-impact' analysis on interference events
- Smart notification to end-users based on alert level
GNSS-Finland Service: An example case for CORS NETWORK Monitoring

Example of Co-operation and handshaking among different data sources

Public GNSS Data Sources

Public GNSS data

Atmospheric data

MIE

External Data Sources related to Earth Science

Timing data

Earth data

VÄYLÄ

Traficom

Government

ANS Finland

Finnish Defence Forces

Maritime

Land

Policy

Air

Security
Agenda

1. Background

2. Actual impact

3. Resilient PNT Actions at FGI

4. Recommendations
Recommendations: Receiver/Antenna Technologies

- Multi-constellation Multi-frequency diversity
- Modernized GNSS signals and services such as Galileo E1 OSNMA (currently under live testing phase) and Galileo E6 CAS encryption (currently under development)
- Intelligent advance algorithms at tracking and measurement layers
- ‘Resilient PNT Conformance framework’* will directly influence the future design, acquisition, and deployment of resilient PNT systems at a global scale.
- Low-cost antenna array solution may improve PNT resilience in the form of interference/spoofing source detection, localization, and mitigation

* https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf
Recommendations: Alternate PNT / Sensor Fusion

- LEO signals and satellite constellations specifically dedicated to PNT
- Receiver specific implementation that is yet to be emerged as a commercial solution to exploit GNSS+INS+LEO+SOOP (5G, etc.) with intelligent fallback mechanism.
- Space-borne interference monitoring at LEO
- Coupling of communication and localization capabilities could be used for positioning in drones, road, in and around airports and coastal areas.
Recommendations: GNSS Performance Monitoring and Alerting Network

- A wide area GNSS threat monitoring system can be developed utilizing existing national or international continuously operated reference stations, that can simultaneously monitor all GNSS frequency bands and report to a central database in case of a vulnerability incident.

- The establishment of an international or EU-level unified interference monitoring hub to identify, detect, locate, and auto-report GNSS disruptions.

- Crowdsourced interference detection could be better utilized for GNSS interference/signal quality heatmap generation.

- Privacy issue is a big concern from a regulatory perspective, and this needs to be tackled for crowdsourced data.

- Dissemination actions among the member states need to be undertaken to increase awareness and motivation among all authoritative bodies.
Advancing together