T4300 – Final User Forum
Spin-off: GNSS Vulnerabilities

Building EGNSS capacity On EU & Neighbouring multimodal Domains

Tallinn, ESTONIA
14th/15th June 2017
Bence Takács, BME
• Received GNSS signals are extremely weak, like a 100W light bulb flying at a height of 20 000 km

• Pseudo random code on carrier wave

  1  0  1  1  0  1  0

  Binary code PRN

  \[\text{Carrier wave}\]

  \[\text{BPSK modulated signal}\]

• GNSS blocking or GNSS jamming or GNSS interference
• For military purposes
  • Operating range: 150-200 km
  • Output power: 4 W
  • Weight: 5-10 kg

http://www.qsl.net/n9zia/wireless/gps_jam-pics.html
Low-cost GPS jammers

- **For civil usage**
  - Limited effective range, < 10 m (?)
  - To block navigation system of a car
  - Why?
    - To steal a car,
    - to hide the vehicle from the dispatchers,
    - To avoid paying toll,
    - ....
  - Multi device: GSM, wifi, GPS
  - Easy to buy on the black market (Internet)
1st test: Effective range, everyday GNSS
Effective range, everyday GNSS

- about 10 m
2\textsuperscript{nd} test: Effective range, professional GNSS

GPS jammer, in varying position

professional GNSS receiver
Effective range, professional GNSS

- up to 170 m
3rd test: Guided exercise with DINTEL

Location of BME EGNOS monitor station
Detected interference events

<table>
<thead>
<tr>
<th>#event</th>
<th>date</th>
<th>power [dBm]</th>
<th>frequency [MHz]</th>
<th>bandwidth [kHz]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2016-05-06</td>
<td>-118.2</td>
<td>1581.73</td>
<td>16.37</td>
</tr>
<tr>
<td>3</td>
<td>2016-05-06</td>
<td>-113.6</td>
<td>1568.86</td>
<td>12.98</td>
</tr>
<tr>
<td>14</td>
<td>2016-05-06</td>
<td>-120.3</td>
<td>1571.93</td>
<td>5.41</td>
</tr>
<tr>
<td>15</td>
<td>2016-05-06</td>
<td>-116.1</td>
<td>1578.54</td>
<td>31.85</td>
</tr>
<tr>
<td>17</td>
<td>2016-05-06</td>
<td>-120.1</td>
<td>1574.86</td>
<td>6.17</td>
</tr>
<tr>
<td>18</td>
<td>2016-05-07</td>
<td>-109.9</td>
<td>1579.93</td>
<td>42.11</td>
</tr>
<tr>
<td>32</td>
<td>2016-05-07</td>
<td>-111.0</td>
<td>1580.12</td>
<td>23.13</td>
</tr>
<tr>
<td>41</td>
<td>2016-05-07</td>
<td>-118.8</td>
<td>1583.24</td>
<td>17.60</td>
</tr>
</tbody>
</table>

Measurement campaign

- 6th – 26th May 2016
- A few events per day
- Source???

GPS L1 frequency: 1575.42 MHz
Examples of detected interference events

<table>
<thead>
<tr>
<th>time</th>
<th>frequency [MHz]</th>
<th>power [dBm]</th>
<th>bandwidth [kHz]</th>
</tr>
</thead>
<tbody>
<tr>
<td>06:17:18</td>
<td>1583.47</td>
<td>-106.7</td>
<td>63.95</td>
</tr>
<tr>
<td>06:17:22</td>
<td>1583.40</td>
<td>-102.7</td>
<td>97.06</td>
</tr>
<tr>
<td>06:17:26</td>
<td>1583.19</td>
<td>-106.1</td>
<td>51.41</td>
</tr>
<tr>
<td>06:17:26</td>
<td>1583.36</td>
<td>-112.7</td>
<td>31.86</td>
</tr>
<tr>
<td>06:17:30</td>
<td>1583.14</td>
<td>-105.2</td>
<td>82.05</td>
</tr>
<tr>
<td>06:17:34</td>
<td>1583.17</td>
<td>-113.3</td>
<td>37.01</td>
</tr>
</tbody>
</table>

GPS L1 frequency: 1575.42 MHz
SNR during an interference event

- SNR [dB-Hz] vs GPS time [h:m]
  - prn=13
  - prn=18
  - prn=15
  - prn=19
  - prn=17
  - prn=24
Performance during an interference event

Number of satellites vs GPS time [h:m]

Position error level vs GPS time [h:m]

Solution mode vs GPS time [h:m]

Protection level vs GPS time [h:m]
• Another example at BME EGNOS monitor station (21st February 2017)

• No SBAS PA position for a short period
Right after the event: less satellites used, higher DOP and higher vertical protection level
• A low cost GPS jammer can block everyday GPS within 10 m.

• It has effect on professional GNSS receivers even in 170 m range.

• Several interference events have been detected at BME EGNOS monitor station. Their source has not yet been proven, but these events might be caused by low cost GPS jammers installed in vehicles passing nearby.

• Outage in positioning may take up to a few minutes due to the initialization of smoothing.
Thank you

Bence TAKÁCS
takacs.bence@epito.bme.hu

BEYOND
Building EGNSS capacity On EU & Neighbouring multimodal Domains