Developing a GNSS resiliency framework for timing receivers

By Guy Buesnel and Adam Price

Spirent Communications, October 2017
Overview of Spirent Positioning and Timing
Real world threats to GNSS
Impacting Time and Position

Typical GNSS Vulnerabilities

- **Spoofing**
  - Covert
  - Deception

- **Interference**
  - Intentional
  - Unintentional

- **GNSS Segment Errors**
  - Erroneous upload data
  - SV Faults (E.g. SVN49)

- **Multipath**

- **Cyber Attacks**
  - Non-RF

- **Atmosphere**
  - Scintillation
  - Solar Activity
The spread of GNSS jamming
GNSS jamming – Real world reports

From the timing community…

“I have a NTGS50AA GPSDO (close cousin to the NTBW50AA and Thunderbolt) with the OCXO removed and a SRS PRS-10 rubidium oscillator in its place. I have been running Lady Heather 5.0 and have changed the damping, gain, and time constant to give me a 20,000 second time constant with a damping of .6. I have attached a Lady Heather screen shot of the weird behavior. You can see that my GPS antenna is in a very none ideal location (window on the west side of the building).

Once per day (about 8am) something disturbs the system. So, the GPSDO spends much of its time recovering and never gives me anywhere near the performance that this system is capable of. I would think that it is not the PRS-10 as it has no knowledge of time. I would also think that it is not the GPS system or receiver, since the GPS constellation repeats twice per day.

Kind of the two things that I am left with are a glitch by the power company every morning (there is some large industrial machinary across the street (but then I would kind of expect glitches at 8am and 5pm), and perhaps Lady Heather doing something funny. This system has been running for quite some time, I have not tried restarting Lady Heather yet.

Anybody seen anything like this, or have any good ideas?”
Segment errors—Real world reports

- Following high profile GPS timing error (Jan 2016) …and GLONASS corrupted ephemeris (April 2014)

- Galileo had problems in May 2017…… Navigation messages were not refreshed from 15:50/14th May – 12:44/16th May

- Need to check for user segment faults
GPS jamming – Detection in the real world

- Spirent has seen over 15000 GPS L1 interference events since fielding sensors in 2015
- Our interest is in the characterization and replay of threat waveforms in a simulated environment (impact assessment)
GPS Spoofing – emergence as real threat

- Low cost Software Defined Radios are the hackers’ equipment of choice
  - All code to make a GPS transmitter is available to download from internet (Github or other sources…)

Reported in press 17th December 2015

- Highlighted attempts to jam and spoof drones patrolling US/Mexico border
- Attempted GPS spoofing in the real world reported for the very first time
- Criminals using technology to attempt to disrupt GNSS
Press Story 27 December 2016

- Reports that Car drivers experienced “strange problems” in St Petersburg
- Car Sat navigation systems show location near Pulkovo airport when they are actually in city centre
- Possible GNSS spoofing?

Sep 2017: US Maritime Advisory (MARAD) issued

- GPS disruption in Black Sea region – interference and evidence of an “incorrect signal”
- 20+ ships affected – complaints of GPS interference and several false positions being reported by on-board navigation systems during June.
- Maritime Advisory subsequently issued by U.S.
Turning the clock back

DEFCON 25, August 2017, Caesar’s Palace

- How to spoof NTP using a programmed SDR
- Masterclass in One Time Authentication Token misuse…
- Later on that afternoon – tv server in the hotel was 2hrs out compared to my watch….(which was accurate)
  - Weather applications wouldn’t open properly
  - Streaming services all failed
  - Spoofing GPS signals indoors is easy
    - GPS enabled equipment will often acquire the first signals it receives
Real GNSS Spoofing

September 2017 – ION GNSS+

- Highly prestigious Global Satellite Navigation conference and exhibition organised by the Institute of Navigation
  - This year held at the Portland Convention Centre, Oregon
- Thursday 28th September - Multiple incidents of smart phones erroneously indicating incorrect time and position as reported by numerous users (Time in the past, position showing as somewhere in Europe)
- Some types of phones recovered in minutes after the anomaly – other phones took several hours to recover
- Some users had to ask for assistance from retailer or service provider
- Incident traced to inadvertent leak of RF radiation from an exhibitor’s stand

Accidental on this occasion and occurred at a conference of the world’s PNT experts

The impacts would have been more severe under other circumstances
Issues around quantifying robustness for timing receivers

- Traditionally….

- Issue - Position error isn’t the best way to derive timing errors
  - 1PPS - Receiver clock synched to GPS clock – GPS signal unavailable – 1PPS still outputs (but becomes inaccurate very quickly)
  - Stability of time delay through receiver also very important
  - C/N0 used by some standards but does C/N0 degradation affect 1PPS or the receiver time delay?

5.4.2.2 Use case: Static Location Target
5.4.2.2.1 Operational environment: Open area

The performance requirements are specified in table 18.

Table 18: Performance requirements for GNSS Time Accuracy, Static location target, Open area

<table>
<thead>
<tr>
<th>Metric</th>
<th>Maximum time error (ns)</th>
<th>Mean value</th>
<th>95th percentile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td></td>
<td>6</td>
<td>17</td>
</tr>
<tr>
<td>Class B</td>
<td></td>
<td>17</td>
<td>30</td>
</tr>
<tr>
<td>Class C</td>
<td></td>
<td>75</td>
<td>117</td>
</tr>
</tbody>
</table>

5.4.2.2.2 Operational environment: Urban area

The performance requirements are specified in table 19.

Table 19: Performance requirements for GNSS Time Accuracy, Static location target, Urban area

<table>
<thead>
<tr>
<th>Metric</th>
<th>Maximum time error (ns)</th>
<th>Mean value</th>
<th>95th percentile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td></td>
<td>216</td>
<td>260</td>
</tr>
<tr>
<td>Class B</td>
<td></td>
<td>260</td>
<td>359</td>
</tr>
<tr>
<td>Class C</td>
<td></td>
<td>520</td>
<td>597</td>
</tr>
</tbody>
</table>

5.4.2.2.3 Operational environment: Asymmetric area

The performance requirements are specified in table 20.

Table 20: Performance requirements for GNSS Time Accuracy, Static location target, Asymmetric area

<table>
<thead>
<tr>
<th>Metric</th>
<th>Maximum time error (ns)</th>
<th>Mean value</th>
<th>95th percentile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td></td>
<td>403</td>
<td>653</td>
</tr>
<tr>
<td>Class B</td>
<td></td>
<td>517</td>
<td>850</td>
</tr>
<tr>
<td>Class C</td>
<td></td>
<td>670</td>
<td>1557</td>
</tr>
</tbody>
</table>
Other Issues

- Normal performance indicators don’t provide full picture
  - Processing algorithms
  - Latency
  - For augmented systems
    - Robustness – how well does the system resist a real world GNSS threat?
      - How well does it detect an anomaly?
      - When does it switch over to augmentation or hold-over system?
      - Does it still provide independent traceability to UTC during an event? If not, what are the implications?
    - Resilience - following exposure to a GNSS threat, how well does the system recover to its original operating condition?
      - Under what conditions does the system revert to original operating state?
    - A complicated picture.....
  - Difficult today to compare performance of equipment and systems across common set of criteria
Evaluating Resilience

Risk Assessment

Characterisation of environment – derive requirements for operation in degraded/denied GNSS

Assess Robustness

Test against a baselined set of threat tests and measure common performance criteria

Implement mitigation strategy

Evaluate performance – repeat risk assessment periodically
Evaluating Robustness – Implementation in the real world

Detect and Capture Real interference Events DETECTOR

Use captured interference to generate / synthesise interference file

Mix with GNSS Simulation With Spirent SimGen

Launch Spoofing Attacks with Spirent SimSAFE

Download Latest Threats from a Cyber Threat intelligence Library

DEVICE / SYSTEM UNDER TEST
Spirent Insights

- Spirent are concerned at the lack of improved robustness in devices and systems (manufacturers and integrators)
  - We are working with Cranfield University (Aviation Security) and University of Warwick Manufacturing Group (looking at ground based connected autonomous vehicles)
  - Working towards gaining an understanding of the factors that are critical to the assessment of PNT system robustness/resilience
- We are noting the trend of increasing GNSS-related incidents that are causing significant impact
- Spirent believe that there is a need to responsibly create awareness in many application segments
- We are happy to work with industrial and academic partners to promote improved awareness and understanding of the relevant risks
GPS: Trust but verify!

guy.buesnel@spirent.com

http://www.spirent.com/Solutions/Robust-PNT

Join the GNSS Vulnerabilities group on Linked In to find out more about GNSS jamming and spoofing