Adaption of a recent presentation.

Results from Measuring Campaign of Electromagnetic Interference in GPS L1-band

Patrik Eliardsson[1], Mikael Alexandersson[1], Michael Pattinson[2], Steve Hill[3], Åsa Waern[1], Yeqiu Ying[2], Dimitrios Fryganiotis[2]

[1] Dept. of Robust Telecommunications, Swedish Defence Research Agency, Linköping, Sweden

[2] Nottingham Scientific Ltd, Nottingham, England

[3] Satellite Applications Catapult Limited, Harwell, England

FOI

Overview

- Introduction
- Background
- STRIKE3 Project
- Interference detection equipment
- Host site locations
- Overview of results
- Detailed site analysis
- Conclusions

Introduction

- In this presentation, the results from a 3 month period international interference data collection campaign is presented
- The 2016 measurement campaign was carried out with the use of existing monitoring and reporting systems within the STRIKE3 project

Background

- In today's society we can see an ever increasing reliance on wireless technologies
- GNSS is being used for increasing range of safety, security, business and policy critical applications
- Intentional EMI (jamming) previously only used in the military domain is now spreading to civilian actors because dedicated jamming equipment is sold openly and inexpensively on the Internet

STRIKE3 – Long abbreviation…

Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation

Project homepage: http://www.gnss-strike3.eu/

STRIKE3 Project

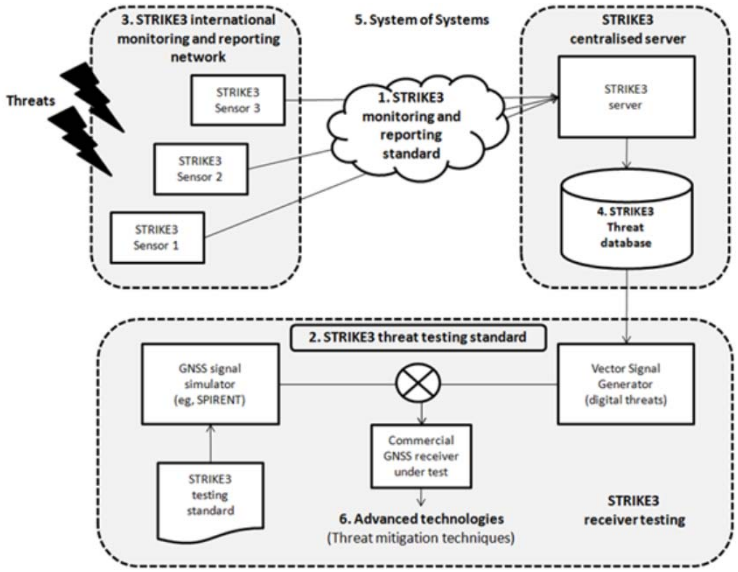
- The STRIKE3 project has been awarded by the European GNSS Agency (GSA) within the Horizon 2020 research program to address the need to monitor, detect, characterize and mitigate threats to GNSS services and applications
- The overall aim of the project is to develop and validate new international standards for the monitoring, reporting and testing of GNSS threats

Interference detection equipment

- Detector V1 (NSL)
- RF Oculus (FOI)
  - Software defined radio (SDR)
  - COTS GNSS receiver (Civil GPS L1
  - Computer with HDD storage
  - Measures power continuously
  - Store relevant measures (C/N_0, IR, time, position etc.) when limits are exceeded
  - Network connection to server

Back-office server and database

- Network connection to nodes
- Receive, collect and store events
- Classification of events
- Web interface for accessing data

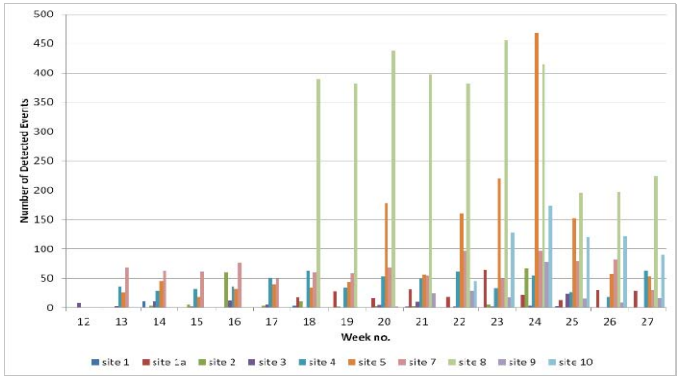


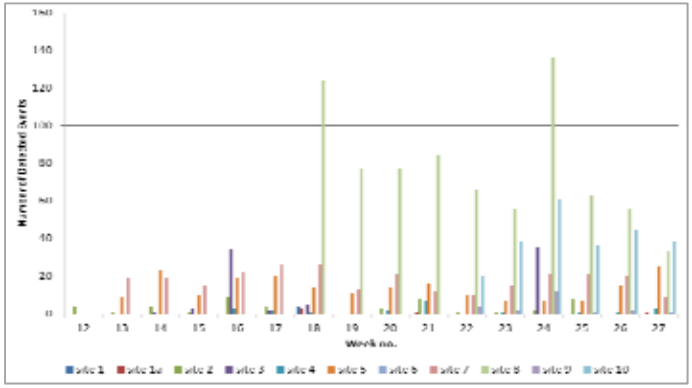
Host site locations

- Deployment countries
  - Sweden
  - UK
  - France
  - Poland
  - Czech Republic
  - Slovakia
  - Finland

Overview of results

- Huge variation between sites
- Week-to-week variations
- Different jamming waveforms are used
- Most “busy” sites:
  - ✓ office building in busy city area
  - ✓ vincinity of major road
- Remote sites are more quiet…
- Different detection systems results in different number of events

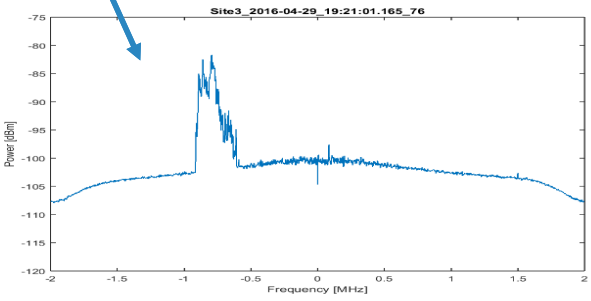


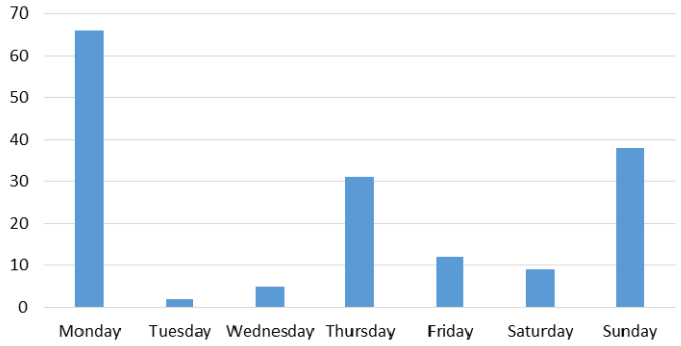


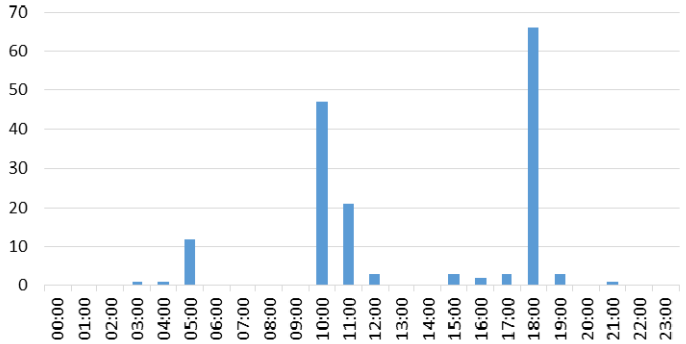
Detailed site analysis: Site 3

Site 3: Swedish Airport (March 2016)

- 163 events detected
  - 80 events with duration > 1 second
- Events during working hours
- Variation between days
- 13 seconds event:
  - 10 dB drop in signal quality (C/N_0)





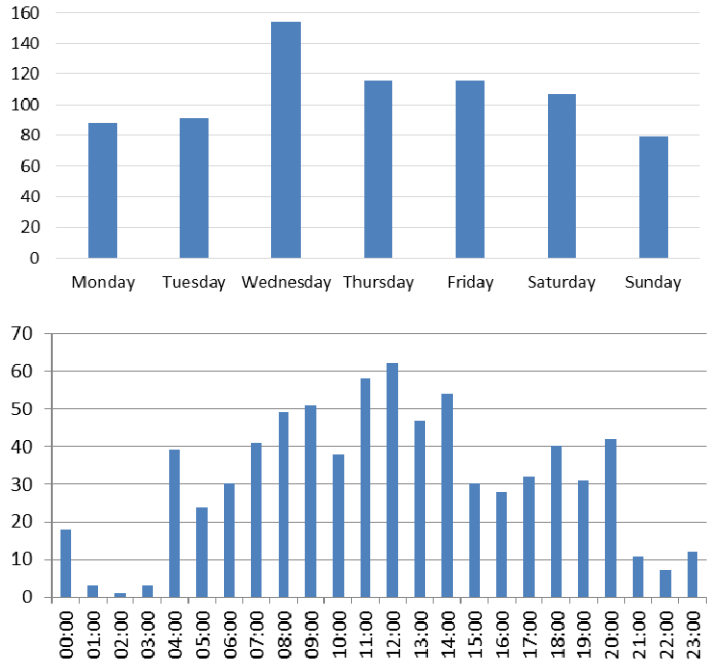


FOI

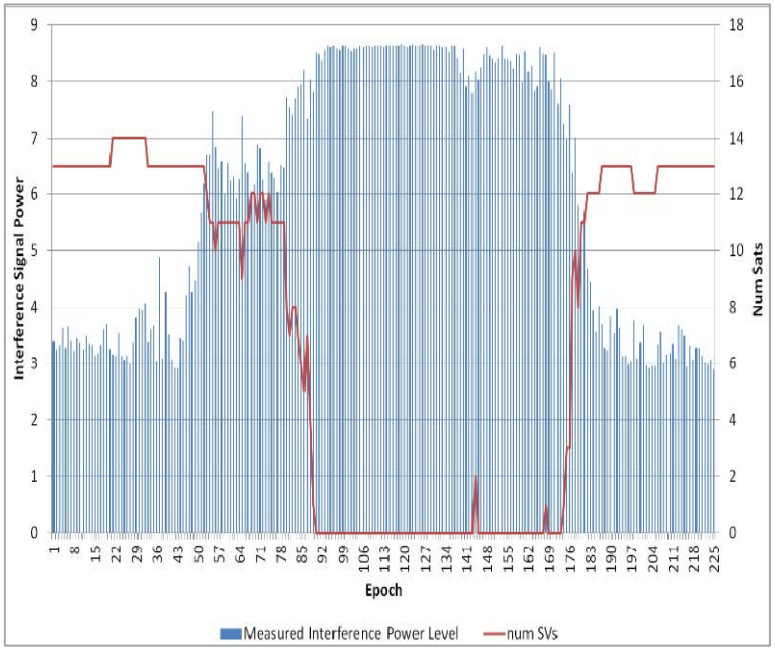
Detailed site analysis: Site 8

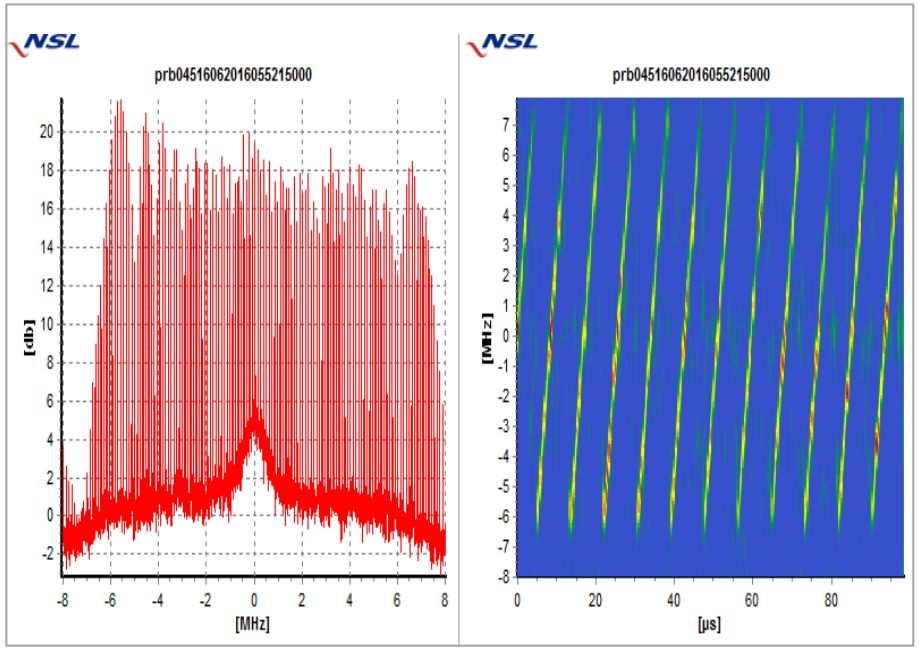
Site 8: Office in major city (April 2016)

- 2 months of data
- 3000 events detected
  - 643 events are possible jammers
- More events during working hours
- Less variation between days
- 7.5 minutes event on 22/6 2016:
  - Loss of GPS tracking



Detailed site analysis: Site 8





Conclusions

- Interference events have been detected at all sites although there is a huge variation in the number of weekly events at each site
- Not all detections are intentional interference, and many are low power or last for short time periods
- Most active site over 100 detections of significant events in some weeks (~ 15 events per day)
- In terms of impact, many events do not have noticeable impact on the embedded GPS receiver
- GPS receiver reported large position errors (hundreds of meters) during some interference events

FOI

Thanks for your time!

Björn Gabrielsson
Email: bjorn.gabrielsson@foi.se
Swedish Defense Research Agency, FOI