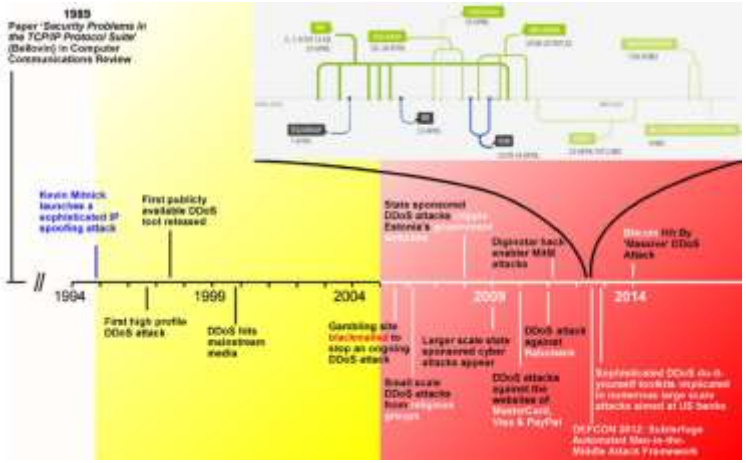
Towards categorizing the level of protection that GNSS Receivers provide in adverse environments

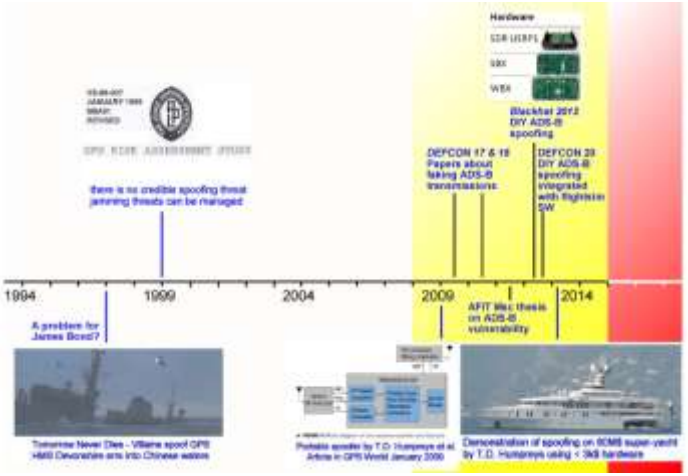
Guy Buesnel CPhys AFRIN

Introduction

Bradford Parkinson "Protect Toughen Augment GPS", RIN/KTN GNSS Vulnerabilities and Resilient PNT, Feb 2014, Teddington

Erik Theunissen "So you think you are Safe" – comparison of IP and GNSS threat evolution, ENC-GNSS 2014, Rotterdam





What is the most likely threat scenario that GNSS Receivers should be toughened against?

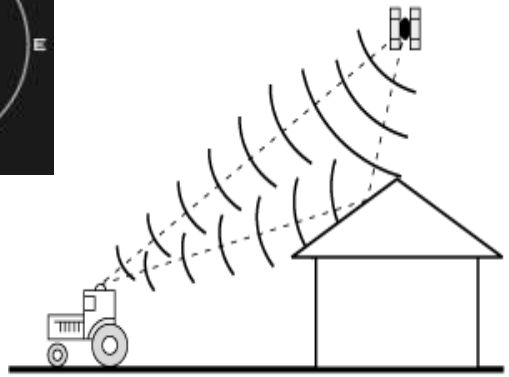
SPIRENT

(Image from Mebourneer website)

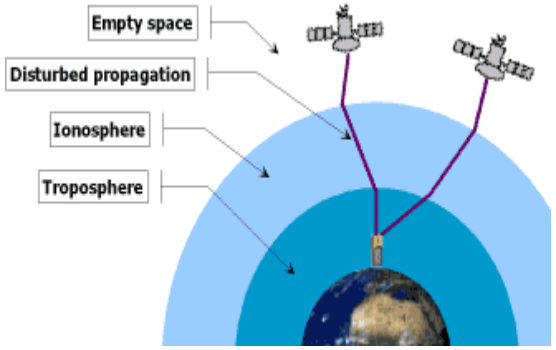
SPIRENT

GNSS Adverse environments - natural

Availability



High Multipath environments



Solar Weather

SPIRENT

GNSS Adverse Environments – Man made

- Poor installation (or cheap unreliable system)

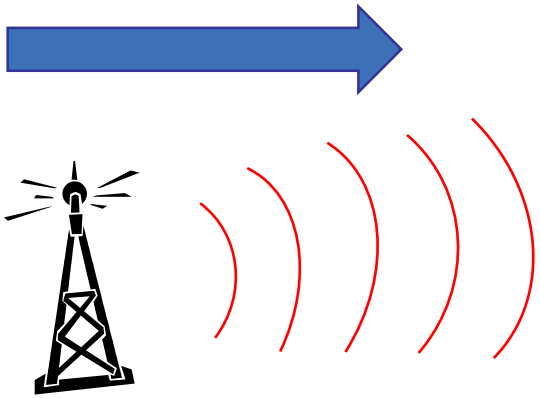
- Deliberate jamming
- Cyber Attack
- Spoofing

- Difficult installation – e.g. high Electromagnetic Compatibility (EMC)

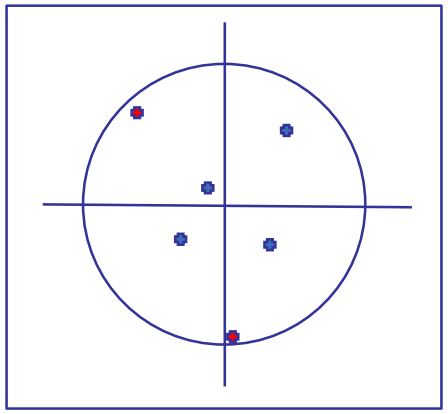
- Transmitter harmonics or other (accidental) interference sources

SPIRENT

GPS Jamming



GPS interference source



At the GPS Receiver:

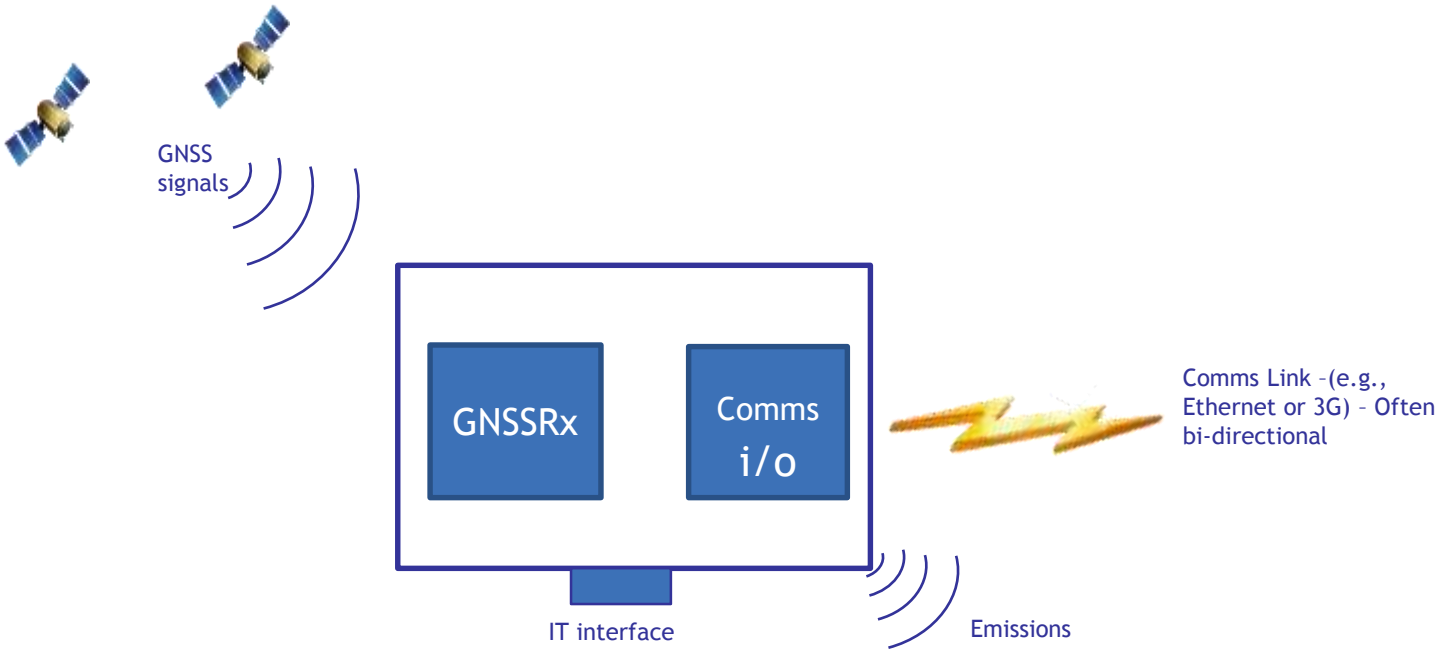
- Carrier to Noise Ratio (CNR) degraded – the low elevation satellites are affected first…..
- Noise increases – increasing errors in positioning and timing
- Eventually Receiver cannot track any more

Jamming trials in the North Sea (project STAVOG, 2012) showed that it was possible for a shore based jammer to induce large positional uncertainty in the host GNSS receiver without any alarms or other indication of poor accuracy

SPIRENT

Cyber Attack

- A GNSS Receiver isn't only vulnerable to RF jamming and conventional spoofing attacks….



The GNSS signal channel is one available door for a cyber-attacker

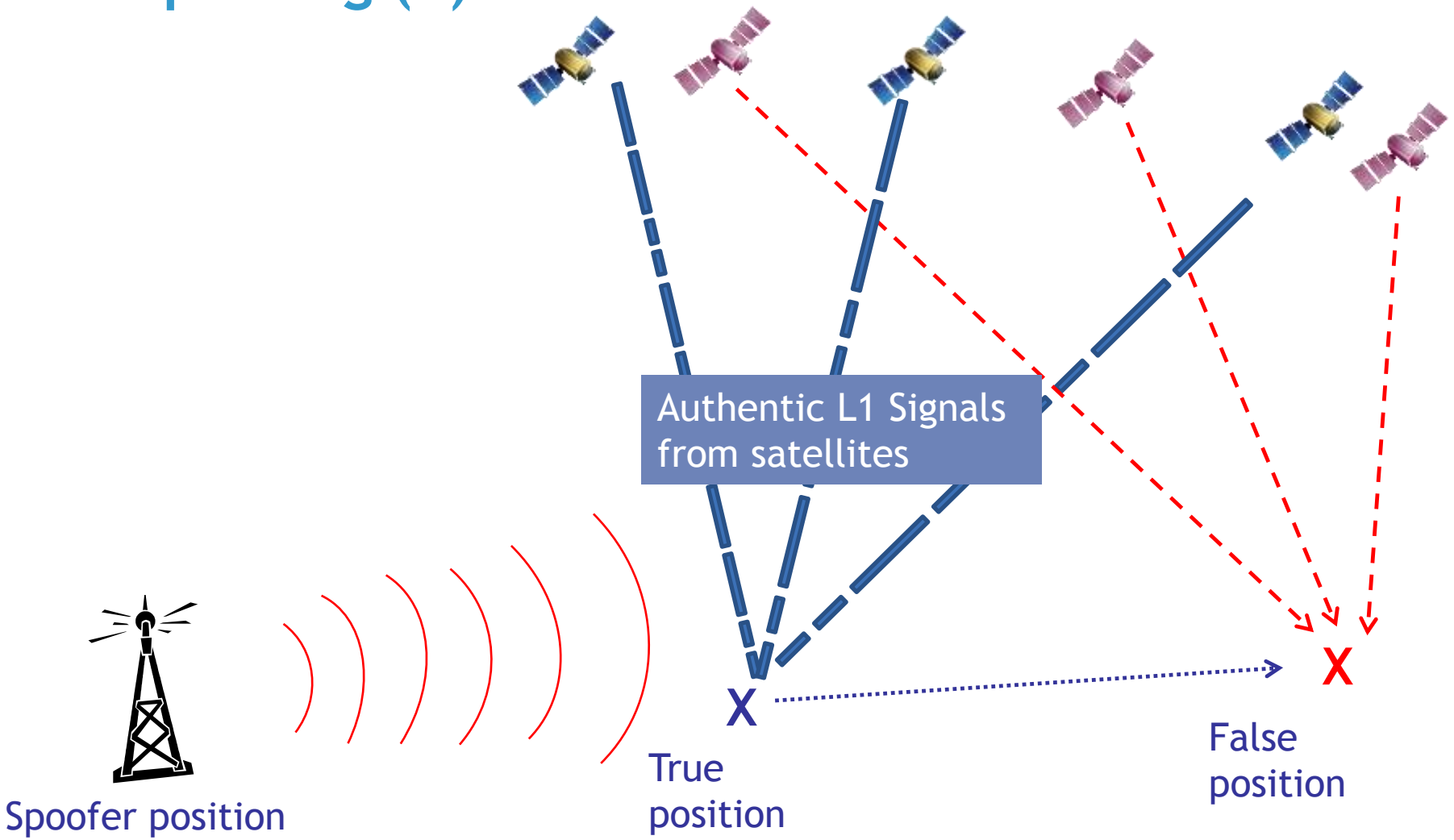
Real GNSS events

- May 2014, Australia
- User equipment incorrectly processed data from GPS SVN-49 even though the satellite status was set to unhealthy
- Large number of devices in Australia known to be affected
- Problem occurred with specific chipset
- In unobscured environment, the effect was that there were complete outages that lasted for several hours at a time!
- S/W test to GPS SPS ICD would have detected this…

- April 2014
- Corrupted ephemerides uploaded to GLONASS satellites
- GLONASS receivers affected for 12 hrs
- Some GPS + GLONASS Receivers experienced problems
- S/W test to the Open Service ICD would **not** have detected this….

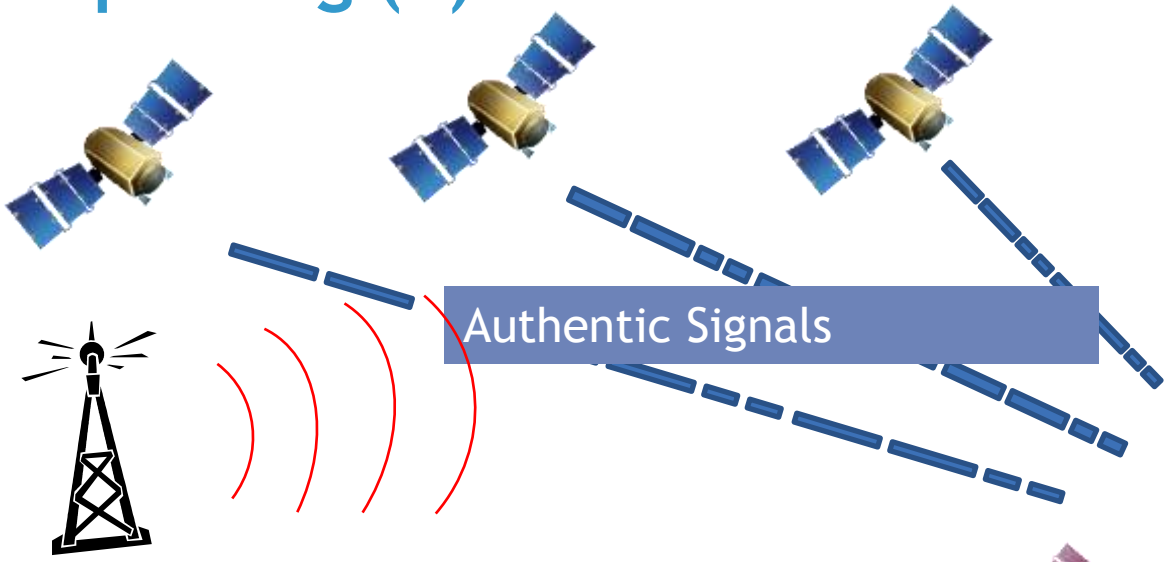
Examples are anecdotal - customers would like to recreate these scenarios

GPS Spoofing (1)



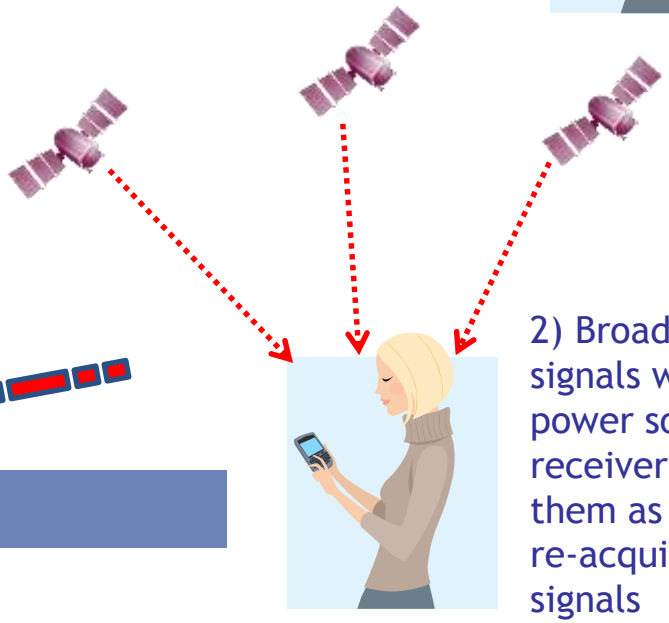
SPIRENT

GPS Spoofing (2)



1) Jam the user's GPS Receiver so it can no longer track GNSS signals

GPS interference source



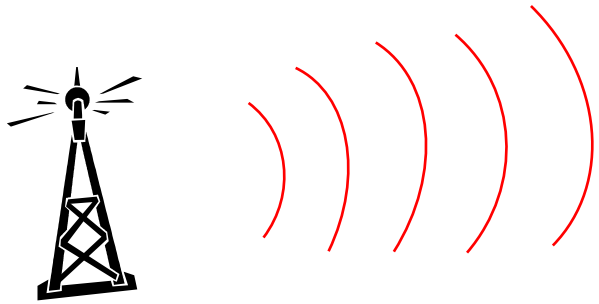
2) Broadcast fake signals with strong power so the user's receiver locks on to them as it tries to re-acquire GPS signals

GPS Spoofer

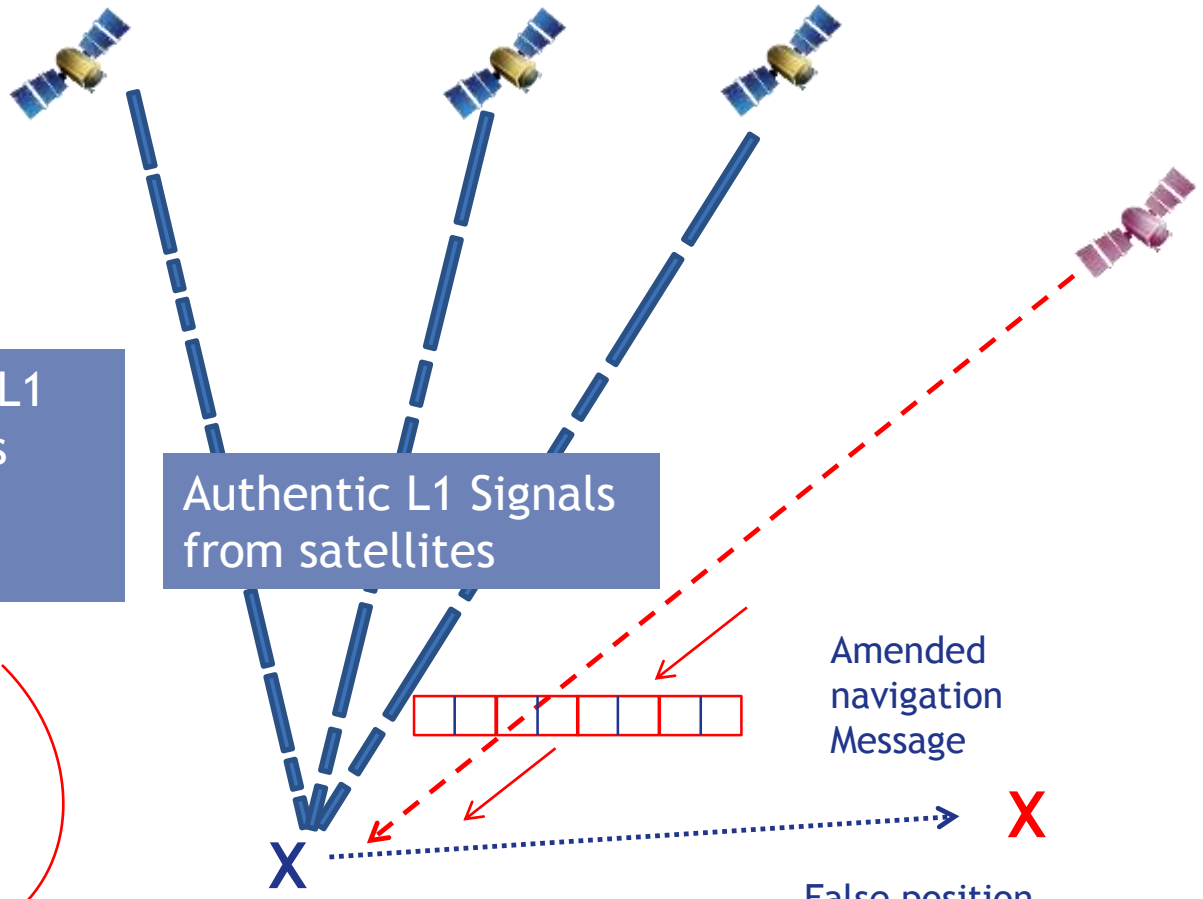
SPIRENT

GPS Spoofing (3) – A faked message

Spoofing Signal – A faked L1 GPS signal with a spurious navigation message is introduced…

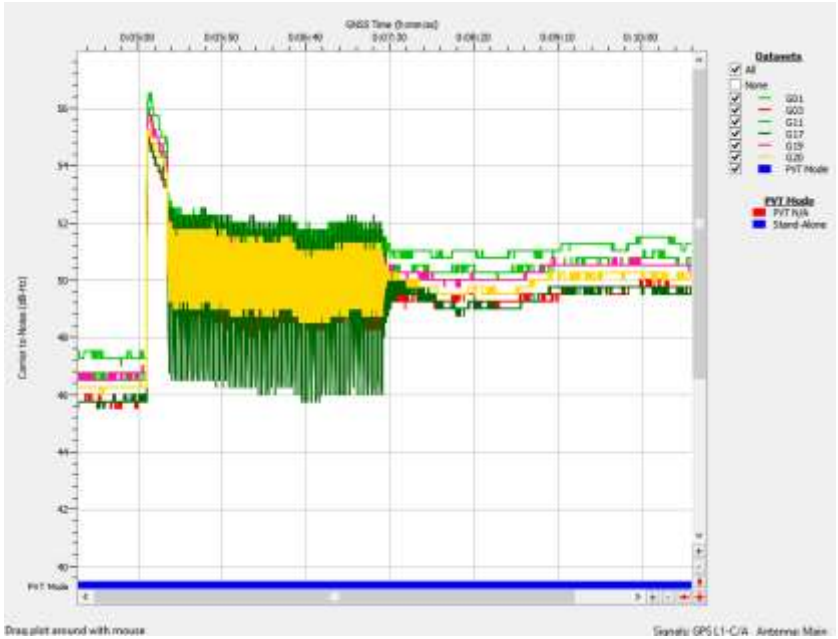


Spoofer position



SPIRENT

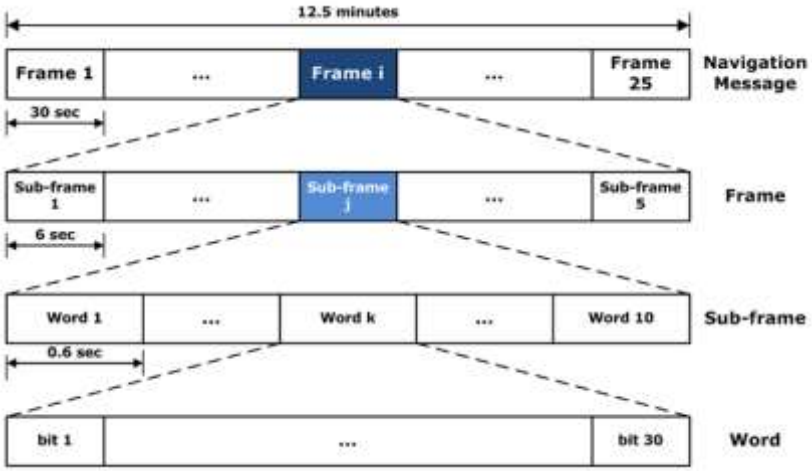
Detection in the GNSS Receiver



- Plot of Carrier to Noise Ratio CN0 of a GNSS Receiver under an attack
- Other interesting Receiver parameters to monitor are:-
  - Residuals – Pseudorange and Doppler yield interesting results during a spoofing attack
  - Automatic Gain Control (AGC) – Input signal levels are a good indicator of unusual events

SPIRENT

Level of trust in Nav message



Open Service GPS L1 Message structure

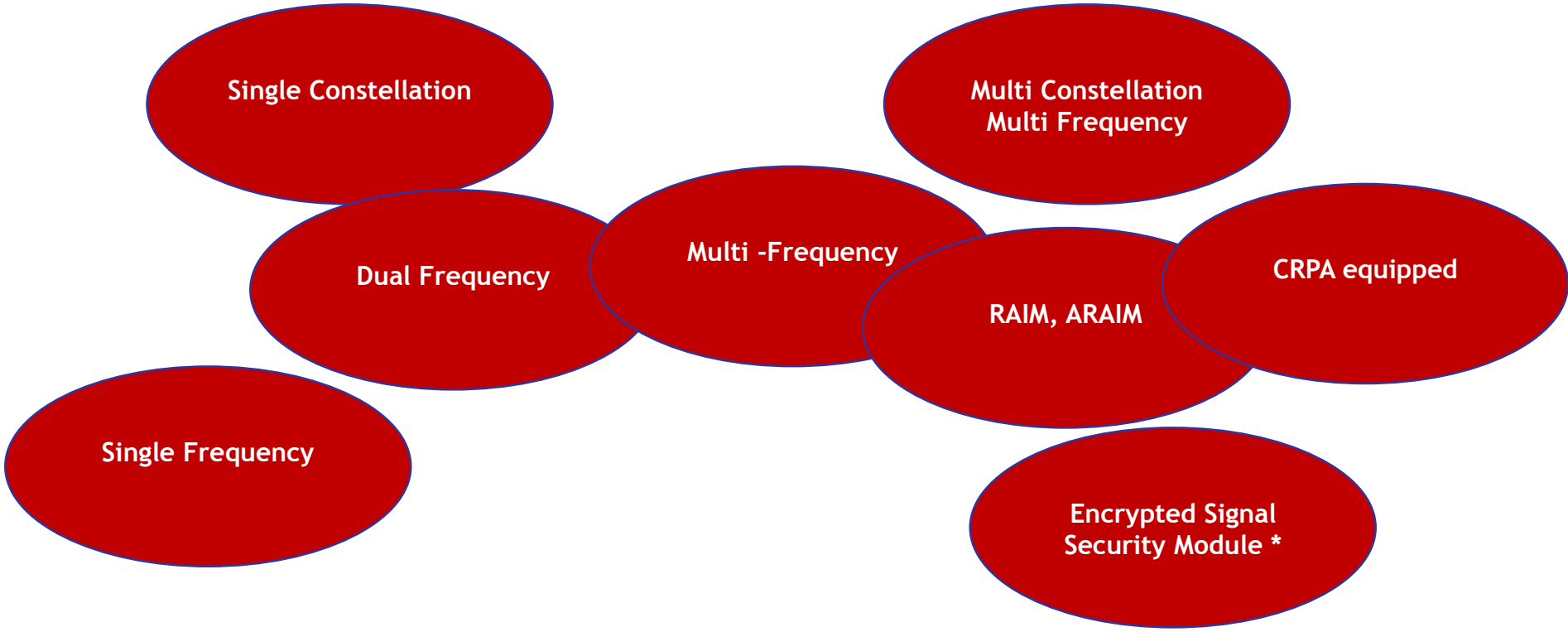
- Based on number of changes to message in unexpected places…
- Possible to formulate a mathematical model of trust (work is currently ongoing in this area – e.g., *"A trust framework for evaluating GNSS Signal Integrity, Xihui Chen, Gabriele Lenzini, Miguel Martins, Sjouke Mauw, Jun Pang, University of Luxembourg"*
- Integrity of received GNSS signals is defined – detection method based on the ideas of the relationship between consistency of attributes and signal integrity
- Could be used to detect attempts to fake the navigation message
- A warning could be generated if the level of trust falls below a certain value

GNSS Receiver operating modes

A GNSS Receiver has different modes of operation – these modes of operation affect the vulnerability level of the receiver. The US Air Force defined these modes of operation as:

- **State 1:** Normal Acquisition (L1 C/A code)
- **State 2:** Direct Acquisition (applies to GPS L2 P(Y)frequency)
- **State 3:** Code lock (Receiver maintains code lock but cannot maintain precise carrier tracking)
- **State 4:** Carrier lock (Receiver locks on carrier but pseudorange and pseudorange delta values may be inaccurate)
- **State 5:** Carrier Track/Data demodulation (Receiver tracks carrier and demodulates signal, accurate pseudorange and pseudorange delta values)
- **State 6:** Sequential resynchronisation (N/A for receivers with continual tracking)
- **State 7:** Signal reacquisition (Receiver that was tracking in State 5 but lost lock on GPS signals and is in search mode

Starting to Categorise – in general…

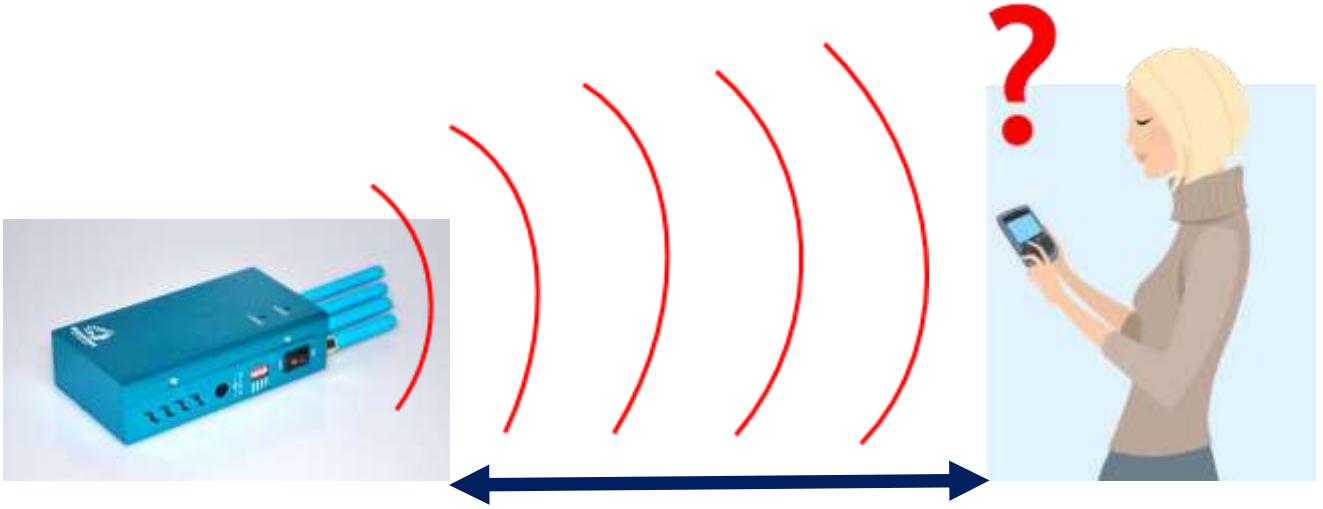


* Little/no protection against RF interference unless used in conjunction with other protection mechanism

SPIRENT

Starting to Standardise (1)

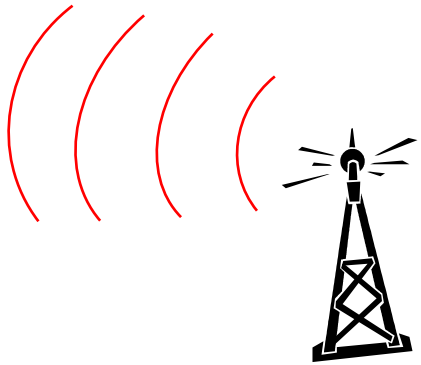
- Some universal measures
  - E.g. Jammer/Signal Ratio (J/S) for measuring performance during RF interference
    - Some sensitivities over publishing exact J/S that certain classes of GNSS Receiver can cope with – for obvious reason
    - But perhaps we could work towards a categorisation scheme that would deal with sensitivities whilst providing an indication of the interference environment the receiver can cope with
    - The J/S would allow a user to work out (for example) how close to a typical PPD the GNSS Receiver would operate (acquire, track etc)



SPIRENT

Starting to Standardise (2)

- Example Scenarios to test against:-
  - **Multipath**
    - Representative Urban environment (town centre)
    - Receiver in State 1 (Normal Acquisition)
  - **RF interference (including EMC issues)**
    - Multiple Broadband Personal protection Device in vehicles (urban environment)
    - Receiver in State 5 (tracking)
  - **Spoofing**
    - GPS L1 Frequency, 6 satellite channels – spoofing attack
      - Stationary transmitter, stationary receiver in State 5 (tracking)
      - Ramped power increase over authentic signals
      - Timing offset introduced on a slow ramp
  - Cyber
    - Simulation of fake navigation message parameters
    - Example Scenario – Injection of fake clock correction message to Receiver in State 7 (reacquisition)



Conclusions

- Categorisation and Standardisation of level of robustness of GNSS Receivers is complicated
  - Different attack vectors
  - Different Receiver operating modes
  - No standard framework for reporting GNSS vulnerabilities in a systematic and responsible manner
    - This would aid the categorisation and standardisation processes
    - Need to calibrate perceived vs real world threats…
- Some categorisation of devices is possible now
- Additional work needed to categorise threats and to devise applicable test scenarios and frameworks
- But it is possible to start toughening Receivers now – no need to wait for standards
    - Receiver manufacturers can set up some “most likely” scenarios and test against
    - OEM publishing some data on robustness would help purchasers with buy decision…

SPIRENT

Thank You

SPIRENT