transforming the way the world works

GNSS Vulnerabilities: Real or Really?

Haroon Muhammad

Senior Product Manager

Time & Frequency Division

Jun 12, 2014

Market perceptions

PBS NEWSHOUR

Researchers Steer Off Course to Show Potential Power of 'GPS Spoofing'
August 2, 2013 at 12:00 AM EDT

WIRED

GPS Hijacking Catches Feds, Drone Makers Off Guard
07.19.12 | 5:32 PM |

GPS spoofing the new game in town

College students hijack $80 million yacht with GPS signal spoofing

FOX NEWS .com
Fair & Balanced

EXCLUSIVE: GPS flaw could let terrorists hijack ships, planes
Published July 26, 2013

Was Malaysia Flight 370 Boeing 777 in fact GPS Terrorism Spoofing

GNSS as reference source

- Since the launch of first CDMA network in 1990 more than 685 commercial networks in 120 countries rely on GPS for time reference
- GPS timing is used in 15 of the “Critical Infrastructure Sectors”
- According to a US study of the 20 methods of getting time, all but two of them depended on GPS
- IEEE 1588 is also dependent on GNSS for primary reference

Jamming vs. Spoofing

Jamming and Spoofing are two entirely different concepts but they are often used together which tends to create confusion and false alarm

Jamming

- Generally unintentional
- RF Generation only
  - Knocks out GNSS system
  - Unable to track GPS signal
- Easy to produce
- Limited Area
- Easy to identify

Spoofing

- Always intentional
- Generate counterfeit signal
  - Full GNSS data reproduction
  - Can alter position/time information
- Complex / sophisticated equipment is needed
- Limited Area
- Difficult to distinguish from real signal

How many spoofing events?

- Trimble has shipped/deployed over 3 million GNSS timing receivers since 2000
- We have only received one report of a limited area "potential" spoofing incident in early 2000's reported by a network next to Chinese military installation
- The U.S. Department of Homeland Security assessed jamming disruptions to be more likely than spoofing incidents*

** DHS: National Risk Estimate, released November 2012*

GPS Outages vs. Network Breaches YTD

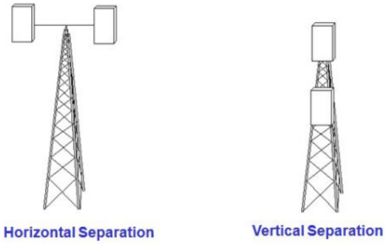
- **Major Network Hacking of 2014**
  - Jan: Microsoft's corporate email hacked
  - Feb: University of Maryland hacked, +300K SSN stolen
  - Mar: NSA hacked into Huawei's servers
  - Apr: Australian parliament computers hacked
  - May: E-Bay's DB hacked, 145 million accounts compromised
- **Live Network Attacks**

- Where as, there were no GPS outages reported this year
- Though there was a GLONASS outage in April

Trimble's GNSS timing receivers were unaffected by the GLONASS outage of April 1, 2014. Our units continued to function normally during the 10-hour outage.

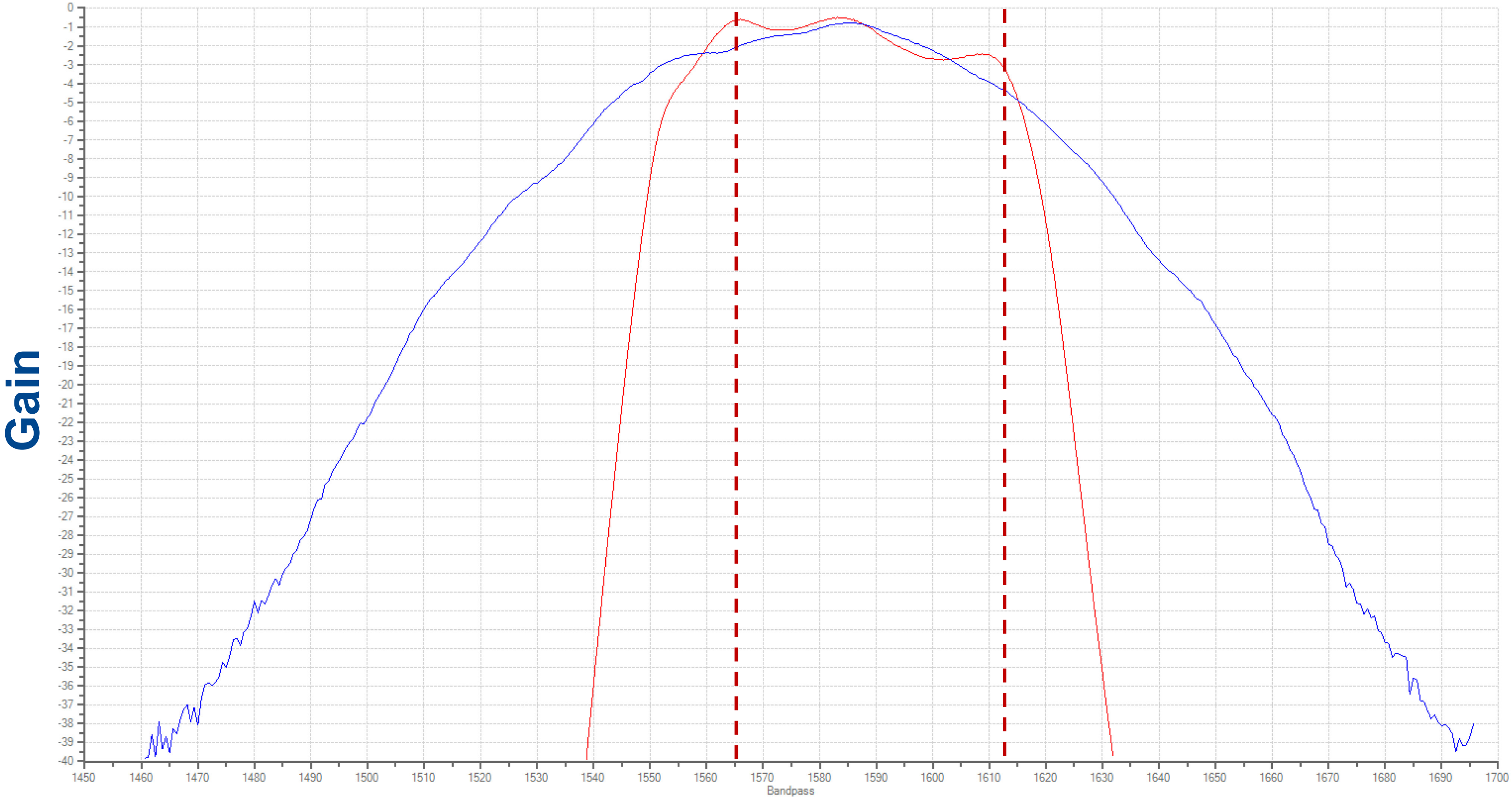
Mitigation the effects of jamming

- Knowing the environment
  - Spectrum sweep to characterize the RF
  - Site survey
- Selection of Antenna
  - Multiple layers of filtering
  - Larger ground plane
    - *May need ground plane treatment*
  - High linearity in the LNA design
- Antenna Installation
  - Spatial Diversity
  - Frequency Diversity (L1/L2)
  - Pattern Diversity



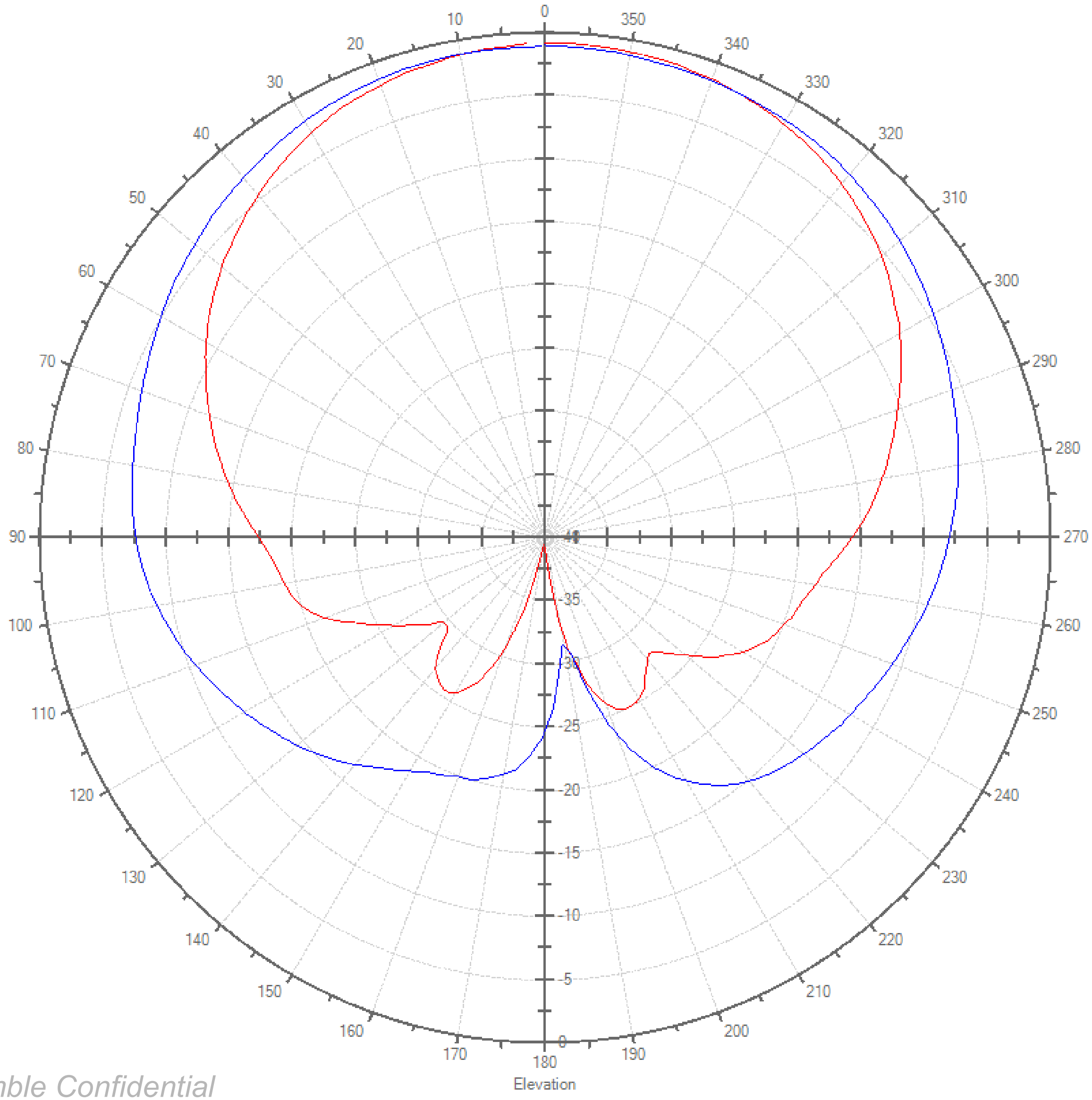
Bandpass Measurement (L1)

Filter vs. well Filtered Antenna



Frequency (MHz)

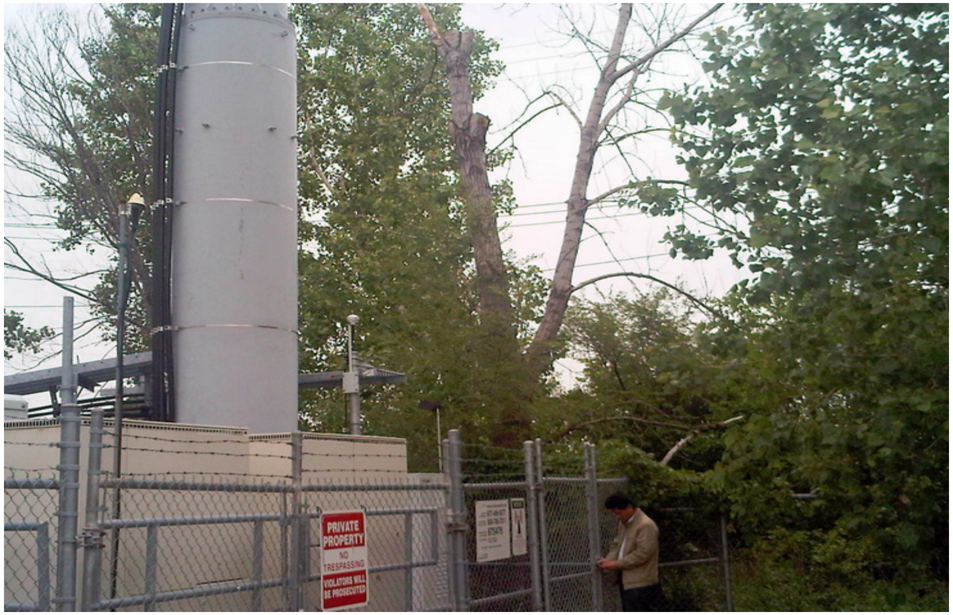
Elevation Pattern (L1)

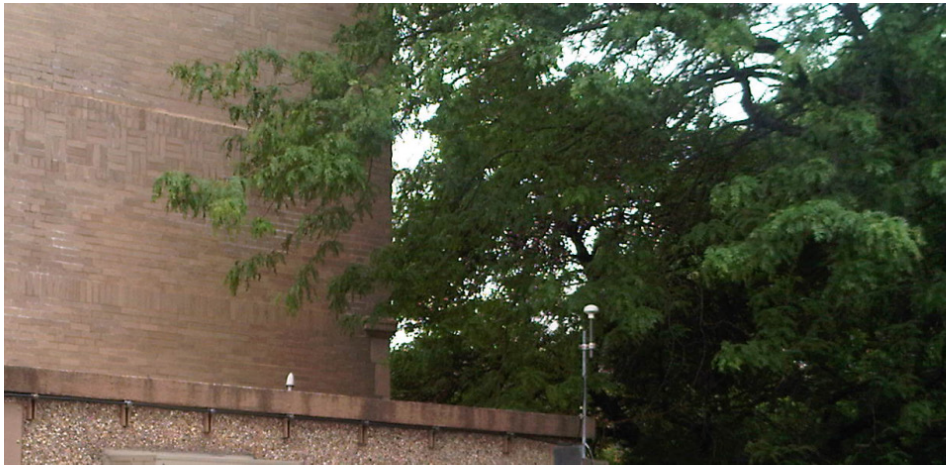


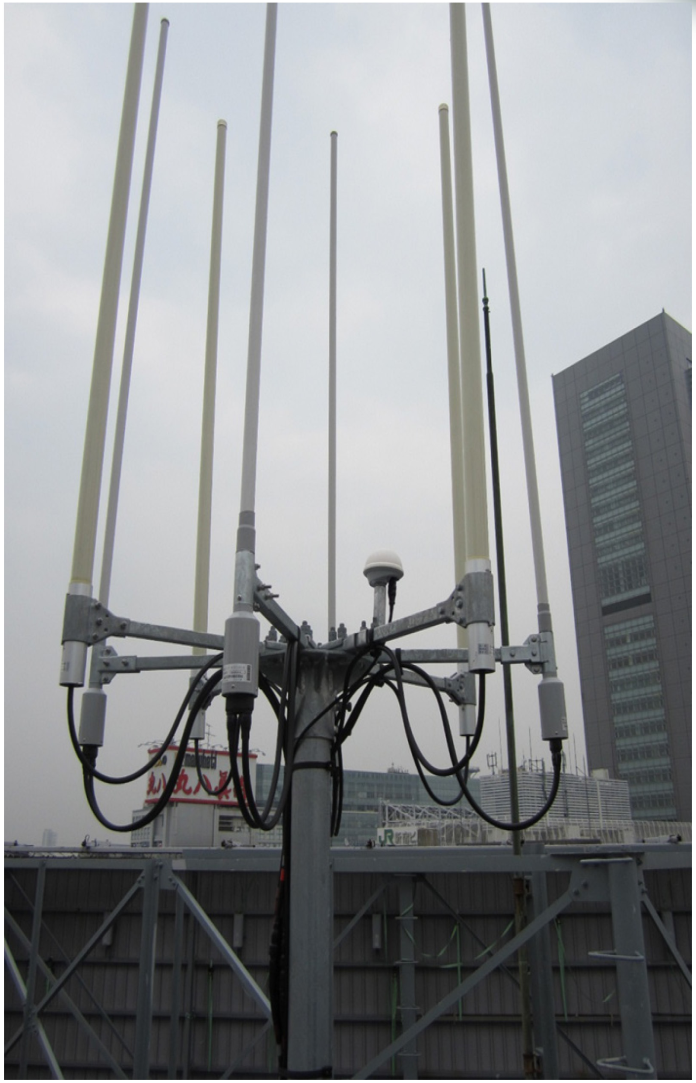
Small vs. Large Ground Plane

The amount of signal captured below the horizon is much higher with a smaller ground plane thus restricts the placement options

How not to install a GNSS antenna







Other Mitigation Techniques

- Secondary reference signal
  - Dual GNSS band, like GPS L1 & L2
  - Multi-Constellation
  - PTP (IEEE-1588) / SyncE
  - Good quality oscillator
- Improved Sensitivity
- Multi-stage Filtering
- Weak signal extraction
- Proper antenna site selection

Conclusion

- GNSS reference is still the only solution for distributed time
  - IEEE-1588 is based on GNSS (PRTC)
- Multi-constellation, multi-band provides the most robust solution
- The application and end-use case will determine the selection of timing source, but in some cases GPS is the only primary reference source