GNSS Security Issues
Jamming, Interference and Spoofing

Dinesh MANANDHAR

Center for Spatial Information Science

The University of Tokyo

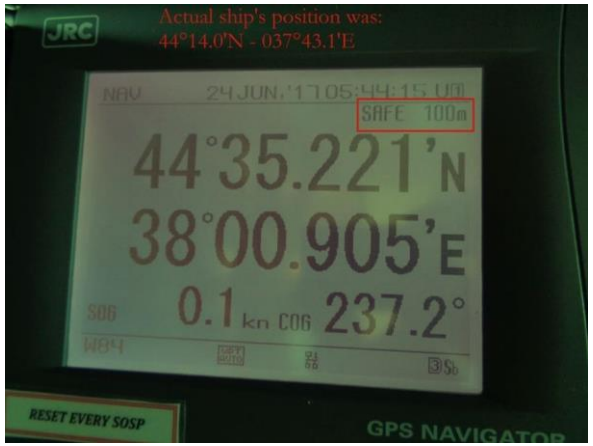
dinesh@iis.u-tokyo.ac.jp

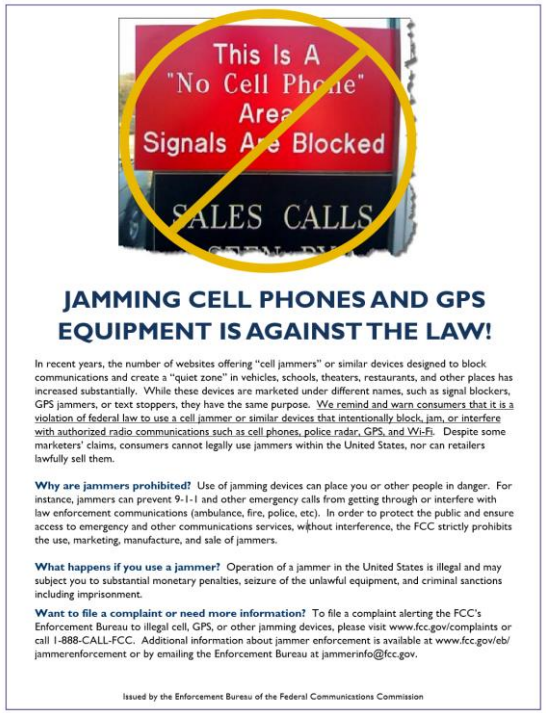
28th JAN 2021

GPS Security Issues

- **Jamming and Interference**
  - **Intentional or Non-Intentional**
  - **Many research and studies**
  - **Some solutions exist**
- **Spoofing**
  - **Intentional**
  - **Not so many research and studies**
  - **No perfect solution for Civilian Signals**
    - Galileo has announced authentication solution
    - We are conducting studies for authentication as well

Thousands using GPS jammers on UK roads pose risks, say experts : The Guardian
- https://www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks

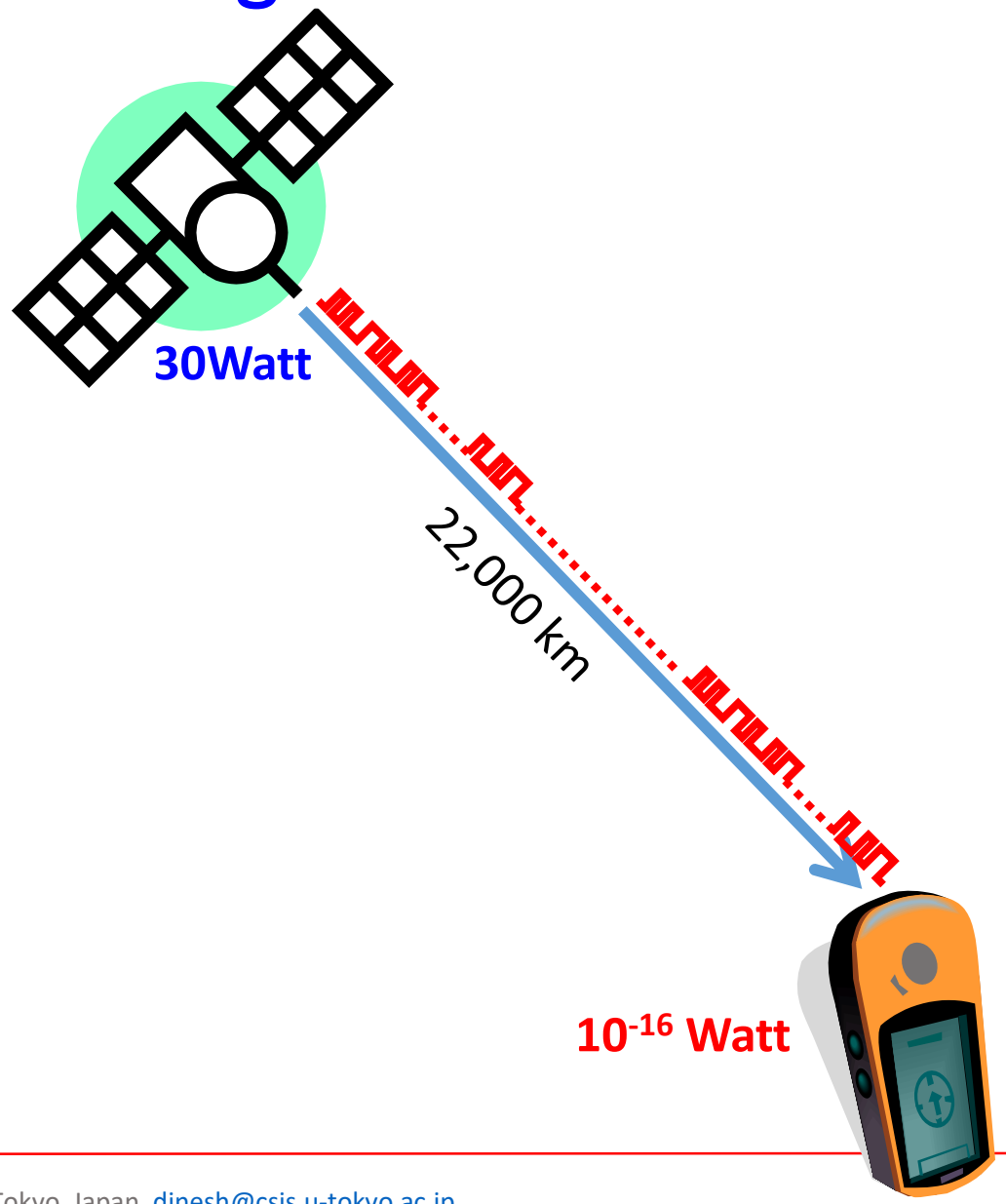




Source:
http://www.gps.gov/spectrum/jamming/

GPS Signal Power: How Strong or How Weak?

- GPS satellites are about 22,000km away
- Transmit power is about 30W
- This power when received at the receiver is reduced by 10^{16} times.
  - The power reduces by 1/(distance)^2
  - This is similar to seeing a 30W bulb 22,000Km far away
- GPS signals in the receiver is about 10^{-16} Watt, which is below the thermal noise

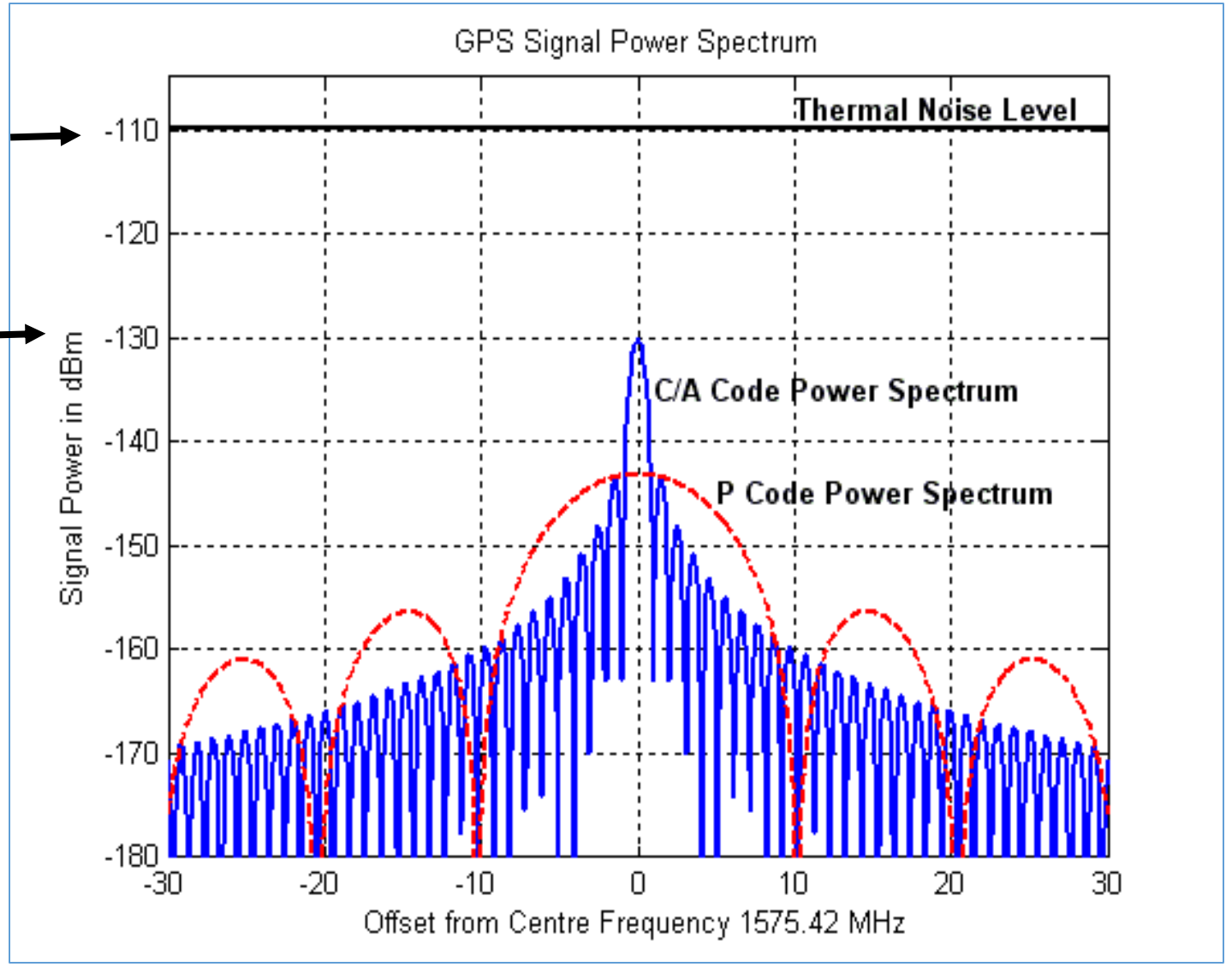


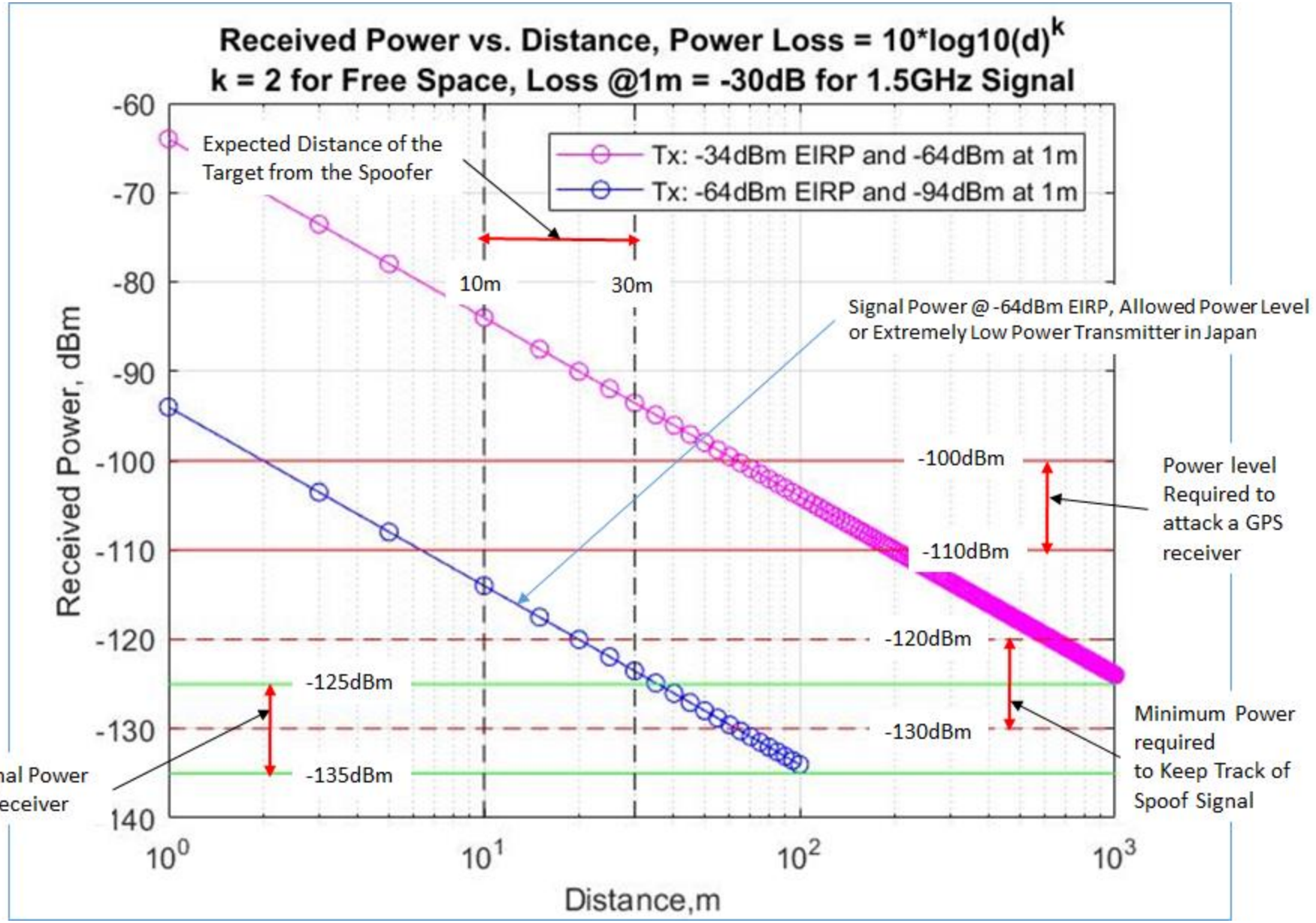
GPS Signal Power

Noise Power
Any Signal below this noise level can't be measured in a Spectrum Analyzer

GPS Signal Power at Antenna
-130dBm

Mobile phone, WiFi, BT etc have power level above -110dBm, much higher than GPS Signal Power



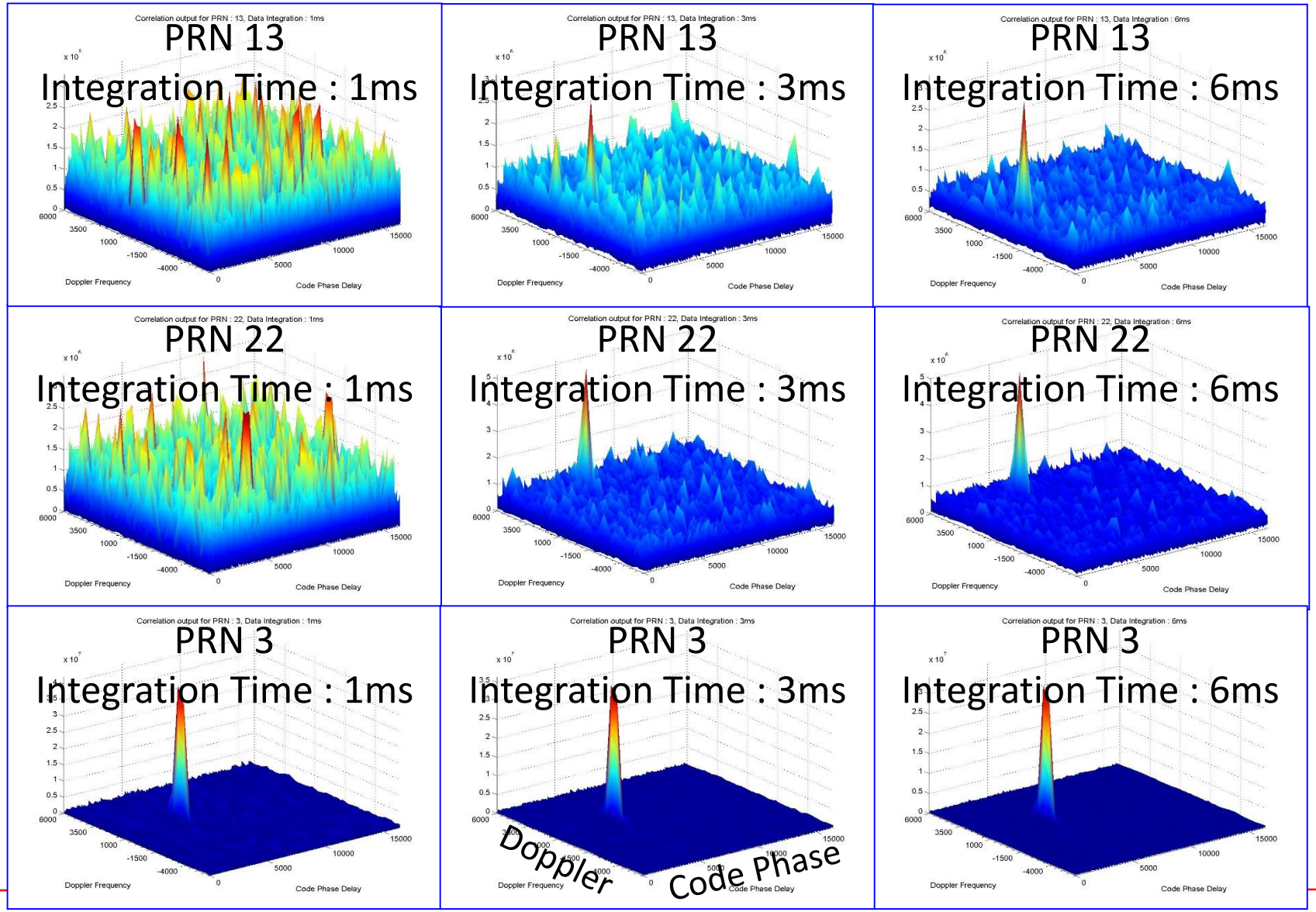

Received Power vs. Distance, Power Loss = 10*log10(d)^k
k = 2 for Free Space, Loss @1m = -30dB for 1.5GHz Signal
Expected Distance of the Target from the Spoofer
Tx: -34dBm EIRP and -64dBm at 1m
Tx: -64dBm EIRP and -94dBm at 1m
10m
30m
Signal Power @ -64dBm EIRP, Allowed Power Level or Extremely Low Power Transmitter in Japan
-100dBm
-110dBm
Power level Required to attack a GPS receiver
-120dBm
-125dBm
-130dBm
-135dBm
GPS Signal Power at the Receiver
Minimum Power required to Keep Track of Spoof Signal
Received Power, dBm
Distance,m
-60
-70
-80
-90
-100
-110
-120
-130
140
10^0
10^1
10^2
10^3

Impact on Signal Processing due to Noise or Interference Signal

Presence of high level noise
This requires longer integration of data
More processing power

Presence of noise

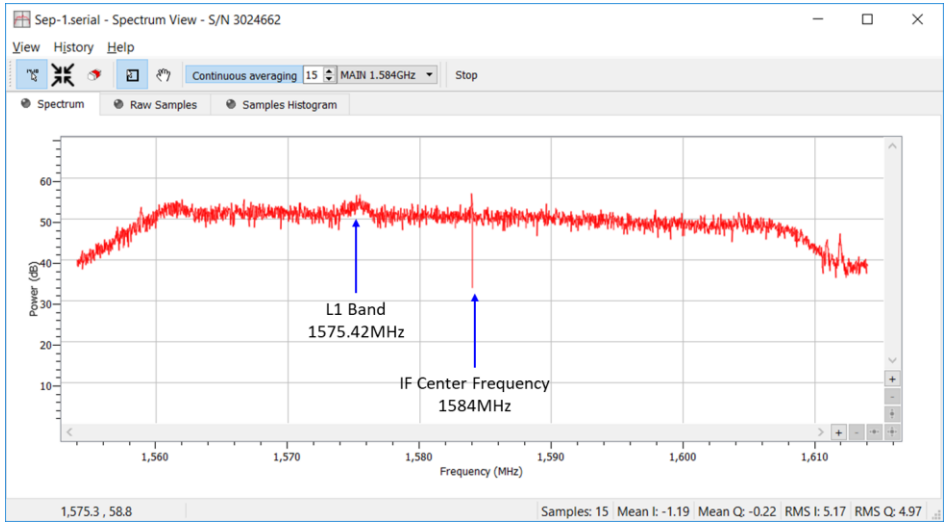
Very small noise

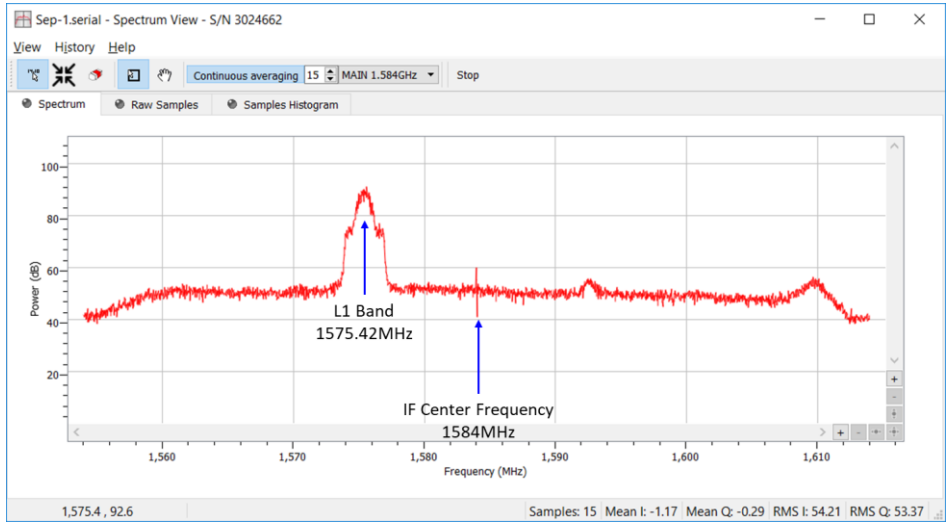


GNSS Signal Quality

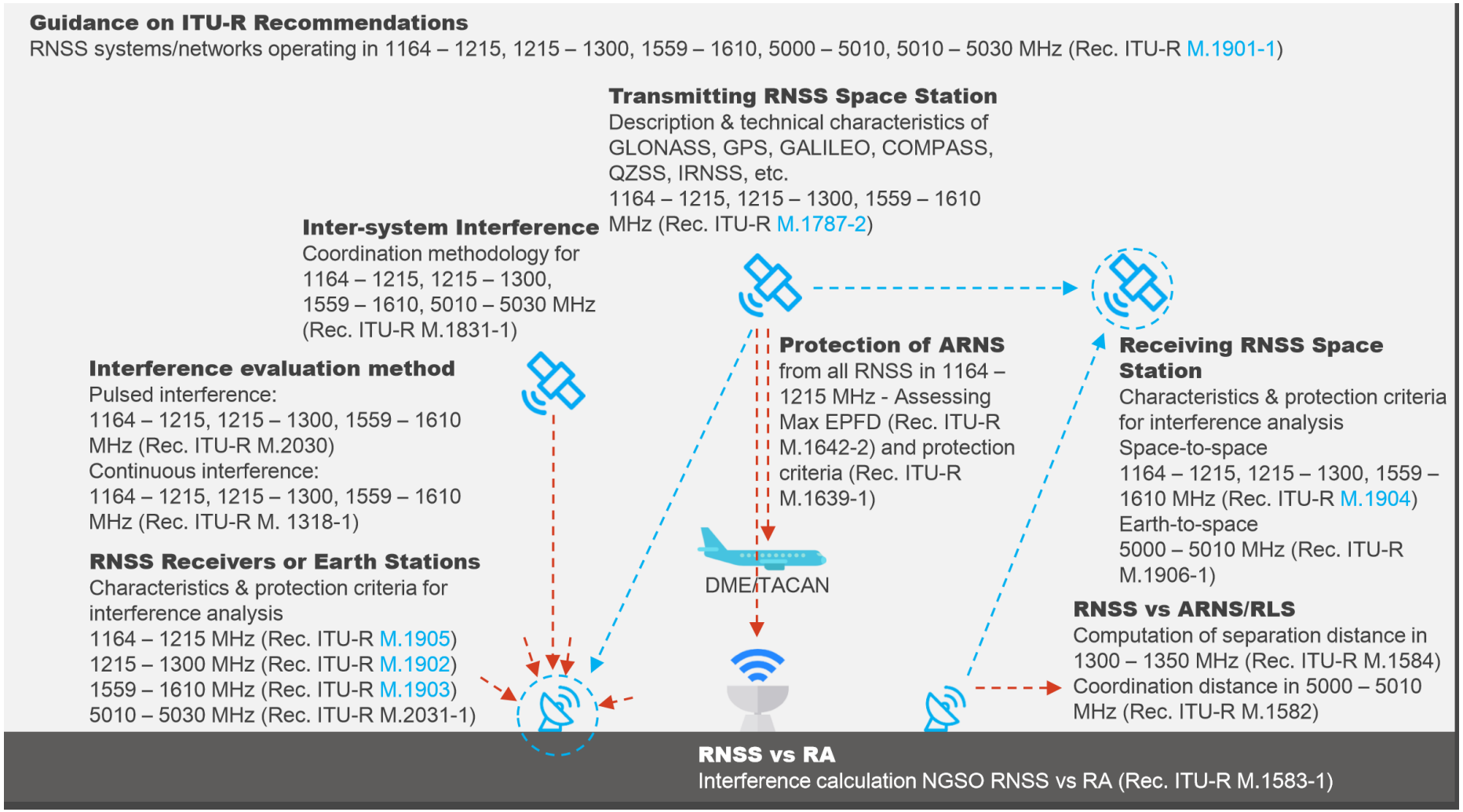
Normal GNSS Signal

GNSS Signal with Interference



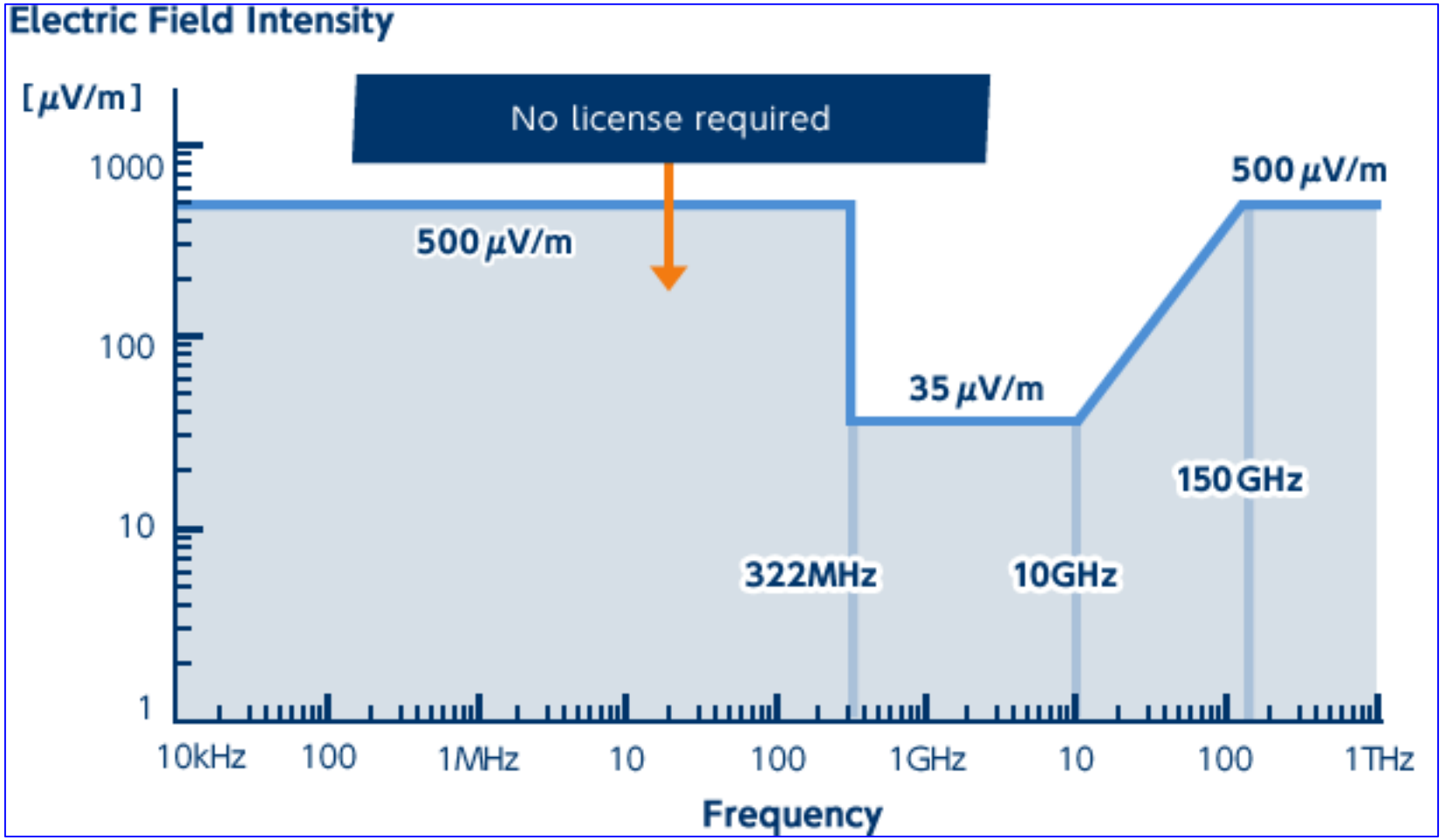


ITU RNSS Documents



Please refer ITU documents for details on regulations related with GNSS signals

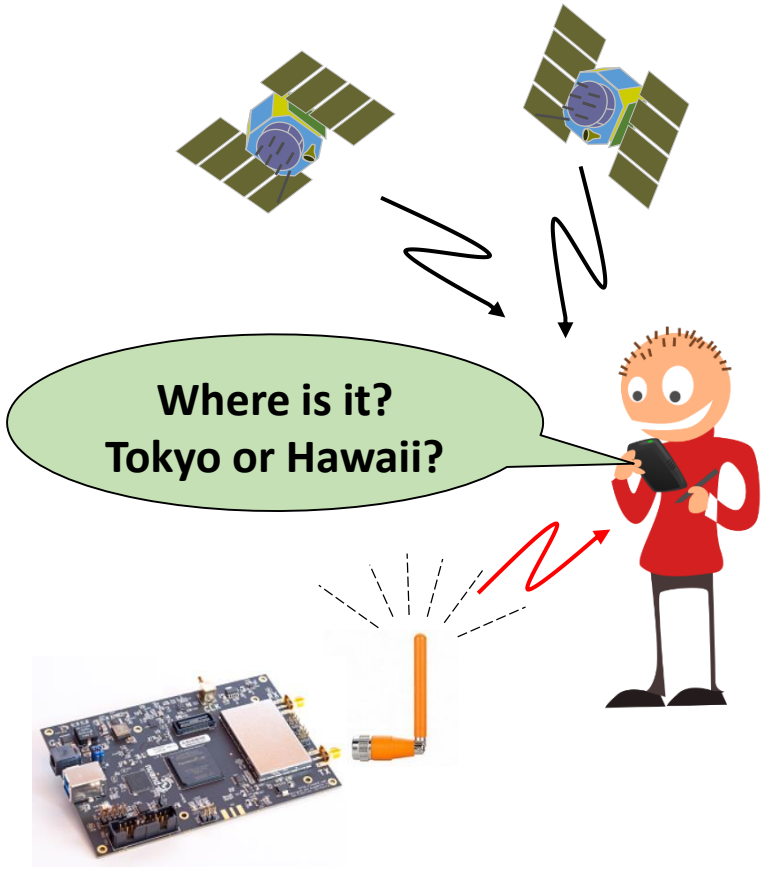
Maximum Field Intensity at 3m Distance from Antenna for Operation of License Free Weak Signals in Japan



Maximum Field Intensity of RF signal at 3m for License Free operation in Japan
For GPS , it is 35micro-volt/m at 3m from antenna. This corresponds to about -64dBm EIRP at antenna

What is Spoofing?

- **Falsify Location Data as If it were True Location**



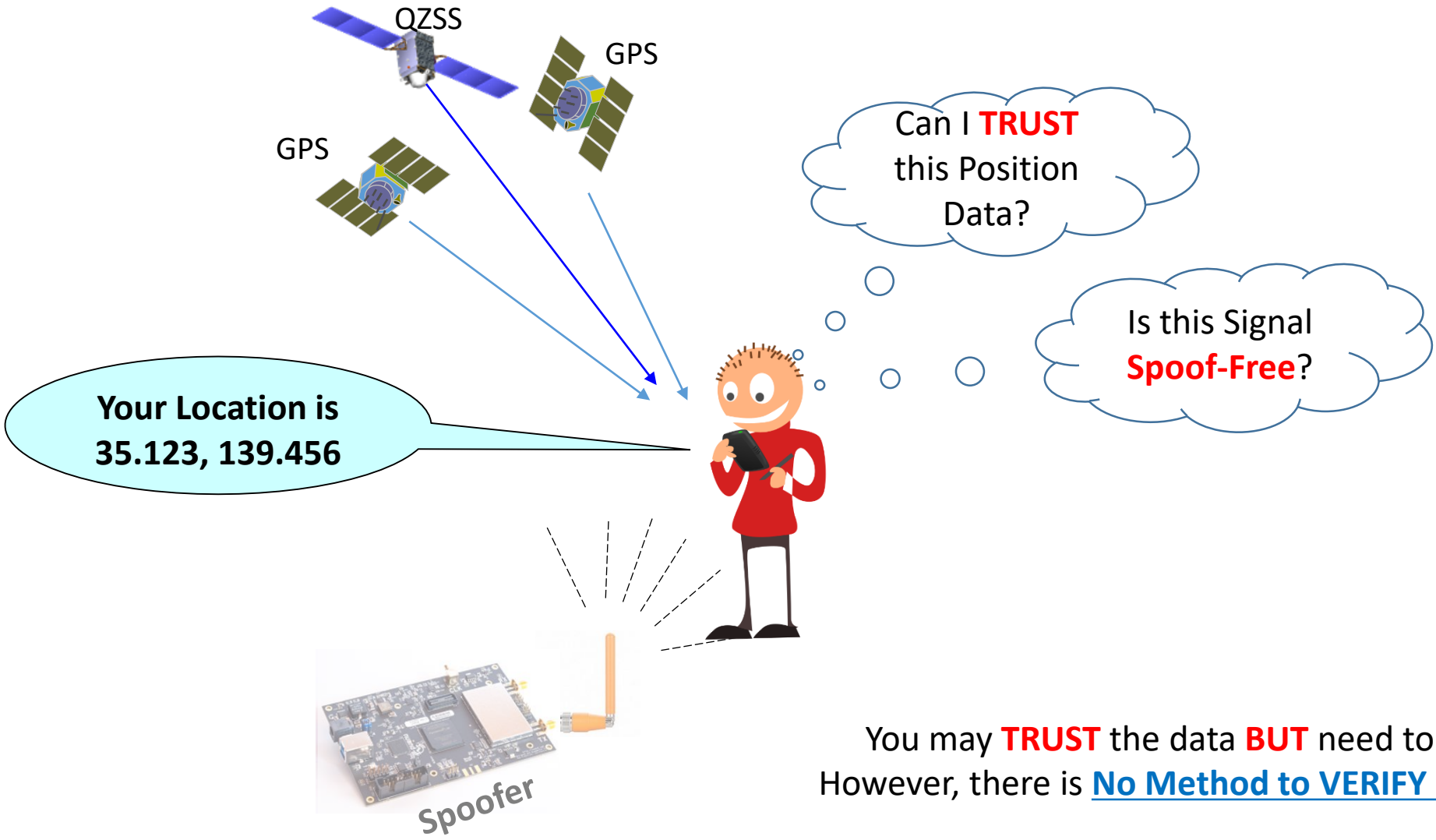
Spoofer

TOKYO Or Hawaii?

Watch James Bond's Movie: **"Tomorrow Never Dies"** to understand How a GPS receiver can be spoofed.

This movie is all about GPS Spoofing

Current Situation with Position Data from GNSS

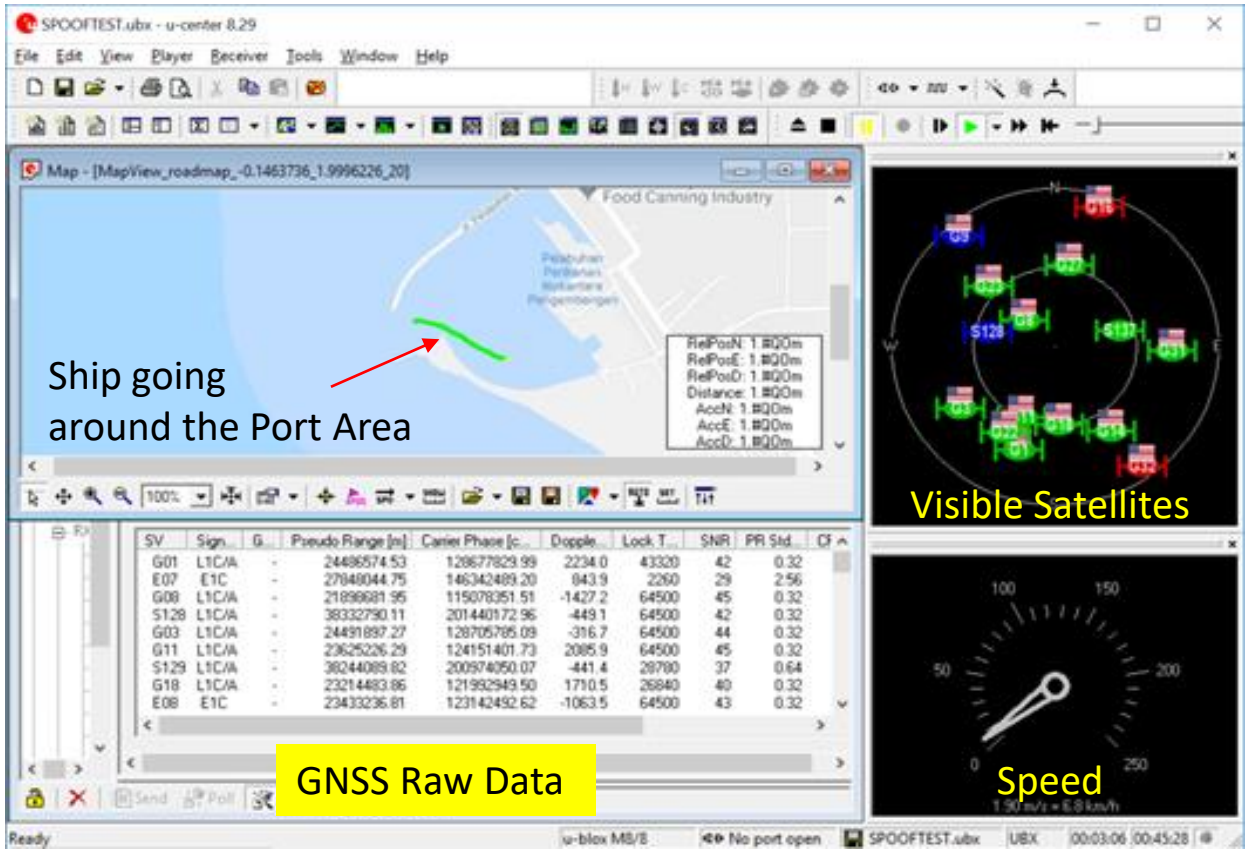


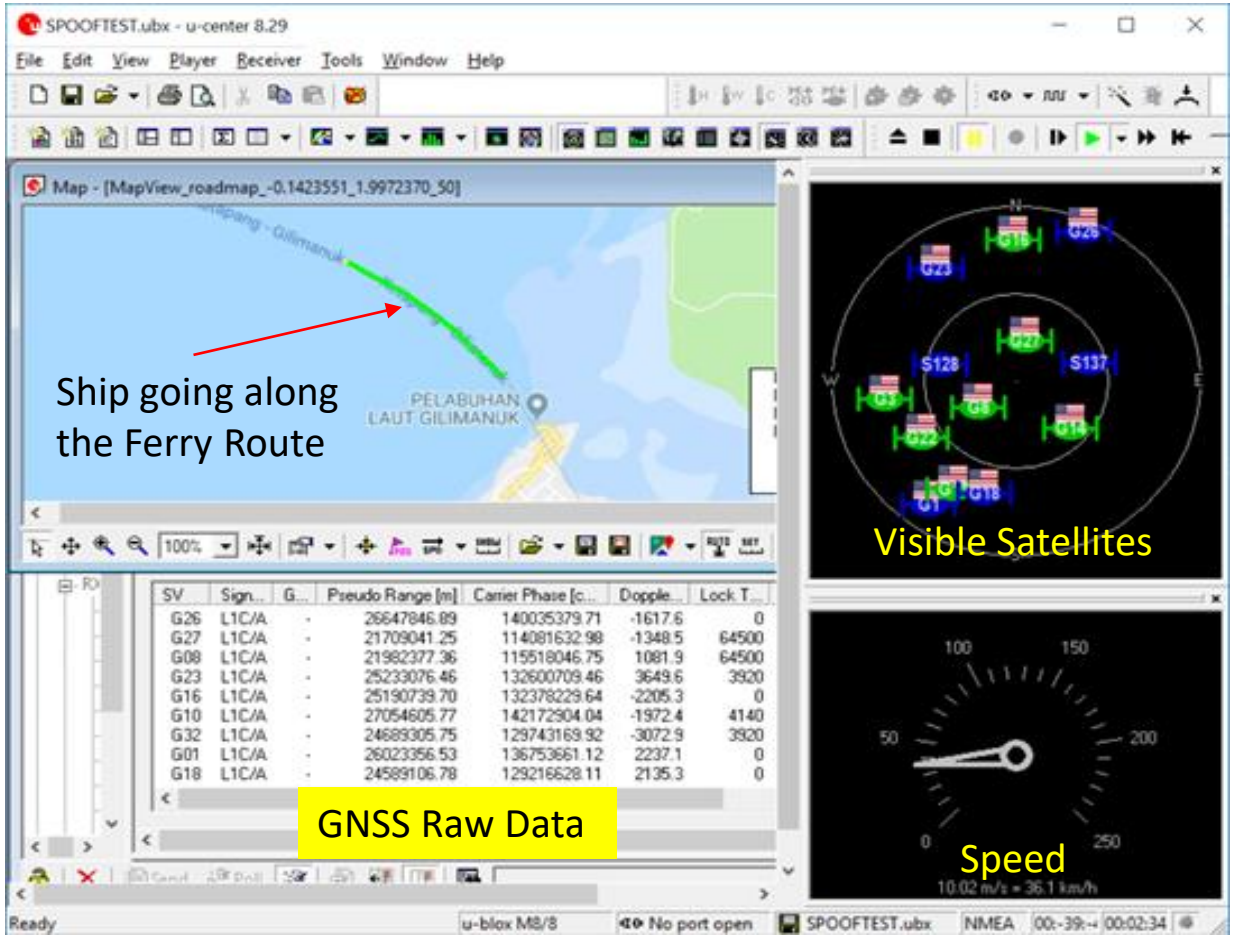
You may **TRUST** the data **BUT** need to **VERIFY**
However, there is **No Method to VERIFY GPS Signal**

SPOOFing a Car: Is he driving the car?

Output of GNSS Receiver, True Data and Spoof Data

Quiz: Can you identify TRUE Data and SPOOF Data?





Contact and Additional Information

- **Homepage**
  - **Main Page** : https://home.csis.u-tokyo.ac.jp/~dinesh/
  - **Webinar Page** : https://home.csis.u-tokyo.ac.jp/~dinesh/WEBINAR.htm
    https://gnss.peatix.com/
  - **Training Data Etc** : https://home.csis.u-tokyo.ac.jp/~dinesh/GNSS_Train.htm
  - **Low-Cost Receiver** : https://home.csis.u-tokyo.ac.jp/~dinesh/LCHAR.htm
  - **Facebook** : https://www.facebook.com/gnss.lab/
- **Contact**
  - **E-mail** : dinesh@csis.u-tokyo.ac.jp
  - **Skype** : **mobilemap**