

# GNSS Security Issues

## Jamming, Interference and Spoofing

**Dinesh MANANDHAR**  
**Center for Spatial Information Science**  
**The University of Tokyo**  
[dinesh@iis.u-tokyo.ac.jp](mailto:dinesh@iis.u-tokyo.ac.jp)

**28<sup>th</sup> JAN 2021**

# GPS Security Issues

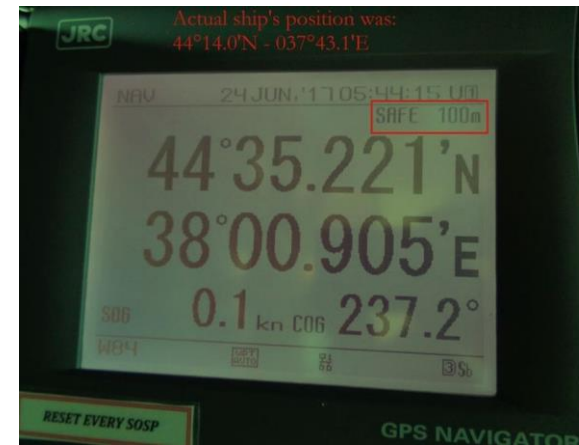
## • Jamming and Interference

- 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>



Vessel Position in Black Sea  
Is this Spoofing?



### JAMMING CELL PHONES AND GPS EQUIPMENT IS AGAINST THE LAW!

In recent years, the number of websites offering "cell jammers" or similar devices designed to block communications and create a "quiet zone" in vehicles, schools, theaters, restaurants, and other places has increased substantially. While these devices are marketed under different names, such as signal blockers, GPS jammers, or text stoppers, they have the same purpose. We remind and warn consumers that it is a violation of federal law to use a cell jammer or similar devices that intentionally block, jam, or interfere with authorized radio communications such as cell phones, police radar, GPS, and Wi-Fi. Despite some marketers' claims, consumers cannot legally use jammers within the United States, nor can retailers lawfully sell them.

**Why are jammers prohibited?** Use of jamming devices can place you or other people in danger. For instance, jammers can prevent 9-1-1 and other emergency calls from getting through or interfere with law enforcement communications (ambulance, fire, police, etc). In order to protect the public and ensure access to emergency and other communications services, without interference, the FCC strictly prohibits the use, marketing, manufacture, and sale of jammers.

**What happens if you use a jammer?** Operation of a jammer in the United States is illegal and may subject you to substantial monetary penalties, seizure of the unlawful equipment, and criminal sanctions including imprisonment.

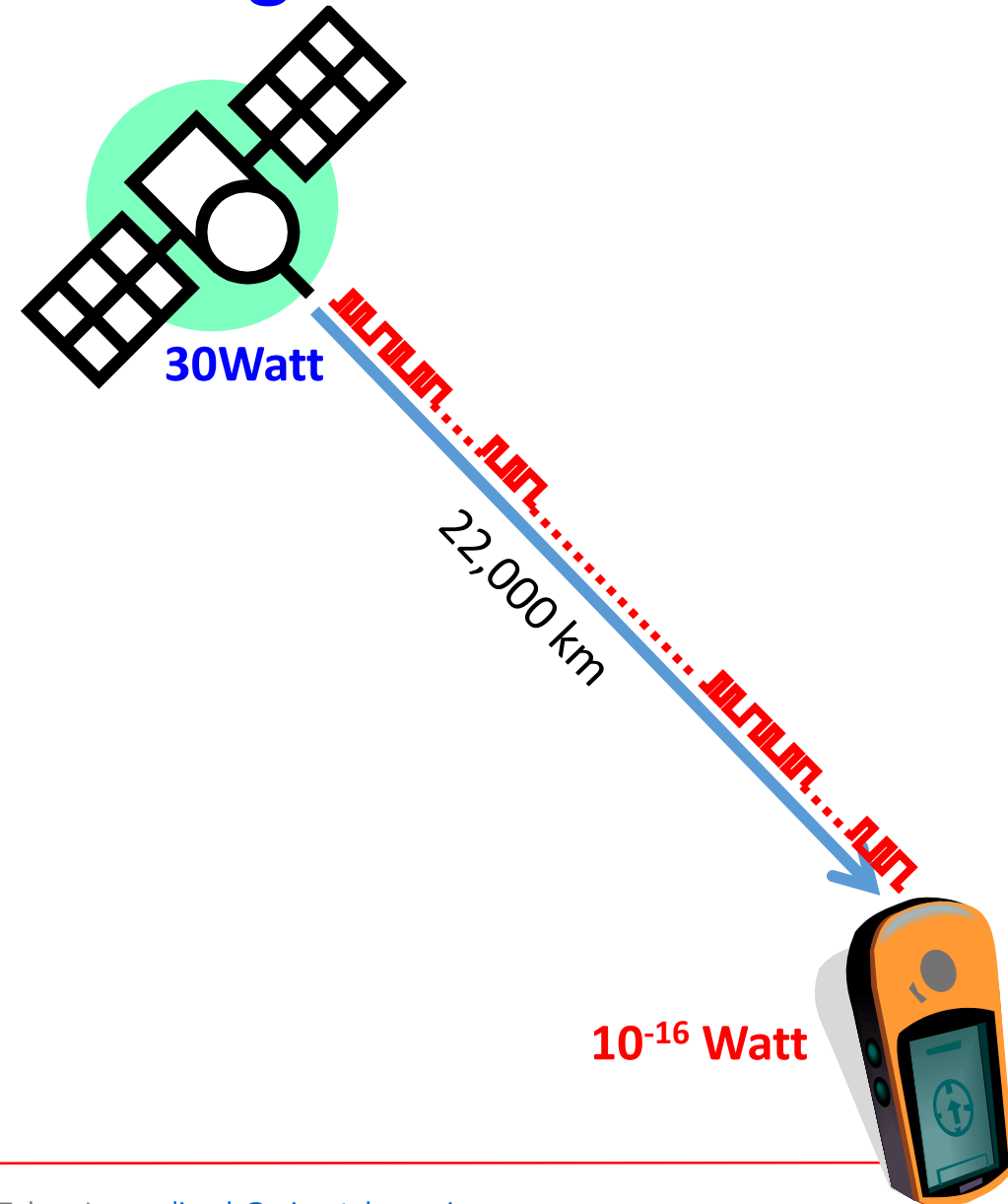
**Want to file a complaint or need more information?** To file a complaint alerting the FCC's Enforcement Bureau to illegal cell, GPS, or other jamming devices, please visit [www.fcc.gov/complaints](http://www.fcc.gov/complaints) or call 1-888-CALL-FCC. Additional information about jammer enforcement is available at [www.fcc.gov/eb/jammerenforcement](http://www.fcc.gov/eb/jammerenforcement) or by emailing the Enforcement Bureau at [jammerinfo@fcc.gov](mailto:jammerinfo@fcc.gov).

Issued by the Enforcement Bureau of the Federal Communications Commission

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  $1/(\text{distance})^2$
  - 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

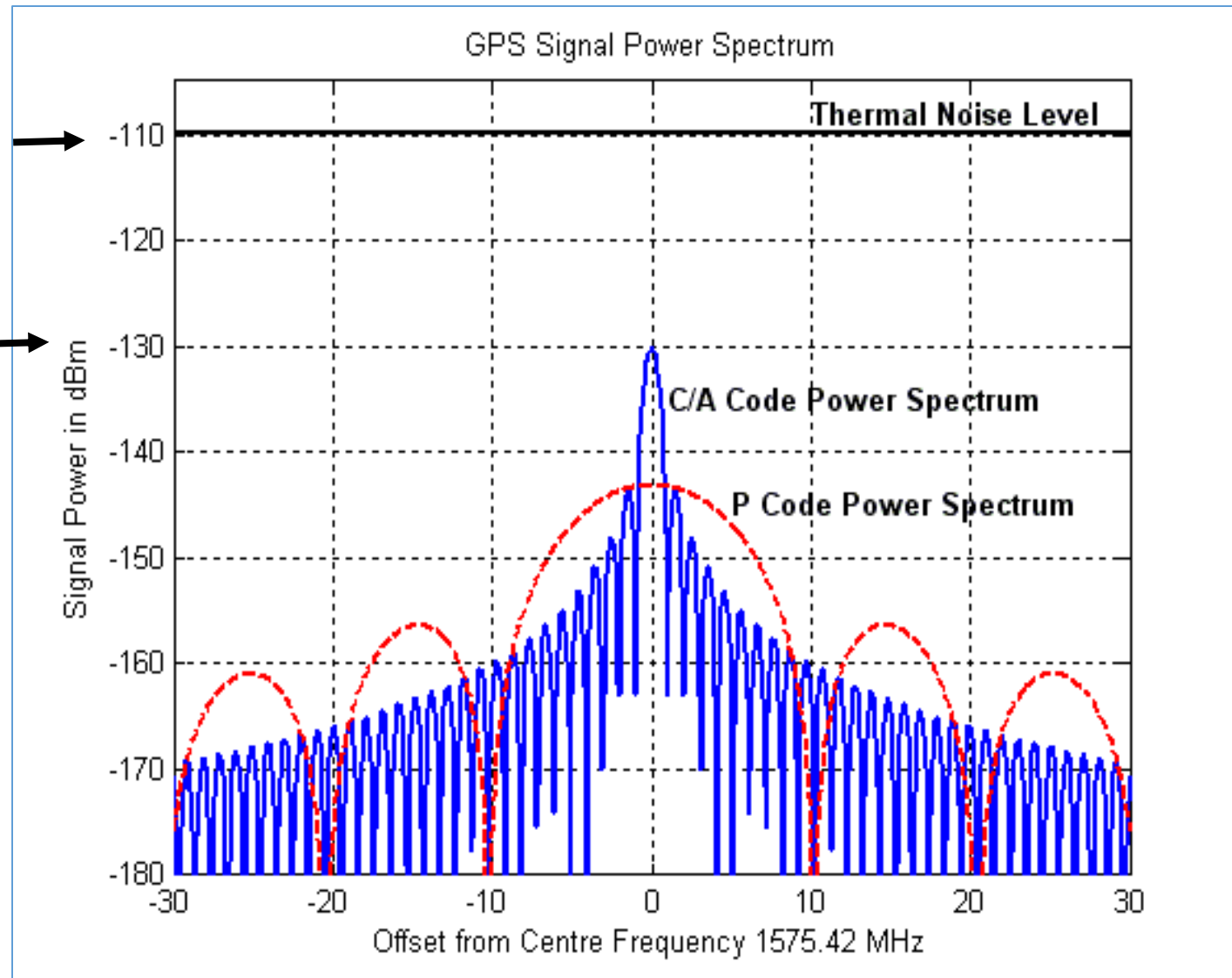


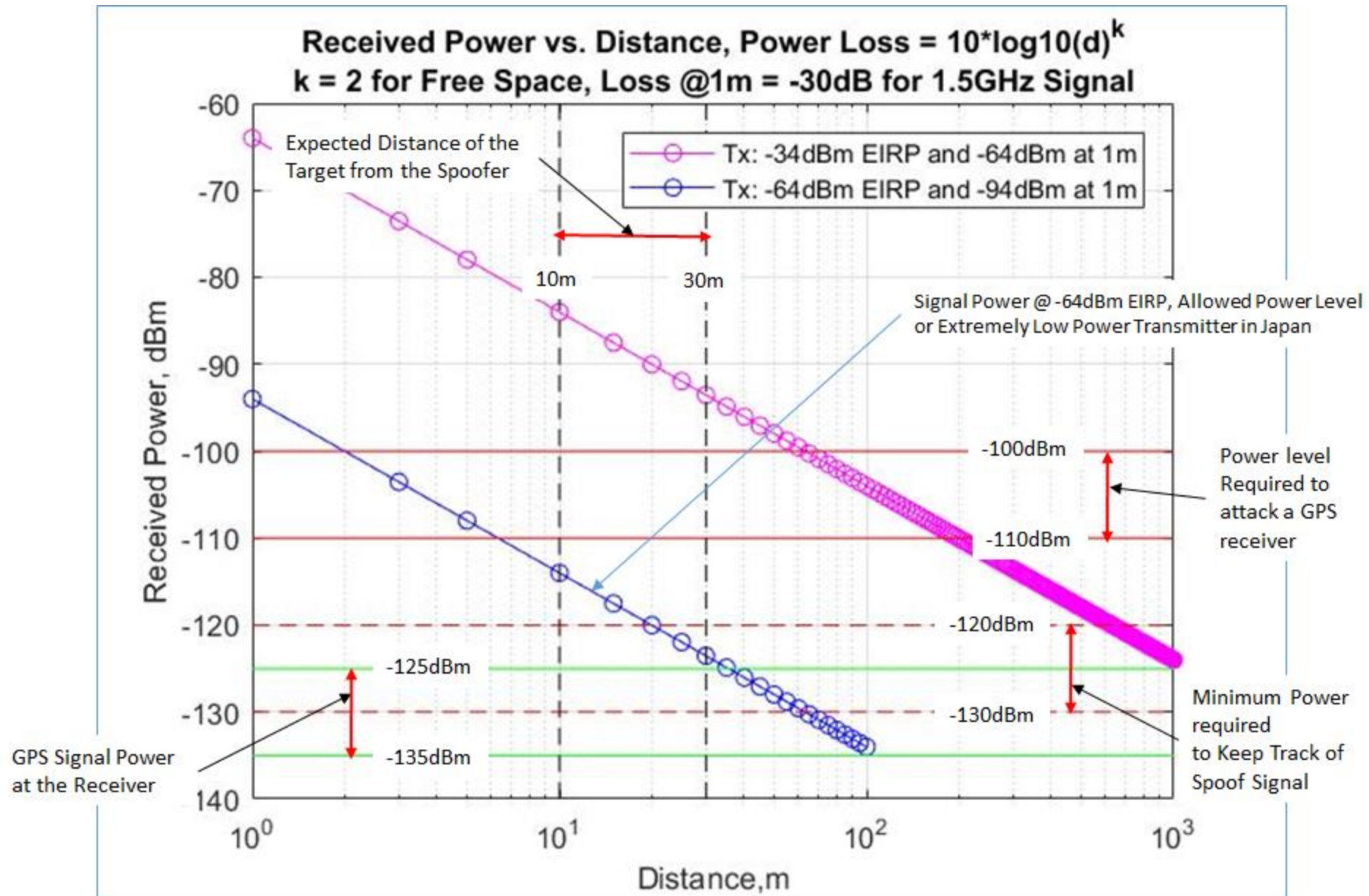
# GPS Signal Power

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

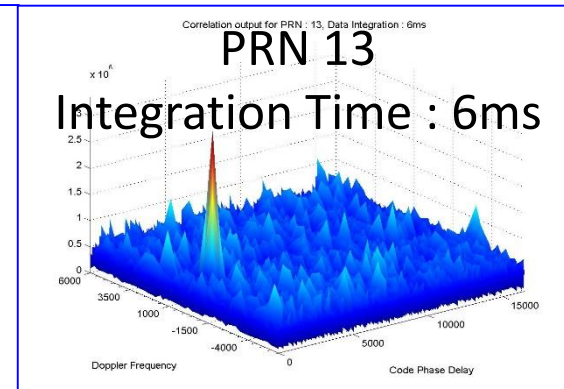
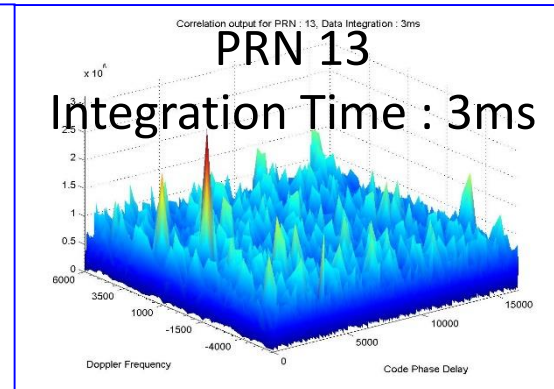
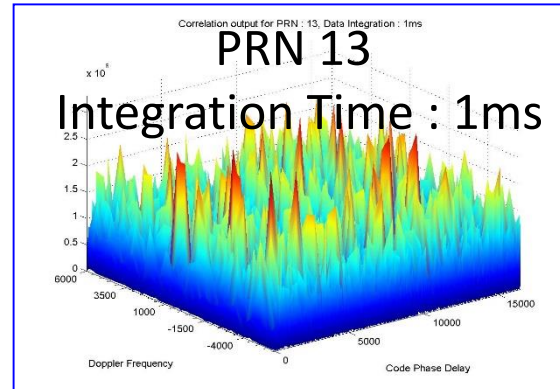




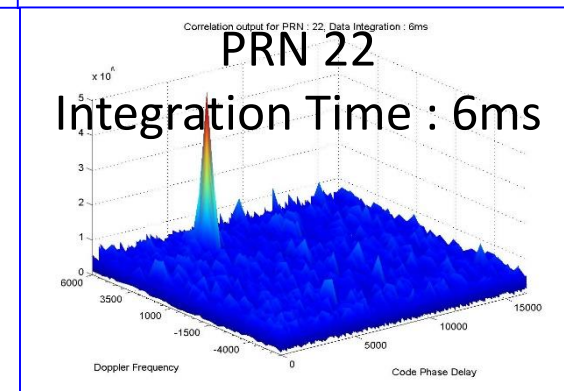
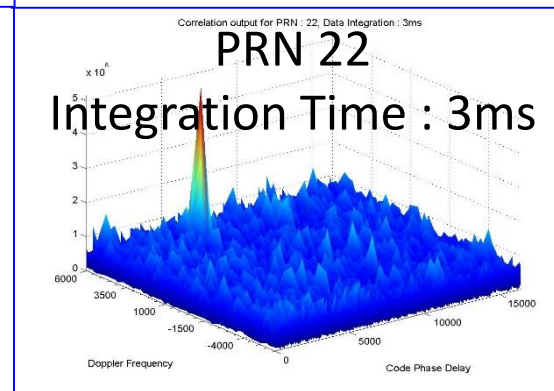
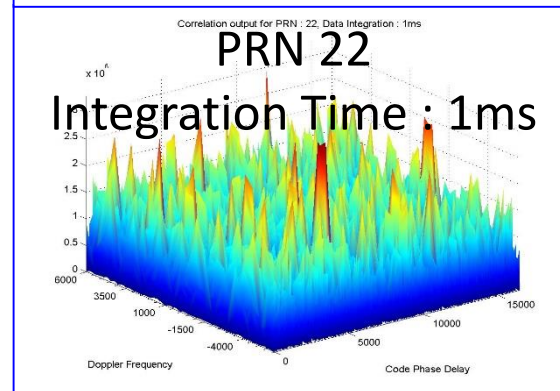


# Impact on Signal Processing due to Noise or Interference Signal

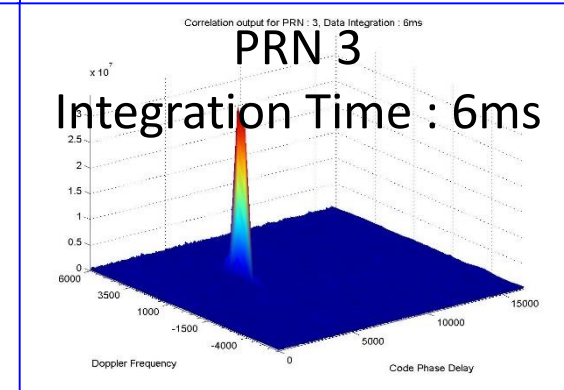
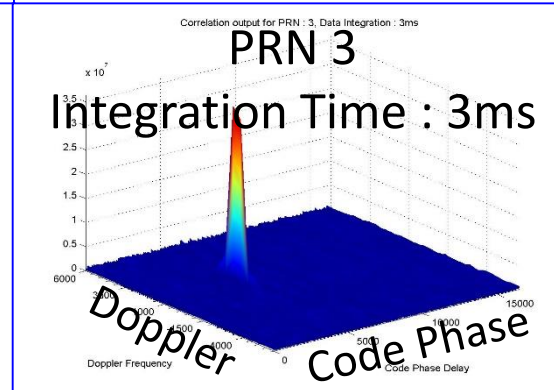
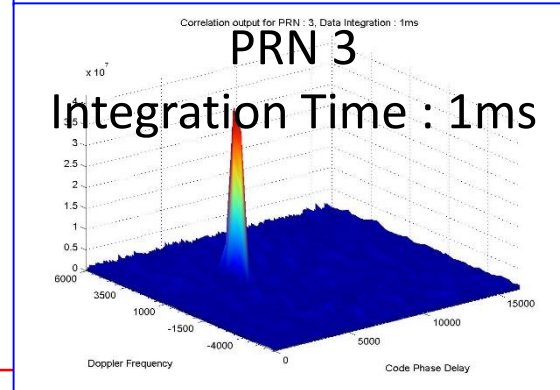
Presence of high level noise  
This requires longer  
integration of data  
More processing power



Presence of noise



Very small noise

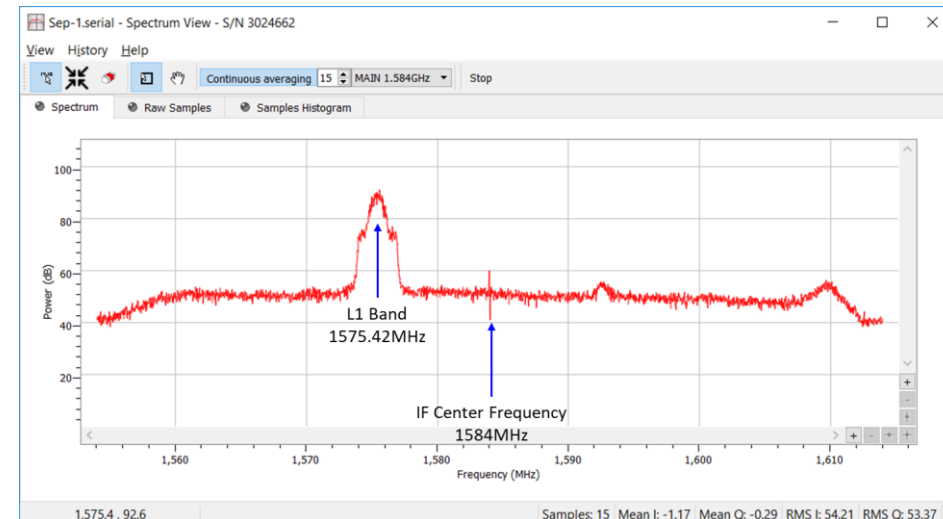
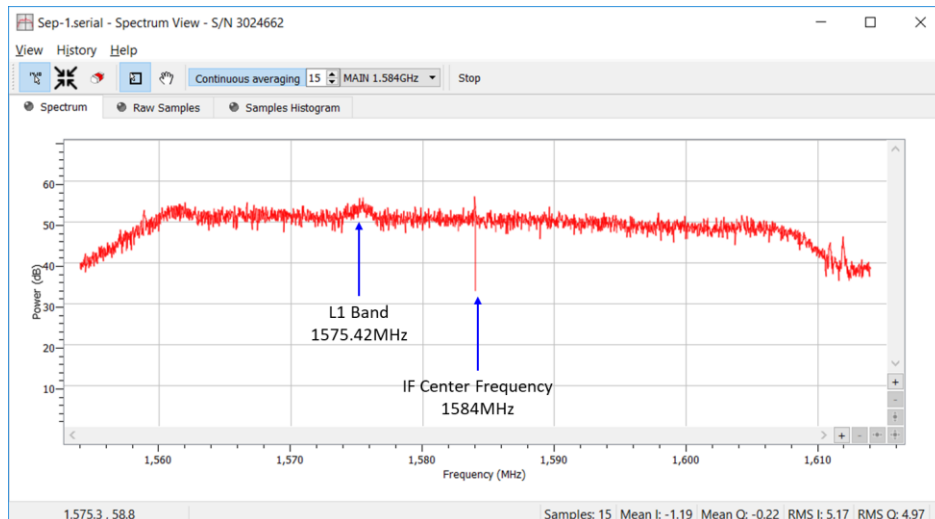


# GNSS Signal Quality

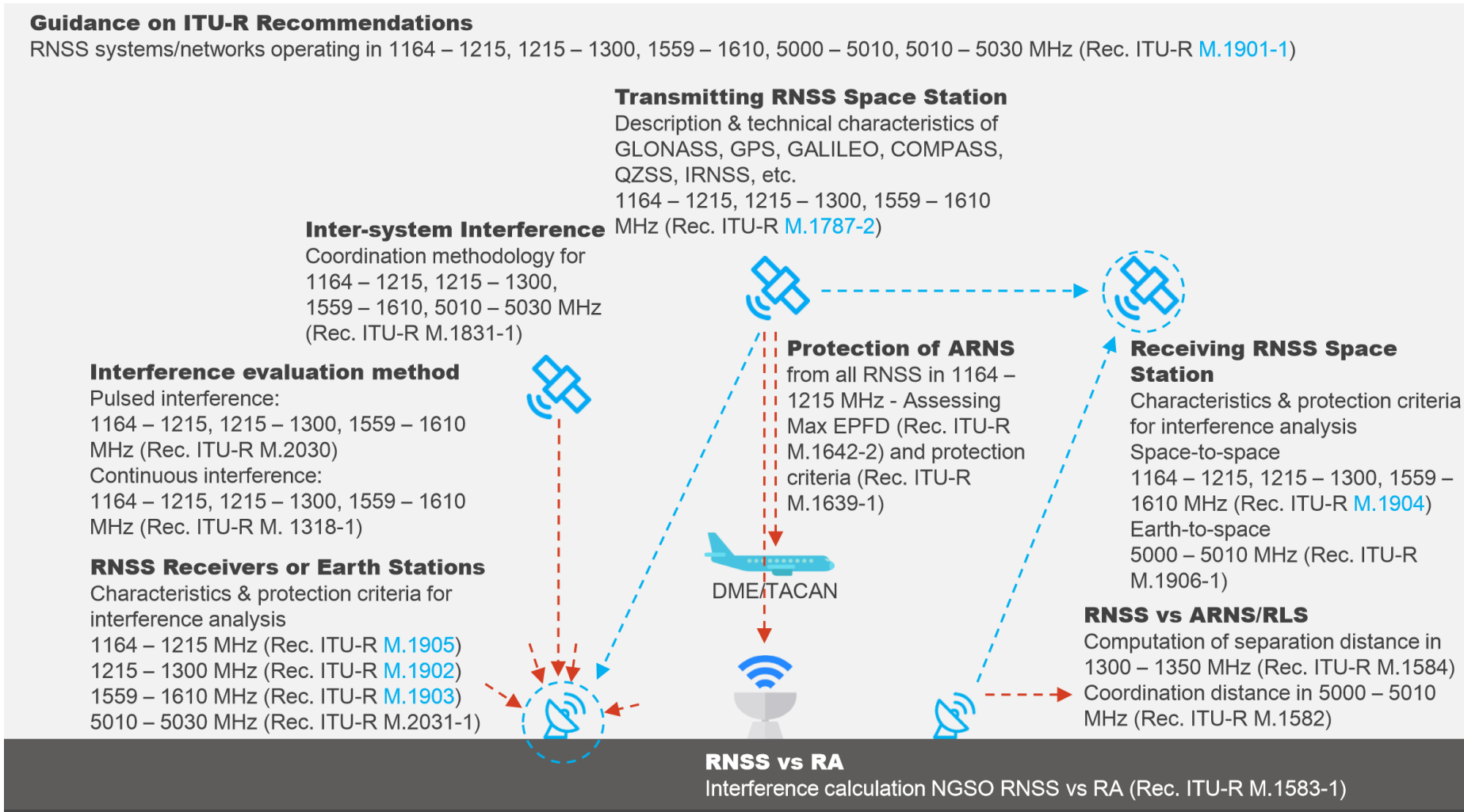
## Normal GNSS Signal



## GNSS Signal with Interference



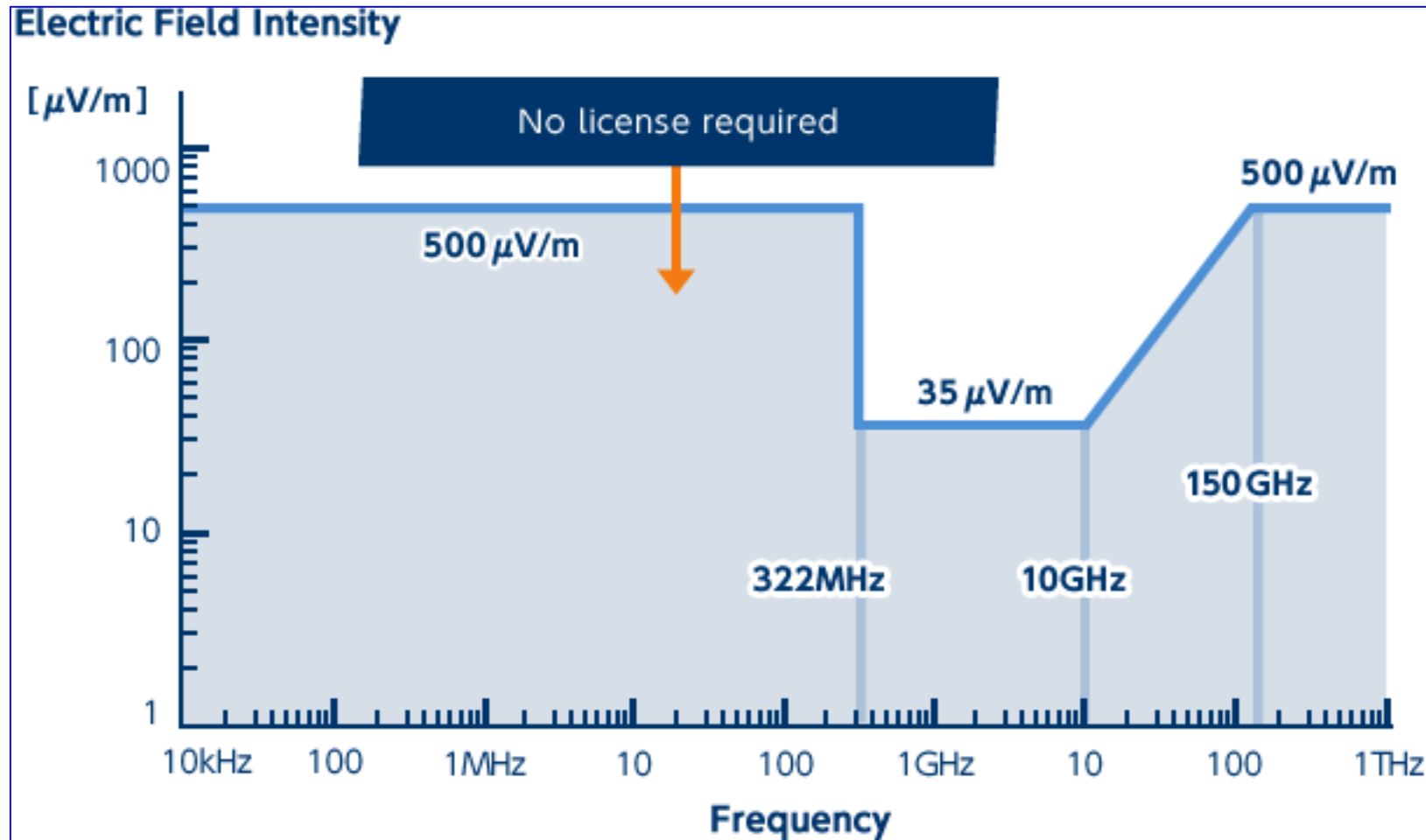
# ITU RNSS Documents



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

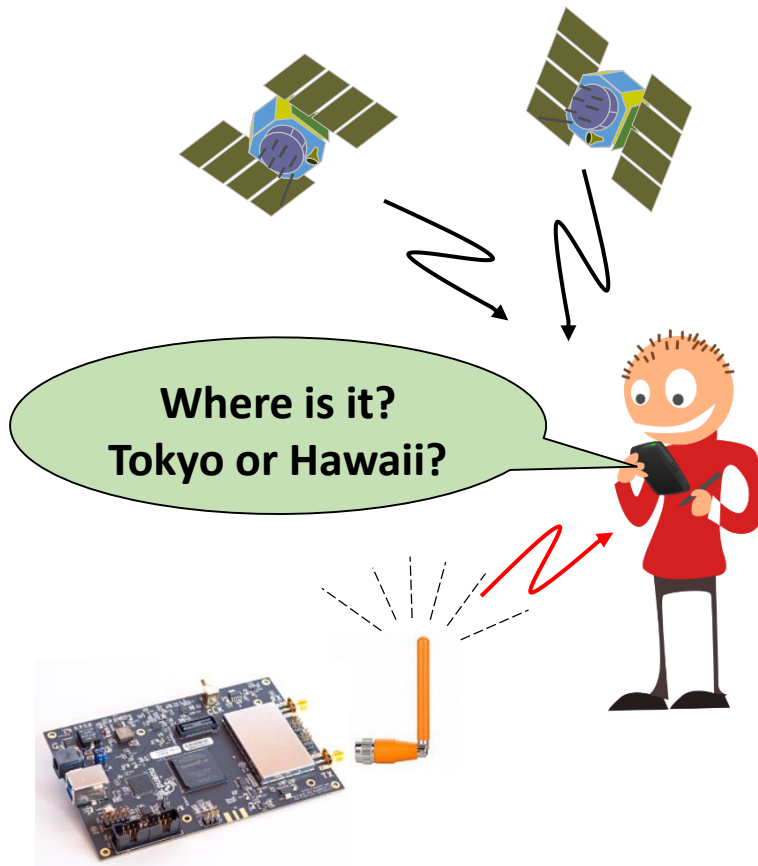


Maximum Field Intensity of RF signal at 3m for License Free operation in Japan

For GPS , it is 35micro-volt/m at 3m from antenna. This corresponds to about -64dBm EIRP at antenna

# What is Spoofing?

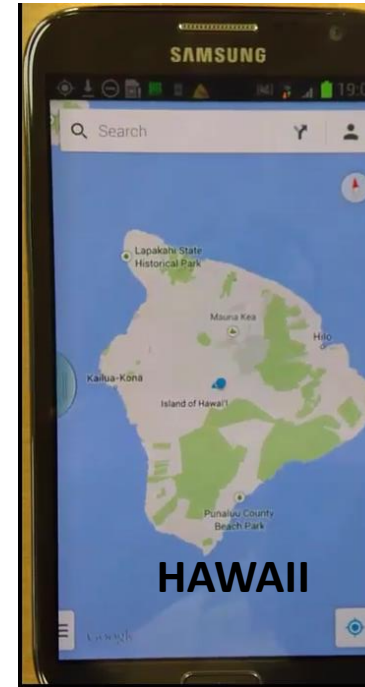
- Falsify Location Data as If it were True Location



Spoofing



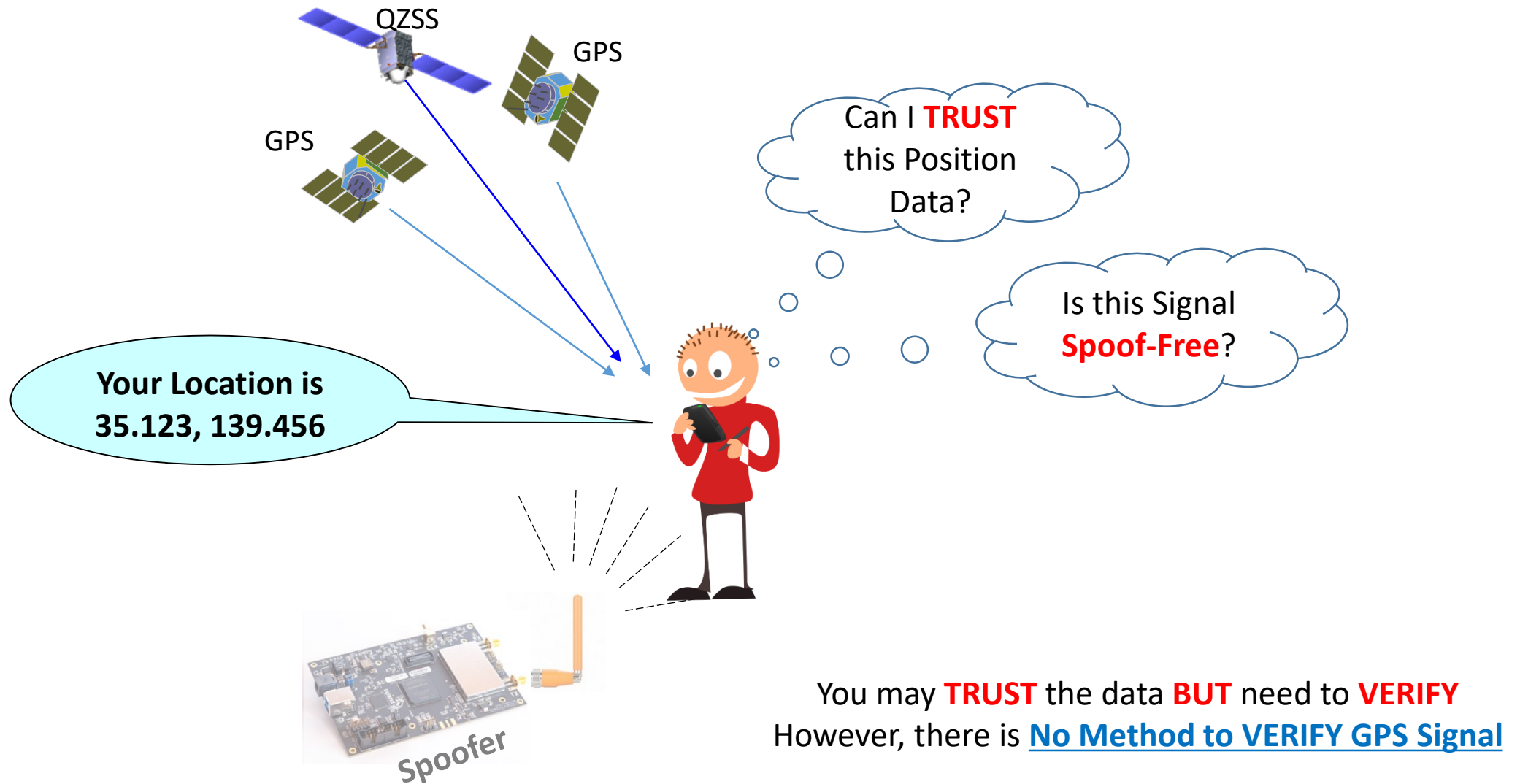
TOKYO  
Or  
Hawaii?



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



# SPOOFing a Car: Is he driving the car?

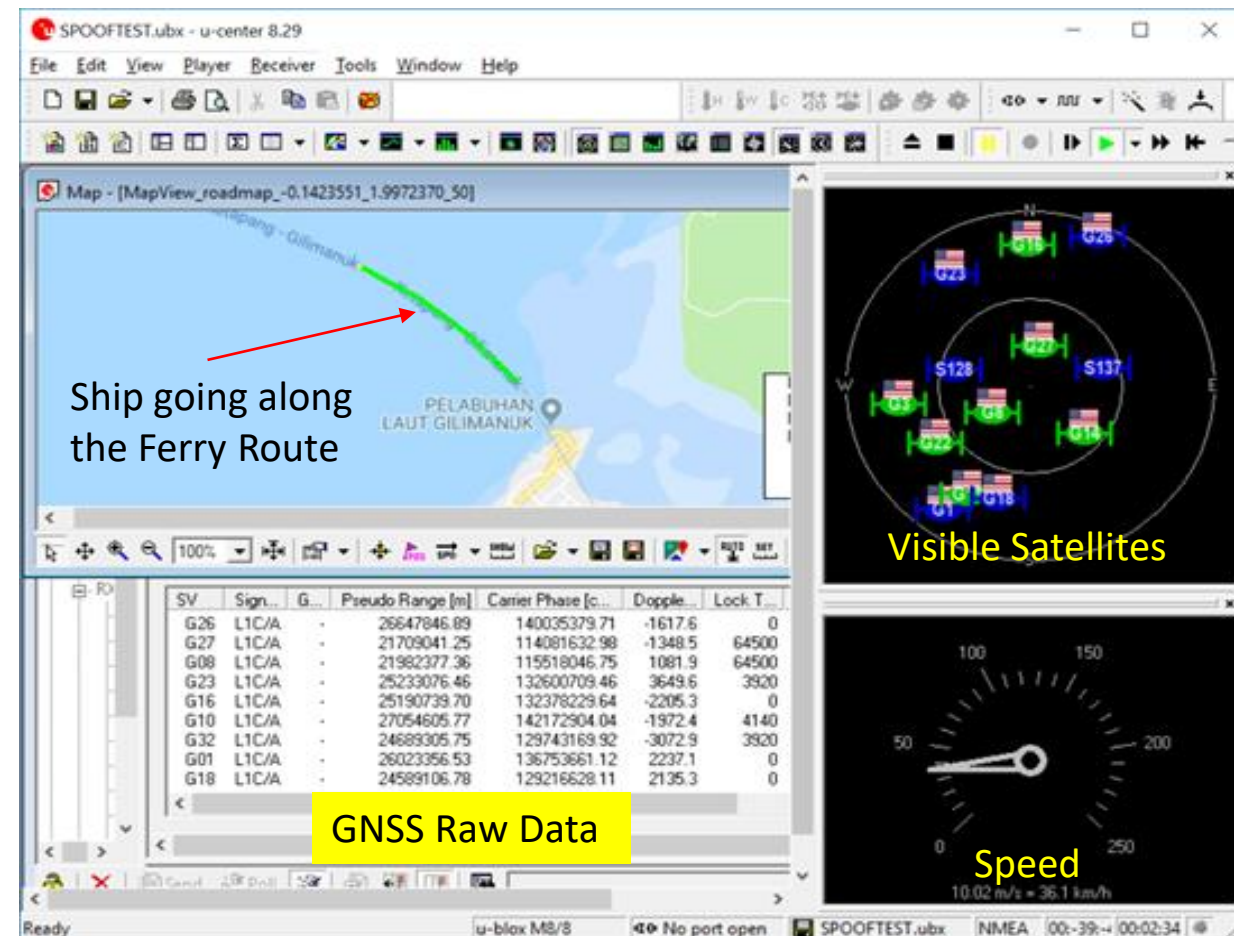
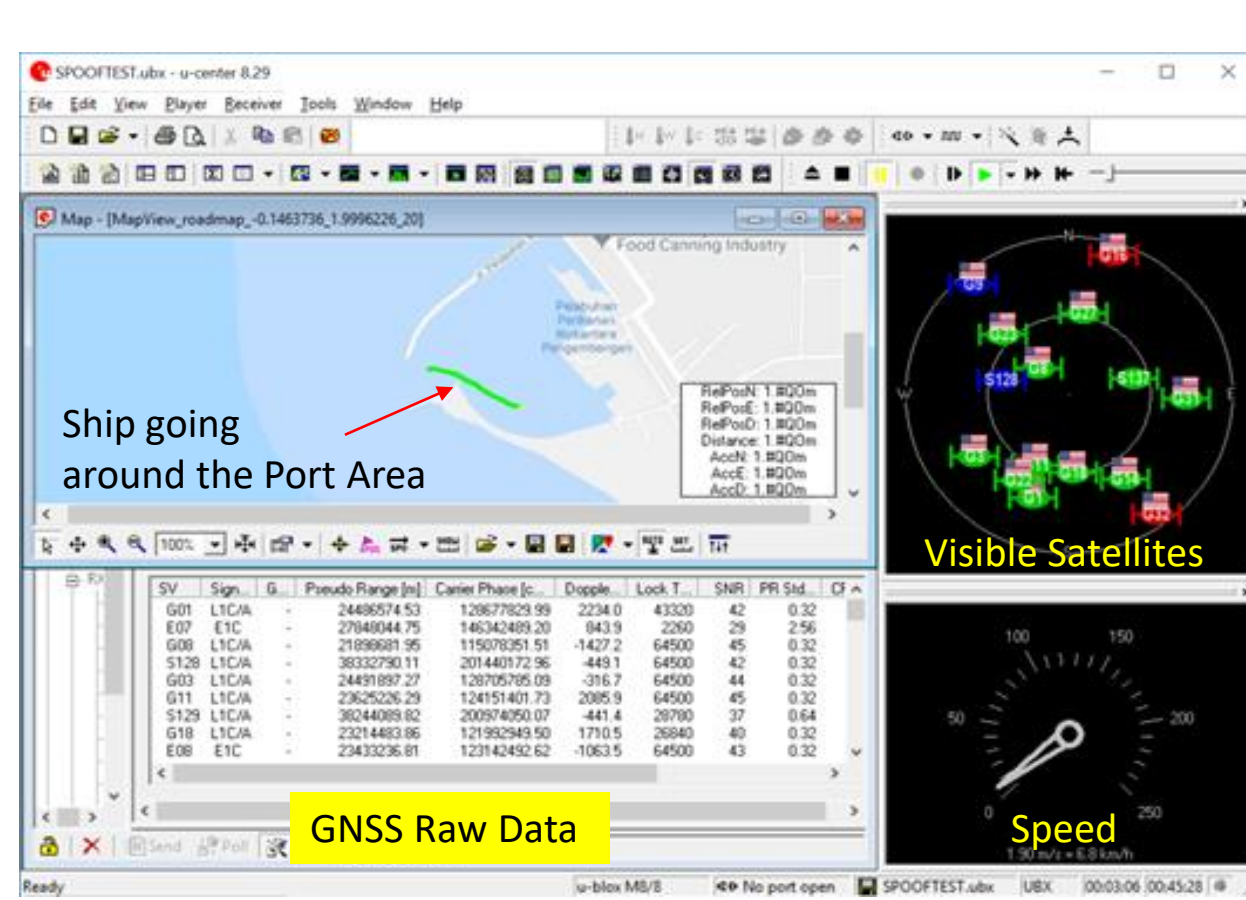
The SPOOF Signal is received by GNSS Receiver.

The Car is Actually in Parking Area.  
But, using SPOOF Signal,  
We show that We are Driving.



# 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](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](mailto:dinesh@csis.u-tokyo.ac.jp)
- **Skype** : mobilemap