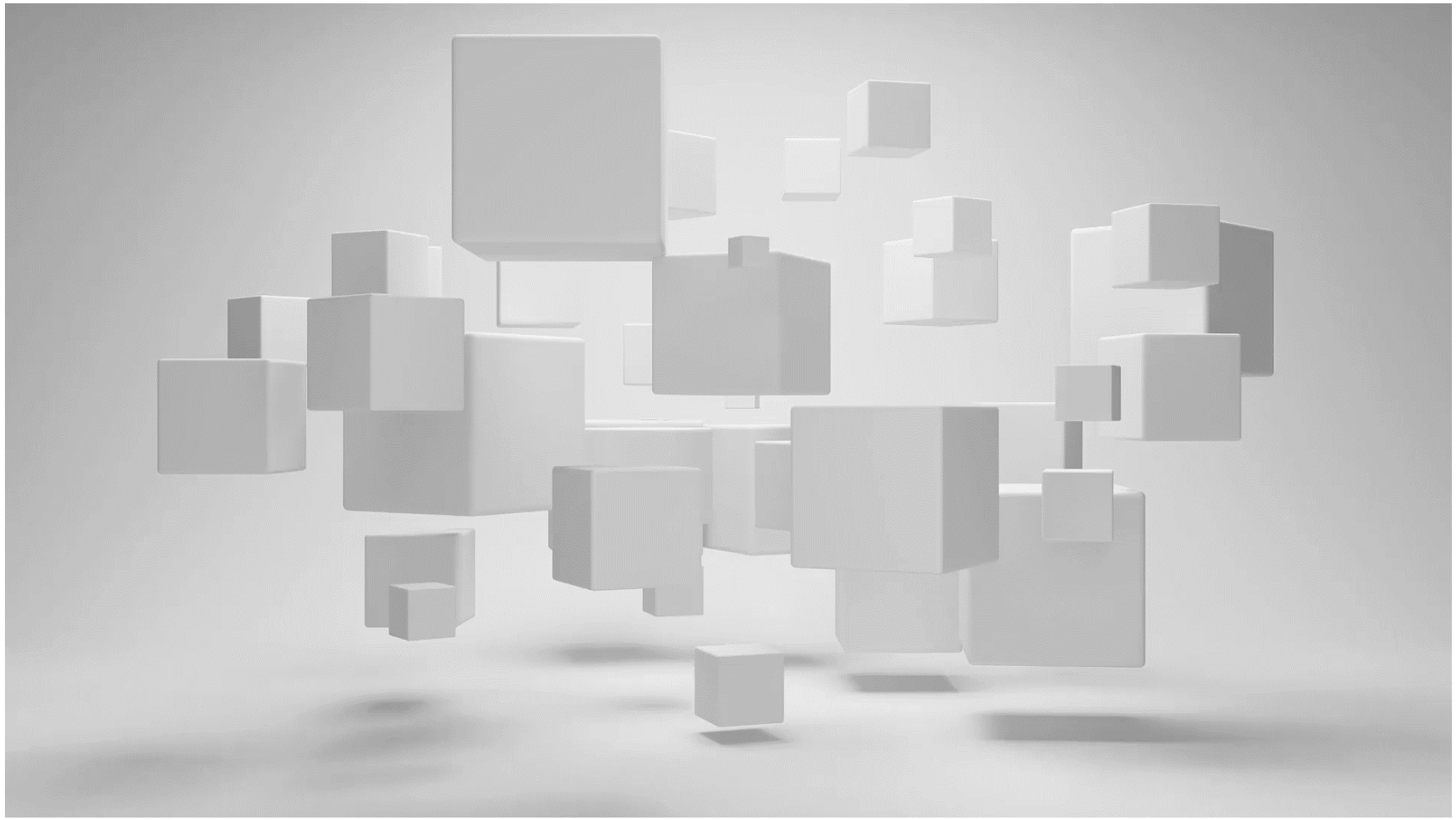
GNSS Signal Spoofing Tests

Dinesh MANANDHAR
Center for Spatial Information Science, The University of Tokyo

United Nations/Finland Workshop on
the Applications of Global Navigation Satellite Systems
23 – 26 October 2023, Helsinki, Finland

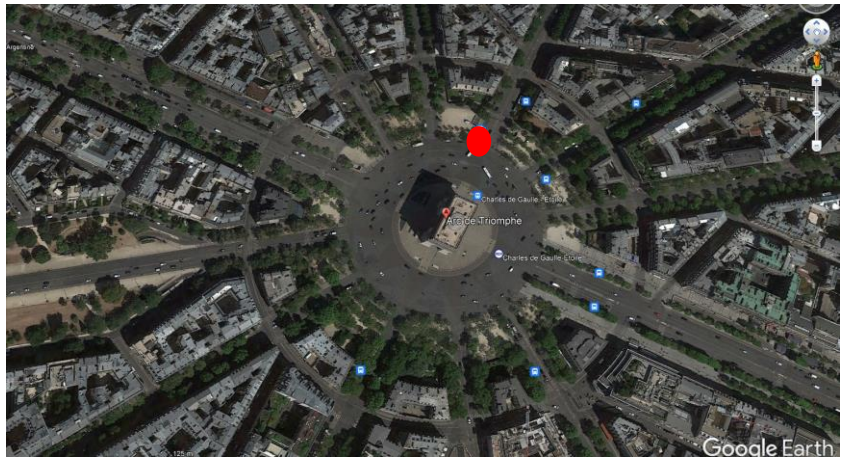
dinesh@csis.u-tokyo.ac.jp
Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

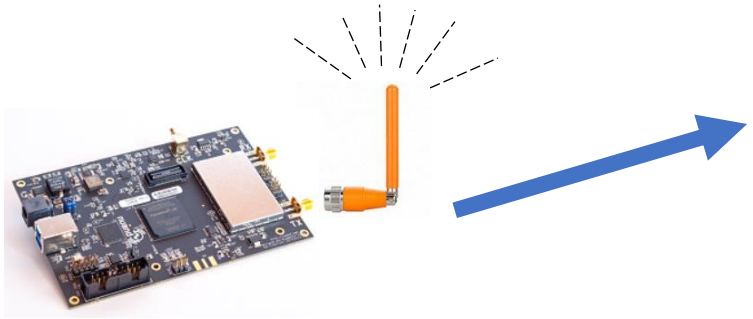
Spoofing a GPS Watch

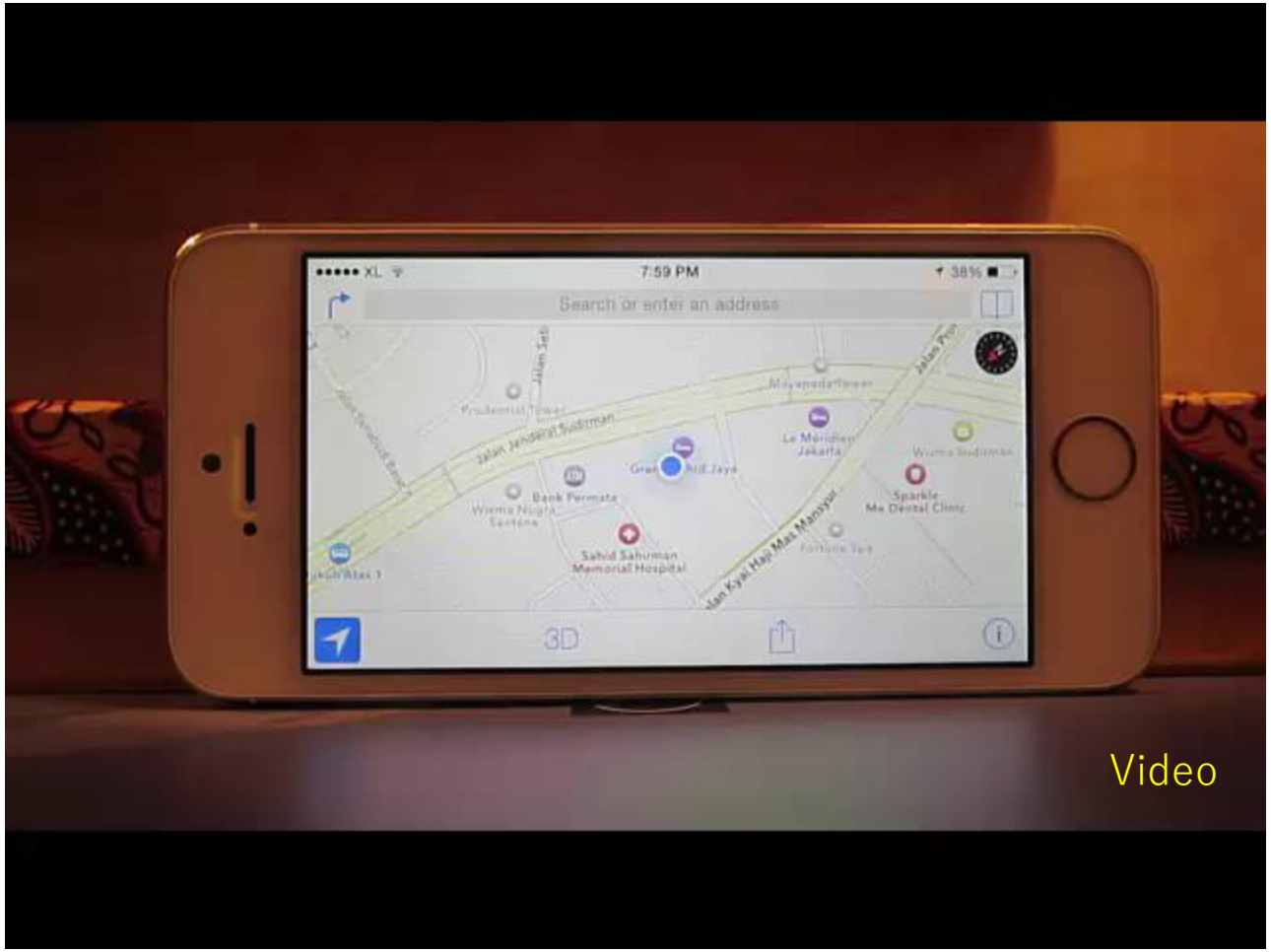


Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Mobile Phone Spoofing (Jakarta or Paris?)







Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Spoofing a Car Navigation System

Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Spoofing Targets, Methods and Types

Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Spoofing Target Device or System

Target Device or System	
Spoofing a GNSS Receiver	A GNSS receiver module or device A system only based on GNSS such as RTK, VRS, HAS, CLAS, MADCOA PPP etc.
Spoofing a system that has a GNSS receiver	A system that uses GNSS for PNT as a primary source of PNT data. Other sensors if present may only work as secondary device or only provide dead-reckoning solutions such INS sensors. Examples: Car navigation system, drone, UAV, UMV, AIS, GPS/IMU
Spoofing a system or an application that uses GNSS and other sensors for PNT solutions	A system or application that uses GNSS or other sensors to output PNT data even if GNSS signal is absent. Examples: Mobile phone, Mimamori Device, Google location engines

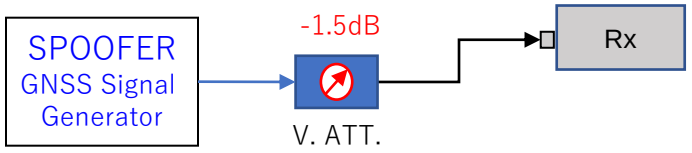
Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Spoofing Methods and Types

Spoofing Methods	
Direct Attack	Connect the target device directly by a cable Spoof signal is not transmitted by antenna
Over-The-Air Attack (OTA)	Transmit spoof signal over-the-air

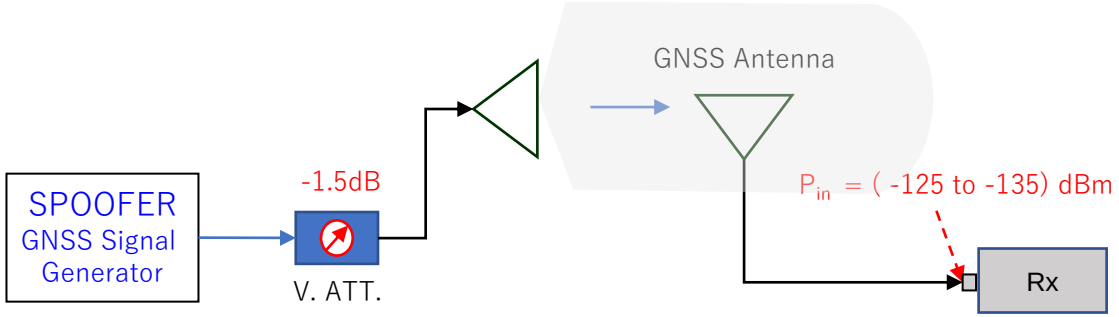
Spoofing Types	
Self-Spoofing	Spoof a receiver that is under own control
3rd Party Spoofing	Spoof a receiver that does not belong to you Or you don't have control over the target receiver

Direct Attack



Self-Spoofing

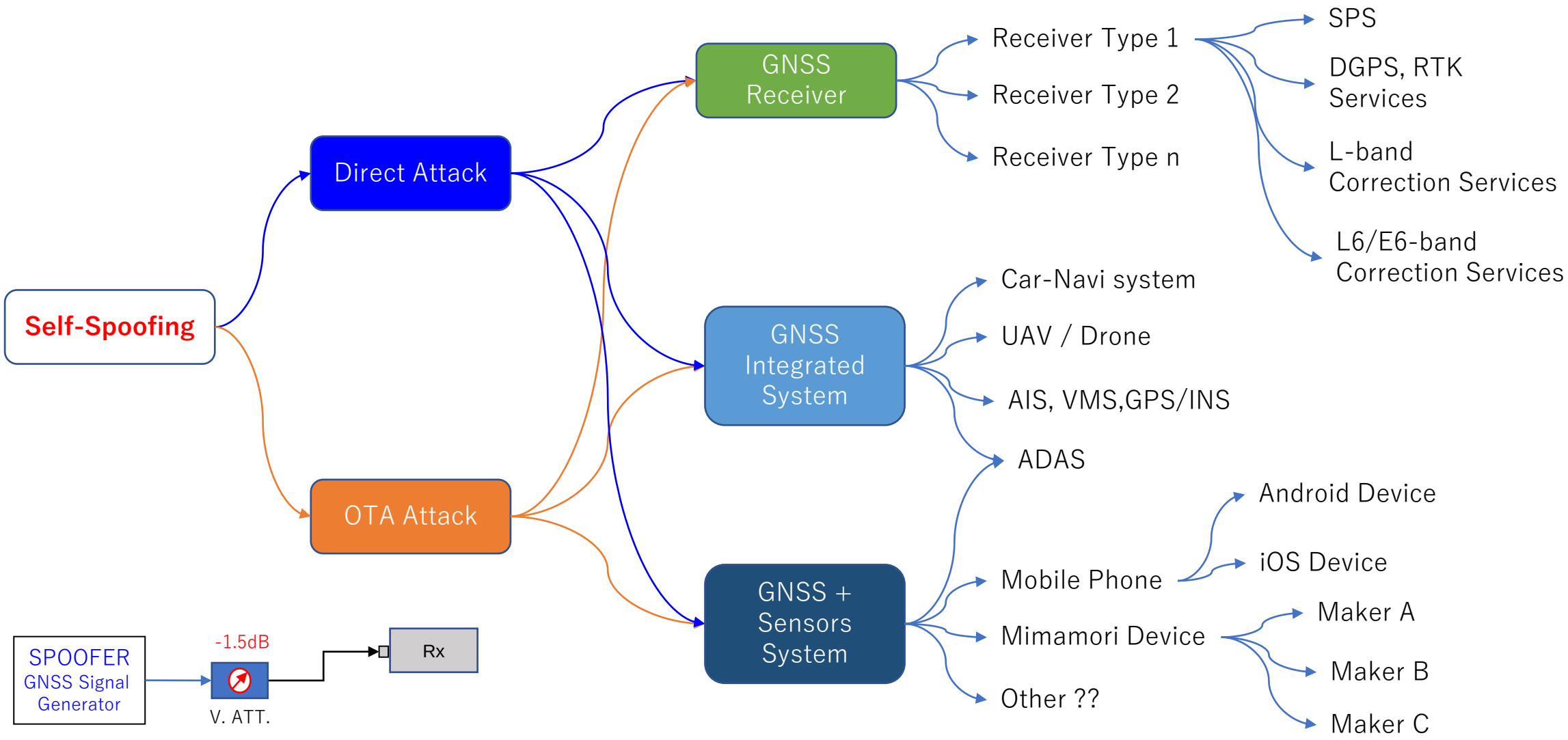
OTA (Over The Air) Attack



3rd Party Spoofing

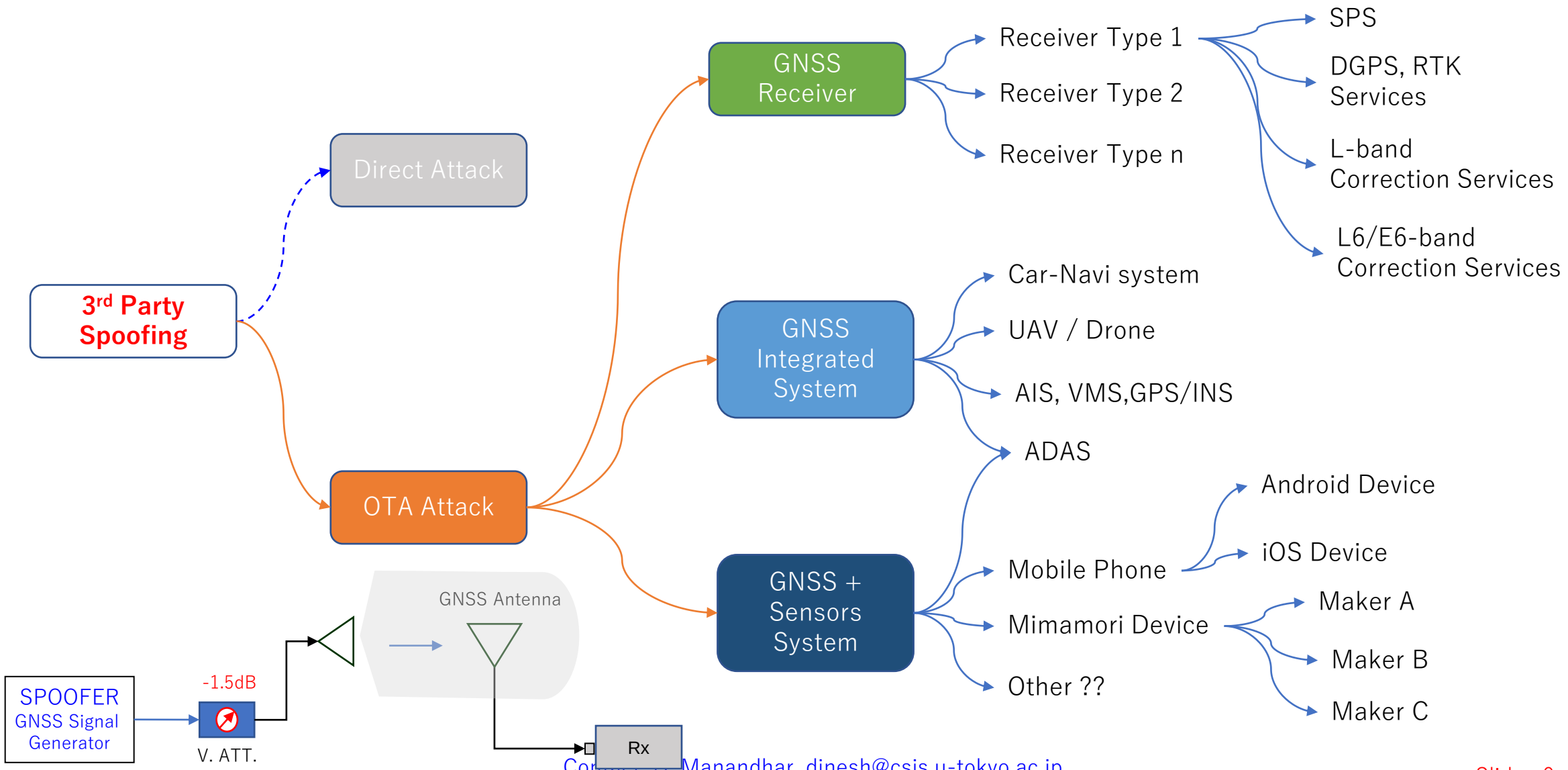
Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Self-Spoofing



Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

3rd Party Spoofing

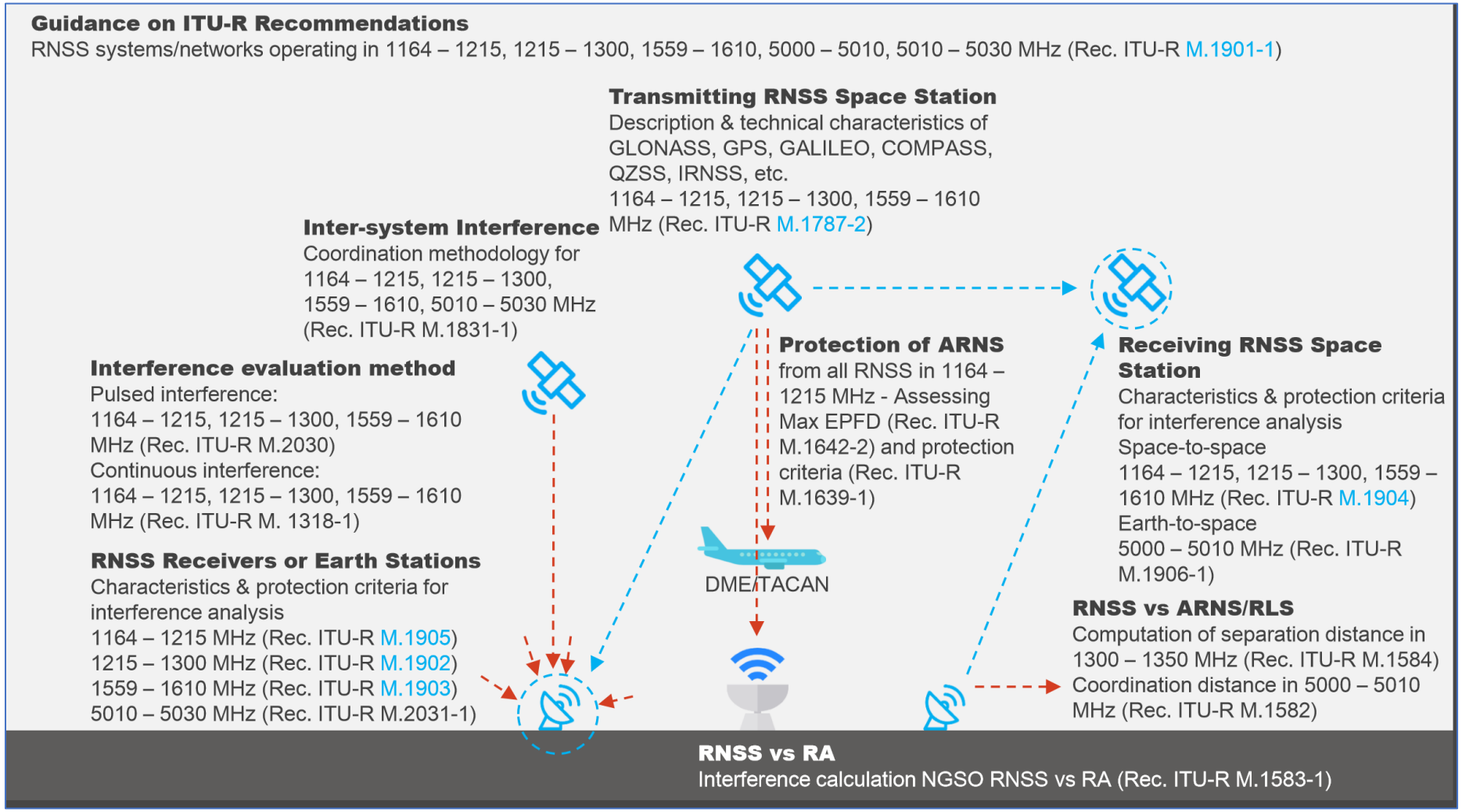


Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

GPS Signal Power and Spoof Signal Power

Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

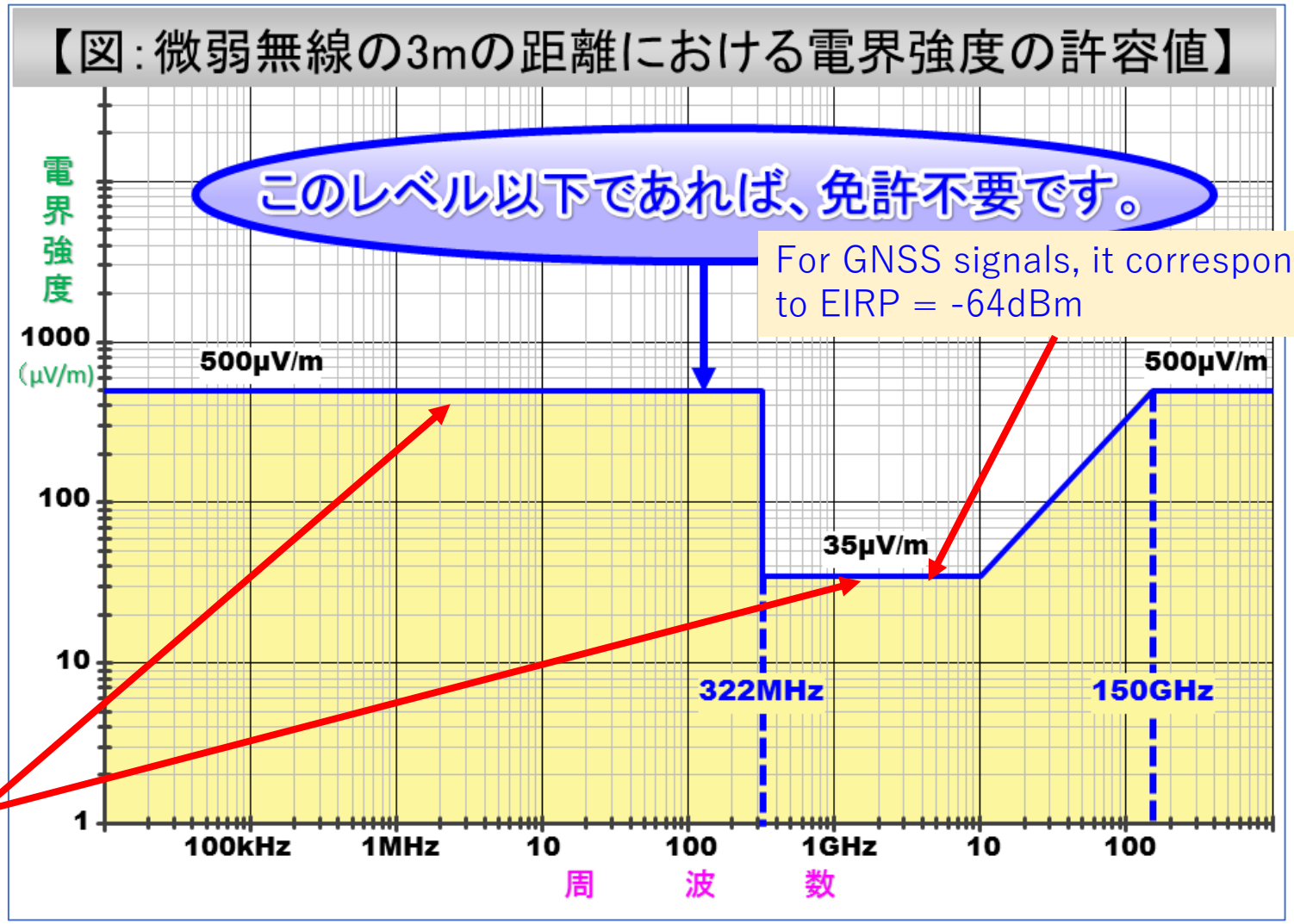
ITU-R Regulation



Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Japanese Radio Regulation for License Free Weak Signal Transmission

https://www.tele.soumu.go.jp/j/ref/material/rule/index.htm

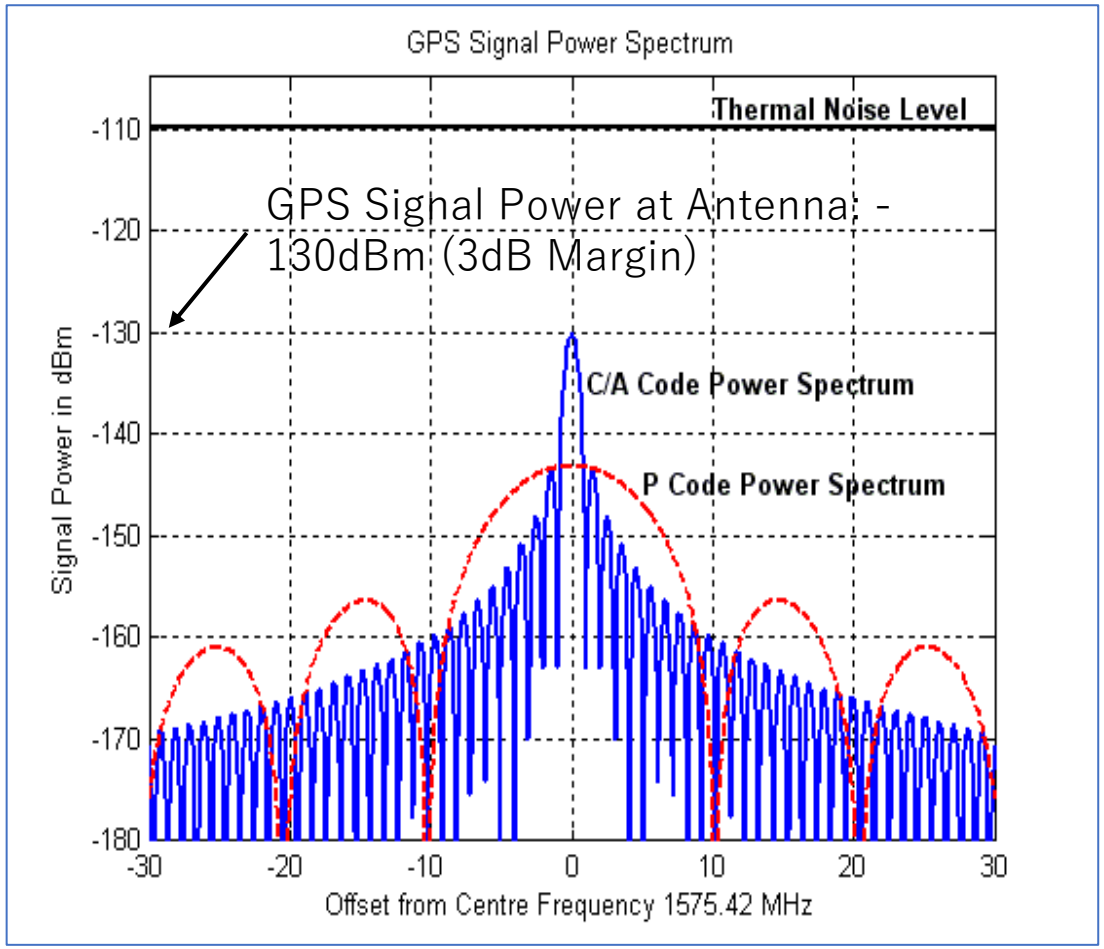


No license if the signal power at 3m is below this level

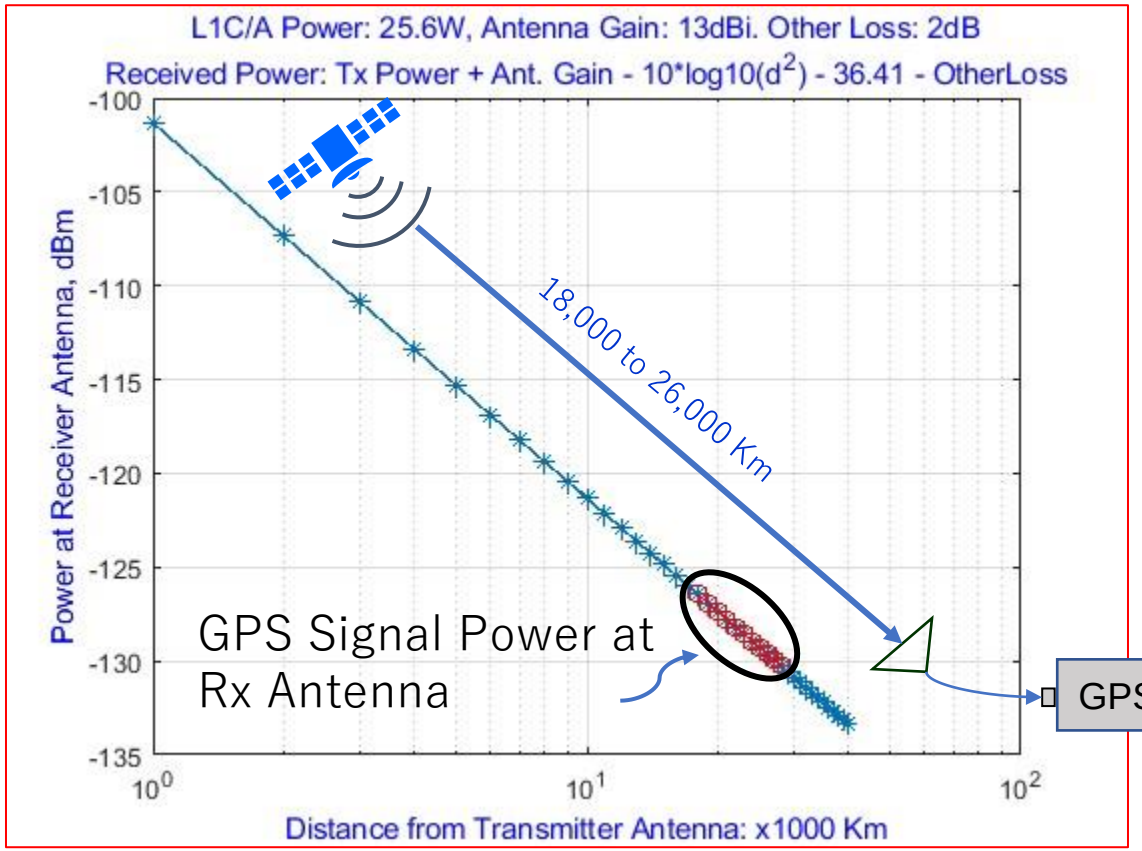
What is your country's regulation?

Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

GPS Signal Power



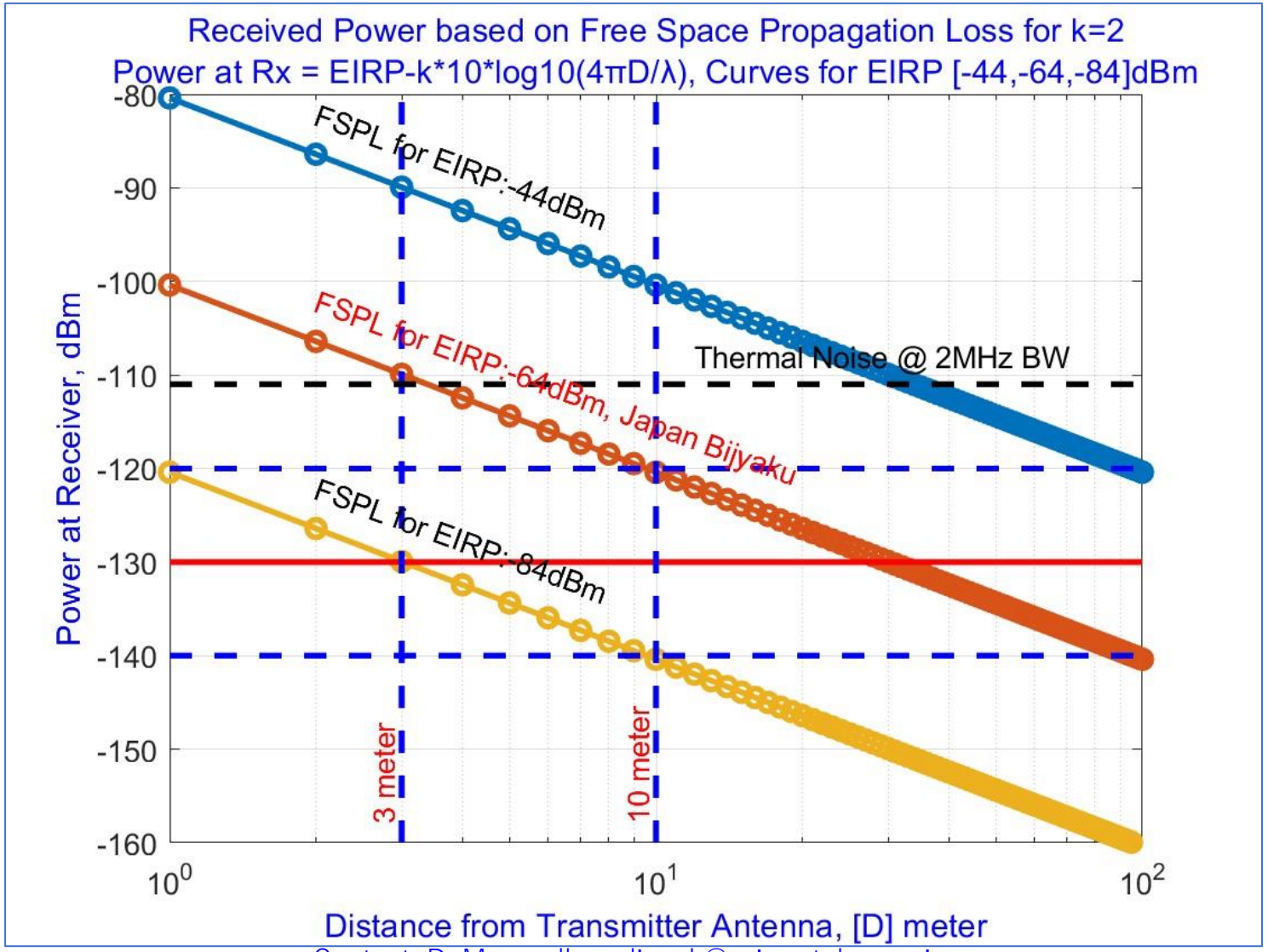
Mobile phone, WiFi, BT etc. have power levels above -111dBm, much higher than GPS Signal Power



GPS L1C/A Signal Power at Receiver Antenna: -130 dBm or -193 dBm/Hz or -105 dBm/m2

Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

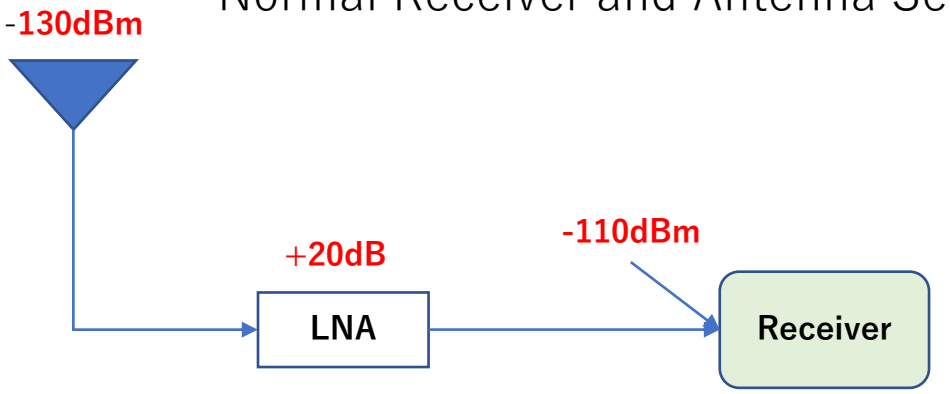
Free Space Propagation Loss (FSPL)



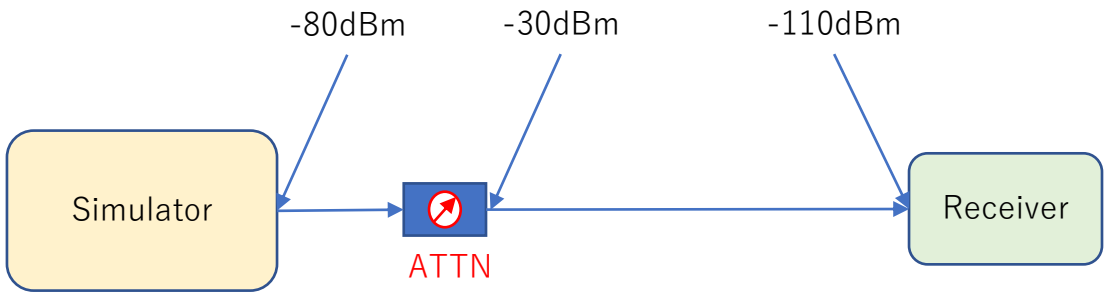
Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Spoofer Power Settings

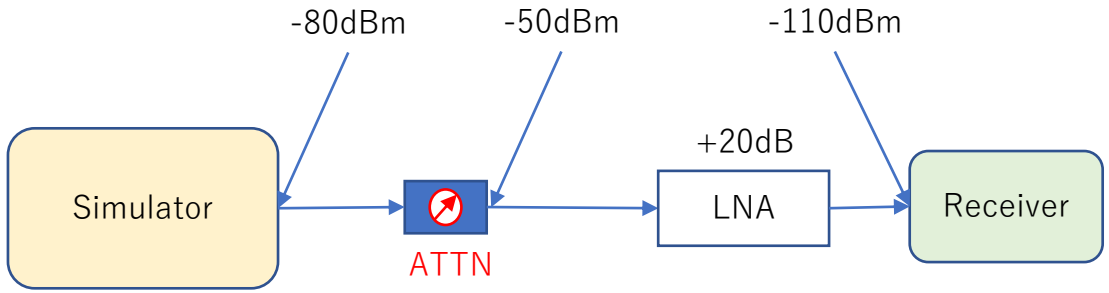
Normal Receiver and Antenna Setup



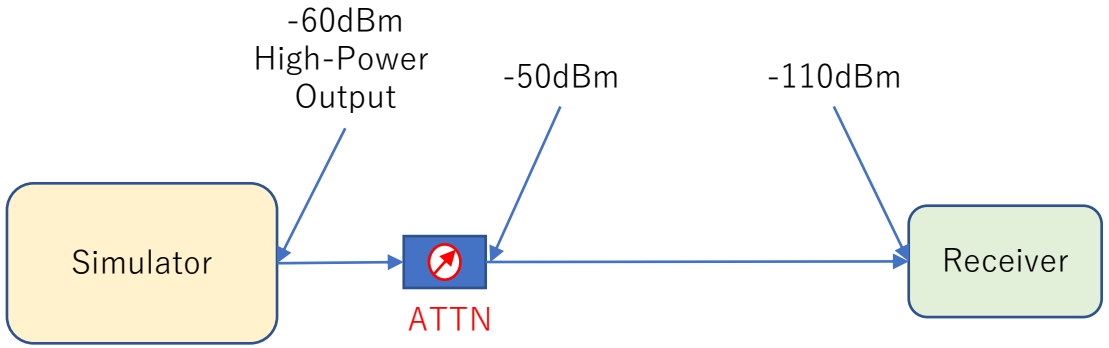
Direct connection, Without LNA



Direct connection, With LNA



Direct connection, Without LNA

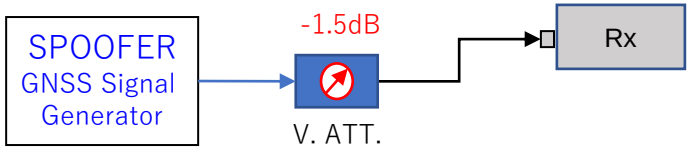


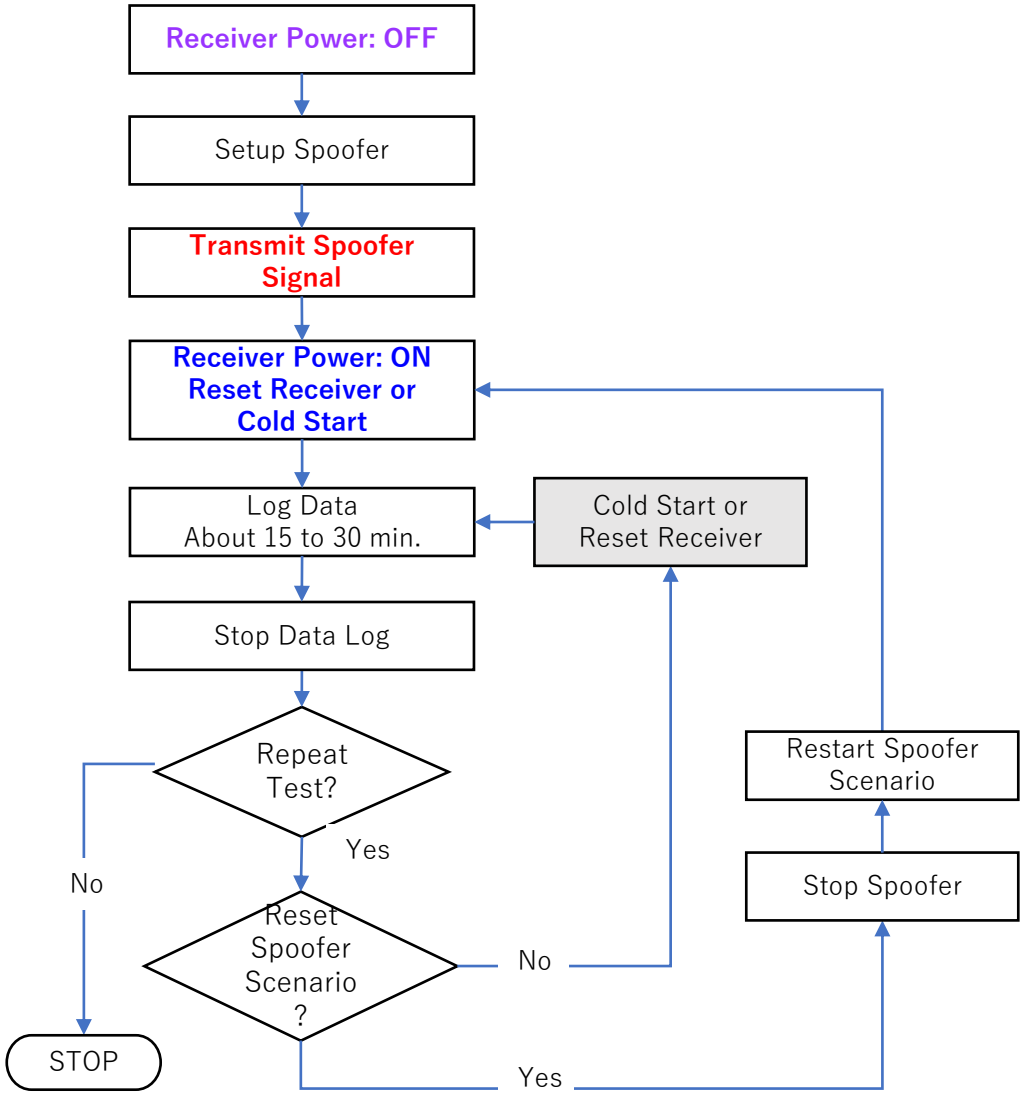
Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Spoofing Test Methods

Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

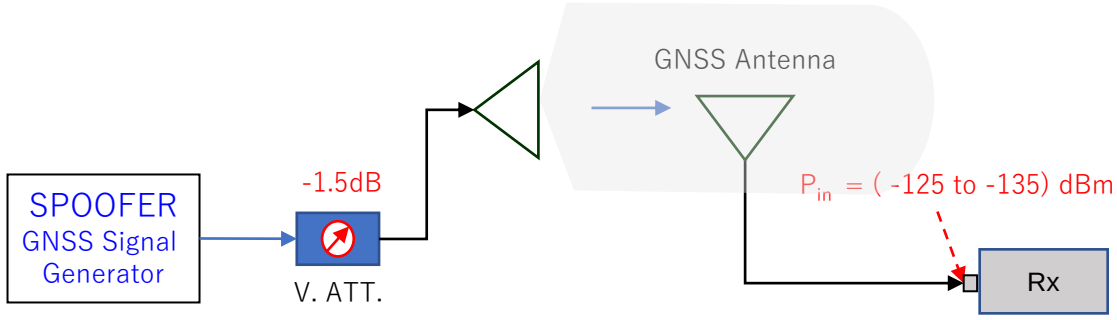
Direct Attack (DA) Test

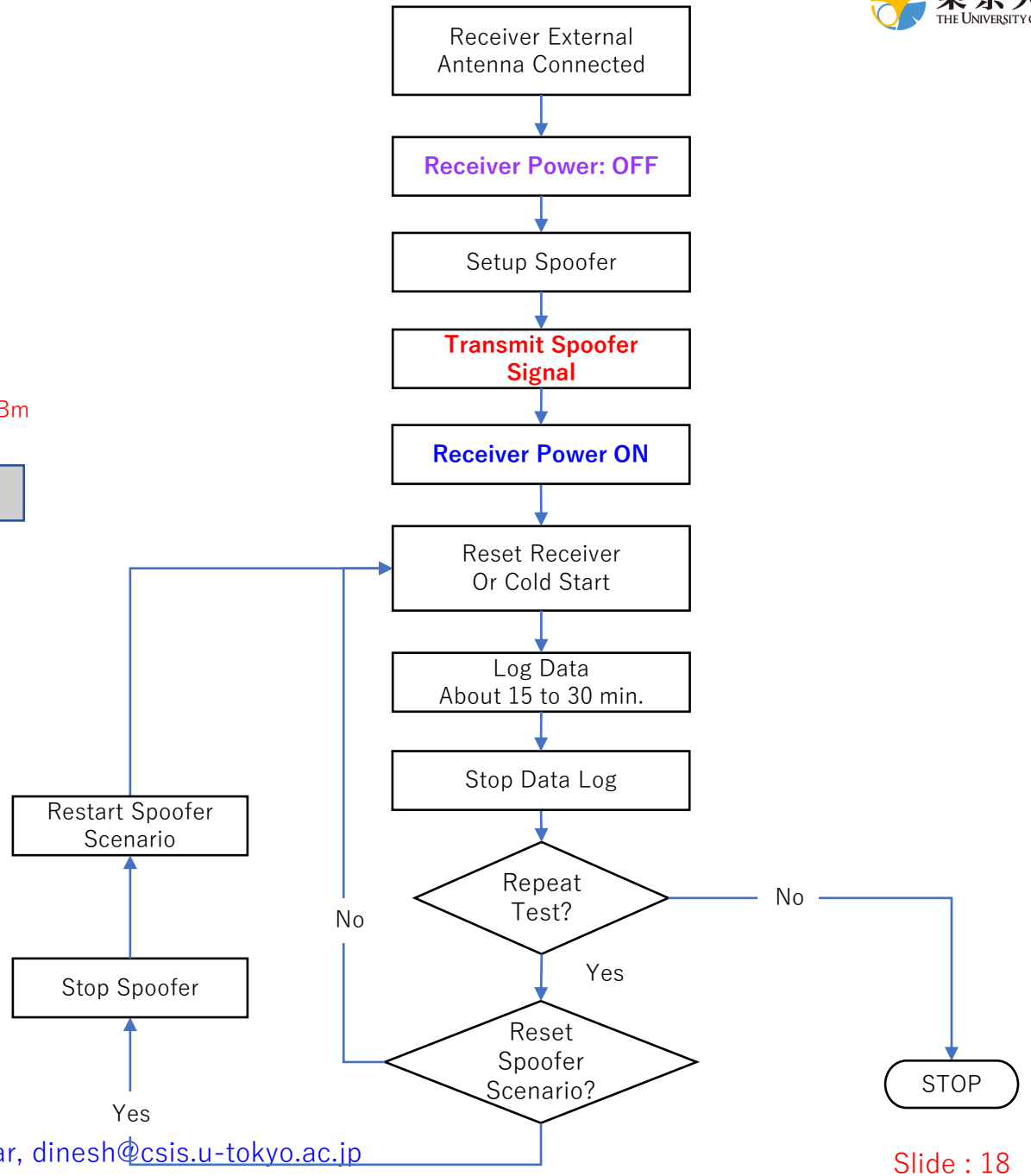




Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

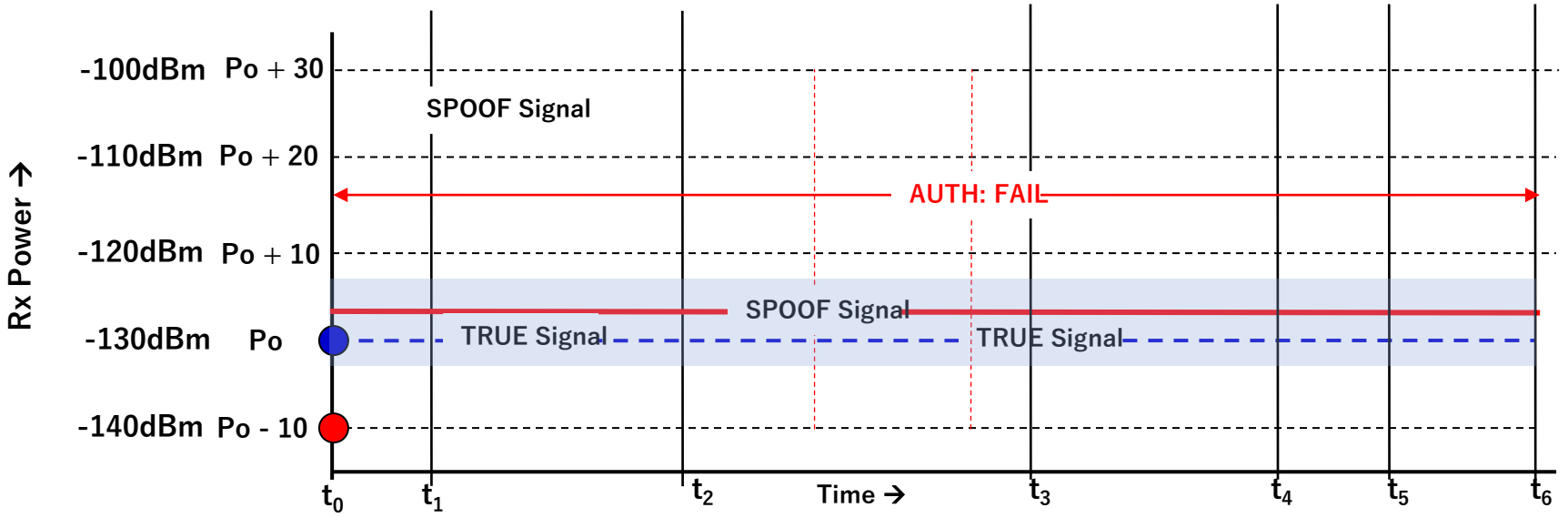
Over-The-Air (OTA) Test





Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

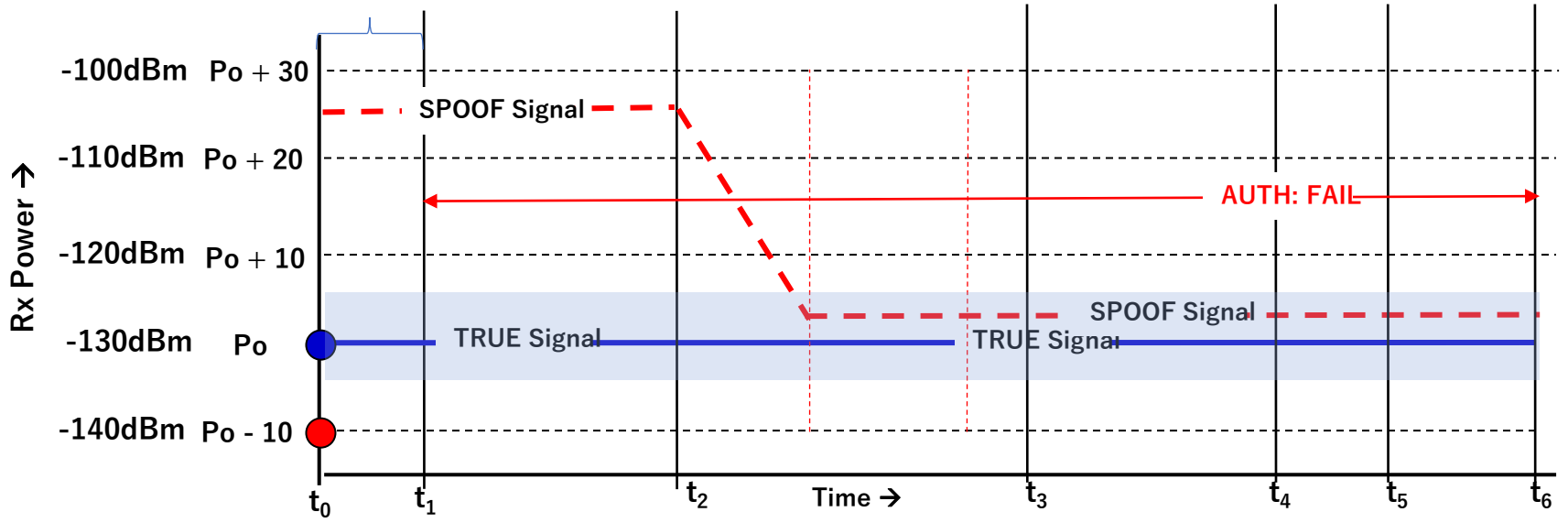
Spoofing Test: Power Control



Spoof signal is transmitted before the receiver power is turned on

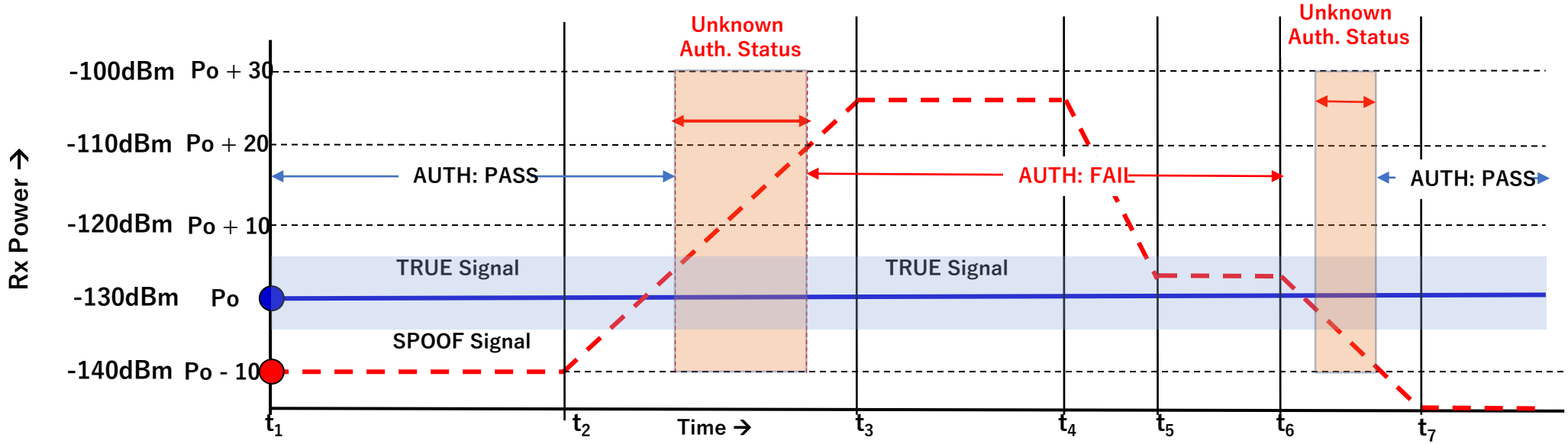
Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Spoofing Test: Power Control



Spoof signal is transmitted after the receiver power is turned on

Spoofing Test: Power Control



SPOOFING Signal Power is less than TRUE Signal
AUTH Status : PASS

SPOOFING Signal Power is slowly increased to overcome the TRUE Signal
AUTH Status : Changes from PASS to FAIL
NAV BIT Error may happen in the Yellow Zone

SPOOFING Signal Power is more than TRUE Signal
AUTH Status : FAIL

SPOOF Signal Power is reduced and kept at about 3 - 6dB above the TRUE Signal to Keep Lock on SPOOF Signal
AUTH Status : FAIL

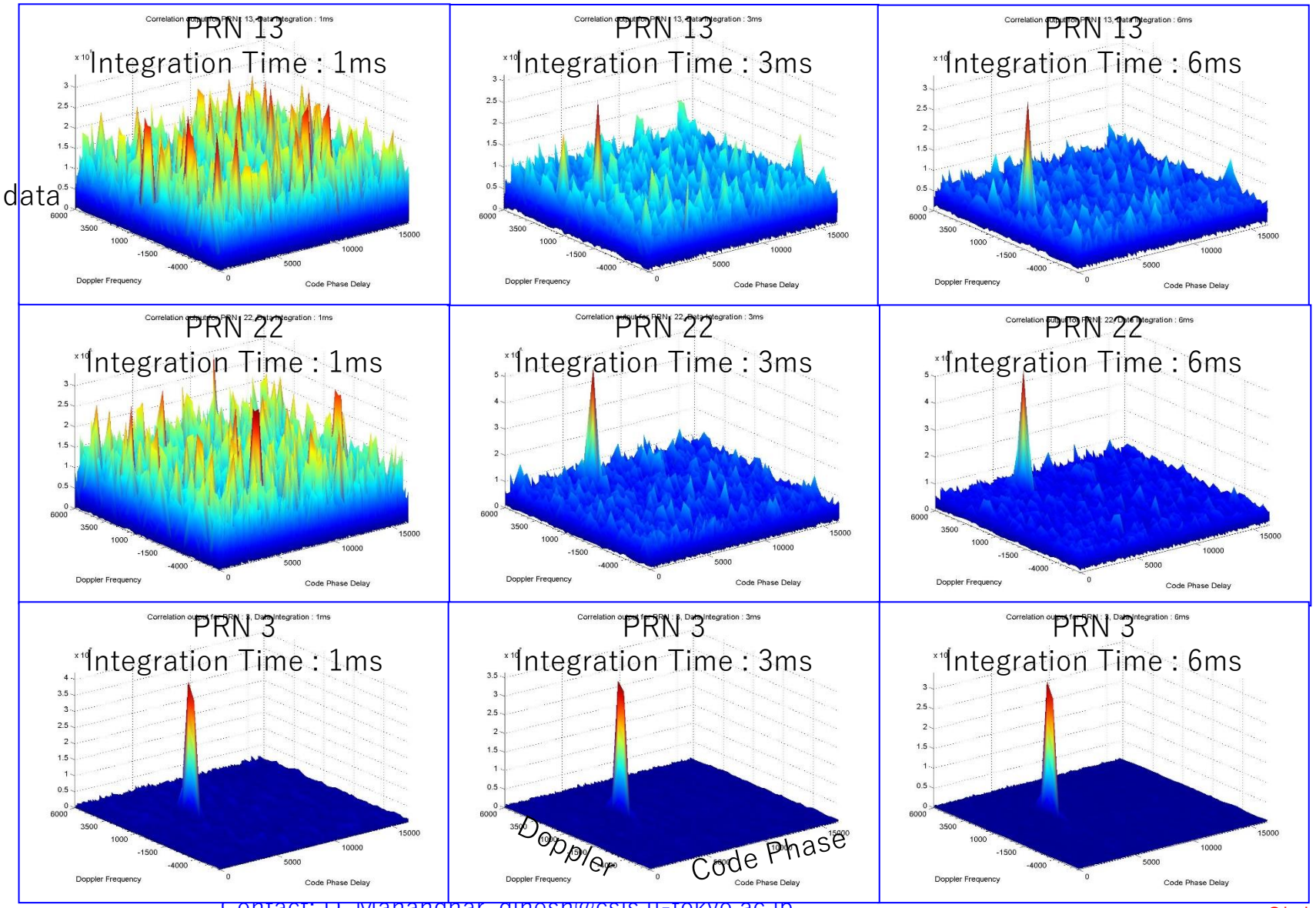
Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Impact on Signal Processing due to Interference or Spoof Signal

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

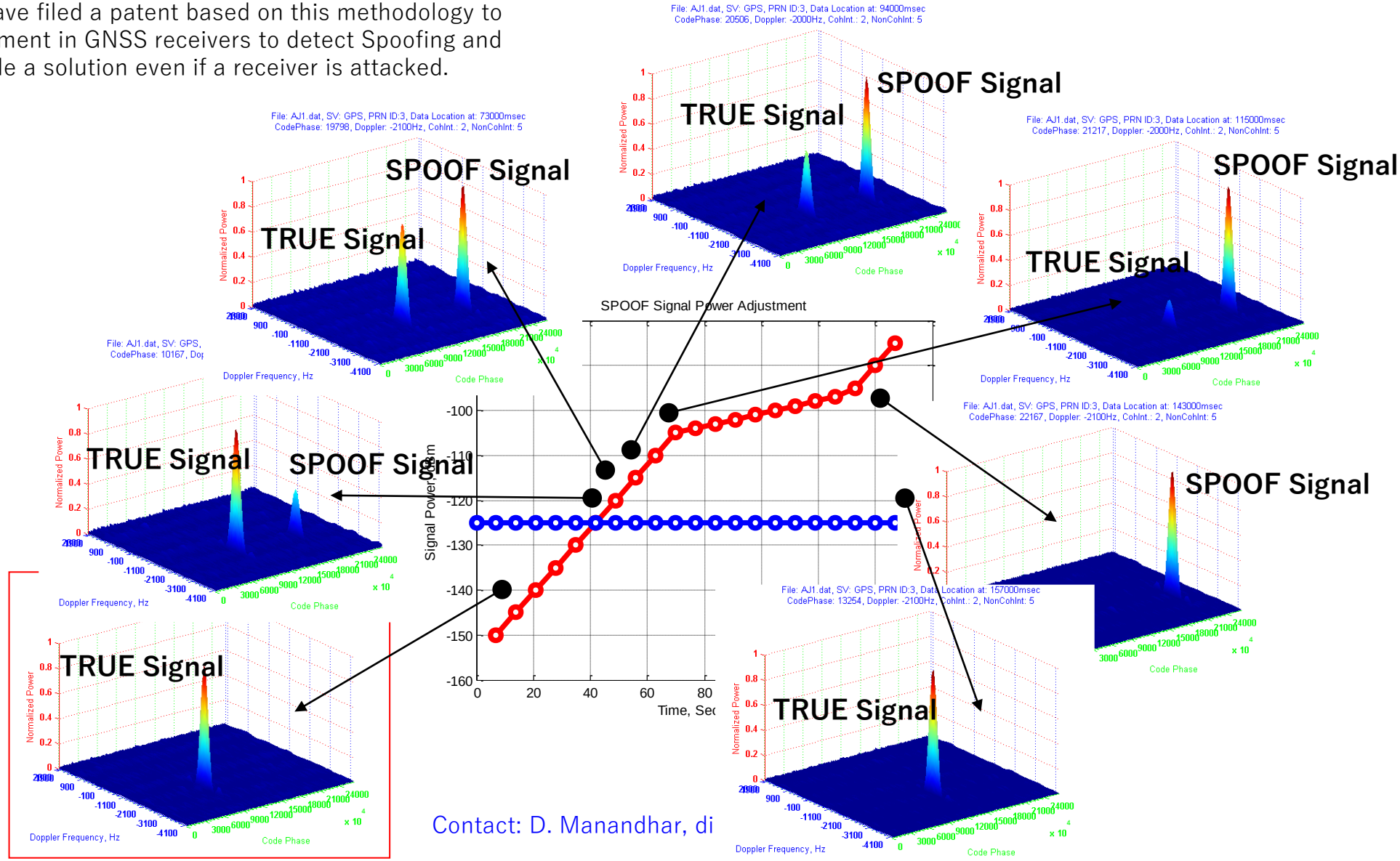
Presence of noise

Very small noise



True Signal vs. SPOOF Signal when attacked by a Spoof Signal

We have filed a patent based on this methodology to implement in GNSS receivers to detect Spoofing and provide a solution even if a receiver is attacked.



Contact: D. Manandhar, di

Spoofing Attack Video

Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp

Summary

- Spoofing impacts on receivers as well as GNSS based systems shall be studied in detail.
  - However, it is quite complex to understand spoofing attacks.
- Anti-spoofing solutions require spoofing detection methods
- Thus, we recommend and request the stakeholders for support to conduct spoofing-related studies, field tests etc. through the IPNTJ, working group.

Contact: D. Manandhar, dinesh@csis.u-tokyo.ac.jp