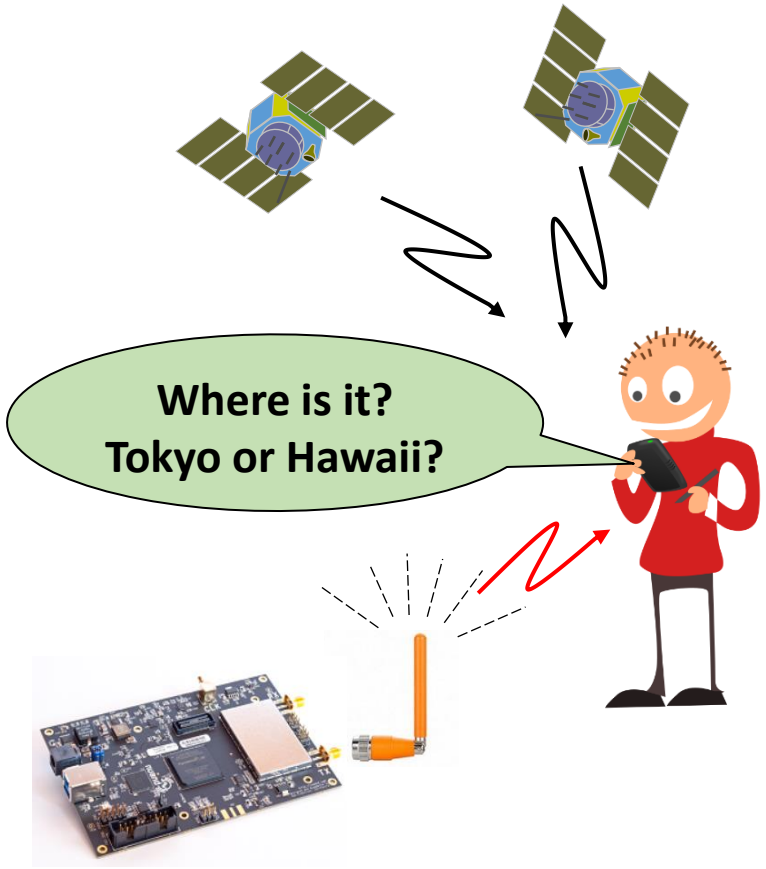
Overview of GNSS Spoofing and Some Test Results of Signal Authentication

Dinesh MANANDHAR
Center for Spatial Information Science (CSIS)
The University of Tokyo
dinesh@csis.u-tokyo.ac.jp

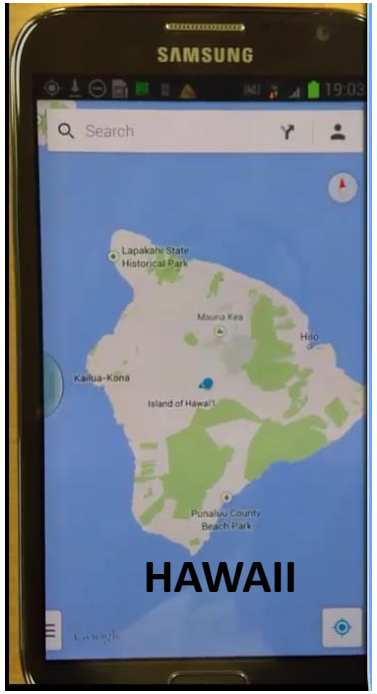
What is Location Spoofing?

- Falsify Location Data as If it were True Location



Spoofer

TOKYO
Or
Hawaii?



007

Tomorrow Never Dies

This movie is all about GPS Spoofing

Dinesh Manandhar, The University of Tokyo, Japan, dinesh@csis.u-tokyo.ac.jp

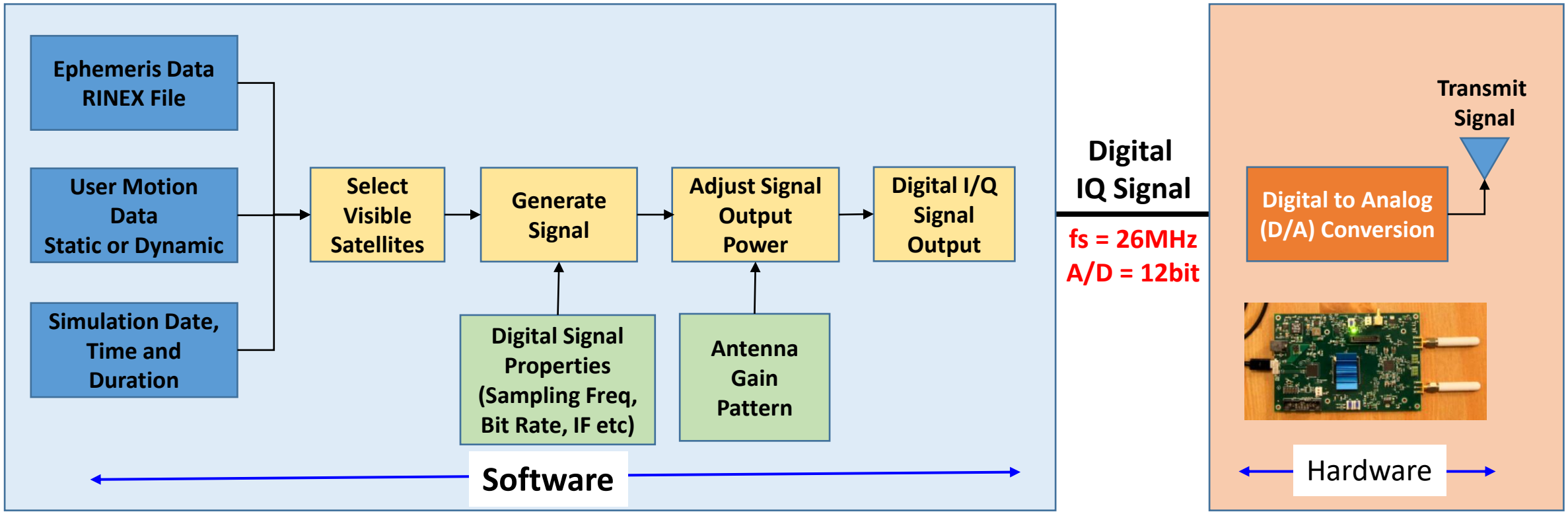
Introduction

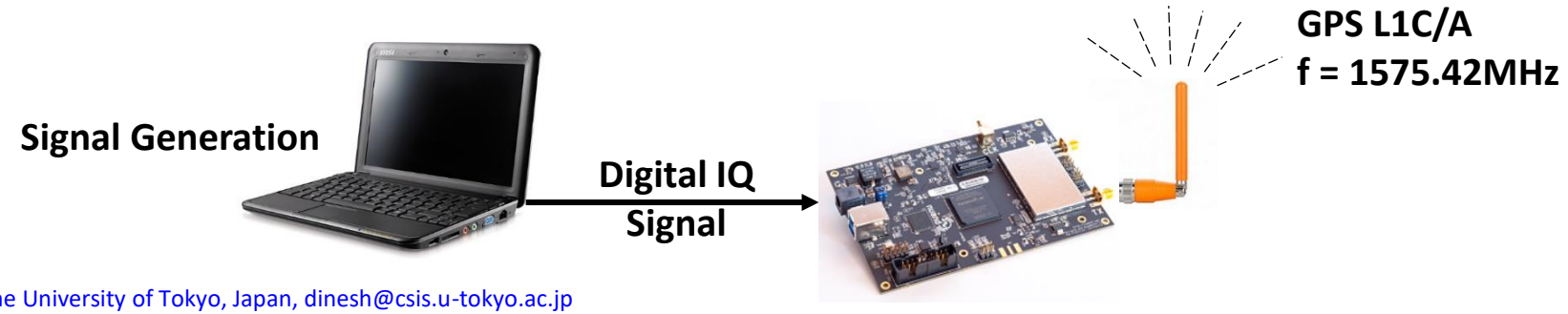
Main Issues of GNSS Signal Security : Jamming, Interference and Spoofing (JIS)

	Jamming	Interference	Spoofing
Attack Method	Intentional or Non-Intentional	Intentional or Non-Intentional	Intentional
Detection Possibility	It can be detected	Normally it can be detected Sometimes, non-detectable	Difficult to detect
Research and Studies	Many research and studies conducted	Many research and studies conducted	Very limited research and studies
Existing Solutions	Limited solutions exist Not effective for mass-market receiver systems	Limited solutions exist Not effective for mass-market receiver systems	No solutions exist. Recently, QZSS and Galileo are providing solutions for Spoofing detection
Severity Impact	Severe impact to deliver a service because the system may not work Non-availability of solutions	Severe impact to deliver quality service if the system is still working Non-reliable solutions	Severe and extremely dangerous impacts Spoofed solutions available as true solution

Dinesh Manandhar, The University of Tokyo, Japan, dinesh@csis.u-tokyo.ac.jp

Software-Based GPS Signal Generator (Spoofer?)





Dinesh Manandhar, The University of Tokyo, Japan, 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

Spoofing Methods and Types

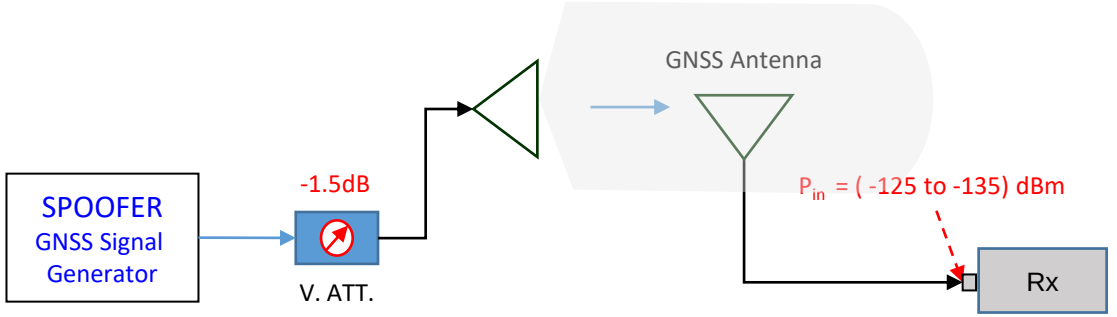
Spoofing Methods	
Direct Attack	Connect the target device directly by a cable Spoof signal is not transmitted by antenna
Over-The-Air Attack (OTA)	Transmit spoof signal over-the-air

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

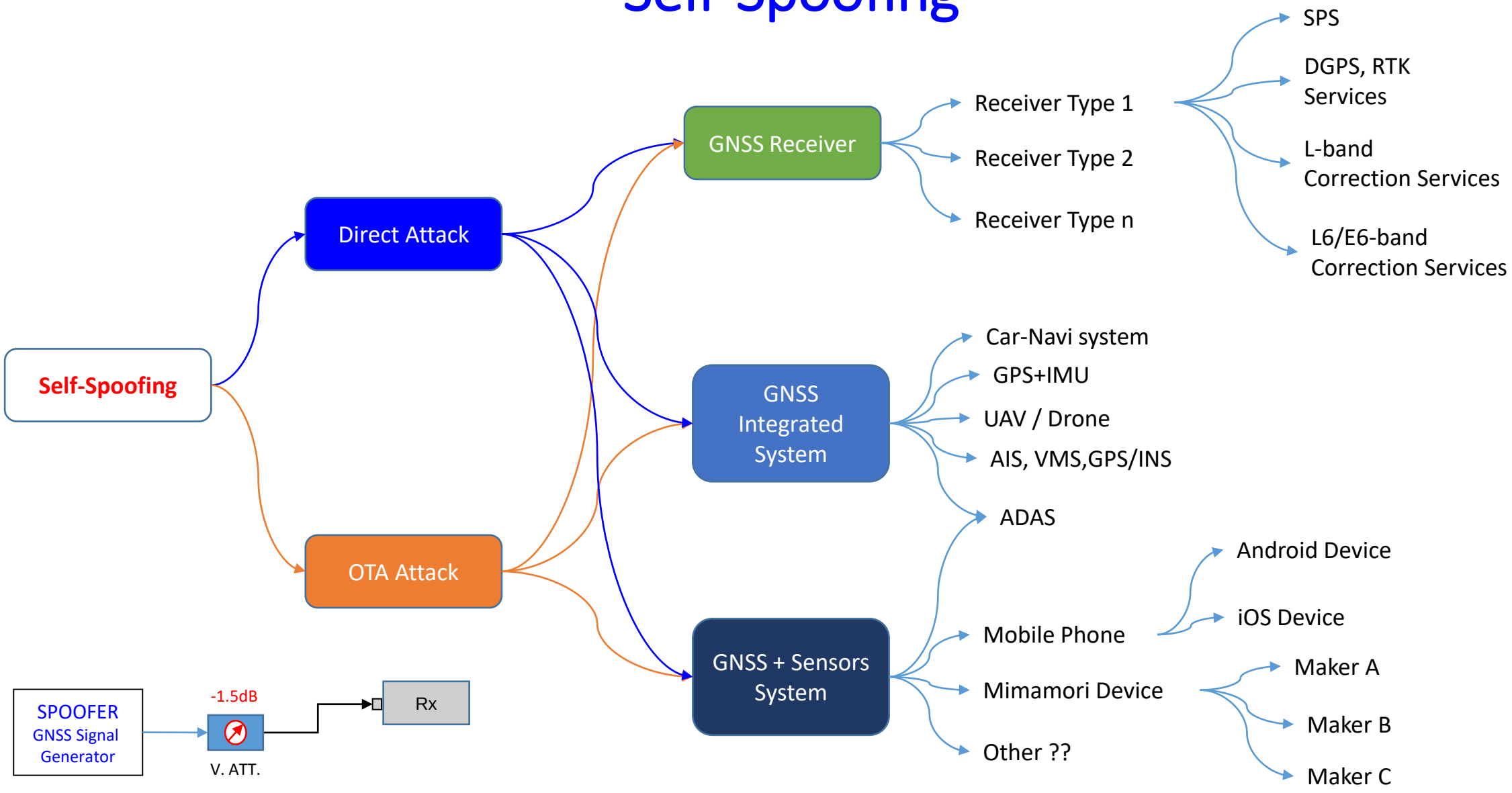
OTA (Over The Air) Attack



3rd Party Spoofing

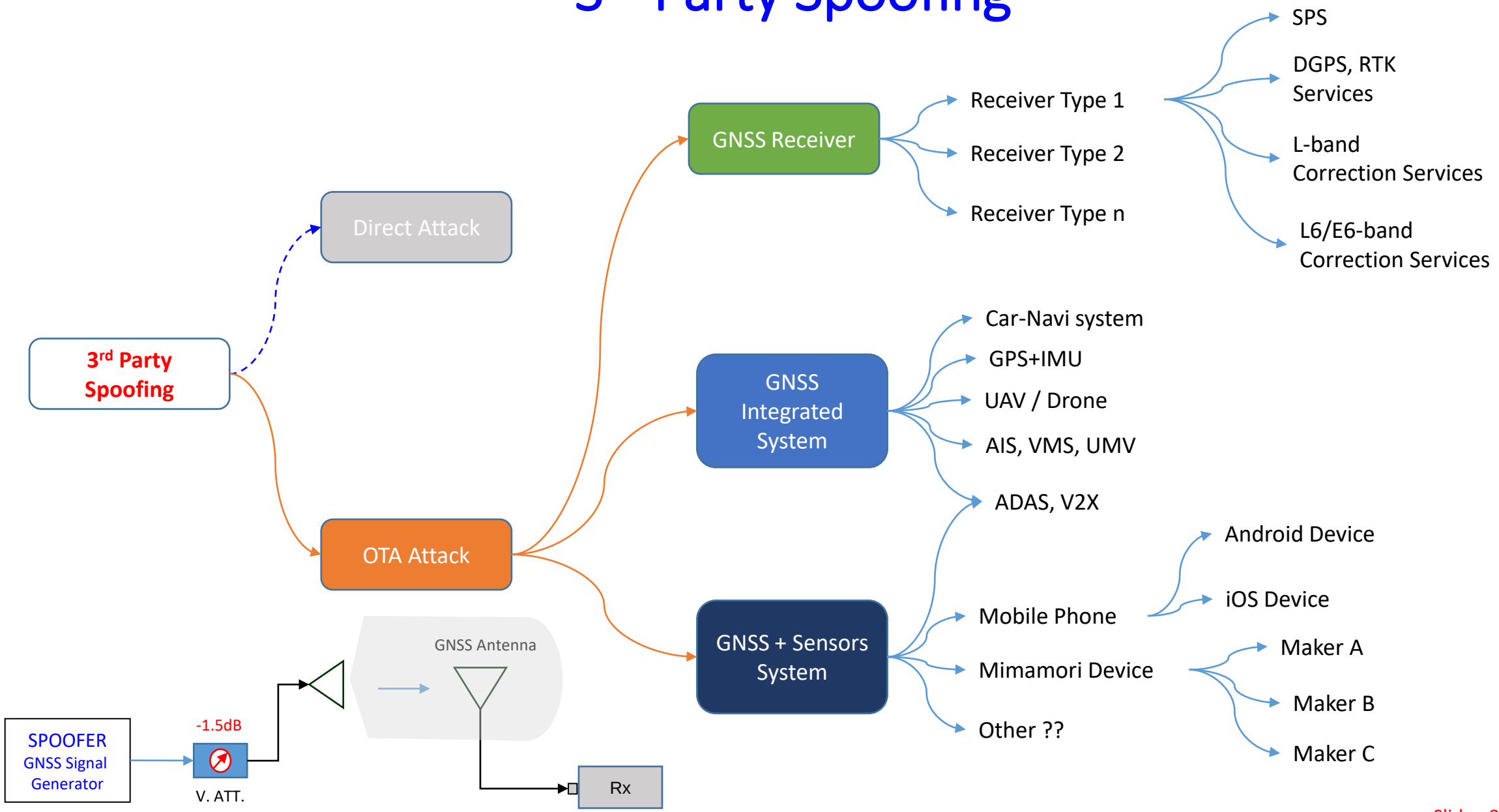
Dinesh Manandhar, The University of Tokyo, Japan, dinesh@csis.u-tokyo.ac.jp

Self-Spoofing



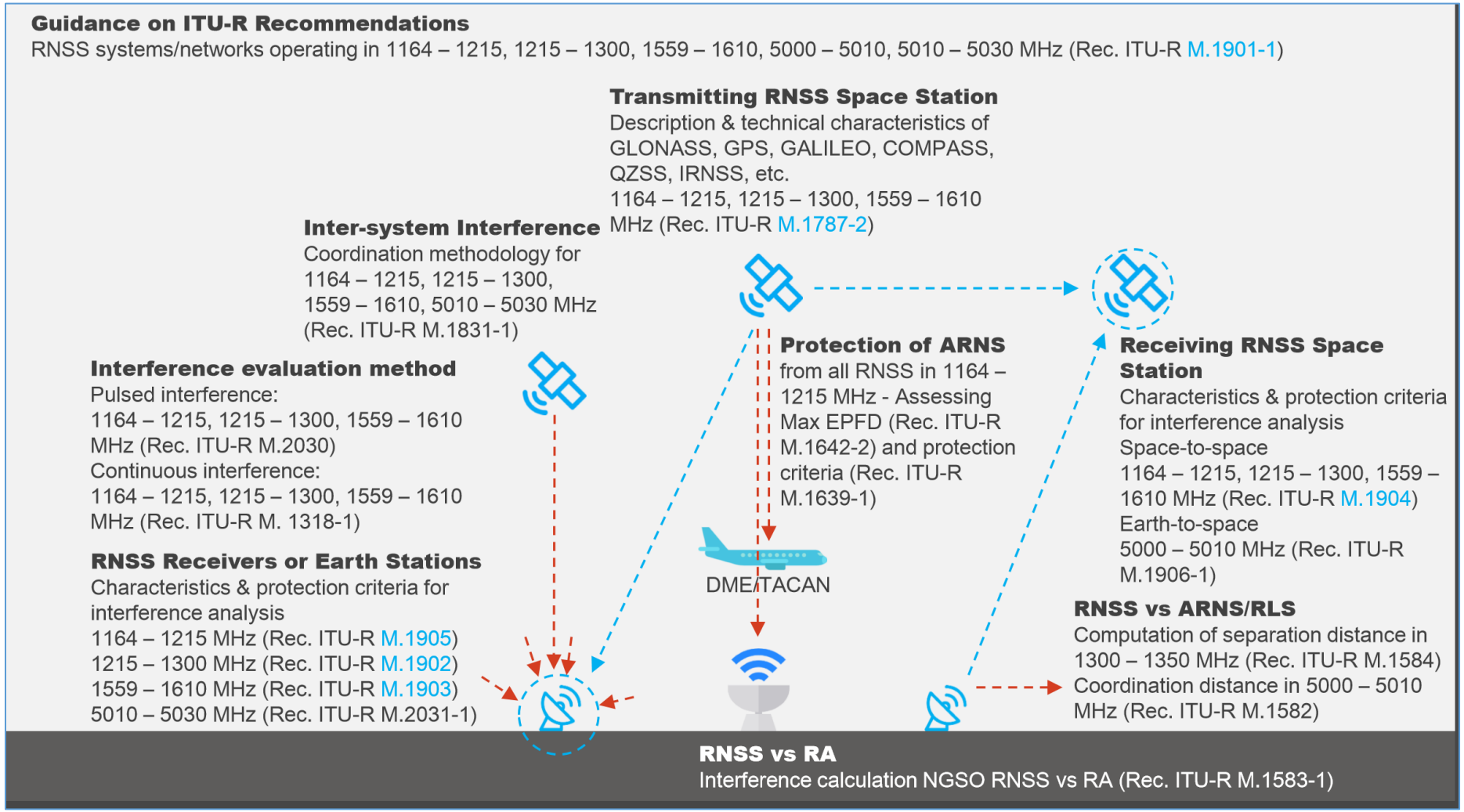
Dinesh Manandhar, The University of Tokyo, Japan, dinesh@csis.u-tokyo.ac.jp

3rd Party Spoofing



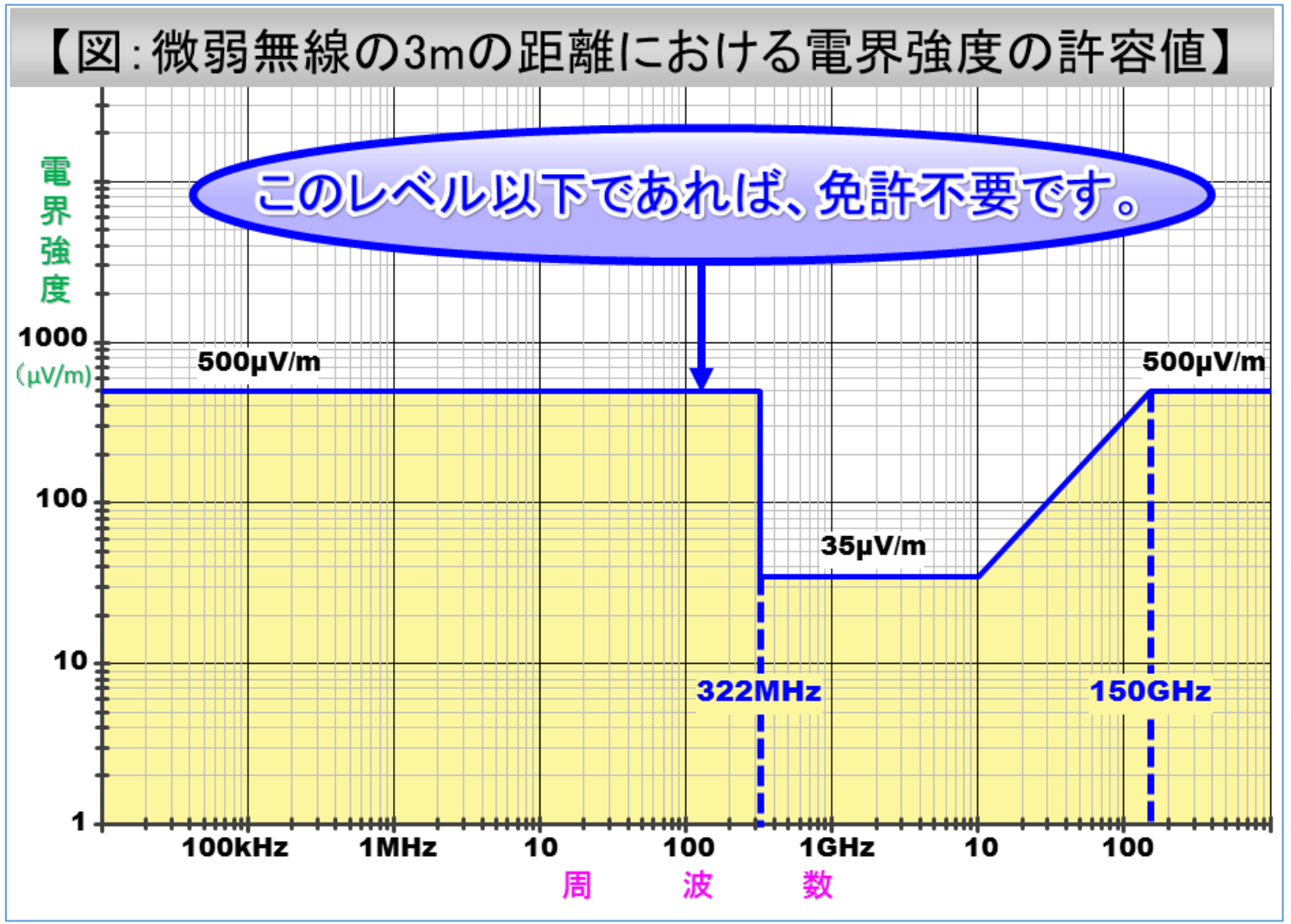
Dinesh Manandhar, The University of Tokyo, Japan, dinesh@csis.u-tokyo.ac.jp

ITU-R Regulation



微弱無線局の規定

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

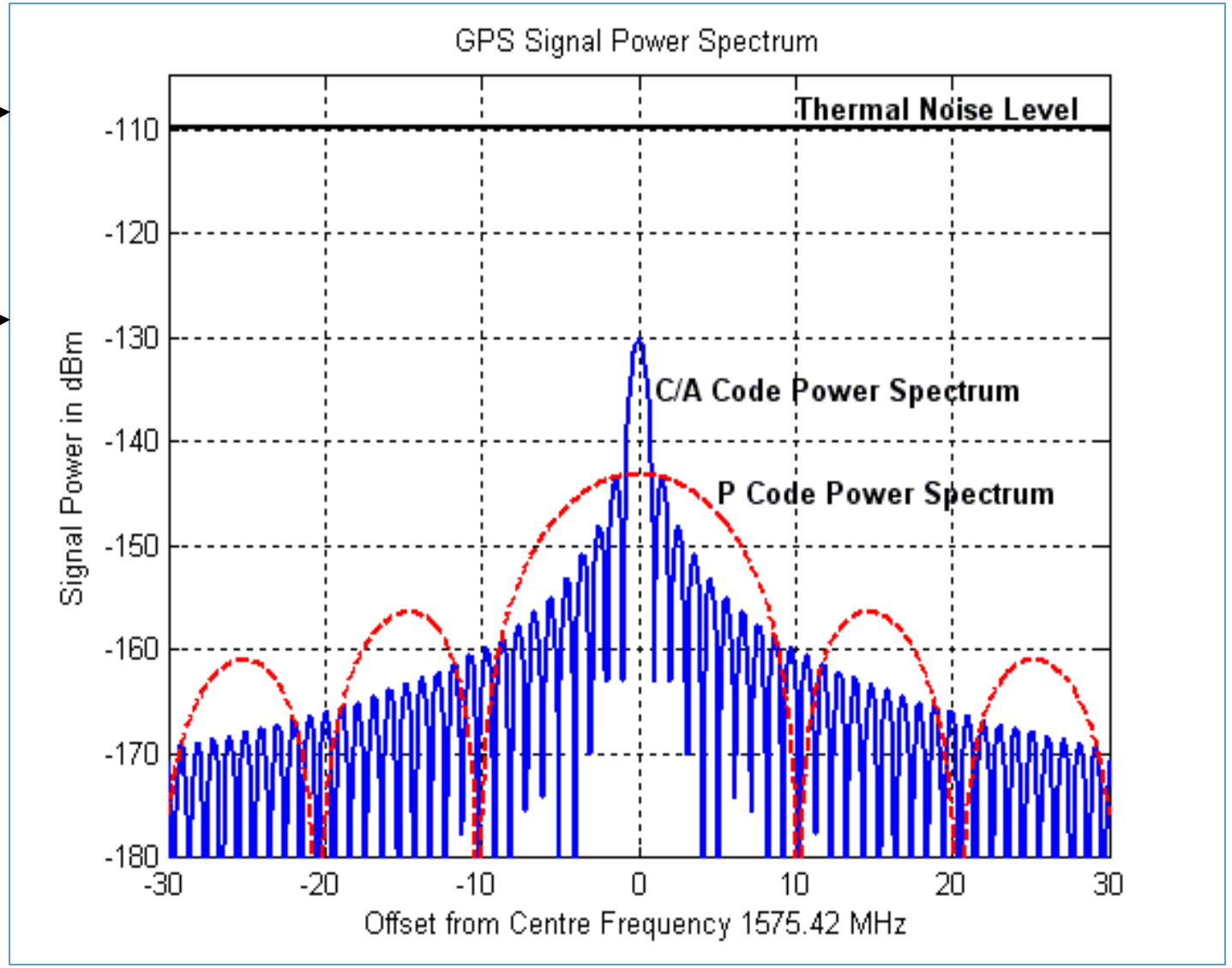


GPS Signal Power

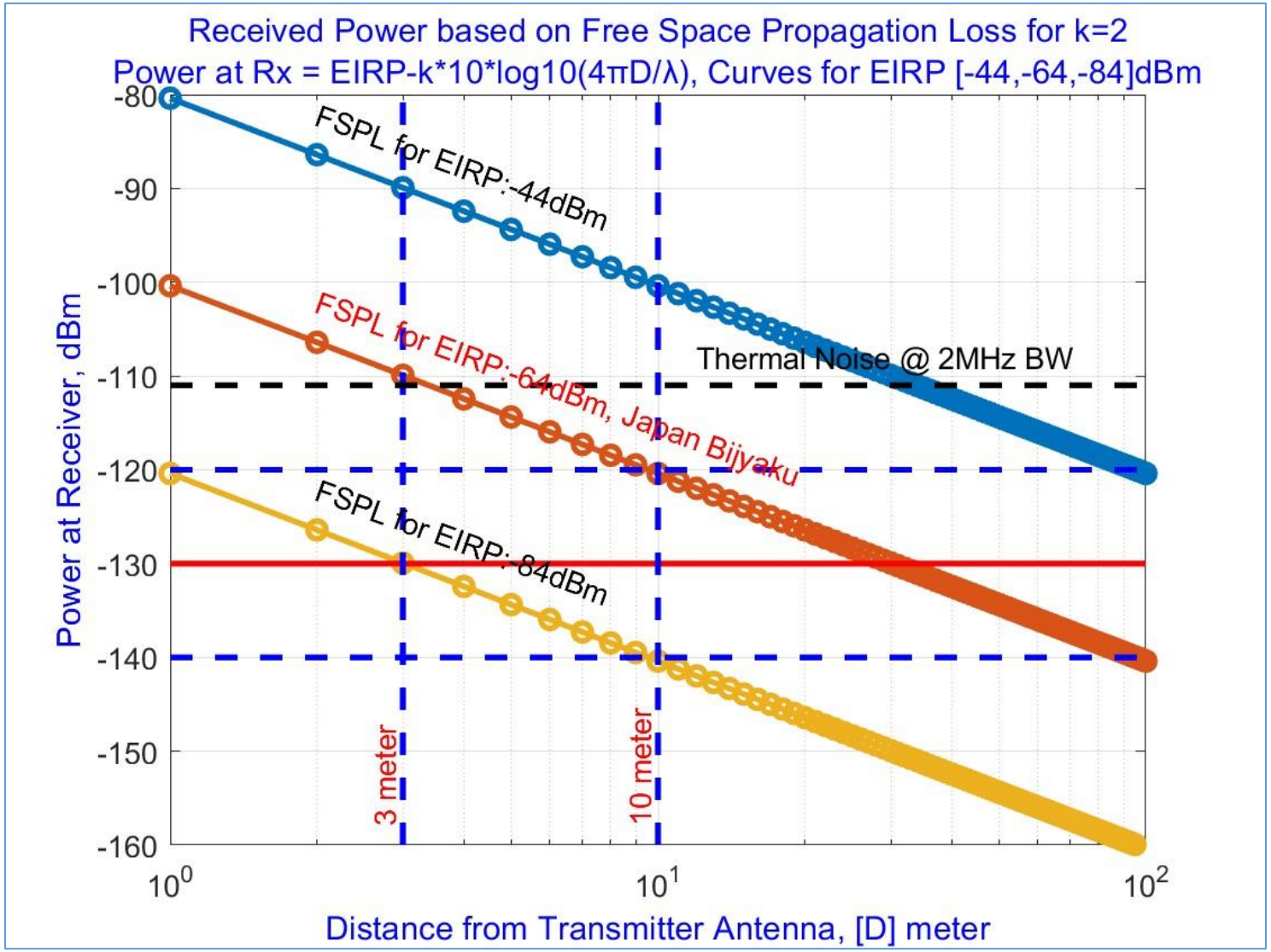
Noise Power
Any Signal below this noise level can't be measured in a Spectrum Analyzer

GPS Signal Power at Antenna -130dBm

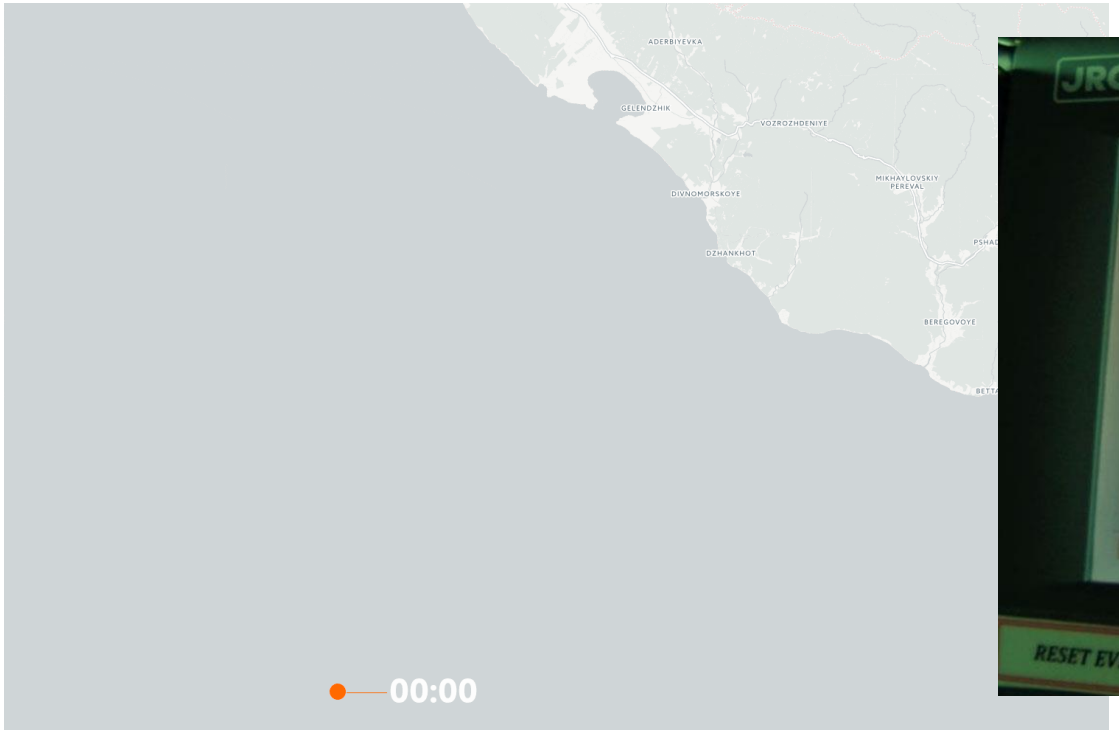
Mobile phone, WiFi, BT etc have power level above -110dBm, much higher than GPS Signal Power

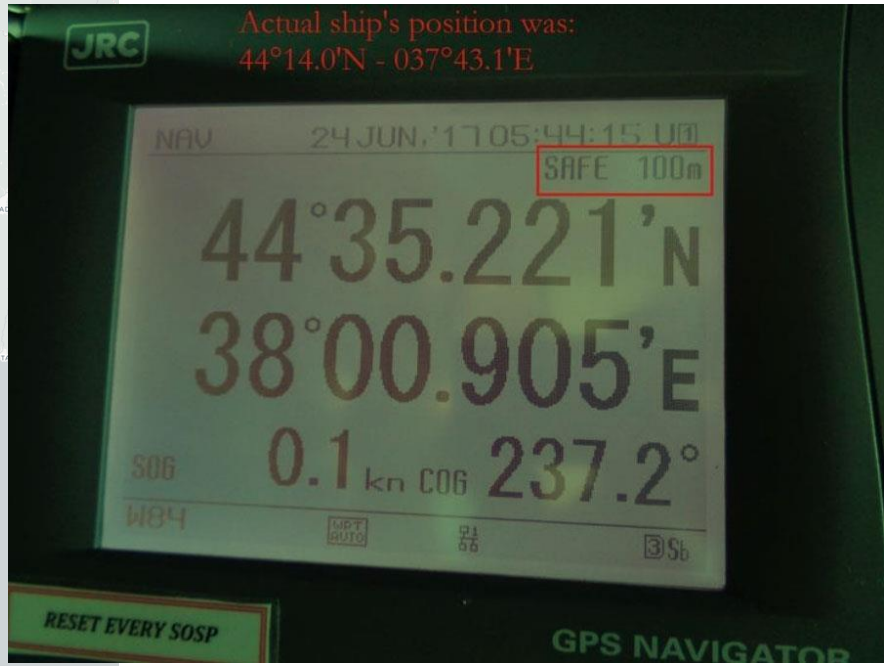


Free Space Propagation Loss (FSPL)



Spoofing Incident in Black Sea

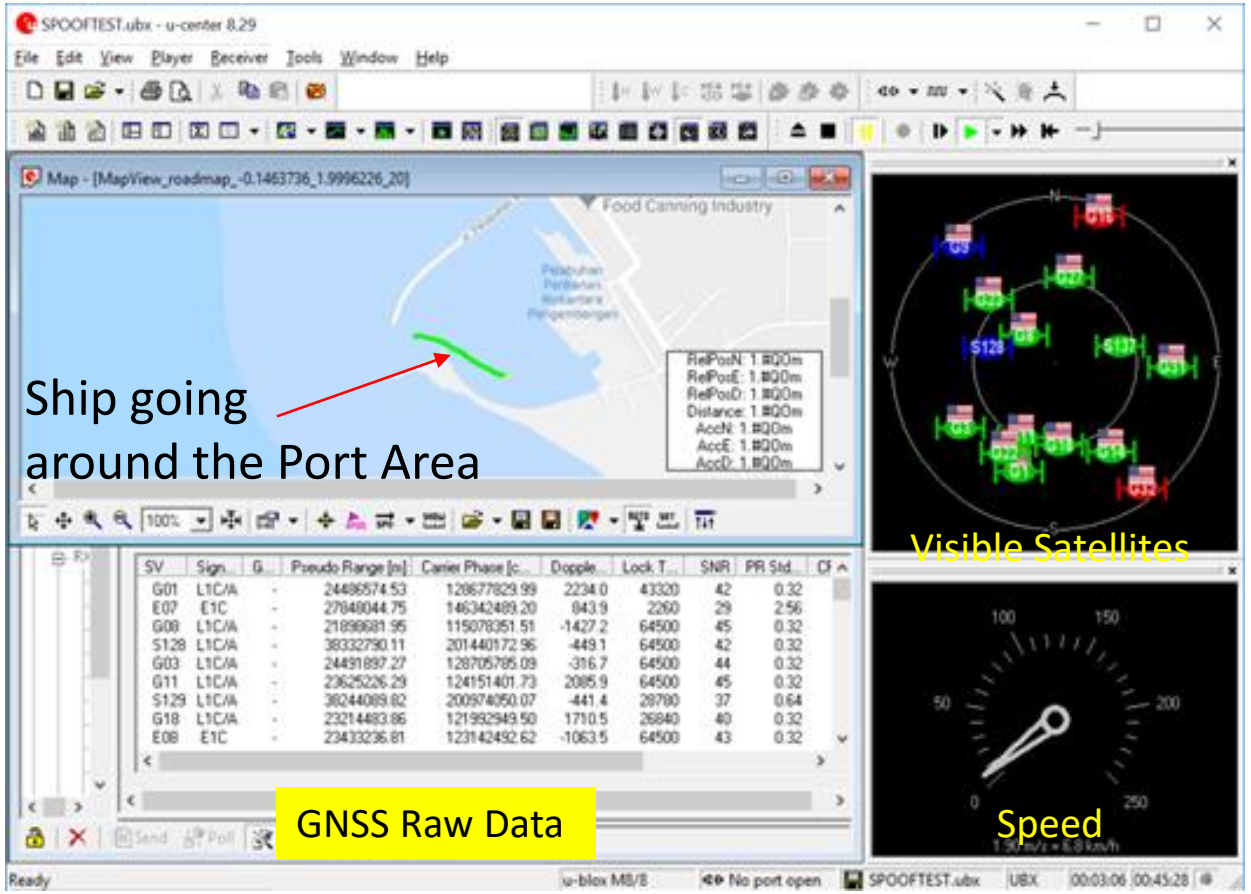


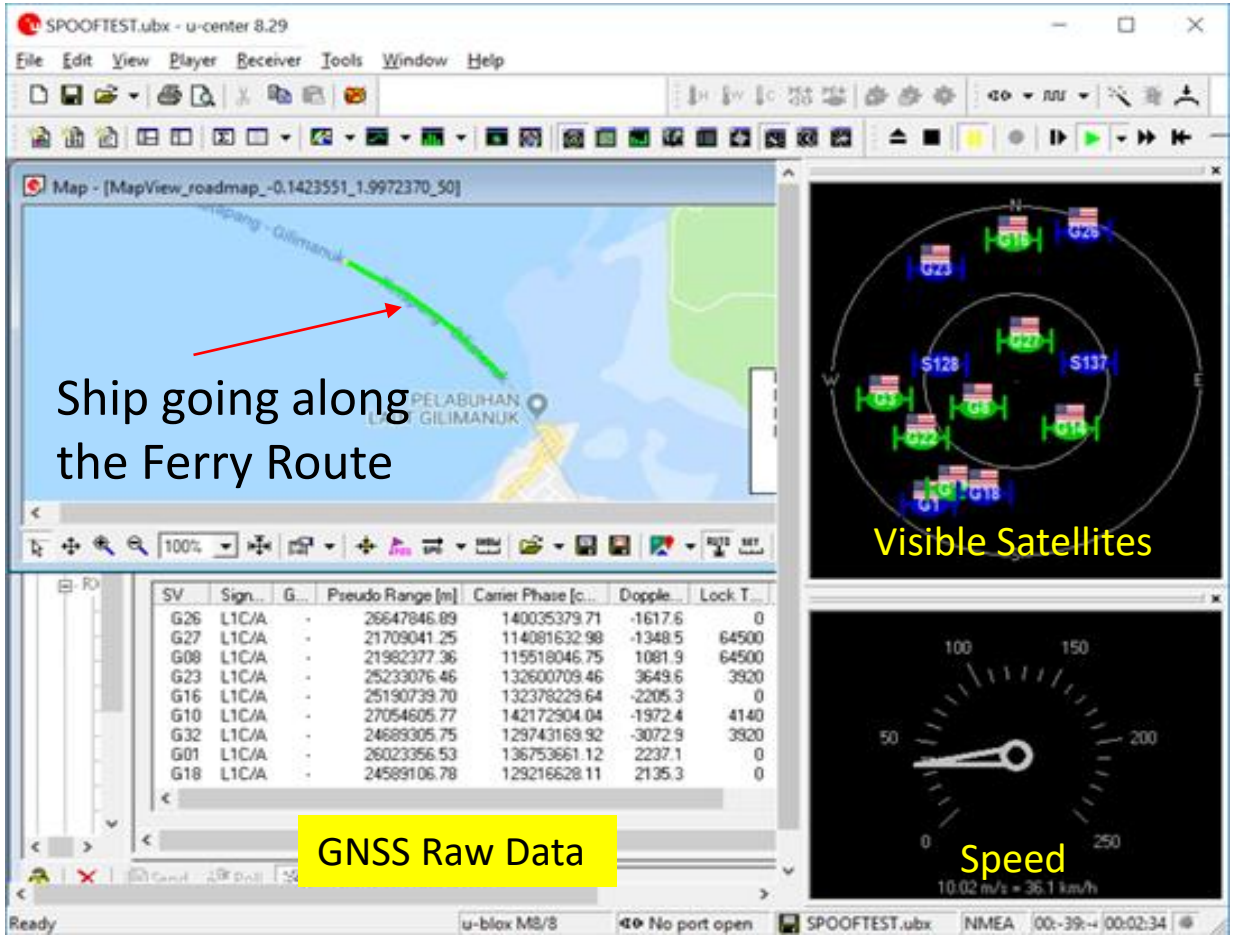


These are actually recorded data

SPOOFing a Car: Is he driving the car?

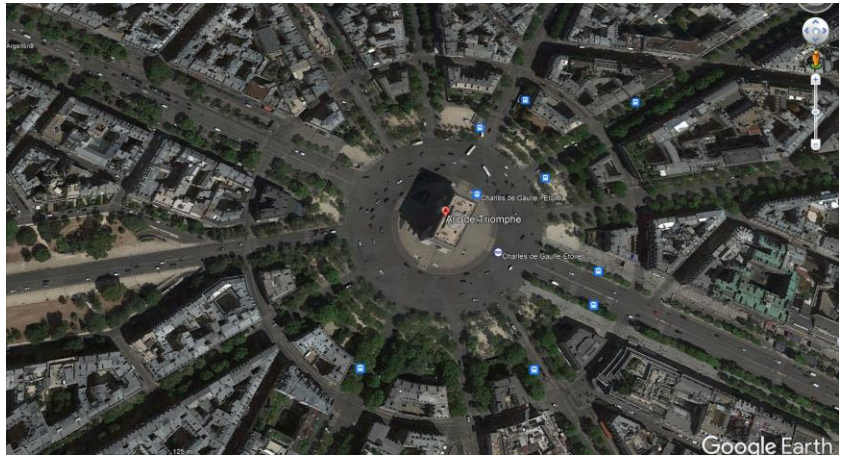
Can you identify TRUE Data and SPOOF Data?

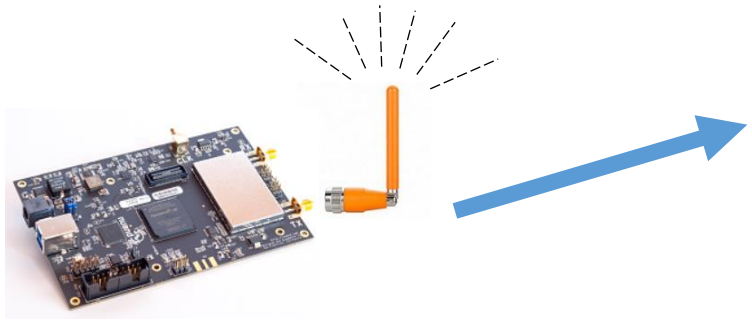


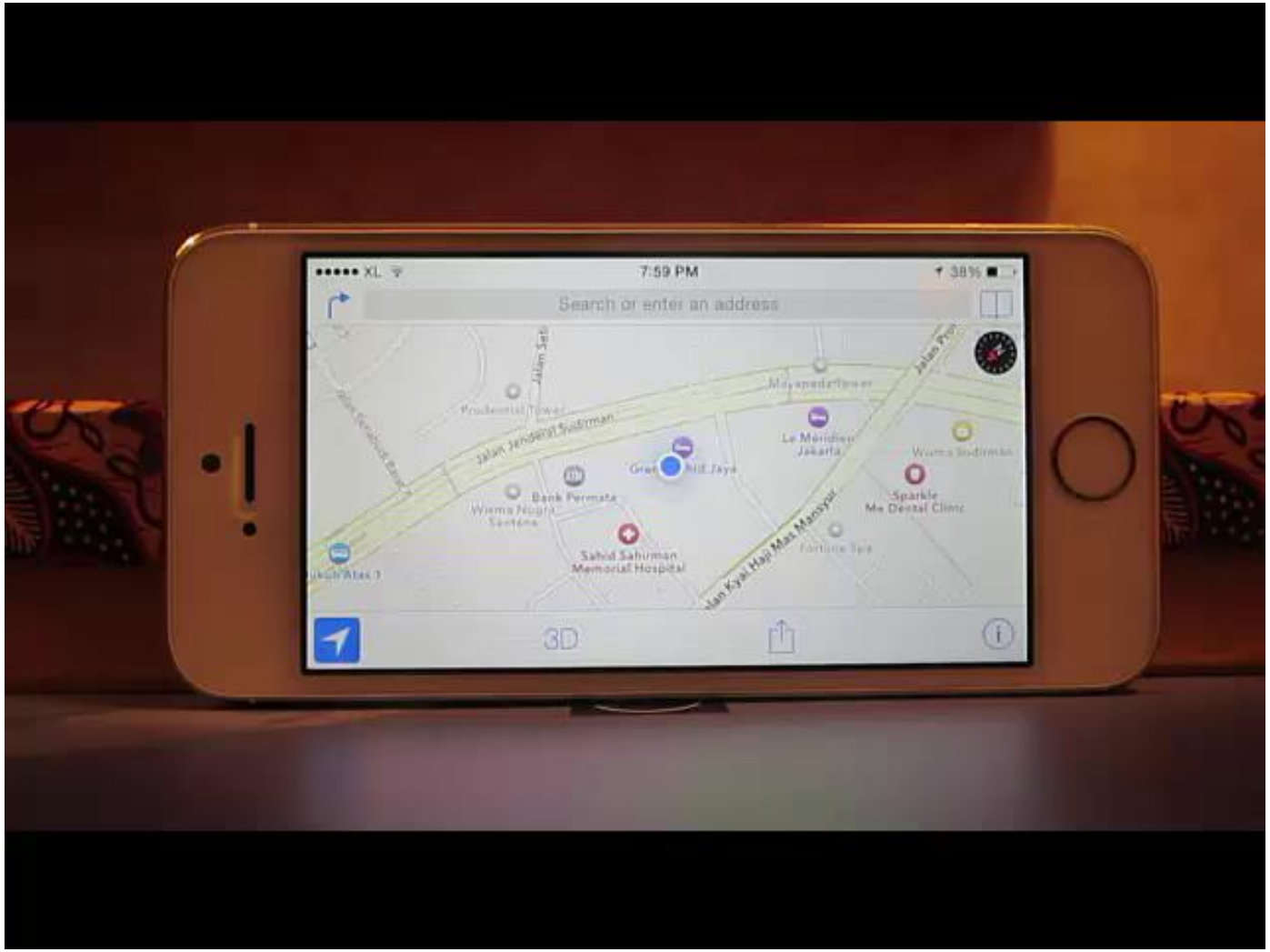


Mobile Phone Spoofing (Jakarta or Paris?)

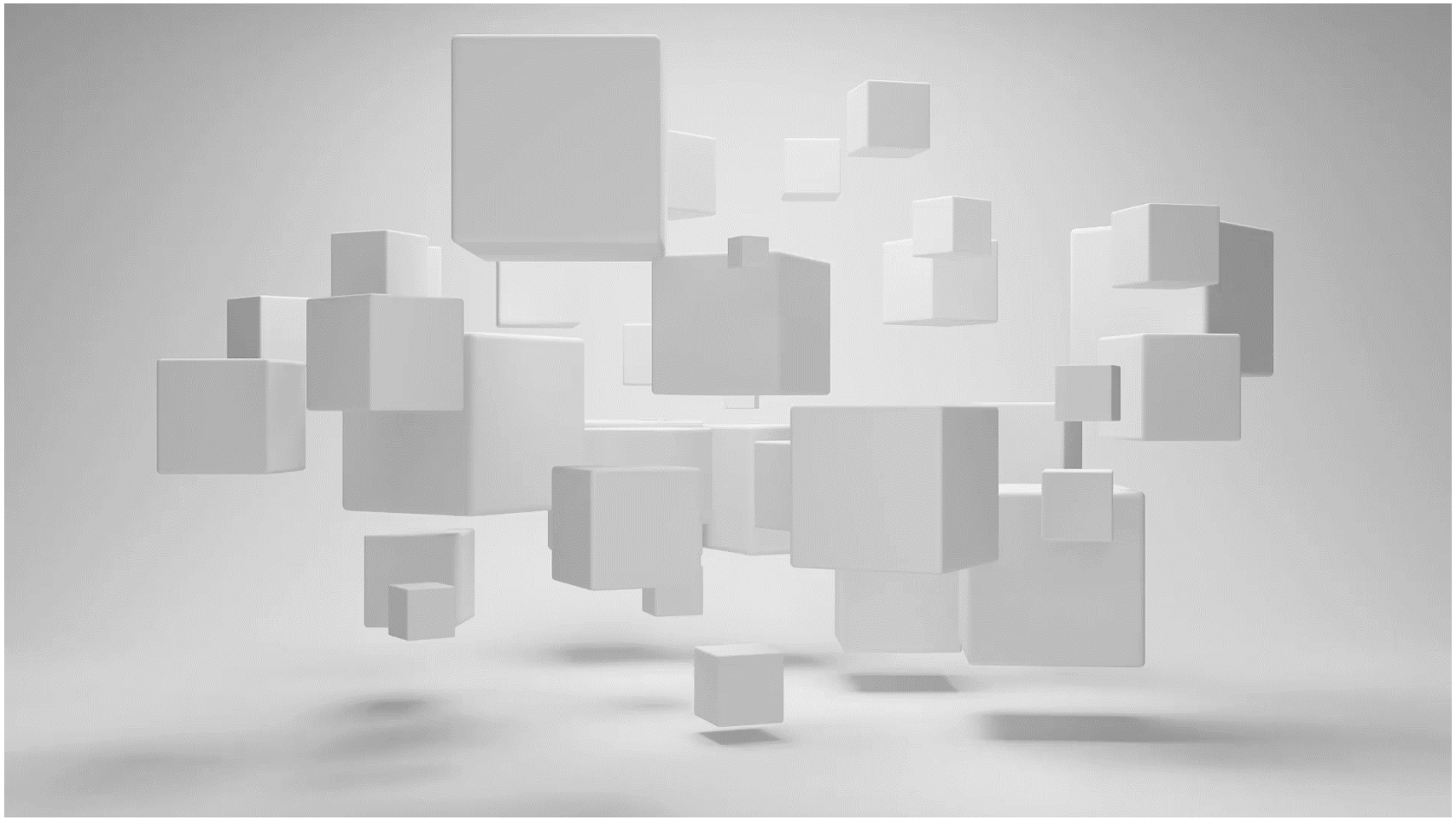
Spoofer was programmed to broadcast signal so that location data will changed to a driving car in Paris, Triumph Square



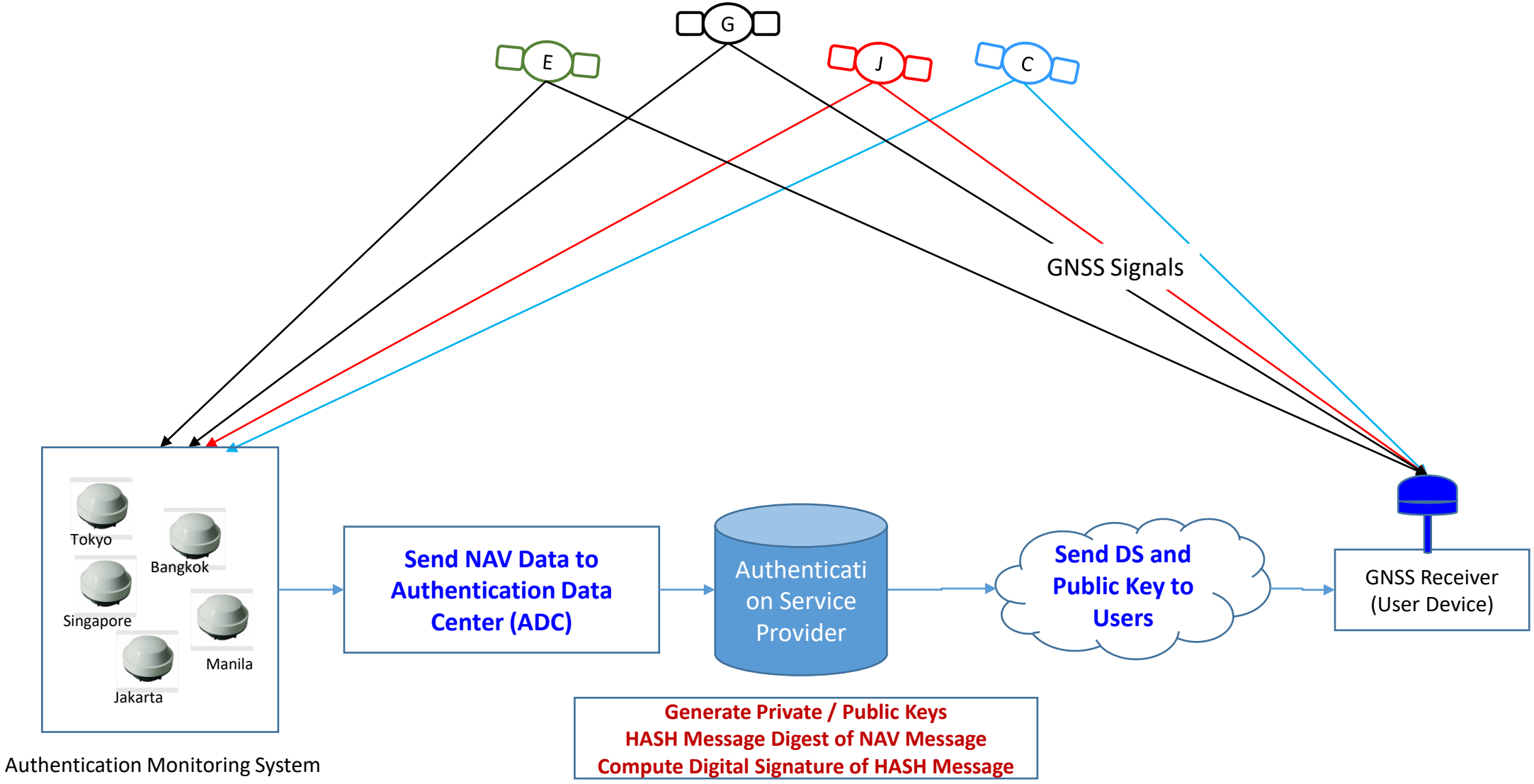




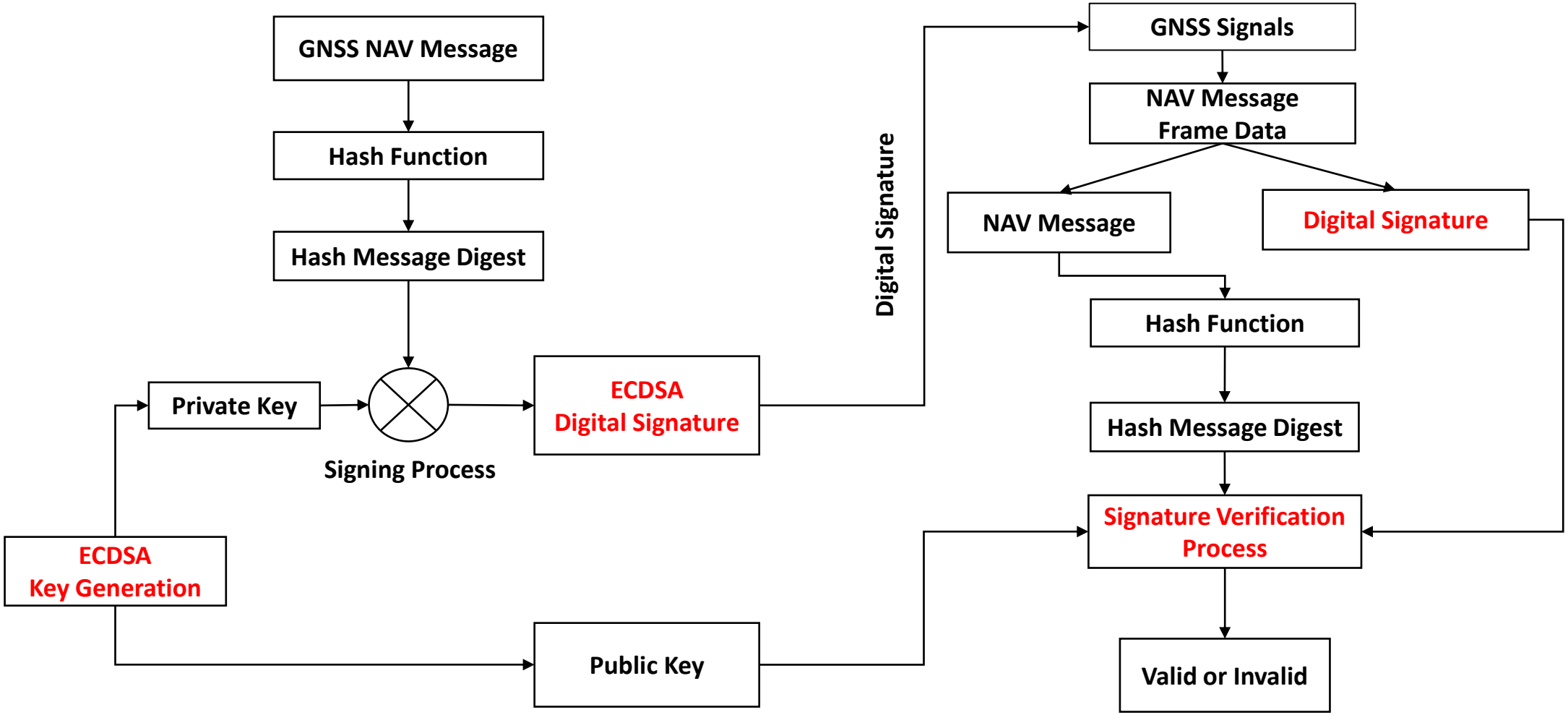
Spoofing a GPS Watch



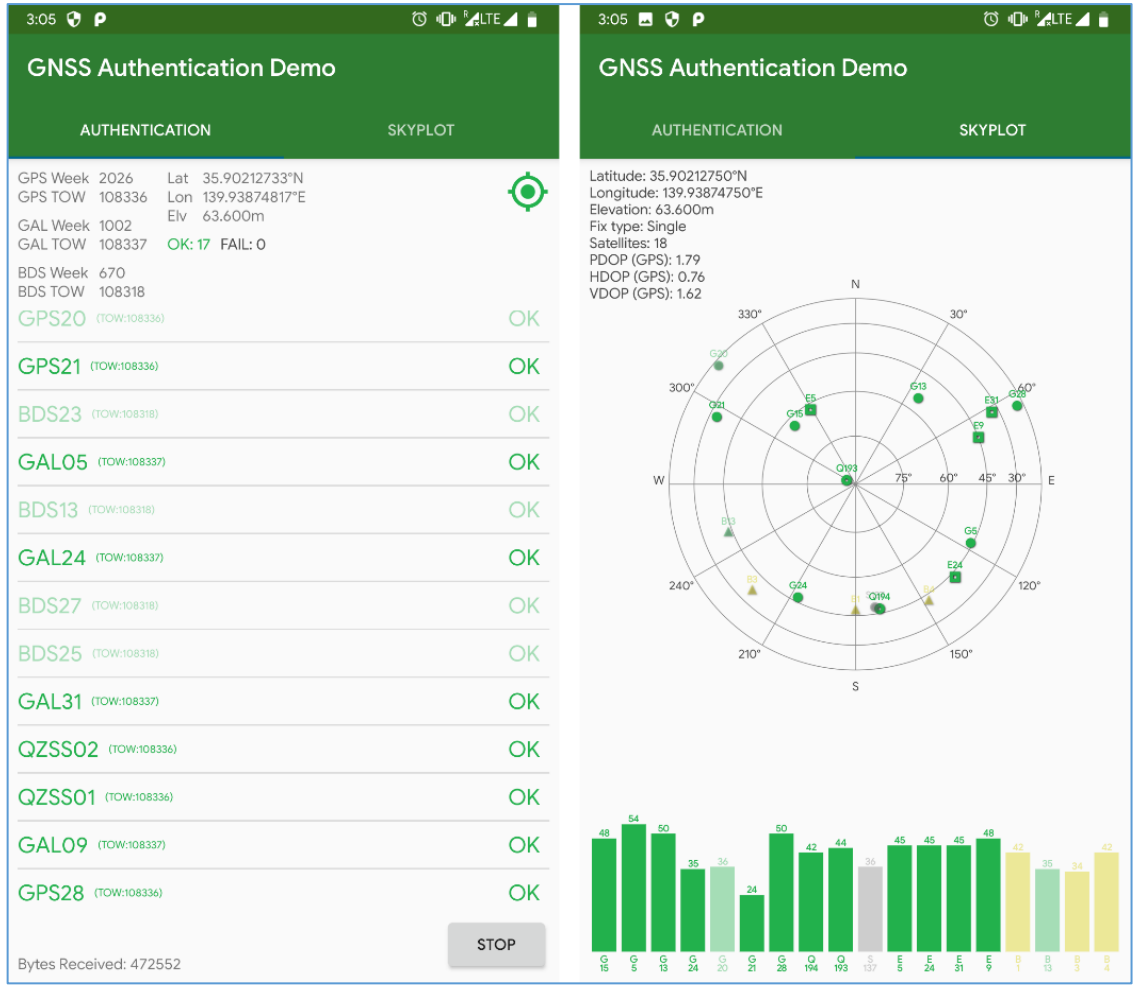
Internet-based GNSS Signal Authentication

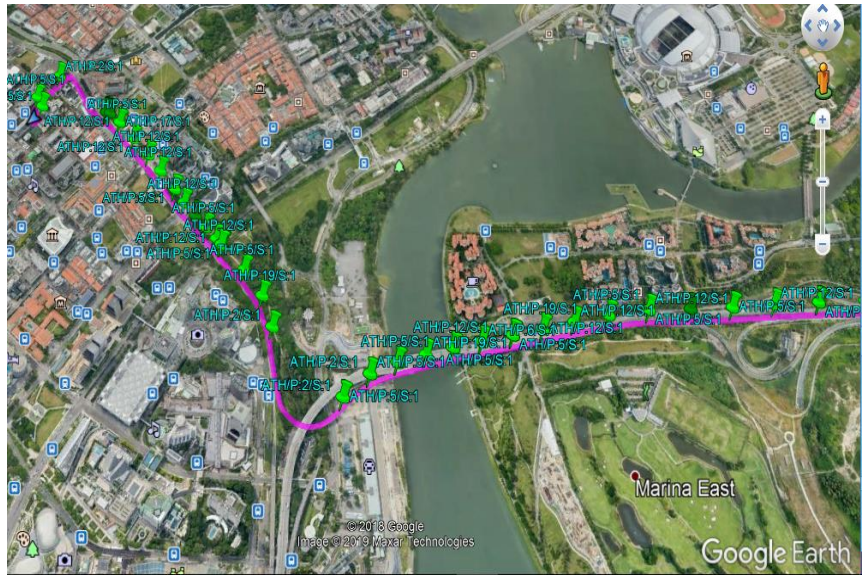


GNSS Signal Authentication Concept

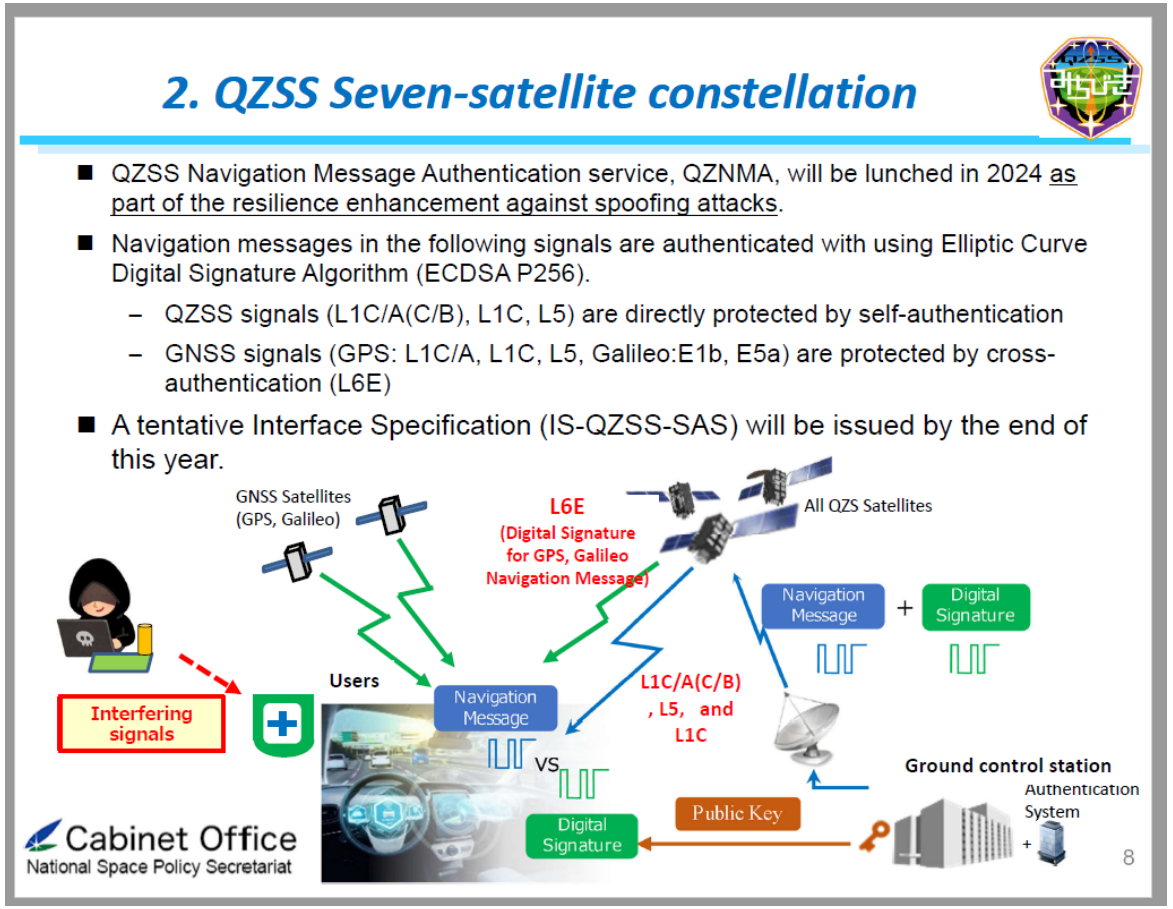


GNSS Signal Authentication (Prototype System)





GNSS Signal Authentication by QZSS



Trial transmission of the navigation message authentication

Mar.09,2021

Like 1 Tweet

National Space Policy Secretariat, Cabinet Office

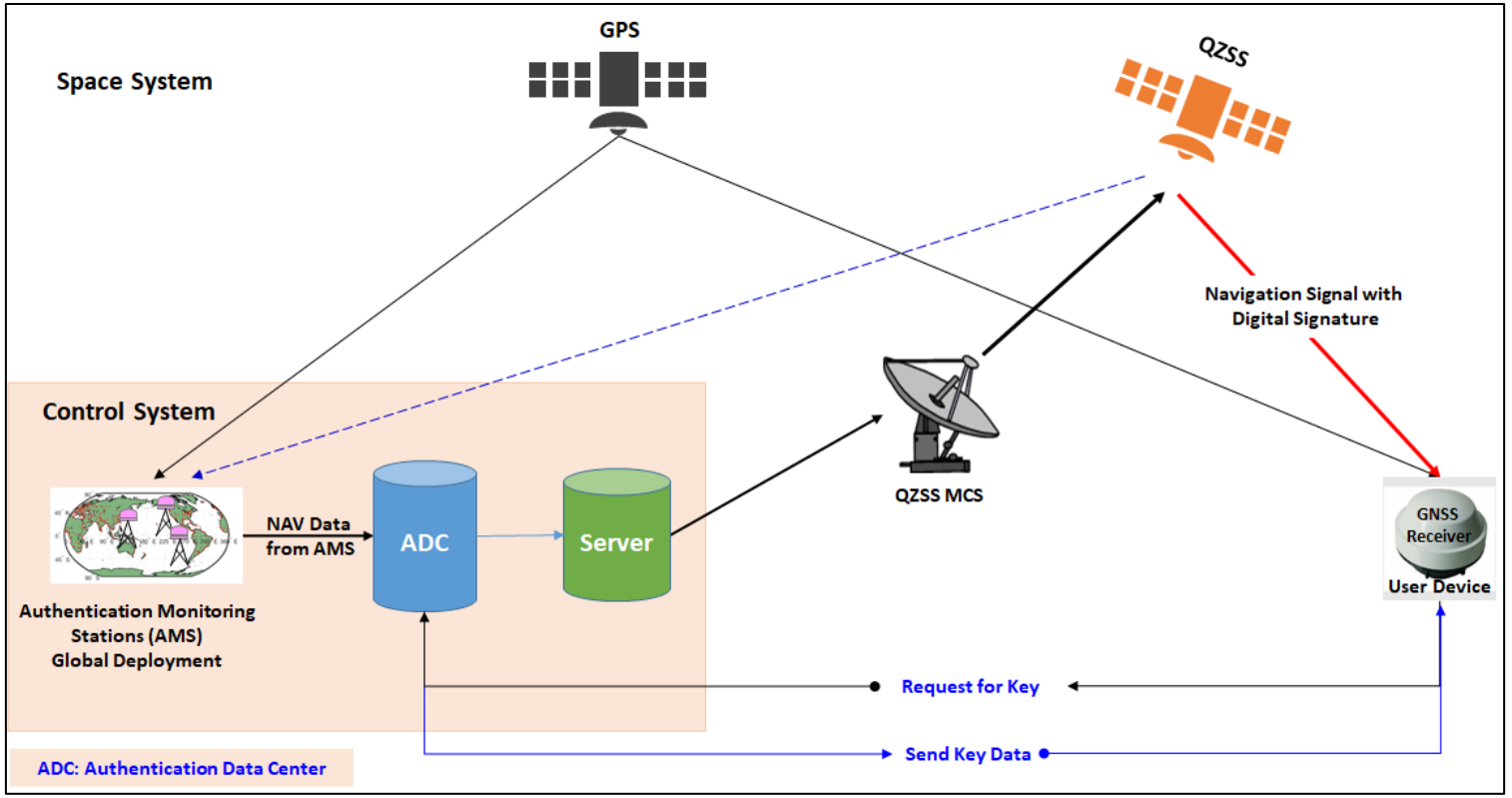
National Space Policy Secretariat is developing an authentication system for navigation messages in the QZSS signals, as a measure to ensure GNSS security against spoofing. In order to investigate the planned authentication message performance characteristics in actual environment and define some design parameters for system implementation, we will broadcast the test message on the L1C/A of QZS and evaluate its performance.

- Satellite : QZS1, 2, 3, 4
- Trial period : After March 11, 2021 to Early April 2021

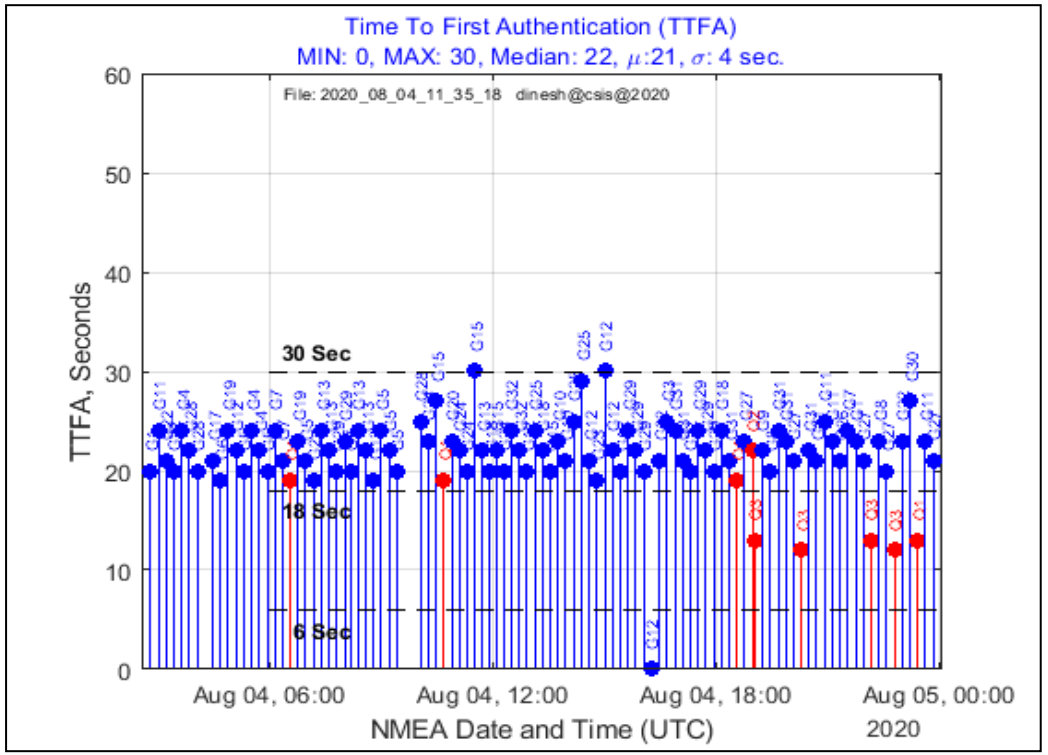
This test authentication message will be broadcasted in the currently unused ID defined as "Test mode" in Subframe5 of the LNAV message. Please refer to IS-QZSS-PNT-004 Table 4.1.2-2 for more detail.

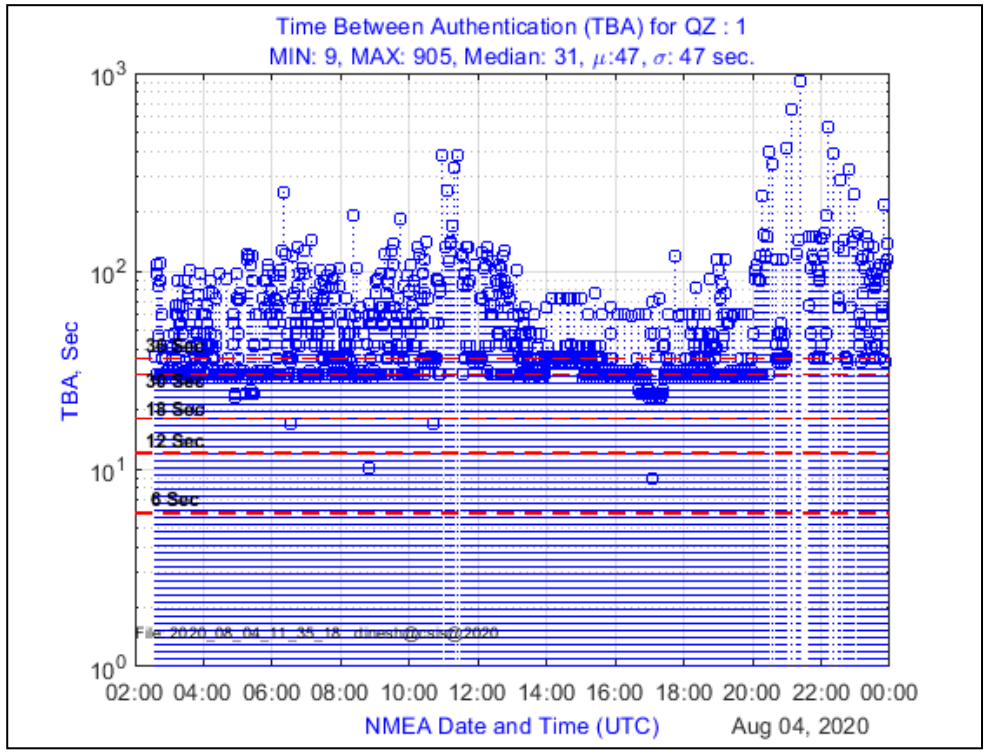
https://qzss.go.jp/en/overview/notices/qzss_210309.html

GPS and QZSS L1C/A Signal Authentication using QZSS L5S Test Signal

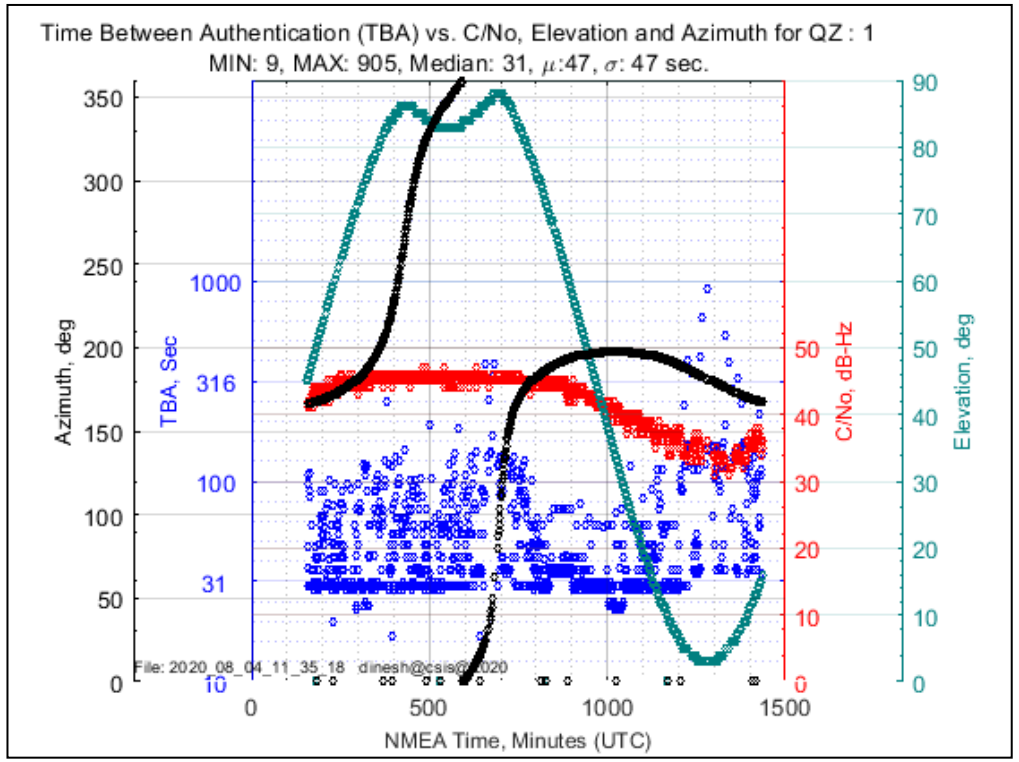


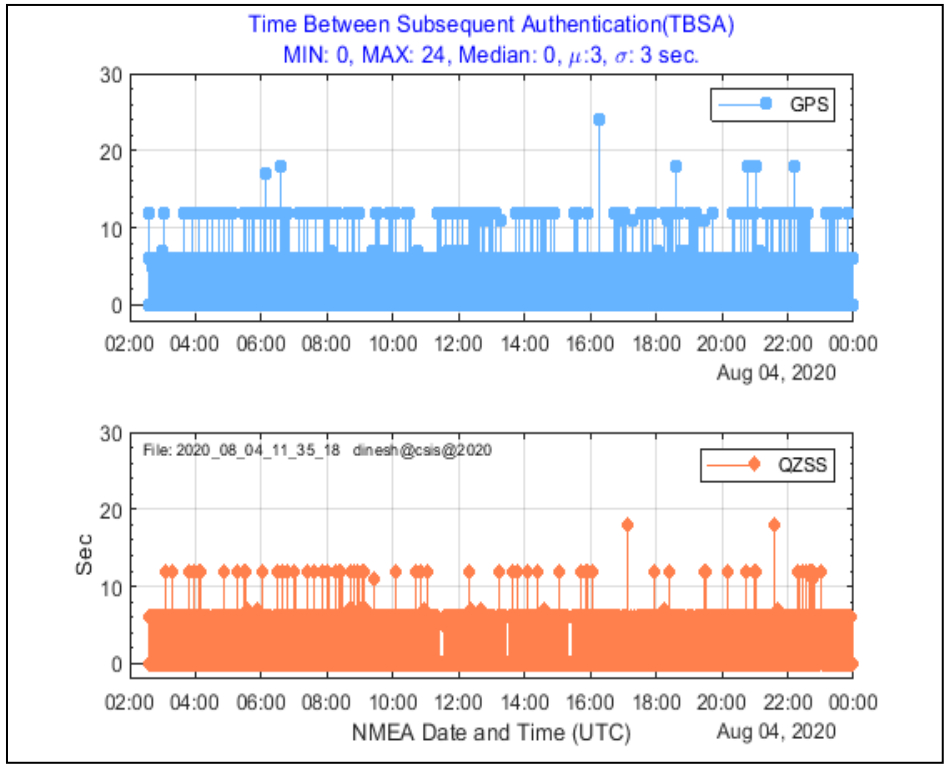
Signal Authentication: TTFA and TBA





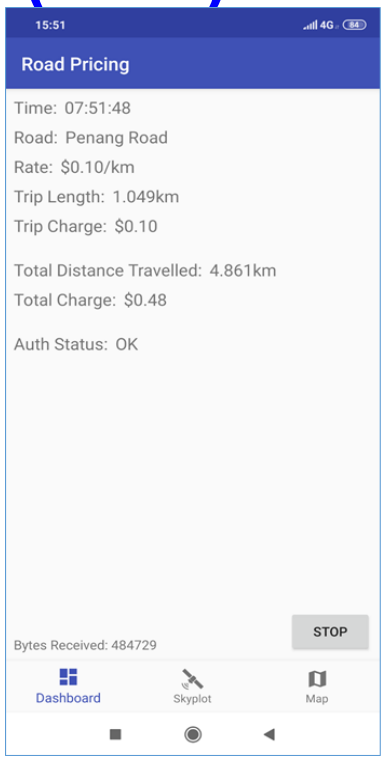
Signal Authentication: TBA

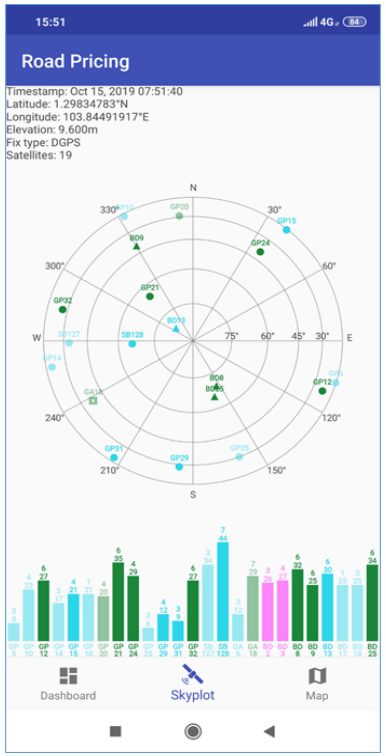


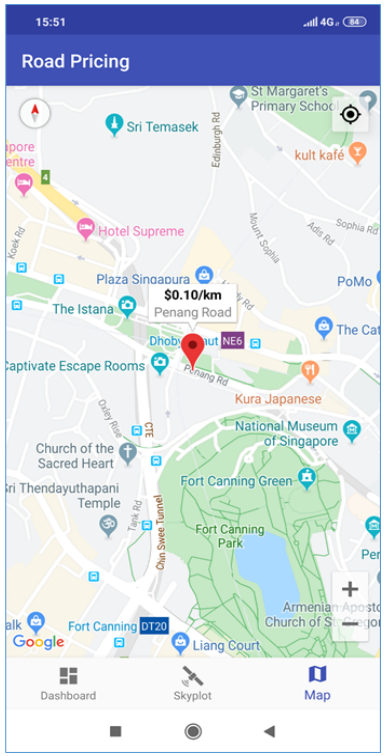


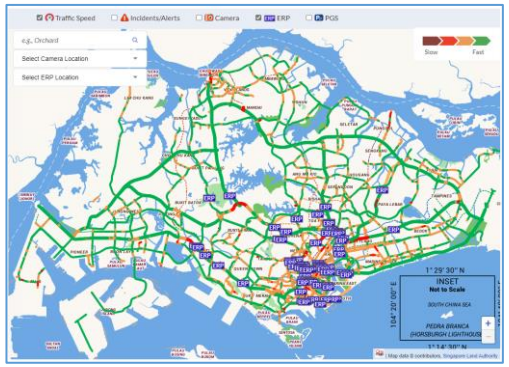
Dynamic Road Pricing (DRP) based on GNSS

- Dynamically charge for road usage
  - Pricing is variable and based on
    - Distance, time, location,
    - Vehicle type, lane and occupancy
    - Traffic congestion condition
- Reward road users for using alternate routes to avoid congested route
  - Payback the drivers who help to minimize traffic congestion
- No Physical Toll Gates
  - GPS-based system is used for Location, Distance and Lane occupation
  - Can be implemented on any road section
    - Not limited to only highways, express ways or toll roads
- Global Seamless Implementation
  - The same system can be implemented globally
  - The same In-vehicle device can be used globally
    - Single system for smooth cross-border operation
    - Once a border is crossed, charging or rewarding rates can be updated automatically









Dinesh Manandhar, The University of Tokyo, Japan, dinesh@csis.u-tokyo.ac.jp

References

- My Homepage
  - https://home.csis.u-tokyo.ac.jp/~dinesh/
- GNSS Training related materials
  - Lecture Notes, Software Link, Sample Data for RTK Exercise
  - https://home.csis.u-tokyo.ac.jp/~dinesh/GNSS_Train.htm
- Low-Cost High-Accuracy Receiver System
  - Software Request Page (RTKDROID, MAD-WIN, MAD-PI)
  - https://home.csis.u-tokyo.ac.jp/~dinesh/LCHAR.htm
- Multi- GNSS Asia, RPD (Rapid Prototype Development) Challenge
  - https://www.rpdchallenge.com/
- GNSS Webinar Page
  - https://home.csis.u-tokyo.ac.jp/~dinesh/WEBINAR.htm
- Facebook
  - https://www.facebook.com/gnss.lab/