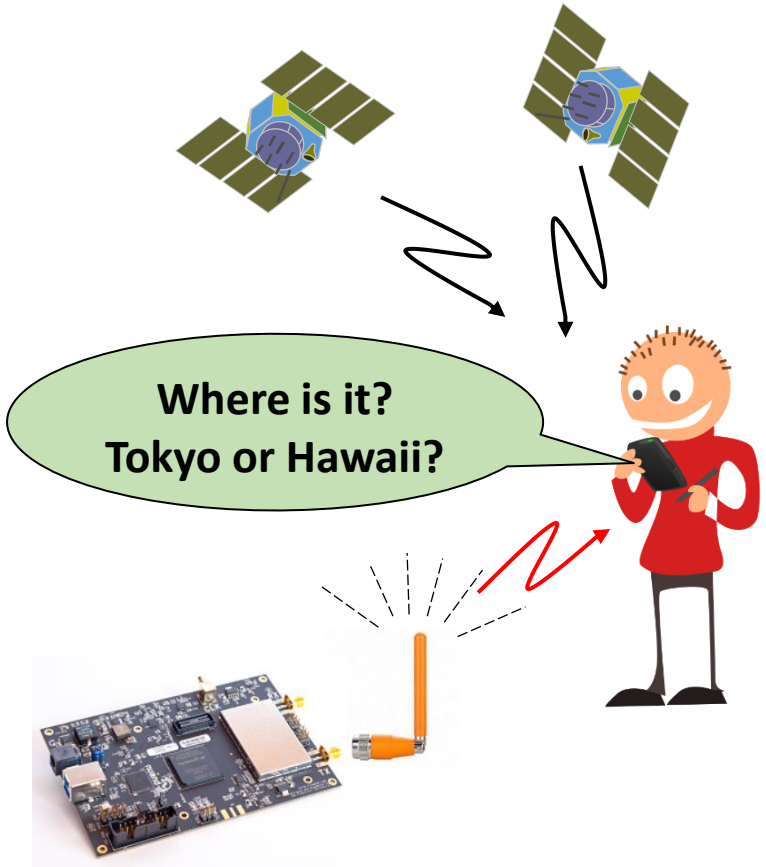
GNSS SPOOFING ATTACKS, MITIGATION METHODS AND IT'S APPLICATION IN DYNAMIC ROAD PRICING

Dinesh MANANDHAR
Associate Professor (Project)
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
- Putting a Magnet beside a Compass



Spoofer

TOKYO Or Hawaii?

Tomorrow Never Dies

007

This movie is all about GPS Spoofing

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

Link to "Tomorrow Never Dies" Movie Clips

Bing Videos
https://www.bing.com/videos/riverview/relatedvideo?q=Tomorrow%20Never%20Dies%20Full%20Movie&mid=FB3A2EA6FBFDABC18121FB3A2EA6FBFDABC18121&ajaxhist=0
Watch at 1:44 – 2:05

- Looks like an American encoder. They use it to control their navigation satellites, the GPS system.

Bing Videos
https://www.bing.com/videos/riverview/relatedvideo?q=Tomorrow%20Never%20Dies%20Full%20Movie&mid=078335262EBCF0A56672078335262EBCF0A56672&ajaxhist=0
Watch 0:00 – 0:40

- GPS systems do not lie.
- But, our Singapore station picked up a mysterious signal on the GPS frequency at the time of the attack that sent our ship off the course
- Where exactly this mysterious GPS signal is coming from?

Bing Videos
https://www.bing.com/videos/riverview/relatedvideo?q=Tomorrow%20Never%20Dies%20Full%20Movie&mid=8D882D503274AF6410298D882D503274AF641029&ajaxhist=0
0:40 – 3:20

- It's the missing encoder. How did you get it? Did somebody use it to send the ship off the-course?
- Kinda like putting a magnet beside a compass?
- Somebody tampered with your encoders

Spoofing Methods and Types

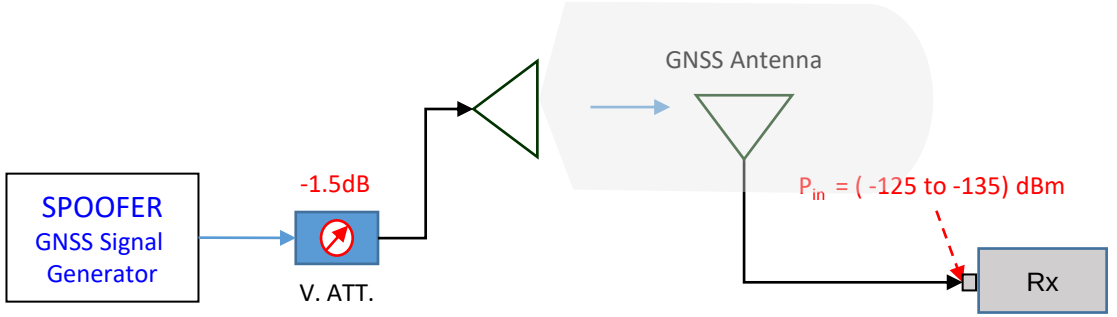
Spoofing Methods	
Direct Attack	Connect the target device directly by a cable Spoof signal is not transmitted by antenna
Over-The-Air Attack (OTA)	Transmit spoof signal over-the-air

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

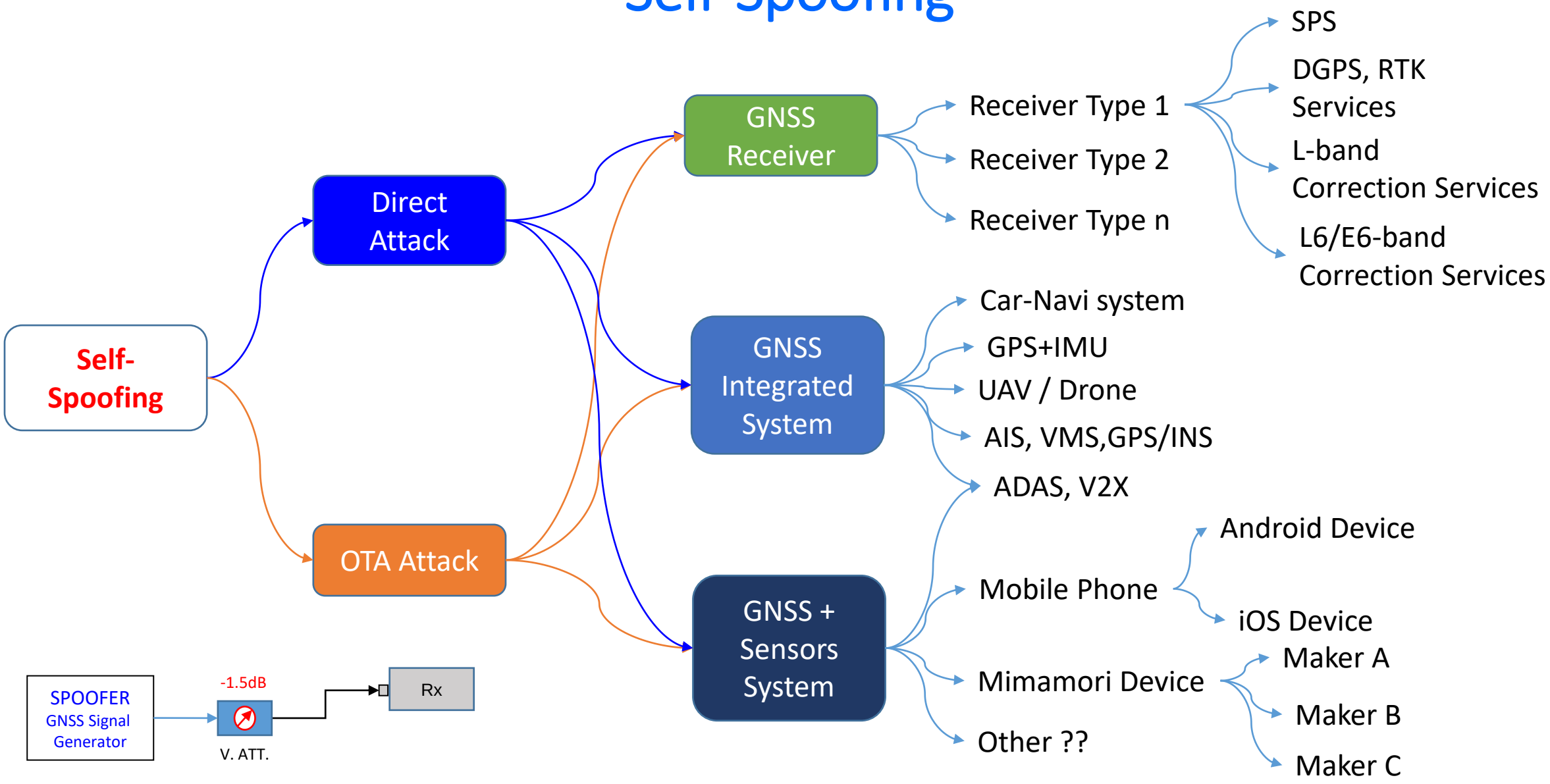
Self-Spoofing

OTA (Over The Air) Attack



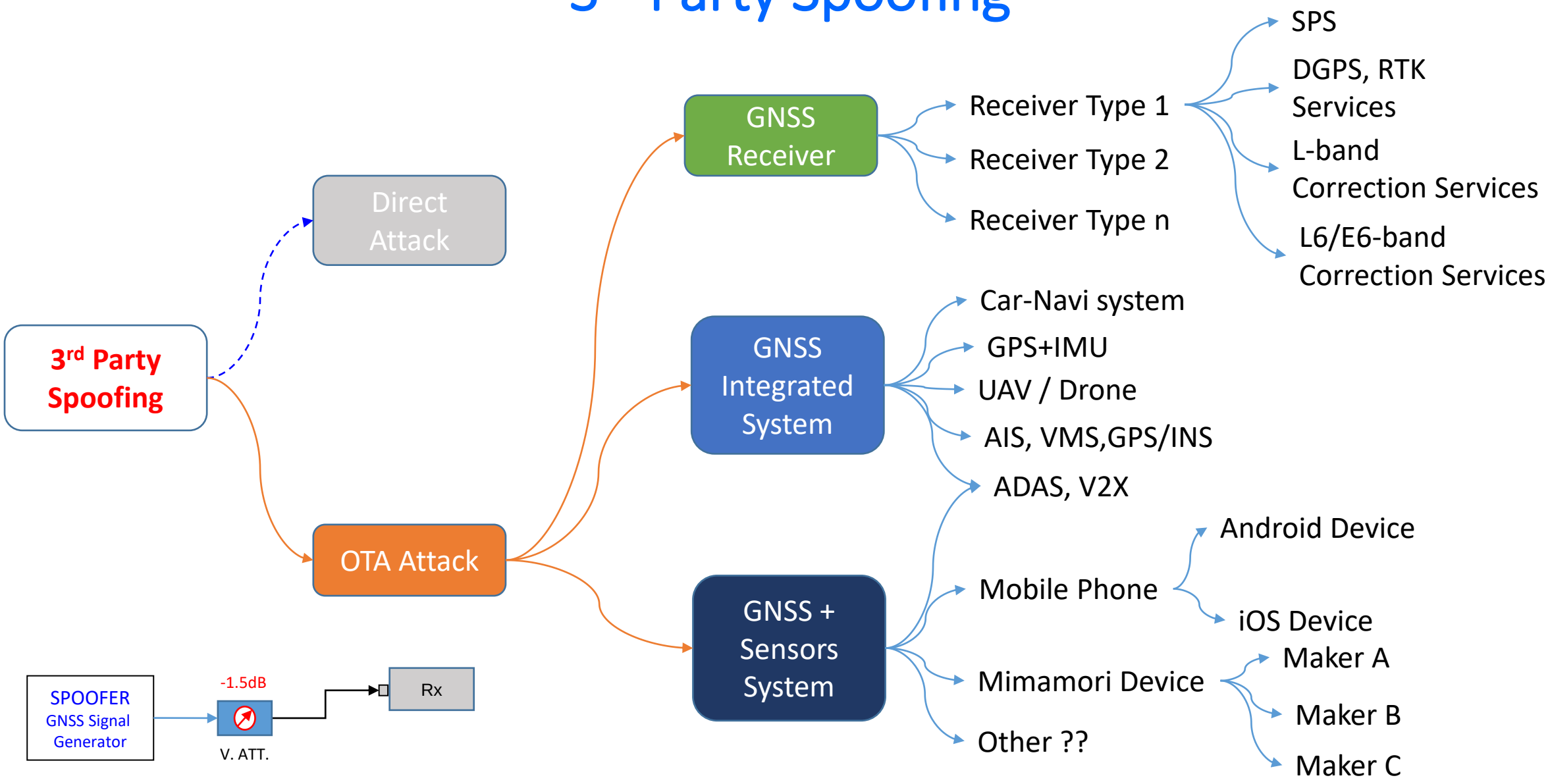
3rd Party Spoofing

Self-Spoofing



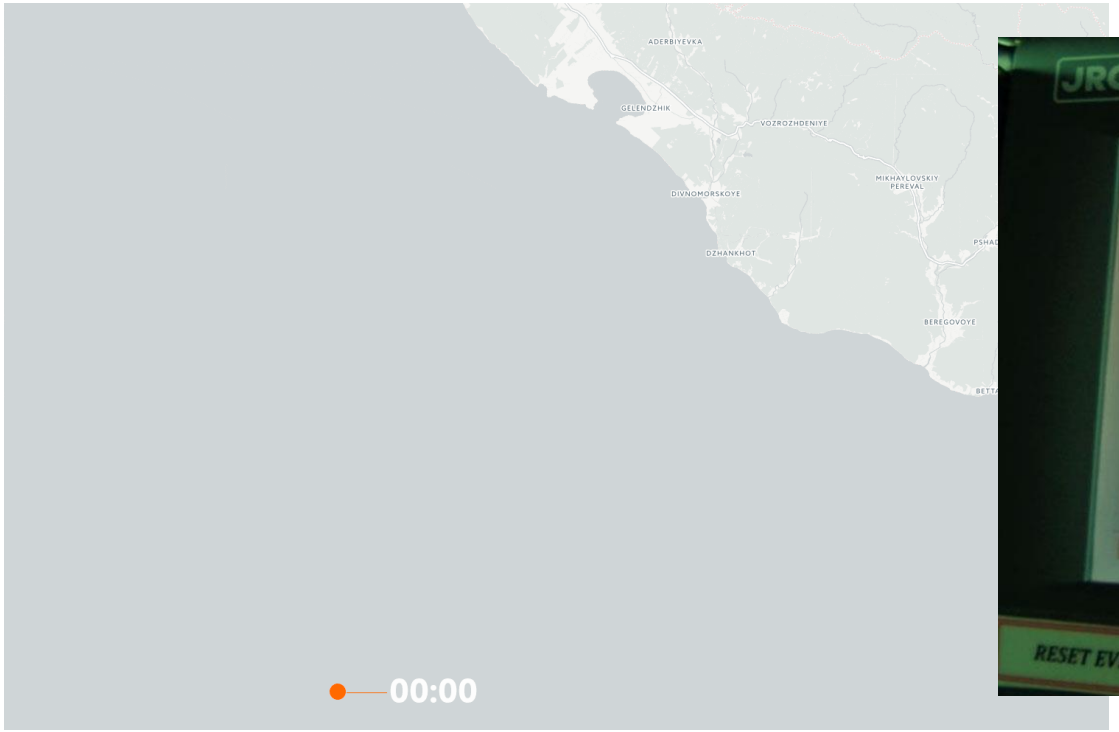
Dinesh Manandhar, The University of Tokyo, Japan, dinesh@csis.u-tokyo.ac.jp

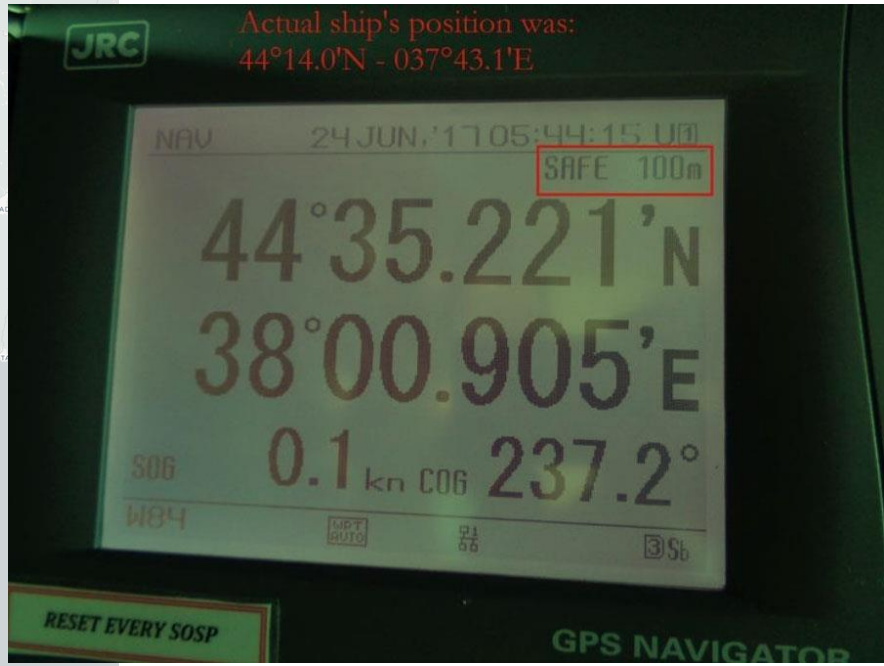
3rd Party Spoofing



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

Spoofing Incident in Black Sea



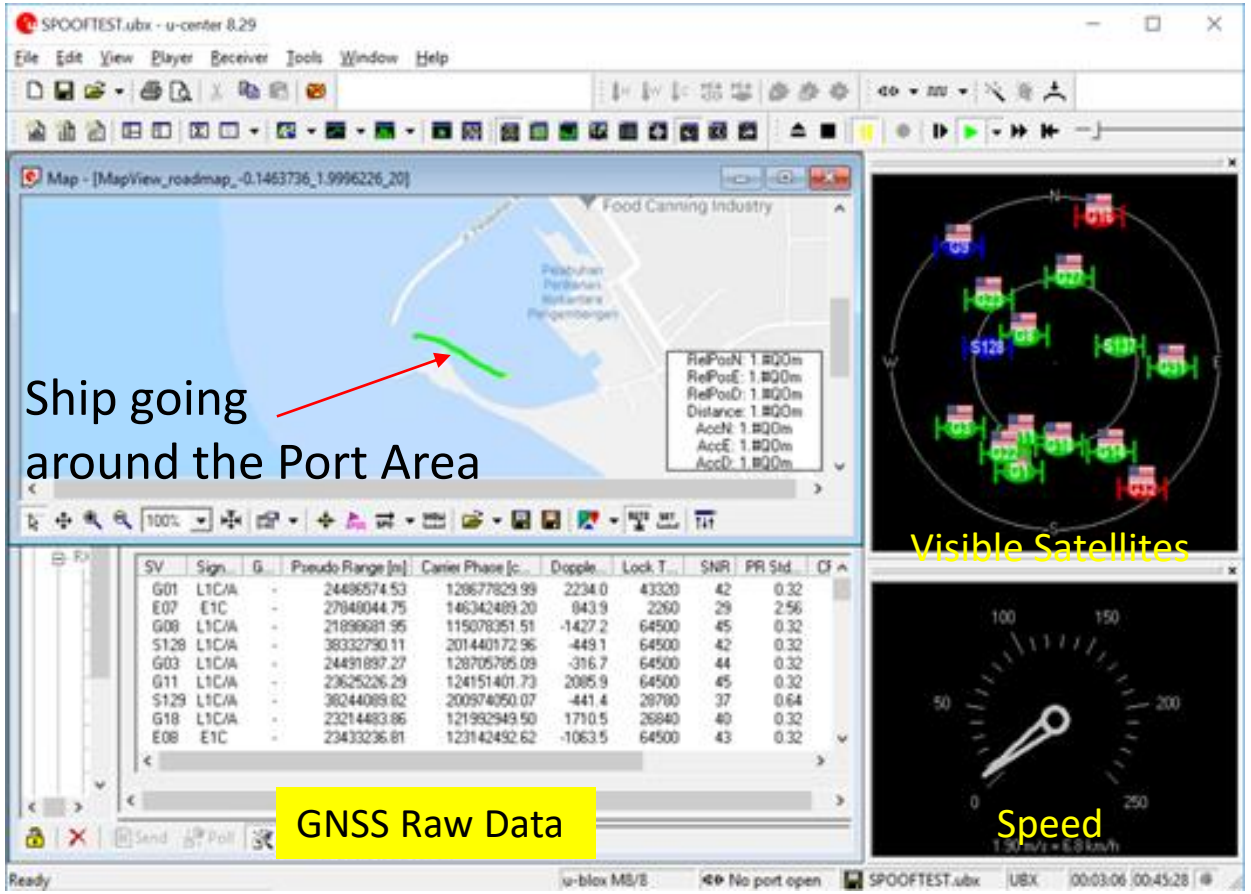


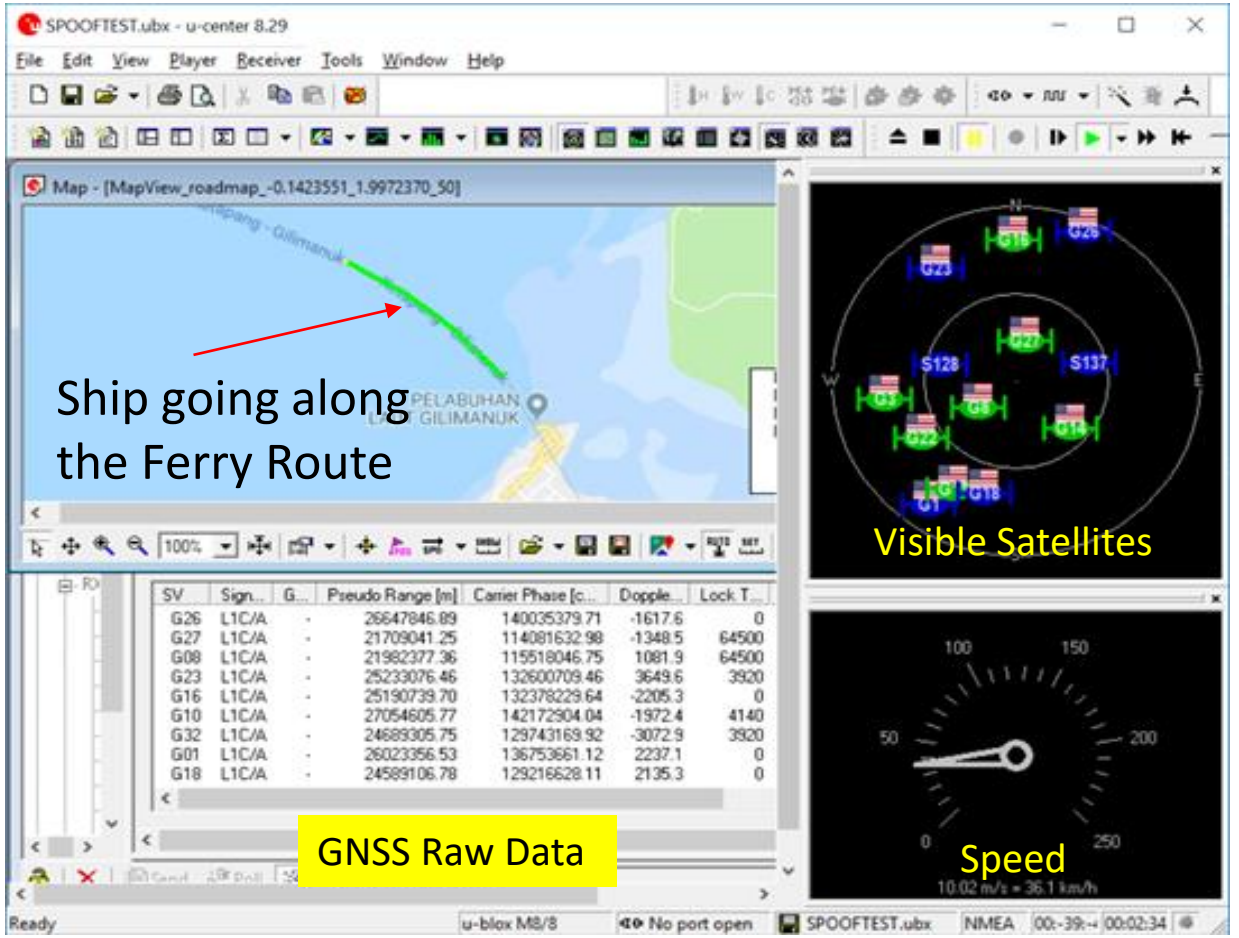
These are actually recorded data

SPOOFing a Car: Is he driving the car?

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

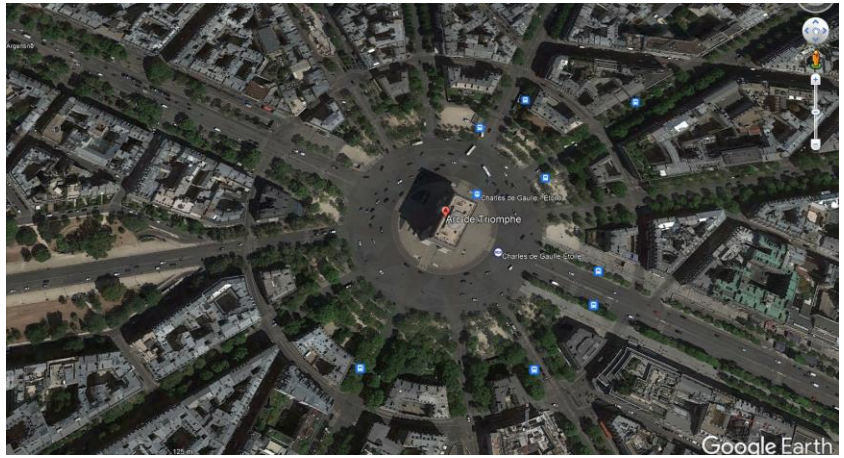
Can you identify TRUE Data and SPOOF Data?

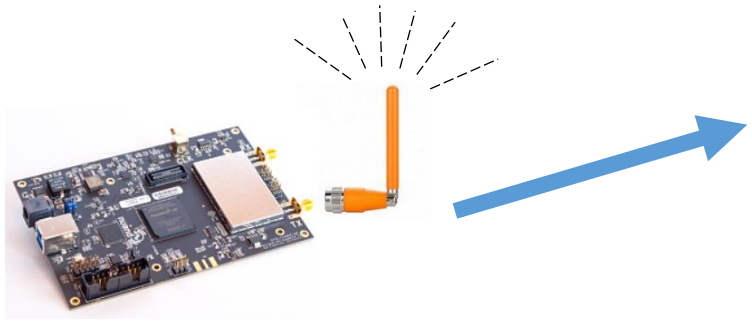


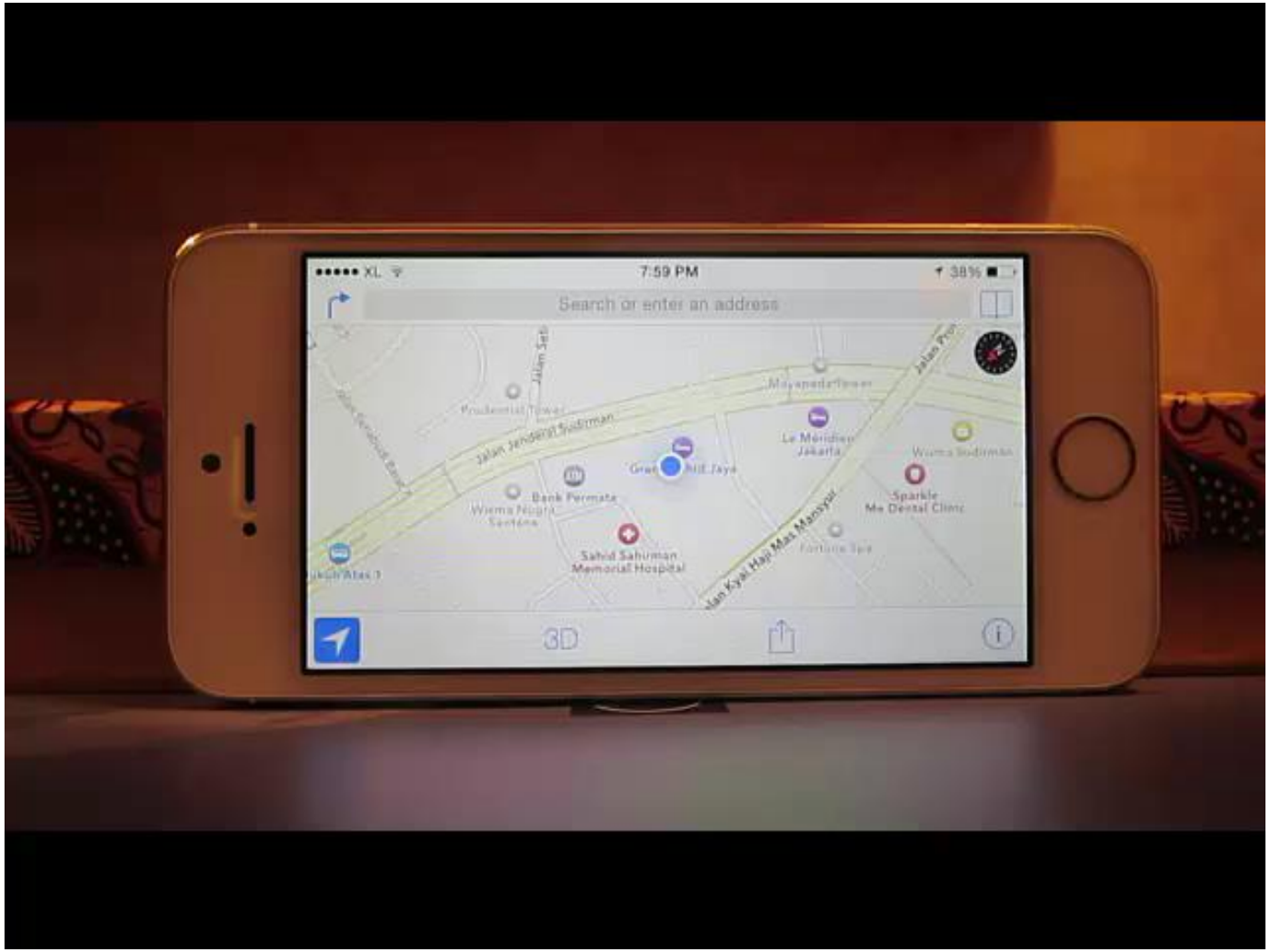


Mobile Phone Spoofing (Jakarta or Paris?)

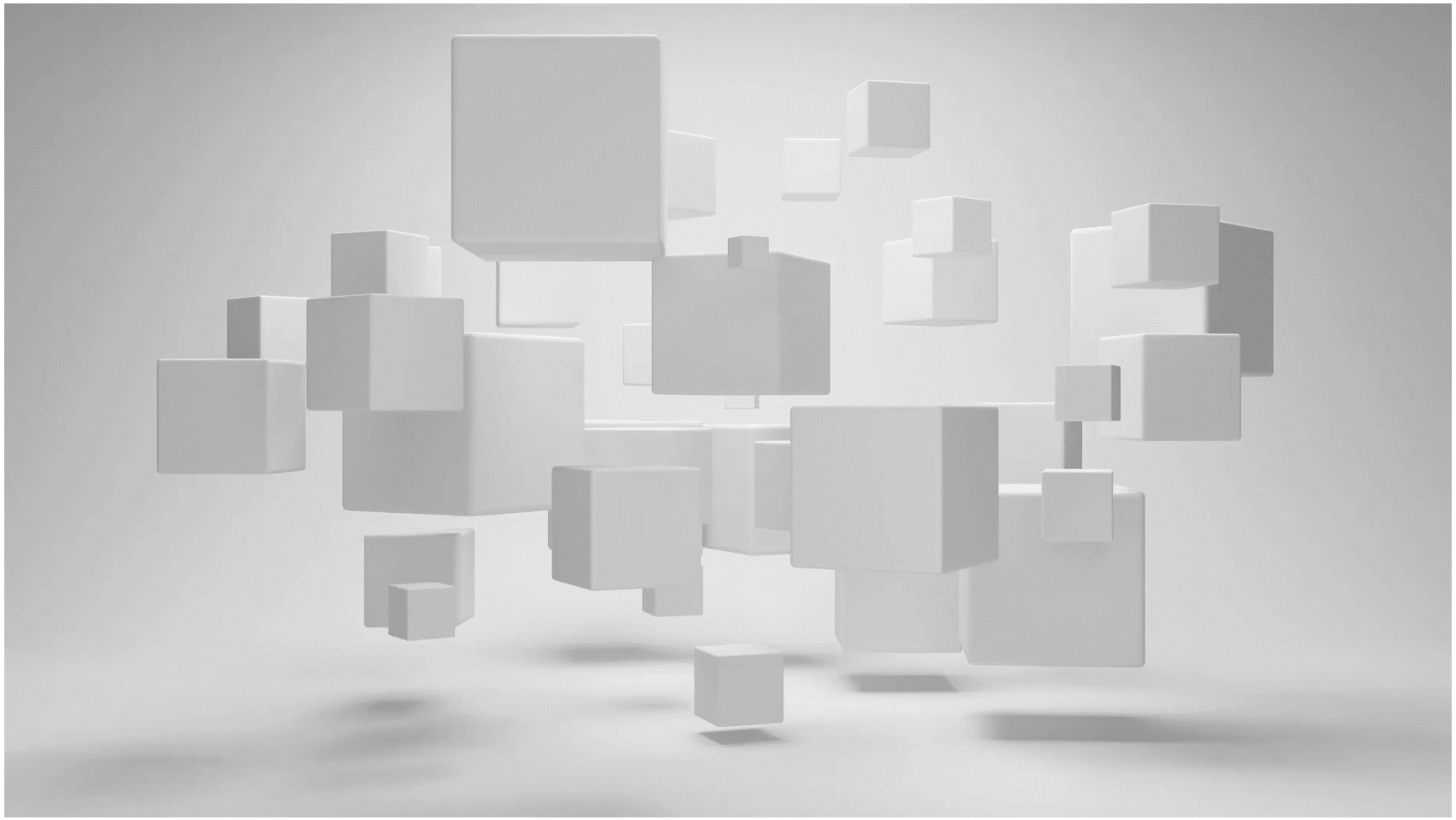
Spoofer was programmed to broadcast signal so that location data will changed to a driving car in Paris, Triumph Square





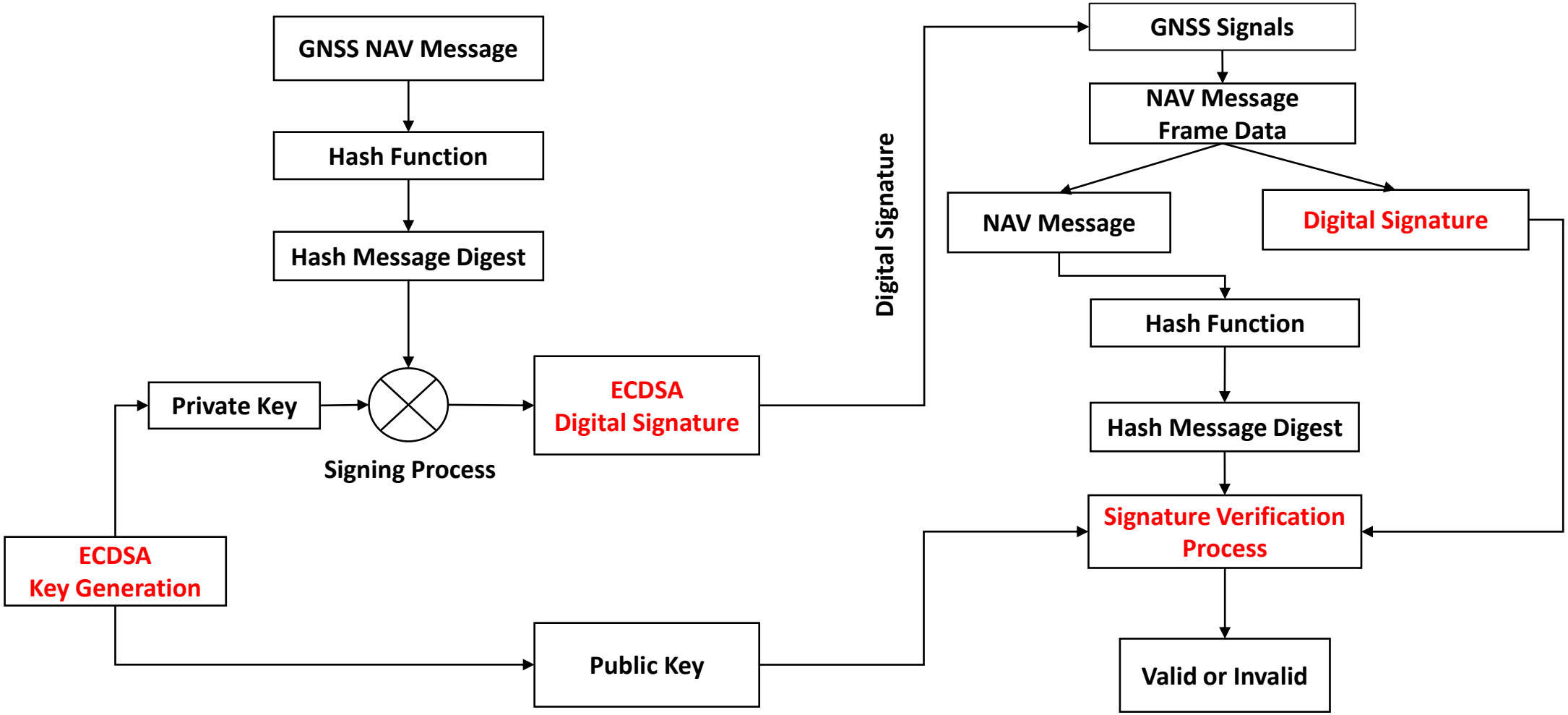


Spoofing a GPS Watch

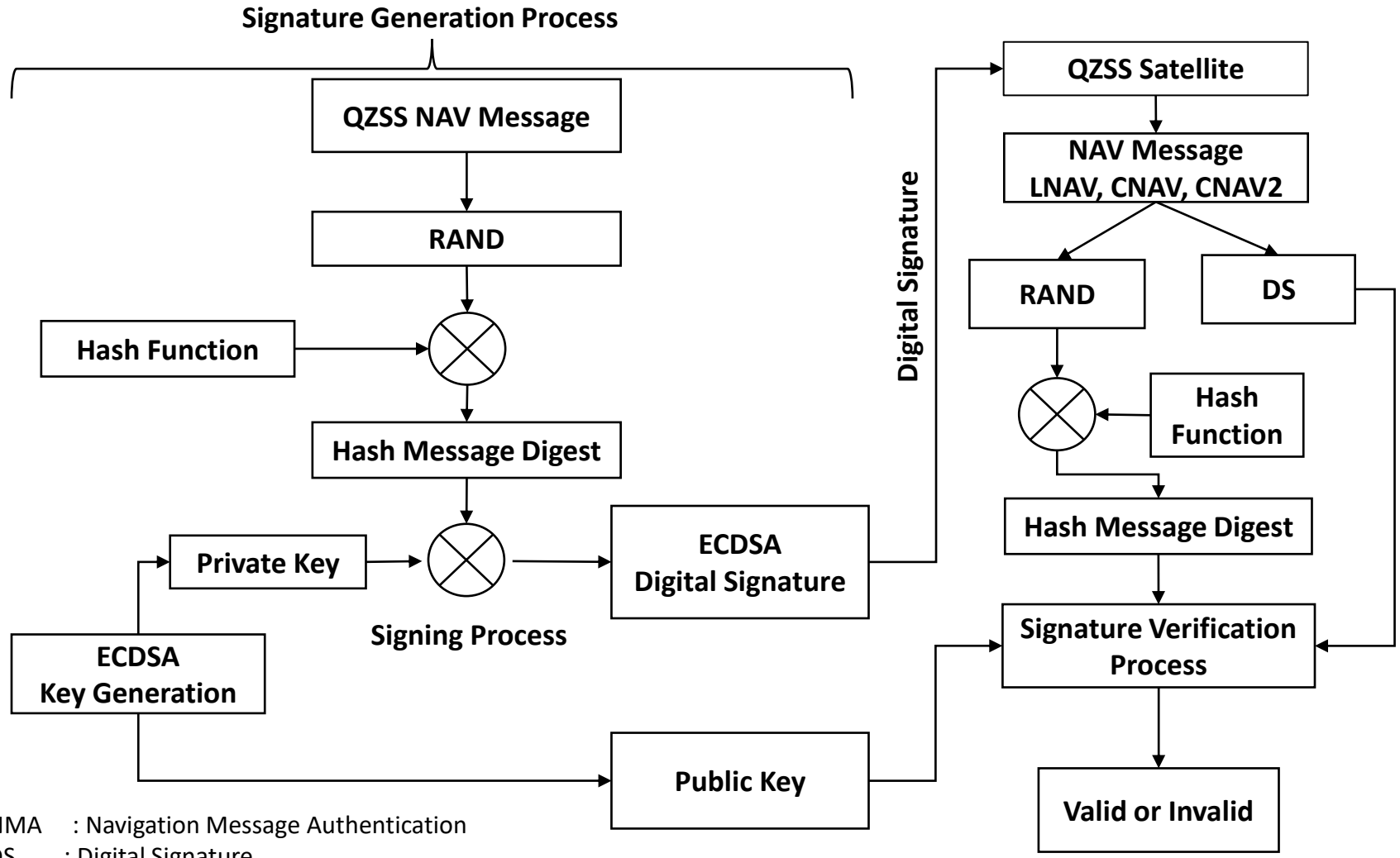


Dinesh Manandhar, The University of Tokyo, Japan, dinesh@csis.u-tokyo.ac.jp

Concept of GNSS Signal Authentication

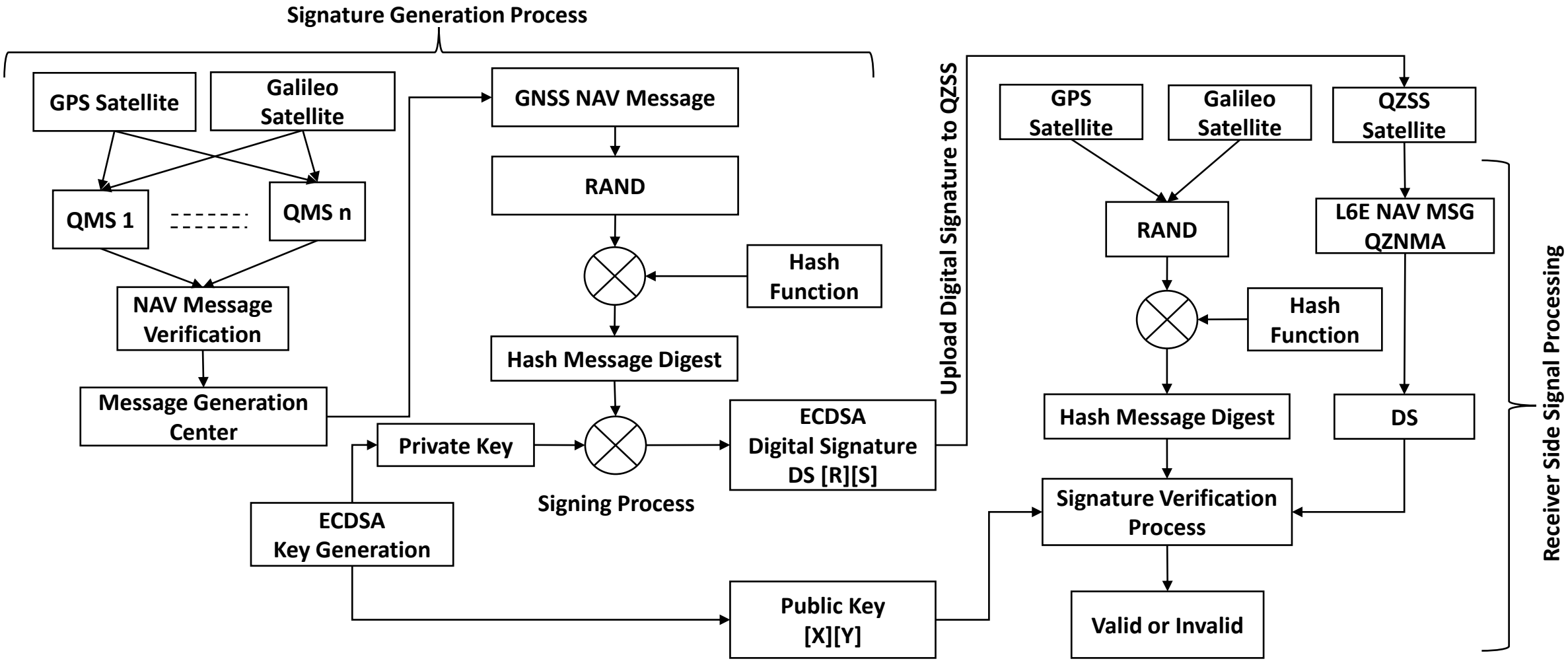


QZSS Signal Authentication System



NMA : Navigation Message Authentication
DS : Digital Signature
ECDSA : Elliptical Curve Digital Signature Authentication
NAV : Navigation
QMS : QZSS Monitoring Station
RAND : Reference Authentication Navigation Data

GNSS Signal Authentication System using QZSS

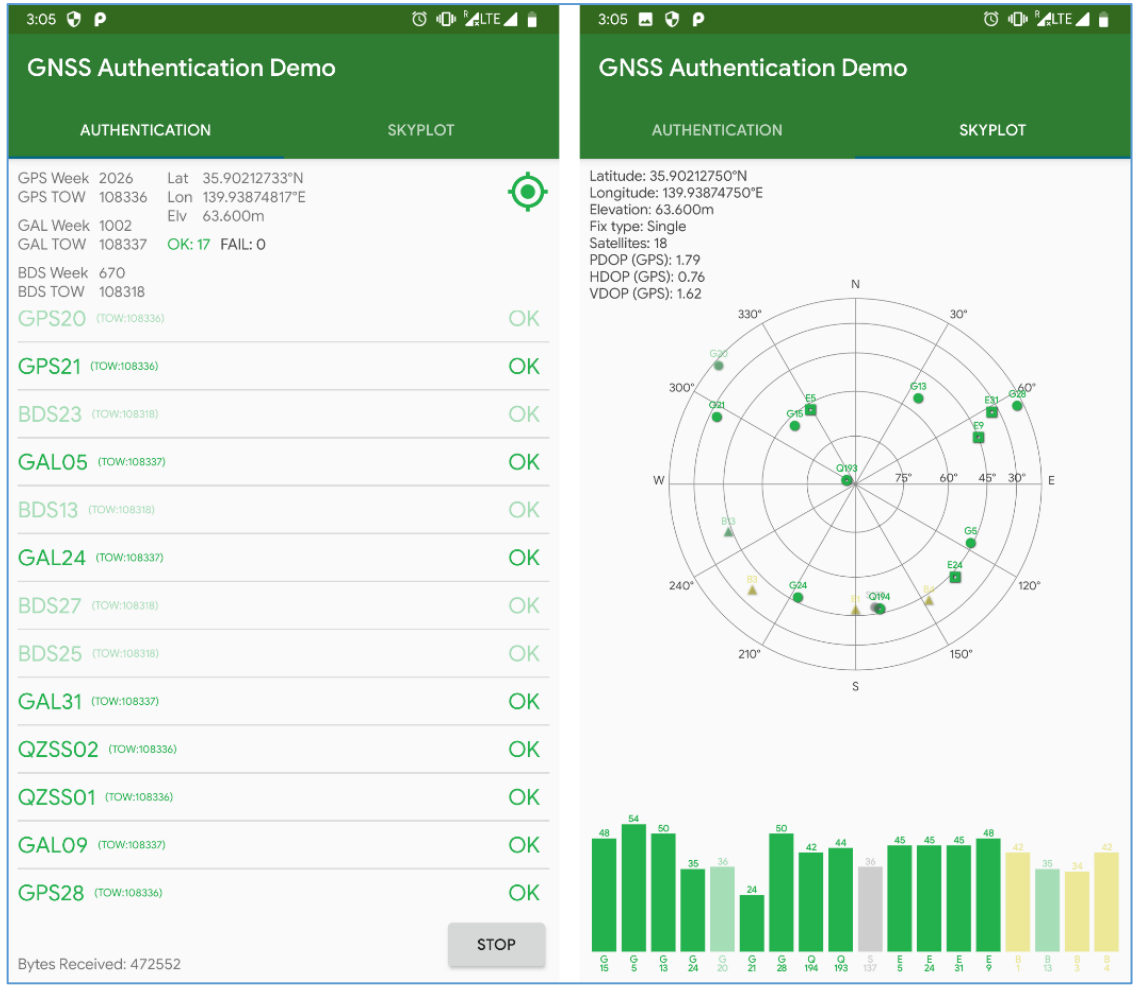


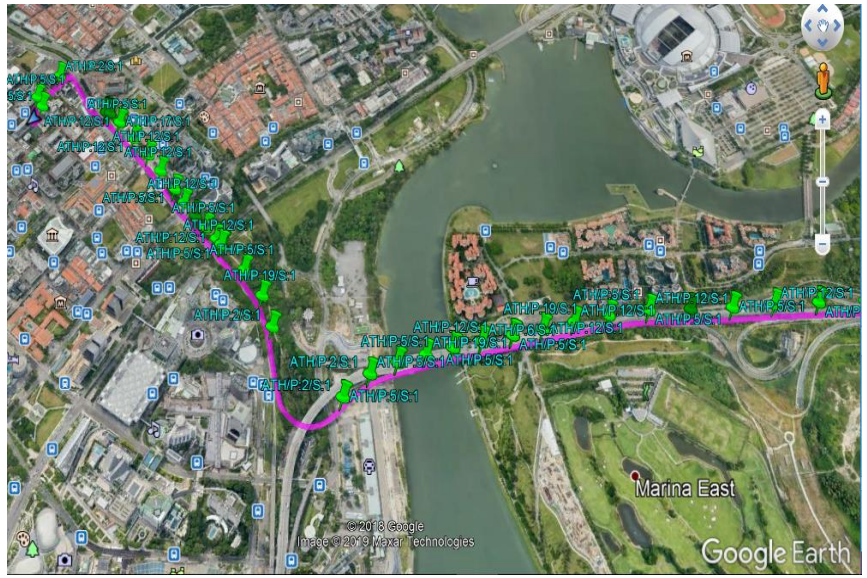
AMS : Authentication Monitoring Station
NMA : Navigation Message Authentication
DS : Digital Signature

ECDSA : Elliptical Curve Digital Signature Authentication
NAV : Navigation
RAND : Reference Authentication Navigation Data
QMS : QZSS Monitoring Station

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

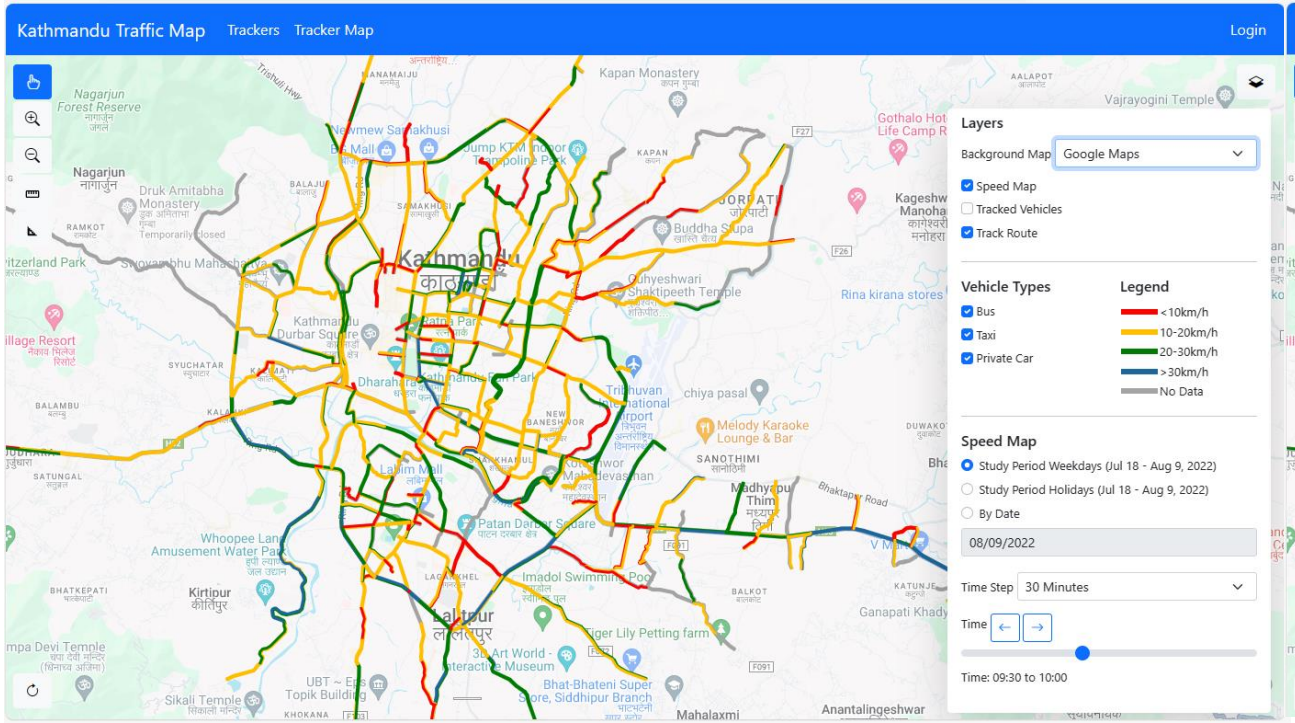
GNSS Signal Authentication



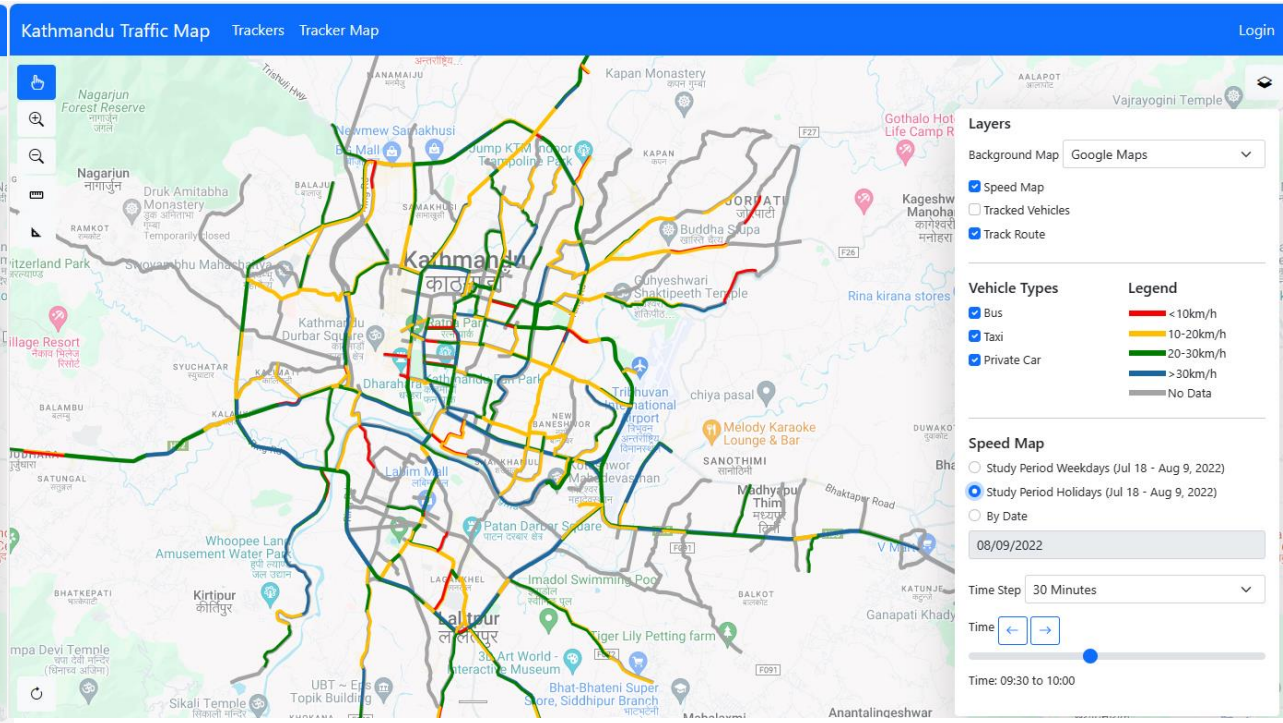


Traffic Congestion poses a Serious Impact on Daily Life

Working Days: July 18 – August 9, 2022



Holidays: July 18 – August 9, 2022



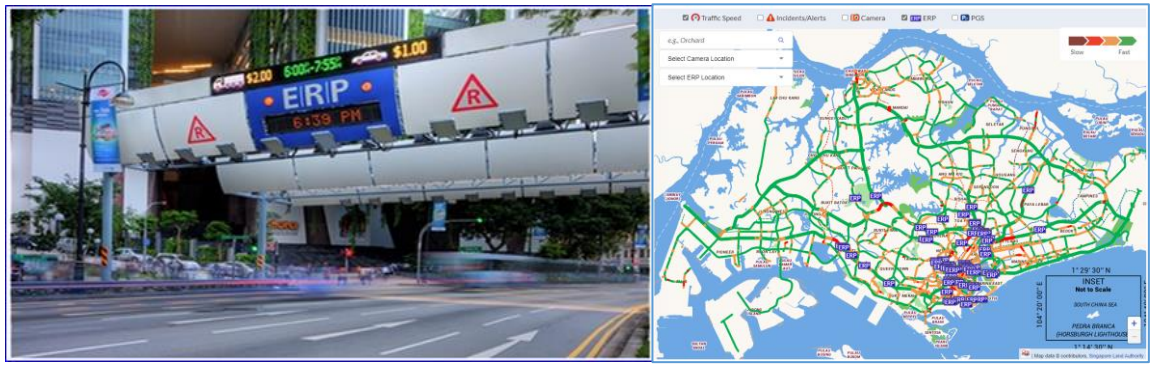
Data Analysis by A. Malla

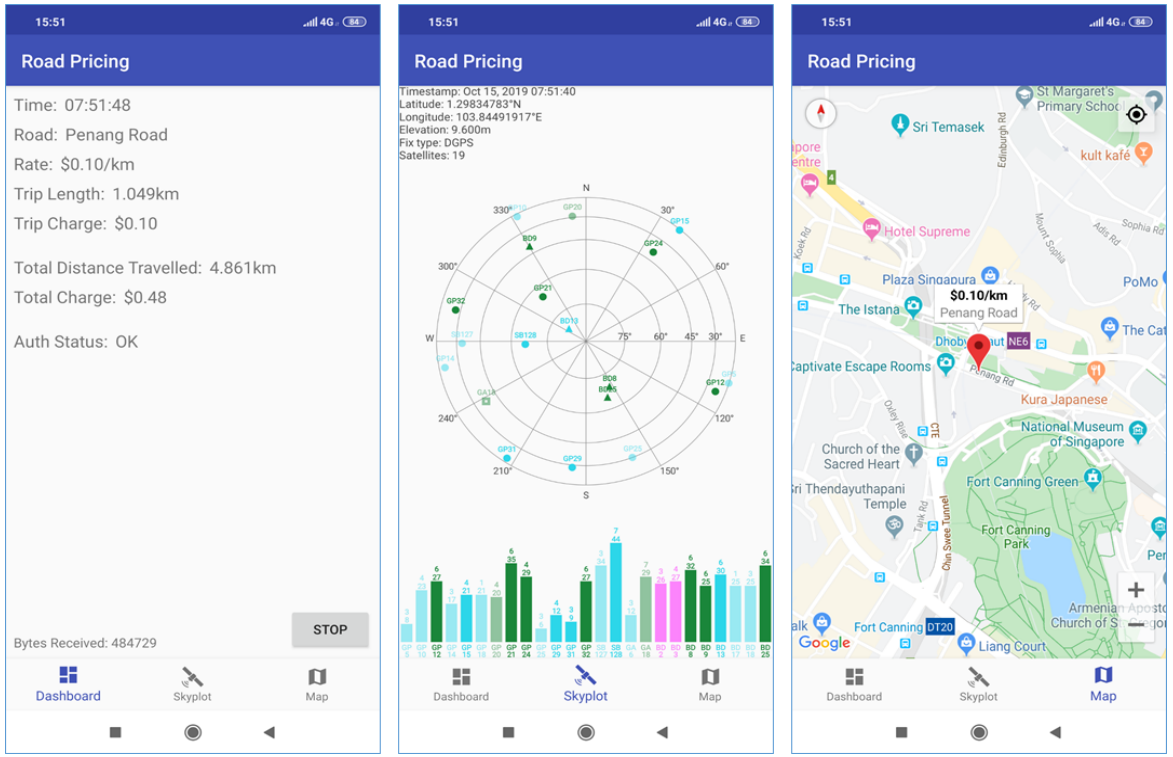
Road Pricing is one of the solutions for Traffic Congestion Management

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

Dynamic Road Pricing (DRP) based on GNSS

- No Physical Toll Gates
  - GPS-based system is used for Location, Distance, and Lane occupation
  - Multi-Lane Free Flow (MLFF)
  - Can be implemented on any road section
    - Not limited to only highways, expressways or toll roads
- 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
- 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
- ERP 2.0: https://onemotoring.lta.gov.sg/content/onemotoring/home/driving/ERP/erp-2-0.html





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

References

- 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
- Facebook
  - https://www.facebook.com/gnss.lab/

We Challenge with Our Ideas

How About You?

Join RPD Challenge