International GNSS Summer School 2019

Organized by Tokyo University of Marine Science and Technology

Course

Module A: GNSS Signal Security
Module B: Spoofing & GNSS Signal Authentication
Module C: Android GNSS Raw Data Processing

Dinesh MANANDHAR
Center for Spatial Information Science
The University of Tokyo
dinesh@iis.u-tokyo.ac.jp

29th July – 3rd August 2019, Tokyo

- Dinesh Manandhar
- Associate Professor (Project), Center for Spatial Information Science, The University of Tokyo
- Adjunct Associate Professor, Asian Institute of Technology, Thailand
- Member, ISO/TC-204, WG18
- Member, ICAO/NSP, DFMC/SBAS Signal Authentication

Outline of the Lecture

- **Module A: GNSS Signal Security**
  - **Introduction to GNSS Vulnerabilities**
    - **Interference**
    - **Jamming**
    - **Spoofing**
- **Module B: Spoofing and GNSS Signal Authentication**
  - **Detail discussions on Spoofing**
  - **Demonstration of Spoofing**
  - **Anti-Spoofing Methods**
  - **Demonstration of Anti-Spoofing Method**
- **Module C: Android GNSS Raw Data Processing**
  - **Introduction**
  - **Android Devices**
  - **Data Logging Tools**
  - **Data Processing Tools**
  - **Data Processing Outputs**
  - **Innovative and Challenging Applications**

Module – B
Spoofing and GNSS Signal Authentication

Module – B: Contents

- Introduction
- Spoofing Issues
  - What is Spoofing?
  - How to Spoof?
- Anti-Spoofing
  - Anti-Spoofing Methods
  - Authentication System Development
  - POC (Proof-Of-Concept) Tests
- GPS & GALILEO Authentication Status
- Conclusions

Can You Trust GPS Position & Time Data?

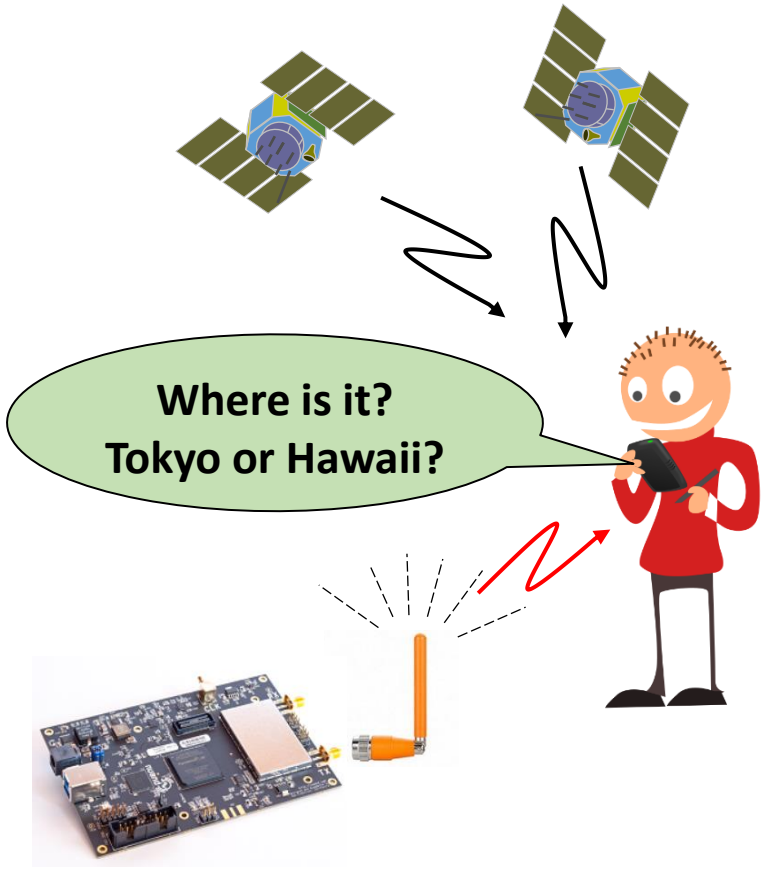
Yes, You can…

…But Need to Verify

Because of Spoofing Issues

What is Location Spoofing?

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



Spoofer

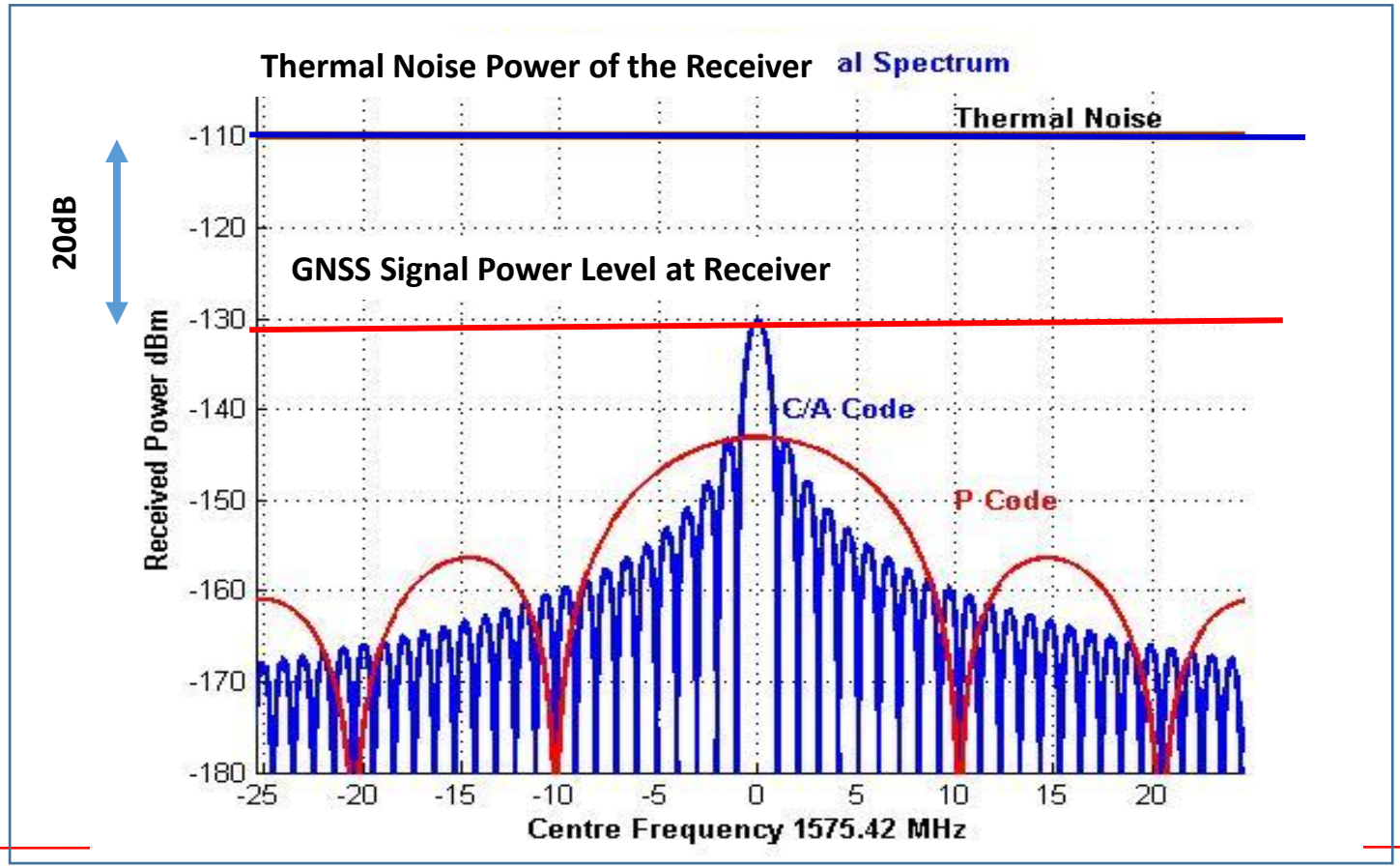
TOKYO
Or
Hawaii?

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

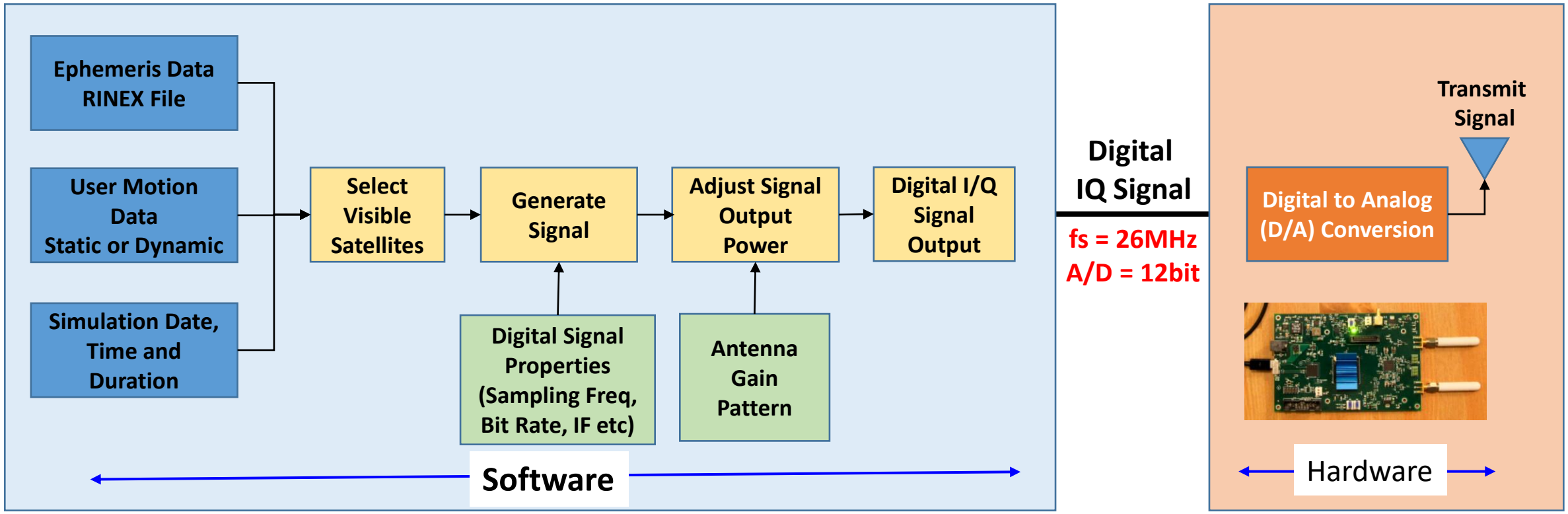
This movie is all about GPS Spoofing

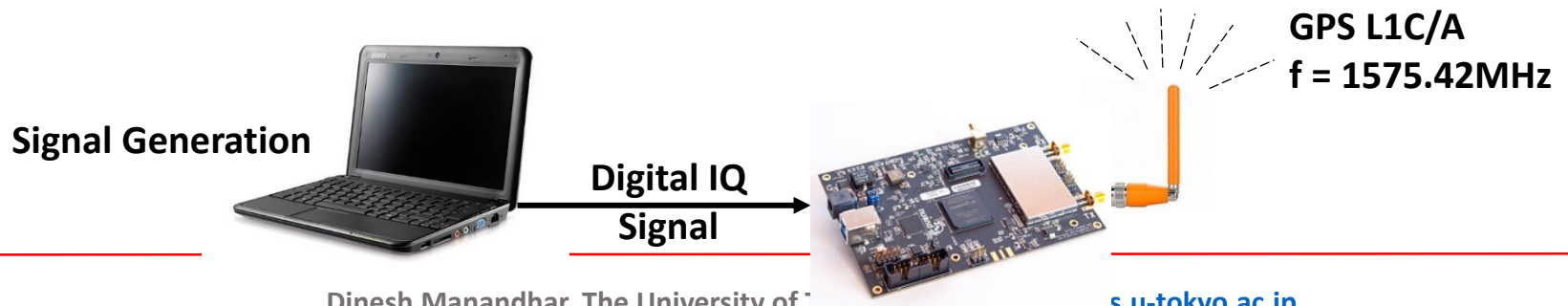
Why GPS is Vulnerable to Spoofing ?

- **GPS Signal Power is Extremely Low**
- **GPS Signal Structures are Published and Accessible to Everyone**

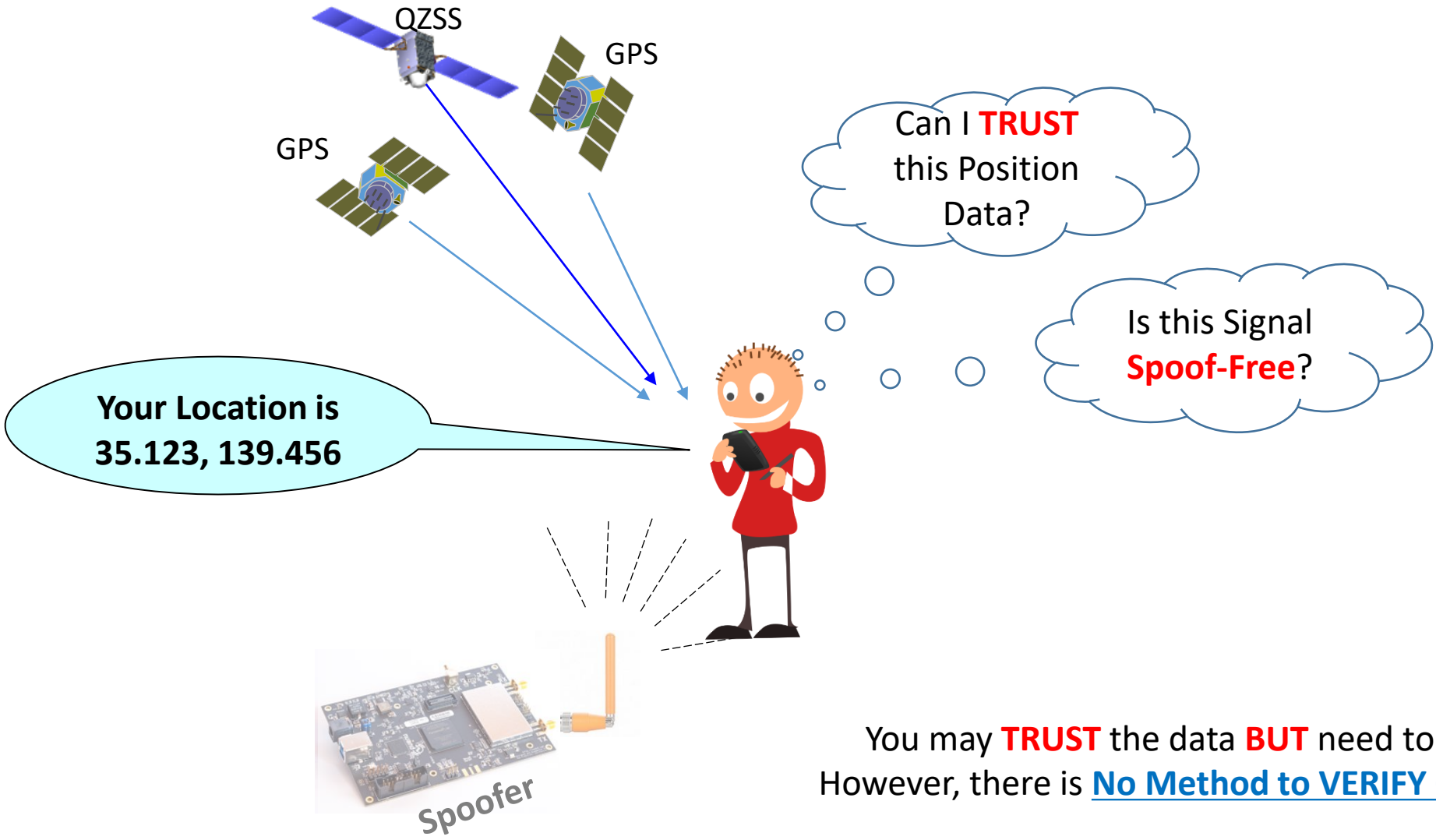


Software-Based GPS Signal Generator (Spoofer?)





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**

What is GPS Signal Authentication?

- **To authenticate or verify that a GPS signal in the receiver is actually from a GPS satellite not a Spoofer**

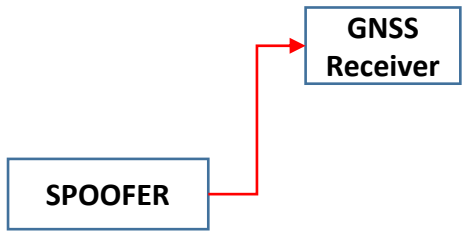
GPS Signal Authentication is necessary to detect SPOOF Signals

Spoofing Methods

Spoofing Level 0
Self-Spoofing

Receiver and Spoofer directly connected by cable

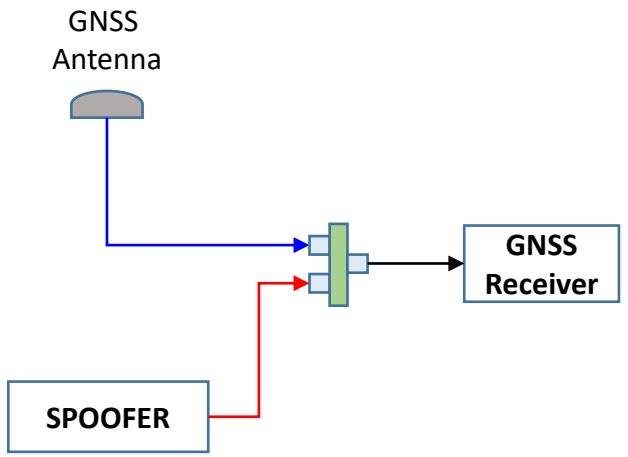
Real Signal not Present



Spoofing Level 1
Self-Spoofing

Receiver and Spoofer directly connected by cable

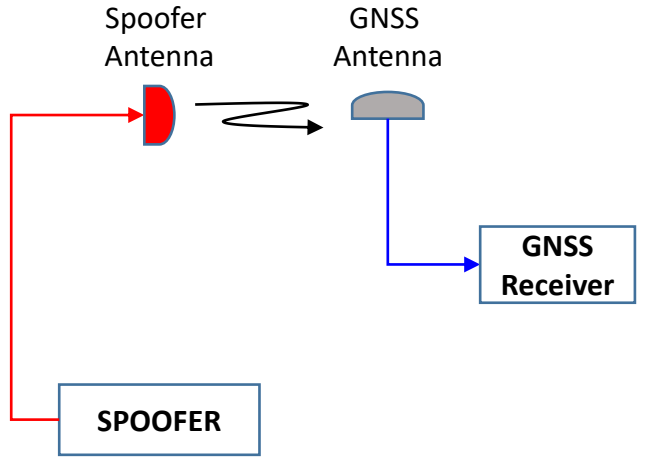
Real Signal Present



Spoofing Level 2
Self-Spoofing or 3rd Party Spoofing

Over-the-Air Spoof Signal Transmission

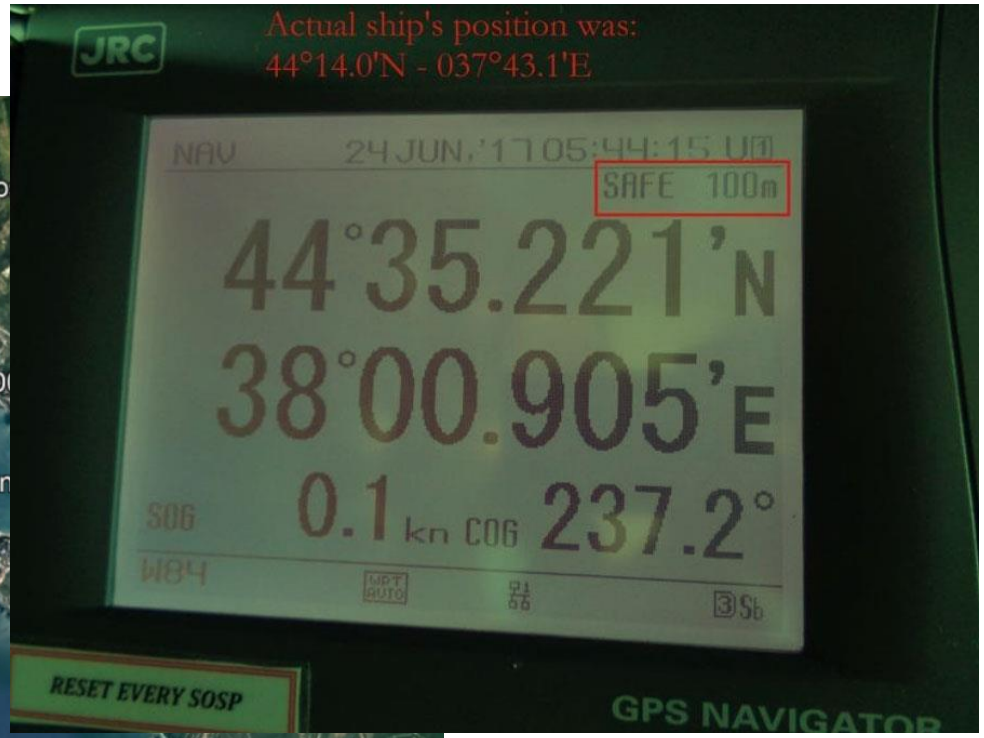
Real Signal Present

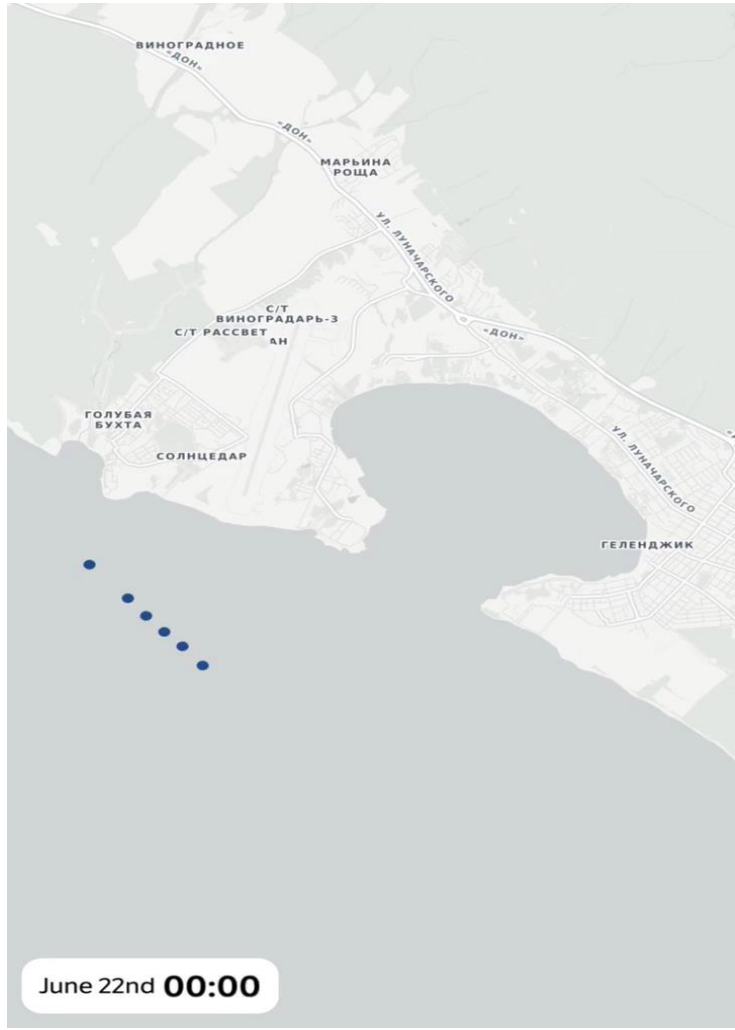


GPS Spoofing in Black Sea?

24th June 2017

A GPS spoofing attack in June, involving over 20 vessels in the Black Sea, has been reported. *Probably the first official record of spoofing.* More…….



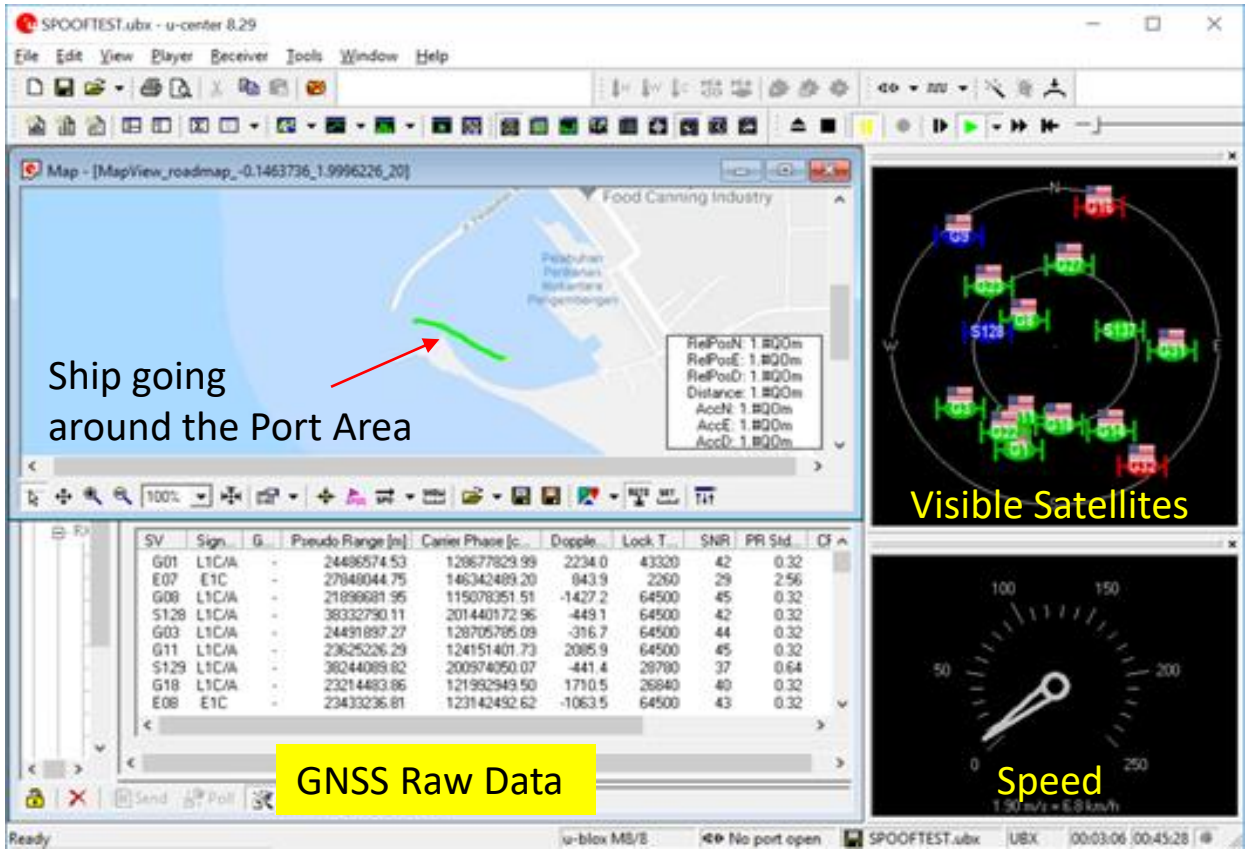


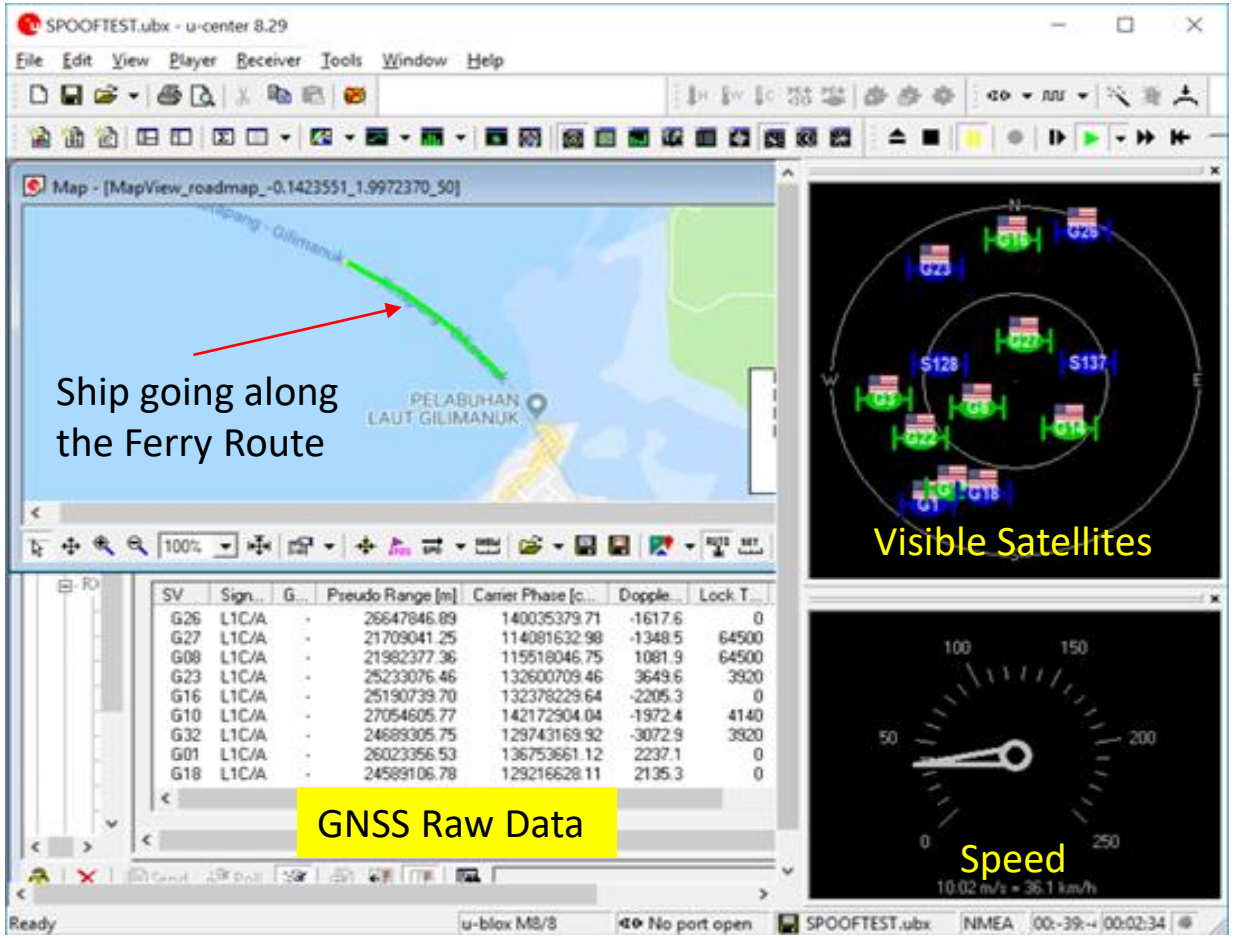
https://www.rin.org.uk/newsitem/4969/GPS-Spoofing-in-Black-Sea

SPOOFing a Car: Is he driving the car?

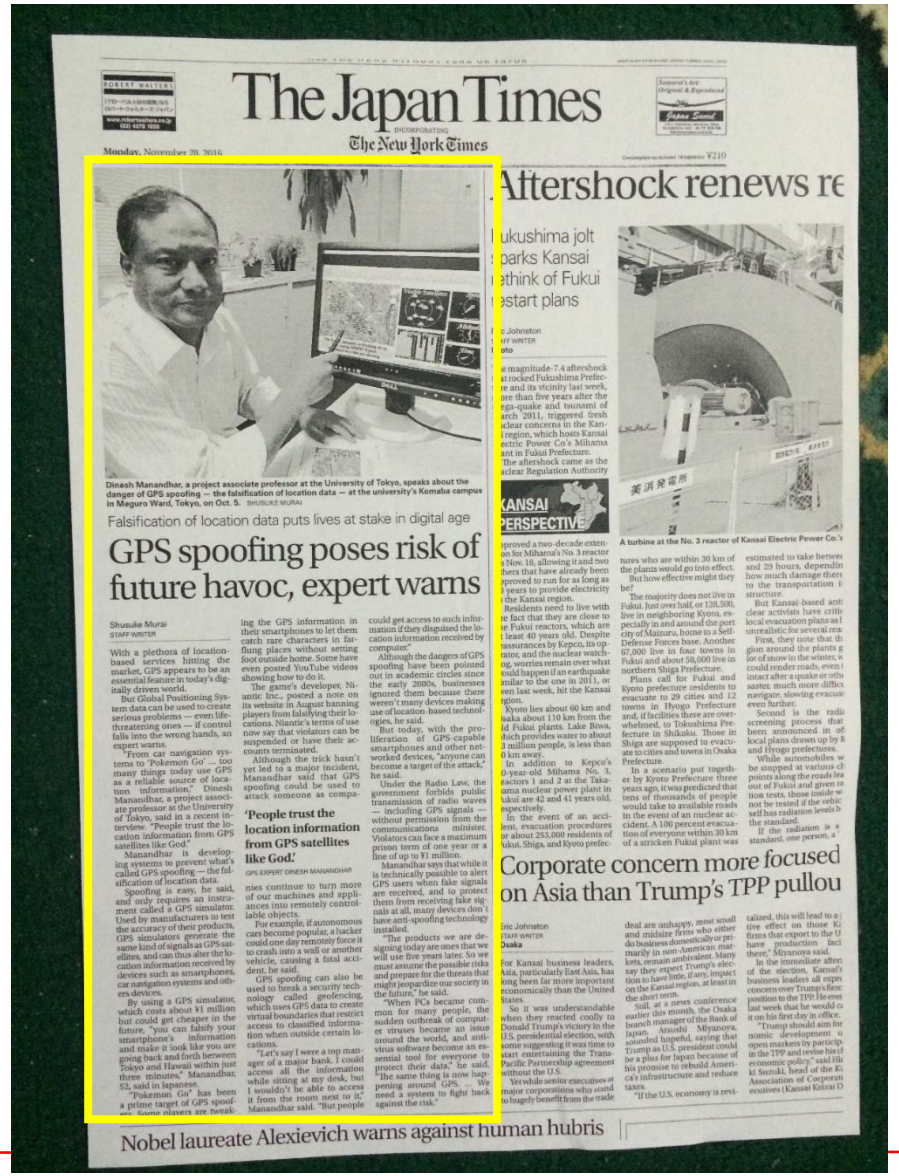
Output of GNSS Receiver, True Data and Spoof Data

Quiz: Can you identify TRUE Data and SPOOF Data?





GPS Spoofing Poses Risk of Future Havoc



The Japan Times
The New York Times
Monday, November 28, 2016

Aftershock renews re

ukushima jolt
parks Kansai
ethink of Fukui
start plans

Dinesh Manandhar, a project associate professor at the University of Tokyo, speaks about the danger of GPS spoofing — the falsification of location data — at the university's Komaba campus in Meguro Ward, Tokyo, on Oct. 5. SHUSUKE MURAI

Falsification of location data puts lives at stake in digital age

GPS spoofing poses risk of future havoc, expert warns

Shusuke Murai
STAFF WRITER

With a plethora of location-based services hitting the market, GPS appears to be an essential feature in today's digitally driven world.

But Global Positioning System data can be used to create serious problems — even life-threatening ones — if control falls into the wrong hands, an expert warns.

"From car navigation systems to 'Pokemon Go' ... too many things today use GPS as a reliable source of location information," Dinesh Manandhar, a project associate professor at the University of Tokyo, said in a recent interview. "People trust the location information from GPS satellites like God."

Manandhar is developing systems to prevent what's called GPS spoofing — the falsification of location data.

Spoofing is easy, he said, and only requires an instrument called a GPS simulator. Used by manufacturers to test the accuracy of their products, GPS simulators generate the same kind of signals as GPS satellites, and can thus alter the location information received by devices such as smartphones, car navigation systems and others devices.

By using a GPS simulator, which costs about ¥1 million but could get cheaper in the future, "you can falsify your smartphone's information and make it look like you are going back and forth between Tokyo and Hawaii within just three minutes," Manandhar, 52, said in Japanese.

"Pokemon Go" has been a prime target of GPS spoofers. Some players are tweaking the GPS information in their smartphones to let them catch rare characters in far-flung places without setting foot outside home. Some have even posted YouTube videos showing how to do it.

The game's developer, Niantic Inc., posted a note on its website in August banning players from falsifying their locations. Niantic's terms of use now say that violators can be suspended or have their accounts terminated.

Although the trick hasn't yet led to a major incident, Manandhar said that GPS spoofing could be used to attack someone as compa-

'People trust the location information from GPS satellites like God.'

GPS EXPERT DINESH MANANDHAR

nies continue to turn more of our machines and appliances into remotely controllable objects.

For example, if autonomous cars become popular, a hacker could one day remotely force it to crash into a wall or another vehicle, causing a fatal accident, he said.

GPS spoofing can also be used to break a security technology called geofencing, which uses GPS data to create virtual boundaries that restrict access to classified information when outside certain locations.

"Let's say I were a top manager of a major bank. I could access all the information while sitting at my desk, but I wouldn't be able to access it from the room next to it," Manandhar said. "But people could get access to such information if they disguised the location information received by computer."

Although the dangers of GPS spoofing have been pointed out in academic circles since the early 2000s, businesses ignored them because there weren't many devices making use of location-based technologies, he said.

But today, with the proliferation of GPS-capable smartphones and other networked devices, "anyone can become a target of the attack," he said.

Under the Radio Law, the government forbids public transmission of radio waves — including GPS signals — without permission from the communications minister. Violators can face a maximum prison term of one year or a fine of up to ¥1 million.

Manandhar says that while it is technically possible to alert GPS users when fake signals are received, and to protect them from receiving fake signals at all, many devices don't have anti-spoofing technology installed.

"The products we are designing today are ones that we will use five years later. So we must assume the possible risks and prepare for the threats that might jeopardize our society in the future," he said.

"When PCs became common for many people, the sudden outbreak of computer viruses became an issue around the world, and anti-virus software become an essential tool for everyone to protect their data," he said. "The same thing is now happening around GPS. ... We need a system to fight back against the risk."

Nobel laureate Alexievich warns against human hubris

KANSAI PERSPECTIVE

A turbine at the No. 3 reactor of Kansai Electric Power Co.'s

proved a two-decade exten-on for Mihama's No. 3 reactor s Nov. 16, allowing it and two thers that have already been proved to run for as long as 0 years to provide electricity the Kansai region.

Residents need to live with he fact that they are close to he Fukui reactors, which are least 40 years old. Despite ssurances by Kepco, its op-rator, and the nuclear watch-og, worries remain over what ould happen if an earthquake milar to the one in 2011, or en last week, hit the Kansai gion.

Kyoto lies about 60 km and aka about 110 km from the id Fukui plants. Lake Biwa, hich provides water to about 3 million people, is less than 0 km away.

In addition to Kepco's 0-year-old Mihama No. 3, eactors 1 and 2 at the Taka-ma nuclear power plant in ukui are 42 and 41 years old, espectively.

In the event of an acci-lent, evacuation procedures or about 253,000 residents of ukui, Shiga, and Kyoto prefec-

Corporate concern more focused on Asia than Trump's TPP pullou

Eric Johnston
STAFF WRITER
Osaka

for Kansai business leaders, Asia, particularly East Asia, has long been far more important economically than the United States.

So it was understandable when they reacted coolly to Donald Trump's victory in the U.S. presidential election, with some suggesting it was time to start entertaining the Trans-Pacific Partnership agreement without the U.S.

Yet while senior executives at major corporations who stand to hugely benefit from the trade deal are unhappy, most small and midsize firms who either do business domestically or primarily in non-American markets, remain ambivalent. Many say they expect Trump's election to have little, if any, impact on the Kansai region, at least in the short term.

Still, at a news conference earlier this month, the Osaka branch manager of the Bank of Japan, Atsushi Miyanoya, sounded hopeful, saying that Trump as U.S. president could be a plus for Japan because of his promise to rebuild America's infrastructure and reduce taxes.

"If the U.S. economy is revi-

estimated to take betwee and 29 hours, dependin how much damage there to the transportation i structure.

But Kansai-based anti clear activists have criti local evacuation plans as unrealistic for several rea

First, they note that th gion around the plants g ioc of snow in the winter, w could render roads, even i intact after a quake or oth aster, much more difficu navigate, slowing evacuat even further.

Second is the radi screening process that been announced in of local plans drawn up by t and Hyogo prefectures.

While automobiles w be stopped at various ch points along the roads lea out of Fukui and given ra tion tests, those inside w not be tested if the vehic self has radiation levels b the standard.

If the radiation is a standard, one person, a

talized, this will lead to a tive effect on those K firms that export to the U have production faci there," Miyanoya said.

In the immediate after of the election, Kansai's business leaders all expr concerns over Trump's fierc position to the TPP. He even last week that he would co it on his first day in office.

"Trump should aim for nomic development u open markets by particip in the TPP and revise his cl economic policy," said Ha ki Suzuki, head of the K Association of Corporat ecutives (Kansai Keizai D

GPS 'Spoofing' is No Joke: Dangers of GPS Data Hacking Realized

GNSS spoofing will attain virus status, warns expert – GPS World

Hacking Global Positioning System with GPS 'Spoofing' Can Lead To Fatalities
http://www.techworm.net/2016/11/gps-spoofing-dangers-gps-data-hacking.html

Dangers of GPS spoofing and hacking for location based services

Faking of GPS Data a growing and potentially lethal danger – The Japan Times, FB

GPS Tracking is Illegal without Warrant: Japan Supreme Court Ruling

15th March 2017

New rules might be implemented to make GPS tracking legal with warrant.

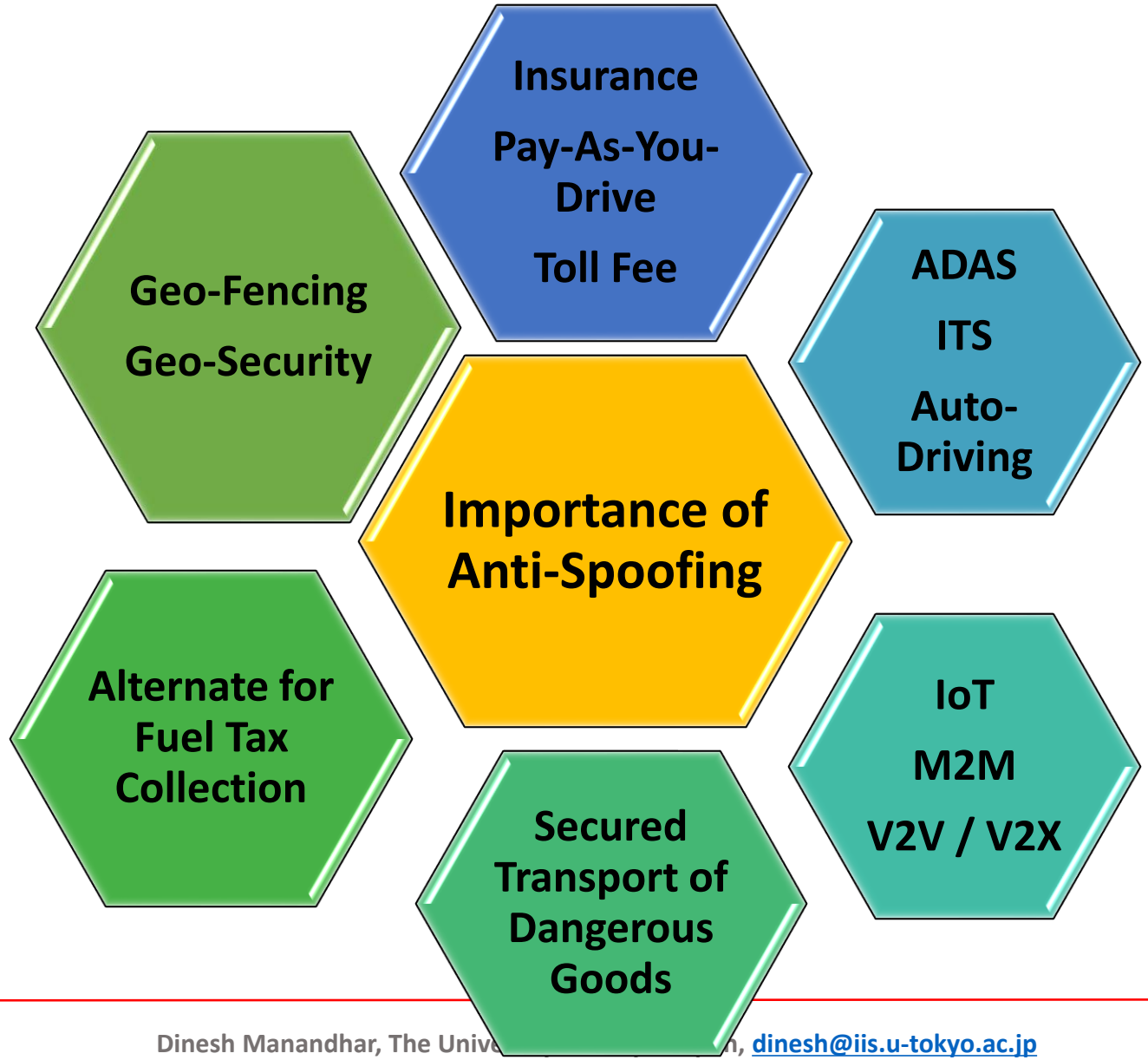
But, there is also fear of GPS Signal Spoofing.

ＧＰＳ捜査訴訟の上告審判決が言い渡された最高裁大法廷。中央は、寺田逸郎裁判長＝15日午後、東京都千代田区（伴龍二撮影）

Why SPOOFING is Dangerous compared to Interference & Jamming?

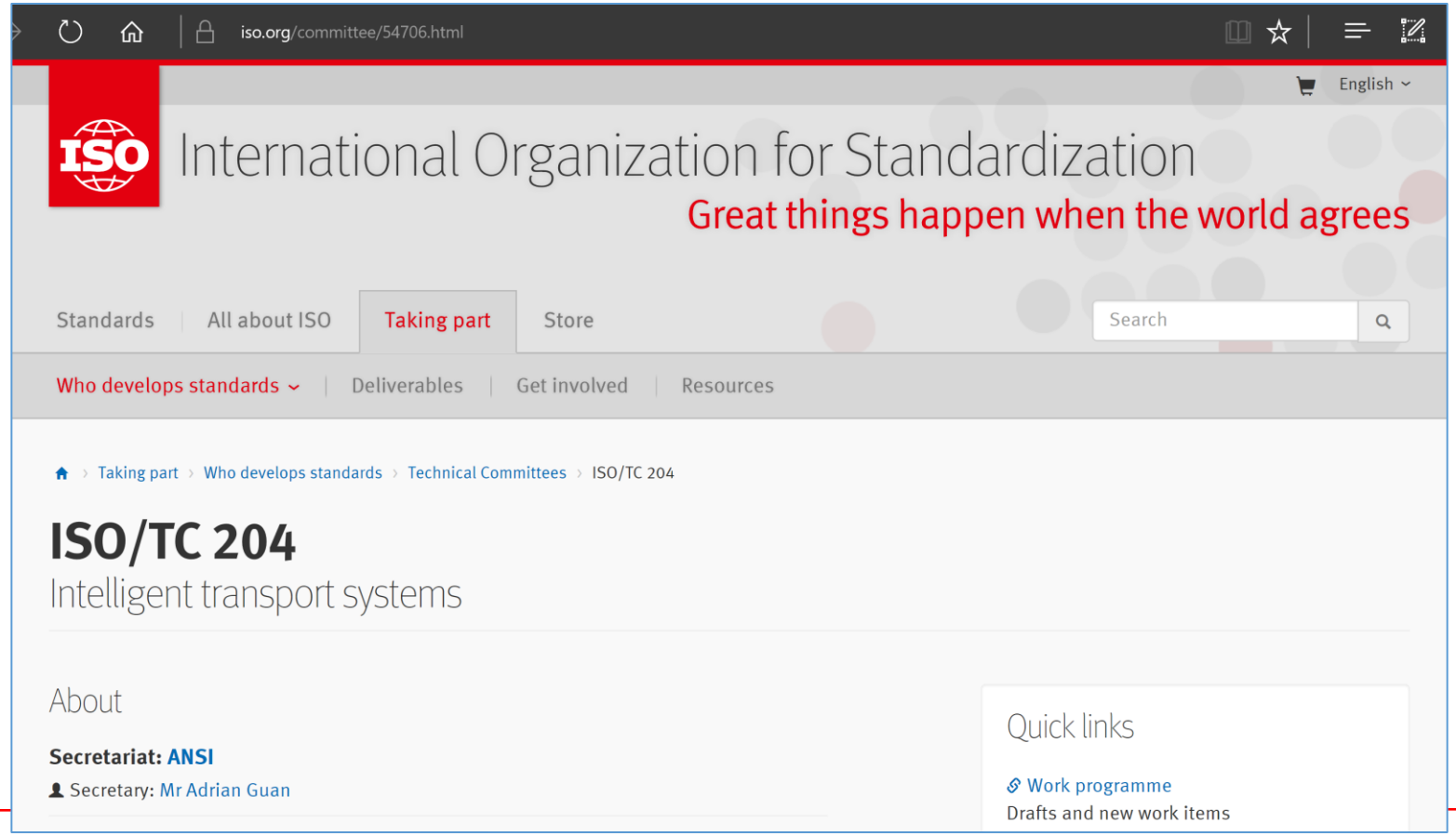
Spoofing	Jamming and Interference
Intentional	Intentional and Non-Intentional
Difficult to Detect	**Can be Detected**
Available of Service but Lead to False Position Data	**Denial of Service**
No Effective Solution for Existing Signals	Many Solutions Exist
Fewer Research and Studies	Many Research and Studies

Why do we need to care about Spoofing?



Importance of Anti-Spoofing for Trust-worthy PVT Data for ITS

- **Discussions in ISO/TC-204, WG18**
  - **To Draft regulations for ITS-S related with PVT Data**



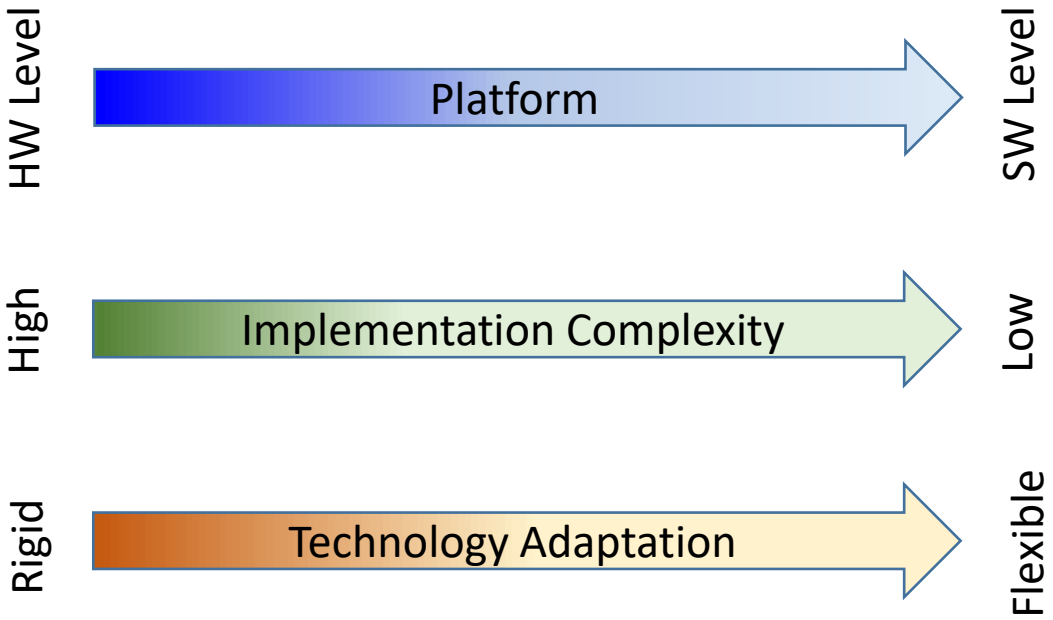
Importance of Anti-Spoofing for Trust-worthy PVT Data for Aviation

- **New SBAS Signals (L5 Band) can also be Authenticated without modifying the current signal structure.**

- **ICAO is already highlighting the necessity and importance of SBAS Signal Authentication**
  - **New regulations that will require to Authenticate SBAS Signals for Anti-spoofing will emerge**

How to Mitigate Spoofing?

- **Hardware Level**
  - Multi-antenna
  - Direction of Arrival
  - ….
- **RF Level**
  - AGC Monitoring
- **Signal Monitoring**
  - P-Code Reference
  - RAIM or ARAIM
  - Signal Sanity Check
  - Multi-Correlator
- **Signal Encryption**
  - PRN Code Encryption
  - NAV Message Encryption
- **Navigation Message Authentication**
  - GALILEO Open Signal Navigation Message Authentication
  - Our Method ➔ Broadcasting Digital Signature



How to Solve Spoofing?

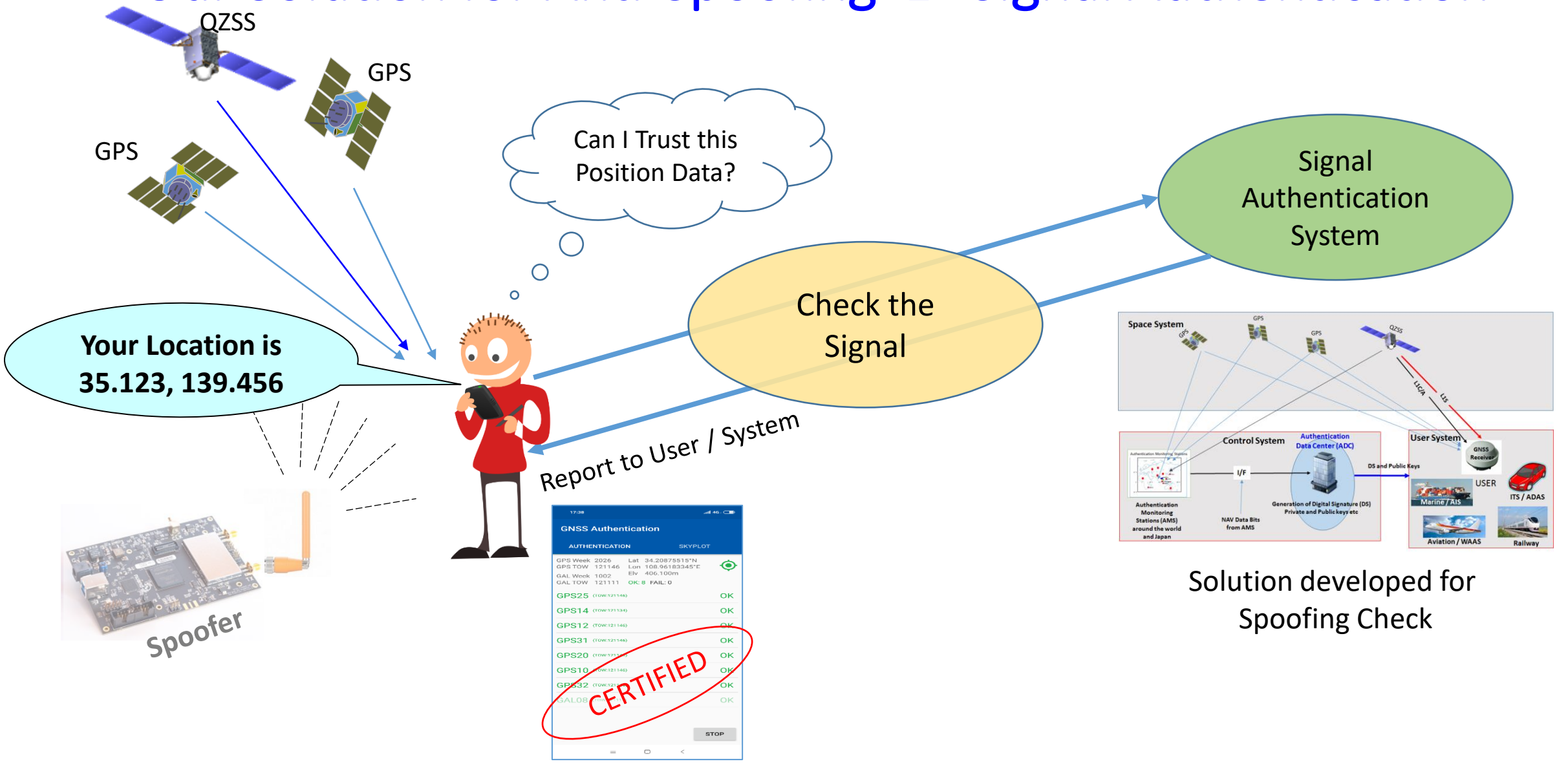
- **Hardware Level**
  - **Multi-antenna**
  - **Direction of Arrival**
  - **….**
- **Signal Monitoring**
  - **P-Code Reference**
  - **RAIM or ARAIM**
  - **Signal Sanity Check**
  - **Multi-Correlator**
- **Signal Encryption**
  - **PRN Code Encryption**
  - **NAV Message Encryption**
- **Broadcasting Digital Signature**
  - **Navigation Message Authentication**
- **GALILEO Open Signal Navigation Message Authentication**
  - **TESLA**

Anti-Spoofing Design Requirements

- **No Change in Hardware**
  - **Receiver side, Control System or Satellite system**
- **No Change in Signal Structure**
  - **Satellite Side**
- **Shall be able to**
  - **Implement only with FW/SW modification in the receiver**
  - **Provide Position Solution even if Authentication Fails**
  - **Authenticate only when required**
  - **Authenticate in Real-time as well as in Post-processing mode**
  - **Authenticate GPS L1C/A Signals as well**
  - **Authenticate consumer grade receivers**
    - IoT, ITS, ADAS, V2X, Mobile Phones etc

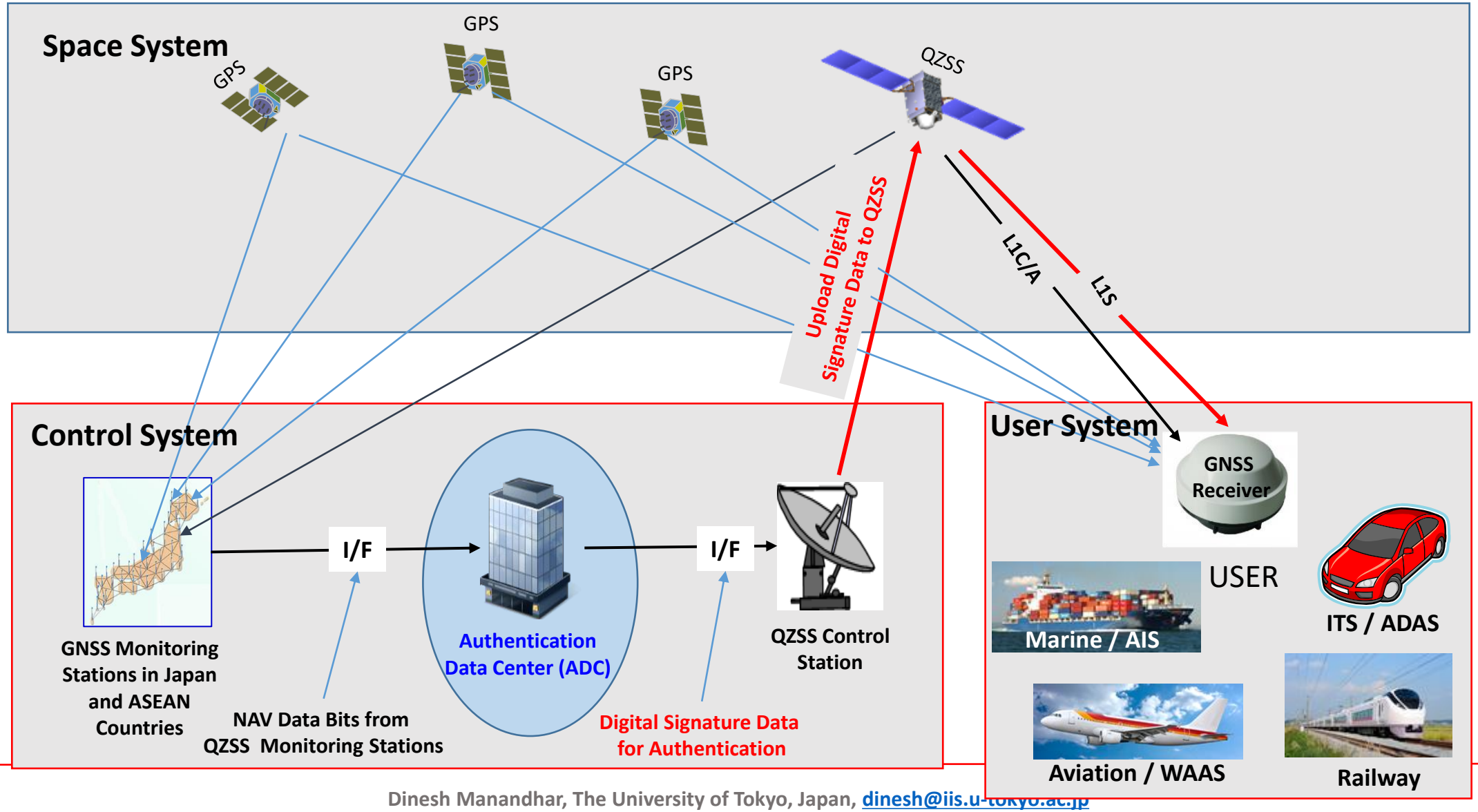
These requirements impose certain limitations on Authentication

Our Solution for Anti-Spoofing ➔ Signal Authentication

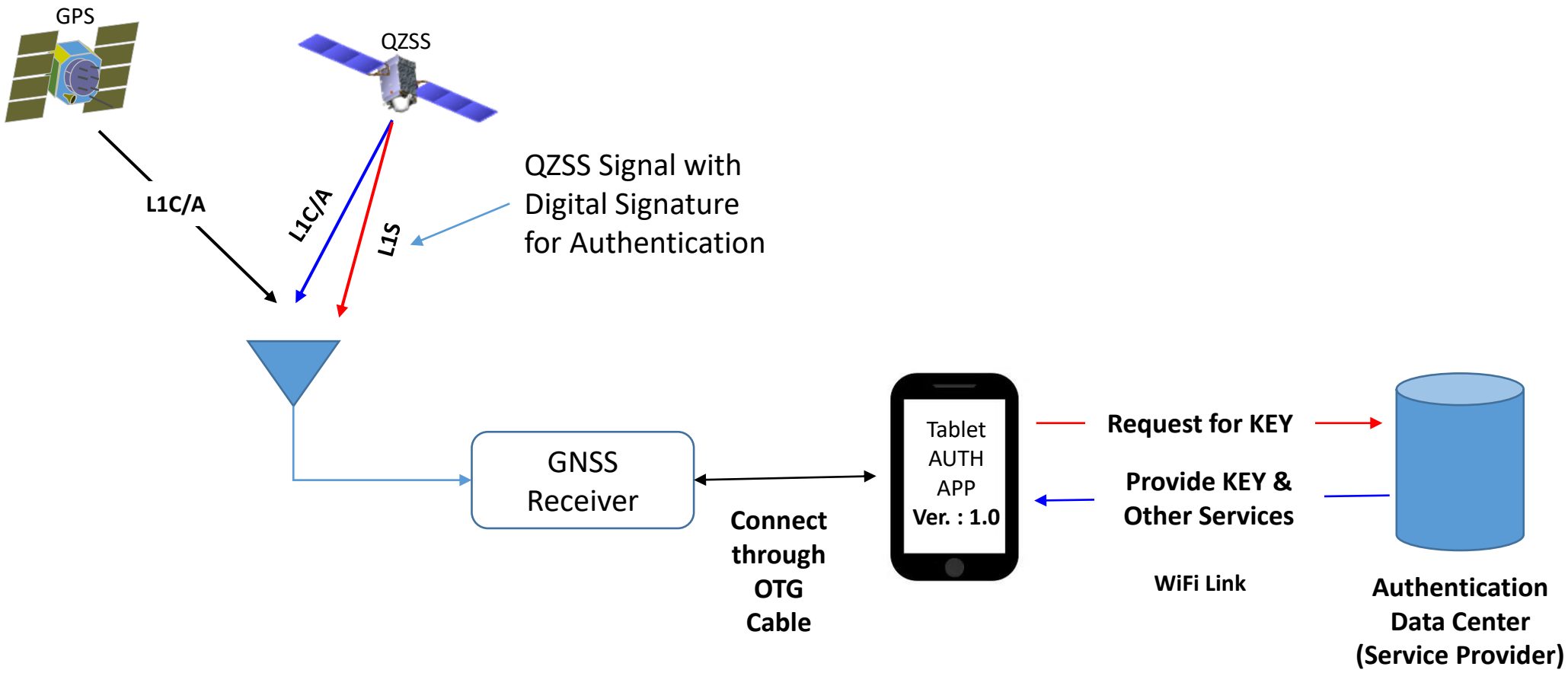


Solution developed for Spoofing Check

Authentication System: Space, Control and User Systems



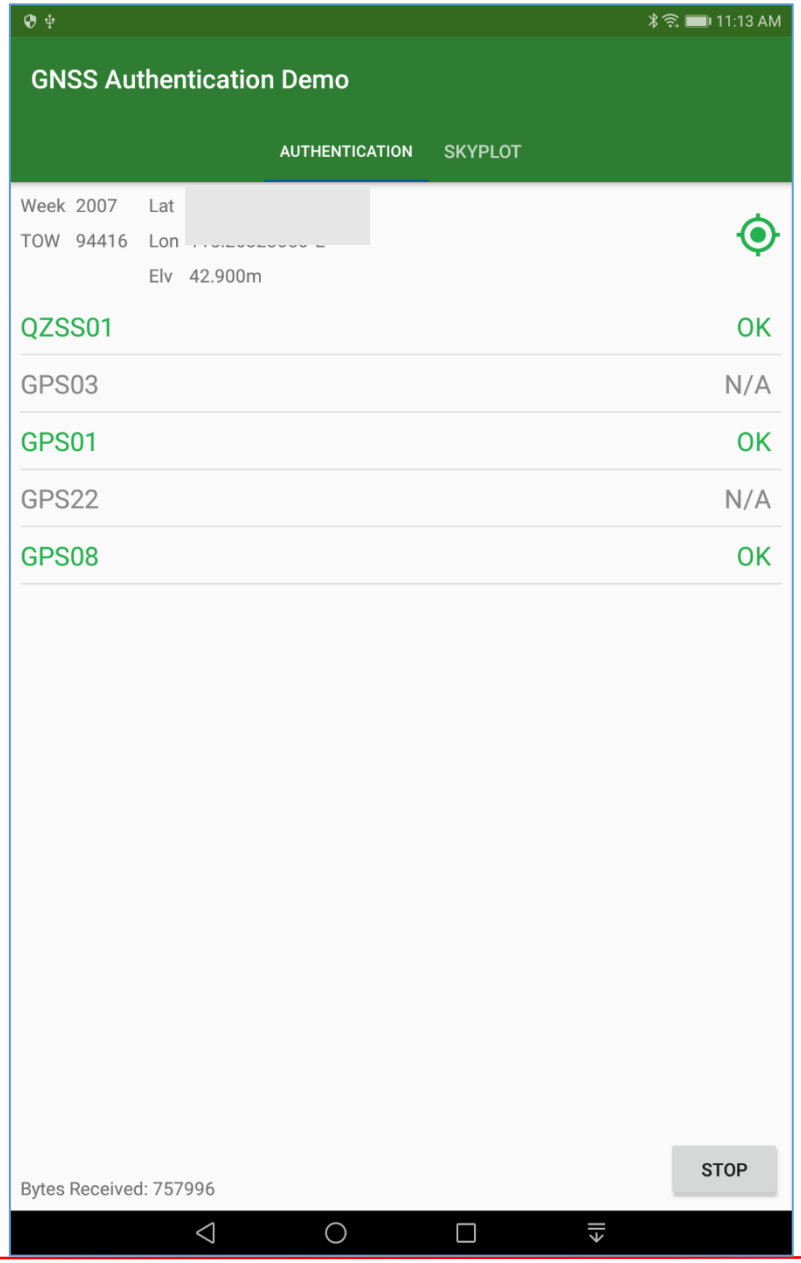
Prototype Anti-Spoofing Receiver

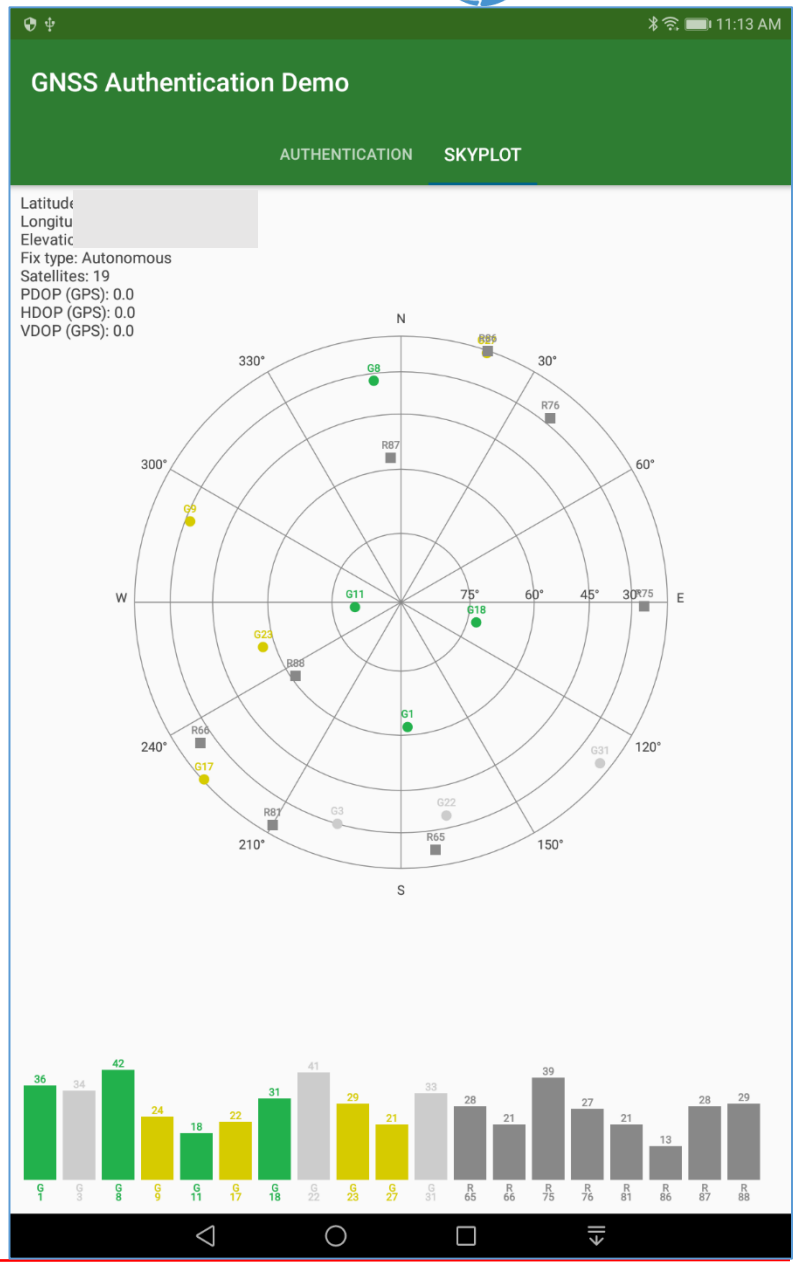


GPS Signal Authentication

Output of Signal Authentication APP when visible GPS signals are successfully authenticated.

Green : Authentication Successful
Red : Authentication Fail

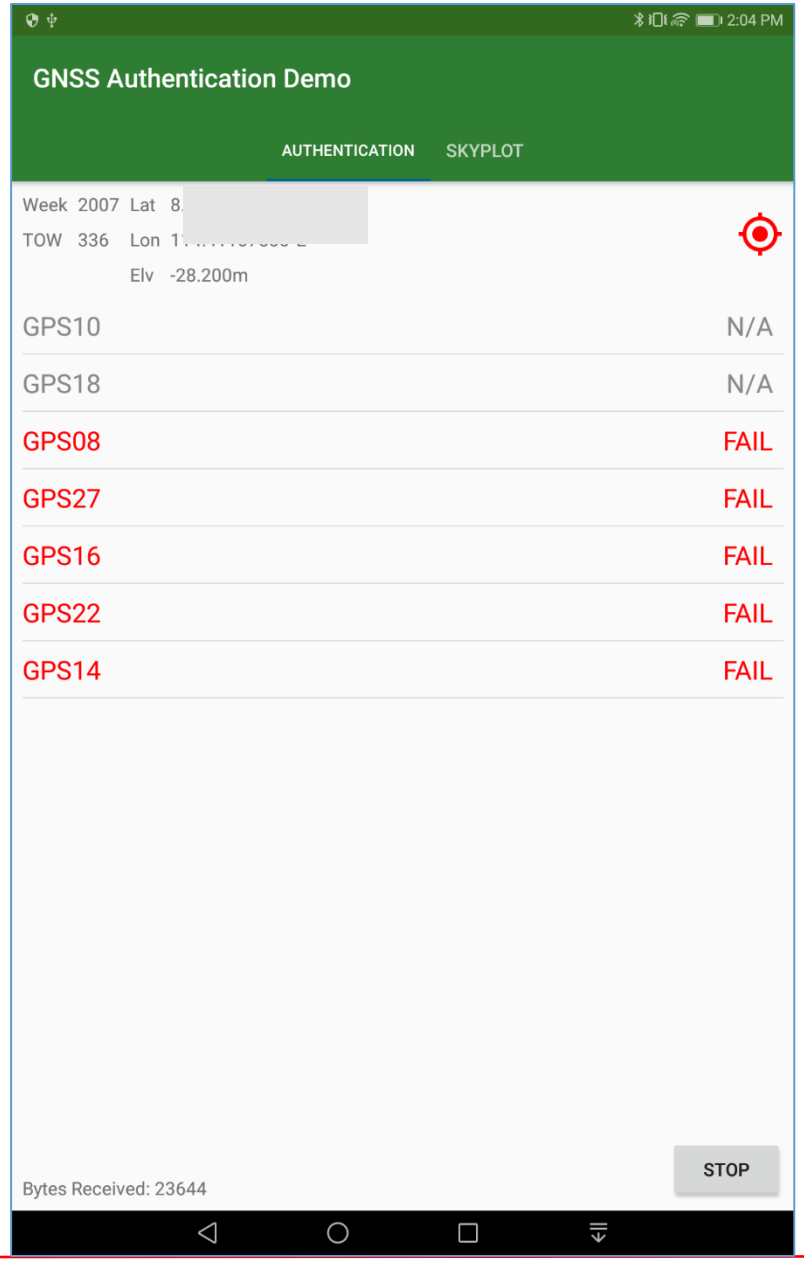


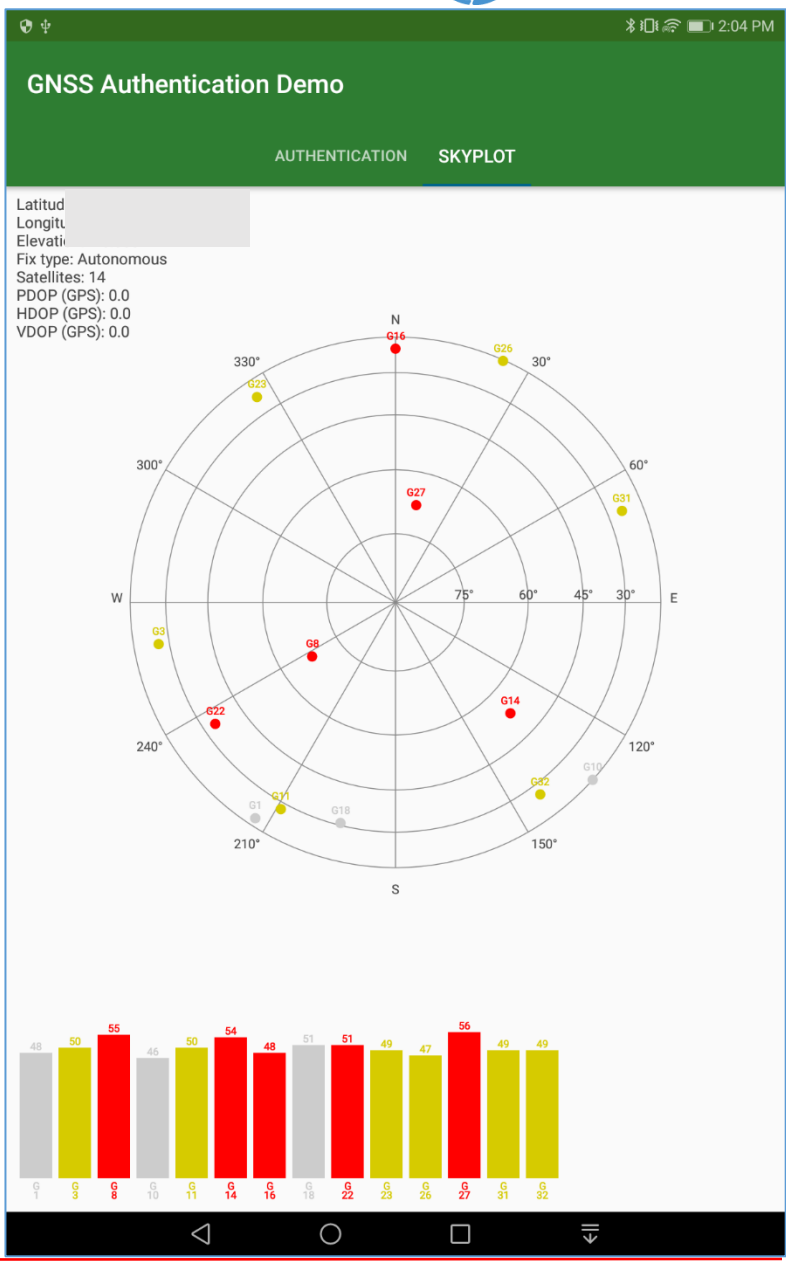


GPS Signal Authentication

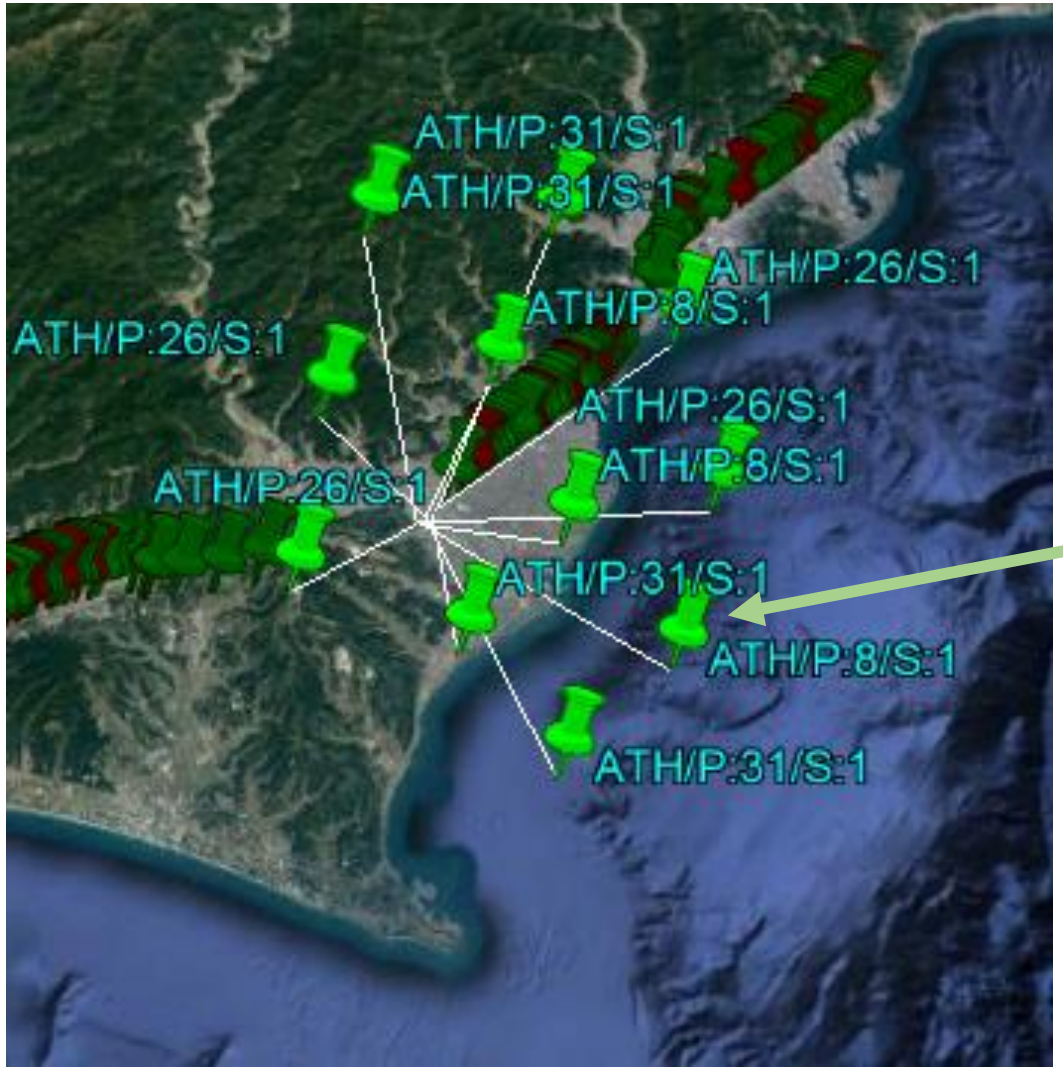
Output of Signal Authentication APP when visible GPS signals are successfully authenticated.

Green : Authentication Successful
Red : Authentication Fail / SPOOF Signal





Sample Authentication Output (KML)

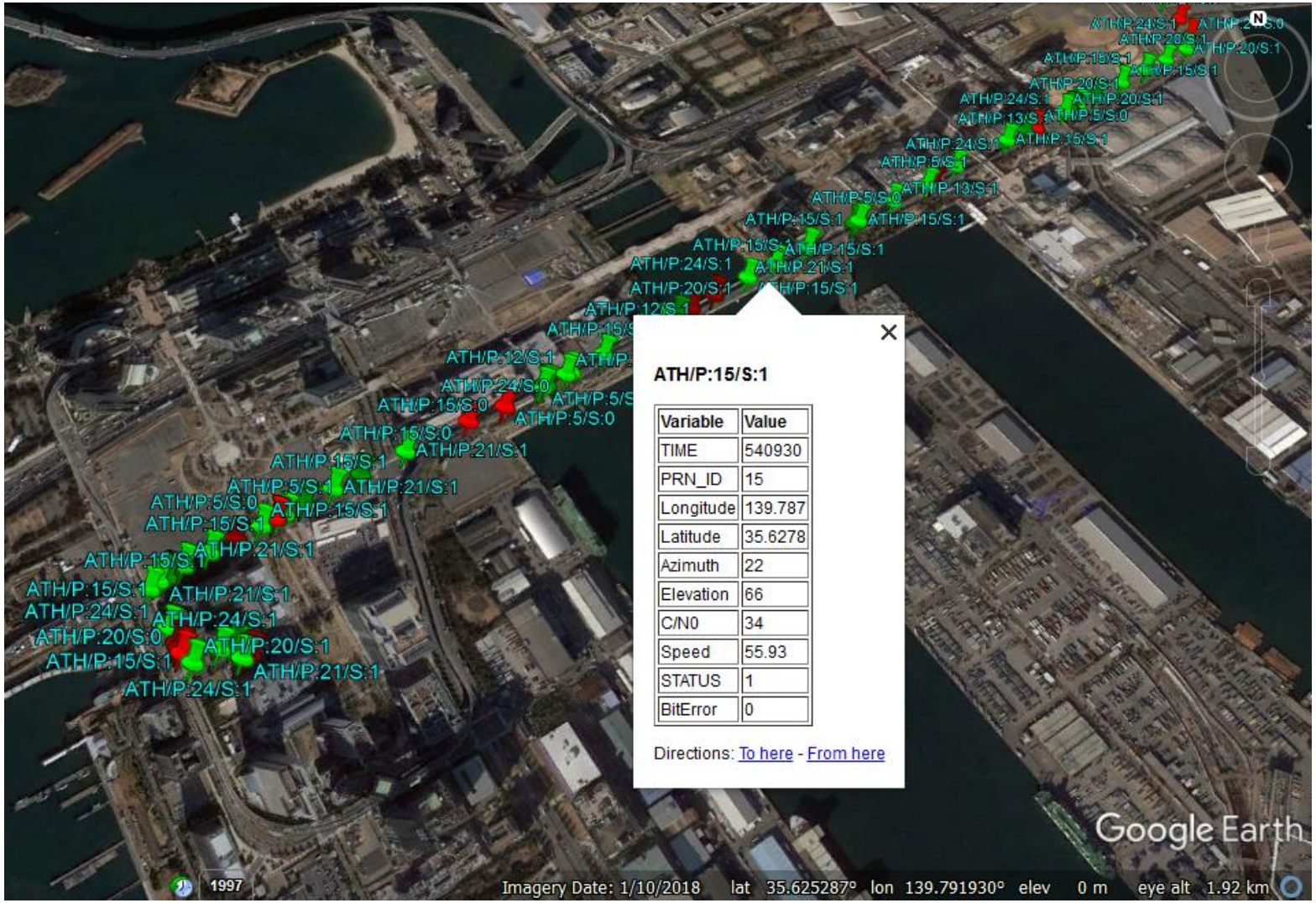


ATH/P:8/S:1

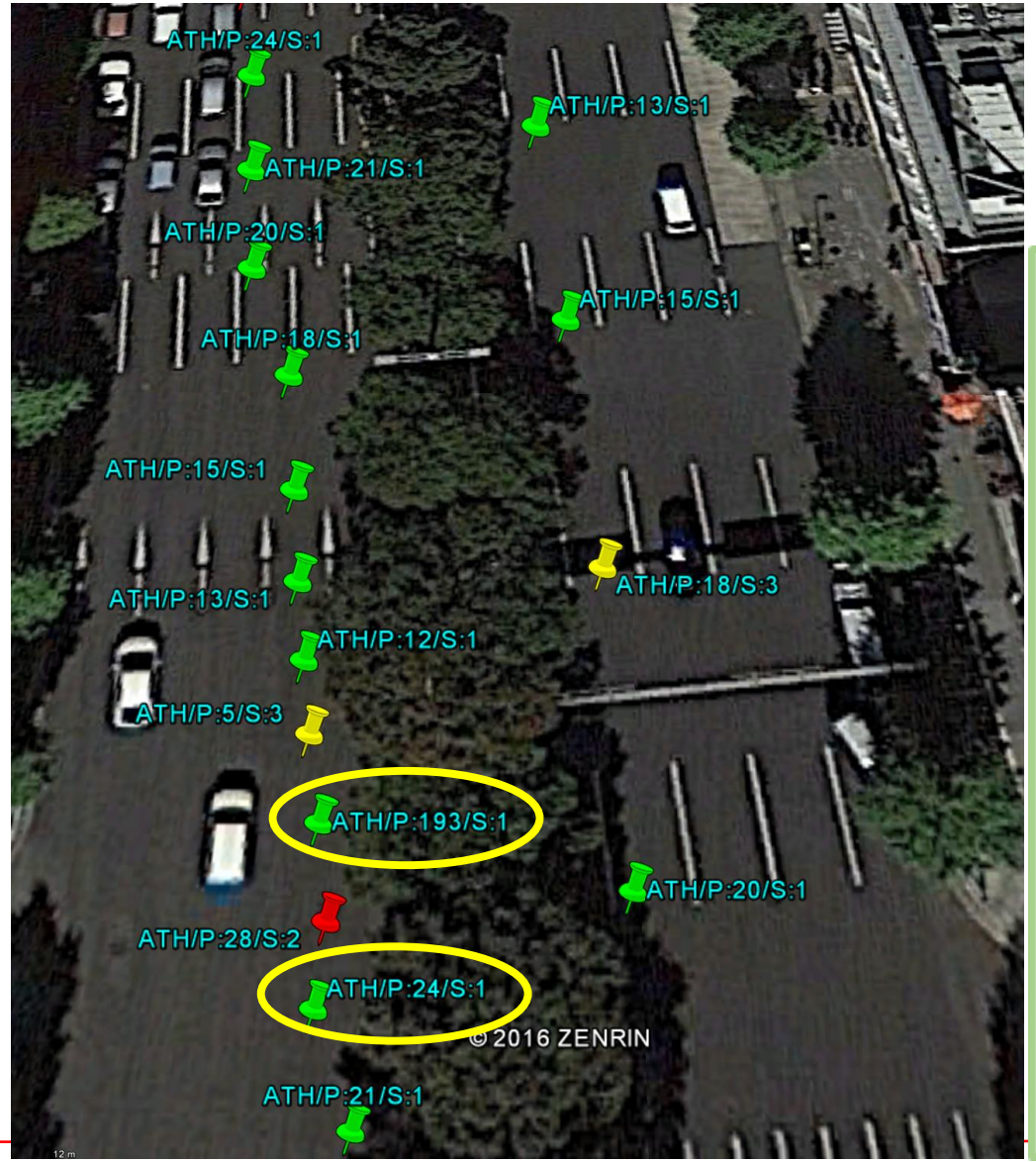
Variable	Value
TIME	120078
PRN_ID	8
Longitude	138.222
Latitude	34.8141
Azimuth	260
Elevation	52
C/N0	26
Speed	280.948
STATUS	1
BitError	1

Directions: To here - From here

Sample Authentication Output (KML)



POC Test Results, Dynamic User, Car Driving



ATH/P:24/S:1

Variable	Value
TIME	07:28:56
PRN_ID	24
NO of SAT	5
LONGITUDE	[redacted]
LATITUDE	
IODC	
DIST_T[m]	1026.66
DIST_P[m]	5.197
STATUS	1

Directions: To here - From here

ATH/P:28/S:2

Variable	Value
TIME	07:28:57
PRN_ID	28
NO of SAT	5
LONGITUDE	[redacted]
LATITUDE	
IODC	
DIST_T[m]	1030.07
DIST_P[m]	3.41
STATUS	2

Directions: To here - From here

ATH/P:193/S:1

Variable	Value
TIME	07:28:58
PRN_ID	193
NO of SAT	5
LONGITUDE	[redacted]
LATITUDE	
IODC	
DIST_T[m]	1034.32
DIST_P[m]	4.25
STATUS	1

Directions: To here - From here