DANGERS of SPOOFING and ANTI-SPOOFING SOLUTIONS

Dinesh Manandhar, Ryosuke Shibasaki
Center for Spatial Information Science (CSIS)
The University of Tokyo, Japan
Contact: dinesh@iis.u-tokyo.ac.jp
http://www.csis.u-tokyo.ac.jp/~dinesh/

Can You Trust GPS Position & Time Data?

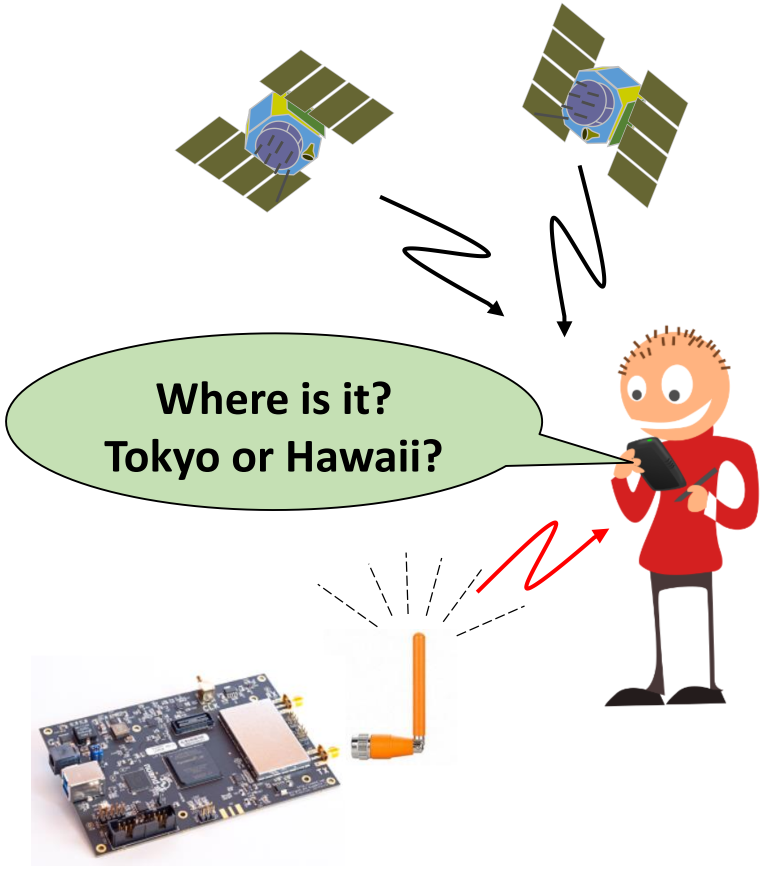
Yes, You can…

…But Need to Verify

Because of Spoofing Issues

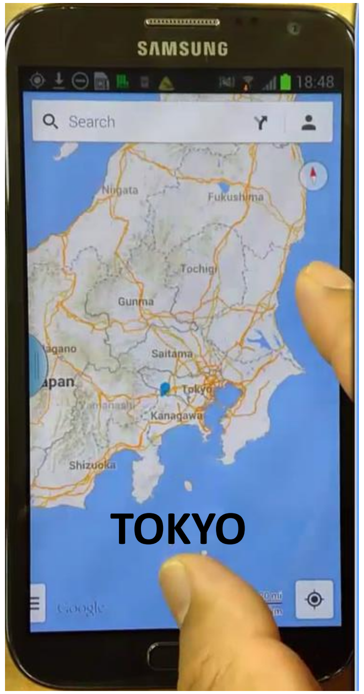
What is Location Spoofing?

- Falsify Location Data as If it were True Location



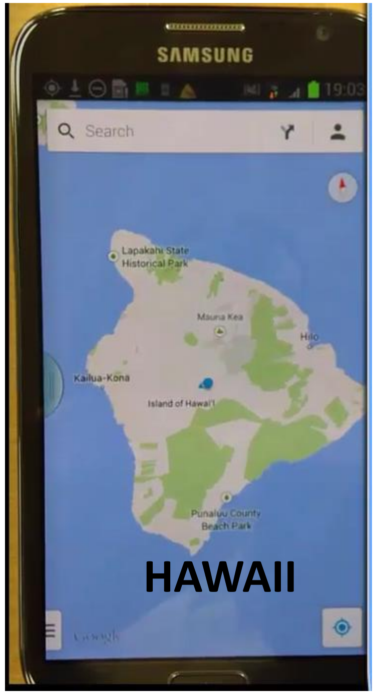
Where is it?
Tokyo or Hawaii?

Spoofer

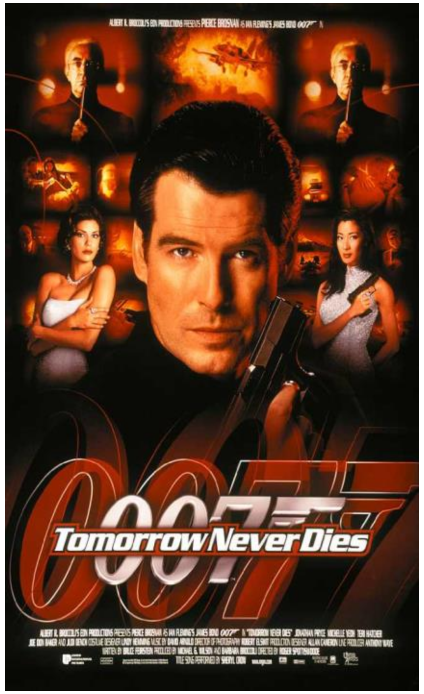


TOKYO

TOKYO
Or
Hawaii?

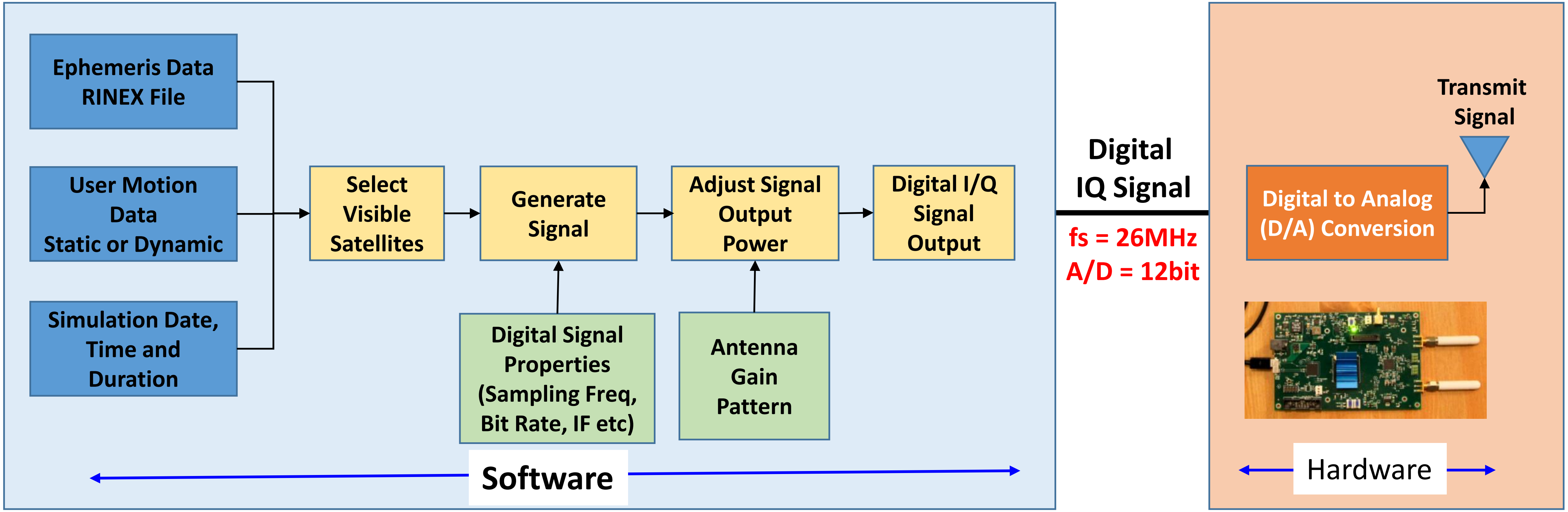


HAWAII



This movie is all about GPS Spoofing

Software-Based GPS Signal Generator (Spoofer?)



Ephemeris Data RINEX File

User Motion Data Static or Dynamic

Simulation Date, Time and Duration

Select Visible Satellites

Generate Signal

Adjust Signal Output Power

Digital I/Q Signal Output

Digital Signal Properties (Sampling Freq, Bit Rate, IF etc)

Antenna Gain Pattern

Software

Digital IQ Signal

fs = 26MHz

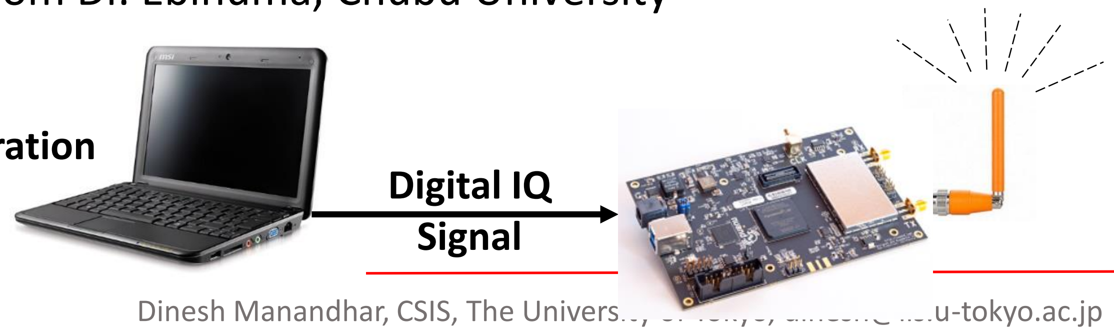
A/D = 12bit

Transmit Signal

Digital to Analog (D/A) Conversion

Hardware

Software Source available from Dr. Ebinuma, Chubu University



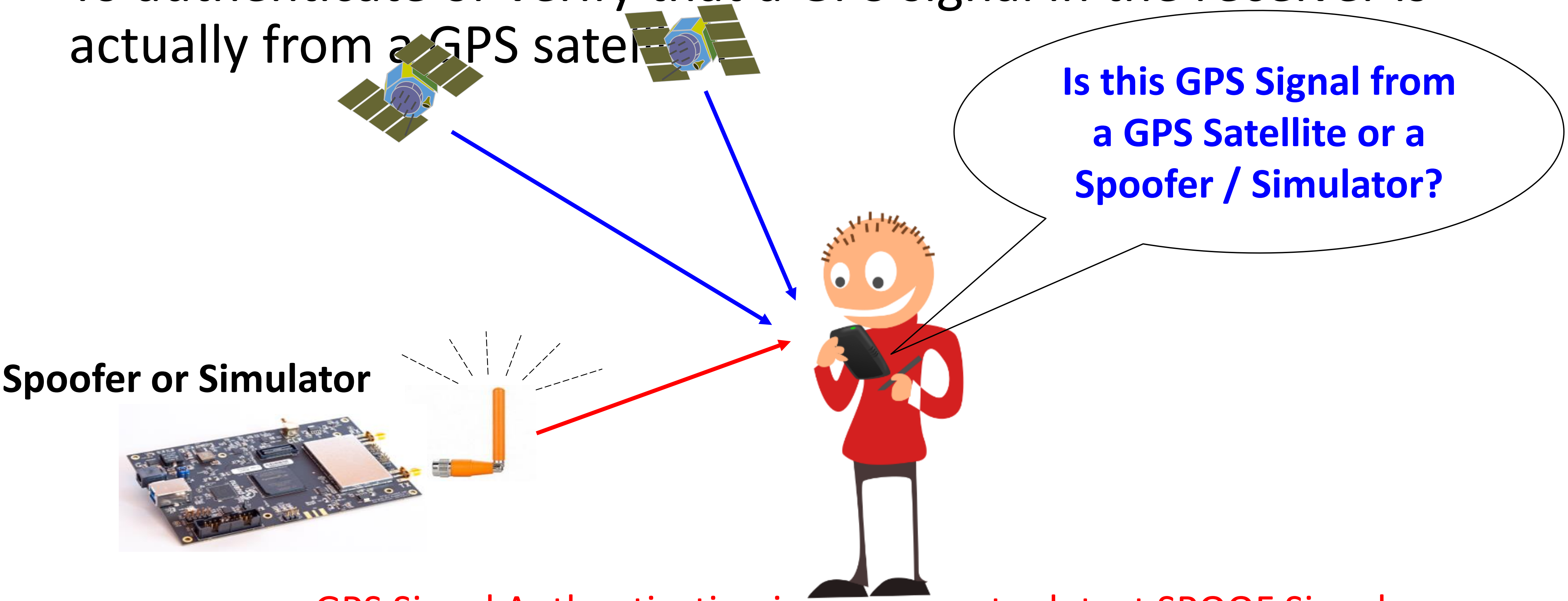
Signal Generation

Digital IQ Signal

GPS L1C/A
f = 1575.42MHz

What is GPS Signal Authentication?

- To authenticate or verify that a GPS signal in the receiver is actually from a GPS satel



Spoofer or Simulator

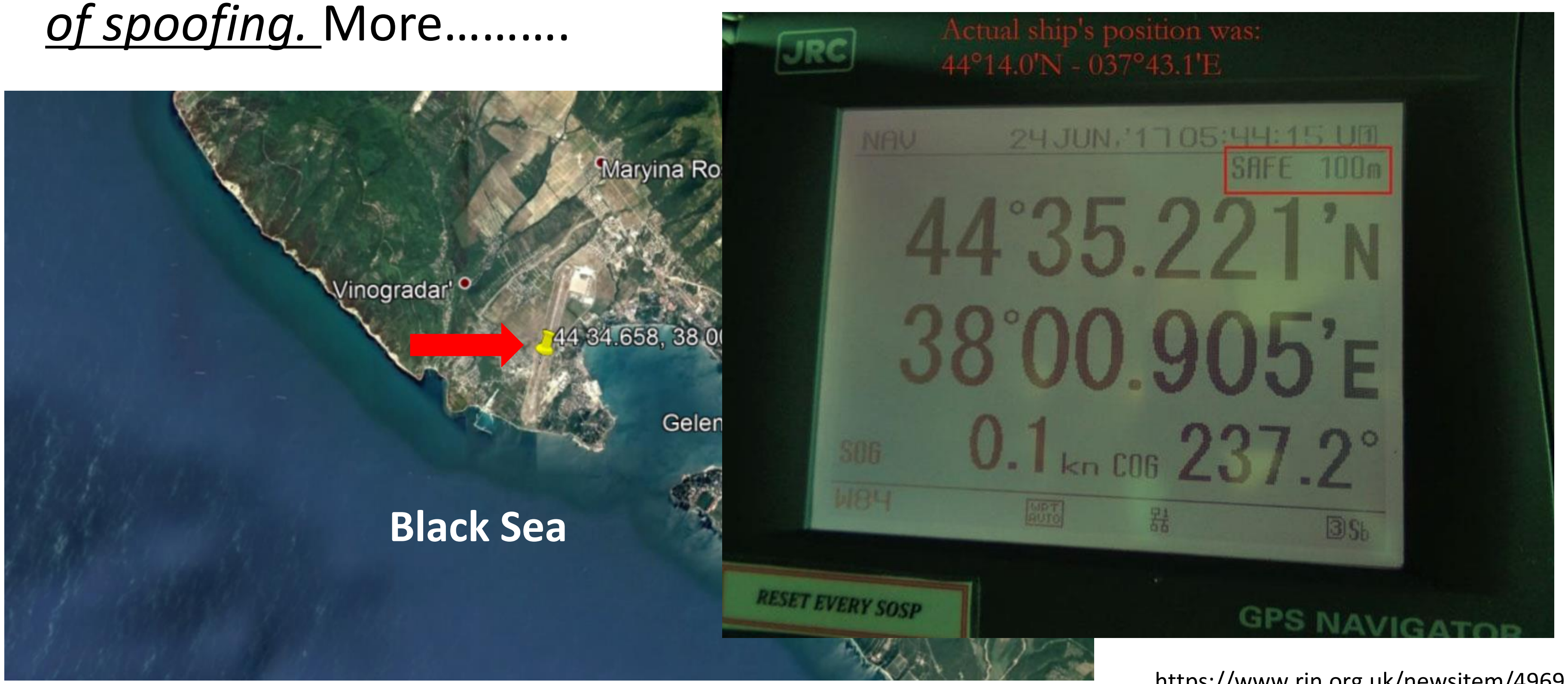
Is this GPS Signal from a GPS Satellite or a Spoofer / Simulator?

GPS Signal Authentication is necessary to detect SPOOF Signals

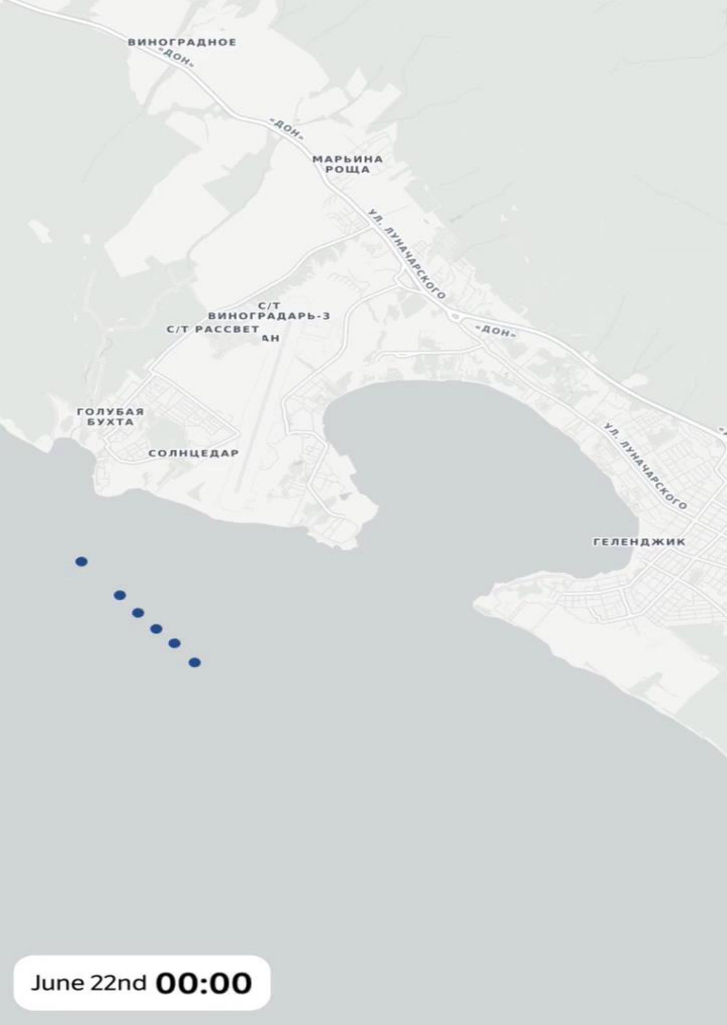
GPS Spoofing in Black Sea?

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……….



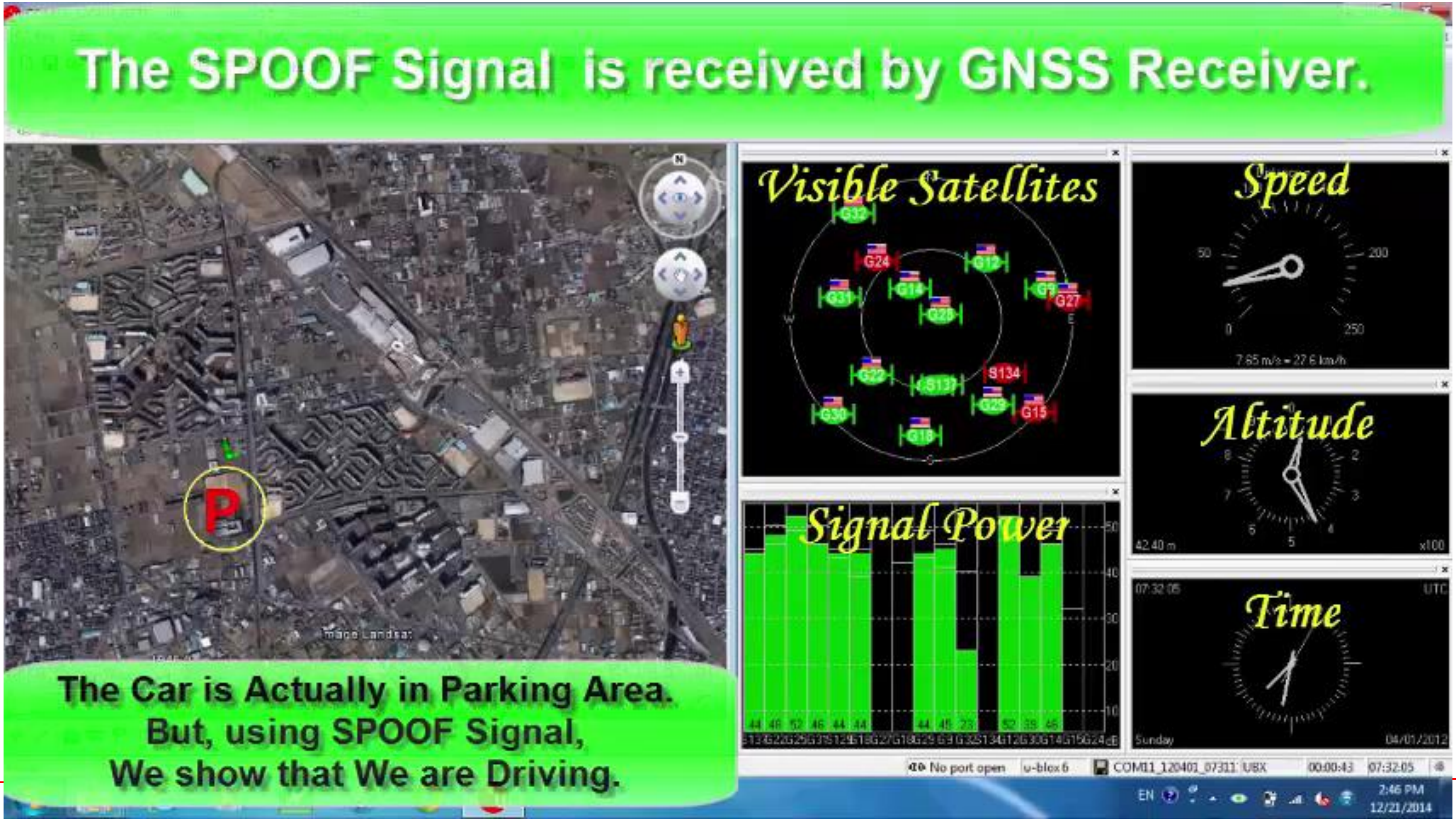
Actual ship's position was:
44°14.0'N - 037°43.1'E



June 22nd 00:00

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

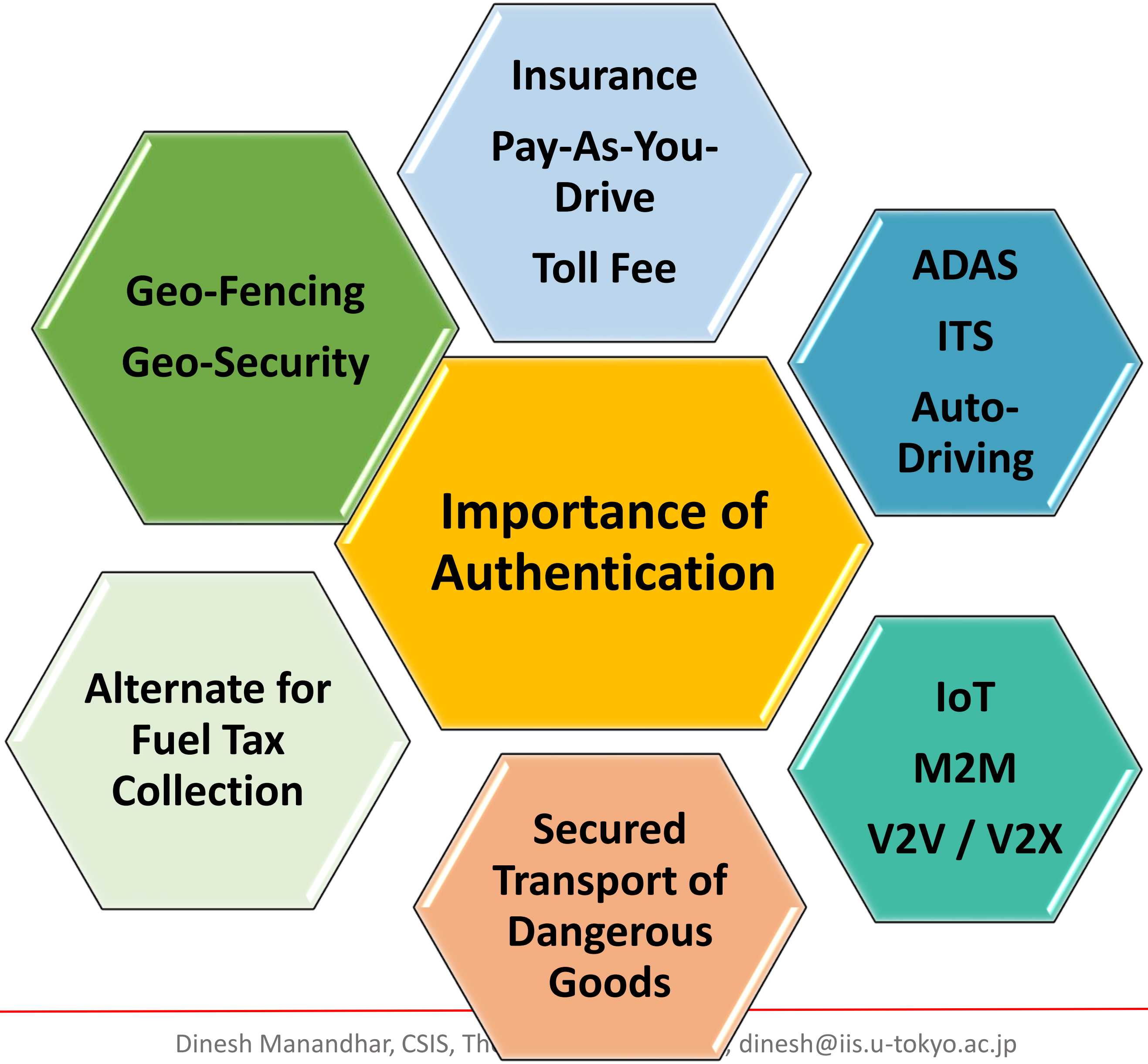
SPOOFing a Car: Is he driving the car?



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.

Why Authentication or Anti-Spoofing is Necessary ?



Importance of Authentication

Insurance

Pay-As-You-Drive

Toll Fee

Geo-Fencing

Geo-Security

ADAS

ITS

Auto-Driving

Alternate for Fuel Tax Collection

Secured Transport of Dangerous Goods

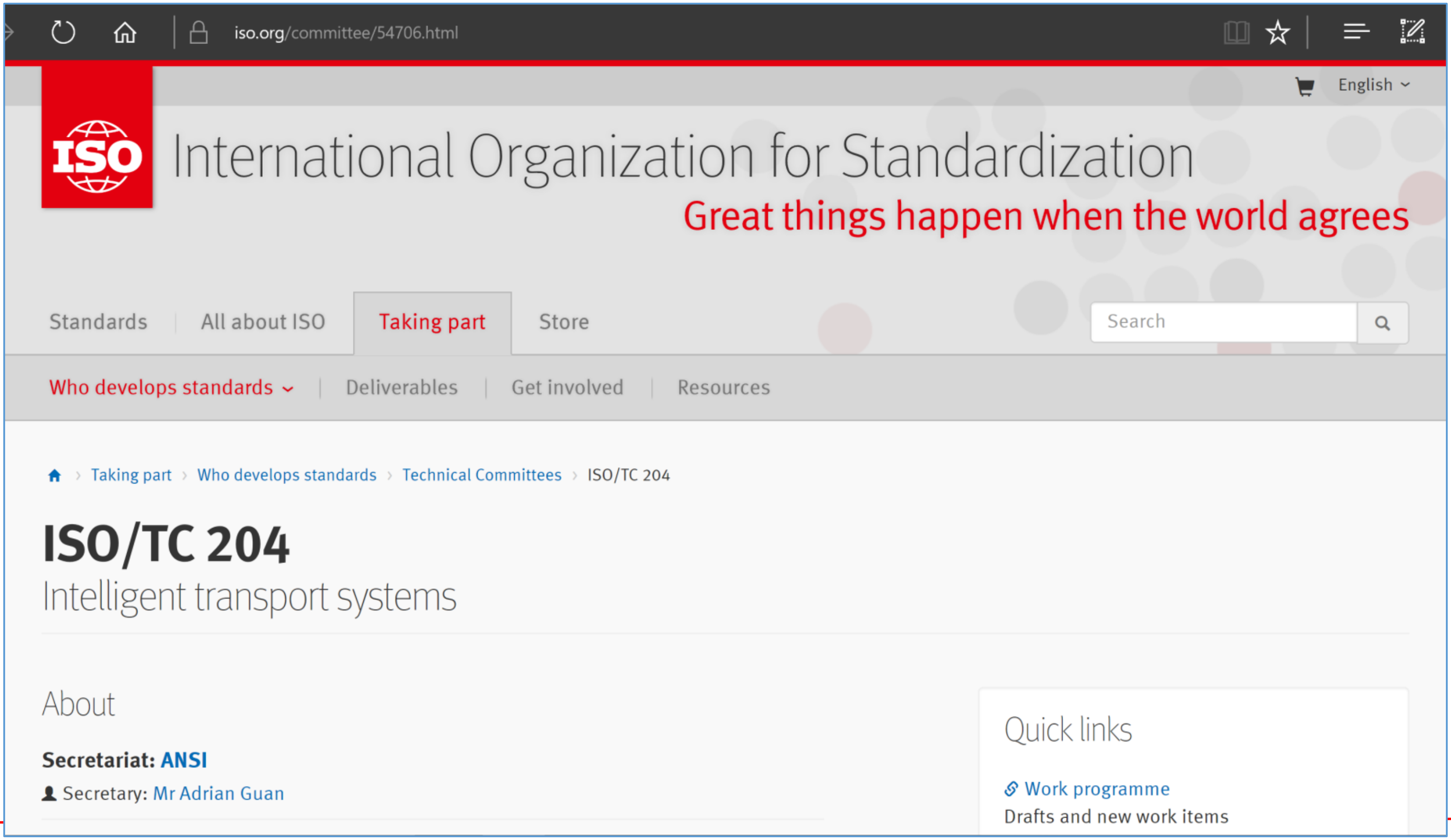
IoT

M2M

V2V / V2X

ISO/TC204 WG-18

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



iso.org/committee/54706.html
English
ISO
International Organization for Standardization
Great things happen when the world agrees
Standards
All about ISO
Taking part
Store
Search
Who develops standards
Deliverables
Get involved
Resources
Taking part › Who develops standards › Technical Committees › ISO/TC 204

ISO/TC 204

Intelligent transport systems

About

Secretariat: ANSI

Secretary: Mr Adrian Guan

Quick links

Work programme

Drafts and new work items

SBAS Signal Authentication

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

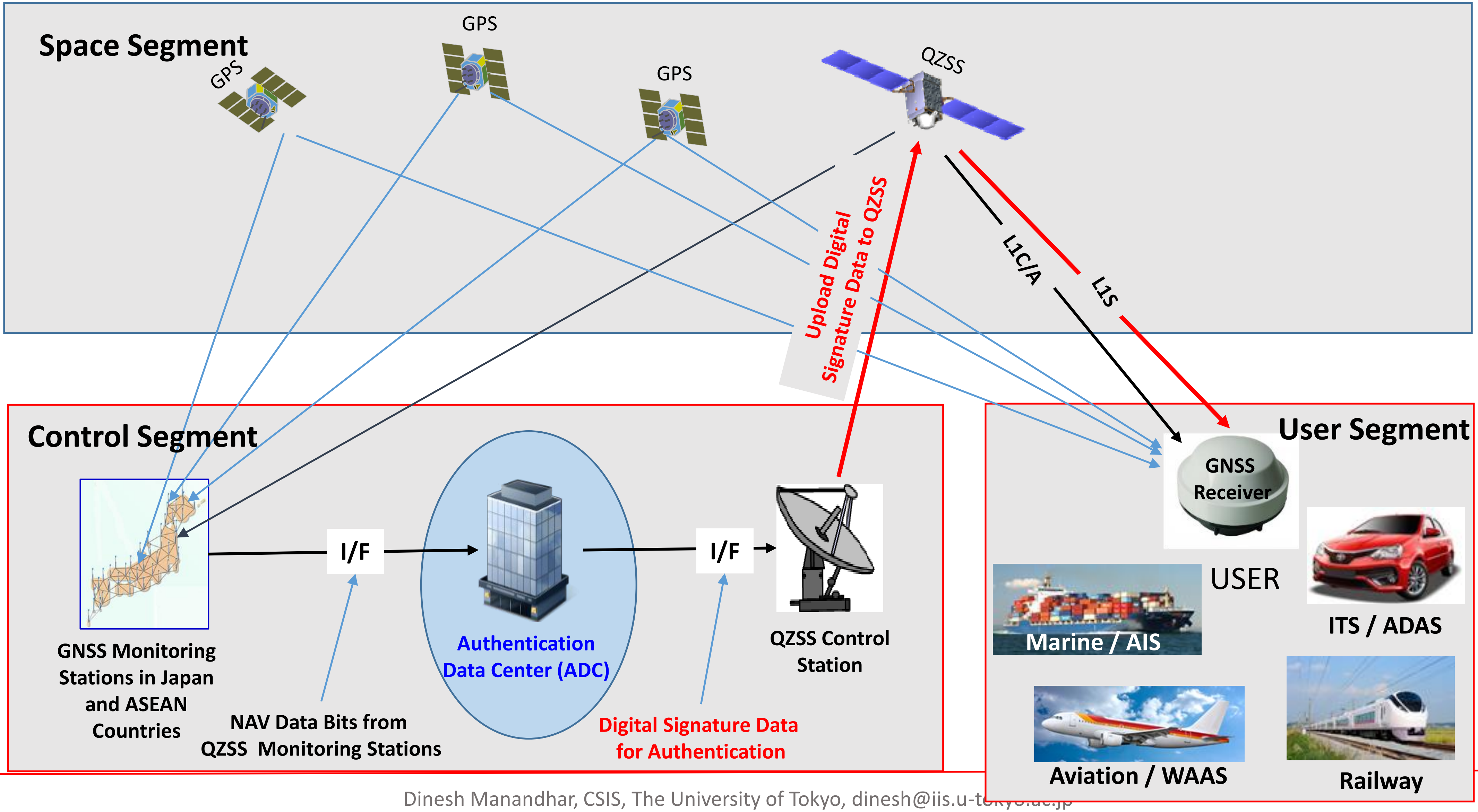
- ICAO is already highlighting the necessity and importance of SBAS Signal Authentication
  - New regulations that will require to Authenticate SBAS Signals for Anti-spoofing will emerge

We or You can solve the problem of Spoofing by Signal Authentication

Concept of Signal Authentication or Anti-Spoofing

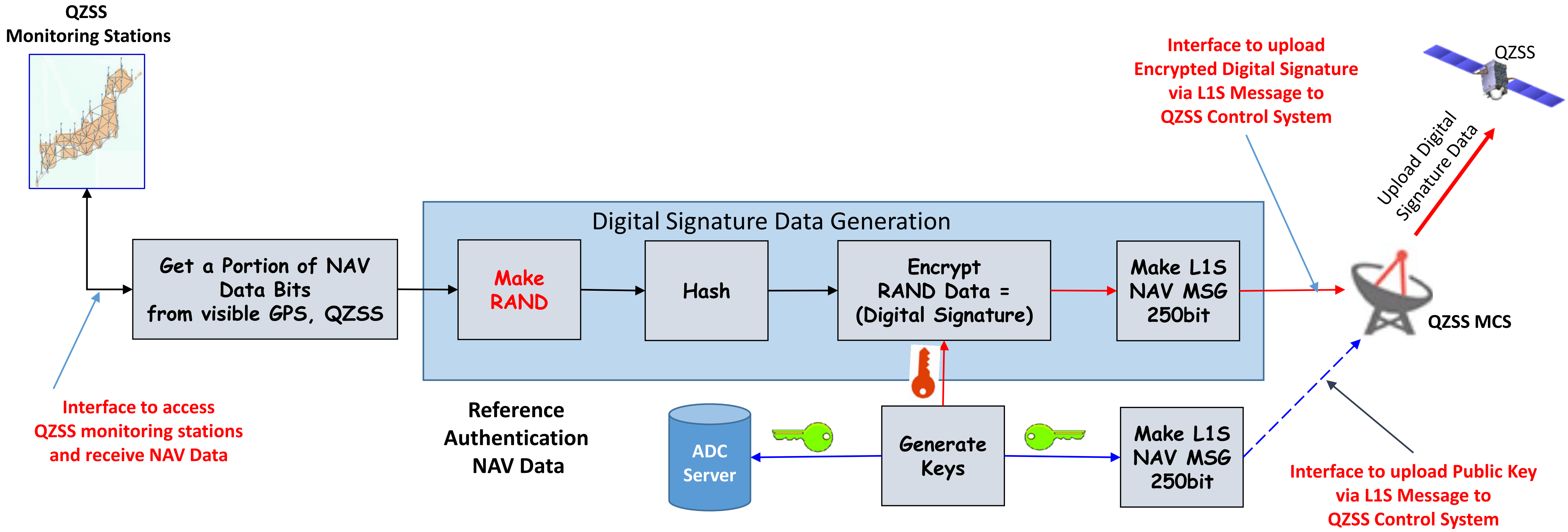
Simply, Broadcast a Digital Signature Data from QZSS Navigation Message

Authentication System Architecture

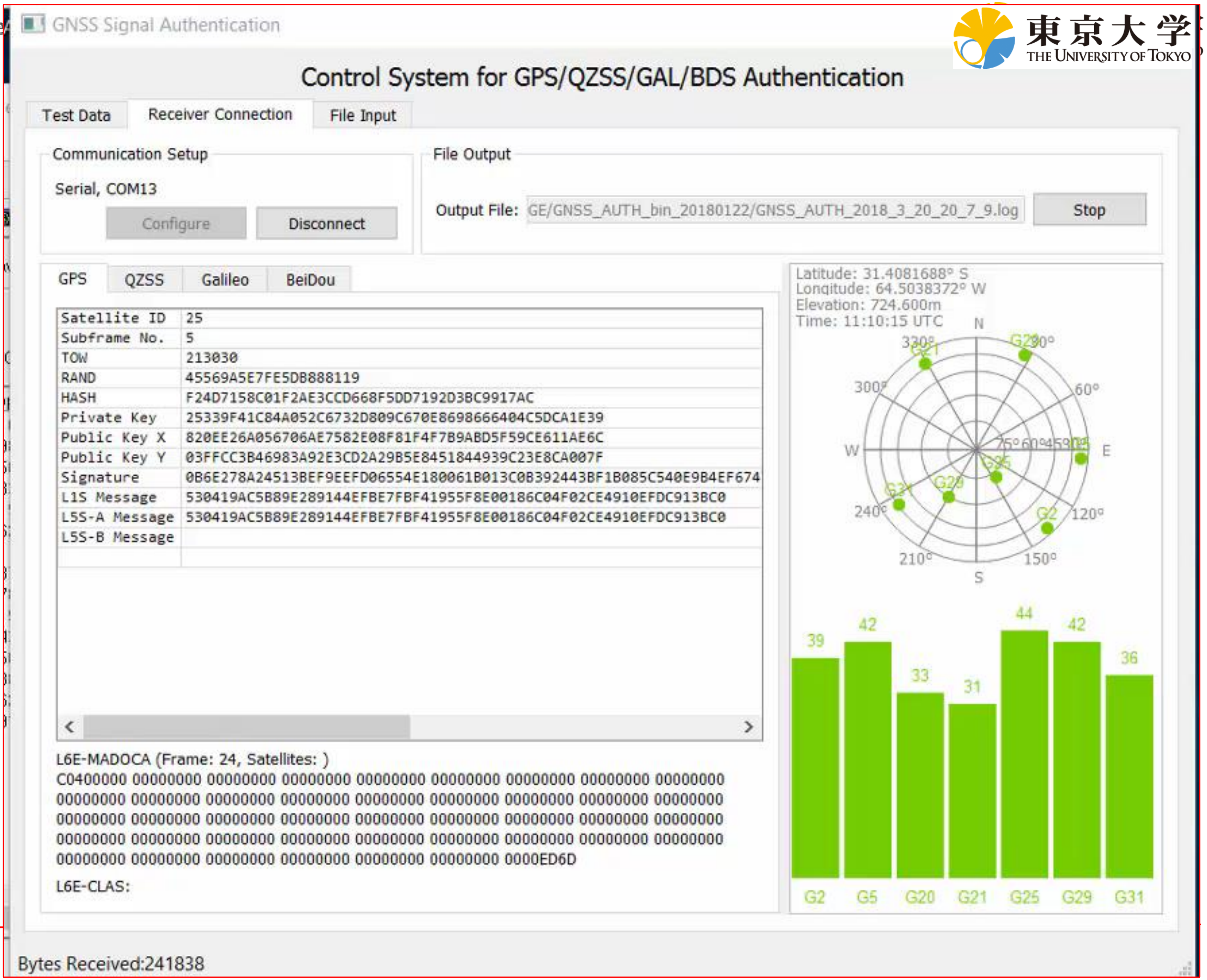


Space Segment
GPS
GPS
GPS
QZSS
Upload Digital Signature Data to QZSS
L1C/A
L1S
Control Segment
GNSS Monitoring Stations in Japan and ASEAN Countries
I/F
Authentication Data Center (ADC)
I/F
QZSS Control Station
NAV Data Bits from QZSS Monitoring Stations
Digital Signature Data for Authentication
User Segment
GNSS Receiver
USER
Marine / AIS
ITS / ADAS
Aviation / WAAS
Railway

Authentication System: Control Segment Development



Digital Signature Generation for Authentication



GNSS Signal Authentication

Control System for GPS/QZSS/GAL/BDS Authentication

Test Data | Receiver Connection | File Input

Communication Setup

Serial, COM13

Configure | Disconnect

File Output

Output File: GE/GNSS_AUTH_bin_20180122/GNSS_AUTH_2018_3_20_20_7_9.log

Stop

GPS | QZSS | Galileo | BeiDou

Satellite ID	25
Subframe No.	5
TOW	213030
RAND	45569A5E7FE5DB888119
HASH	F24D7158C01F2AE3CCD668F5DD7192D3BC9917AC
Private Key	25339F41C84A052C6732D809C670E8698666404C5DCA1E39
Public Key X	820EE26A056706AE7582E08F81F4F7B9ABD5F59CE611AE6C
Public Key Y	03FFCC3B46983A92E3CD2A29B5E8451844939C23E8CA007F
Signature	0B6E278A24513BEF9EEFD06554E180061B013C0B392443BF1B085C540E9B4EF674
L1S Message	530419AC5B89E289144EFBE7FBF41955F8E00186C04F02CE4910EFDC913BC0
L5S-A Message	530419AC5B89E289144EFBE7FBF41955F8E00186C04F02CE4910EFDC913BC0
L5S-B Message	

L6E-MADOCA (Frame: 24, Satellites:)

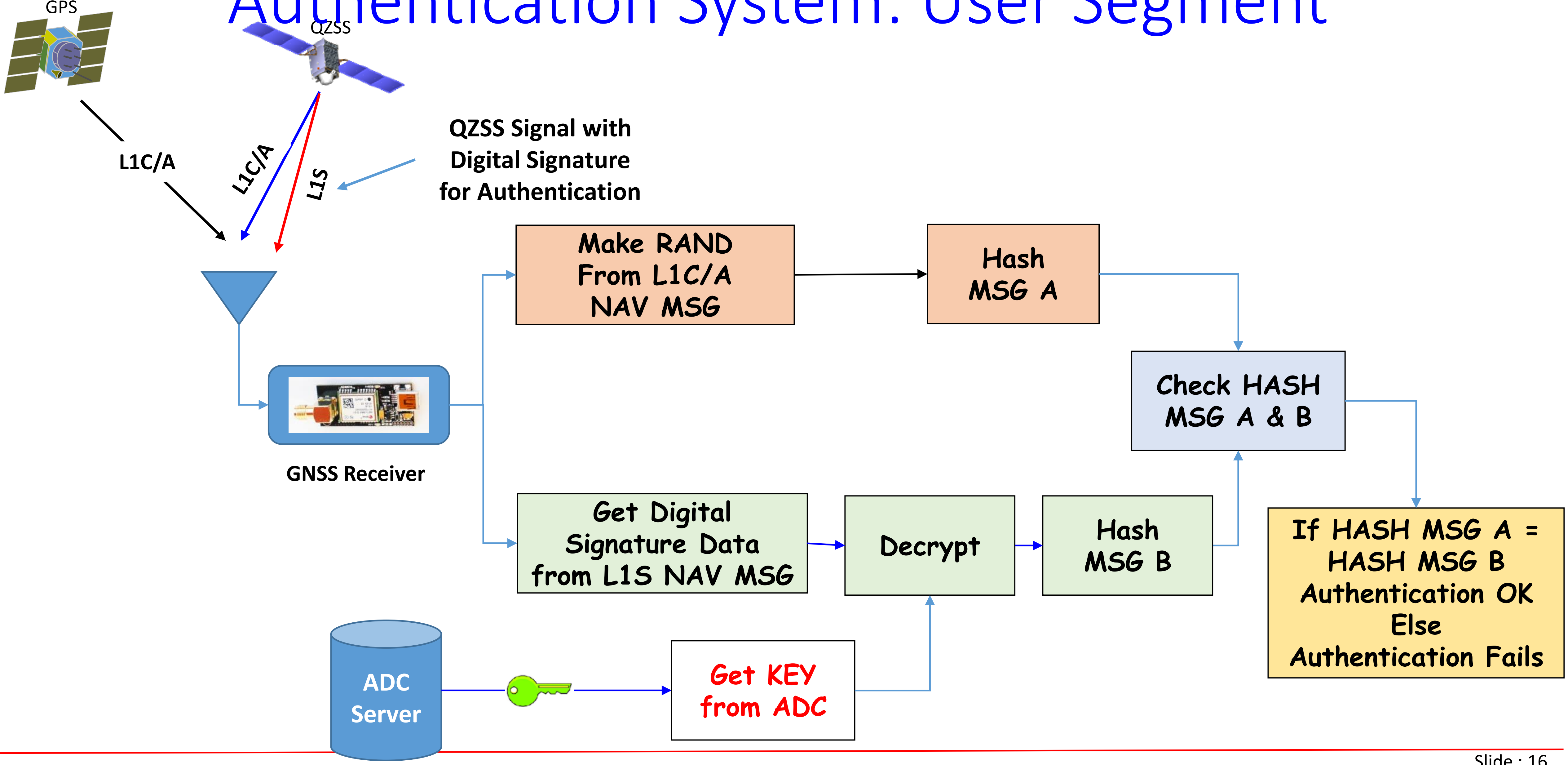
```
C0400000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 0000ED6D
```

L6E-CLAS:

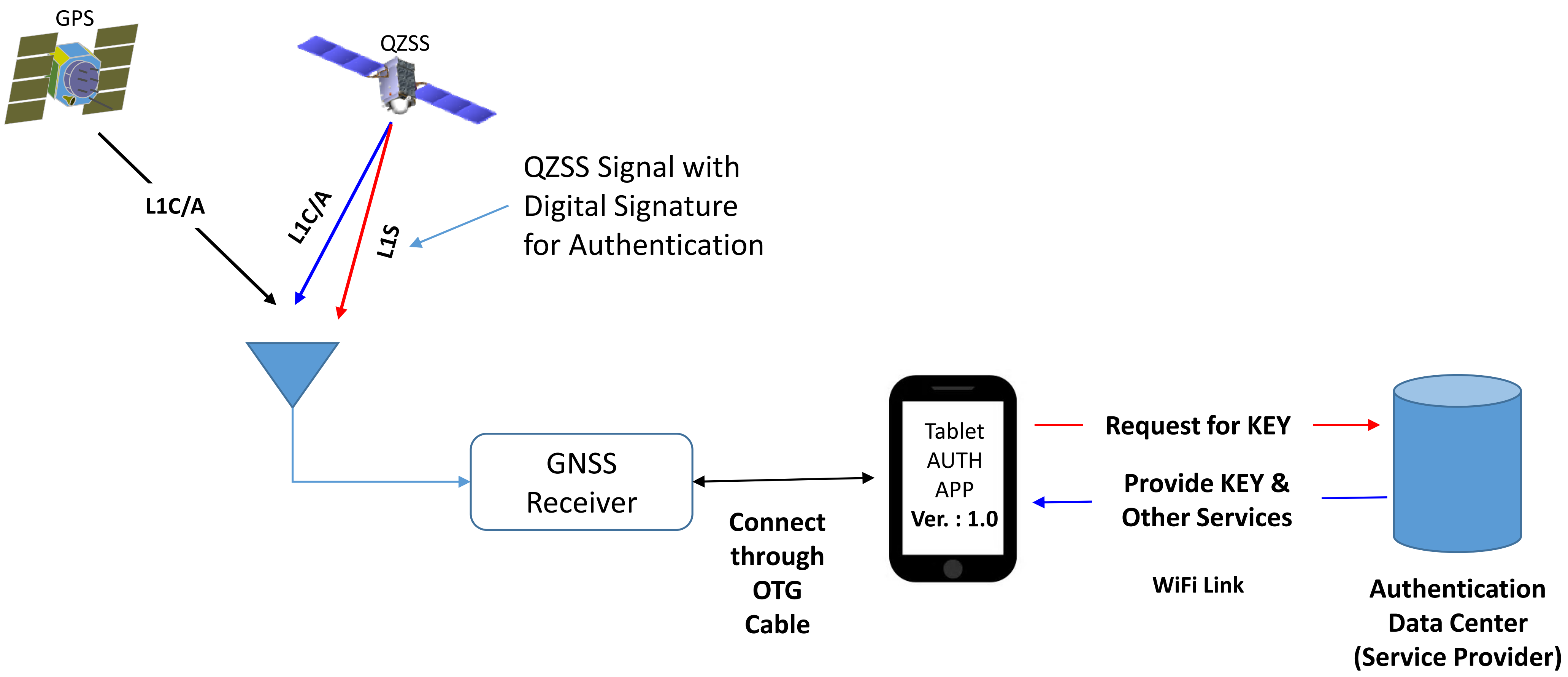
Latitude: 31.4081688° S
Longitude: 64.5038372° W
Elevation: 724.600m
Time: 11:10:15 UTC

Bytes Received:241838

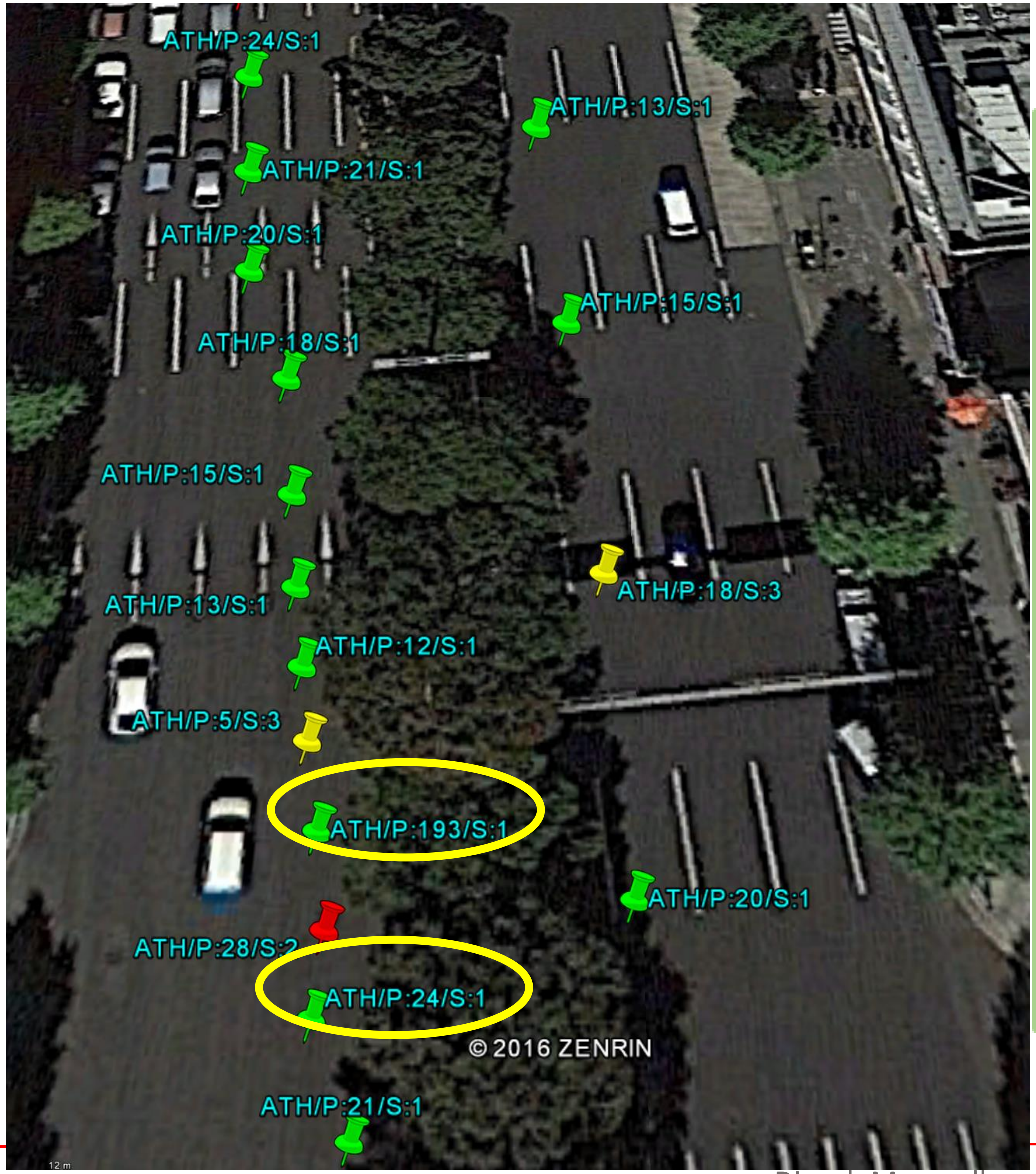
Authentication System: User Segment

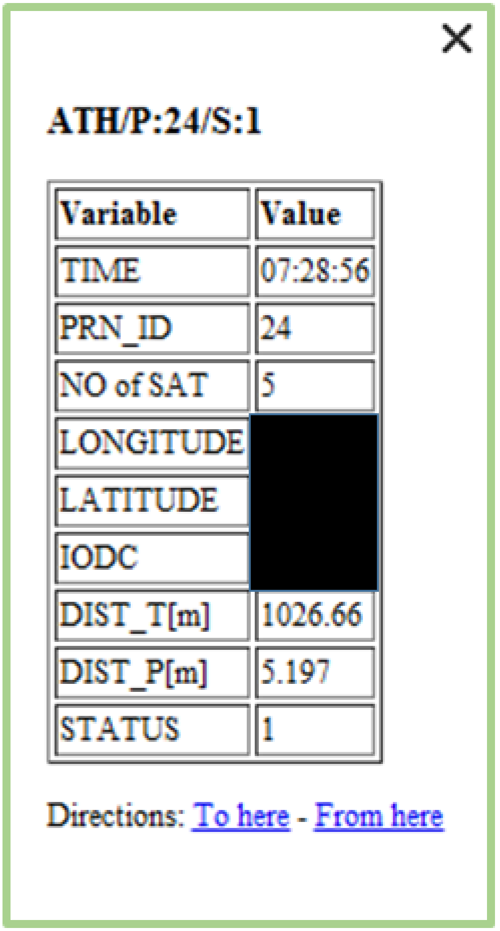


Prototype Anti-Spoofing Receiver


GPS
QZSS
L1C/A
L1C/A
L1S
QZSS Signal with Digital Signature for Authentication
GNSS Receiver
Connect through OTG Cable
Tablet AUTH APP Ver. : 1.0
Request for KEY
Provide KEY & Other Services
WiFi Link
Authentication Data Center (Service Provider)

Real-time Authentication Test by Car Driving

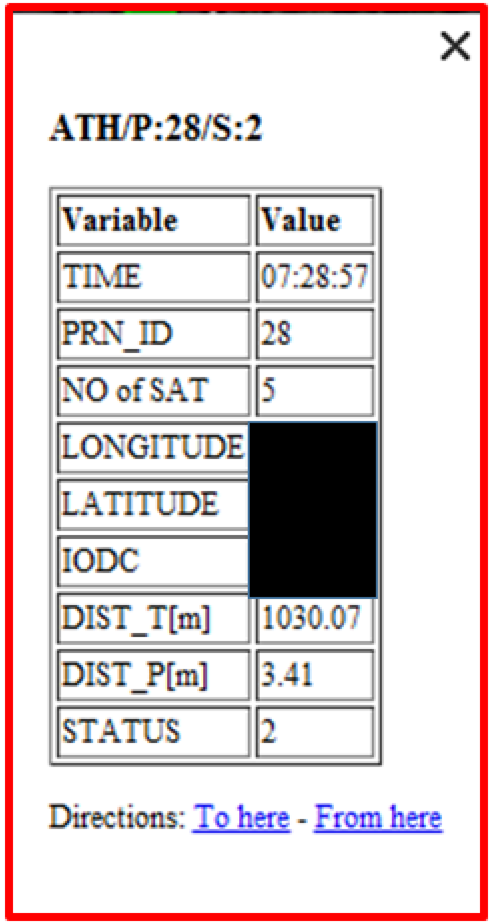




ATH/P:24/S:1

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

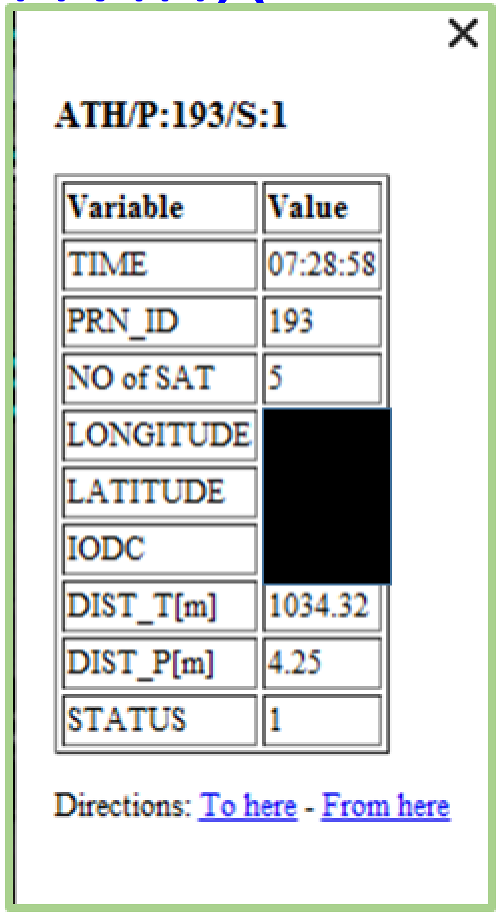
Directions: To here - From here



ATH/P:28/S:2

Variable	Value
TIME	07:28:57
PRN_ID	28
NO of SAT	5
LONGITUDE	[redacted]
LATITUDE	[redacted]
IODC	[redacted]
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	[redacted]
IODC	[redacted]
DIST_T[m]	1034.32
DIST_P[m]	4.25
STATUS	1

Directions: To here - From here

Authentication Signal is broadcasted from QZSS L1S signal for 3 months on various occasions for Live Authentication Test.

Thanks to JAXA for broadcasting Test Authentication Signal.

Summary

- QZSS Signals can be used to Authenticate GPS
  - Other GNSS signals can also be authenticated
    - GALILEO, BEIDOU etc

- This method can be implemented without any impact on HW
  - Only Software/Firmware modifications are required control and user systems

Recommendation

Please include SPOOFING and ANTI-SPOOFING Issues in ICG IDM WG

Additional Information

Please visit website at

http://www.csis.u-tokyo.ac.jp/~dinesh/

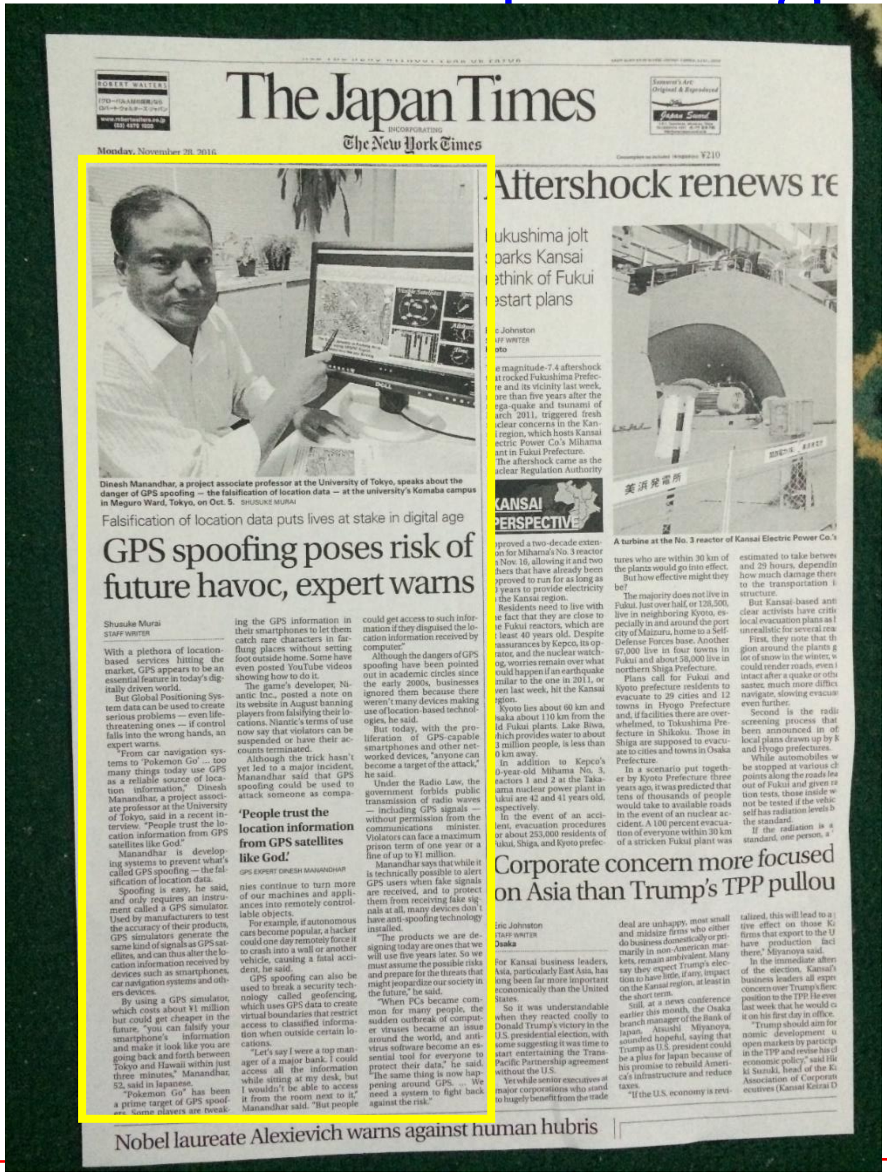
Or Contact:

dinesh@csis.u-tokyo.ac.jp

Reference Slides

GPS Spoofing Poses Risk of Future Havoc

NOV 28, 2016



ALL THE NEWS WITHOUT FEAR OR FAVOR

The Japan Times
INCORPORATING
The New York Times

Monday, November 28, 2016

¥210

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

> 'People trust the location information from GPS satellites like God.'
> GPS EXPERT DINESH MANANDHAR

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."

Aftershock renews re

ukushima jolt
parks Kansai
ethink of Fukui
estart plans

c Johnston
AFF WRITER
oto

e magnitude-7.4 aftershock
t rocked Fukushima Prefec-
re and its vicinity last week,
ore than five years after the
ega-quake and tsunami of
arch 2011, triggered fresh
clear concerns in the Kan-
i region, which hosts Kansai
ectric Power Co.'s Mihama
ant in Fukui Prefecture.
The aftershock came as the
clear Regulation Authority

KANSAI
PERSPECTIVE

pproved a two-decade exten-
on for Mihama's No. 3 reactor
Nov. 16, allowing it and two
hers that have already been
pproved to run for as long as
years to provide electricity
the Kansai region.
Residents need to live with
e fact that they are close to
e Fukui reactors, which are
least 40 years old. Despite
assurances by Kepco, its op-
ator, and the nuclear watch-
og, worries remain over what
ould happen if an earthquake
milar to the one in 2011, or
ven last week, hit the Kansai
gion.
Kyoto lies about 60 km and
saka about 110 km from the
ld 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-
ama nuclear power plant in
ukui are 42 and 41 years old,
espectively.
In the event of an acci-
ent, evacuation procedures
or about 253,000 residents of
ukui, Shiga, and Kyoto prefec-

美浜発電所

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

tures who are within 30 km of the plants would go into effect.

But how effective might they be?

The majority does not live in Fukui. Just over half, or 128,500, live in neighboring Kyoto, especially in and around the port city of Maizuru, home to a Self-Defense Forces base. Another 67,000 live in four towns in Fukui and about 58,000 live in northern Shiga Prefecture.

Plans call for Fukui and Kyoto prefecture residents to evacuate to 29 cities and 12 towns in Hyogo Prefecture and, if facilities there are overwhelmed, to Tokushima Prefecture in Shikoku. Those in Shiga are supposed to evacuate to cities and towns in Osaka Prefecture.

In a scenario put together by Kyoto Prefecture three years ago, it was predicted that tens of thousands of people would take to available roads in the event of an nuclear accident. A 100 percent evacuation of everyone within 30 km of a stricken Fukui plant was

estimated to take betwe
and 29 hours, dependin
how much damage there
to the transportation i
structure.
But Kansai-based ant
clear activists have criti
local evacuation plans as l
unrealistic for several rea
First, they note that th
gion around the plants g
lot of snow in the winter, w
could render roads, even i
intact after a quake or oth
saster, much more diffic
navigate, slowing evacua
even further.
Second is the radi
screening process that
been announced in of
local plans drawn up by K
and Hyogo prefectures.
While automobiles w
be stopped at various c
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

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

ric 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-

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
concern over Trump's fierc
position to the TPP. He eve
last week that he would c
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 Hi
ki Suzuki, head of the K
Association of Corporat
ecutives (Kansai Keizai D

Nobel laureate Alexievich warns against human hubris

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

Japan Supreme Court Ruling: GPS Tracking is Illegal without Warrant

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 令状なし違法

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）

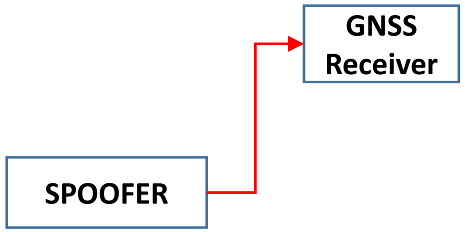
Spoofing Methods

Spoofing Level 0

Self-Spoofing

Receiver and Spoofer directly connected by cable

Real Signal not Present

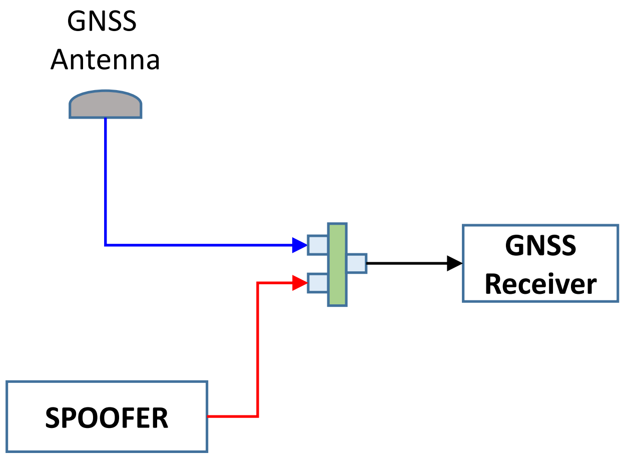


Spoofing Level 1

Self-Spoofing

Receiver and Spoofer directly connected by cable

Real Signal Present

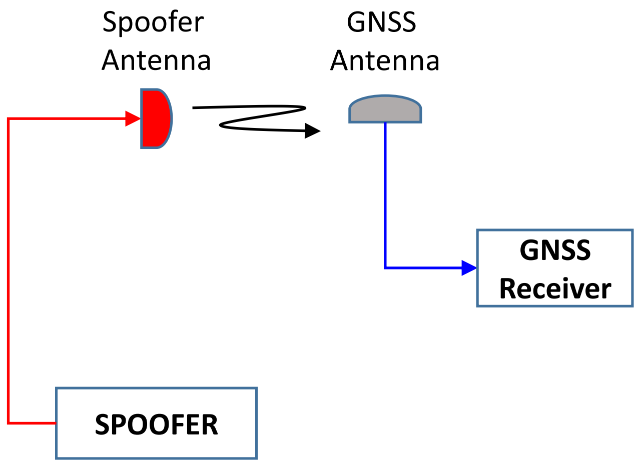


Spoofing Level 2

Self-Spoofing or 3rd Party Spoofing

Over-the-Air Spoof Signal Transmission

Real Signal Present



How to get Anti-Spoofing Solutions?

- Encrypt PRN Codes
  - Similar to GPS P(Y) Code
  - Very Secure but not a practical solution for normal operation
  - Can’t use for existing signals
  - Requires signal modification
  - All applications do not need Anti-Spoofing protection
- Encrypt Navigation Message (NAM: Navigation Message Authenticate)
  - Secure but position output always requires decryption of navigation data
  - Not a practical solution for normal operation
  - All applications do not need anti-spoofing protection
  - Requires signal modification
- Broadcast Digital Signature in Navigation Message
  - Broadcast a Digital Signature based on the Satellite Signal that need to be authenticated
  - Very practical solution
  - Need to verify only when required
  - Can be used for existing signals
  - No impact on Hardware. Only software modification