

GPS and QZSS Signal Authentication using QZSS Signal

Dinesh Manandhar, R. Shibasaki
Center for Spatial Information Science (CSIS)
The University of Tokyo, Japan

dinesh@iis.u-tokyo.ac.jp

Can You Trust GPS Position & Time Data?

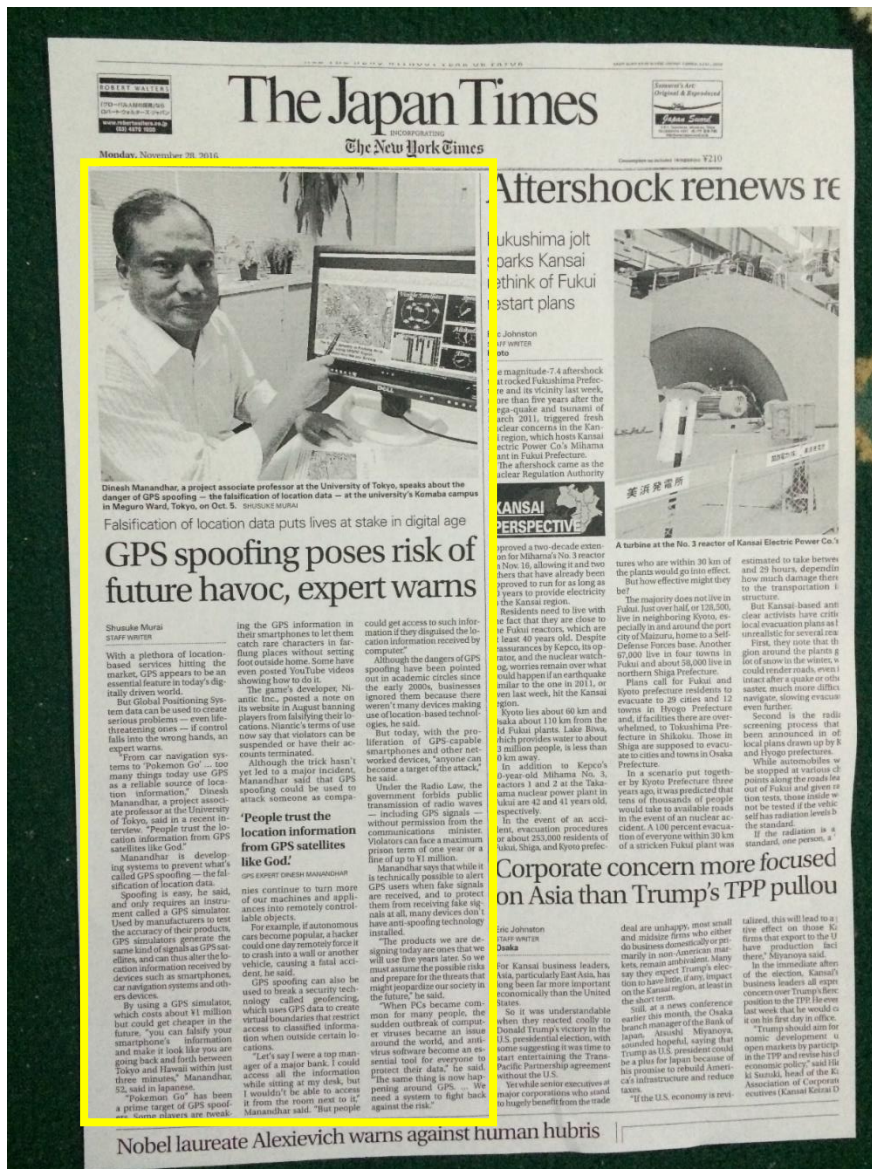
Yes, You can...

...But Need to Verify

Because of Spoofing Issues

GPS Spoofing Poses Risk of Future Havoc

NOV 28, 2016



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.

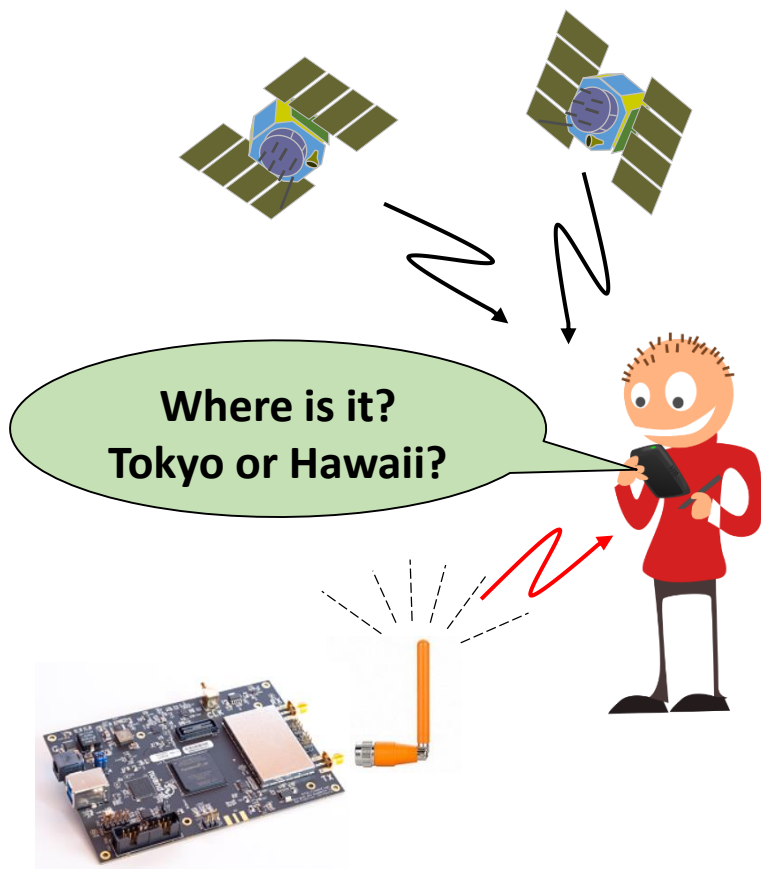
GPS捜査 令状なし違法



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）

What is Location Spoofing?

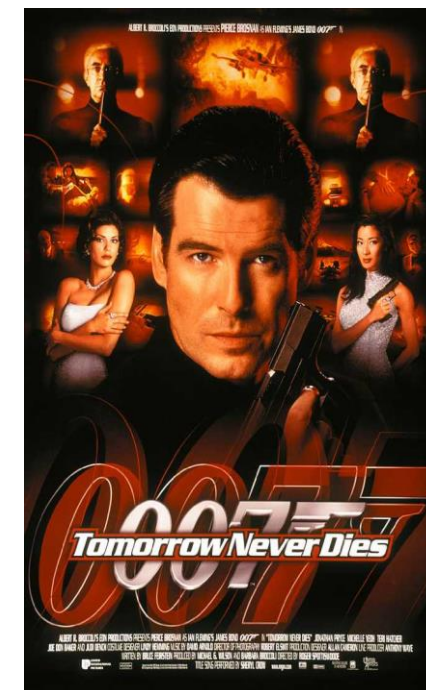
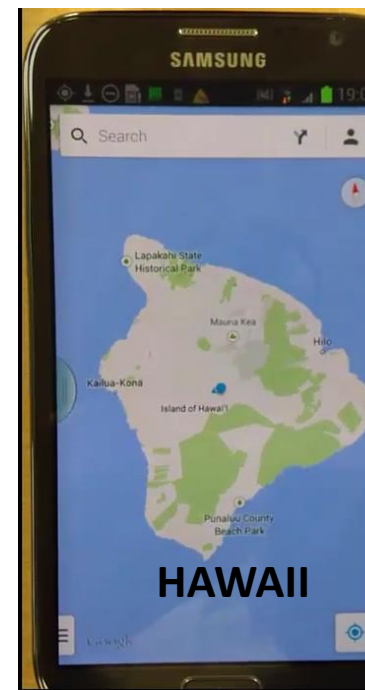
- Falsify Location Data as If it were True Location



Spoofing board

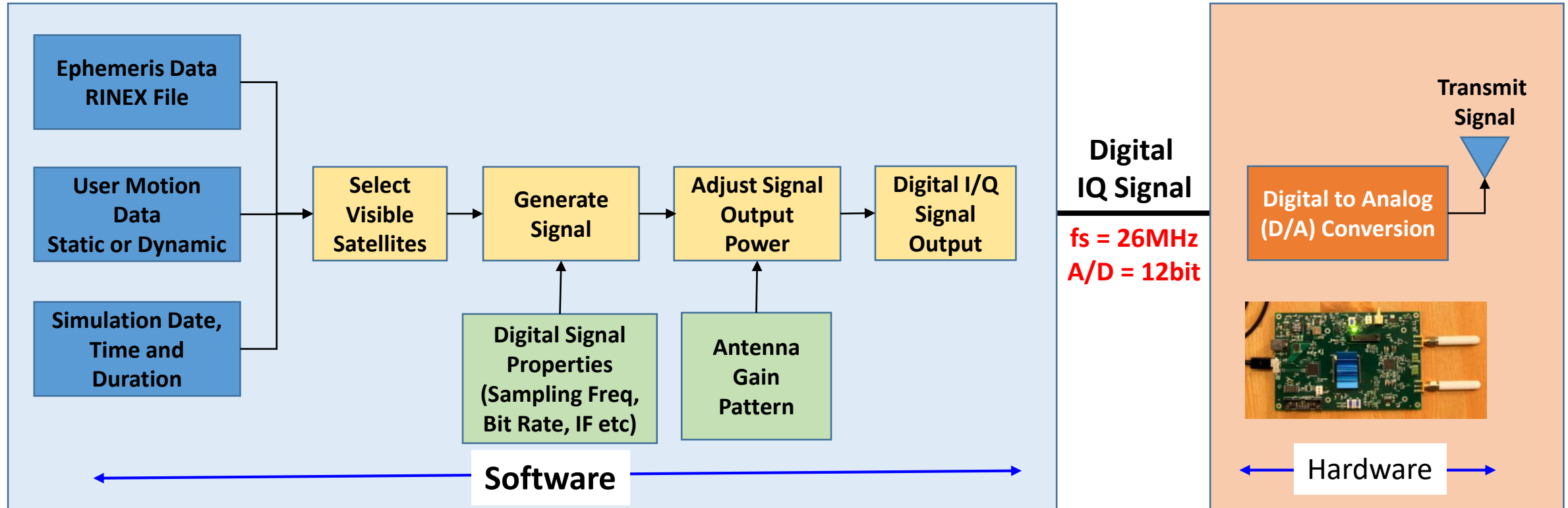


TOKYO
Or
Hawaii?

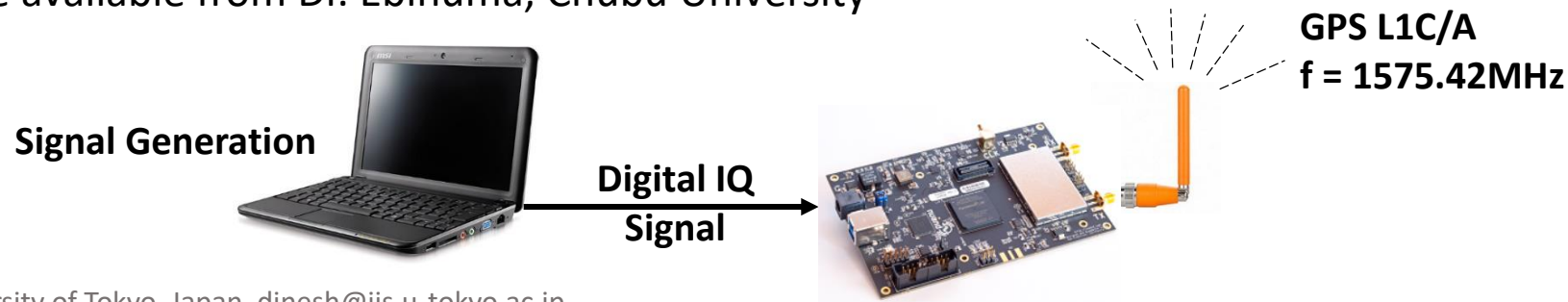


This movie is all about GPS Spoofing

Software-Based GPS Signal Generator (Spoofer?)

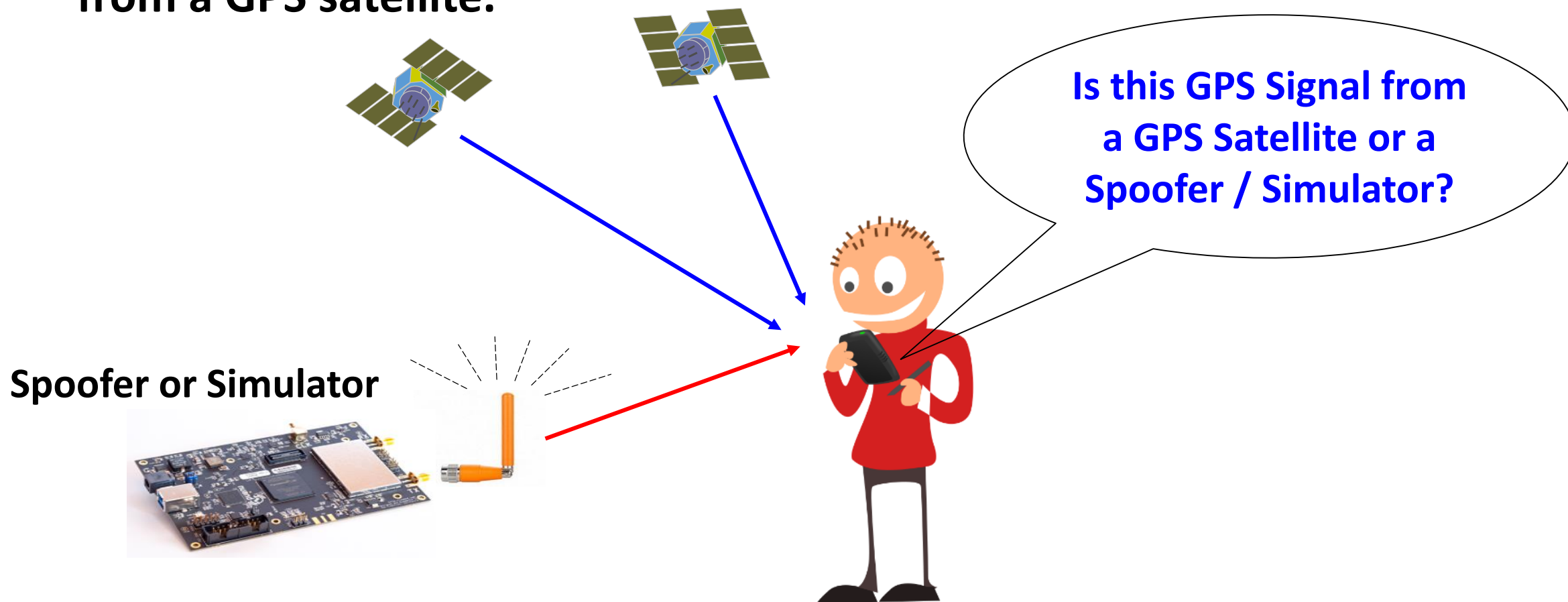


Software Source available from Dr. Ebinuma, Chubu University



What is GPS Signal Authentication?

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

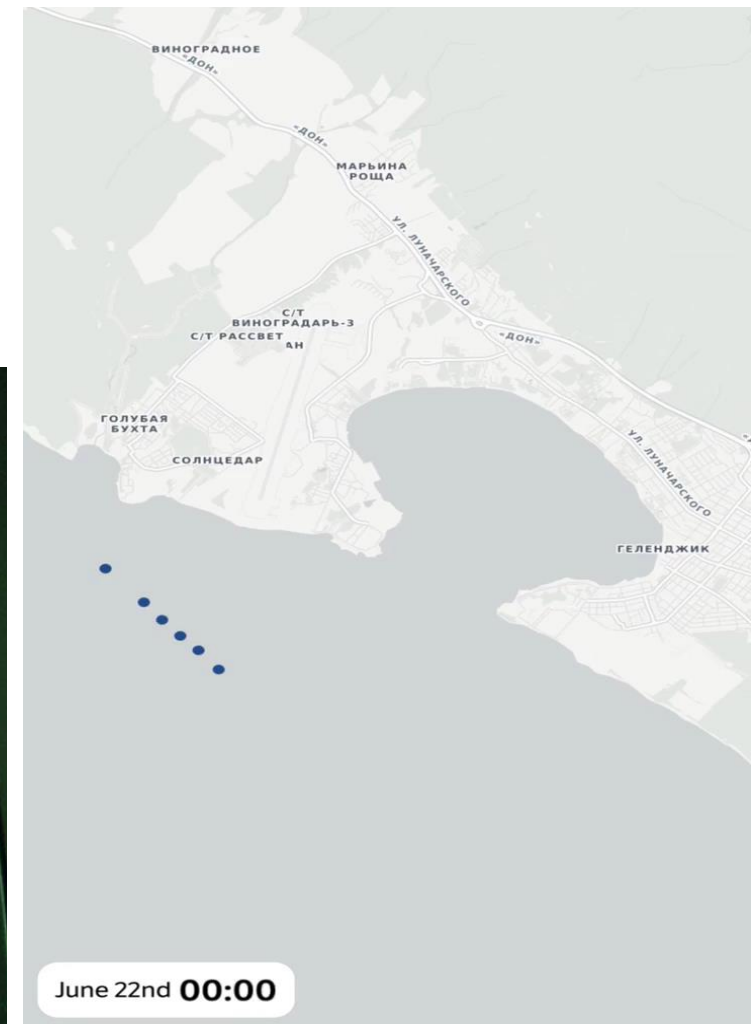
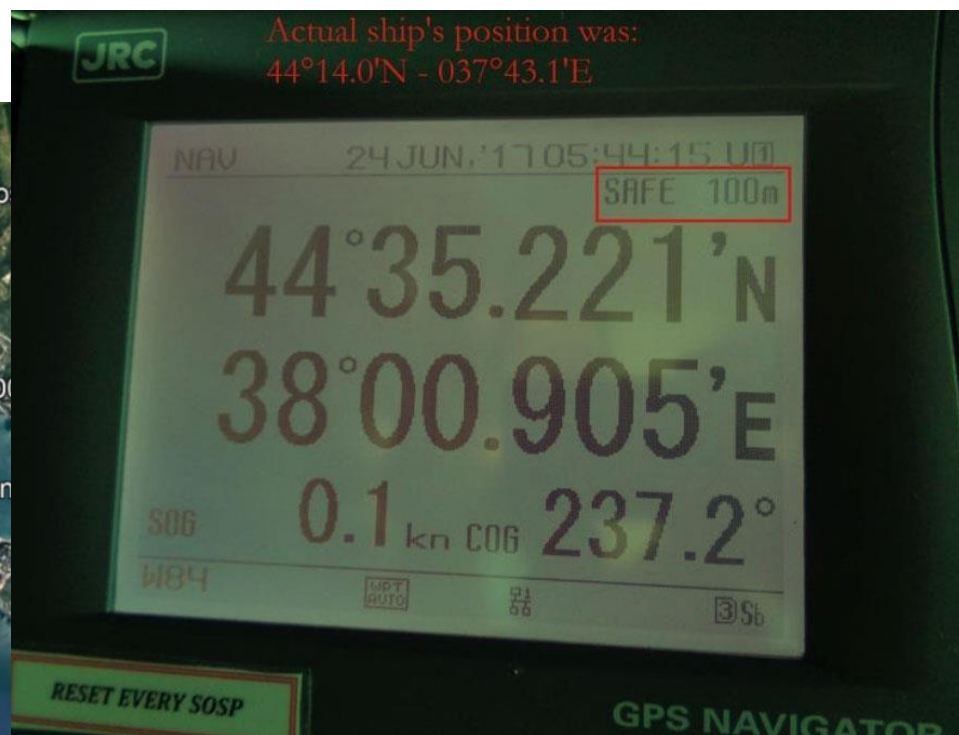


GPS Signal Authentication is necessary to detect SPOOF Signals

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.....



SPOOFing a Car: Is he driving the car?



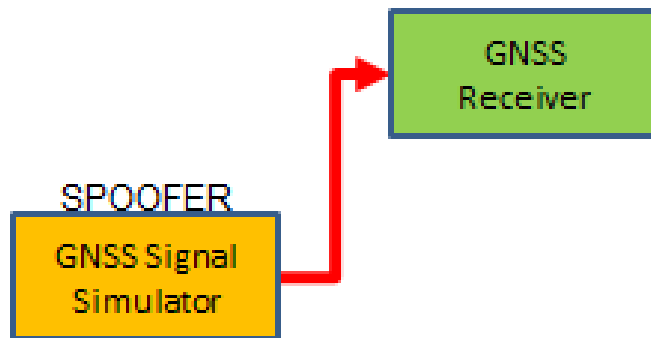
Spoofing Methods

Self-Spoofing
Connect by cable, No Real Signal,

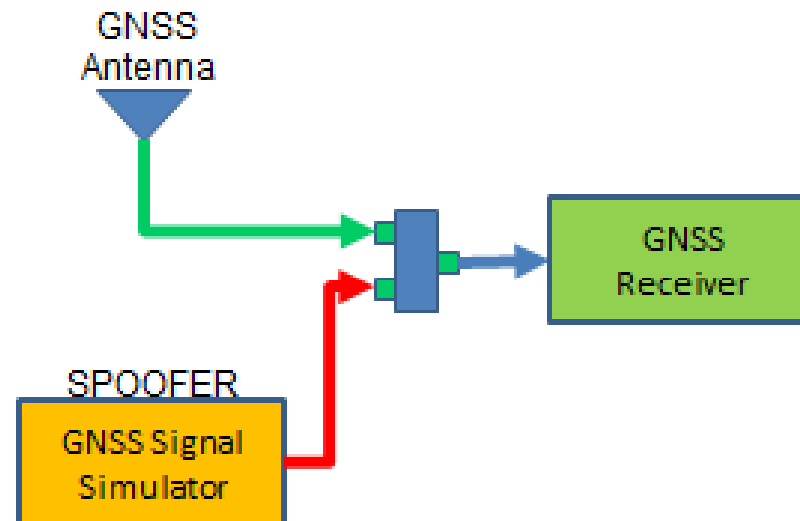
Self-Spoofing
Connect by cable, Real Signal Present

Self or 3rd Party Spoofing
Over the air transmission

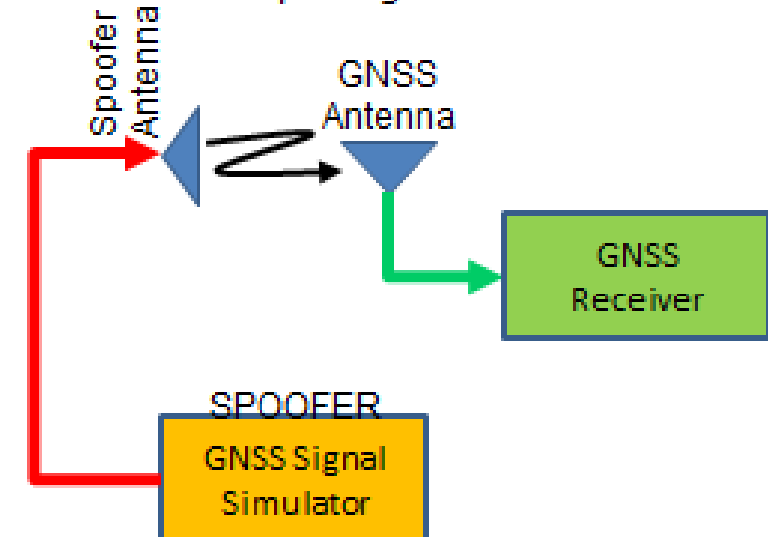
Spoofing Level 0



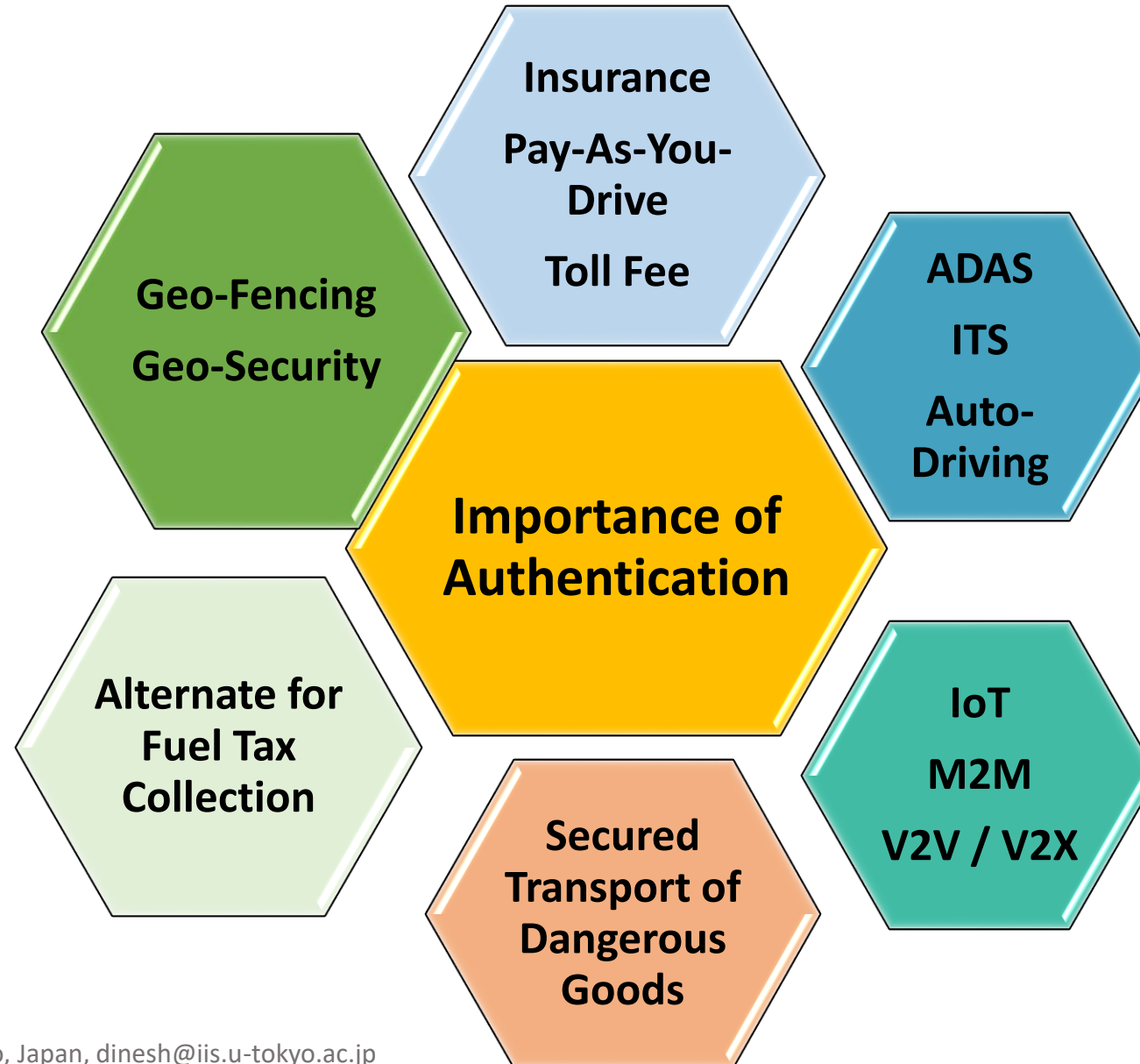
Spoofing Level 1



Spoofing Level 2

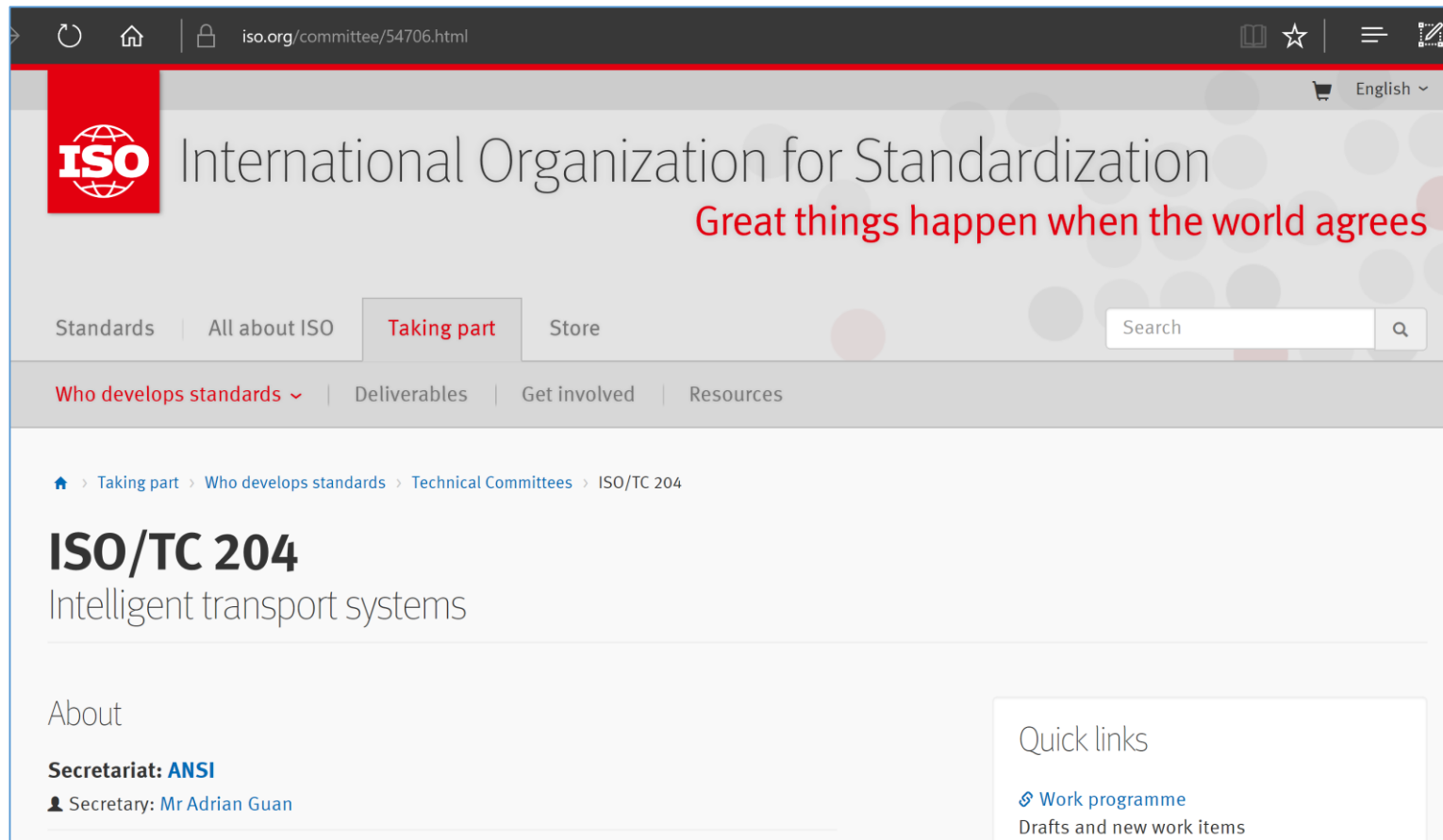


Why Authentication is Necessary ?



ISO/TC204 WG-18

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



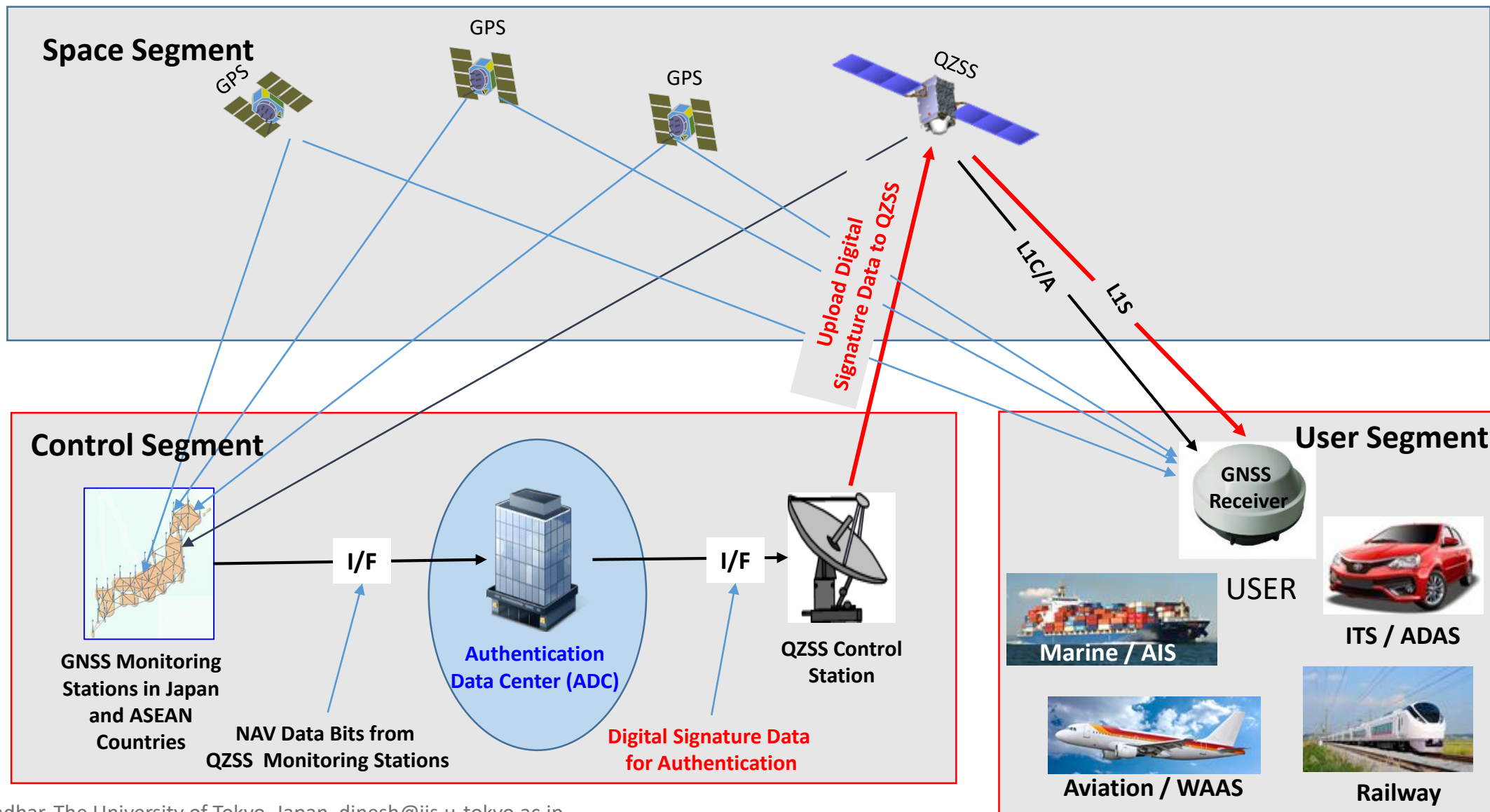
The screenshot shows the ISO website page for ISO/TC 204. The page features the ISO logo and the text "International Organization for Standardization" and "Great things happen when the world agrees". The navigation menu includes "Standards", "All about ISO", "Taking part", and "Store". The breadcrumb trail is "Home > Taking part > Who develops standards > Technical Committees > ISO/TC 204". The main heading is "ISO/TC 204" with the subtitle "Intelligent transport systems". The "About" section lists the secretariat as ANSI and the secretary as Mr Adrian Guan. The "Quick links" section includes "Work programme" and "Drafts and new work items".

We can solve the problem of Spoofing by Signal Authentication

Concept of Signal Authentication

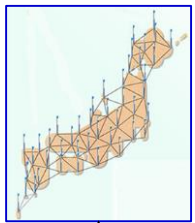
**Broadcast a Digital Signature Data
in the QZSS Navigation Message**

Authentication System Architecture

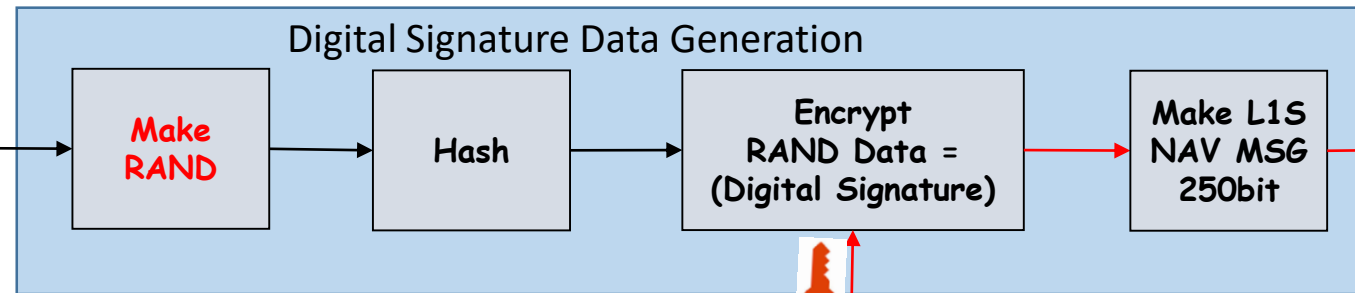


Authentication System: Control Segment Development

QZSS
Monitoring Stations



Get a Portion of NAV
Data Bits
from visible GPS, QZSS



Interface to access
QZSS monitoring stations
and receive NAV Data

Reference
Authentication
NAV Data



Generate
Keys

Interface to upload
Encrypted Digital Signature
via L1S Message to
QZSS Control System

Interface to upload Public Key
via L1S Message to
QZSS Control System



Digital Signature Generation for Authentication

GNSS Signal Authentication

File

Test Data Receiver Connection File Input

Communication Setup

Serial, COM16

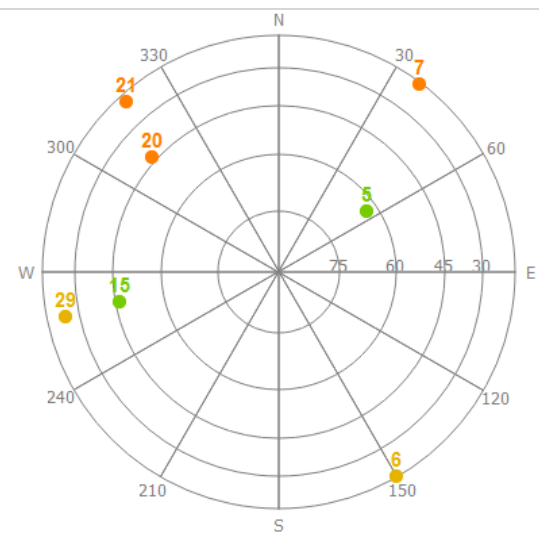
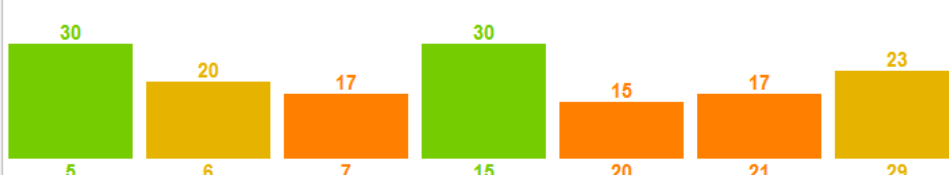
Configure Disconnect

File Output

Output File: C:/Dinesh/QZSS_AUTH_RESEARCH/SystemDevelopment/SSAGE/GNSS_Auth_bin_20171204/GNSS_Auth_bin/20171204-1.csv

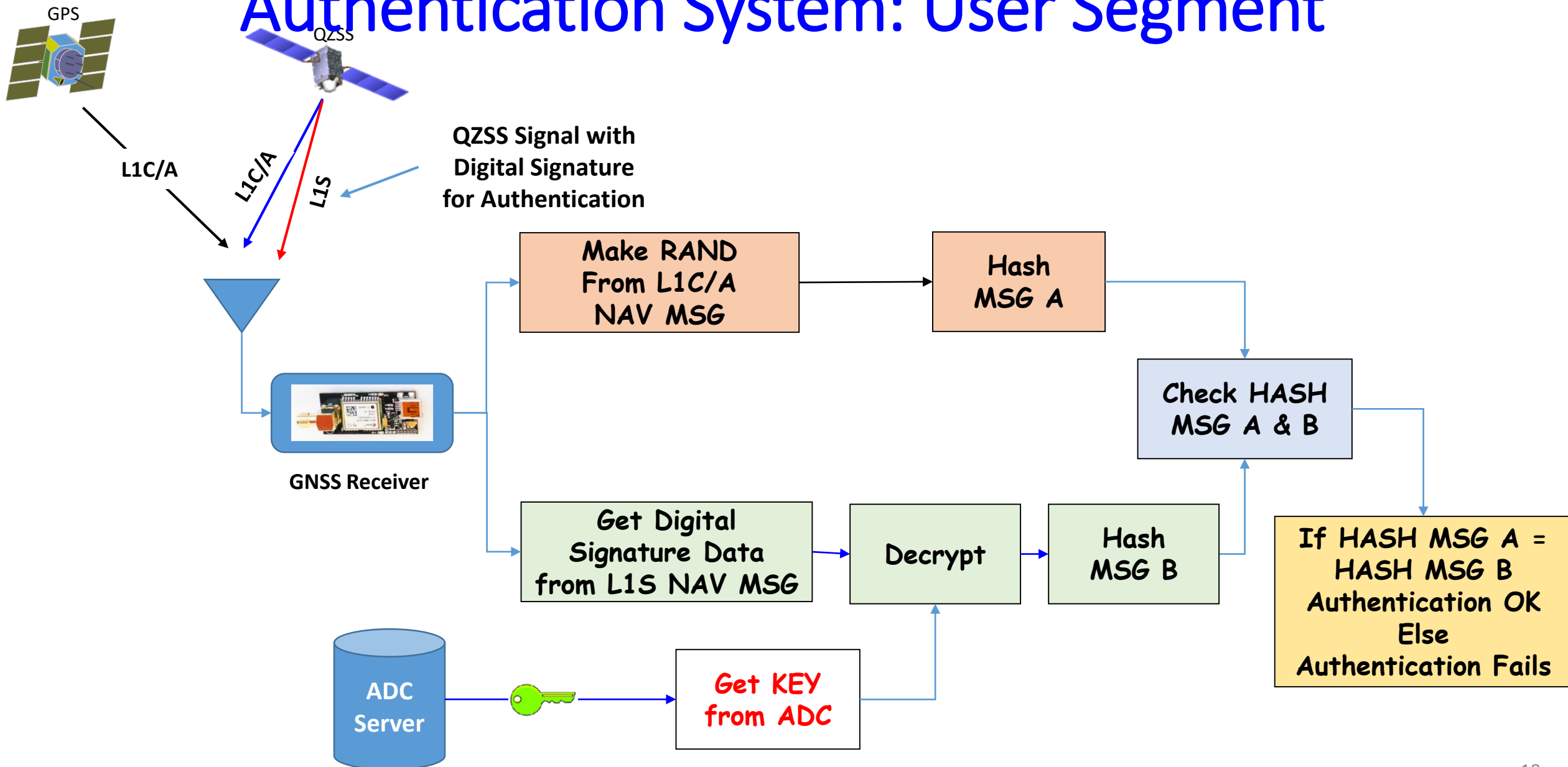
Browse Stop

| | |
|--------------|---|
| Satellite ID | 5 |
| Subframe No. | 1 |
| TOW | 185796 |
| RAND | 3C7B16DA00057EA47305 |
| HASH | 054C79C50C60A2F2446CA92186ACF4B97CA5F7F2 |
| Private Key | DF6266778D1DA835275709BF01AF60F51E91606851C9F1C8 |
| Public Key X | 592288D2E37D46671DD004A702FD208BE306CA936787AF06 |
| Public Key Y | 19D49B6E4BC5251364405885E6C30DA5883F79C59149170E |
| Signature | D581BDE05F21C1647F035CF98A29CC86FE9FFEEFB02365308AF48D6C78000C01C1080BD47DB1F6F9D015110F0F69ECD25 |
| L1S Message | 9A04053DF7E0EFF817C8F0591FC0D7FEE28AF3EDFFE7FFBEC08D94C80000000 |
| | |
| Satellite ID | 13 |
| Subframe No. | 1 |
| TOW | 185796 |
| RAND | 3C7B16DA7FFF79CDF70D |
| HASH | 3F586F128131479BE57E30133629BD7AC067F8F3 |
| Private Key | DF6266778D1DA835275709BF01AF60F51E91606851C9F1C8 |
| Public Key X | 592288D2E37D46671DD004A702FD208BE306CA936787AF06 |
| Public Key Y | 19D49B6E4BC5251364405885E6C30DA5883F79C59149170E |
| Signature | 40E0DFE3AA2FAF279165F99FF36C875F83D8B1D8255A68A48CF45E5C481DC53A0D3C39E4F084BAE99E9F867A7AFE461D |
| L1S Message | 9A040D3DF6F8F7F8EA8BEBC9E459FEE7FCDBE1D7E0F6ECF609569AE900000000 |
| | |
| Satellite ID | 15 |
| Subframe No. | 5 |
| TOW | 185790 |
| RAND | |
| HASH | |
| Private Key | DF6266778D1DA835275709BF01AF60F51E91606851C9F1C8 |
| Public Key X | 592288D2E37D46671DD004A702FD208BE306CA936787AF06 |
| Public Key Y | 19D49B6E4BC5251364405885E6C30DA5883F79C59149170E |
| Signature | |
| L1S Message | |

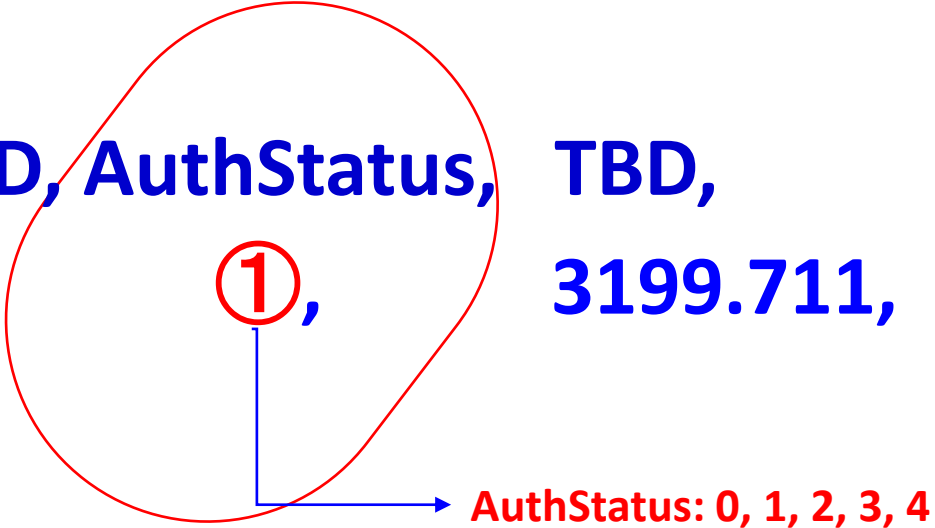
Bytes Received:1379543

Authentication System: User Segment



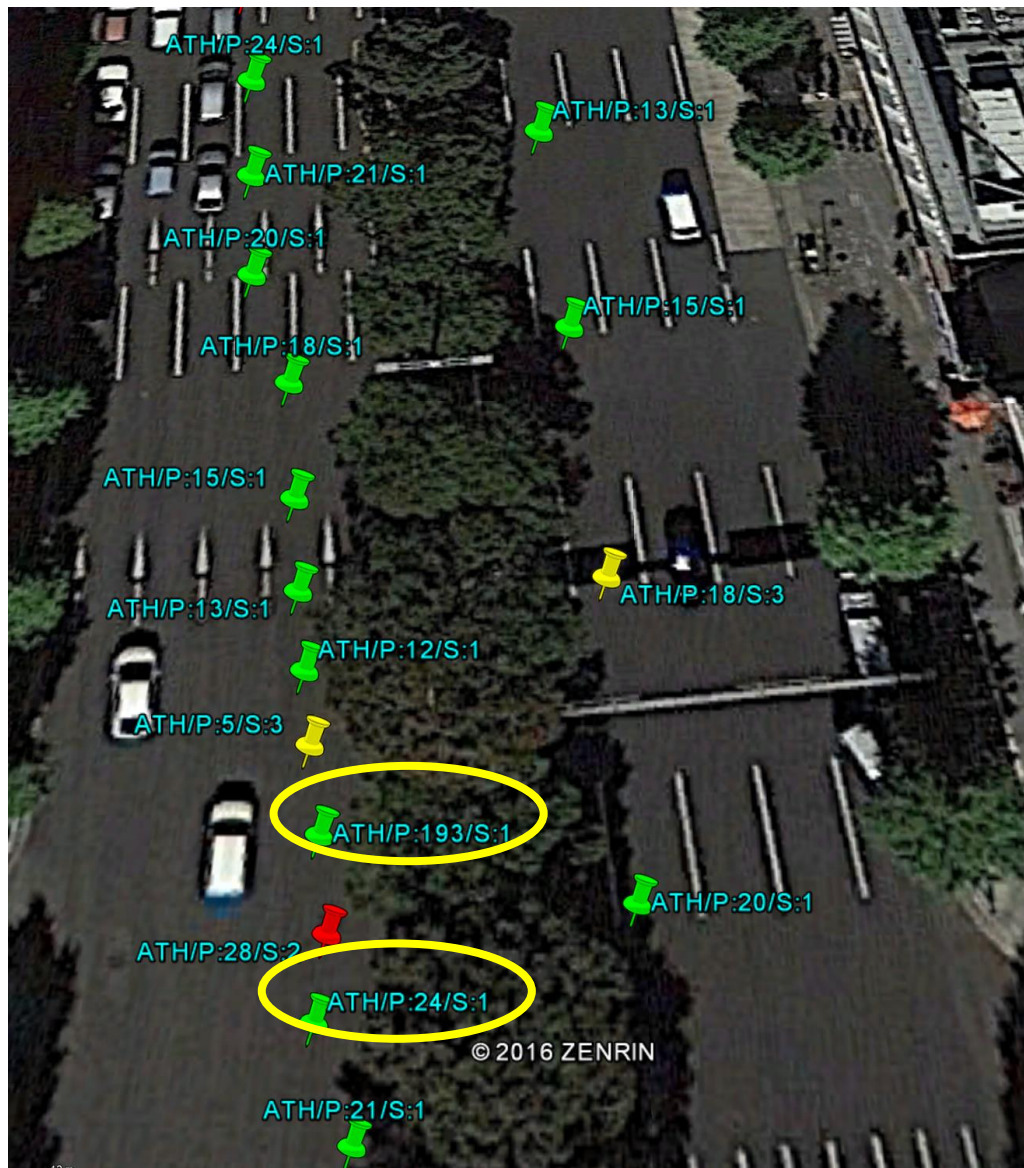
Proprietary NMEA Sentence for Authentication Status

\$TalkerID, GPSTIME, PRNID, TBD, AuthStatus, TBD, *CRC_Check
\$QZATH, 071557.40, 20, 31, ①, 3199.711, *FF



AuthStatus: 0, 1, 2, 3, 4

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 | |
| 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 | |
| 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 | |
| LATITUDE | |
| IODC | |
| 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 and QZSS Signals**
 - **Other GNSS signals also possible**
- **This method can be implemented without any impact on HW**
 - **Only Software/Firmware modification in the control and user system**

Recommendation & Request to ICG

- **Spooing, Anti-Spooing, Authentication issues shall be included in the agenda of IDM WG of ICG**
- **Navigation Data Bits shall be monitored in the IGMA observations**
 - **Observations focused on resiliency and quality of service**