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…

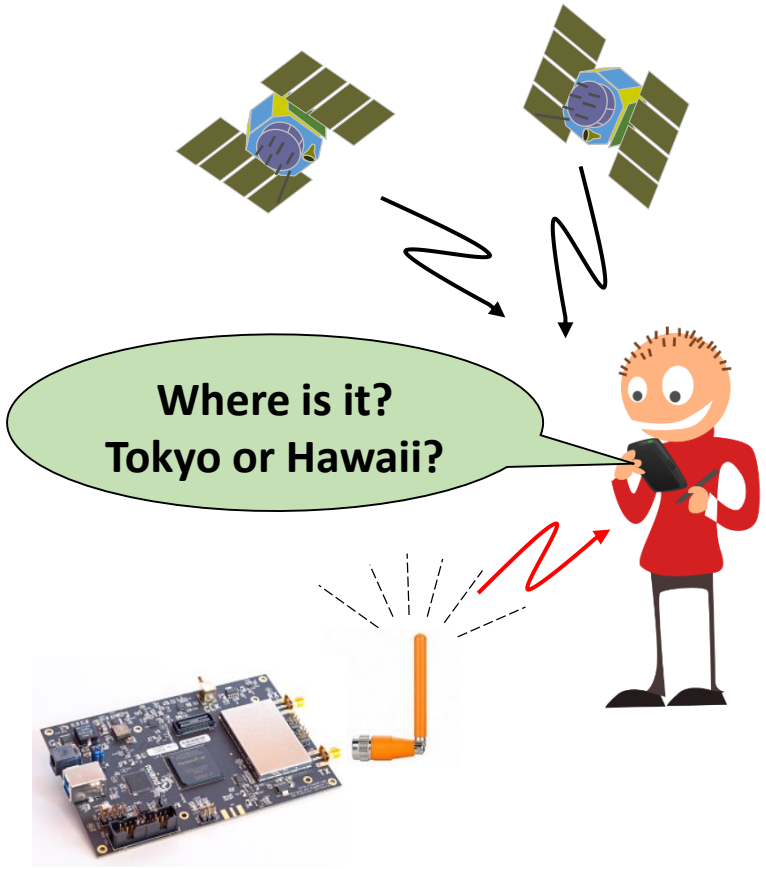
…But Need to Verify

Because of Spoofing Issues

Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

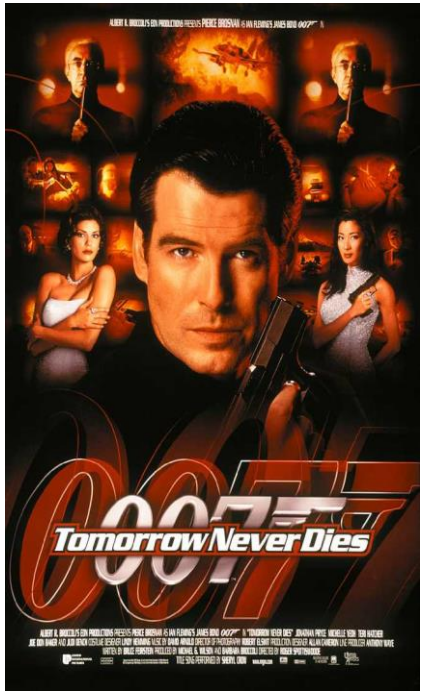
What is Location Spoofing?

- Falsify Location Data as If it were True Location



Spoofer

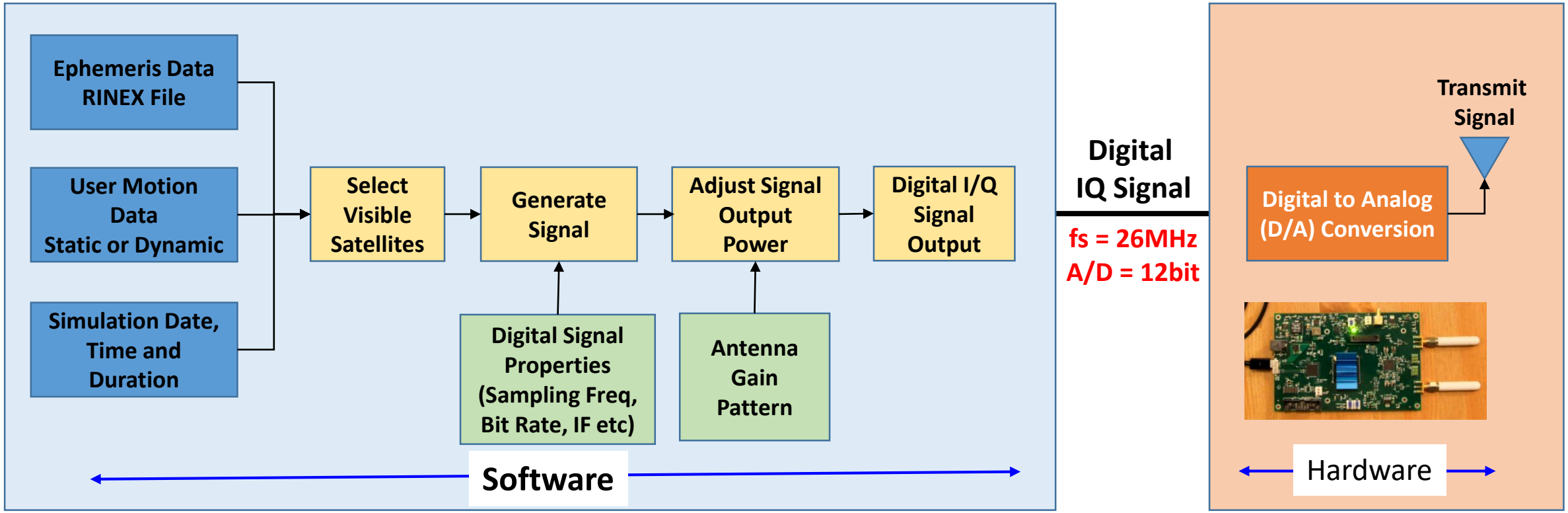
TOKYO
Or
Hawaii?



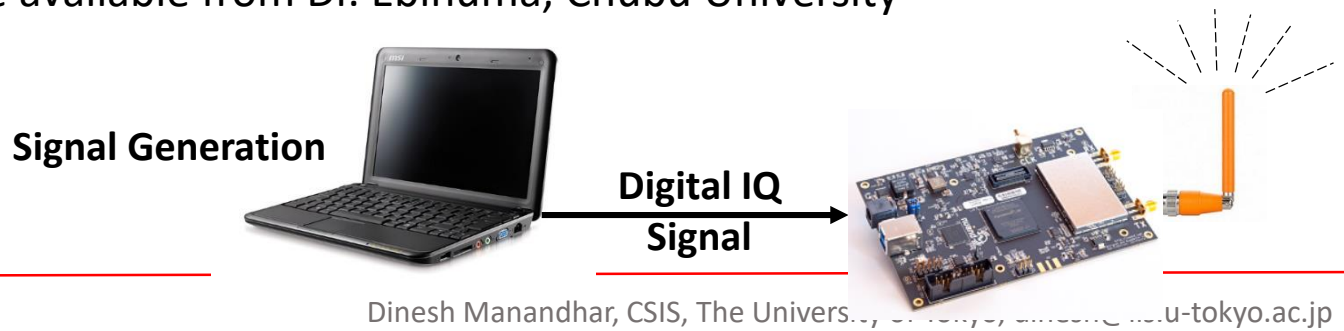
This movie is all about GPS Spoofing

Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

Software-Based GPS Signal Generator (Spoofer?)



Software Source available from Dr. Ebinuma, Chubu University

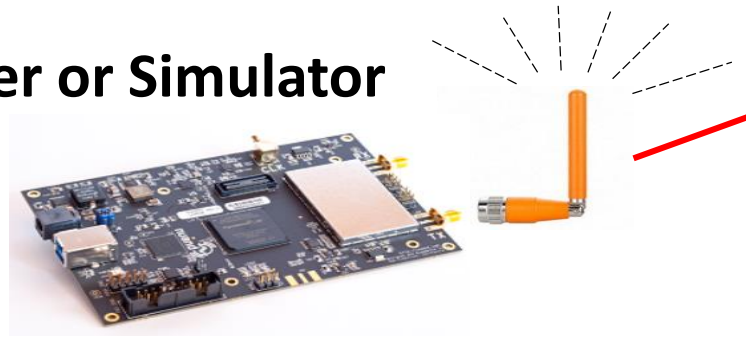


What is GPS Signal Authentication?

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

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

Spoofer or Simulator

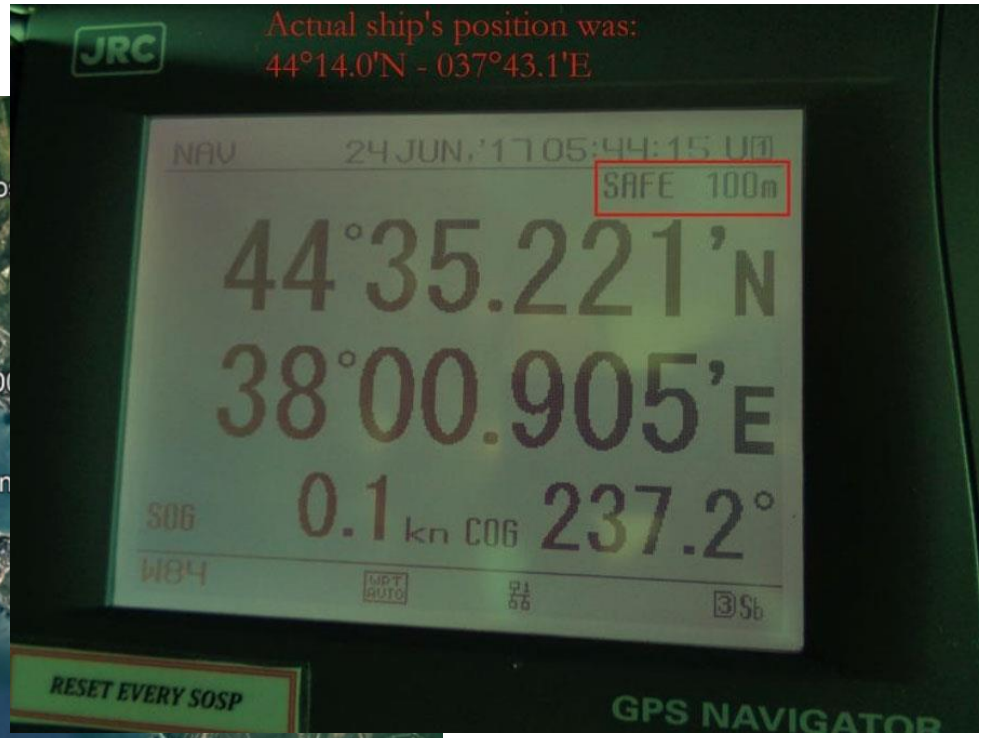


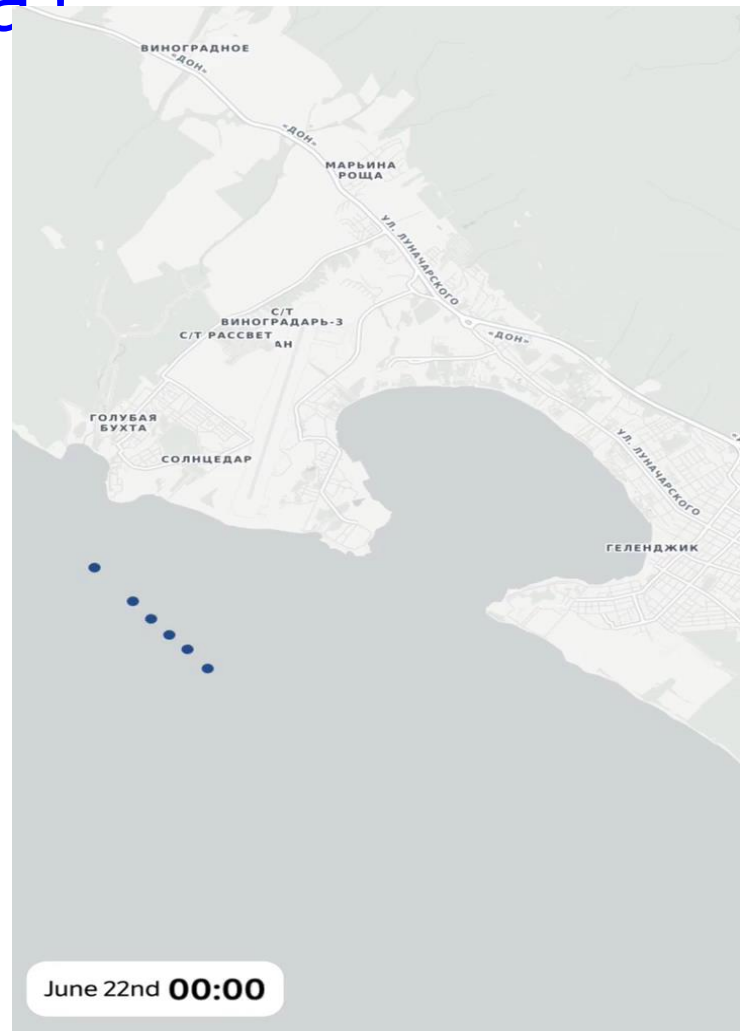
GPS Signal Authentication is necessary to detect SPOOF Signals

GPS Spoofing in Black Sea?

24th June 2017

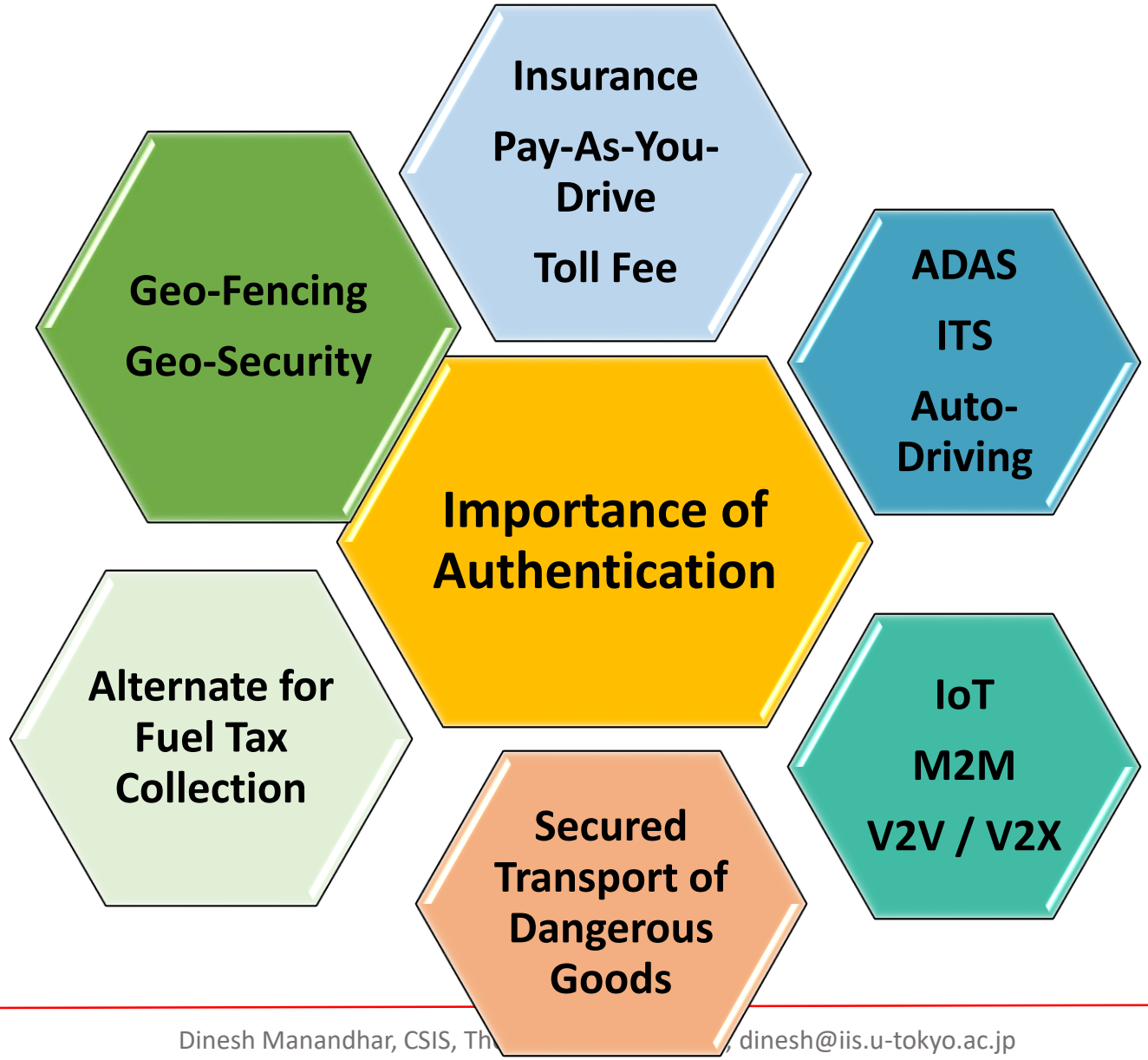
A GPS spoofing attack in June, involving over 20 vessels in the Black Sea, has been reported. *Probably the first official record of spoofing.* More…….





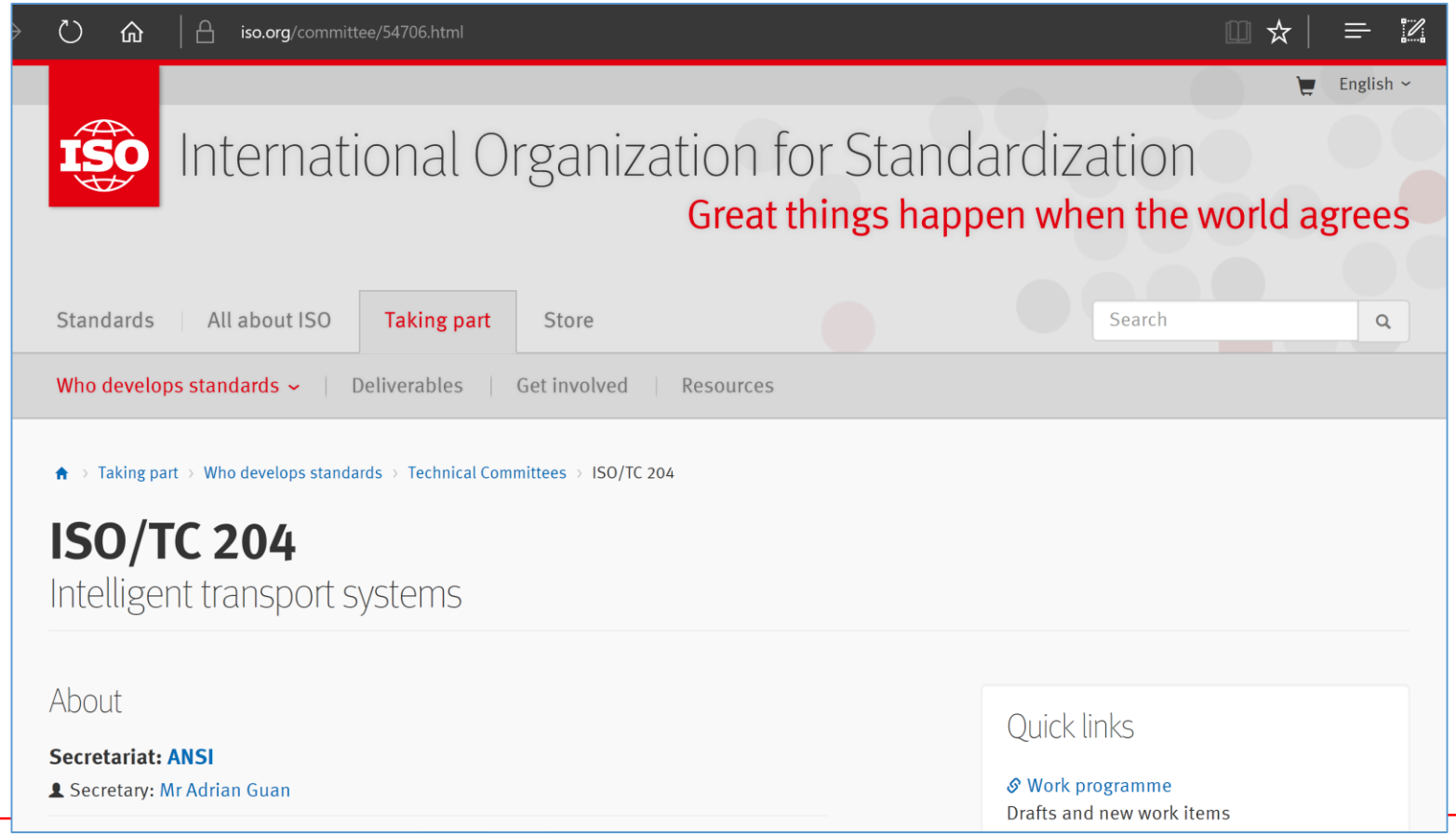
SPOOFing a Car: Is he driving the car?

Why Authentication or Anti-Spoofing is Necessary ?



ISO/TC204 WG-18

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



Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

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

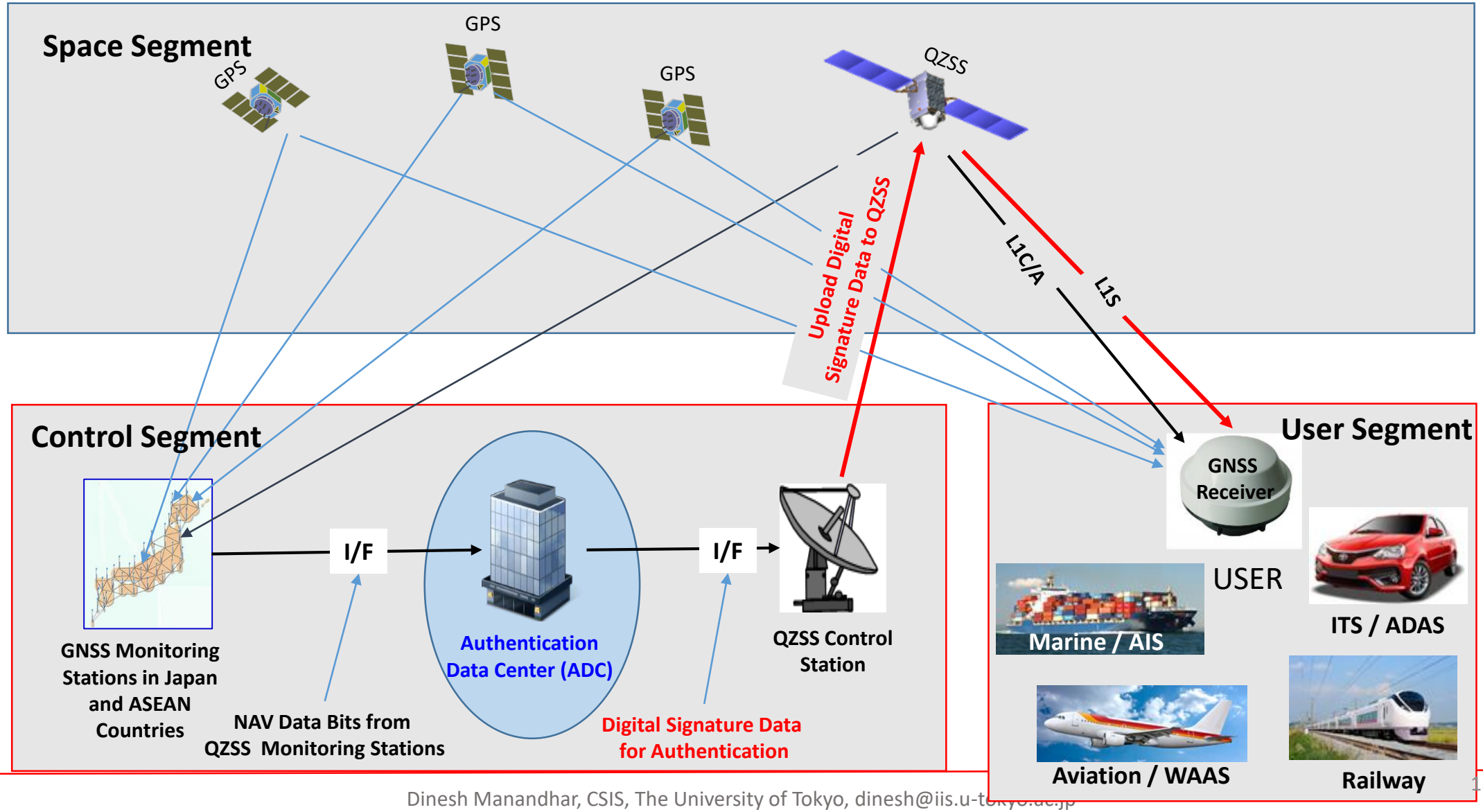
Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

Concept of Signal Authentication or Anti-Spoofing

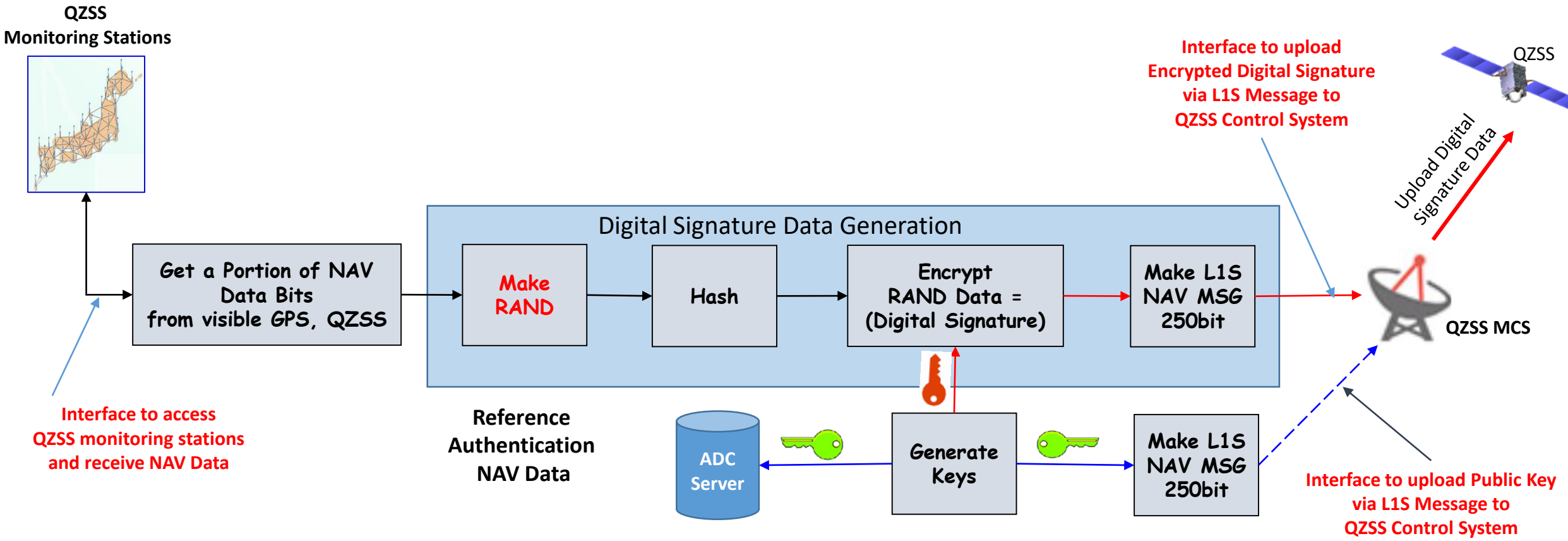
Simply, Broadcast a Digital Signature Data from QZSS Navigation Message

Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

Authentication System Architecture

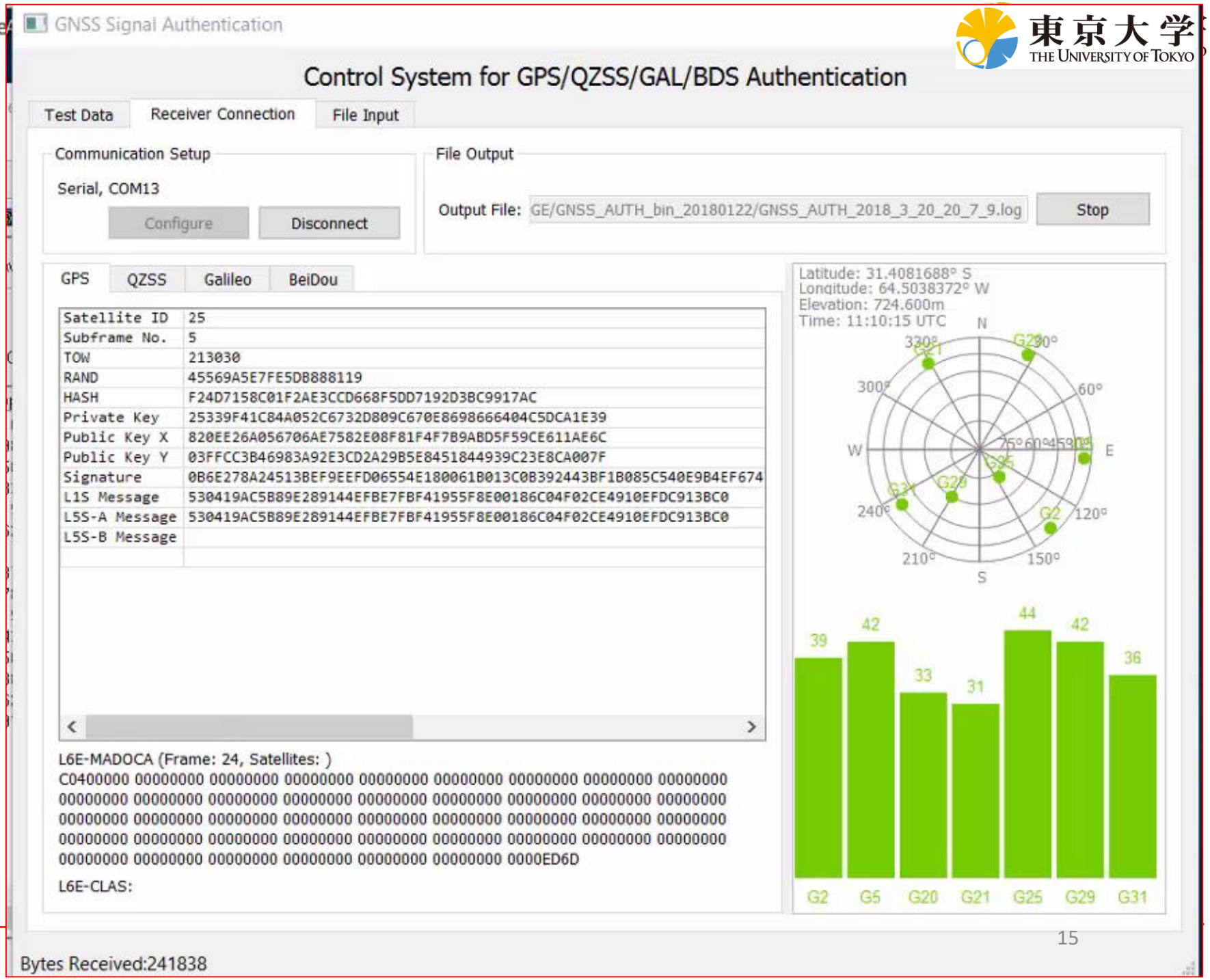


Authentication System: Control Segment Development

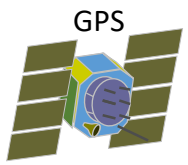


Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

Digital Signature Generation for Authentication



Authentication System: User Segment

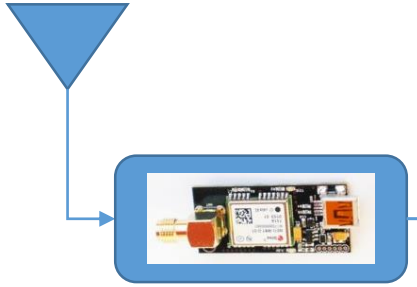


L1C/A

L1C/A

L1S

QZSS Signal with
Digital Signature
for Authentication



GNSS Receiver

Make RAND
From L1C/A
NAV MSG

Hash
MSG A

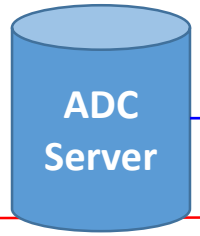
Check HASH
MSG A & B

Get Digital
Signature Data
from L1S NAV MSG

Decrypt

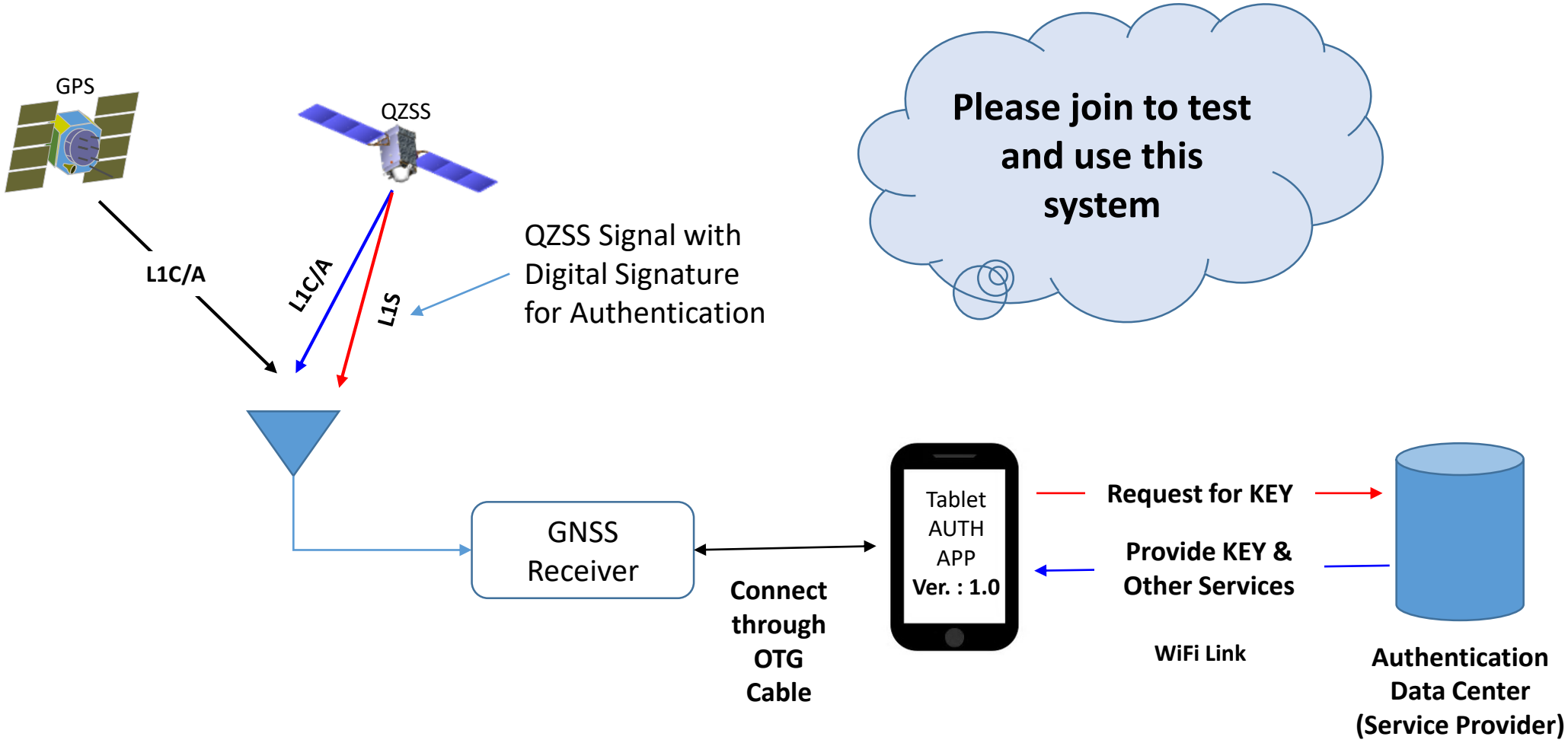
Hash
MSG B

If HASH MSG A =
HASH MSG B
Authentication OK
Else
Authentication Fails



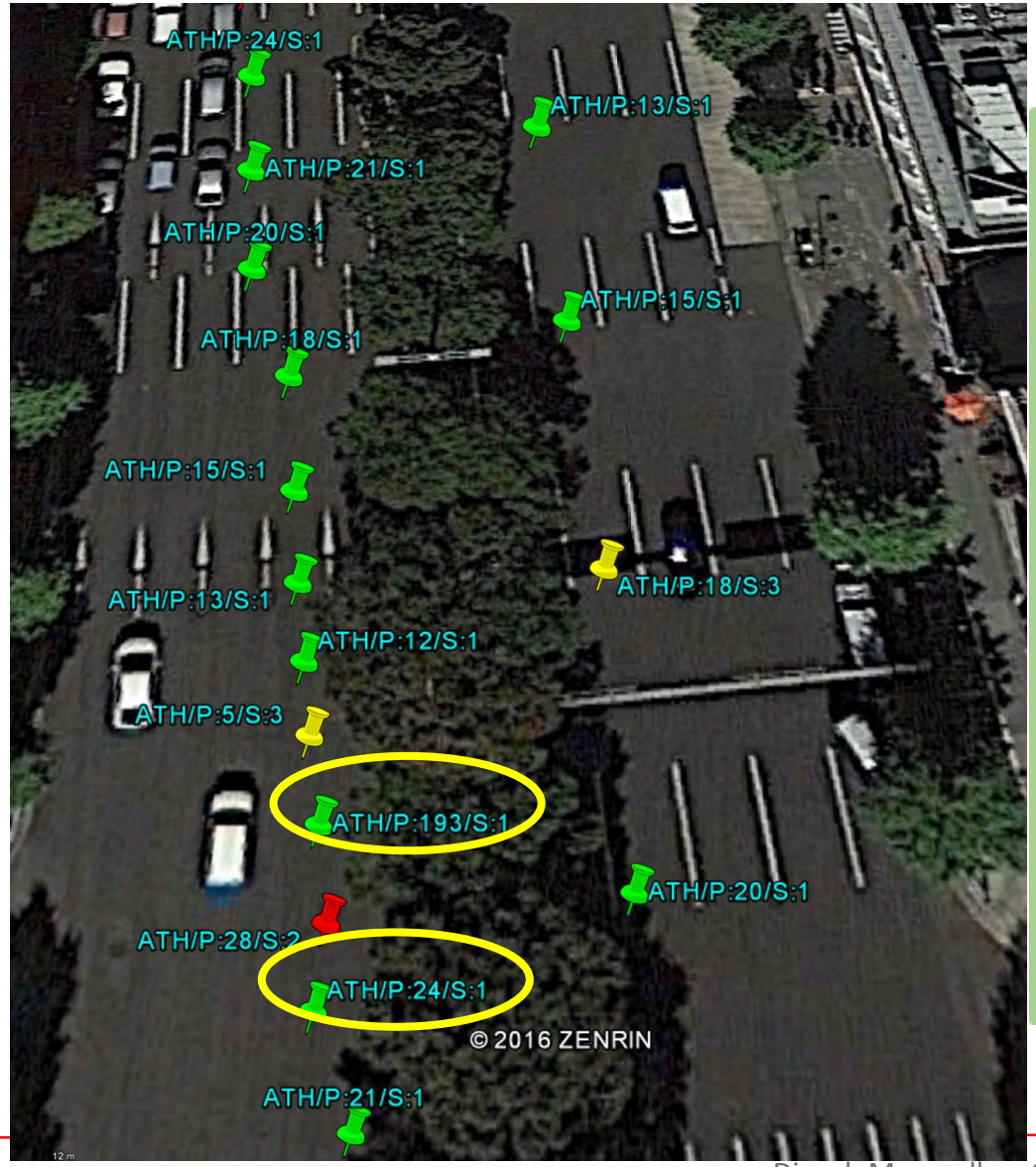
Get KEY
from ADC

Prototype Anti-Spoofing Receiver



Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

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	
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

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:

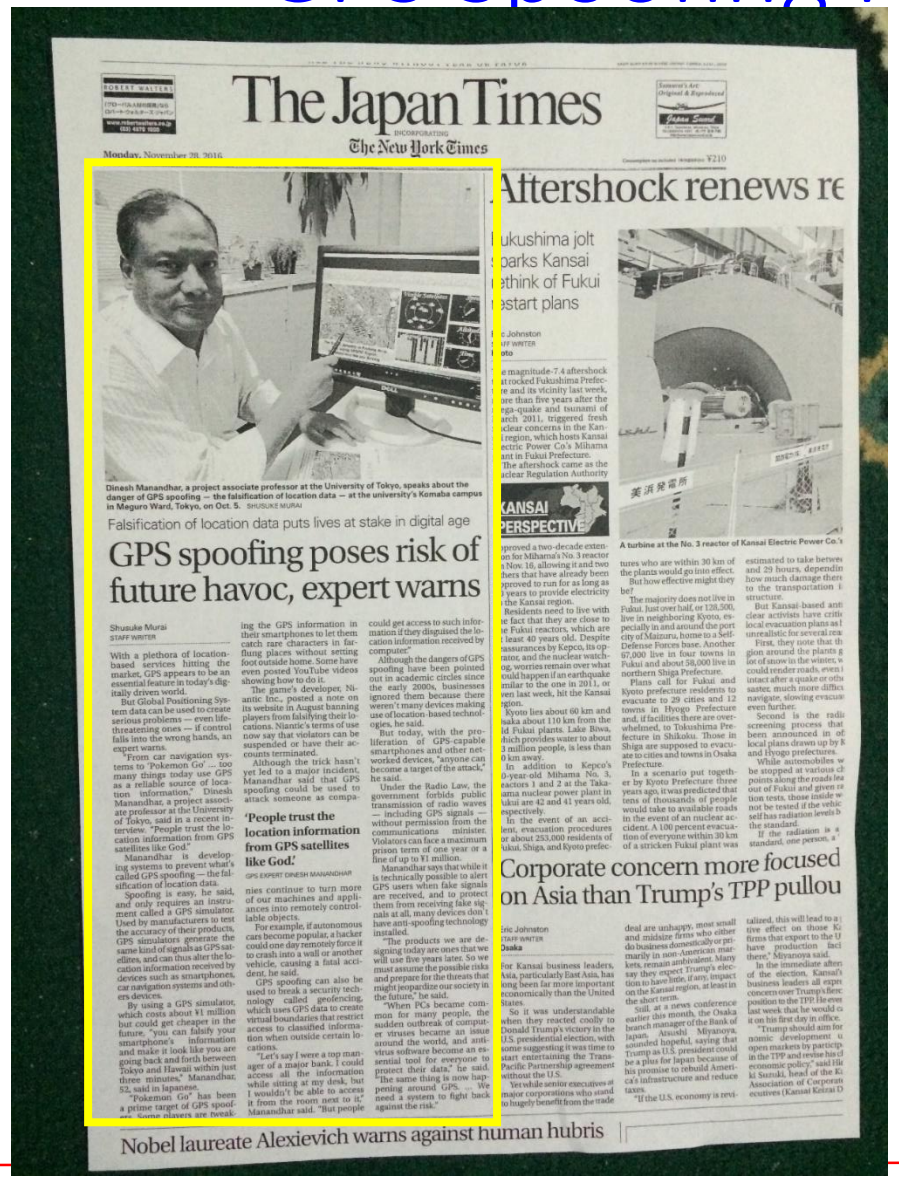
dinesh@csis.u-tokyo.ac.jp

Reference Slides

Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

GPS Spoofing Poses Risk of Future Havoc

NOV 28, 2016



The Japan Times
INCORPORATING 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 spoof- ... 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

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

KANSAI PERSPECTIVE

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

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.

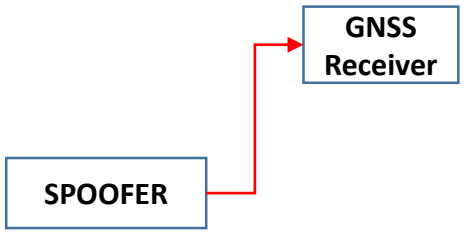
ＧＰＳ捜査訴訟の上告審判決が言い渡された最高裁大法廷。中央は、寺田逸郎裁判長＝15日午後、東京都千代田区（伴龍二撮影）24

Spoofing Methods

Spoofing Level 0
Self-Spoofing

Receiver and Spoofer directly connected by cable

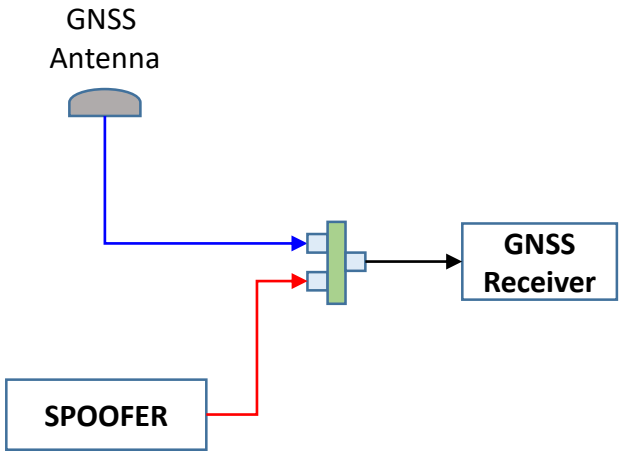
Real Signal not Present



Spoofing Level 1
Self-Spoofing

Receiver and Spoofer directly connected by cable

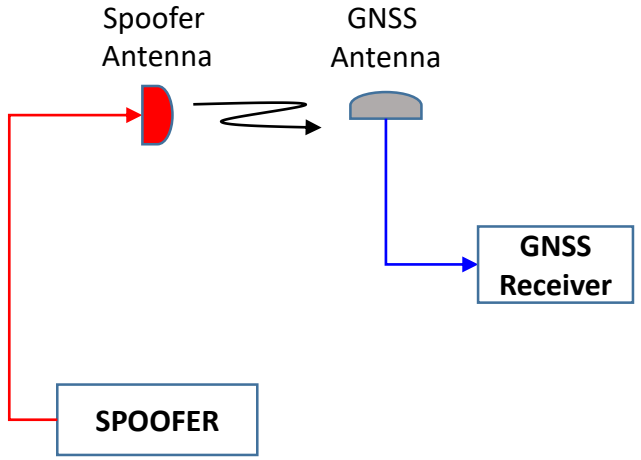
Real Signal Present



Spoofing Level 2
Self-Spoofing or 3rd Party Spoofing

Over-the-Air Spoof Signal Transmission

Real Signal Present



Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp

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