MGA Webinar Series : 5
Threats to GNSS : Can We Falsify GPS Data?

Dinesh Manandhar

Center for Spatial Information Science

The University of Tokyo

Contact Information: dinesh@iis.u-tokyo.ac.jp

22nd June 2018

Webinar Information

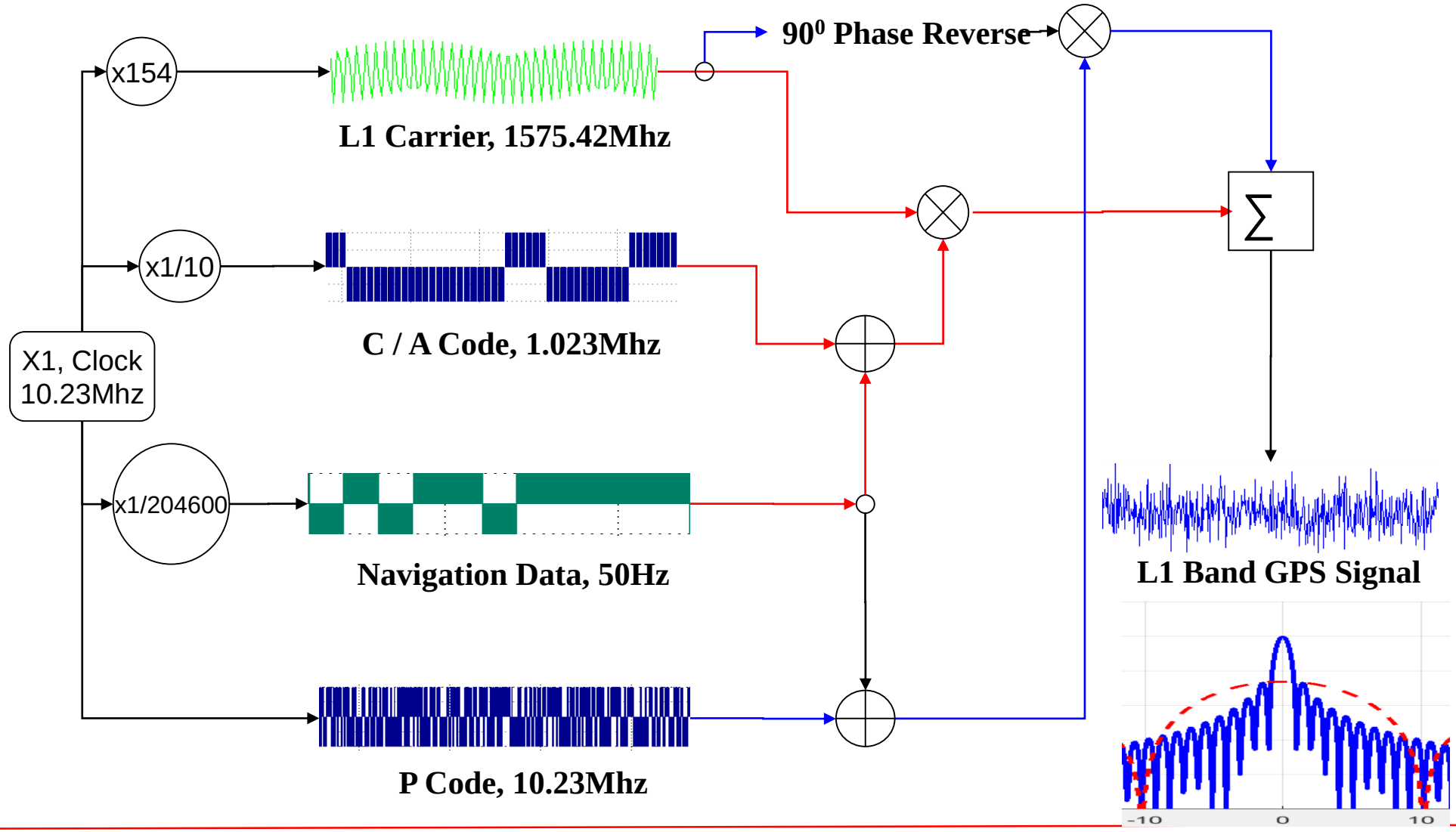
- Webinar ID : MGA Webinar # 5
- Webinar Topic :
  - Threats to GNSS : Can We Falsify GPS Data?
- Date :
  - 22nd June 2018 Friday, Time : 18:00 (JST) 09:00 (UTC)
- Duration : 45min + 15min (Q/A)
- Resource Person :
  - Dinesh Manandhar, Associate Professor, The University of Tokyo
- Registration : https://gnss.peatix.com
- Further Information:
  - http://www.csis.u-tokyo.ac.jp/~dinesh/WEBINAR.htm

Threat Types

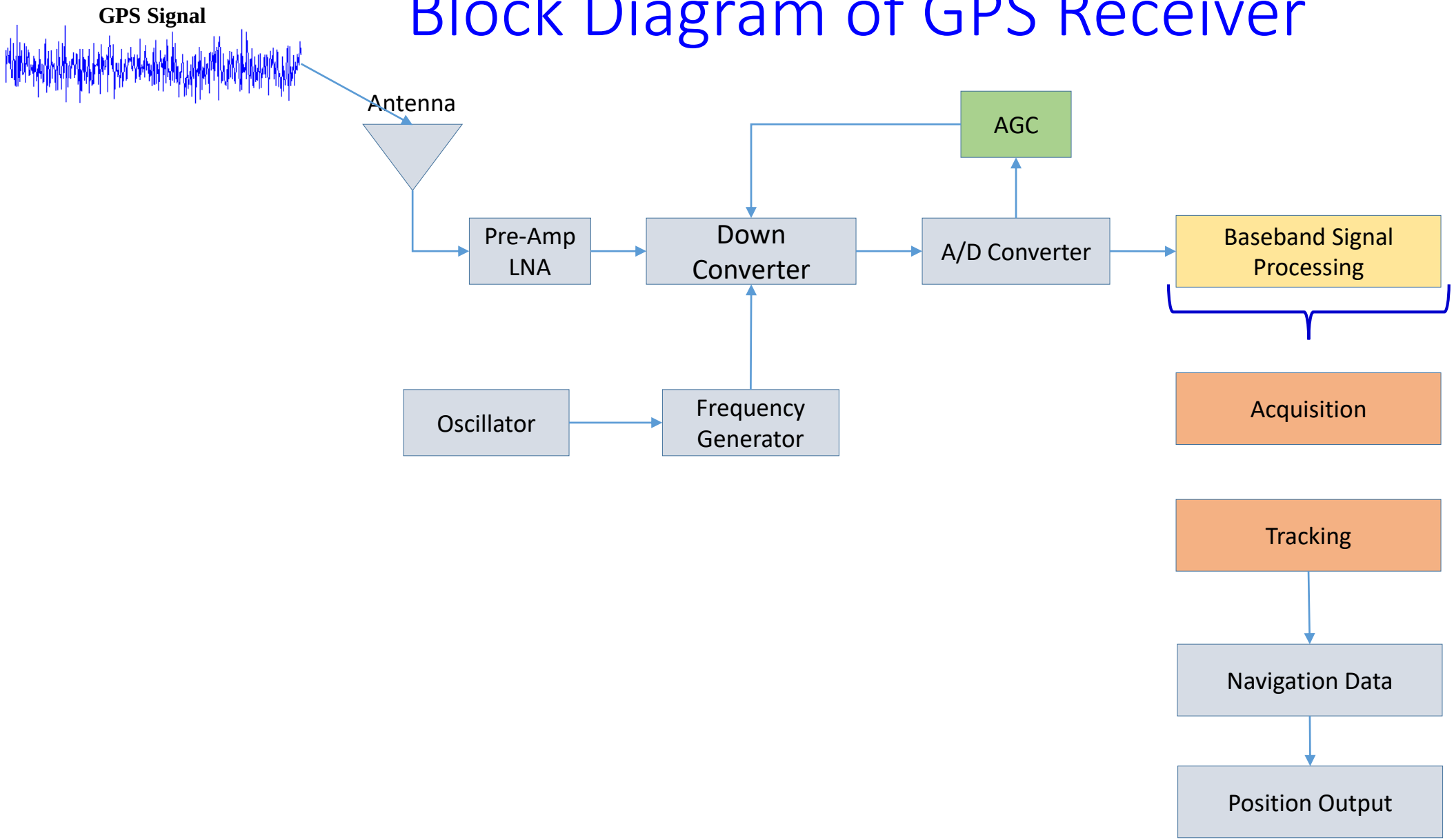
- Intentional Threats
  - Interference, Jamming, Spoofing and Meaconing
- Non-Intentional Threats
  - Interference, Jamming
    - Interference from Cell-towers
- Natural Threats
  - Solar Flares, Sun Spots (Space Weather)
  - Impact on Satellite Orbit

In this webinar, we discuss about SPOOFING Threats

Background Information : GPS Signal Structure

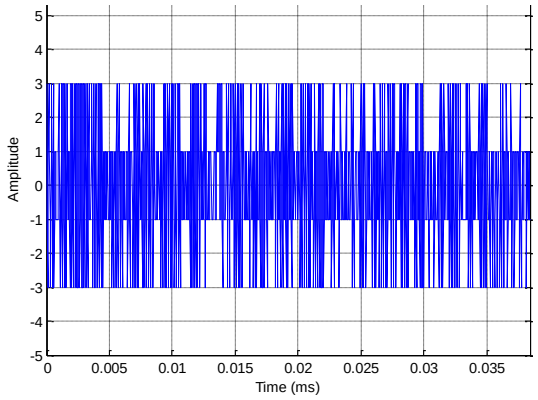


Block Diagram of GPS Receiver

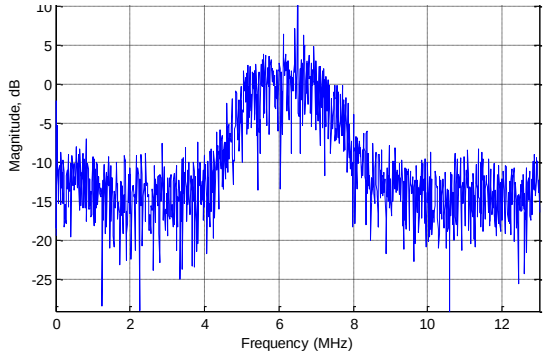


How does GPS Signal Look Like?

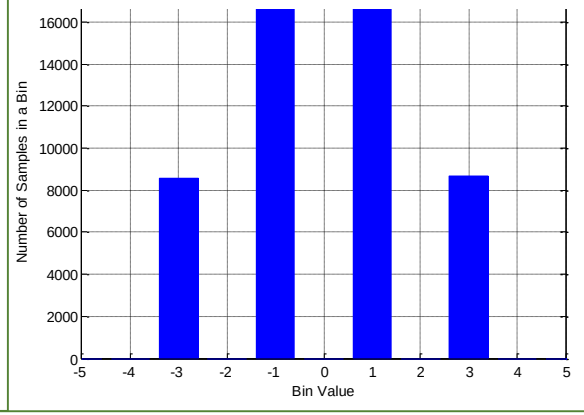
Time-domain Plot of GPS IF Signal

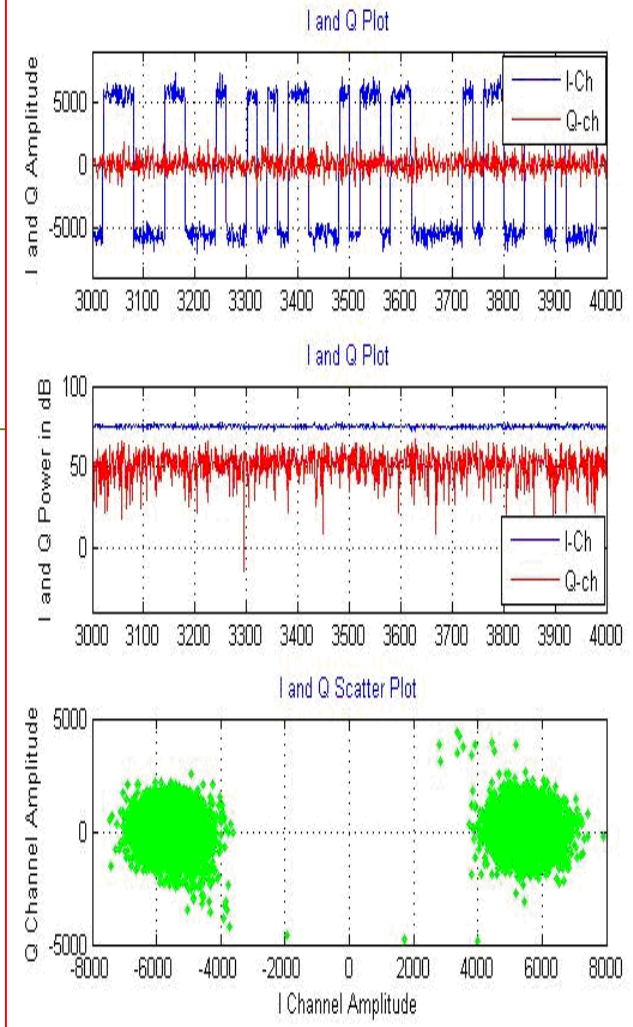


Frequency-domain Plot of GPS IF Signal (Fourier Transform)

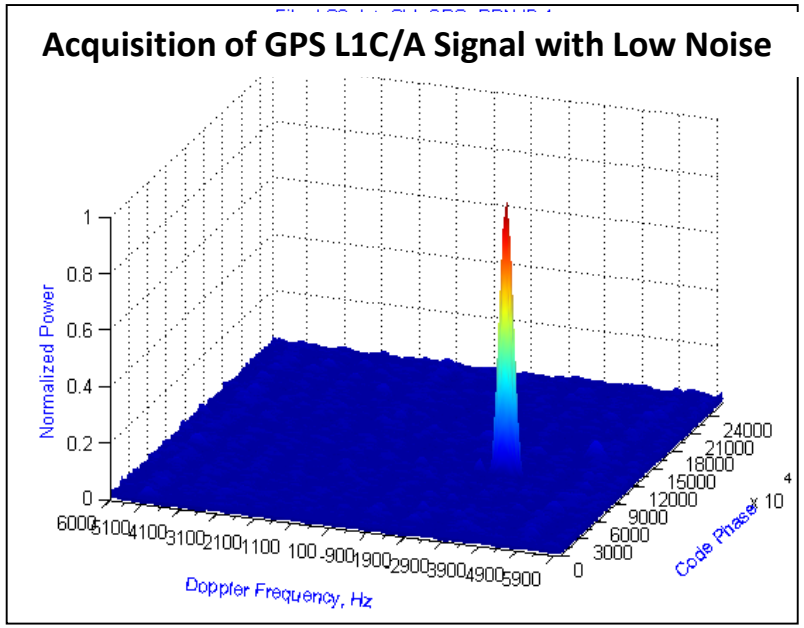


Histogram of GPS IF Signal

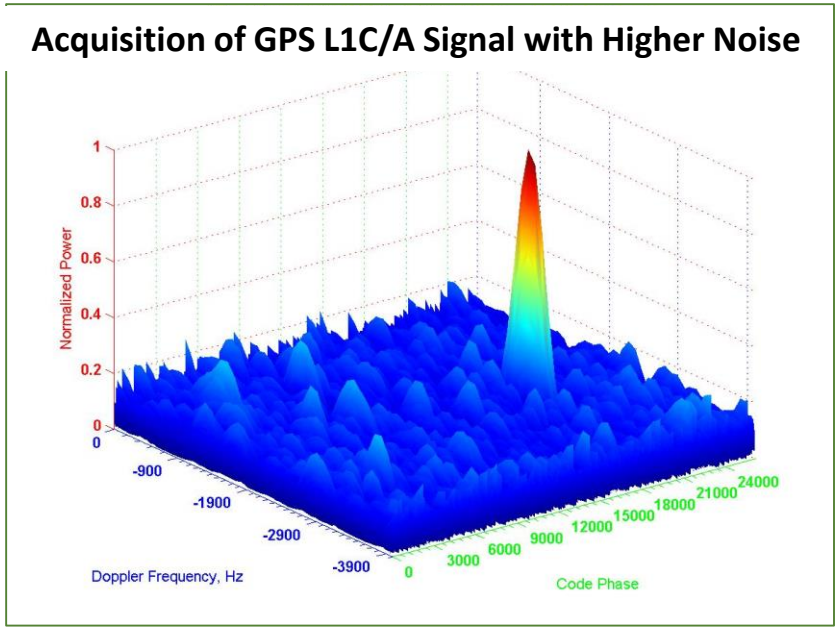




Acquisition of GPS L1C/A Signal with Low Noise



Acquisition of GPS L1C/A Signal with Higher Noise



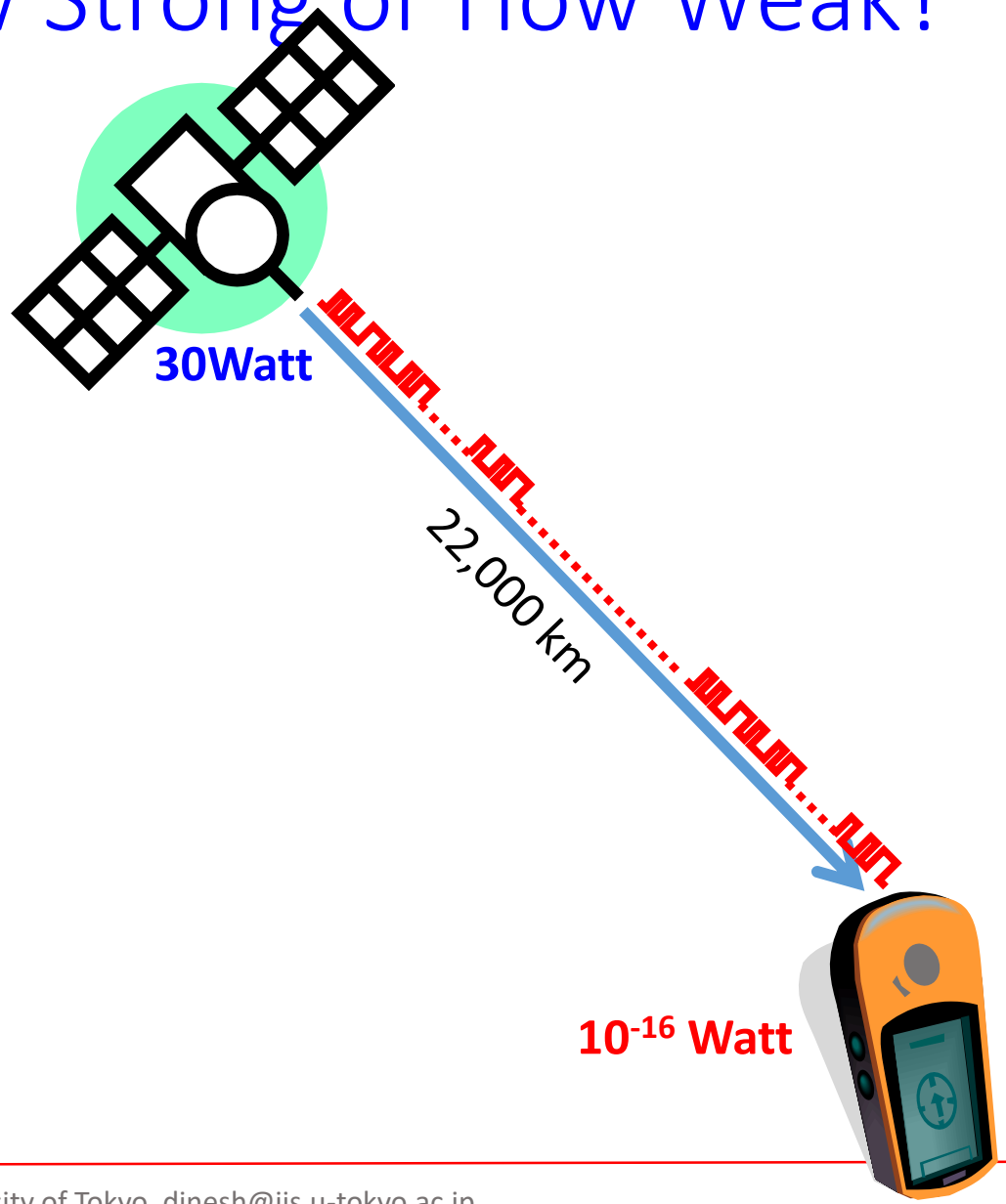
Why is GPS Signal So Vulnerable?

- The signal is extremely weak
  - It is below the thermal noise of the receiver,-111dBm
- No signal protection scheme is implemented
  - except P(Y) code, military use signal
- Signal specifications are open to everyone
- Even new signals do not have protection plans against spoofing
- QZSS Signal is also equally vulnerable as GPS signal
  - QZSS signals are almost the same as GPS signals
- JIS devices are commercially available off-the-shelf

JIS: Jamming, Interference & Spoofing

GPS Signal Power: How Strong or How Weak?

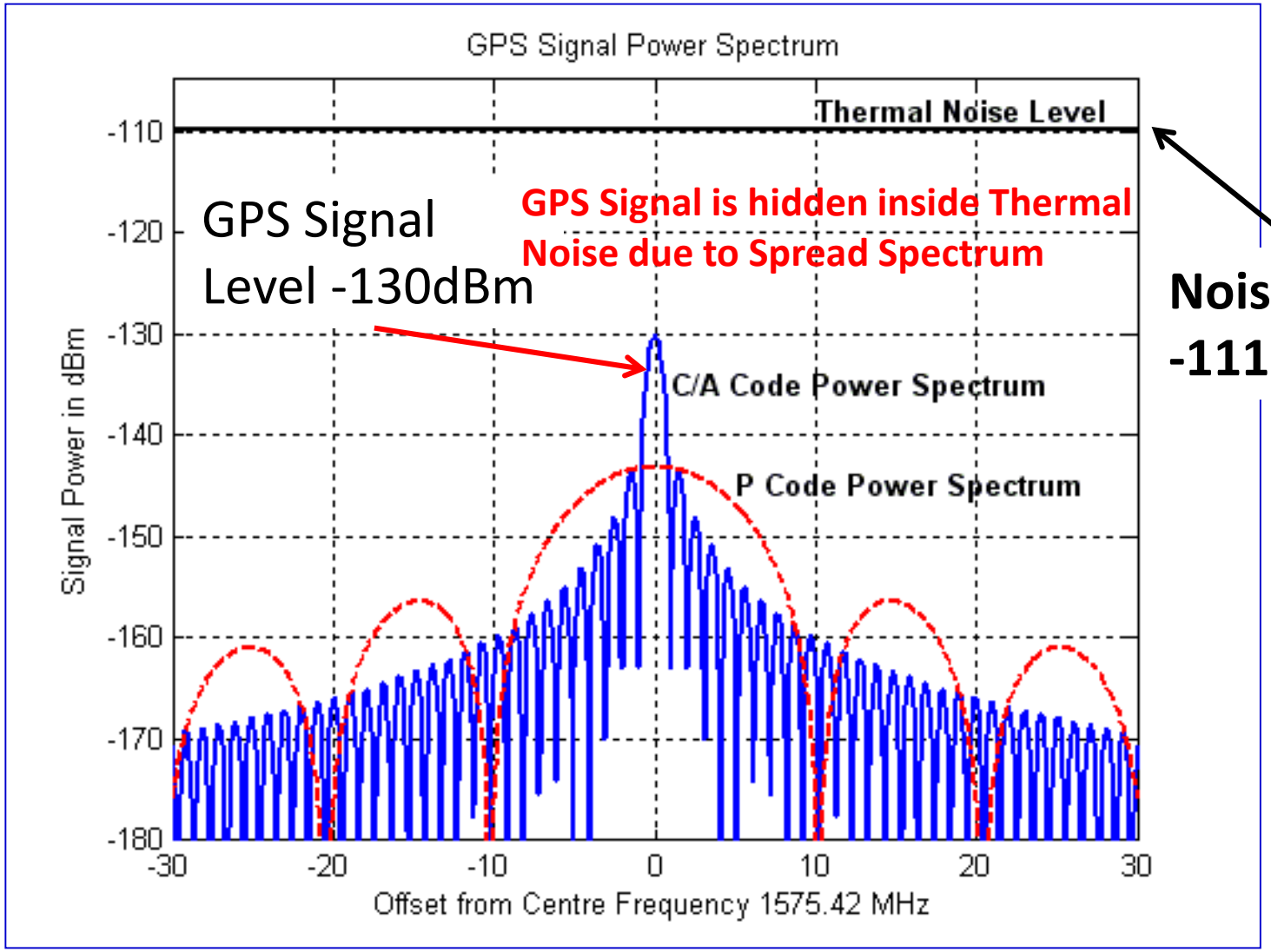
- GPS satellites are about 22,000km away
- Transmit power is about 30W
- This power when received at the receiver is reduced by 10^{16} times.
  - The power reduces by 1/distance^2
  - This is similar to seeing a 30W bulb 22,000Km far
- GPS signals in the receiver is about 10^{-16} Watt, which is below the thermal noise



GPS Signal Power: How Strong or How Weak?

- GPS Signal Power at Receiver
  - -130dBm or -160dBW
- Thermal Noise Power
  - Defined by $kT_{eff}B$, where
    - $K = 1.380658e\text{-}23JK^{-1}$, Boltzman Constant
    - $T_{eff} = 362.95$, for Room temperature in Kelvin at 290
      - Teff is effective Temperature based on Frii's formula
    - $B = 2.046MHz$, Signal bandwidth
  - Thermal Noise Power = -110dBm for 2MHz bandwidth
  - If Bandwidth is narrow, 50Hz
    - Noise Power = -156dBm

GPS Signal Power



GPS Signal power level is below the thermal noise level of the system. Hence, it is not possible to measure GPS signal level without demodulation (de-spreading).

Power of GPS Signal vs. Other Signals

	Signal Type	Power (based on calculations, not measured)		
		Watt	dBW	dBm
Above Noise	Mobile Phone Handset TX Power *	1W	0dBW	30dBm
	RX Power at Mobile Phone Handset*	100e-6W	-40dBW	-70dBm
	ZigBee	316e-16W	-115dBW	-85dBm
	VHF	200e-16W	-137dBW	-107dBm
	Thermal Noise	**79e-16W**	**-141dBW**	**-111dBm**
Below Noise	**GPS****	**1e-16W**	**-160dBW**	**-130dBm**

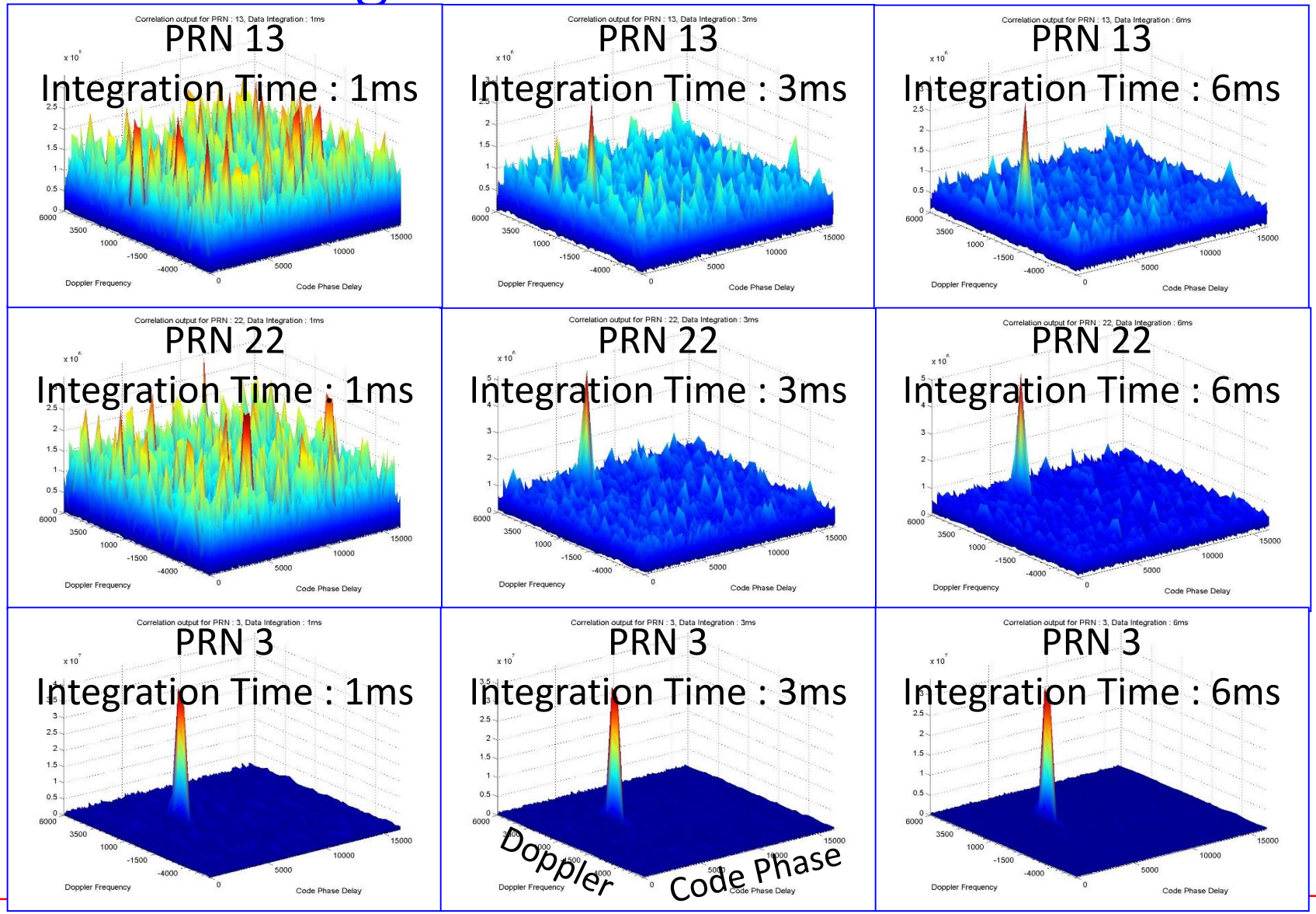
- * Actual power values will differ. These are just for comparison purpose
- ** GPS Signals are hidden under the noise. Thus, it can't be measured directly e.g. using a Spectrum Analyzer

Impact on Signal Processing due to Noise or Interference Signal

Presence of high level noise
This requires longer integration of data
More processing power

Presence of noise

Very small noise



GPS Spoofing

Quiz : Can You Trust GPS Position & Time Data?

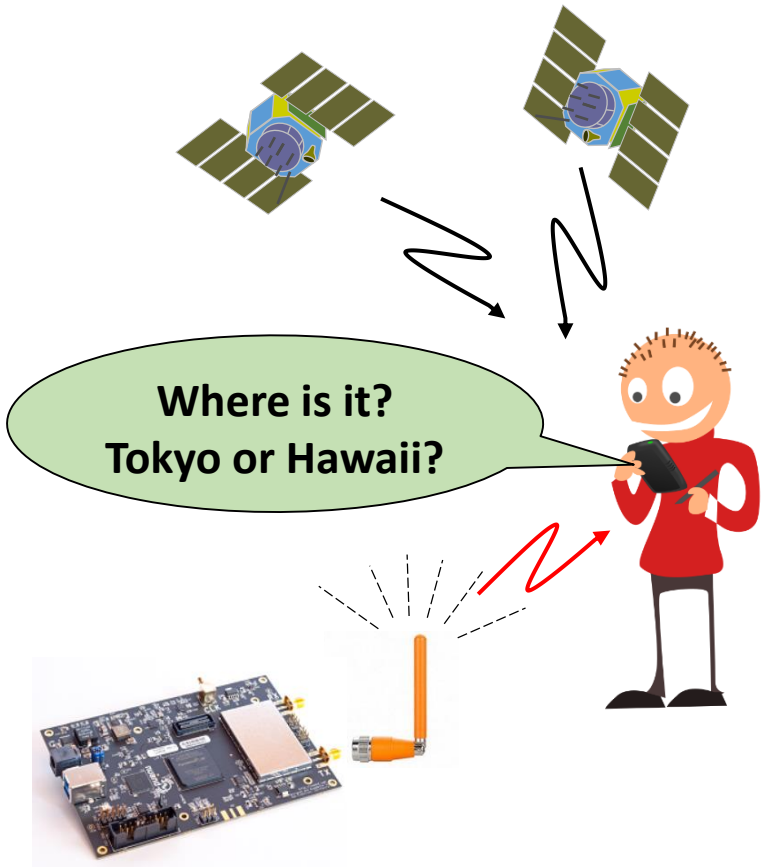
Yes, You can…

…But Need to Verify

Because of Spoofing Issues

What is Location Spoofing?

- Falsify Location Data as If it were True Location



Spoofer

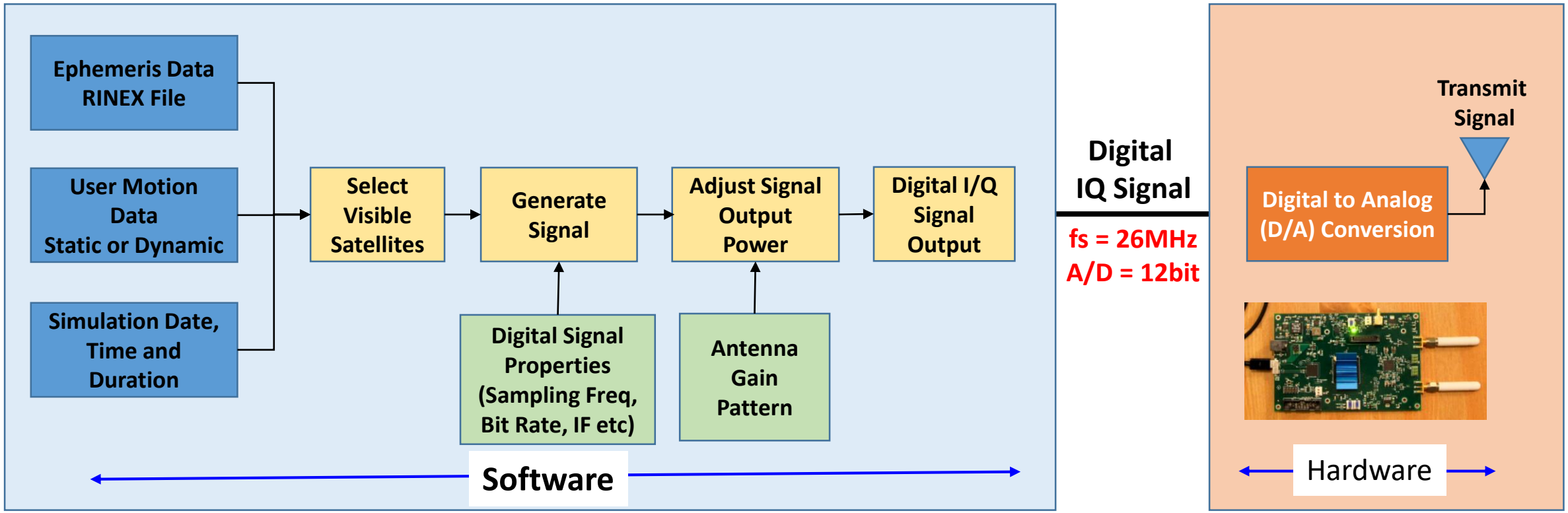
TOKYO Or Hawaii?

James Bond's **Tomorrow Never Dies** movie is all about GPS Spoofing by using a Spy Satellite to broadcast GPS like spoof signal.

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

Software-Based GPS Signal Generator (Spoofer?)

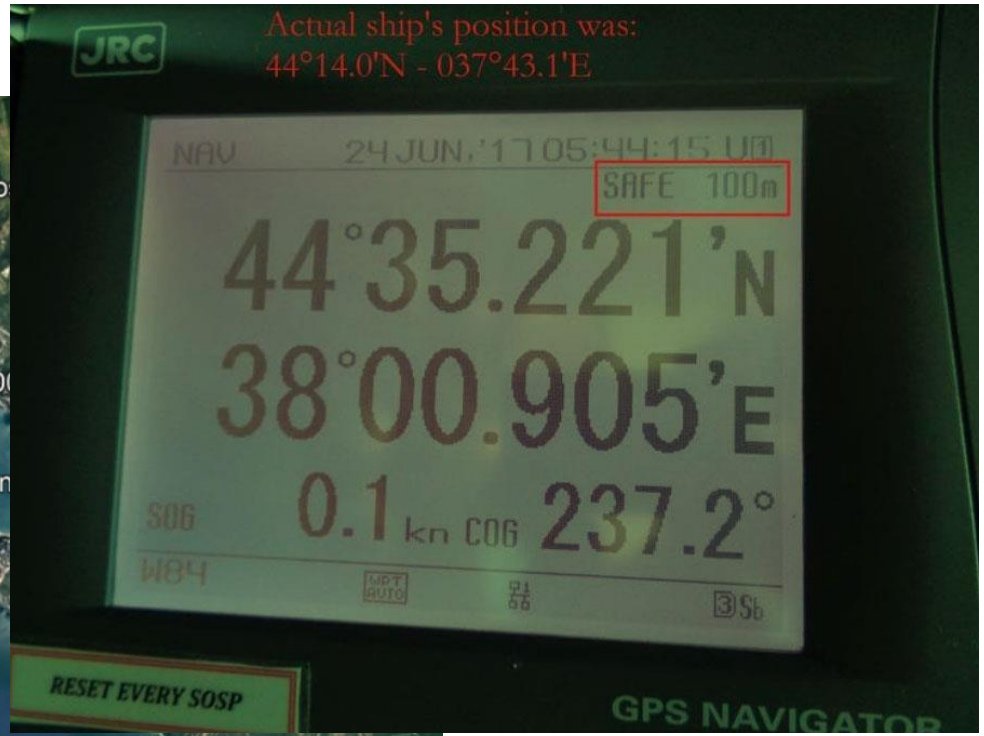


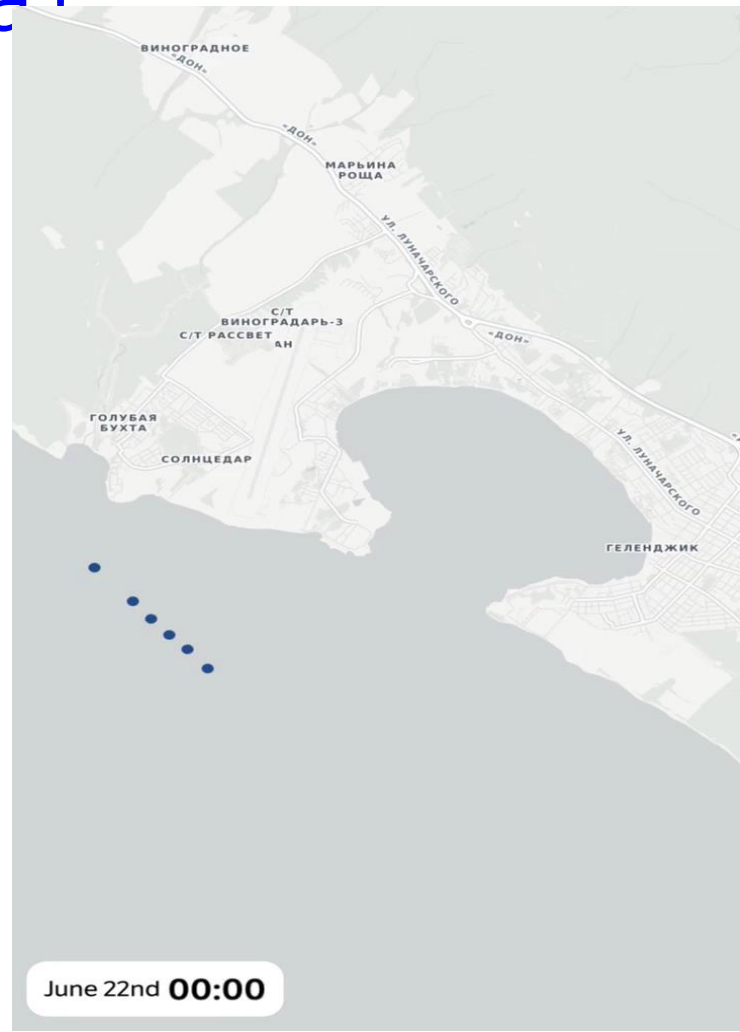
SPOOFing a Car: Is he driving the car?

GPS Spoofing in Black Sea?

24th June 2017

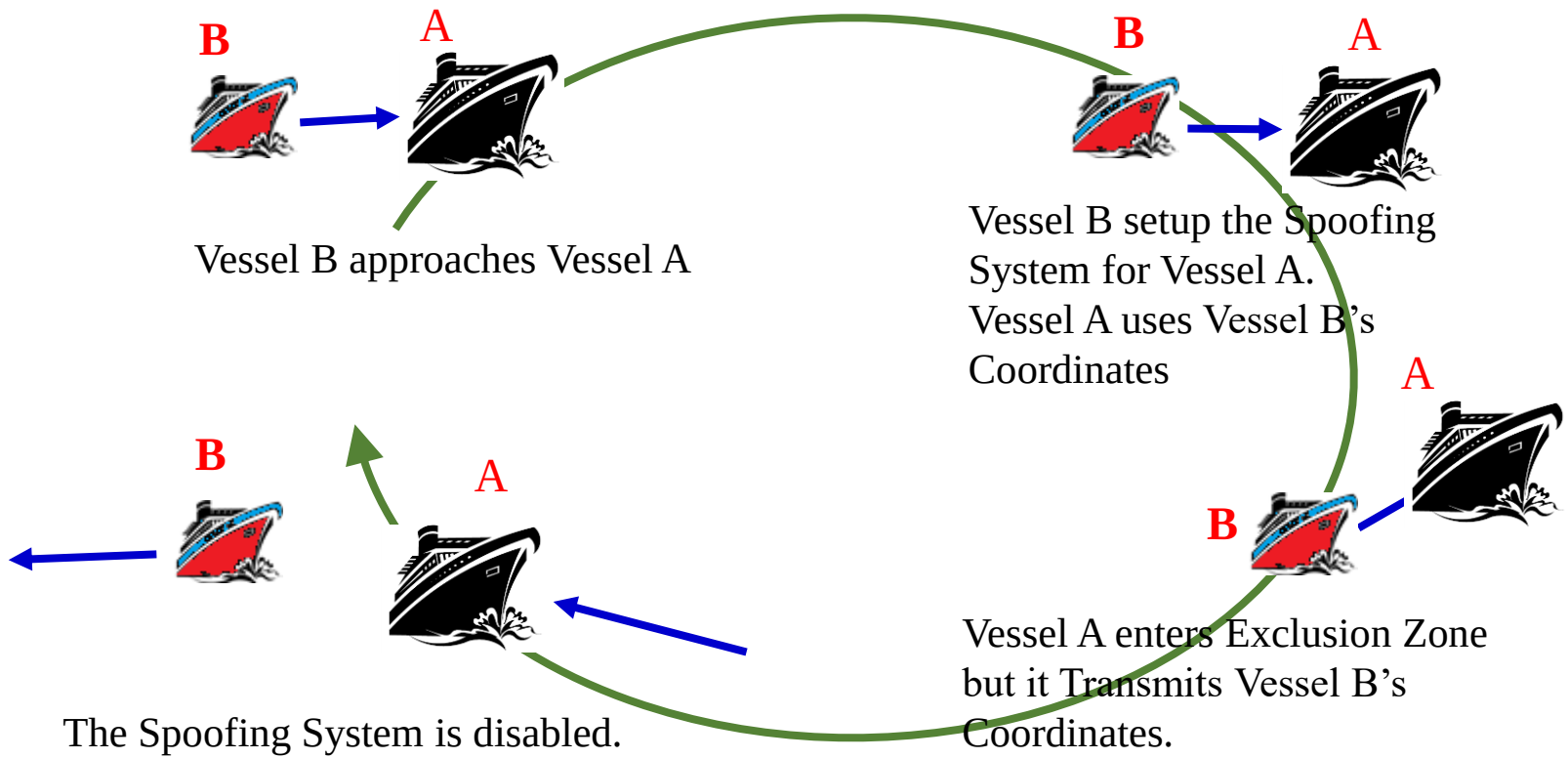
A GPS spoofing attack in June, involving over 20 vessels in the Black Sea, has been reported. *Probably the first official record of spoofing.* More…….





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

Fishing Vessels might be Spoofed !



Based on JRC Technical notes: Report on Authentication in Fisheries Monitoring

Drug Traffickers Are Spoofing Border Drones: DHS, USA

DHS: Department of Homelands Security, USA

http://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/

Published on 10th NOV 2017

US Defense Bill 2018:

Use GPS with Galileo and QZSS to Improve Accuracy and Resiliency

The House and Senate agreed Wednesday on the final National Defense Authorization Act (NDAA) for 2018. It included at least two provisions of interest to our readers:

SEC. 1606. DEMONSTRATION OF BACKUP AND COMPLEMENTARY POSITIONING, NAVIGATION, AND TIMING CAPABILITIES OF GLOBAL POSITIONING SYSTEM - Requires the Departments of Defense, Transportation and Homeland Security to conduct a $10M technology demonstration/ proof of concept for a GPS backup system. This demonstration is to be based upon information gathered from a requirements and alternatives analysis study mandated by last year's NDAA.

SEC. 1607. ENHANCEMENT OF POSITIONING, NAVIGATION, AND TIMING CAPACITY - Requires the Secretary of Defense to ensure DoD receivers incorporate Europe's Galileo and Japan's QZSS satellite signals along side GPS in order to improve accuracy and resiliency. It also directs the secretary to assess use of non-allied satellite navigation in DoD receivers.

Architect of the Capital Photo

Defense Bill 2018: GPS Backup Demo, Use Other GNSS

US President Signs Law Requiring GPS Backup Demo

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

H. R. 2810

One Hundred Fifteenth Congress
of the
United States of America

AT THE FIRST SESSION

Begun and held at the City of Washington on Tuesday, the third day of January, two thousand and seventeen

An Act

To authorize appropriations for fiscal year 2018 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Defense Authorization Act for Fiscal Year 2018".

SEC. 2. ORGANIZATION OF ACT INTO DIVISIONS; TABLE OF CONTENTS.

(a) DIVISIONS.—This Act is organized into four divisions as follows:

(1) Division A—Department of Defense Authorizations.
(2) Division B—Military Construction Authorizations.
(3) Division C—Department of Energy National Security Authorizations and Other Authorizations.
(4) Division D—Funding Tables.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 1606. DEMONSTRATION OF BACKUP AND COMPLEMENTARY POSITIONING, NAVIGATION, AND TIMING CAPABILITIES OF GLOBAL POSITIONING SYSTEM.

(a) PLAN.—During fiscal year 2018, the Secretary of Defense, the Secretary of Transportation, and the Secretary of Homeland Security (referred to in this section as the "Secretaries") shall jointly develop a plan for carrying out a backup GPS capability demonstration. The plan shall—

(1) be based on the results of the study conducted under section 1618 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 130 Stat. 2595); and

(2) include the activities that the Secretaries determine necessary to carry out such demonstration.

(b) BRIEFING.—Not later than 120 days after the date of the enactment of this Act, the Secretaries shall provide to the appropriate congressional committees a briefing on the plan developed under subsection (a). The briefing shall include—

(1) identification of the sectors that would be expected to participate in the backup GPS capability demonstration described in the plan;

(2) an estimate of the costs of implementing the demonstration in each sector identified in paragraph (1); and

(3) an explanation of the extent to which the demonstration may be carried out with the funds appropriated for such purposes.

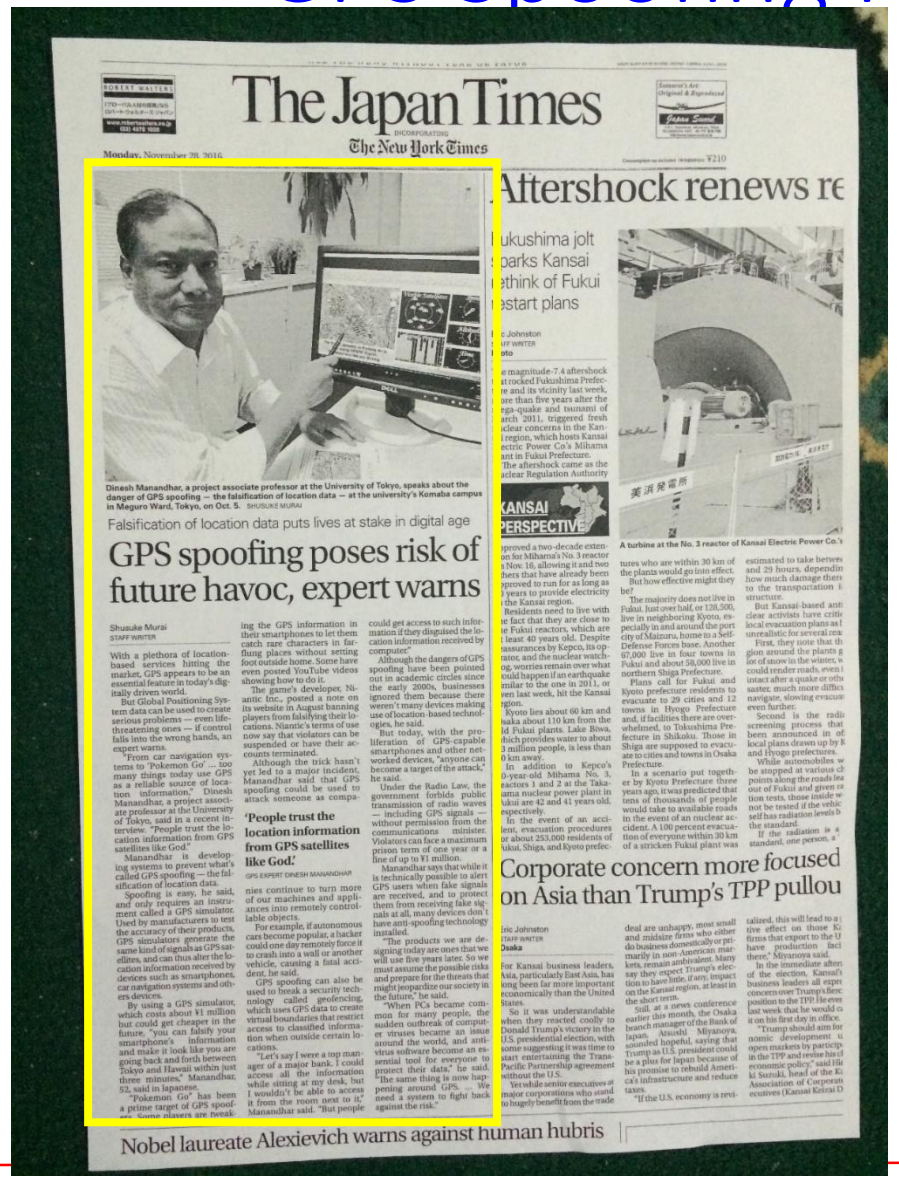
(c) IMPLEMENTATION.—

(1) IN GENERAL.—Subject to the availability of appropriations and beginning not earlier than the day after the date on which the briefing is provided under subsection (b), the Secretaries shall jointly initiate the backup GPS capability demonstration to the extent described under subsection (b)(3).

QZSS could be a part of GPS back-up system for Resiliency

Source: https://www.congress.gov/bill/115th-congress/house-bill/2810/text

GPS Spoofing Poses Risk of Future Havoc



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

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 spoofing. 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 cop 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
start plans

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

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

GPS Tracking is Illegal without Warrant: Japan Supreme Court Ruling

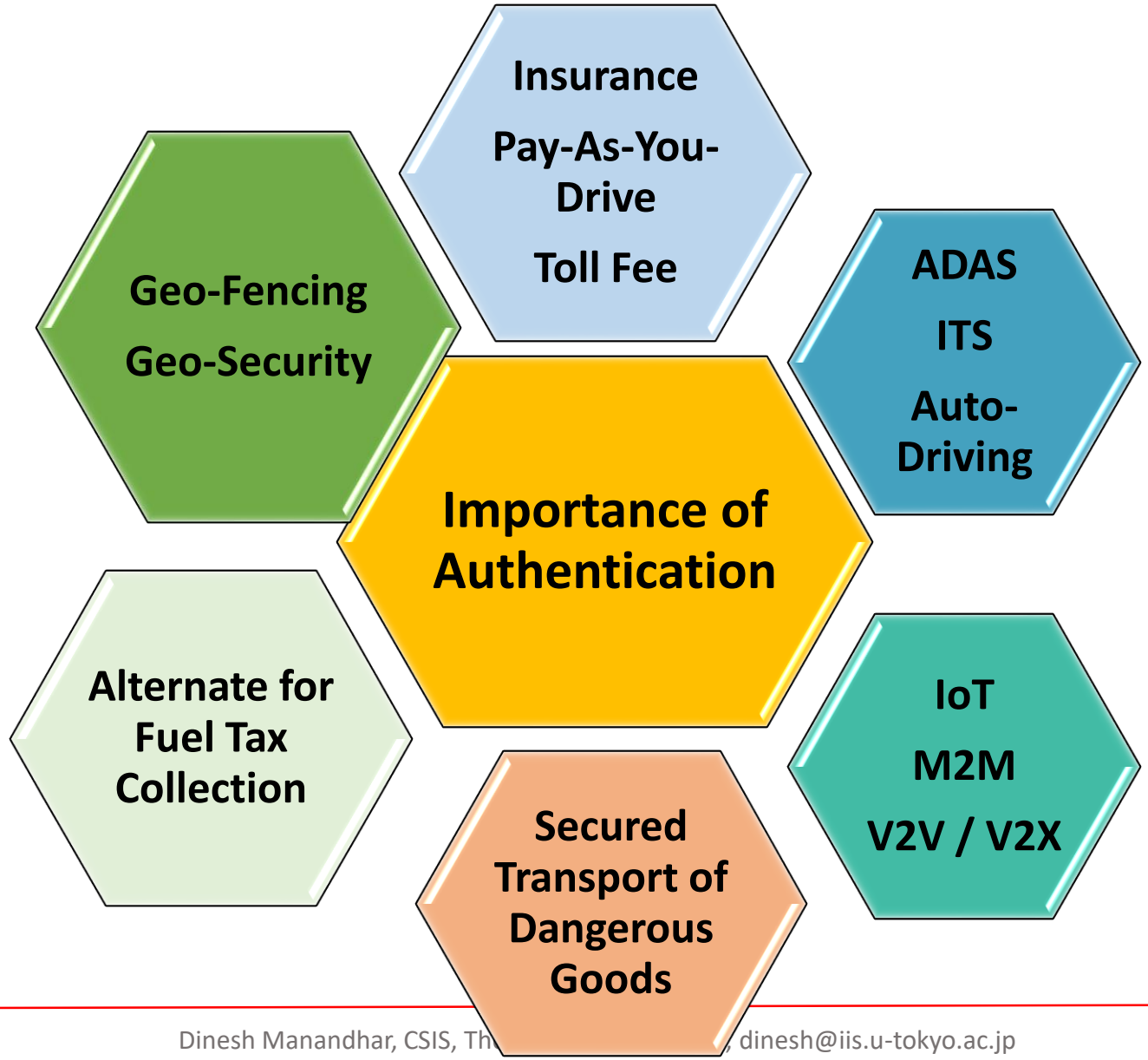
15th March 2017

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

But, there is also fear of GPS Signal Spoofing.

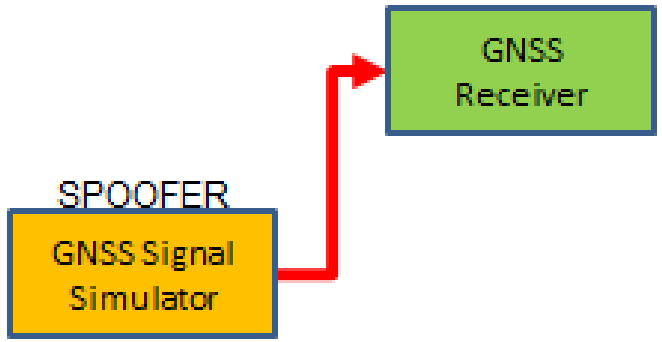
ＧＰＳ捜査訴訟の上告審判決が言い渡された最高裁大法廷。中央は、寺田逸郎裁判長＝15日午後、東京都千代田区（伴龍二撮影）

Why Authentication is Necessary ?

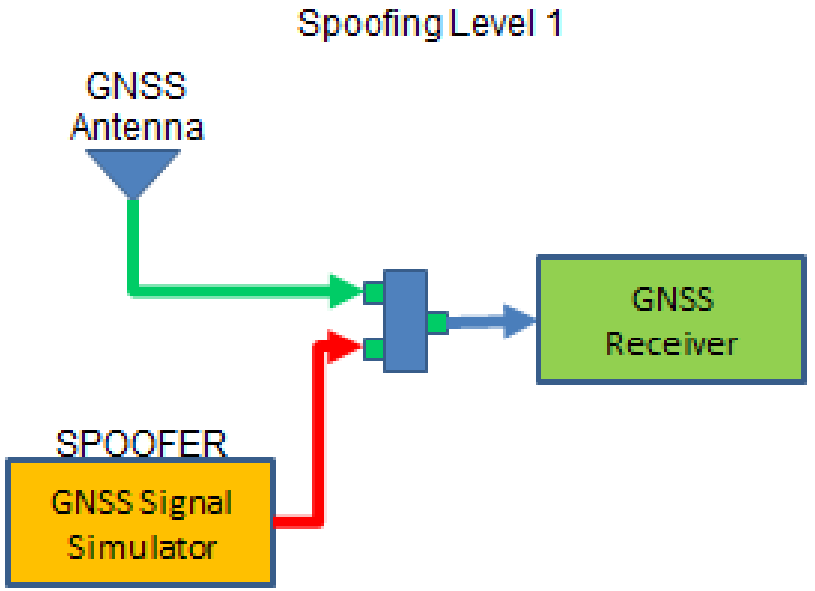


Spoofing Methods

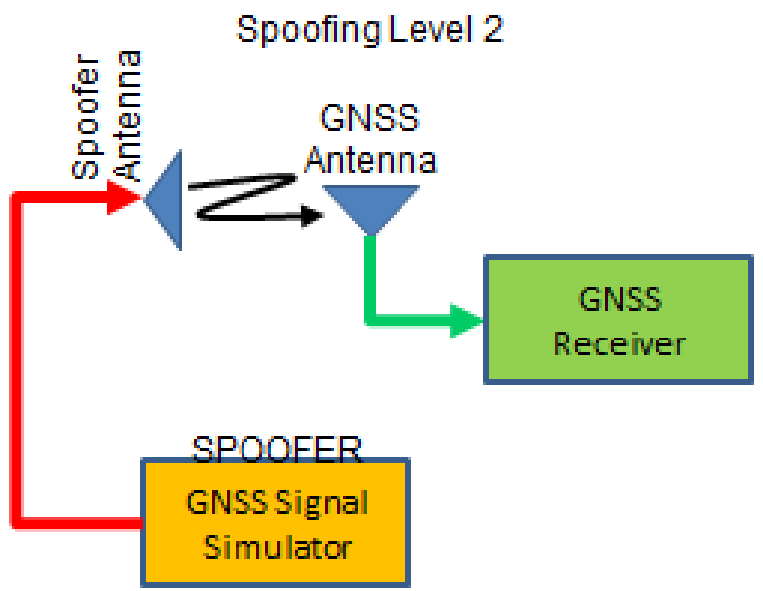
Self-Spoofing
Connect by cable
Real Signal Absent



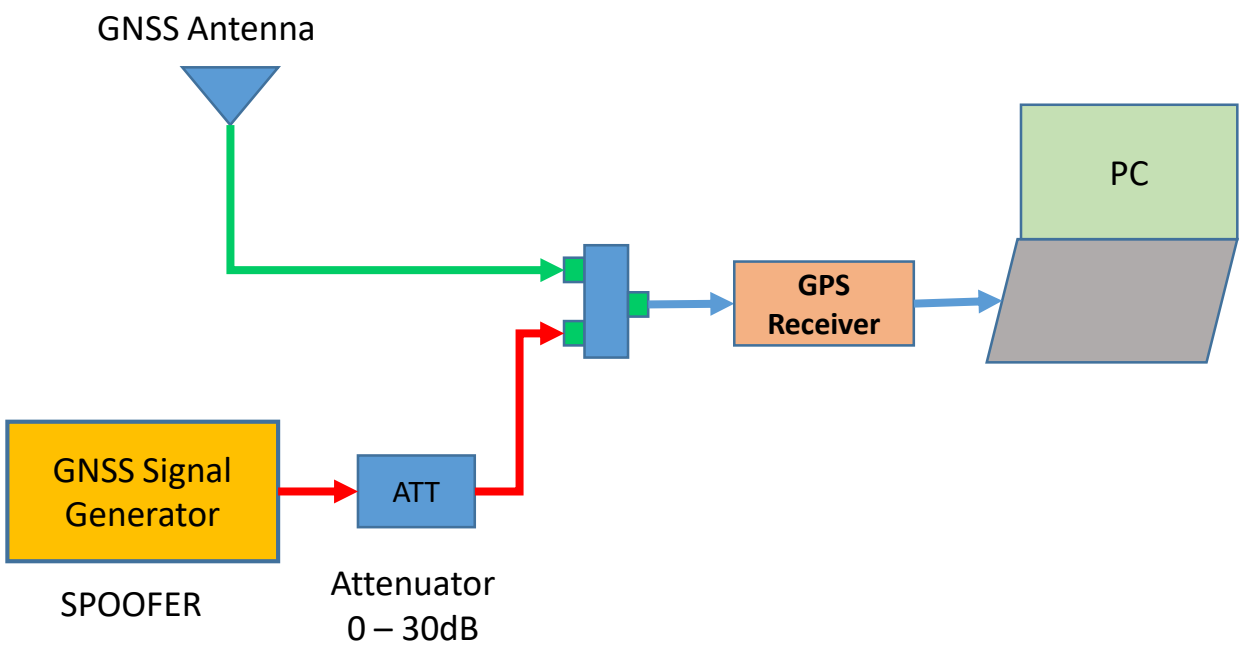
Self-Spoofing
Connect by cable
Real Signal Present

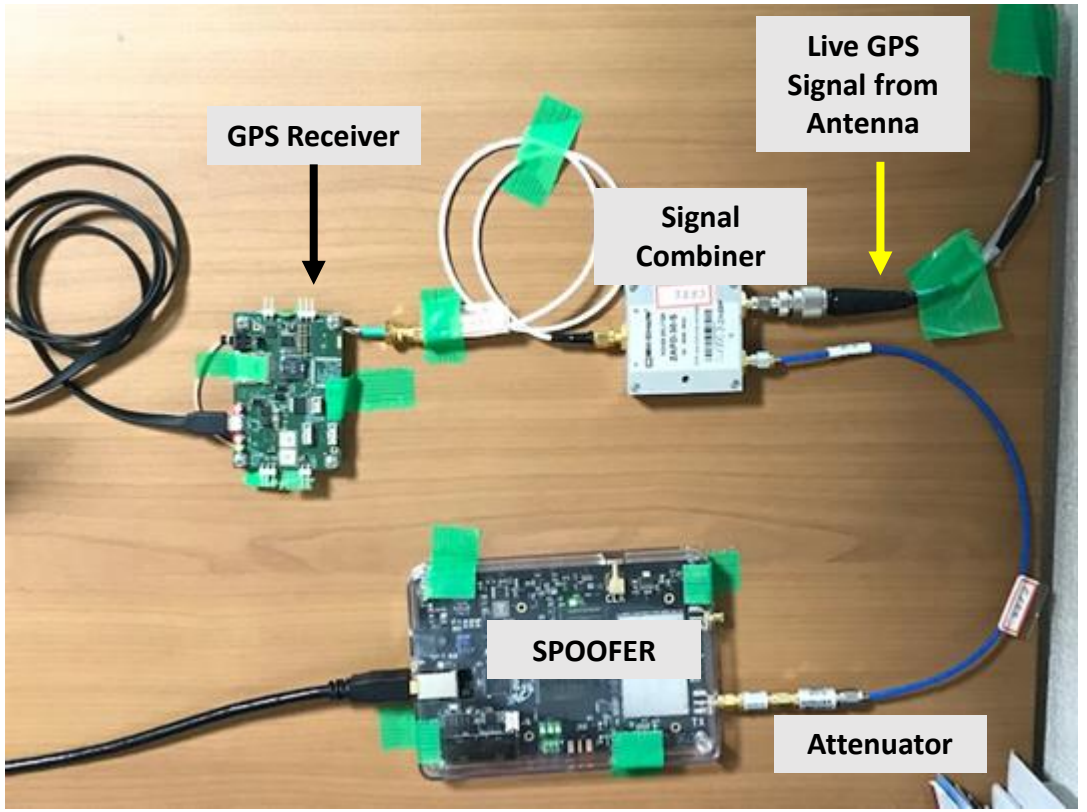


Self or 3rd Party Spoofing
Over the air transmission



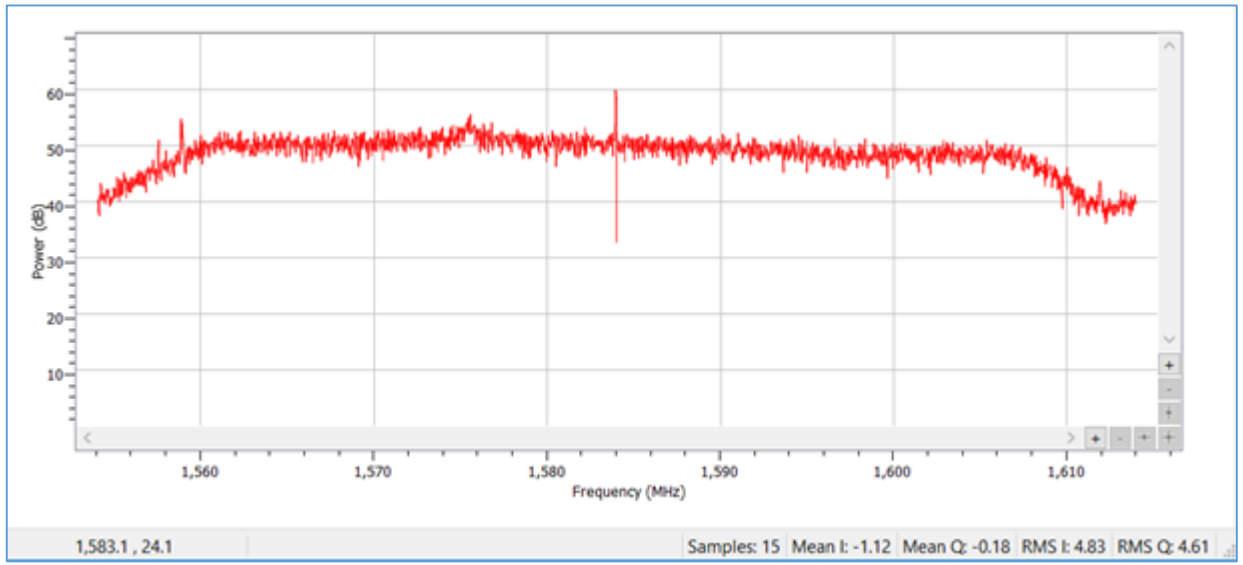
Experiment Setup to Test GPS Spoofing



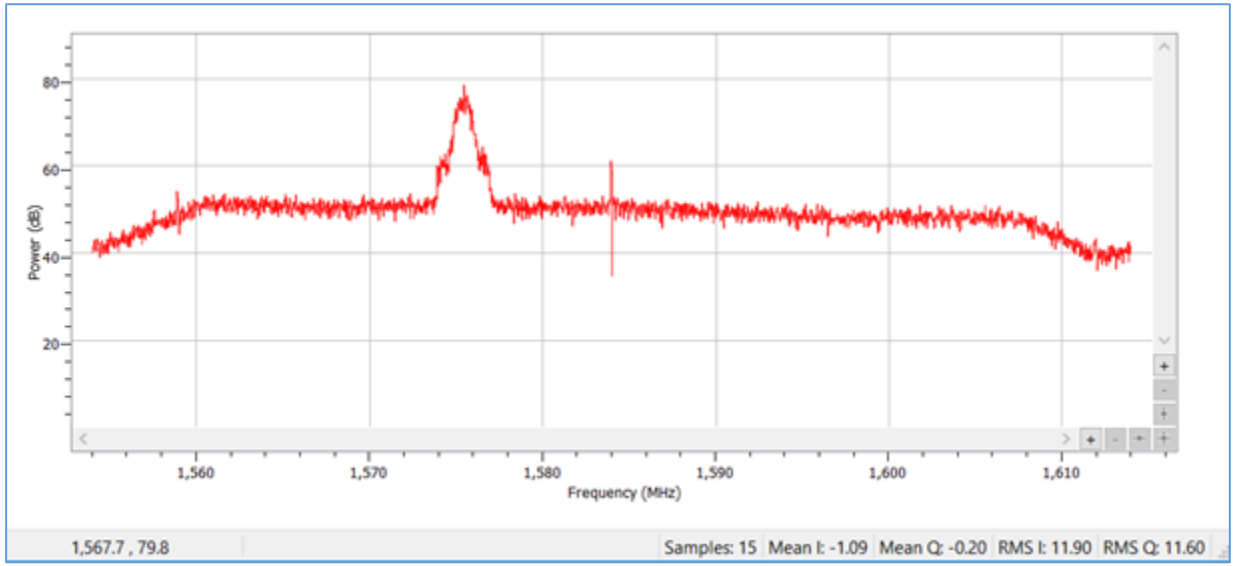


Online Spoofing Demo

Examples of TRUE signal and SPOOF Signal Power Spectrum of IF Data

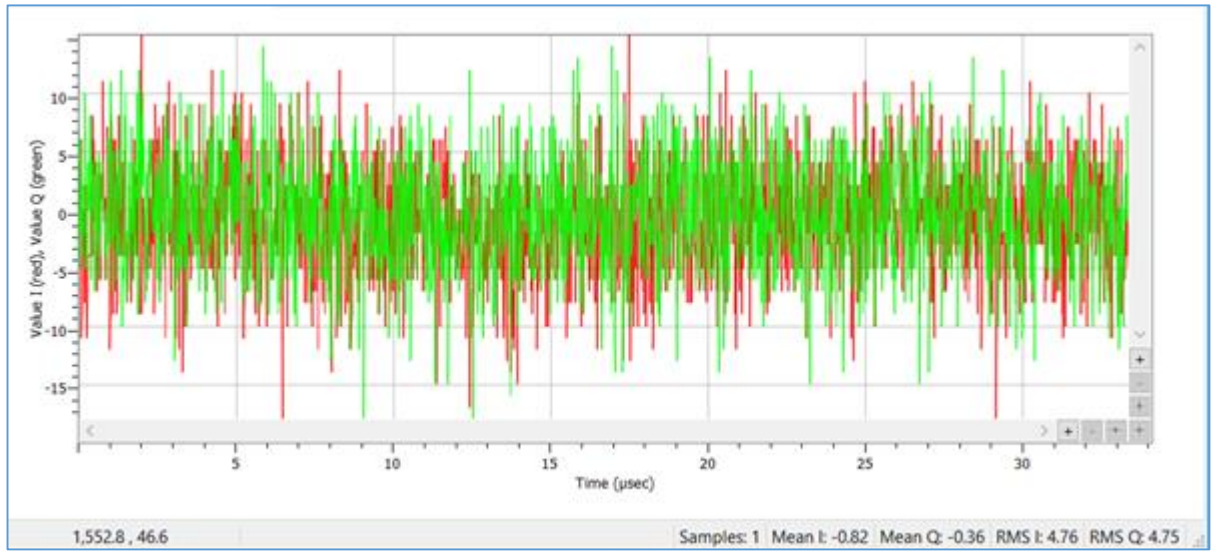


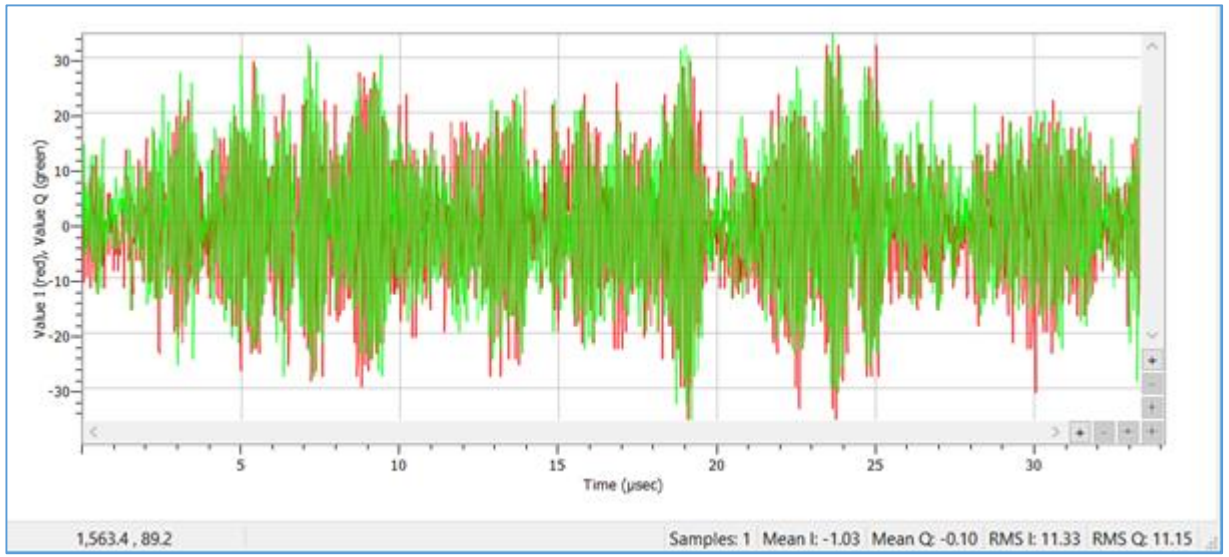
TRUE Signal



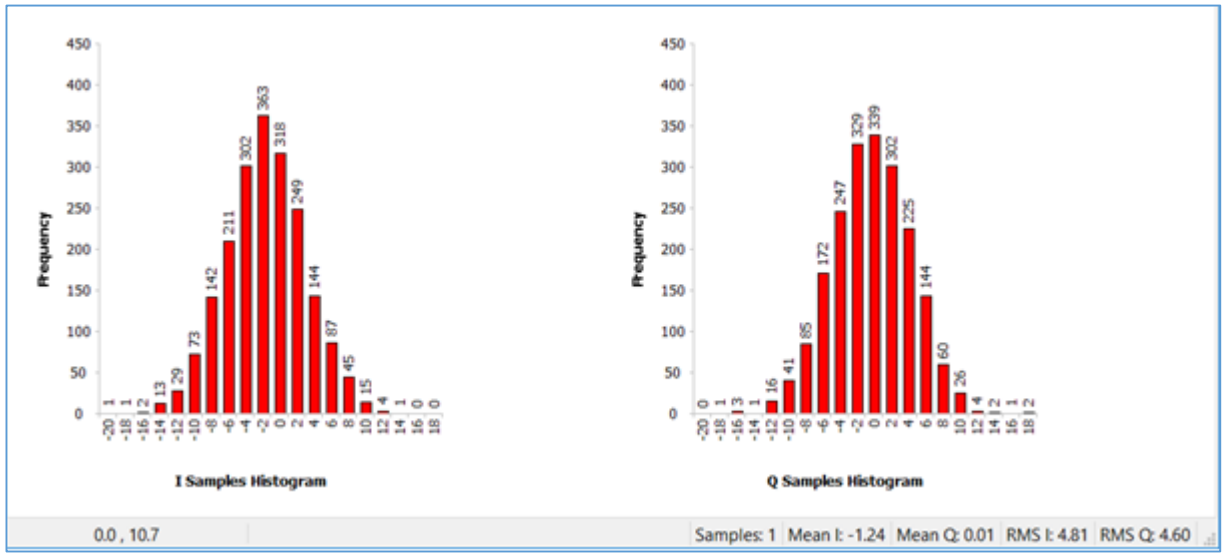
SPOOF Signal during the Attack Period

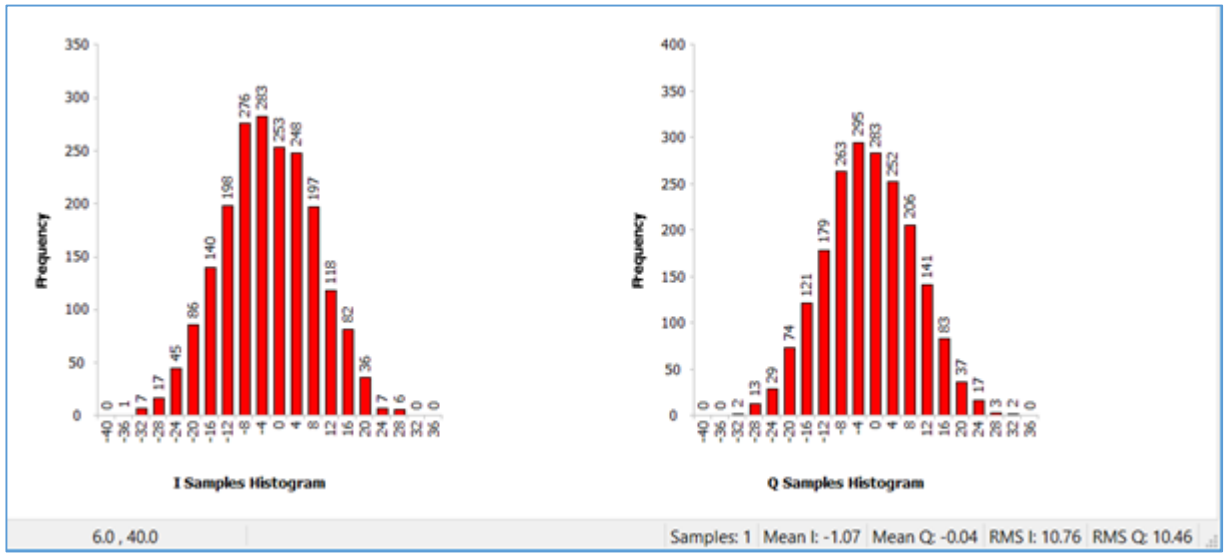
Examples of TRUE signal and SPOOF Signal Time Series IF Data, I & Q Channels



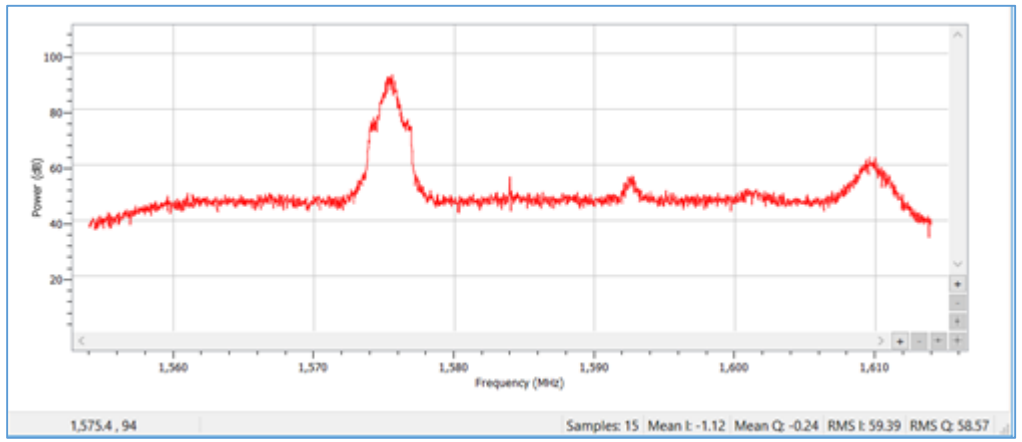


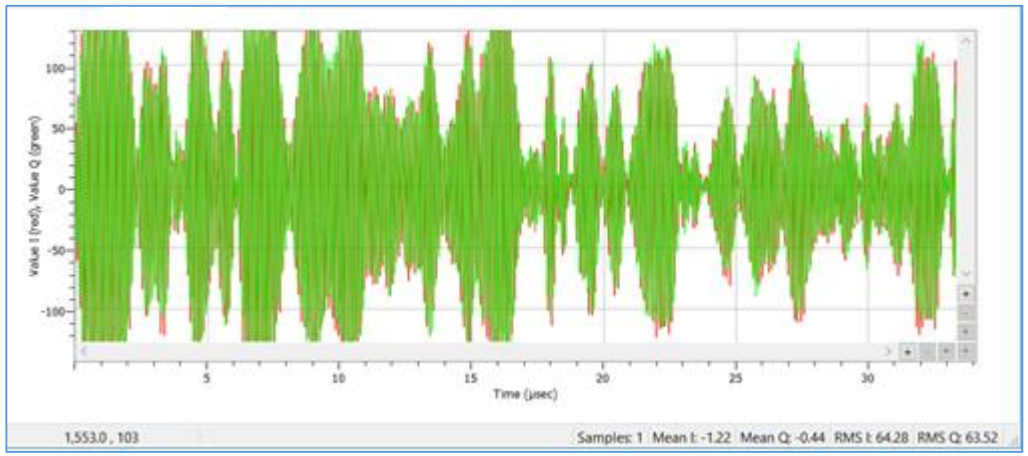
Examples of TRUE signal and SPOOF Signal Histogram of IF Data, I & Q Channels

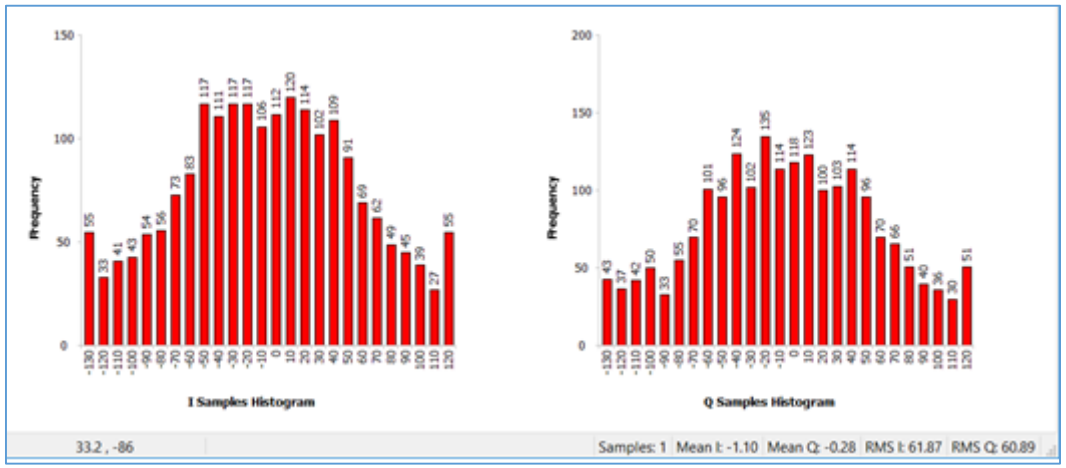




Examples of TRUE signal and Very Strong SPOOF Signal Power Spectrum, Time Series and Histogram of IF Data







We will cover Anti-Spoof Solutions in the next webinar

Additional Information

Please visit websites

For Webinar: http://www.csis.u-tokyo.ac.jp/~dinesh/WEBINAR.htm

https://gnss.peatix.com

Contact:

dinesh@iis.u-tokyo.ac.jp