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?

This movie is all about GPS Spoofing
Software-Based GPS Signal Generator (Spoofing?)

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 I/Q Signal

Transmit Signal

Digital to Analog (D/A) Conversion

Hardware

Software

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

Antenna Gain Pattern

GPS L1C/A
- f = 1575.42MHz

Digital IQ Signal

A/D = 12bit

fs = 26MHz

GPS Source available from Dr. Ebinuma, Chubu University

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 or a Spoofer / Simulator.

GPS Signal Authentication is necessary to detect SPOOF Signals

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

![Map of Black Sea](image1)

![GPS Navigator Image](image2)

[Source](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
- Geo-Fencing Geo-Security
- Alternate for Fuel Tax Collection
- Secured Transport of Dangerous Goods
- Insurance Pay-As-You-Drive Toll Fee
- ADAS ITS Auto-Driving
- IoT M2M V2V / V2X
- Geo-Fencing Geo-Security
- Alternate for Fuel Tax Collection
- Secured Transport of Dangerous Goods
- Insurance Pay-As-You-Drive Toll Fee
- ADAS ITS Auto-Driving
- IoT M2M V2V / V2X
ISO/TC204 WG-18

• Discussions in ISO/TC-204, WG18
  • To Draft regulations for ITS-S related with PVT Data
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
- GNSS Monitoring Stations in Japan and ASEAN Countries
- NAV Data Bits from QZSS Monitoring Stations

Control Segment
- GNSS Monitoring Stations in Japan and ASEAN Countries
- NAV Data Bits from QZSS Monitoring Stations
- Digital Signature Data for Authentication

Authentication Data Center (ADC)
- QZSS Control Station
- Upload Digital Signature Data to QZSS

User Segment
- USER
- Marine / AIS
- Aviation / WAAS
- Railway
- ITS / ADAS
- GNSS Receiver

Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp
Authentication System: Control Segment Development

- Get a Portion of NAV Data Bits from visible GPS, QZSS
- Make RAND
- Hash
- Encrypt RAND Data = (Digital Signature)
- Make L1S NAV MSG 250bit
- Interface to upload Encrypted Digital Signature via L1S Message to QZSS Control System
- Interface to access QZSS monitoring stations and receive NAV Data
- Reference Authentication NAV Data
- Generate Keys
- Make L1S NAV MSG 250bit
- Interface to upload Public Key via L1S Message to QZSS Control System
Digital Signature Generation for Authentication
Authentication System: User Segment

QZSS Signal with Digital Signature for Authentication

- Make RAND From L1C/A NAV MSG
- Hash MSG A
- Get Digital Signature Data from L1S NAV MSG
- Decrypt
- Hash MSG B
- Check HASH MSG A & B
- If HASH MSG A = HASH MSG B Authentication OK Else Authentication Fails
Prototype Anti-Spoofing Receiver

Please join to test and use this system

QZSS Signal with Digital Signature for Authentication

Tablet AUTH APP Ver. : 1.0

Request for KEY

Provide KEY & Other Services

WiFi Link

Authentication Data Center (Service Provider)

Connect through OTG Cable

Dinesh Manandhar, CSIS, The University of Tokyo, dinesh@iis.u-tokyo.ac.jp
Real-time Authentication Test by Car Driving

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

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


Dangers of GPS spoofing and hacking for location based services

Faking of GPS Data a growing and potentially lethal danger – The Japan Times, FB
15th March 2017

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

But, there is also fear of GPS Signal Spoofing.
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