GPS/QZSS Signal Authentication Concept

Dinesh Manandhar, Koichi Chino, Ryosuke Shibasaki
The University of Tokyo

Satoshi Kogure, Jiro Yamashita, Hiroaki Tateshita
Japan Aerospace Exploration Agency (JAXA)

e-mail: dinesh@iis.u-tokyo.ac.jp
Issues Related with Position Data

• Can we Trust GPS position data?
• Is it necessary to authenticate position data?
  – If so, how to do it?
• Why GPS signal is so vulnerable?
  – What type of vulnerabilities?
• What type of studies have been done?
  – DOT’s Volpe Report
• Are there any solutions?
  – Our Approach
Can We Trust GPS Position Data?

• Yes, We Can......, We believe that PNT Data from GPS are always true
  – Hence, GPS is used for many applications
    • Geo-tagging an incident, event, object, photo, video etc
    • Route navigation of vehicles, ships, aircrafts, railway etc
    • Transportation and management of hazardous and dangerous material
    • Location Based Services (LBS) applications
    • Time synchronization of power grids, telecom networks, computer servers, financial transactions etc
  – We are heavily relying on GPS position data for Critical and Security related applications.
...But, until a false signal is transmitted

- GPS like signals can be transmitted using devices to “fool” the GPS receiver
  - A GPS receiver can not identify whether the signal is coming from the space or from the ground
  - The false signal is designed in such a way that it can imitate as signal from the space

spoofing using a GPS signal simulator

Meaconing using a RF Signal Recording & Playback Device
Is it necessary to Authenticate Position Data?

• Yes it is, because:
  – Many critical services use position data
    • A false position data may lead to loss of life or economy
  – We would like to know that a picture taken at “MITA Hall” is really a “MITA Hall”
  – A ship carrying hazardous materials has travelled a designated route
  – The lock of an armored car should open only near its destination
  – LBS services need certified or reliable position data
  – Authentication applications that exist use position and time data from GPS assuming that GPS data will not be spoofed or tampered.
Why is GPS Signal So Vulnerable?

- The signal is extremely weak
  - The power at the receiver is -130dBm (1e-16W)
  - It is below the thermal noise of the receiver, -110dBm

- No such signal protection scheme is implemented (except P/Y code)

- Signal specifications are open to everyone

- Even newly designed signals do not have such protection plans against spoofing

- QZSS Signal is also equally vulnerable as GPS signal
  - The signal structures are similar to GPS

- Spoofing and Meaconing devices are commercially available off-the-shelf
# GPS Vulnerability Issues

<table>
<thead>
<tr>
<th>Interference and Jamming</th>
<th>Spoofing and Meaconing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intentional and Non-Intentional</td>
<td>Intentional</td>
</tr>
<tr>
<td>Can be Detected</td>
<td>Difficult to Detect</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Available of Service but lead to False Position Data</td>
</tr>
<tr>
<td>Many Solutions Exist</td>
<td>No Effective Solution for Existing Signals</td>
</tr>
<tr>
<td>Many Research and Studies</td>
<td>Fewer Research and Studies</td>
</tr>
</tbody>
</table>
Some Authentication Methods

• **Signal Observation**
  – Signal Power and Rate of Change of Signal Power
  – Pseudorange and Rate of Change of Pseudorange
  – Doppler and Rate of Change of Doppler
  – Observation of P codes in L1 and L2 bands
  – Use of L2 Signal for cross-correlation and range difference between L1 and L2
  – Ephemeris Check
  – Time of Arrival, Polarization Discrimination, Consistency with external sensors

• **Code Encryption**
  – Encrypt PRN Codes

• **Message Encryption**
  – Encrypt Navigation Message Data

• **Our Method**
Role of QZSS in Signal Authentication

- QZSS provides unique opportunities for novel applications, because
  - The navigation message in SF4 and SF5 are not limited to 25 pages
    - Various information can be transmitted using NAV MSG Pattern Table
    - Transmit GPS Almanac Data
  - It broadcasts SBAS compatible L1SAIF Signal
  - The satellite is visible at high elevation angle
  - Example of Some Non-PNT Applications:
    - GNSS Signal Authentication
    - Search And Rescue (SAR) compatible with COSPAR-SARSAT
    - Emergency Mass Alert System (EMAS)
    - Bi-static Remote Sensing
    - GNSS Reflection related Applications
Our Method for Authentication

- Use a portion of Navigation Message Bits that changes with Time
- Apply LDPC encoding to the Selected Message
- Transmit the LDPC Encoded Data
  - Using the Existing Signal
    - Use Reserve NAV MSG Locations,
      - For Example: GPS L1C/A: SF4, Page 1, Word 3, 4, 5, 6, 7, 8, 9, 10
    - Use New Message Type
      - For Example: QZSS L1C/A NAV MSG Pattern Table
  - Using a different signal
    - QZSS L1SAIF Signal, Message Type
    - SBAS/MSAS Signal, Message Type
Get a Portion of NAV MSG Data

Generate SEED Value

Make H-Matrix [80,160]

LDPC Encoding

RAND Message 80bit

LDPC Parity 80bit

Transmit LDPC Encoded Data

RAND Message + LDPC Parity Bits 160 bits

Generate SEED Value

Make H-Matrix [80,160]

LDPC Encoding

RAND Message 80bit

LDPC Parity 80bit

Transmit LDPC Encoded Data

RAND Message + LDPC Parity Bits 160 bits

Transmit Using the same signal or using different signal

GPS L1C/A SF4, Page 1 Word 3 to 10

QZSS L1C/A NAV MSG Pattern Table

OR

QZSS L1SAIF New Message Type

OR

SBAS / MSAS New Message Type
Reference Authentication Navigation Data (RAND)

Example of RAND based on GPS L1C/A Sub-Frame 1 NAV MSG

<table>
<thead>
<tr>
<th>Changes every 6 seconds</th>
<th>The same value for about FOUR hours or until the new Ephemeris data are uploaded</th>
<th>1 for all</th>
<th>ID of Each PRN Constant Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF1, Word 2 Time of Week 17 bit</td>
<td>SF1, Word 8 TOC, 16 bit</td>
<td>SF1, Word 9 af1, 16 bit</td>
<td>SF1, Word 10 af0, 22 bit</td>
</tr>
</tbody>
</table>

80 bit

![Diagram showing the structure of RAND data based on GPS L1C/A Sub-Frame 1 NAV MSG. The diagram includes columns for changes every 6 seconds, the same value for about four hours or until new Ephemeris data are uploaded, and ID of Each PRN Constant Value. Each column contains specific data types such as SF1, Word 2 Time of Week 17 bit, SF1, Word 8 TOC, 16 bit, etc.]
Authentication Concept: For QZSS L1C/A Signal

Get QZSS L1C/A NAV MSG

SF1:W1
SF1:W2
SF1:W3
SF1:W4
SF1:W5
SF1:W6
SF1:W7
SF1:W8
SF1:W9
SF1:W10

Generate SEED Value

Make H-Matrix [80,160]

LDPC Encoding

RAND Message Generation 80bit

RAND Message 80bit

LDPC Parity 80bit

QZSS NAV Message Modification: L1C/A or L1SAIF Message

Modified QZSS L1C/A NAV MSG

SF1:W1
SF1:W2
SF1:W3
SF1:W4
SF1:W5
SF1:W6
SF1:W7
SF1:W8
SF1:W9
SF1:W10

QZ Master Control Station

6th Meeting of International Committee on GNSS, 5-9 September 2011, Japan, Last Edited by: d. manandhar
Authentication Concept: For GPS L1C/A Signal

Get GPS L1C/A NAV MSG

QZ Monitoring Station

Generate SEED Value

Make H-Matrix [80,160]

LDPC Encoding

RAND Message Generation 80bit

RAND Message 80bit

LDPC Parity 80bit

QZSS NAV Message Modification: L1C/A or L1SAIF Message

QZ Master Control Station

QZSS L1C/A OR QZSS L1SAIF

SF1:W1
SF1:W2
SF1:W3
SF1:W4
SF1:W5
SF1:W6
SF1:W7
SF1:W8
SF1:W9
SF1:W10
Authentication Concept: Modification of L1SAIF Message

Modified L1SAIF Data, Total Size 212bit

<table>
<thead>
<tr>
<th>Preamble 8bit</th>
<th>Message Type 6bit</th>
<th>RAND Message 80bit</th>
<th>LDPC Parity Bit 80bit</th>
<th>Other Data 52bit</th>
<th>CRC 24bit</th>
</tr>
</thead>
</table>

6th Meeting of International Committee on GNSS, 5-9 September 2011, Japan, Last Edited by: d. manandhar
**Authentication Procedure Details: At Receiver Side**

**Get Authentication Message Data from the QZ Navigation Data**

**Compare Parity Bits (2) & (3)**
- **YES**
  - Authentication PASS
- **NO**
  - Authentication FAIL

**Verify that the LDPC Parity Bits were actually computed from RAND Message**

**Get H-Matrix**

**LDPC Encoding**

**RAND Message from (1)**

**LDPC Parity Bits (2)**

**RAND Message same as (1)**

**RSA Public and Private Keys**

**Authentication Database Center**

6th Meeting of International Committee on GNSS, 5-9 September 2011, Japan, Last Edited by: d. manandhar
Sample Authentication Message

Input (Transmitted) Authentication Message

<table>
<thead>
<tr>
<th>TOW</th>
<th>PRN ID</th>
<th>RAND MSG</th>
<th>PARITY DATA</th>
<th>SEED VALUE</th>
<th>H-Matrix Data</th>
<th>RSA KEYS</th>
</tr>
</thead>
<tbody>
<tr>
<td>272726</td>
<td>8</td>
<td>58B1A16600000007BC708</td>
<td>73DBEA93E7961A5FB2E3</td>
<td>653012443</td>
<td>HMAT_DAT_1</td>
<td>RSAKEY_DATA_1</td>
</tr>
<tr>
<td>272816</td>
<td>10</td>
<td>58B1A1667FFBFBA6C50A</td>
<td>0D2E53CCA0D967C24BA8</td>
<td>653015706</td>
<td>HMAT_DAT_2</td>
<td>RSAKEY_DATA_2</td>
</tr>
<tr>
<td>272846</td>
<td>13</td>
<td>58B1A1667FFA127FD30D</td>
<td>AD5EB63397267847FCC3</td>
<td>653018415</td>
<td>HMAT_DAT_3</td>
<td>RSAKEY_DATA_3</td>
</tr>
<tr>
<td>272877</td>
<td>26</td>
<td>58B1A1667FD5F7F9731A</td>
<td>E73E9799583AC510FD58</td>
<td>653020857</td>
<td>HMAT_DAT_4</td>
<td>RSAKEY_DATA_4</td>
</tr>
</tbody>
</table>

Output Navigation Message from the Receiver

<table>
<thead>
<tr>
<th>Case</th>
<th>Week</th>
<th>TOW</th>
<th>Word 1</th>
<th>Word 2</th>
<th>Word 3</th>
<th>Word 4</th>
<th>Word 5</th>
<th>Word 6</th>
<th>Word 7</th>
<th>Word 8</th>
<th>Word 9</th>
<th>Word 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1623</td>
<td>272726</td>
<td>8BAAAA</td>
<td>58C712</td>
<td>7958B1</td>
<td>A16600</td>
<td>00007B</td>
<td>C7083C</td>
<td>73DBEA</td>
<td>93E796</td>
<td>1A5FB2</td>
<td>E330FC</td>
</tr>
<tr>
<td>2</td>
<td>1623</td>
<td>272816</td>
<td>8BAAAA</td>
<td>58CE90</td>
<td>7A58B1</td>
<td>A1667F</td>
<td>FBFBA6</td>
<td>C50A3C</td>
<td>0D2E53</td>
<td>CCA0D9</td>
<td>67C24B</td>
<td>A825FC</td>
</tr>
<tr>
<td>3</td>
<td>1623</td>
<td>272846</td>
<td>8BAAAA</td>
<td>58D110</td>
<td>7B58B1</td>
<td>A1667F</td>
<td>FA127F</td>
<td>D30D3C</td>
<td>AD5EB6</td>
<td>339726</td>
<td>7847FC</td>
<td>C32DFE</td>
</tr>
<tr>
<td>4</td>
<td>1623</td>
<td>272877</td>
<td>8BAAAA</td>
<td>58D392</td>
<td>7958B1</td>
<td>A1667F</td>
<td>D5F7F9</td>
<td>731A3C</td>
<td>E73E97</td>
<td>99583A</td>
<td>C510FD</td>
<td>582AFD</td>
</tr>
</tbody>
</table>

RAND, 80 bits

LDPC Parity, 80 bits
Summary

• Authentication of GNSS signals is necessary to provide certified position data

• A general concept of Authentication of GPS and QZSS signals has been introduced
  – Needs further analysis of data flow between the monitoring stations, control station and database server to estimate time latency and anti-spoofing capabilities

• QZSS Signals can be used for Authentication of other Open GNSS Signals

• Authentication issues shall be discussed in the ICG meetings
  – Such discussions will provide means for developing new methodologies for authentication