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

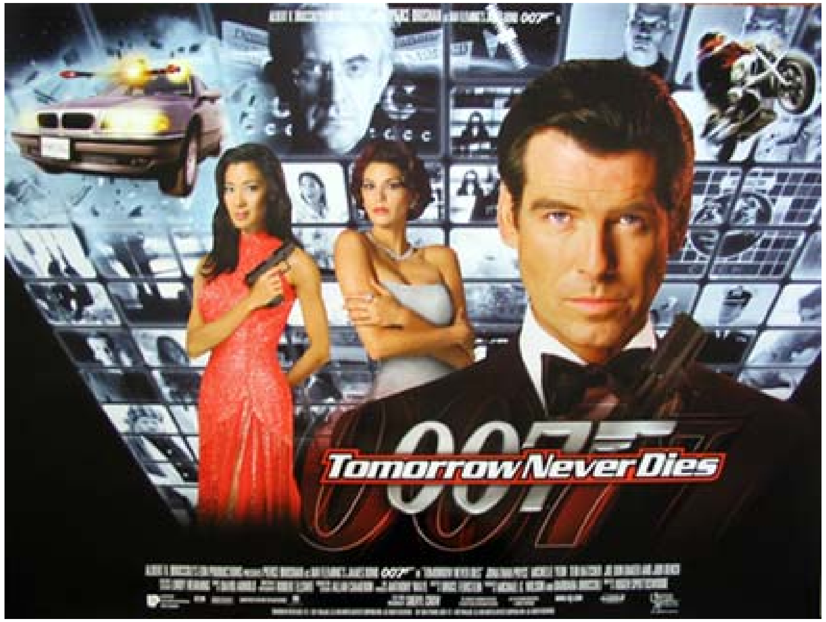
- Can we Trust GPS position data?
- Is it necessary to authenticate position data?
  - If so, how to do it?
- Why GPS signal is so vulnerable?
  - What type of vulnerabilities?
- What type of studies have been done?
  - DOT's Volpe Report
- Are there any solutions?
  - Our Approach

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.

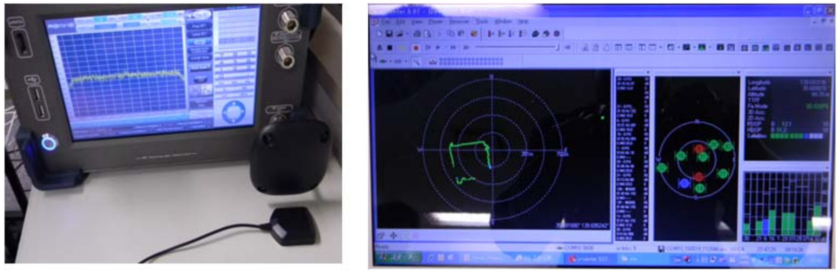
...But, until a false signal is transmitted

- 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



Tomorrow Never Dies

Spoofing using a GPS Signal Simulator



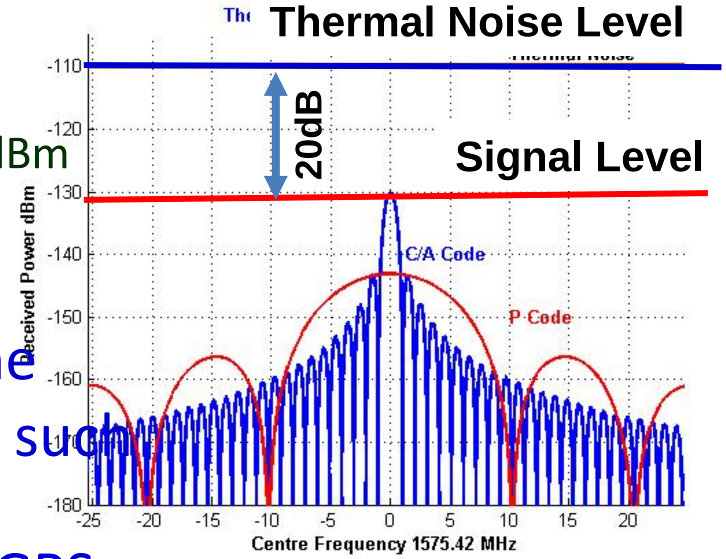
Meaconing using a RF Signal Recording & Playback Device

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

Interference and Jamming	Spoofing and Meaconing
Intentional and Non-Intentional	Intentional
Can be Detected	Difficult to Detect
Denial of Service	Available of Service but lead to False Position Data
Many Solutions Exist	No Effective Solution for Existing Signals
Many Research and Studies	Fewer Research and Studies

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

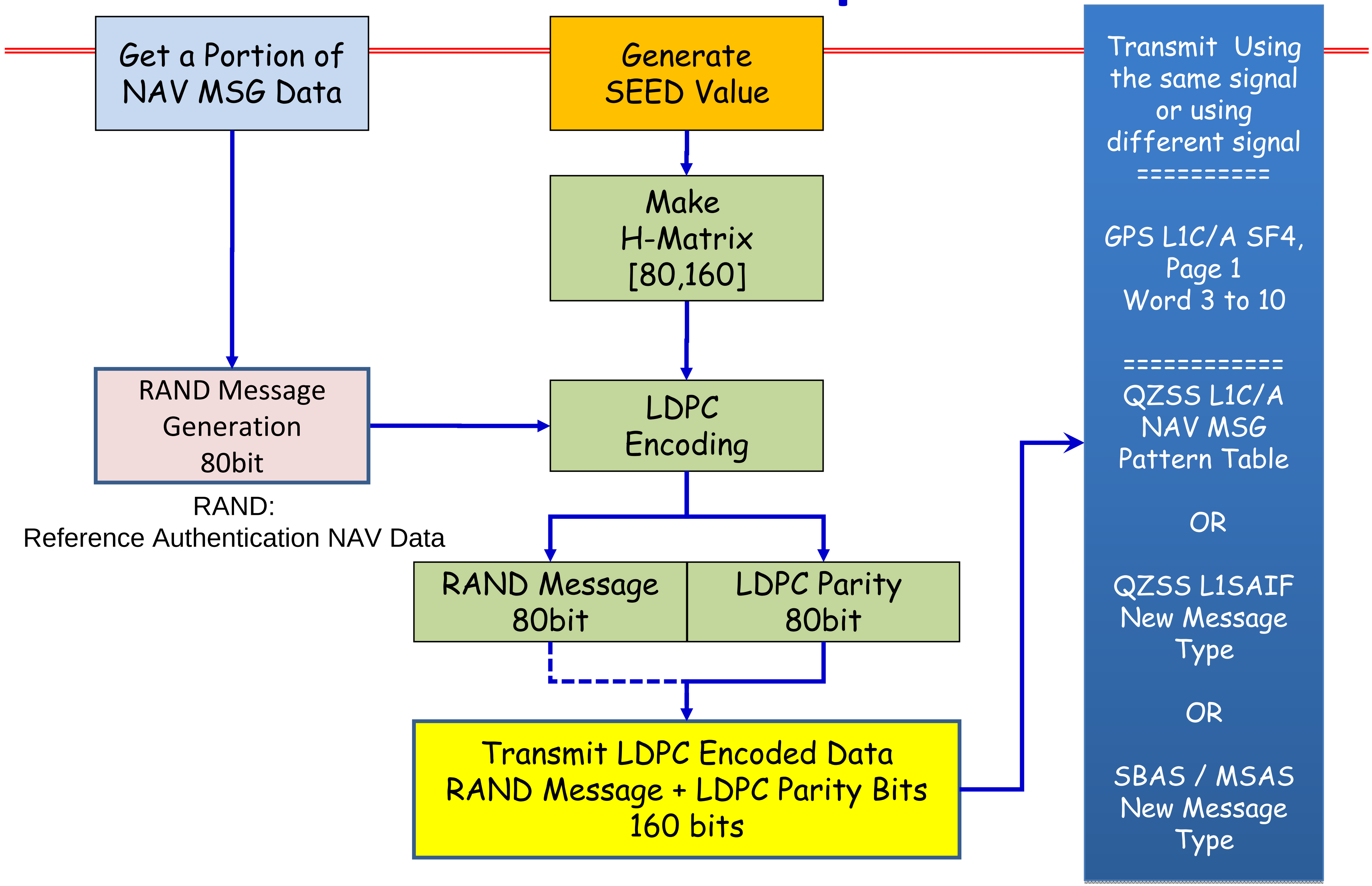
Role of QZSS in Signal Authentication

- 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

Authentication Concept: General

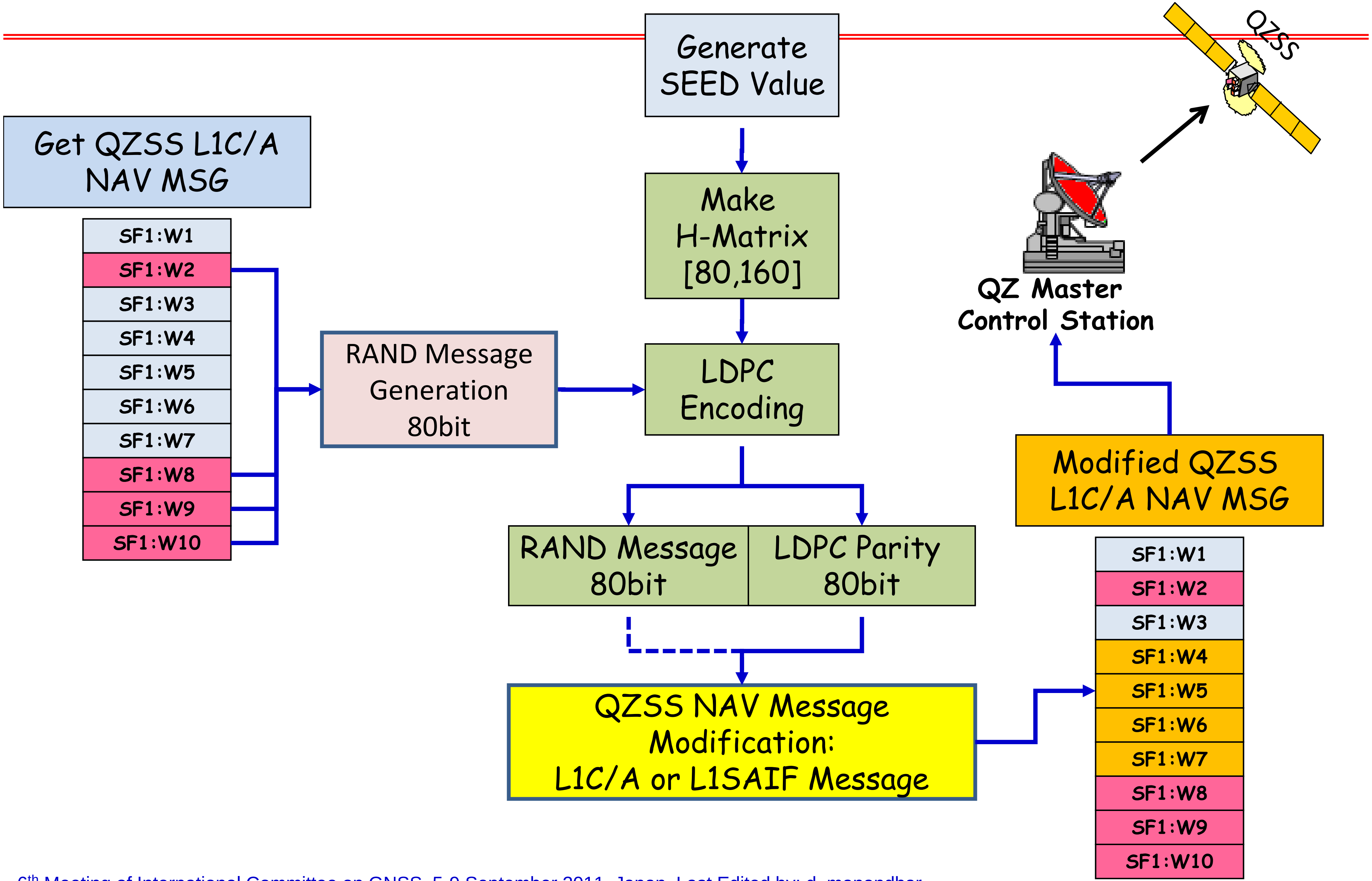


Reference Authentication Navigation Data (RAND)

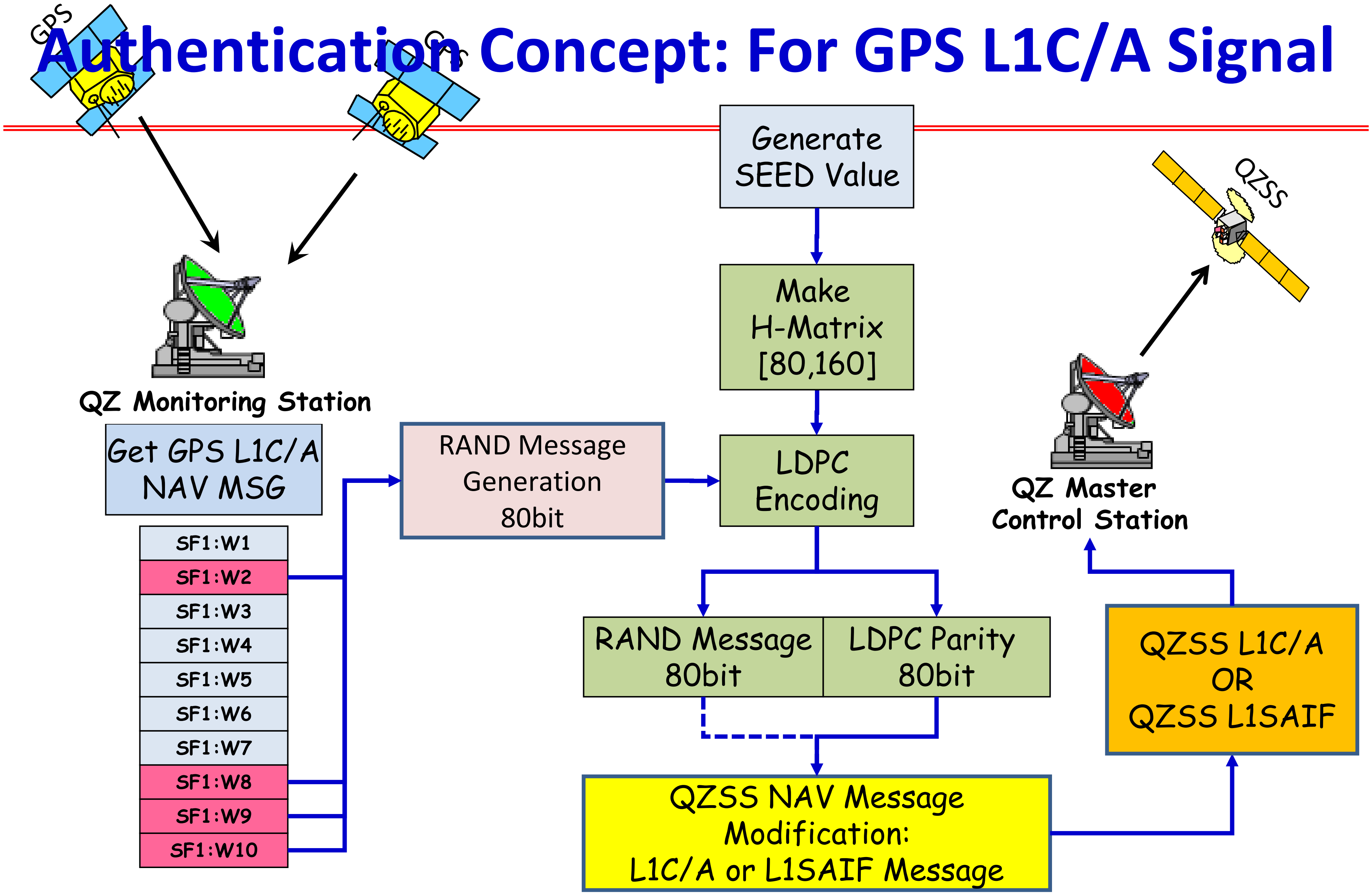
Example of RAND based on GPS L1C/A Sub-Frame 1 NAV MSG

<table>
<tr><td>Changes every 6 seconds</td><td colspan="3">The same value for about FOUR hours or until the new Ephemeris data are uploaded</td><td>1 for all</td><td>ID of Each PRN Constant Value</td></tr>
<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><td>RSV
Bit</td><td>PRN ID
8 bit</td></tr>
<tr><td colspan="6">← 80 bit →</td></tr>
</table>

Authentication Concept: For QZSS L1C/A Signal



Authentication Concept: For GPS L1C/A Signal

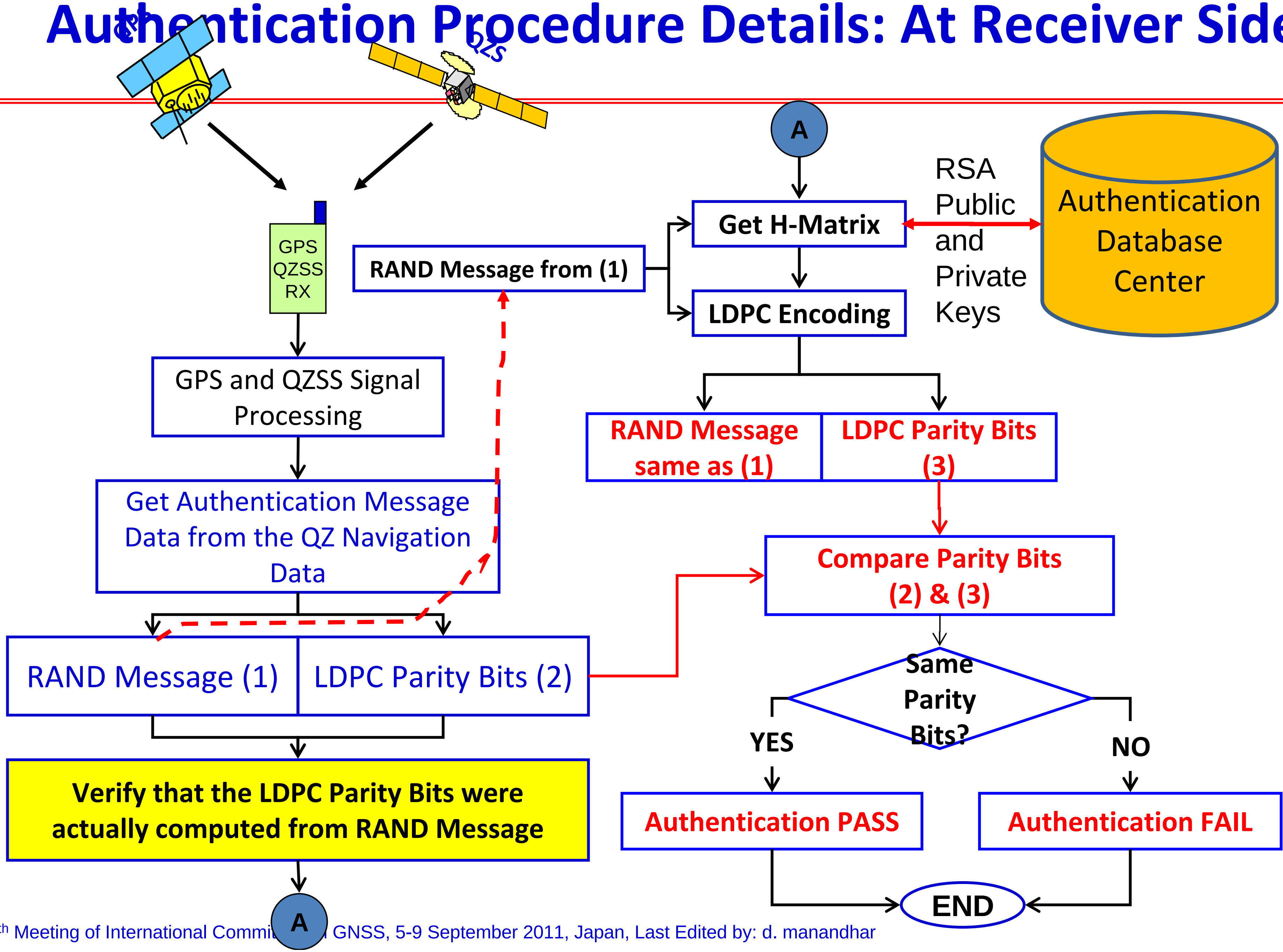


Authentication Concept: Modification of L1SAIF Message

← Modified L1SAIF Data, Total Size 212bit →

Preamble 8bit	**Message Type 6bit**	**RAND Message 80bit**	**LDPC Parity Bit 80bit**	**Other Data 52bit**	**CRC 24bit**

Authentication Procedure Details: At Receiver Side



Sample Authentication Message

Input (Transmitted) Authentication Message

TOW	PRN ID	RAND MSG	PARITY DATA	SEED VALUE	H-Matrix Data	RSA KEYS
272726	8	58B1A1660000007BC708	73DBEA93E7961A5FB2E3	653012443	HMAT_DAT_1	RSAKEY_DATA_1
272816	10	58B1A1667FFBFBA6C50A	0D2E53CCA0D967C24BA8	653015706	HMAT_DAT_2	RSAKEY_DATA_2
272846	13	58B1A1667FFA127FD30D	AD5EB63397267847FCC3	653018415	HMAT_DAT_3	RSAKEY_DATA_3
272877	26	58B1A1667FD5F7F9731A	E73E9799583AC510FD58	653020857	HMAT_DAT_4	RSAKEY_DATA_4

Output Navigation Message from the Receiver

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

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