International Committee on
Global Navigation Satellite Systems

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

GNSS Vulnerability Analysis and Monitoring

Hongliang XU
(Email: xhl@sjtu.edu.cn)

航空航天学院 导航、制导与控制
Guidance, ***N***avigation and ***C***ontrol (GNC)
School of Aeronautics and Astronautics

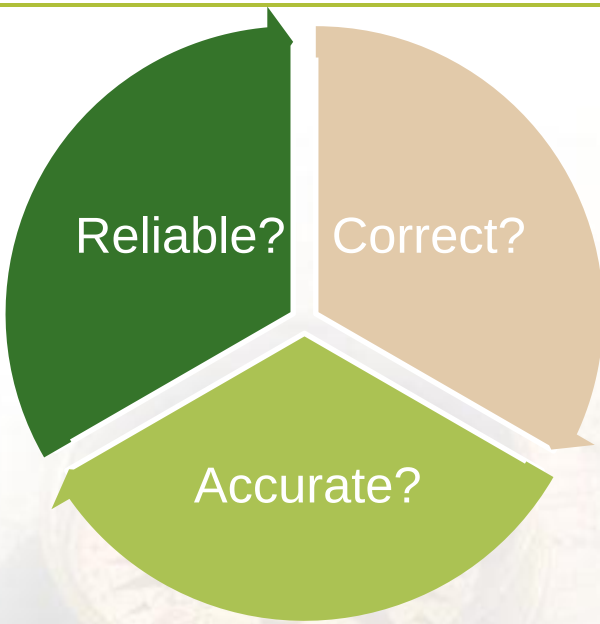
GNSS Vulnerability

- GNSS applications:
  - Military
  - Power grid
  - Telecommunication
  - Transportation
  - Mapping & Surveying
  - Agriculture
  - Electronic financial system
  - Location Based Service
  - Other PNT services

GNSS Vulnerability

- A measure to:
  - Predict
  - Evaluate
  - Monitor

GNSS service impairment



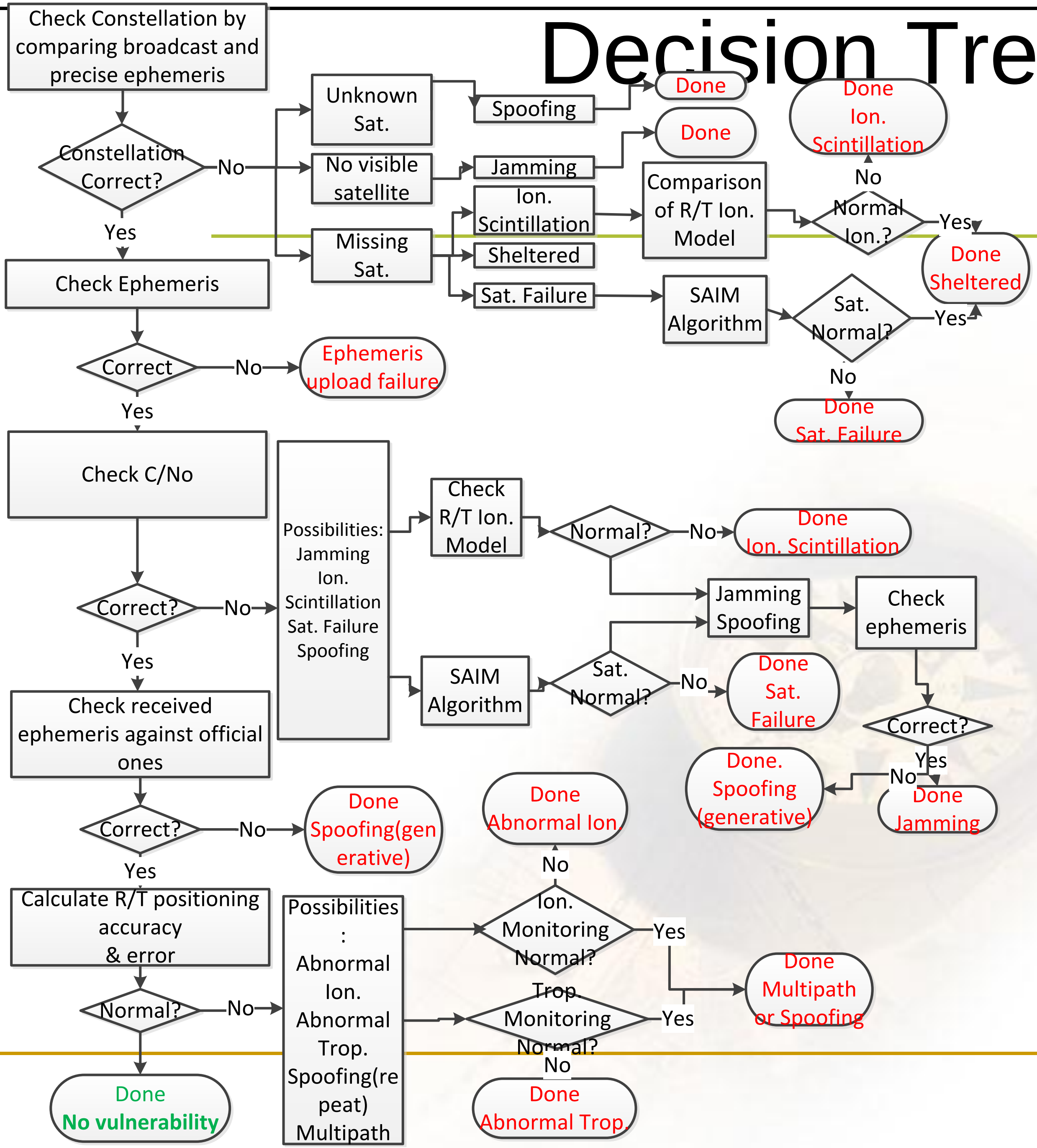
GNSS Vulnerability

- Research funded by Chinese National 863 Program
- Definition：
  - The ability to provide a normal service quality to users under diverse kinds of interference effects.

GNSS Vulnerability

- Vulnerability factors
  - Satellite malfunction and failure;
  - Interferences in the inter-satellite links
  - Interferences in the satellite-ground links;
  - The atmospheric anomaly (ionosphere/troposphere);
  - Electromagnetic interferences ;
  - Multipath effects;
  - Terminal failures;
  - Etc.

Decision Tree



Check Constellation by comparing broadcast and precise ephemeris

Constellation Correct?

No

Unknown Sat.

Spoofing

Done

No visible satellite

Jamming

Done

Missing Sat.

Ion. Scintillation

Comparison of R/T Ion. Model

Normal Ion.?

No

Done Ion. Scintillation

Yes

Done Sheltered

Sheltered

Sat. Failure

SAIM Algorithm

Sat. Normal?

Yes

No

Done Sat. Failure

Yes

Check Ephemeris

Correct

No

Ephemeris upload failure

Yes

Check C/No

Correct?

No

Possibilities: Jamming Ion. Scintillation Sat. Failure Spoofing

Check R/T Ion. Model

Normal?

No

Done Ion. Scintillation

Jamming Spoofing

Check ephemeris

Correct?

Yes

Done Jamming

No

Done. Spoofing (generative)

SAIM Algorithm

Sat. Normal?

No

Done Sat. Failure

Yes

Check received ephemeris against official ones

Correct?

No

Done Spoofing(generative)

Yes

Calculate R/T positioning accuracy & error

Normal?

No

Possibilities: Abnormal Ion. Abnormal Trop. Spoofing(repeat) Multipath

Ion. Monitoring Normal?

No

Done Abnormal Ion.

Yes

Trop. Monitoring Normal?

Yes

Done Multipath or Spoofing

No

Done Abnormal Trop.

Done No vulnerability

GNSS Vulnerability Test Range

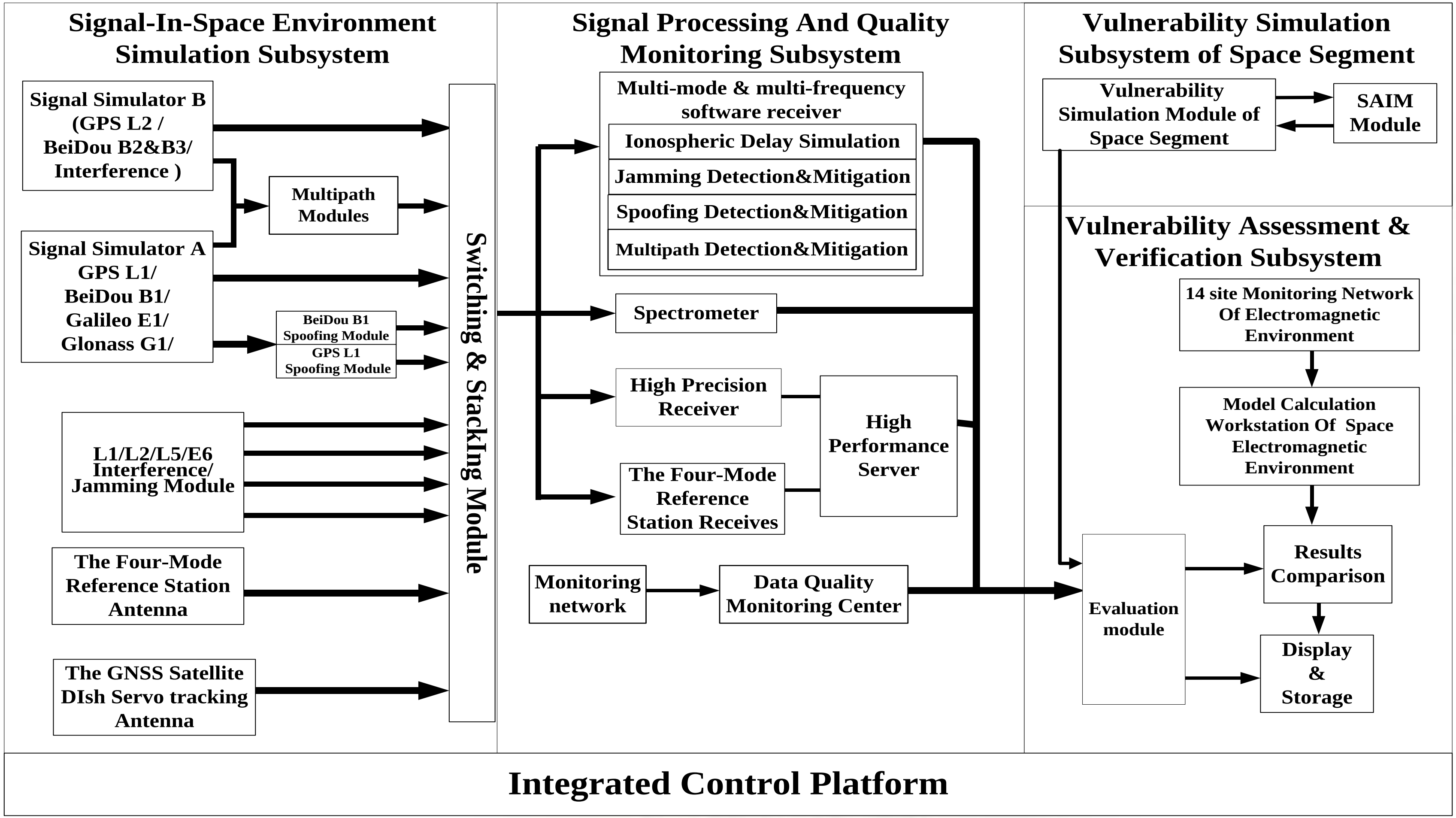
- Research
  - The interference factors
  - Influence mechanism of GNSS vulnerability

- Design and Development
  - A platform for GNSS vulnerability simulation, verification and mitigation

- Test and Verification
  - Detection technologies
  - Mitigation technologies

- Solutions
  - Detect vulnerabilities
  - Provide countermeasures

GNSS Vulnerability Test Range



Signal-In-Space Environment Simulation Subsystem

Signal Simulator B (GPS L2 / BeiDou B2&B3/ Interference)

Multipath Modules

Signal Simulator A GPS L1/ BeiDou B1/ Galileo E1/ Glonass G1/

BeiDou B1 Spoofing Module

GPS L1 Spoofing Module

L1/L2/L5/E6 Interference/ Jamming Module

The Four-Mode Reference Station Antenna

The GNSS Satellite DIsh Servo tracking Antenna

Switching & StackIng Module

Signal Processing And Quality Monitoring Subsystem

Multi-mode & multi-frequency software receiver

Ionospheric Delay Simulation

Jamming Detection&Mitigation

Spoofing Detection&Mitigation

Multipath Detection&Mitigation

Spectrometer

High Precision Receiver

The Four-Mode Reference Station Receives

High Performance Server

Monitoring network

Data Quality Monitoring Center

Vulnerability Simulation Subsystem of Space Segment

Vulnerability Simulation Module of Space Segment

SAIM Module

Vulnerability Assessment & Verification Subsystem

14 site Monitoring Network Of Electromagnetic Environment

Model Calculation Workstation Of Space Electromagnetic Environment

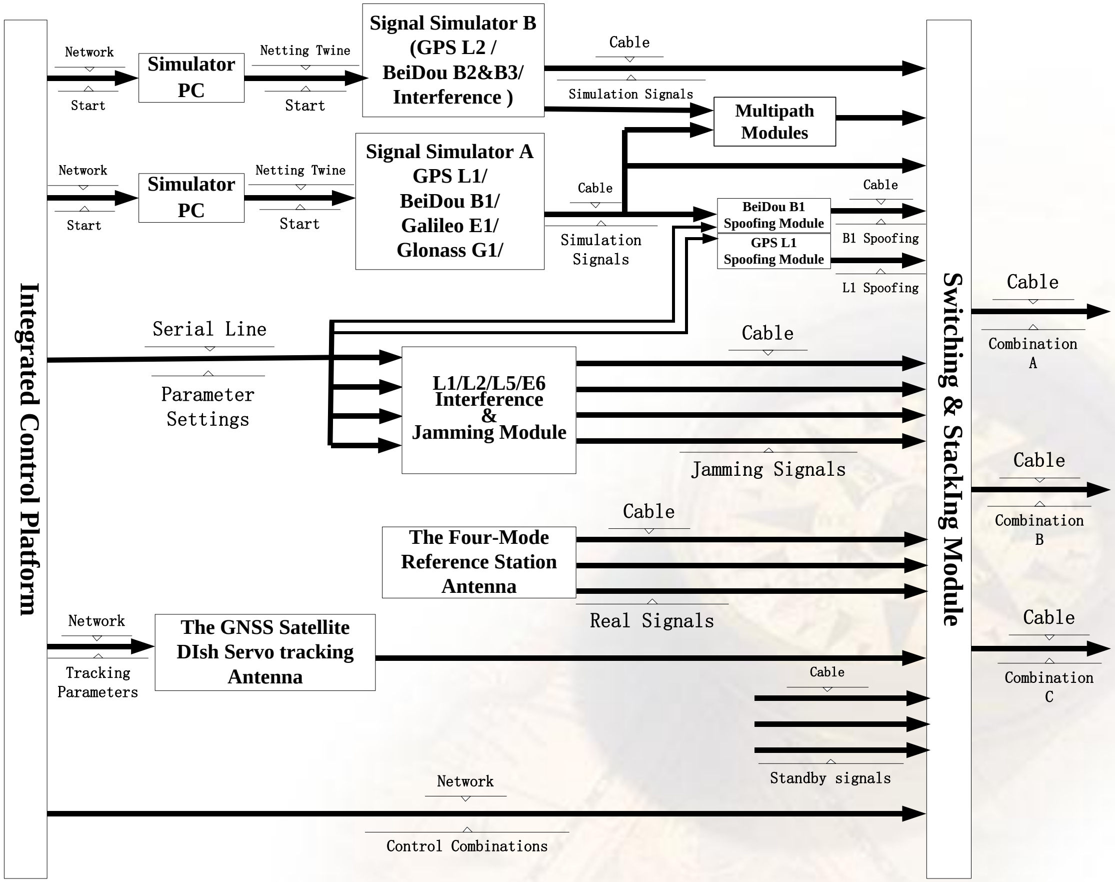
Evaluation module

Results Comparison

Display & Storage

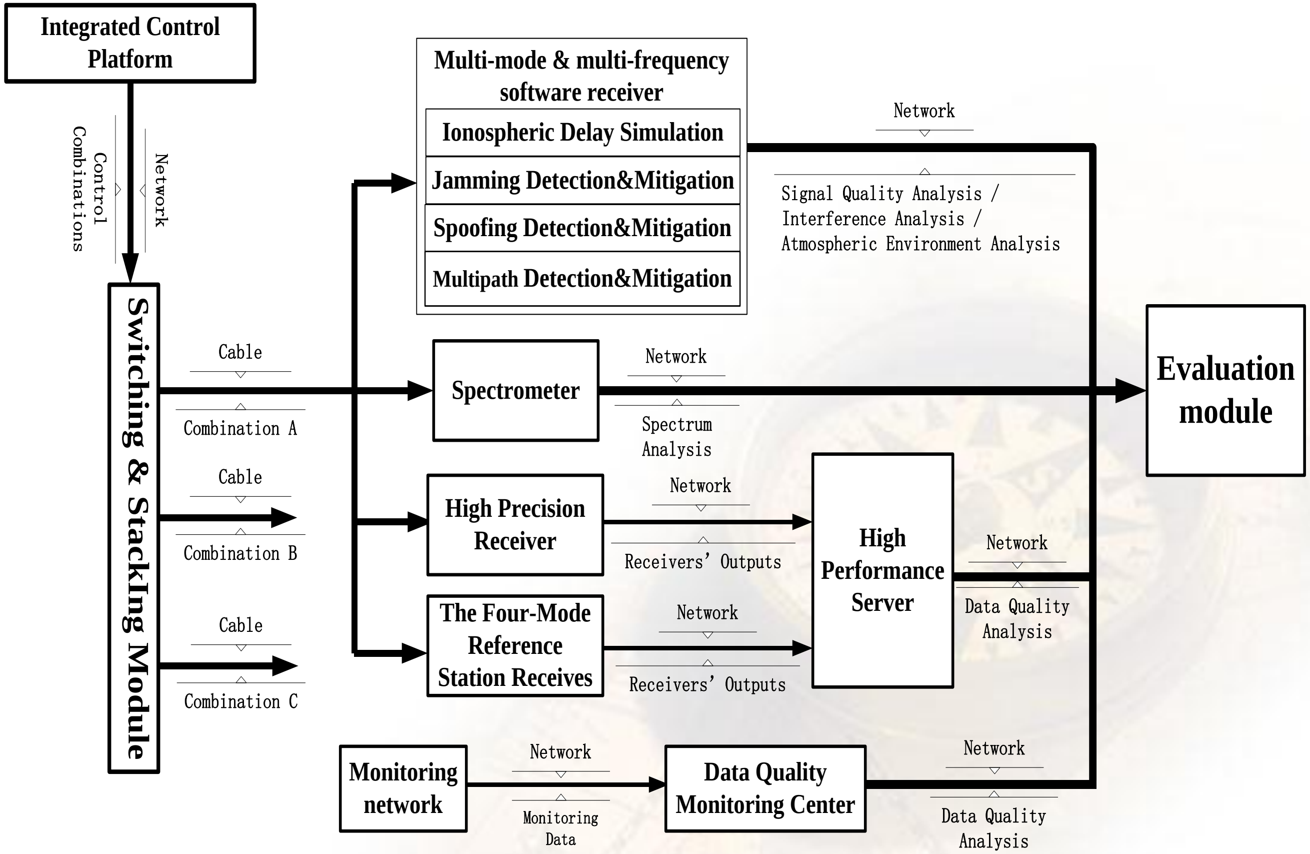
Integrated Control Platform

GNSS Vulnerability Test Range



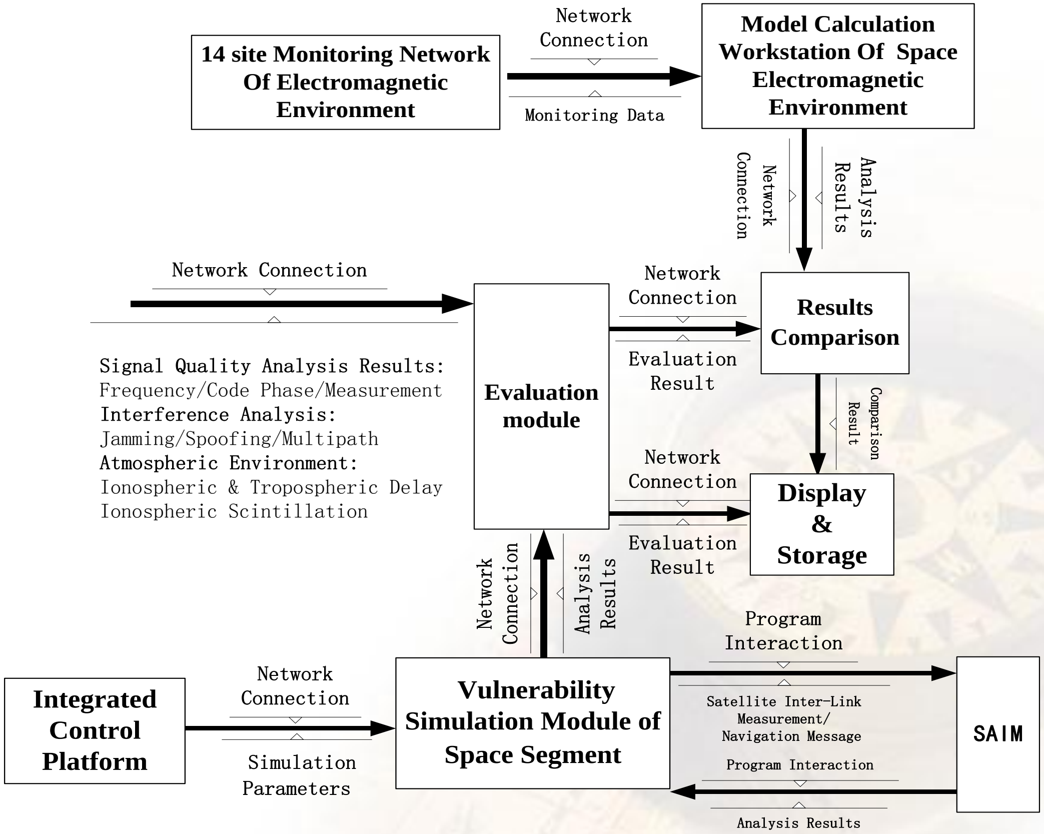
Signal-In-Space Environment Simulation Subsystem

GNSS Vulnerability Test Range


Integrated Control Platform
Control Combinations
Network
Switching & StackIng Module
Cable
Combination A
Cable
Combination B
Cable
Combination C
Multi-mode & multi-frequency software receiver
Ionospheric Delay Simulation
Jamming Detection&Mitigation
Spoofing Detection&Mitigation
Multipath Detection&Mitigation
Network
Signal Quality Analysis / Interference Analysis / Atmospheric Environment Analysis
Spectrometer
Network
Spectrum Analysis
High Precision Receiver
Network
Receivers' Outputs
The Four-Mode Reference Station Receives
Network
Receivers' Outputs
High Performance Server
Network
Data Quality Analysis
Evaluation module
Monitoring network
Network
Monitoring Data
Data Quality Monitoring Center
Network
Data Quality Analysis

Signal Processing And Quality Monitoring Subsystem

GNSS Vulnerability Test Range



14 site Monitoring Network Of Electromagnetic Environment

Network Connection

Monitoring Data

Model Calculation Workstation Of Space Electromagnetic Environment

Network Connection

Analysis Results

Network Connection

Signal Quality Analysis Results:
Frequency/Code Phase/Measurement
Interference Analysis:
Jamming/Spoofing/Multipath
Atmospheric Environment:
Ionospheric & Tropospheric Delay
Ionospheric Scintillation

Evaluation module

Network Connection

Evaluation Result

Results Comparison

Comparison Result

Network Connection

Evaluation Result

Display & Storage

Network Connection

Analysis Results

Program Interaction

Satellite Inter-Link Measurement/ Navigation Message

Integrated Control Platform

Network Connection

Simulation Parameters

Vulnerability Simulation Module of Space Segment

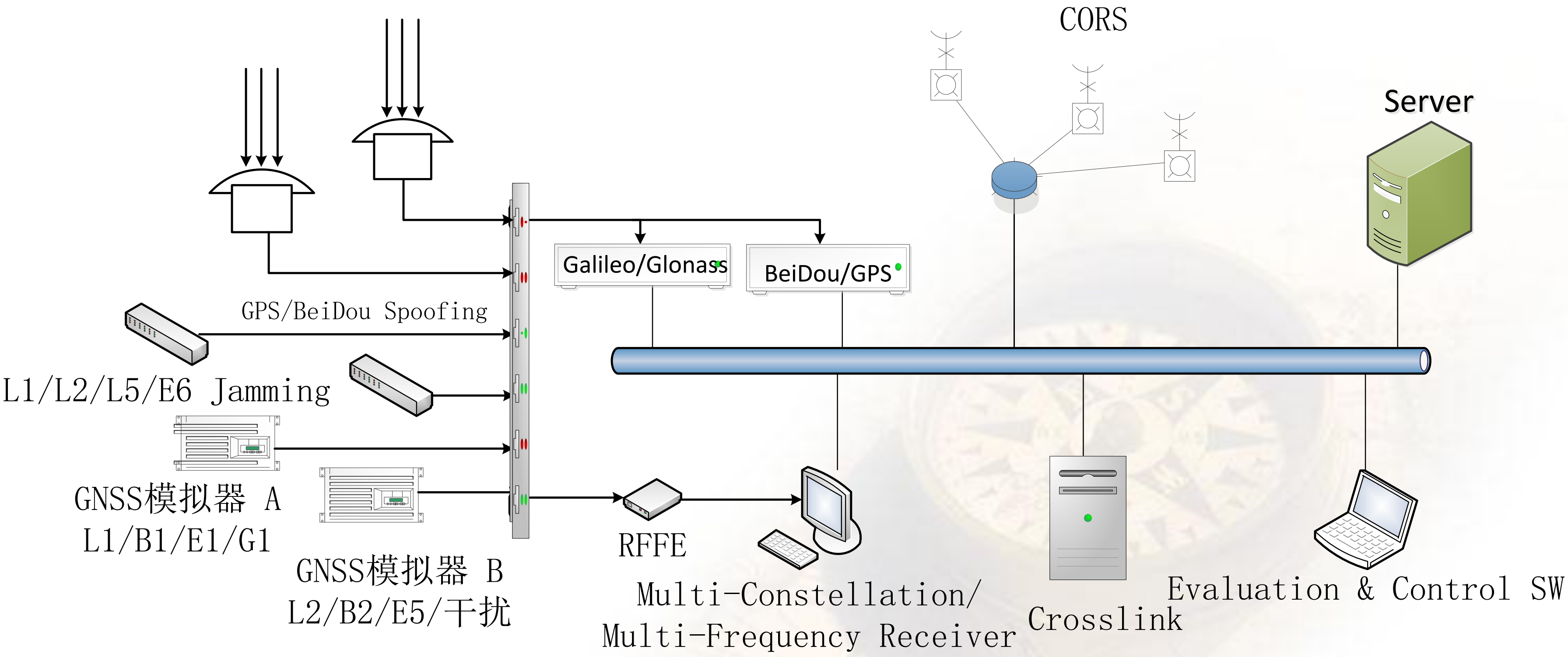
SAIM

Program Interaction

Analysis Results

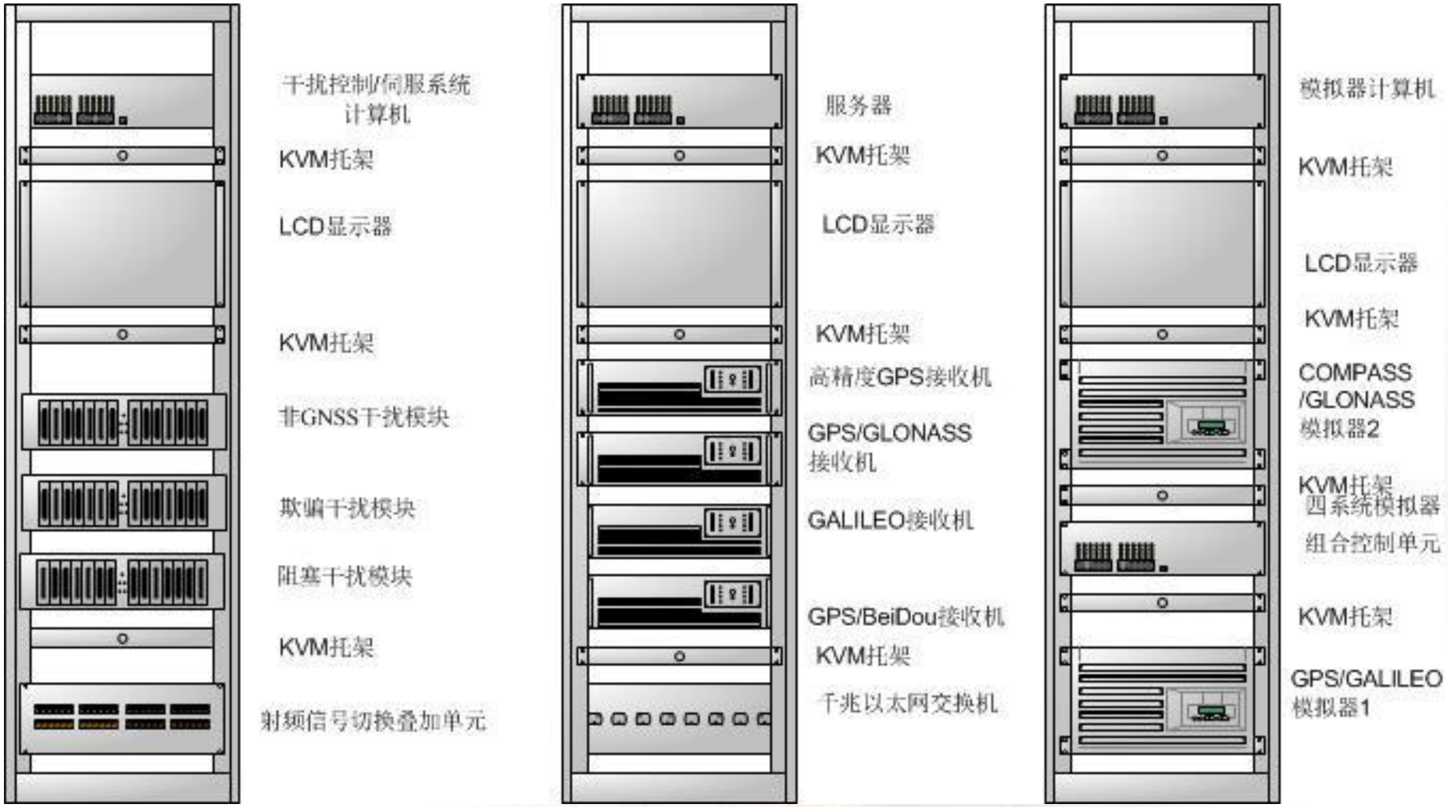
Vulnerability Assessment & Verification Subsystem & Vulnerability Simulation In Space Segment

GNSS Vulnerability Test Range



Interface

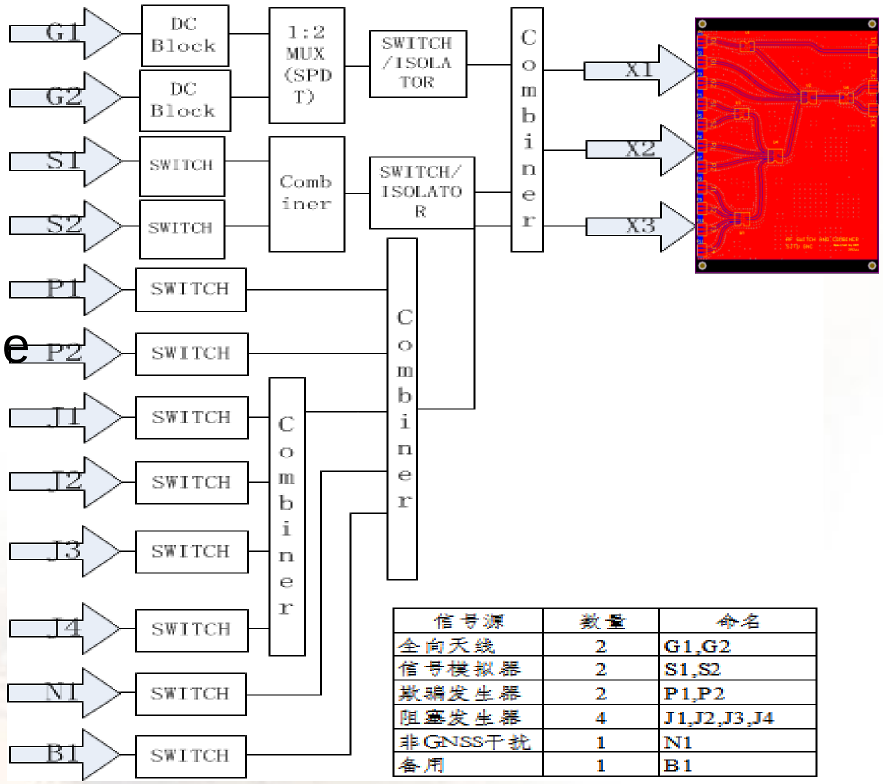
GNSS Vulnerability Test Range



Layout of the Equipment

RF switching and overlay module

- Key modules design
  - Multi-GNSS wideband software L1C/A, L2C, L5, B1, E1B/C, E6B/C, E5a/b.
  - RF switching and overlay module

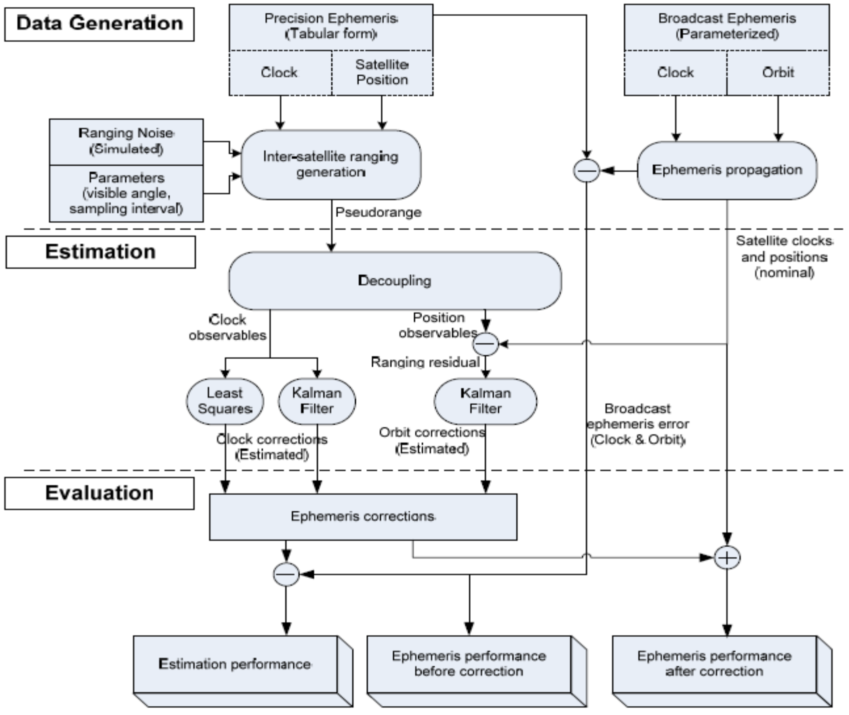


信号源	数量	命名
全向天线	2	G1,G2
信号模拟器	2	S1,S2
欺骗发生器	2	P1,P2
阻塞发生器	4	J1,J2,J3,J4
非GNSS干扰	1	N1
备用	1	B1

Internal logic diagram of RF switching and overlay module

Constellation vulnerability simulation

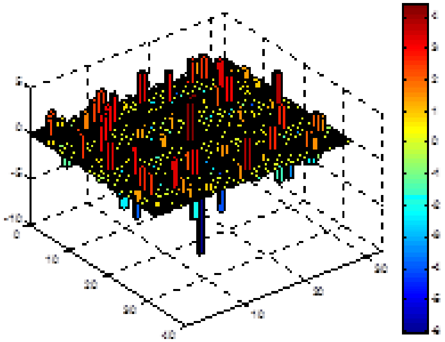
- Simulation of Inter Satellite Link
- SAIM


Data Generation
Precision Ephemeris (Tabular form)
Clock
Satellite Position
Broadcast Ephemeris (Parameterized)
Clock
Orbit
Ranging Noise (Simulated)
Parameters (visible angle, sampling interval)
Inter-satellite ranging generation
Ephemeris propagation
Pseudorange
Estimation
Satellite clocks and positions (nominal)
Decoupling
Clock observables
Position observables
Ranging residual
Least Squares
Kalman Filter
Kalman Filter
Clock corrections (Estimated)
Orbit corrections (Estimated)
Broadcast ephemeris error (Clock & Orbit)
Evaluation
Ephemeris corrections
Estimation performance
Ephemeris performance before correction
Ephemeris performance after correction

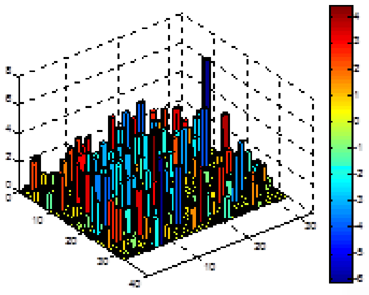
Inter Satellite Link Simulation

Simulation of Constellation Vulnerability

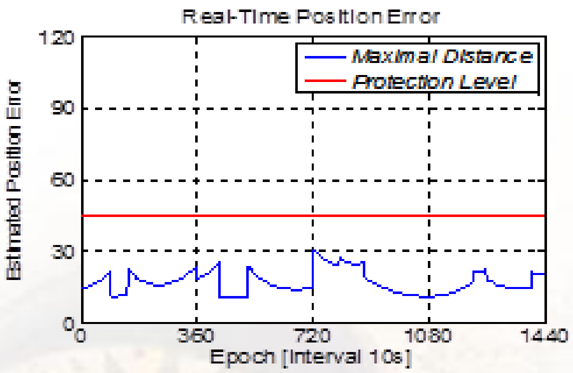
- SAIM Analysis



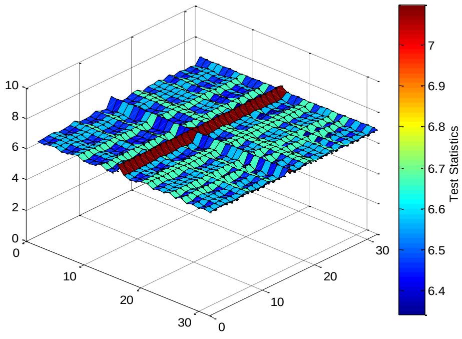
Orbit Error Residual



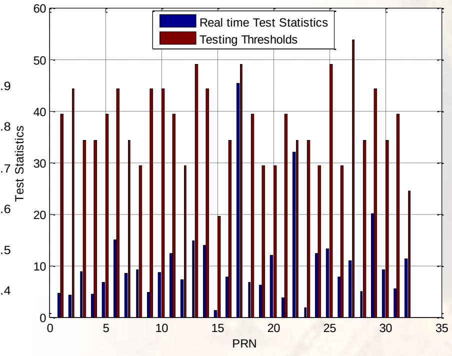
Orbit error residual



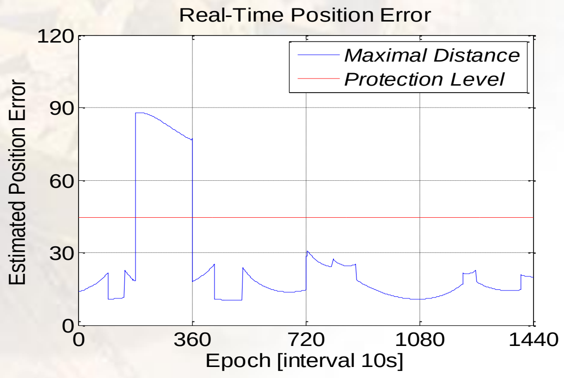
Position Error



Minimal Detectable Bias



Test statistics



Pseudrange coarse error

Satellite Autonomous Integrity Monitoring

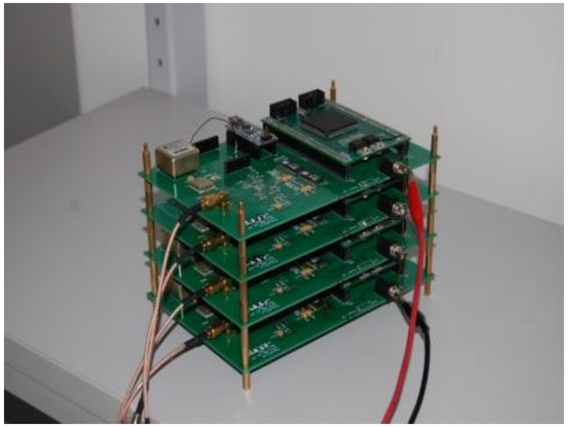
	Broadcast ephemeris	IGS product Ultra-Rapid (predicted half)	SBAS(WAAS)	GDGPS (JPL 2010)	Proposed method
Origins of Measurements	Monitoring Stations	Ground reference stations	Ground reference stations	Ground reference stations	Inter-satellite ranging
Accuracy (orbit)	~100cm	~5cm	>0.75m (UDRE)	<20 cm RMS	~20cm RMS (radial) ~50cm RMS (otherwise)
Accuracy (clock)	~150 cm RMS 75 cm SDev	~90cm RMS ~45cm SDev	-	<20 cm RMS	~20cm RMS
Coverage	Global	Global	Regional	Global	Global
Update rate	4~6h	6h		1Hz	15min
Sample interval	daily	15 min		30s (orbit) / 1s (clock)	15 min
Latency	Real time	Real time	<15 seconds	4-6 seconds	few minutes
Accessibility	broadcast	Internet	SBAS GEO satellites	Network / GEO sat. (TDRSS)	broadcast
Receiver compatibility	Y	N	Y	N	Y (minor F/W update)

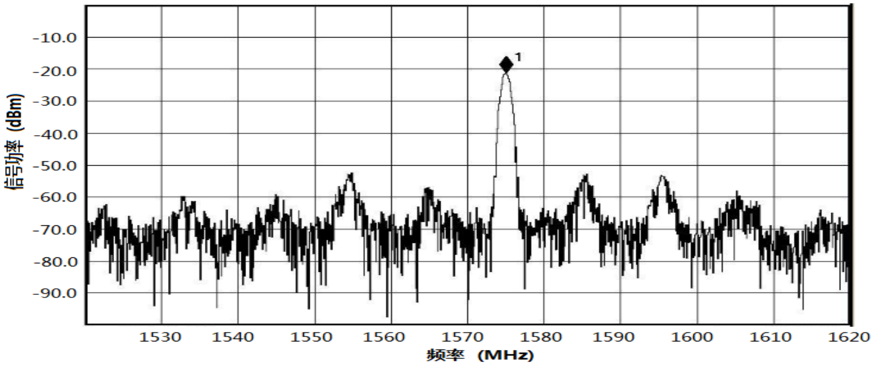
Interference Detection & Mitigation

- GNSS interference and anti-interference technology
  - Aims
    - To provide spoofing and jamming signal simulators based on self-developed pseudolite technology.
    - To evaluate the interference effects on GNSS software receiver
    - To develop anti-spoofing and anti-jamming technologies based on self-developed software GNSS receiver

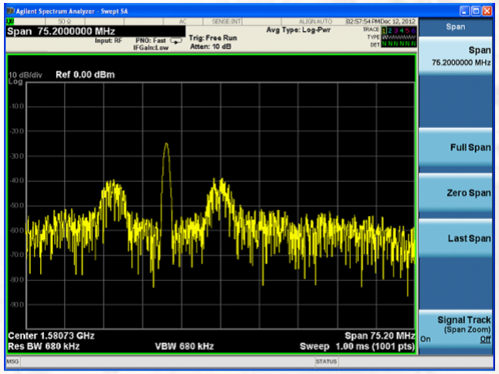
Interference Detection & Mitigation

Jamming Signal Simulator: the jamming interference on the bands of L1/L2/L5/E5 could be generated and other interference could be realized on the L5 jamming device.



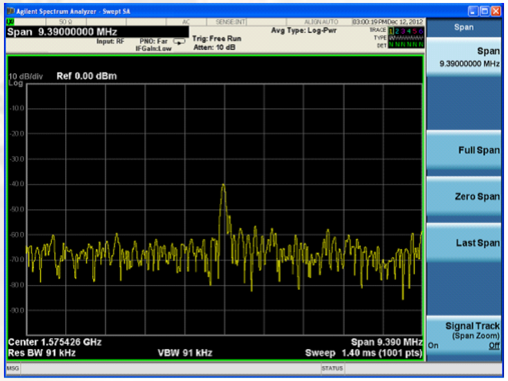


Obstruction spectrogram of single-frequency interference produced by the jamming device



```
50 Ω    AC    SENSE:INT    ALIGN AUTO    02:57:54 PM Dec 12, 2012
Span 75.2000000 MHz        Avg Type: Log-Pwr    TRACE 1 2 3 4 5 6
  Input: RF   PNO: Fast   Trig: Free Run        TYPE
              IFGain:Low  Atten: 10 dB          DET N N N N N N
10 dB/div   Ref 0.00 dBm
Log
Span 75.2000000 MHz
Center 1.58073 GHz                              Span 75.20 MHz
Res BW 680 kHz        VBW 680 kHz        Sweep 1.00 ms (1001 pts)
```

Wide-band jamming

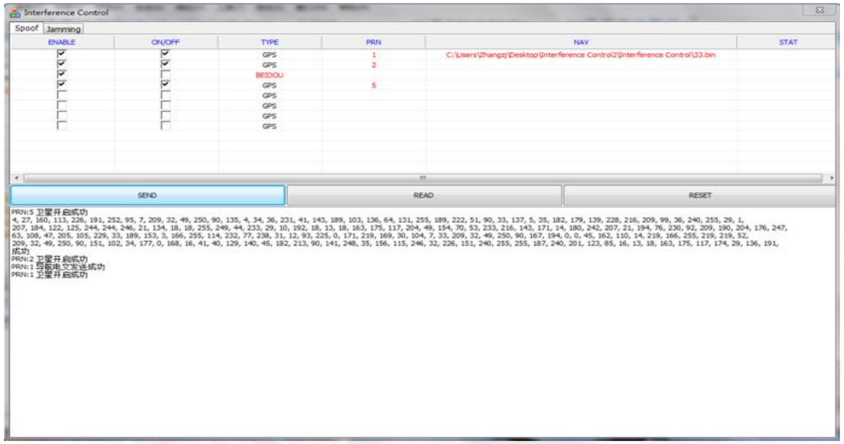


```
50 Ω    AC    SENSE:INT    ALIGN AUTO    03:00:19 PM Dec 12, 2012
Span 9.39000000 MHz        Avg Type: Log-Pwr    TRACE 1 2 3 4 5 6
  Input: RF   PNO: Far    Trig: Free Run        TYPE
              IFGain:Low  Atten: 10 dB          DET N N N N N N
10 dB/div   Ref 0.00 dBm
Log
Span 9.39000000 MHz
Center 1.575426 GHz                             Span 9.390 MHz
Res BW 91 kHz         VBW 91 kHz         Sweep 1.40 ms (1001 pts)
```

Narrow-band jamming

Interference Detection & Mitigation

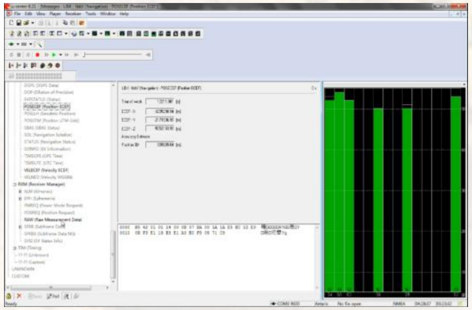
- Spoofing signal simulator
  - generate spoofing signal in GPS L1 and BeiDou B1 bands
  - generate at most 8 fake GNSS signals simultaneously
  - Output power be adjusted through -130dBm to 0dBm
  - The navigation message can be modified or added arbitrarily



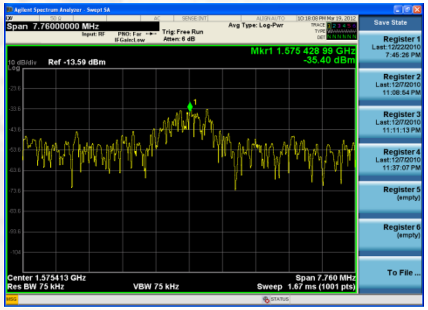
ENABLE	ON/OFF	TYPE	PRN	NAV	STAT
☑	☑	GPS	1	C:\Users\Zhangzj\Desktop\Interference Control2\Interference Control\33.bin	
☑	☑	GPS	2		
☑	□	BEIDOU			
☑	☑	GPS	5		
□	□	GPS			
□	□	GPS			
□	□	GPS			
□	□	GPS			

```
PRN:5 卫星开启成功
4, 27, 160, 113, 226, 191, 252, 95, 7, 209, 32, 49, 250, 90, 135, 4, 34, 36, 231, 41, 143, 189, 103, 136, 64, 131, 255, 189, 222, 51, 90, 33, 137, 5, 35, 182, 179, 139, 228, 216, 209, 99, 36, 240, 255, 29, 1,
207, 184, 122, 125, 244, 244, 246, 21, 134, 18, 18, 255, 249, 44, 233, 29, 10, 192, 18, 13, 18, 163, 175, 117, 204, 49, 154, 70, 53, 233, 216, 143, 171, 14, 180, 242, 207, 21, 194, 76, 230, 92, 209, 190, 204, 176, 247,
63, 108, 47, 205, 105, 229, 33, 189, 153, 3, 166, 255, 114, 232, 77, 238, 31, 12, 93, 225, 0, 171, 219, 169, 30, 104, 7, 33, 209, 32, 49, 250, 90, 167, 194, 0, 0, 45, 162, 110, 14, 219, 166, 255, 219, 219, 52,
209, 32, 49, 250, 90, 151, 102, 34, 177, 0, 168, 16, 41, 40, 129, 140, 45, 182, 213, 90, 141, 248, 35, 156, 115, 246, 32, 226, 151, 240, 255, 255, 187, 240, 201, 123, 85, 16, 13, 18, 163, 175, 117, 174, 29, 136, 191,
成功
PRN:2 卫星开启成功
PRN:1 导航电文发送成功
PRN:1 卫星开启成功
```

The spoofing interference control center



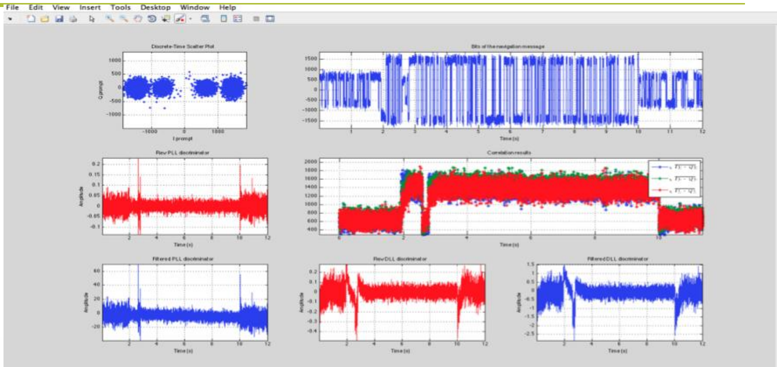
The ublox receiver is cheated and give a wrong navigation result



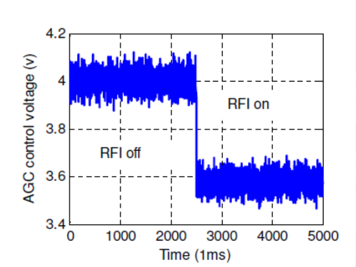
The spectrum of 8 GNSS spoofing signals

Interference Detection & Mitigation

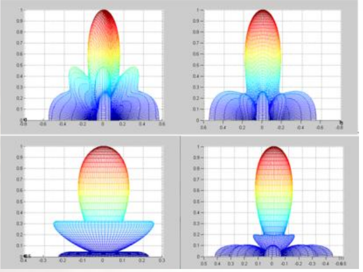
- The anti-interference technology
  - Analyze the influences of spoofing interference on the PLL, DLL and the received signal power.
  - Analyze the influences of jamming interference on the AGC module.
  - Simulate several anti-interference technology
    - LMS based adaptive time domain filter
    - Self-adaptive spatial domain filter anti-interference technology
    - Array-antenna technology


File Edit View Insert Tools Desktop Window Help
Discrete-Time Scatter Plot
Bits of the navigation message
Raw PLL discriminator
Correlation results
Filtered PLL discriminator
Raw DLL discriminator
Filtered DLL discriminator
Time (s)

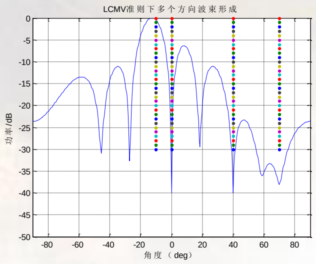
Influences of the Spoofing interference on the tracking loop



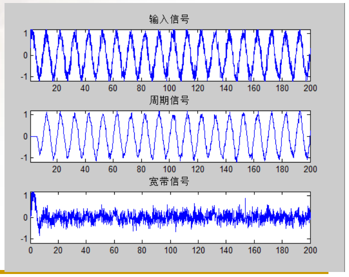
Influences on the AGC



The array-antenna technology



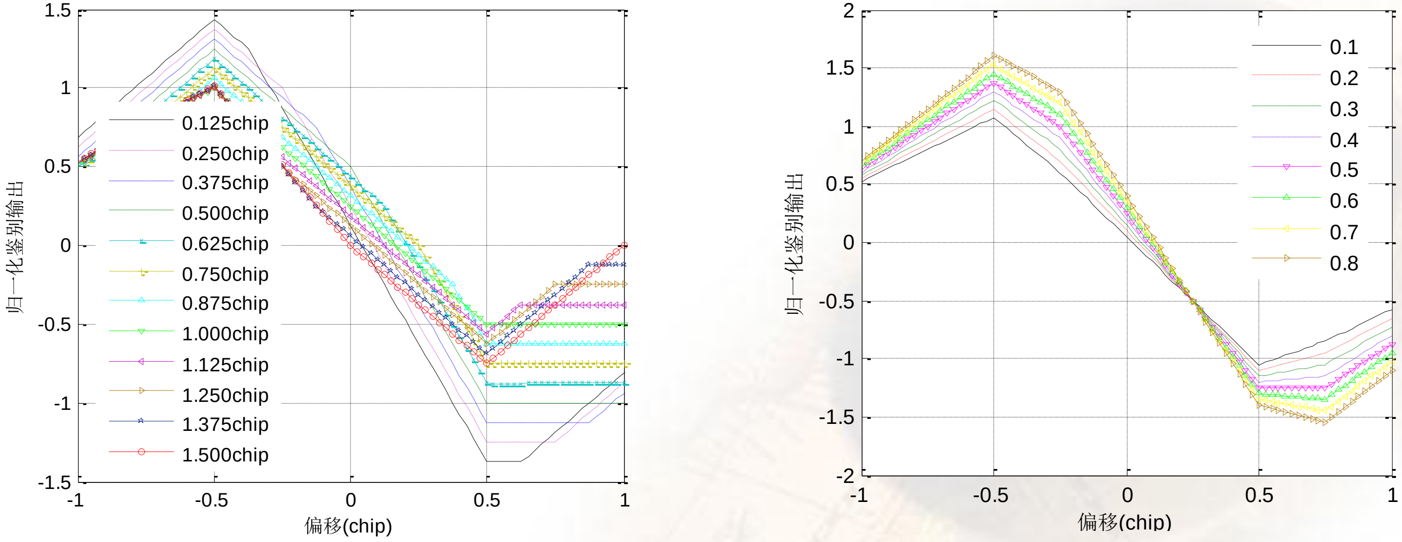
adaptive spatial domain filter



adaptive time domain filter

Multipath Simulation

The phase error code and carrier phase error were caused by the multipath signal, and the spectrum diagram of the single frequency interference signal produced by the GPS L1 jamming device .



The normalized discriminator output in different code delay

GNSS Signal-In-Space Quality Monitoring

- 4-Constellation CORS
  - Civil applications
  - Scientific research
  - Raw binary data
  - Differential correction messages

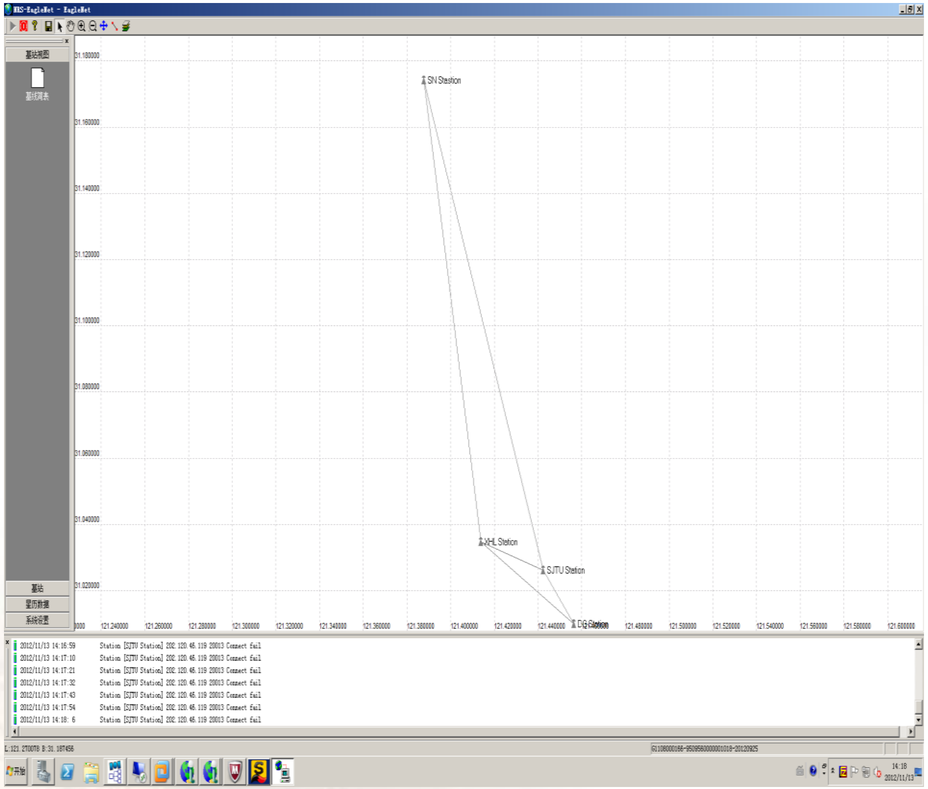
GNSS Signal-In-Space Quality Monitoring

Receivers	GNSS signal
Leica GRX1200+	GPS/GLONASS
Unicore UR240	GPS/BeiDou
Sinan Receiver	GPS/BeiDou
FLEXPAK-6 (NovAtel)	GPS/Galileo /GLONASS

Antennas	signal
Leica	GPS/ Glonass
NovAtel	GPS/BD

GNSS Signal-In-Space Quality Monitoring

- BeiDou/GPS reference station network
  - Containing 4 stations:
    - SJTU Station
    - SN Station
    - DG Station
    - XHL Station
  - NRS-EagleNet software
    - Processing data
    - Monitoring errors
    - Managing users
    - Achieving RTK calculation.



```
2012/11/13 14:16:59        Station [SJTU Station] 202.120.46.119 20013 Connect fail
2012/11/13 14:17:10        Station [SJTU Station] 202.120.46.119 20013 Connect fail
2012/11/13 14:17:21        Station [SJTU Station] 202.120.46.119 20013 Connect fail
2012/11/13 14:17:32        Station [SJTU Station] 202.120.46.119 20013 Connect fail
2012/11/13 14:17:43        Station [SJTU Station] 202.120.46.119 20013 Connect fail
2012/11/13 14:17:54        Station [SJTU Station] 202.120.46.119 20013 Connect fail
2012/11/13 14:18: 6        Station [SJTU Station] 202.120.46.119 20013 Connect fail
```

L:121.270078 B:31.187456

G1108000166-950956000001018-20120925

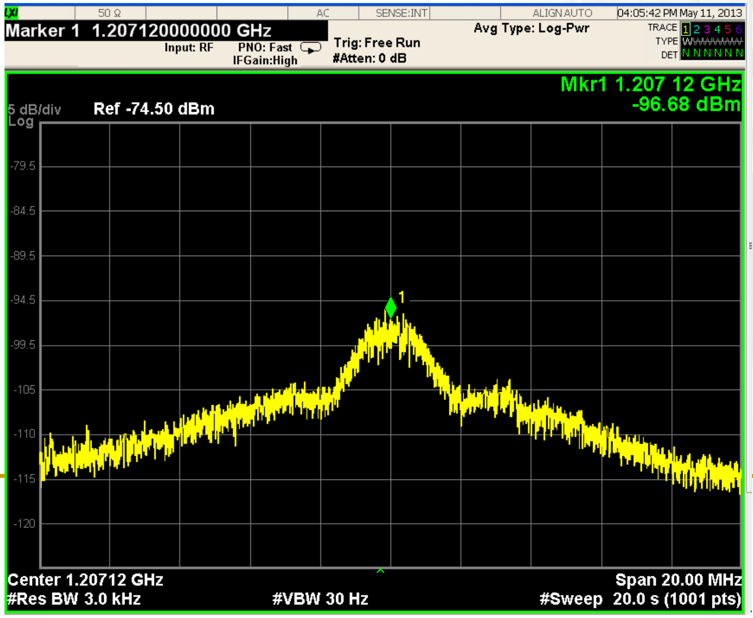
HMI of NRS-EagleNet

GVTR and Vulnerability Monitoring

- GVTR (will) provides a complete set of theories and research platform
- GVTR can be used to predict and evaluate Vulnerability issues and influences
- GVTR can be used as a full functional Vulnerability monitoring station
- Subsets of GVTR can be deployed in many areas

Deployment of GNSS Vulnerability Monitoring

- Central Station
  - Diameter: 3.2m
  - Gain: 31dB@L band(1.1~1.7GHz)
  - Directivity: 5.5deg (3dB Width) @1.2
  - NT: <120k



50 Ω | AC | SENSE:INT | ALIGN AUTO | 04:05:42 PM May 11, 2013

Marker 1 1.207120000000 GHz

Input: RF PNO: Fast IFGain:High

Trig: Free Run #Atten: 0 dB

Avg Type: Log-Pwr

TRACE 1 2 3 4 5 6
TYPE WWWWWW
DET N N N N N N

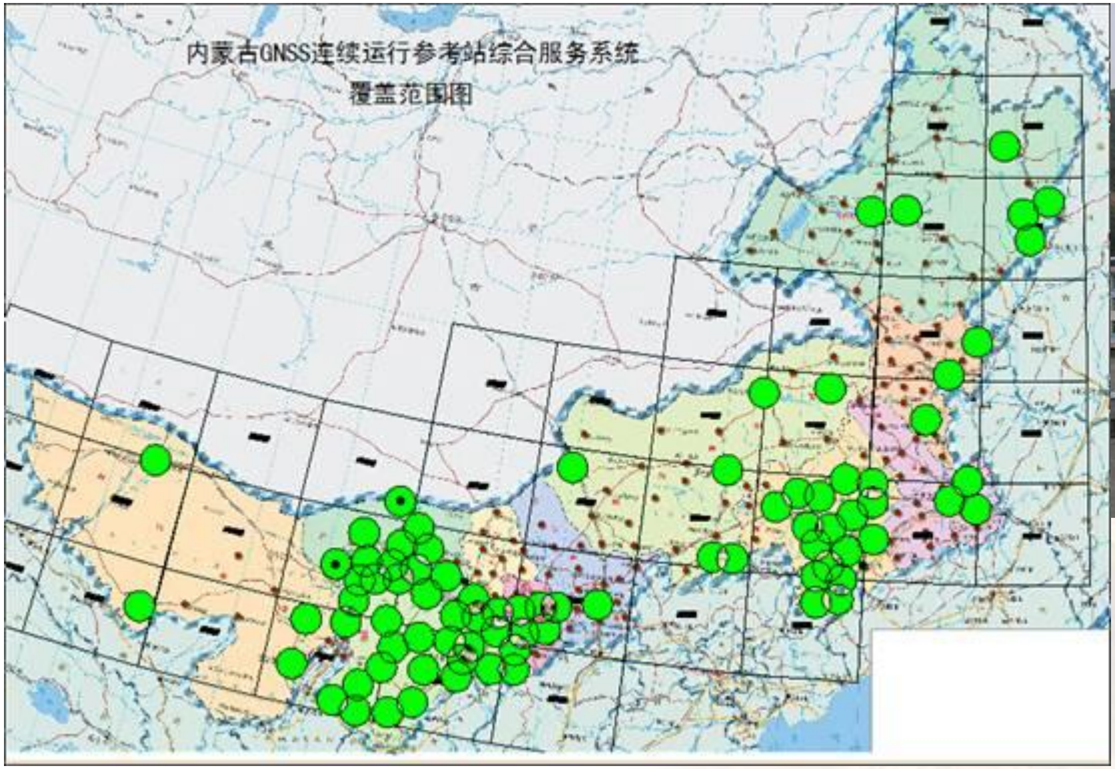
Mkr1 1.207 12 GHz
-96.68 dBm

5 dB/div Log Ref -74.50 dBm

Center 1.20712 GHz Span 20.00 MHz
#Res BW 3.0 kHz #VBW 30 Hz #Sweep 20.0 s (1001 pts)

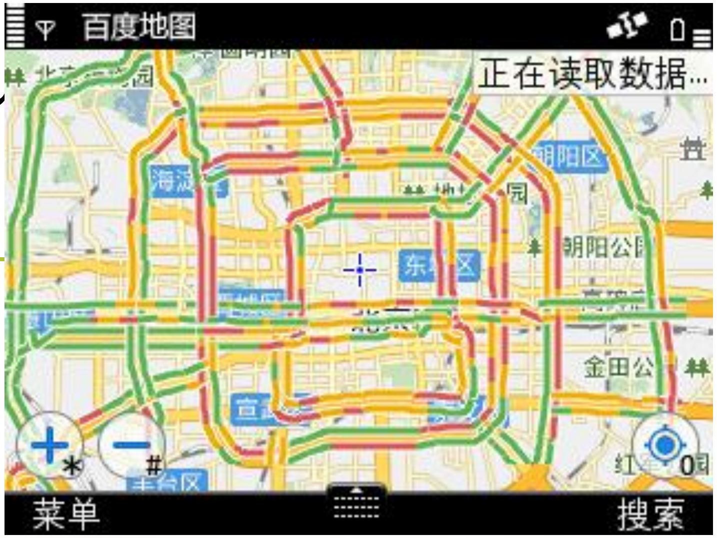
Deployment of GNSS Vulnerability Monitoring

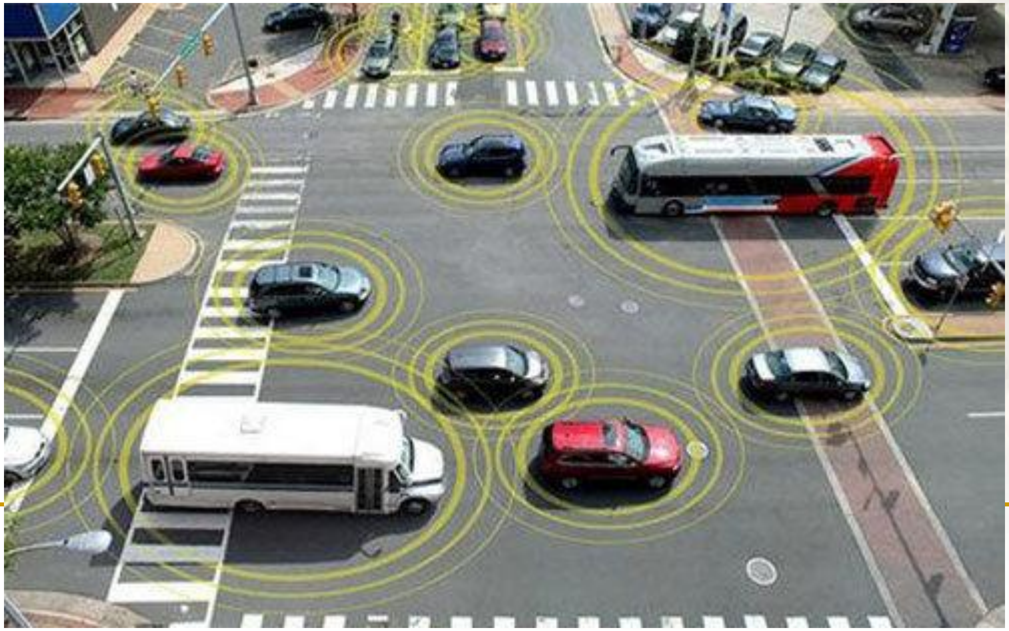
- Based on current & future CORS network

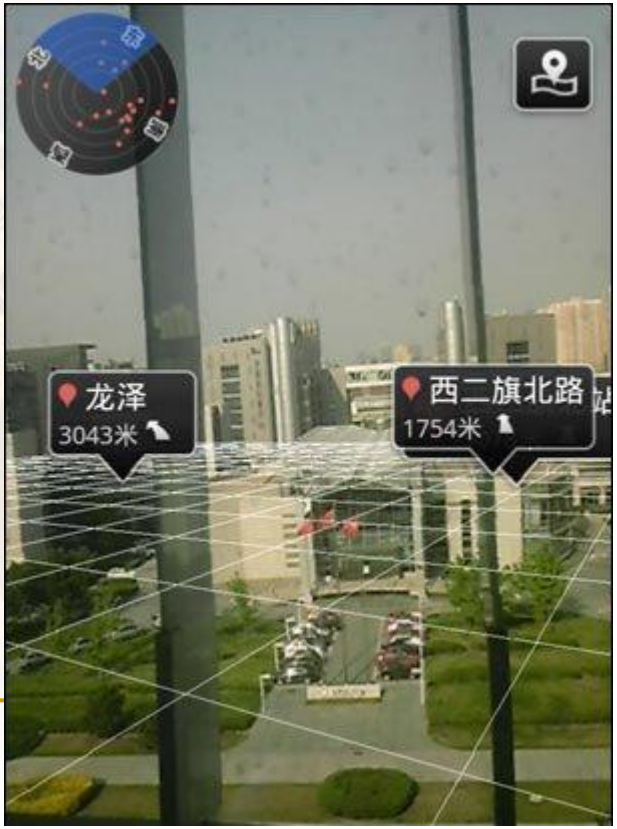


Deployment of GNSS Vu Monitoring

- Crowd sourcing monitoring
  - Smart phones
  - Vehicles: local differential data
  - Base Stations







Thanks for your attention!