上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

Vulnerability
new tool and measure for GNSS

Hongliang Xu (xhl@sjtu.edu.cn)
Shanghai Jiao Tong University, China

航空航天学院 导航、制导与控制
Guidance, Navigation and Control
School of Aeronautics and Astronautics

Outline

- Situations of current GNSS
- Vulnerability study
- Research roadmap of SJTU
- Conclusion

PNT: critical infrastructure

- PNT has become a critical infrastructure; virtually the indispensable one the others (power, telecommunication, etc.) rely on.
- Space-based PNT (GNSS) is the primary PNT source; no alternatives available to provide competing performance.

GNSS Threats and Consequences

- Space
  - S.V. failure
- Environment
  - Solar activity
  - Ionosphere scintillation and disturbance
- Spectrum
  - Unintentional RF Interference
  - Intentional Jamming
  - Spoofing
- Local
  - Restricted Line-of-sight
  - Multipath

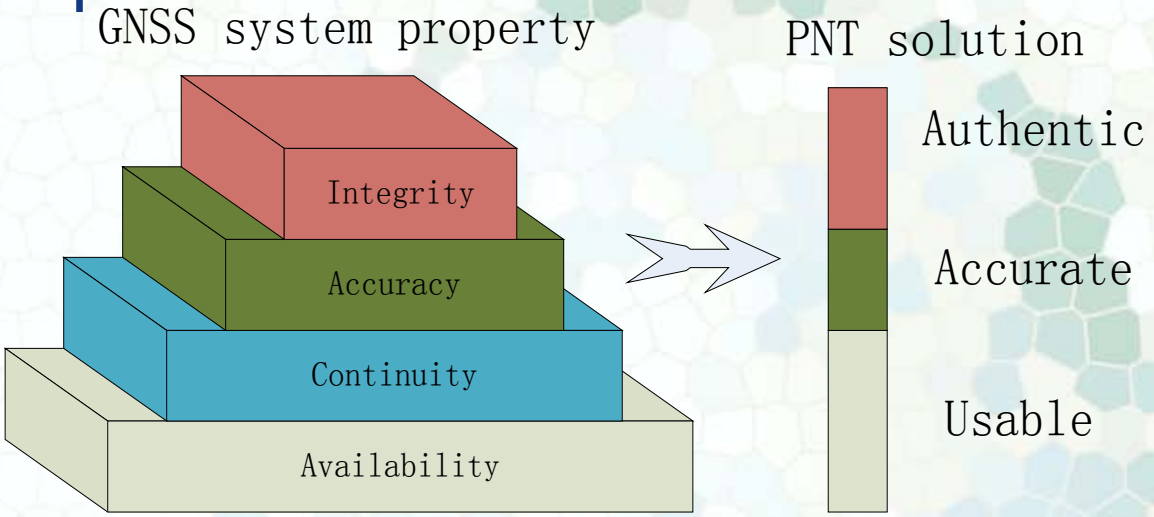
GNSS Threats and Consequences

- Space
  - S.V. failure
- Environment
  - Solar activity
  - Ionosphere scintillation and disturbance
- Spectrum
  - Unintentional RF Interference
  - Intentional Jamming
  - Spoofing
- Local
  - Restricted Line-of-sight
  - Multipath

- Degradation of accuracy
- Required performance not met
- PNT service unavailable
- Hazardous misleading information (HMI)

Current situation

- Current GNSS performance standards
  - Accuracy
  - Integrity
  - Continuity
  - Availability

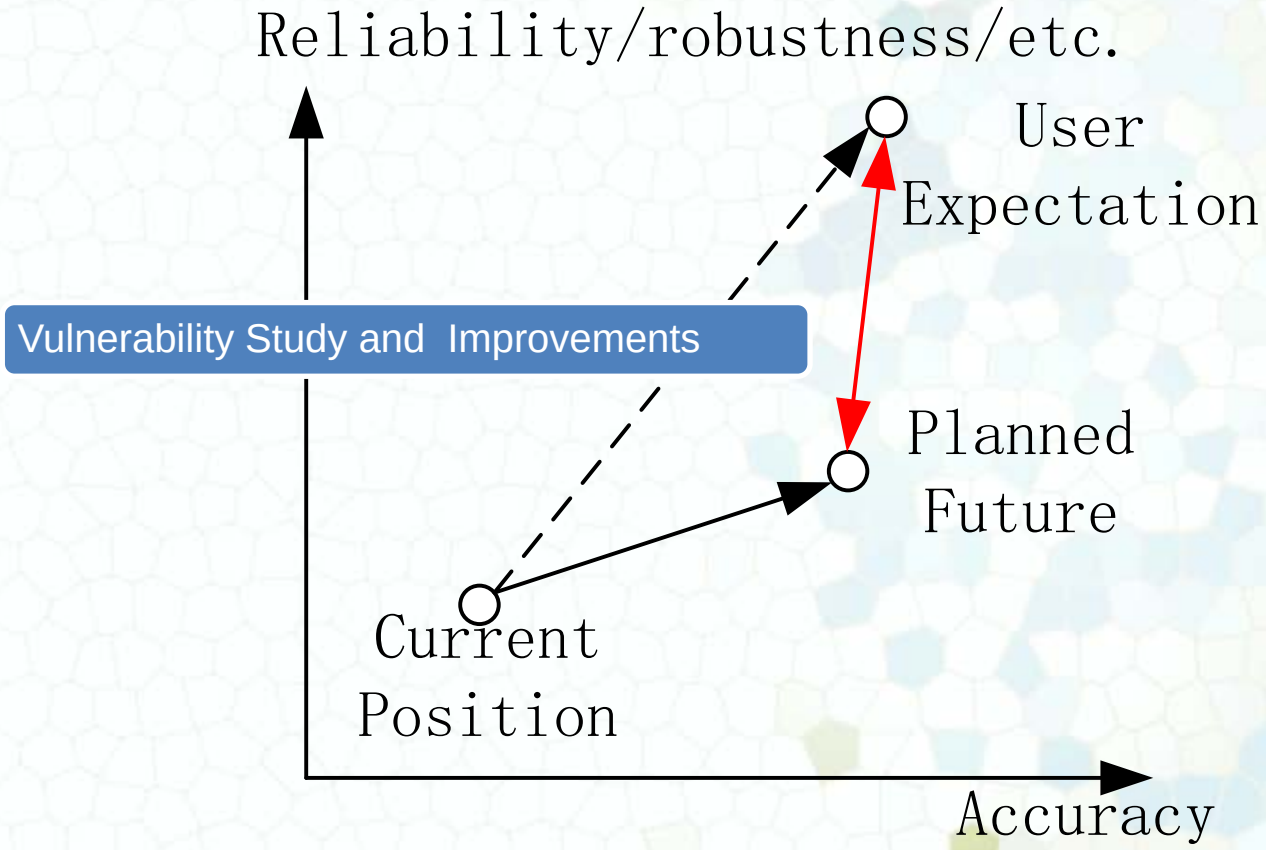


- Performance is evaluated merely by PNT solution.
- Intricate information is simplified and partly discarded.
- Interferences and disturbances are not counted.

Current situation

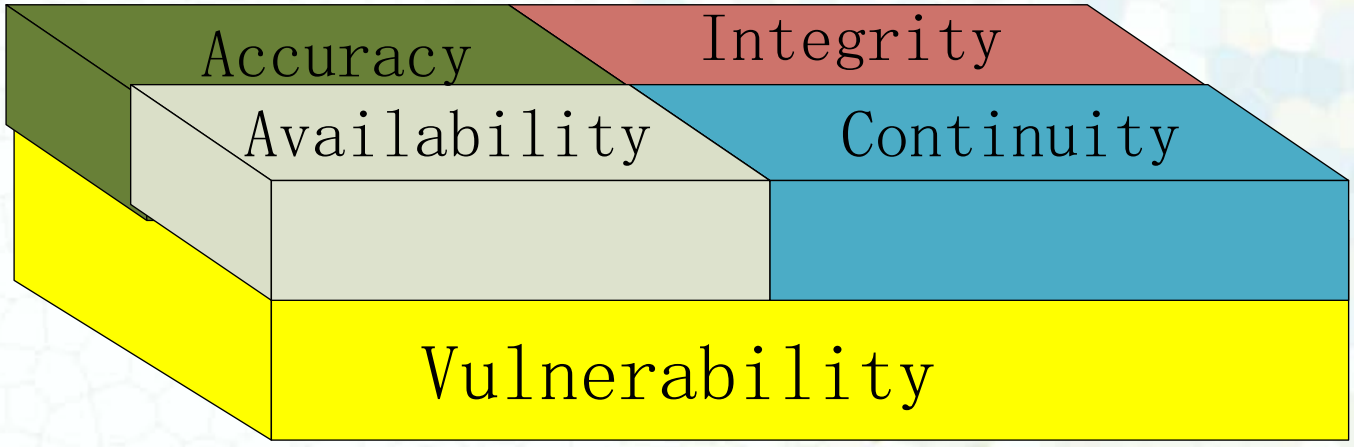
- GNSS provider side
  - System health: inadequate attention
  - Threats and risks: not well covered
  - Performance: not guaranteed (especially for civil/public service)
- User side
  - Increasing concerns
  - No effective and generalized countermeasures
  - GNSS dependency is discouraged
  - Non-GNSS backups chosen (which is of low performance yet high cost)

User Expectations not met



Vulnerability: definition

- **The degree that GNSS users maintain minimum performance requirement and improve service quality under adverse circumstances.**
- Origins: unexpected or excessive interferences and anomalies
- Native property of GNSS (virtually of any other complex systems)
- Another performance criterion (orthogonal with current ones)



Multi-dimensional insight

Vulnerability Study

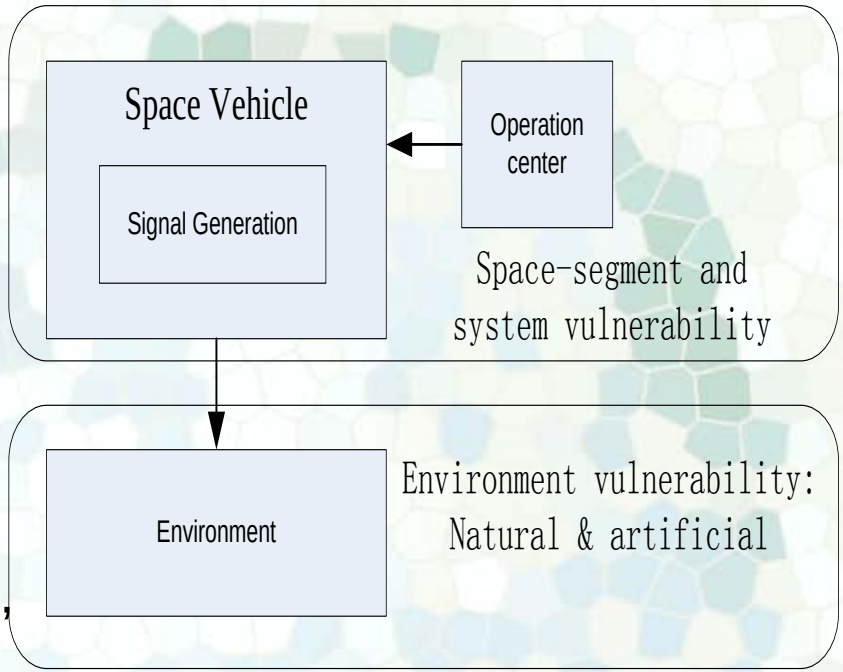
- The research and improvements on the vulnerability issue
- Objectives
  - Research GNSS vulnerability theories
  - Determine application vulnerability tolerance
  - Introduce more robust , reliable and accurate GNSS
  - Enable authentic (trusted) PNT service.
    - SBAS is included as part of space-based PNT.
  - Provide performance-guaranteed service to general civil applications.

Actions and goals

Party	Actions	Gains	Target
User	Interference study	Detection and alleviation techniques	Achieving more trustworthy and robust PNT solution out of GNSS.
	Vulnerability monitoring	Monitoring and information distribution service	
Provider	Re-evaluate	System vulnerability assessment	Providing more reliable GNSS service.
	Improve	Vulnerability improvement measures	

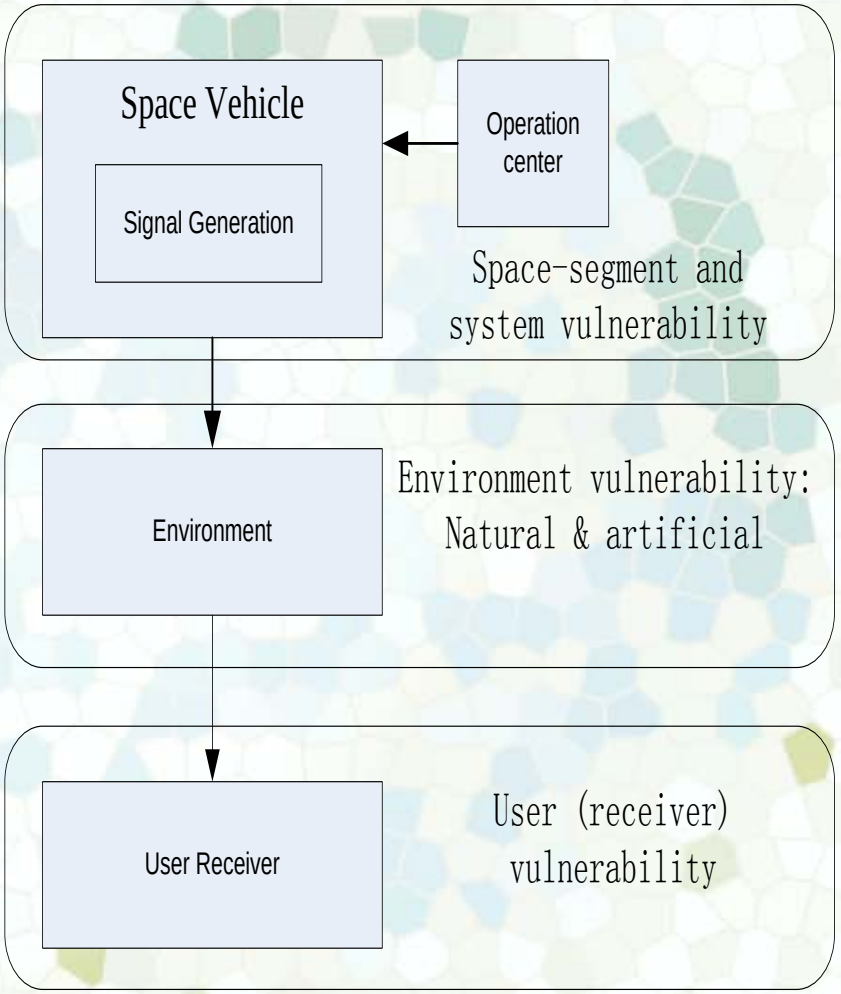
Connotations 1: System Study

- Content
  - Possible disturbing source and influencing mechanism
- Outputs
  - Assessment result
  - Immunity to vulnerability
    - New band, code, modulation, etc.
    - Multi-constellation, Multi-band operation
    - Fail-safe backups



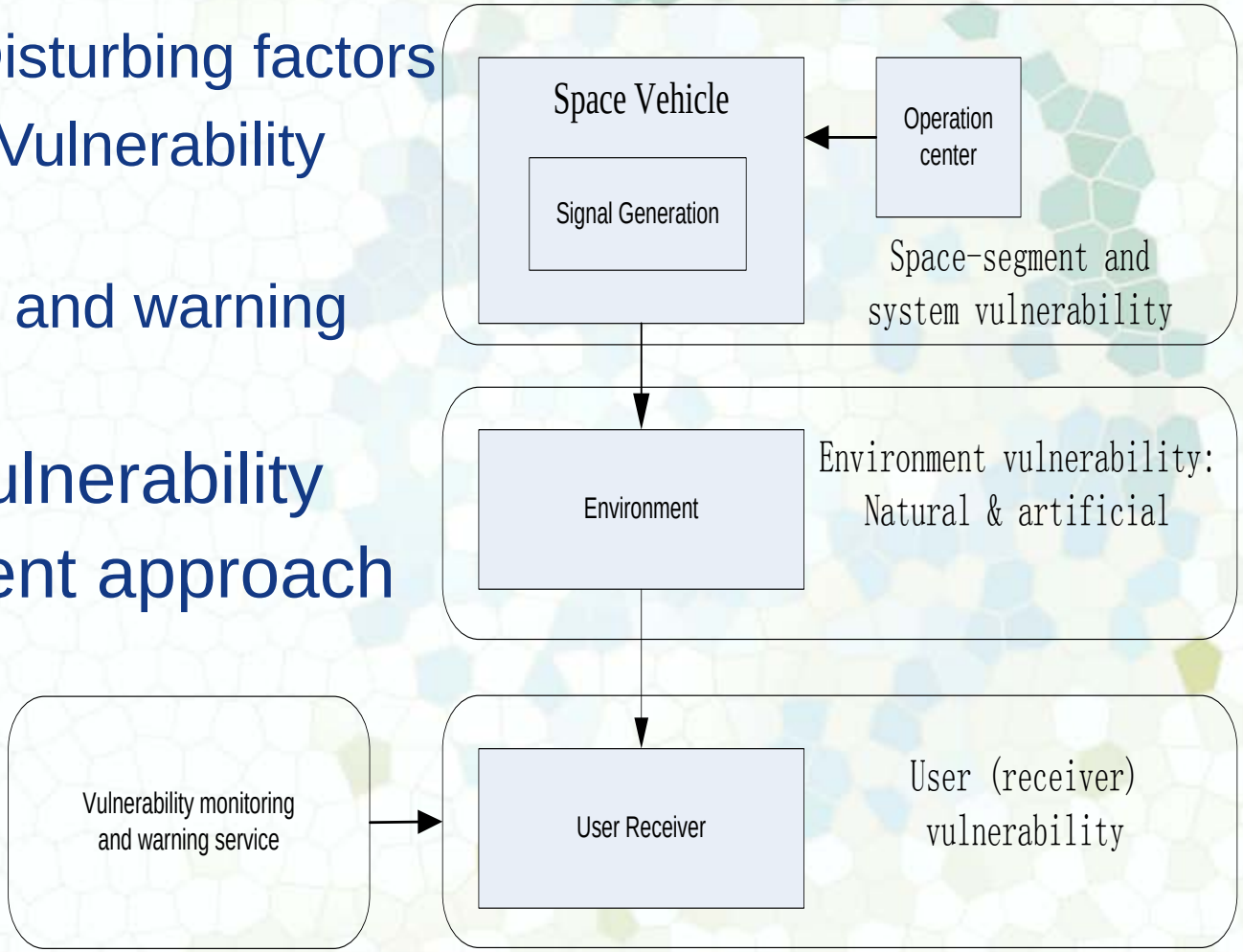
Connotations 2: User awareness

- Application-specific vulnerability tolerance
- IDM on receiver side
  - Combination of all possible approaches
  - A composite of existing and new methods.



Connotations 3: Monitoring Station and Service

- Responsibilities
  - Monitor: Disturbing factors
  - Evaluate: Vulnerability status
  - Broadcast and warning service
- Ultimate vulnerability improvement approach



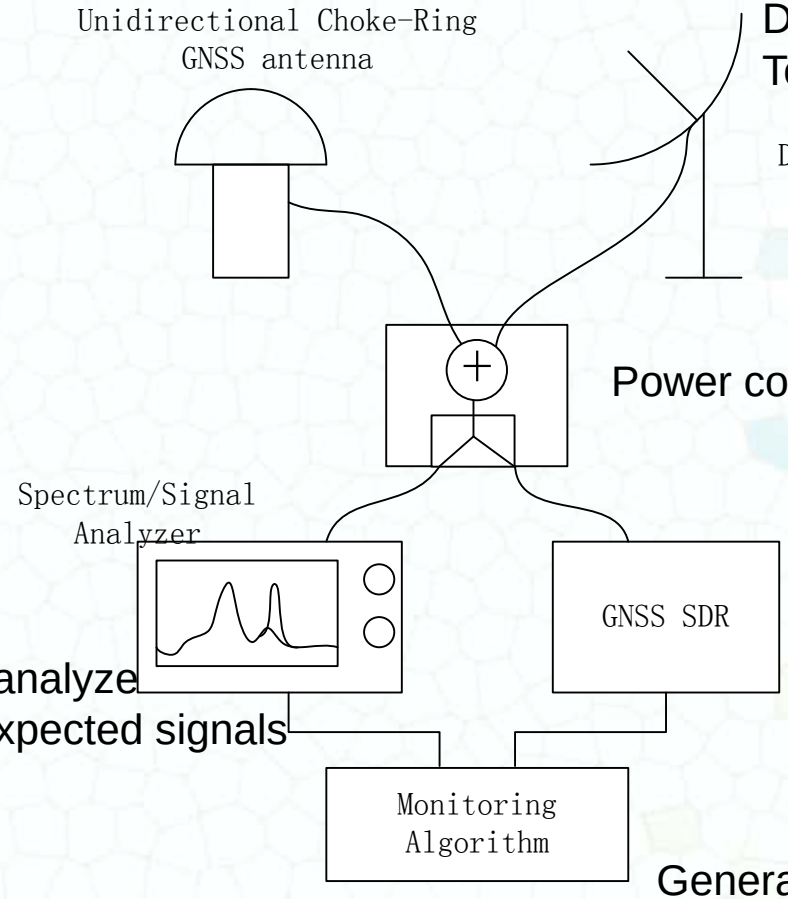
Monitoring Station: Principles

- Functions
  - Evaluate SIS
  - Detect anomalies
  - Diagnosis and identify disturbances
  - Reconstruct and locate sources
  - Generate corrections/solutions
  - Broadcast and warn users of situation

Ensure quality of PNT service

- Characteristics
  - Including both electrical instruments and GNSS receivers
  - Locally coverage
  - Grid located to form seamless coverage with variable radius and flexible density depending on requirement

Monitoring Station: Architecture (Preliminary)



Dish antenna: high gain, narrow beam
To search for and track interferences and anomalies

Power combiner and multiplexer

SA: analyze unexpected signals

Generate and distribute monitoring results

Monitoring Station: Comparison

	Ground Monitoring Station	Continuous Operating Reference Station (CORS)	Vulnerability Monitoring Station
Application	S.V. monitoring and control	Reference/differential data	Interference identification and tracking
Purpose	Maintenance	Precision	Quality
Mode of function	N/A	Passive	Active
Owner	Provider	User	Third-party
Role	Infrastructure (Ground Segment)	Augmentation Facility	Local component

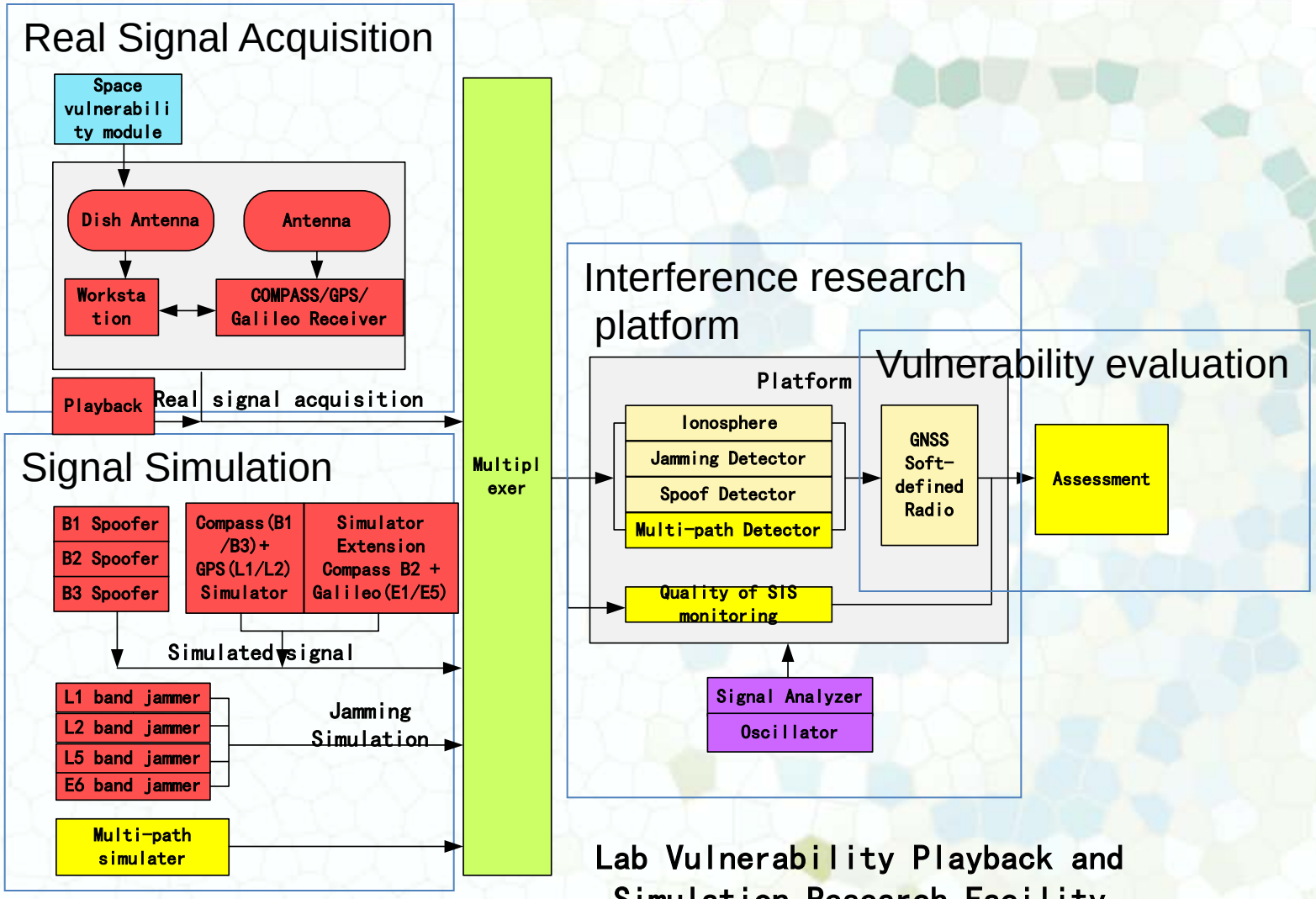
Research Roadmap (SJTU)

1. Lab Vulnerability Playback and Simulation Research Facility (by 2012)
2. Demonstration station (by 2013)
   - Research oriented
3. Provincial deployment and validation
   - several stations to cover Shanghai and adjacent provinces.

Lab Facility (ongoing)

- Functions
  - Playback and simulate GNSS threatened scenarios
  - Evaluate receiver(h/w and s/w) performance
- Purpose
  - Research the impaired performance and solutions

Lab Facility



Lab Vulnerability Playback and Simulation Research Facility

International Cooperation

- International focus and study welcomed
- Mutually agreed understandings
- Joint-built monitoring stations featuring multi-constellation capability favored
- Work for common benefits

Conclusions

- A new measure of service performance
- A new approach for performance enhancement
- For users' benefits
- Valuable vulnerability alleviating methods expected from relevant research
- International cooperated research welcomed

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

谢 谢！

Thanks for your attention!