Detection Techniques of GNSS Spoofing and Ionospheric Scintillation

Ruimin Jin *China Research Institute of Radiowave Propagation(CRIRP)*
Weimin Zhen *China Research Institute of Radiowave Propagation(CRIRP)*

Outline

1 、 Introduction

2、GNSS Spoofing Detection Techniques

（1） The effect analysis of GNSS spoofing

（2） Spoofing detection techniques

3、Ionospheric Scintillation Detection Techniques

（1） The effect analysis of Ionospheric Scintillation

（2） Ionospheric Scintillation detection techniques

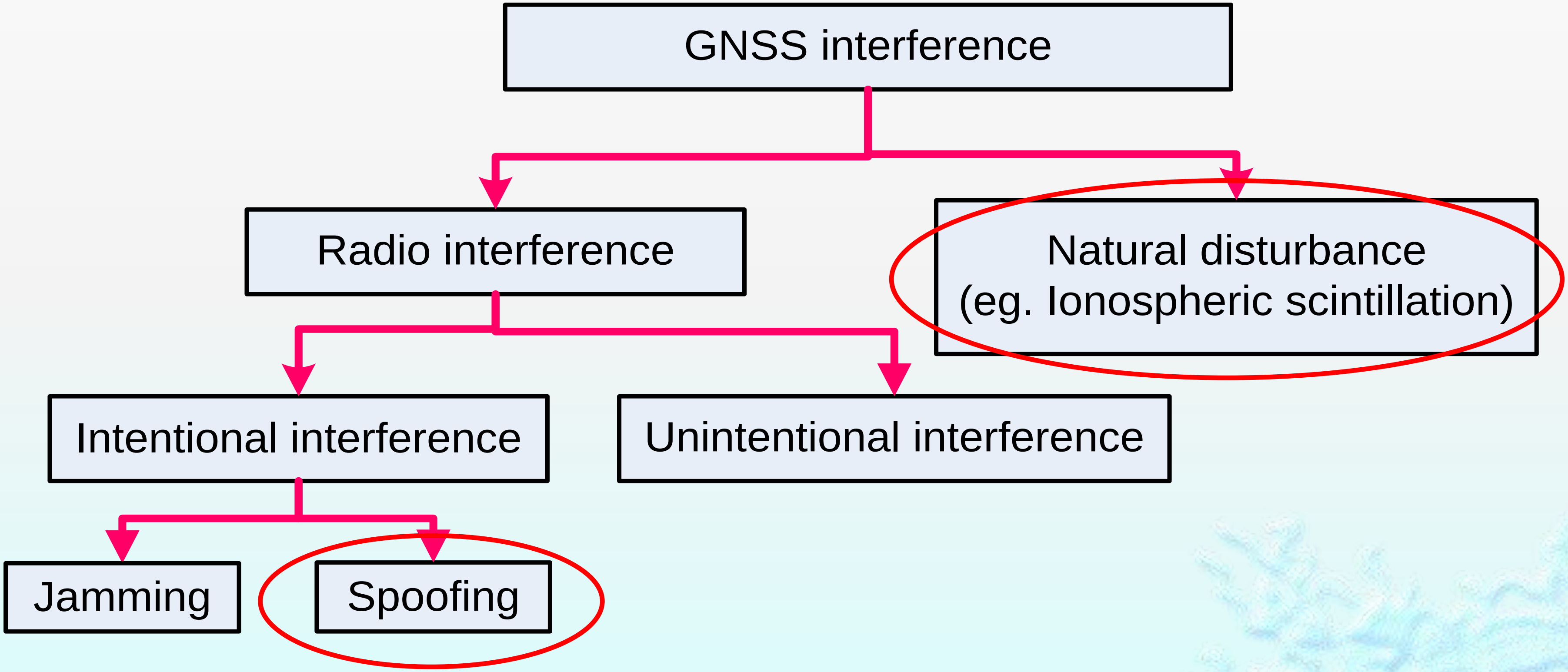
4、Summary

1、Introduction

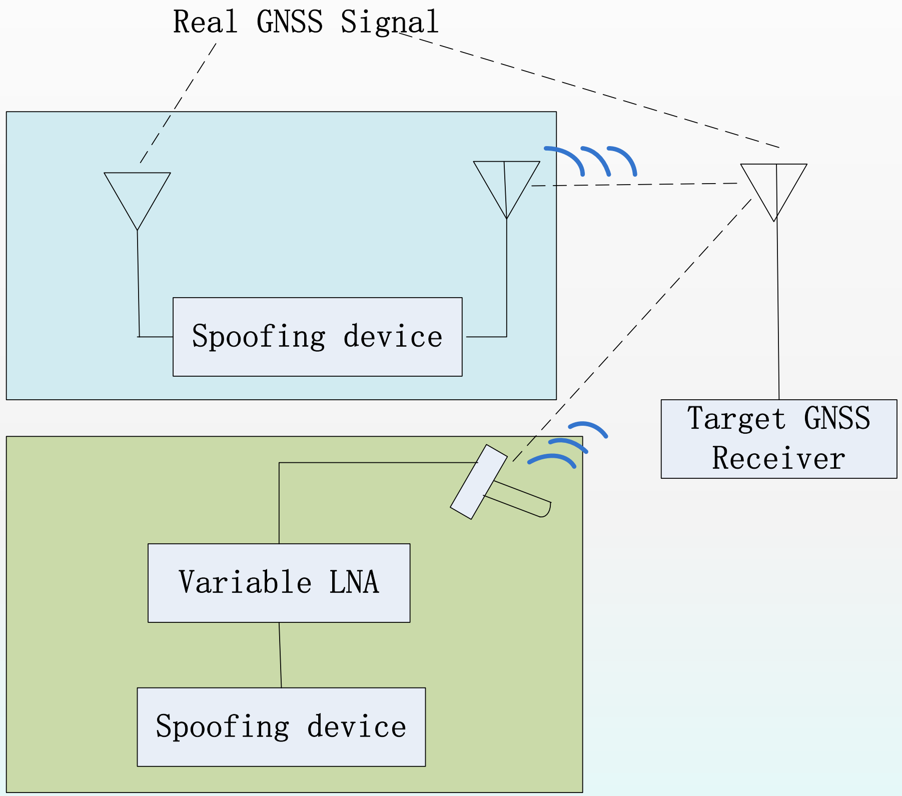
GNSS has become a global Utility

- **GNSS Improves Economic Productivity**
  - Precision Location(aviation, agriculture, transportation, etc.)
  - Precision Timing(telecommunications， banking, power grids, etc.)
- **The world’s citizens rely on GNSS**

But space-based GNSS signals are weak, especially once they reach ground-based receivers. This inherent weakness makes the GNSS signal susceptible to various forms of interference .



2、GNSS Spoofing Detection Techniques



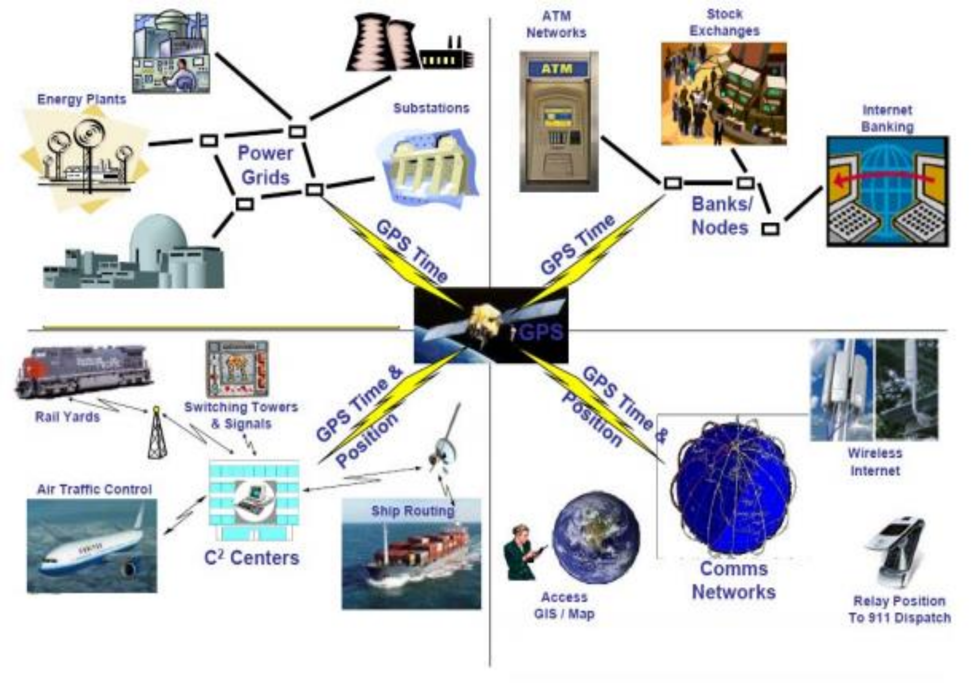
Spoofing refers to the transmission of fraudulent GNSS-like signals that force the victim receiver to accept a manipulated version of GNSS timing or positioning data.

Spoofing scenarios were typically judged to be of higher consequence than jamming scenarios due to the potential duration of time before users or devices detect spoofing. The target receiver will be not aware of the threat and still provide position/navigation solutions which seem to be reliable.

（1）The effect analysis of GNSS spoofing interference

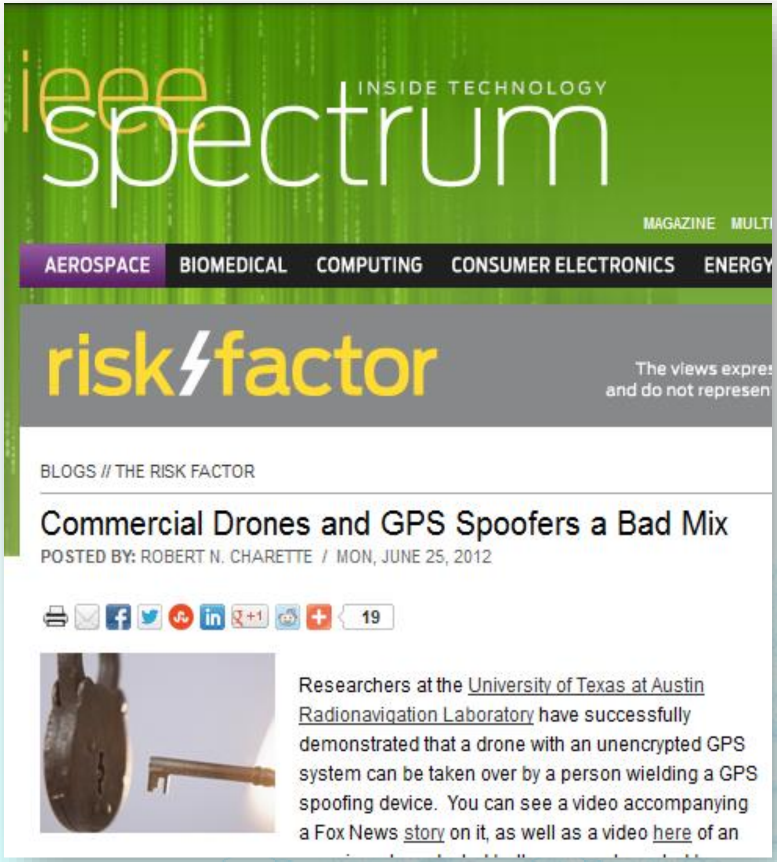
In 2001, the report released by U.S. Department of transportation pointed out that GNSS is susceptible to spoofing attacks.

GNSS spoofing may cause some systems of telecom, power, financial and traffic industry in failure, posing a great threat to national economy and social security.



<u>Spoofing attacks are a major threat for future GNSS applications.</u>

In June 2013, university of Texas students did a experiment that successfully altered the course of yacht by gradually overpowering the signal strength of the actual GPS constellation with their spoofed data.



ieee spectrum INSIDE TECHNOLOGY

MAGAZINE MULTI

AEROSPACE BIOMEDICAL COMPUTING CONSUMER ELECTRONICS ENERGY

risk factor

The views expres
and do not represen

BLOGS // THE RISK FACTOR

Commercial Drones and GPS Spoofers a Bad Mix

POSTED BY: ROBERT N. CHARETTE / MON, JUNE 25, 2012

19

Researchers at the University of Texas at Austin Radionavigation Laboratory have successfully demonstrated that a drone with an unencrypted GPS system can be taken over by a person wielding a GPS spoofing device. You can see a video accompanying a Fox News story on it, as well as a video here of an

（1） Telecommunication Industry

mode		Frequency accuracy	Time synchronization requirement
GSM（2G）		±50ppb	N.A
WCDMA（3G）		±50ppb	N.A
TD-SCDMA（3G）		±50ppb	≤±3*us*
CDMA2000(3G)		±50ppb	≤±3*us*
(4G)	TD-LTE	±50ppb	≤±3*us*
	LTE-FDD	±50ppb	4*us*

- **Telecommunication networks are critically dependent on GNSS-derived timing.**
- **Using "GNSS-disciplined oscillator (GNSS DO) " timing mode.**

1、If GNSS timing receiver can not output time information or the output error exceeds a certain threshold, the base station will switch to reference oscillator. In a short time, there nearly no threat. But oscillator will drift, the timing accuracy will not meet the base station timing requirements more than a certain time, causing the communication network blocked or even paralyzed.

2、If the output error of GNSS timing receiver does not exceed the error threshold, the base station will still use GNSS for time synchronization. In this case, the spoofing will cause telecommunication network in confusion or even paralyzed.

(2) Electrical Industry

System	Accuracy
Line travelling wave fault	1us
Lightning location system	1us
Power angle measuring system	40us
Fault recorder	1ms
Sequence of events recorder	1ms
Microcomputer protection device	10ms
Power telecontrol device	1ms
Dispatching automation system	1ms
Substation monitoring system	1ms
Automatic recording instrument	10ms
Load monitoring system	≤0.5s

- GNSS is mainly used for power network time synchronization in line traveling wave fault location, lightning location , synchronous phasor measurement unit systems. The accuracy requirements of time synchronization is up to 1μs in some of the systems.
- Using "GNSS-disciplined oscillator (GNSS DO) " timing mode.
- Detecting whether the GNSS timing exceeds the set time threshold to determine an exception.
- When the GNSS time error caused by spoofing is within the threshold, the wrong time information will be used to synchronize the power network, which may cause the power network to be disordered。

(3) Financial Industry

- Bank business time, financial transactions, the UnionPay card account password recognition with timestamp information, computer network systems all need precise time synchronization.
- The accuracy requirement of time synchronization is not high, but the reliability is very high. High precision time synchronization equipment does not allow system failure, so a lot of redundant backups are designed. Therefore, GNSS spoofing generally does not pose a deadly threat to the financial sector.

(4) Transportation Industry

- GNSS applications in the transportation industry are dominated by navigation;
- Traffic GNSS navigation terminal generally use multi-system, multi-band mode of operation for navigation, basically do not consider any anti-spoofing protection measures.
- GNSS receiver may easily lock to the spoofing signal . The output of the wrong location information, will result in misleading or even cause major accidents.

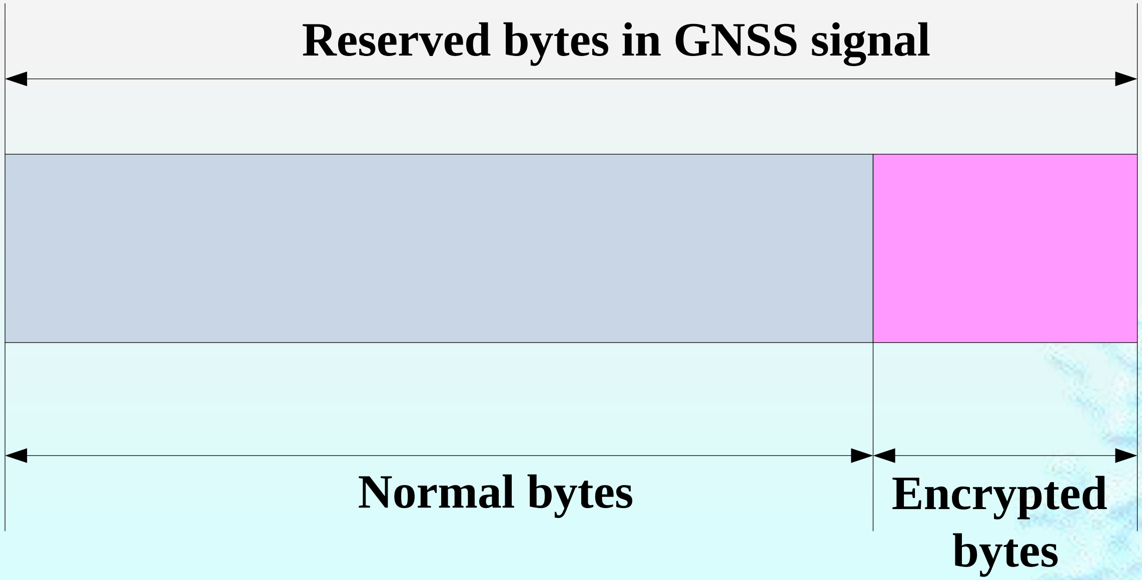
（2） GNSS detection techniques

Spoofing detection techniques

- Signal encryption
- Residual signal detection
- Signal propagation delay detection
- Angle of arrival detection
- Angle difference of arrival detection

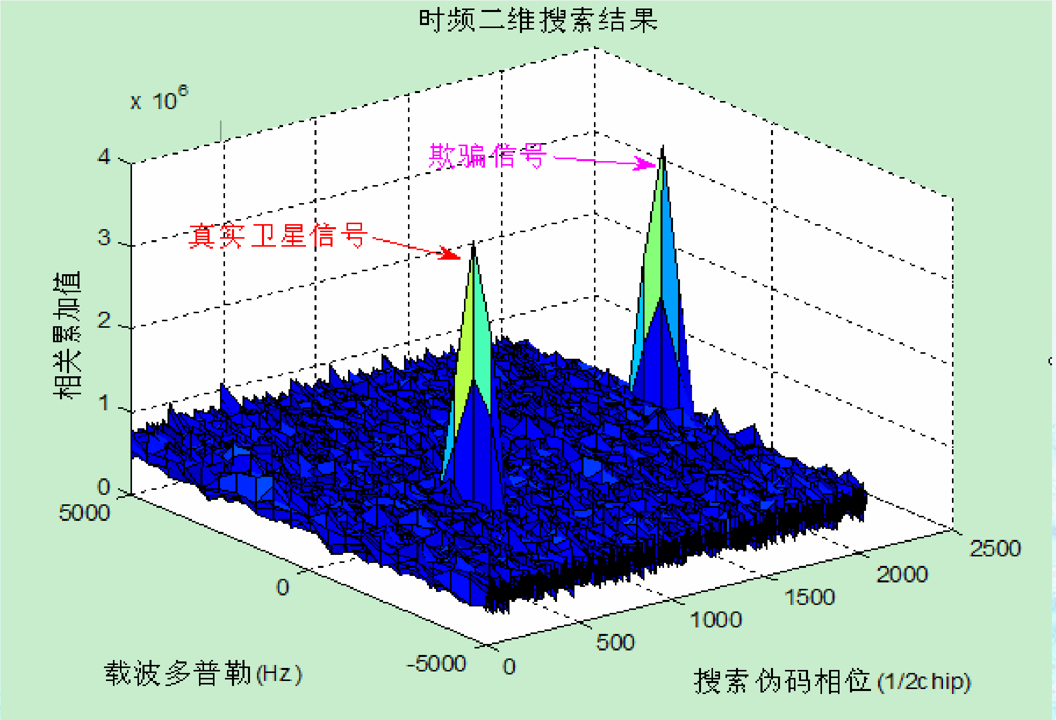
a） Signal encryption

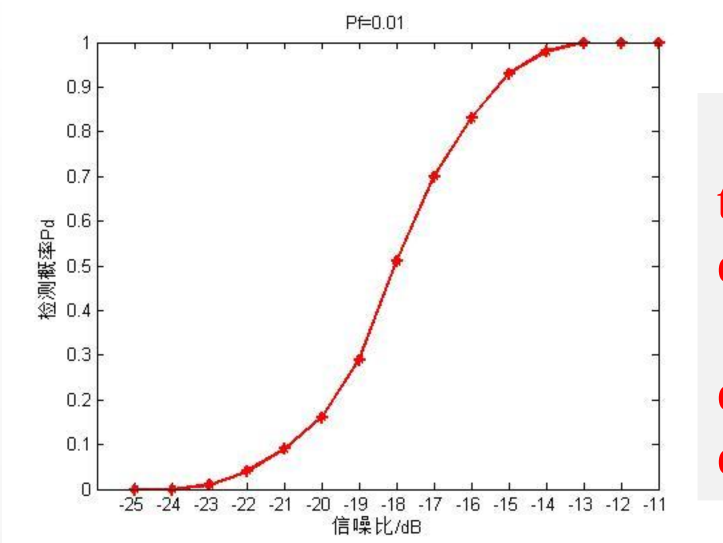
Some bytes are reserved in the designing of GNSS signal and encrypted information can be added into these bytes, after demodulation, spoofing signals will be discriminated from the true signals.



b）Residual signal detection

The prerequisite of residual signal detection is that spoofing signal can not actively restrain the true signal. So both spoofing signal and true signal can be detected from the received signal of receivers.





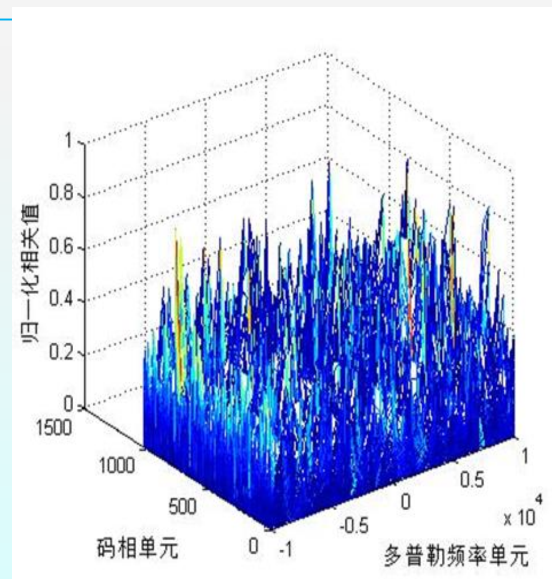
Simulating 1000 times for each SNR to test the probability of the residual signal detection method .

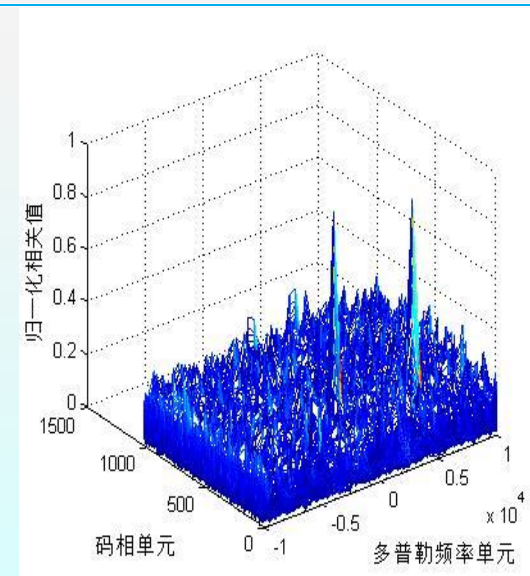
When the SNR is less than -20dB, the detection probability of residual signal detection method is low.

We come up a method that using the navigation bit flip to improve the performance of the residual signals detection method.

	5ms	5ms	5ms	5ms
第1组	数据块1	数据块2	数据块3	数据块4
第2组	数据块1	数据块2	数据块3	数据块4
第3组	数据块1	数据块2	数据块3	数据块4
第4组	数据块1	数据块2	数据块3	数据块4

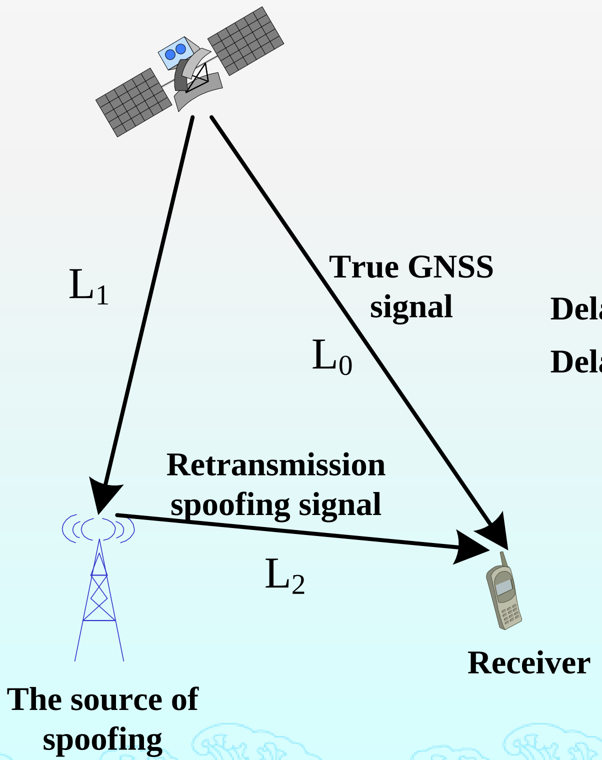
$$\begin{cases} R_1 = \sum_{k=1}^{4} abs\left\{IFFT[FFT(\sum_{i=1}^{5} y_i^1(m)) \times FFT^*(C_k(m))]\right\} \\ R_2 = \sum_{k=1}^{4} abs\left\{IFFT[FFT(\sum_{i=1}^{5} y_i^2(m)) \times FFT^*(C_k(m))]\right\} \\ R_3 = \sum_{k=1}^{4} abs\left\{IFFT[FFT(\sum_{i=1}^{5} y_i^3(m)) \times FFT^*(C_k(m))]\right\} \\ R_4 = \sum_{k=1}^{4} abs\left\{IFFT[FFT(\sum_{i=1}^{5} y_i^4(m)) \times FFT^*(C_k(m))]\right\} \end{cases}$$





c）Signal propagation delay detection

Since the path of true GNSS signal is significantly different from retransmission spoofing signal, propagation delay can be used to identify these two kinds of signals.



Delay of true signal： $t_1 = L_0/c$

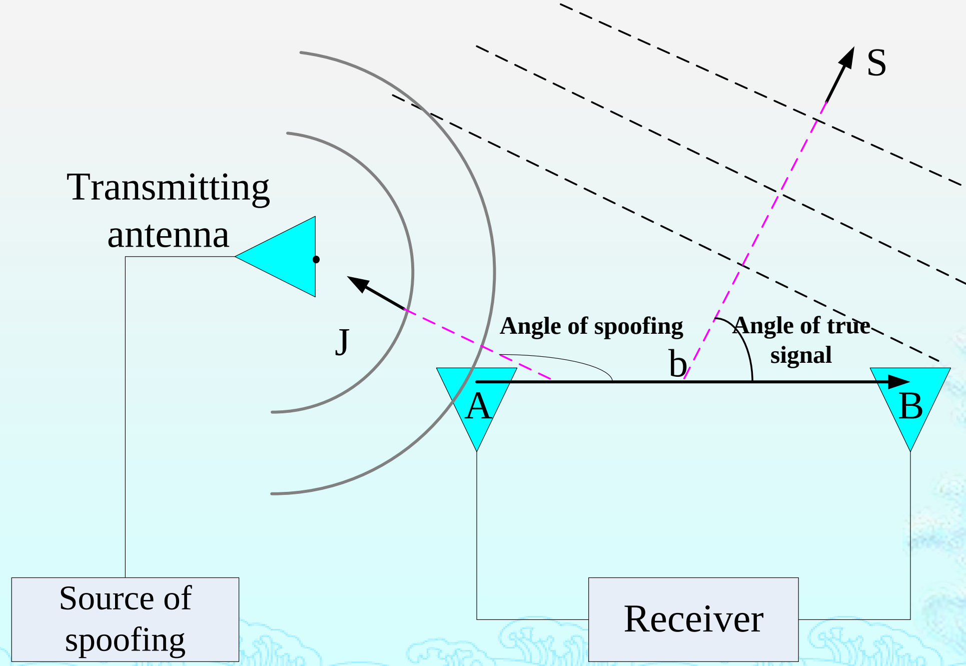
Delay of spoofing： $t_2 = (L_1 + L_2)/c$

d） Angle of arrival detection

Most of the spoofing source use single transmitting antenna, so that

- The angles of received spoofing signal are most the same;
- The true signals from different satellites vary significantly.

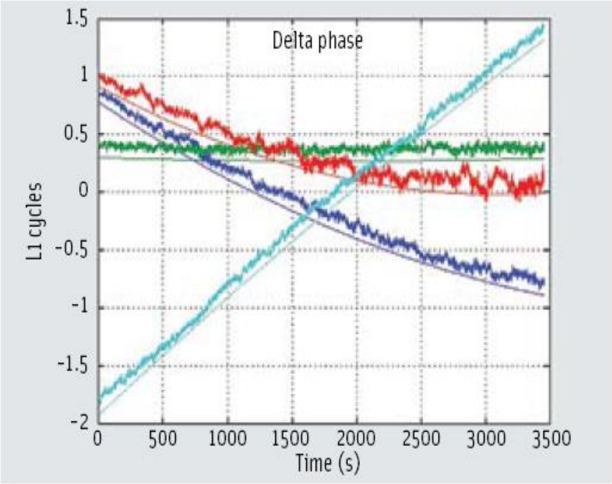
Array of antennae is an effective method for angle of arrival detection to identify spoofing signal from true signal.



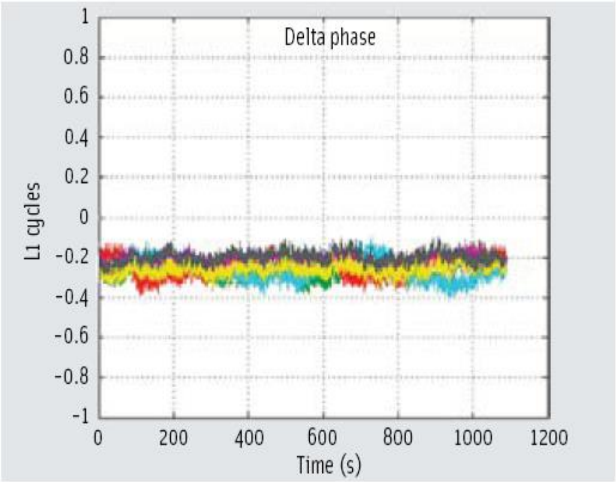
e） Angle difference of arrival detection

If relative motion exists between transmitter and receiver, the angle difference of received signals will vary significantly with time.

Spoofing detection can be implemented by the angle difference monitoring of a dynamic receiver.



True signal



Spoofing signal

Comparison of spoofing detection techniques

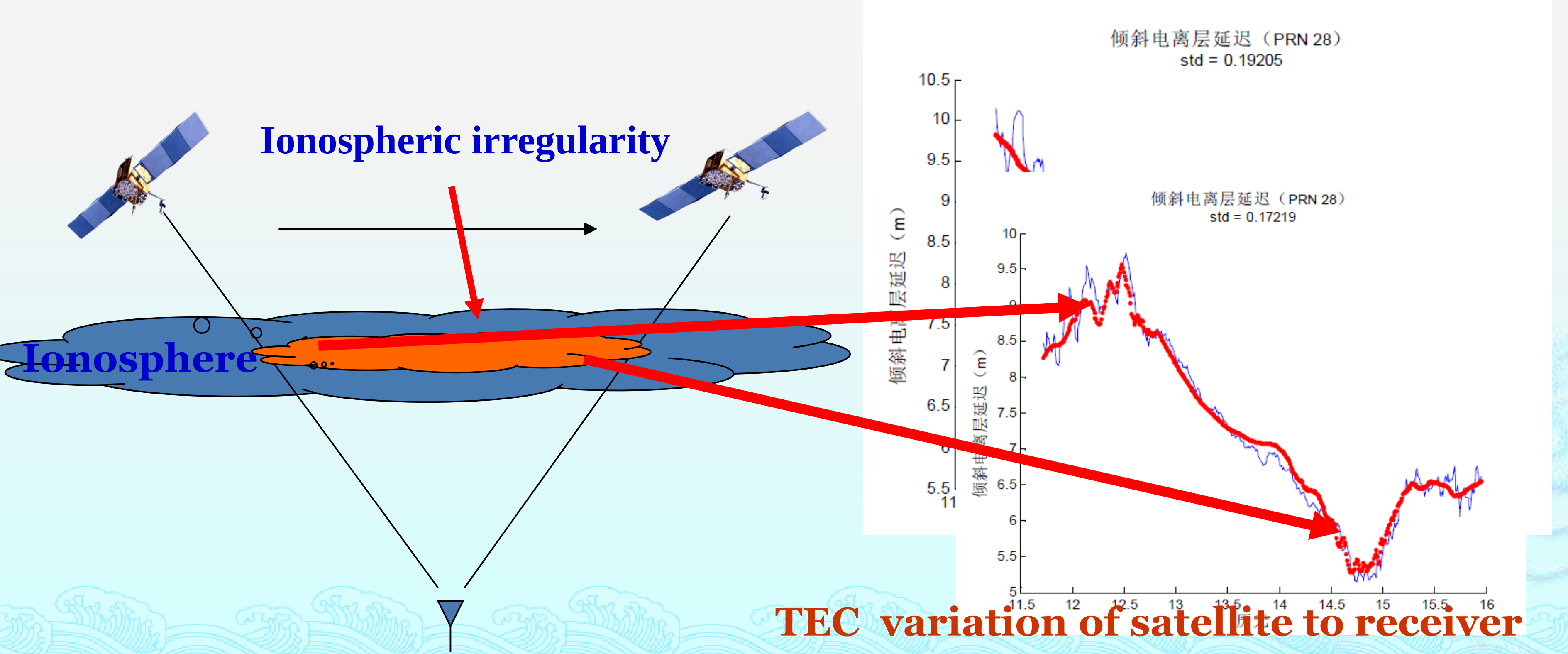
Types of technique	Detection ability	Difficulty for implementation	Detection efficacy
Signal encryption	Detect produced spoofing signal only; Significant latency	Medium	Medium
Residual signal	Detect both kinds of spoofing signals	High	Medium
Signal propagation delay	Detect retransmission spoofing signal	Medium	Common
Angle of arrival	Detect both kinds of spoofing signals	High	Good
Angle difference of arrival	Detect both kinds of spoofing signals	High	Good

Each spoofing detection technique has its limitation. However, combination of these techniques are the future direction so as to obtain the best spoofing detection effect at the lowest cost.

3、Ionospheric Scintillation detection techniques

（1） Effect analysis of ionospheric scintillation

Ionospheric irregularities are the main cause of scintillation. The accuracy of ionospheric models and GNSS localization results can be greatly affected by ionospheric scintillation.

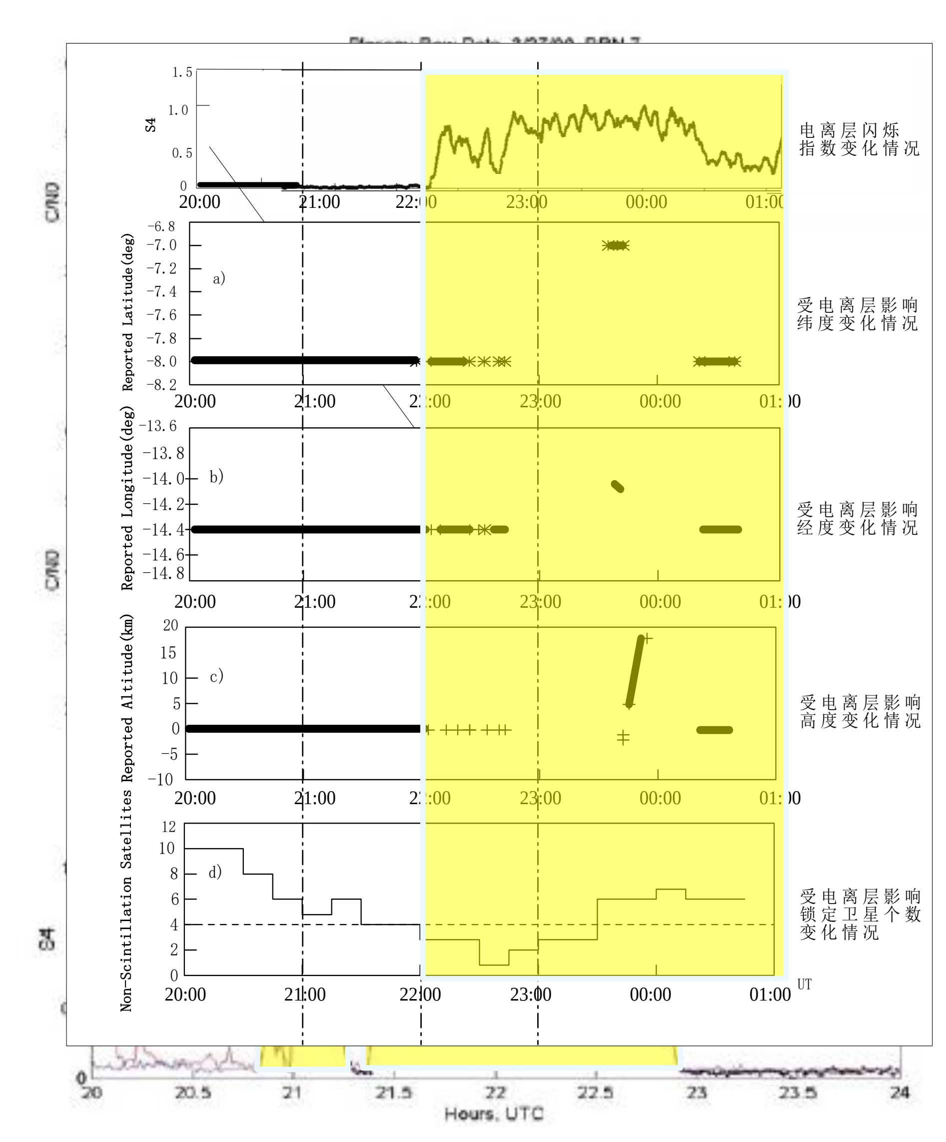


TEC variation of satellite to receiver

The effect of ionospheric scintillation on the performance of GNSS include:

- Received signals;
- Cycle slip in carrier phase;
- Measuring accuracy;
- Localization result.

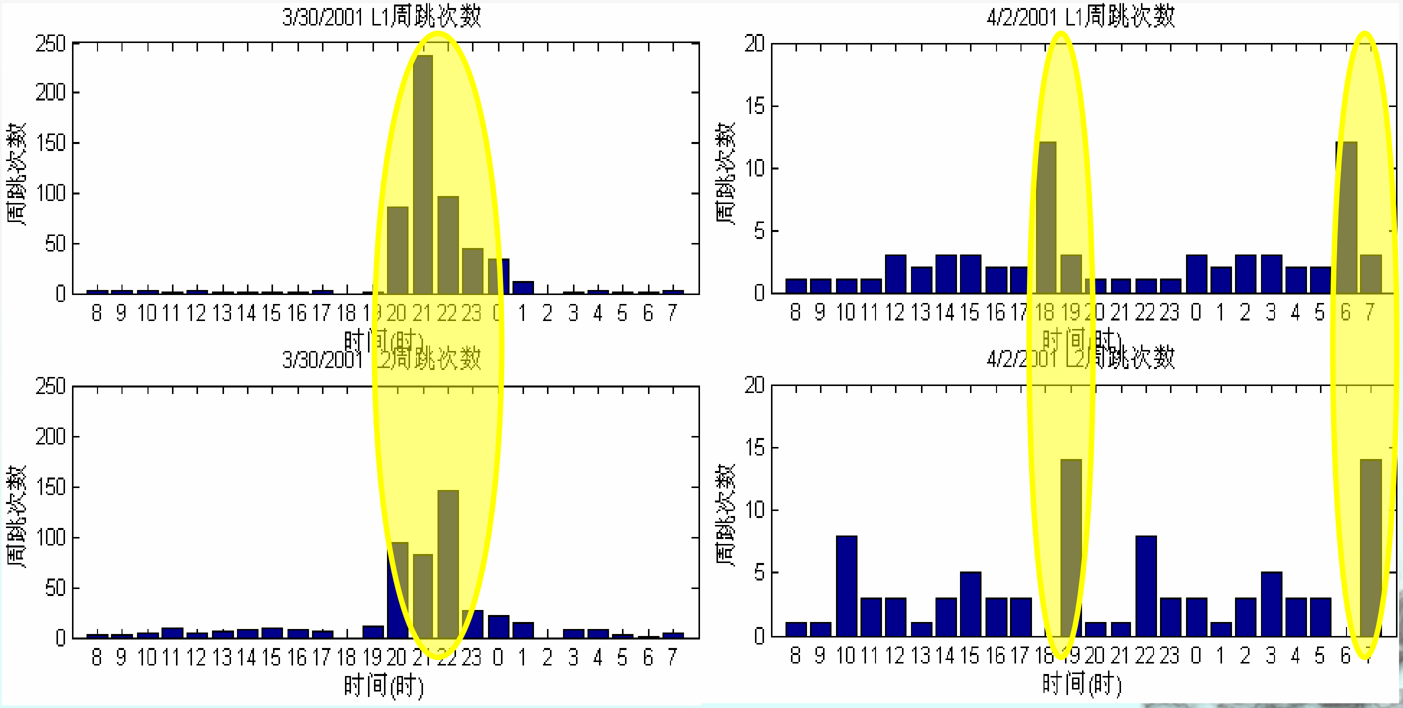
Received signals



- Degradation of C/N0;
- The lose of lock;
- service outage.

Cycle slip in carrier phase

The frequency of cycle slips emerging in carrier phase during scintillation is far more than the time without scintillation.



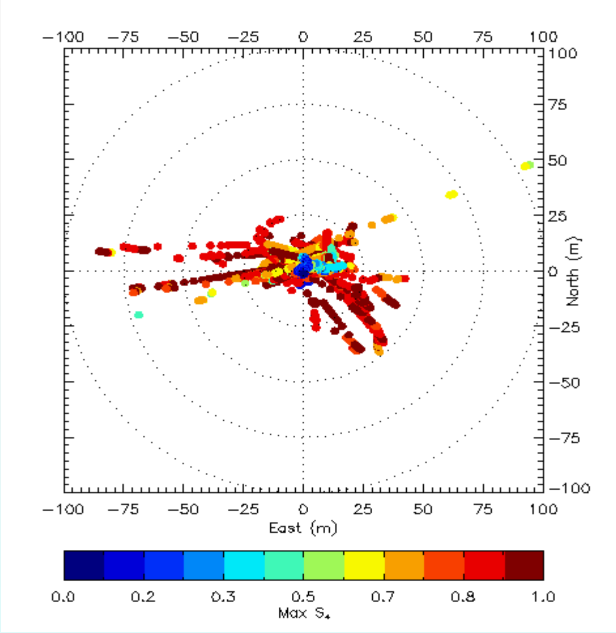
Measuring accuracy

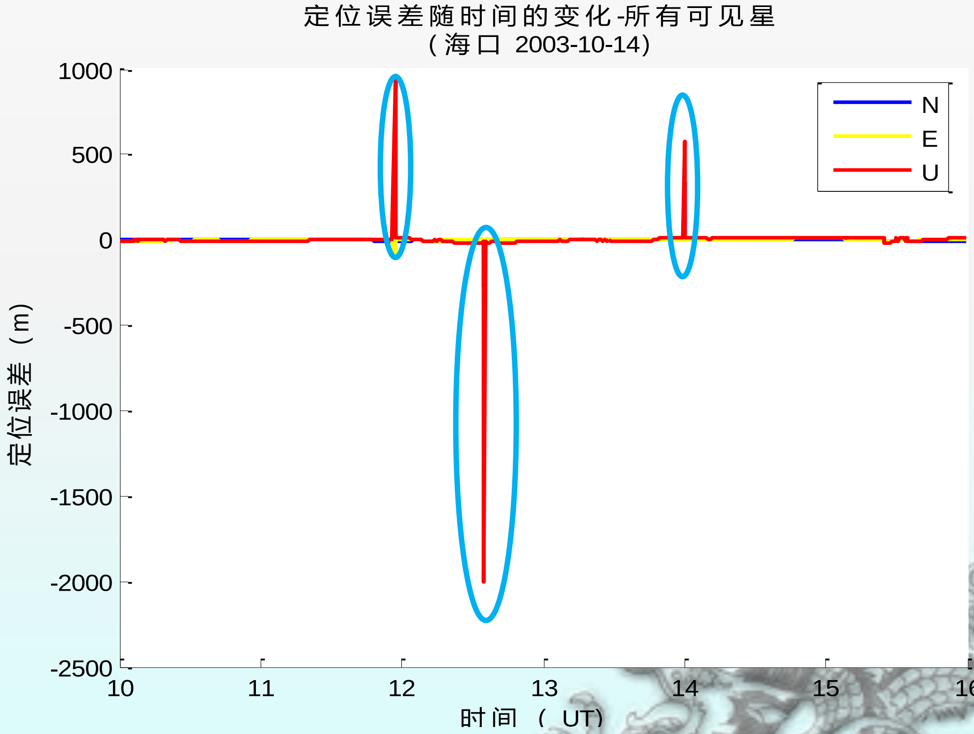
Ionospheric scintillation will lead to the reduce of the measuring accuracy, especially for the condition when losing lock.

PRN	**Measuring accuracy （m） 2014.10.13 （without scintillation）**	**Measuring accuracy （m） 2014.10.14 （scintillation）**
PRN 4	0.156	0.229
PRN 7	0.178	0.247
PRN 8	0.151	1476223.336
PRN 10	0.138	0.137
PRN 11	0.104	0.144
PRN 20	0.142	0.174
PRN 24	0.147	0.169
PRN 27	0.105	0.436
PRN 28	0.192	0.219
PRN 31	0.107	0.128

Localization results

Ionospheric scintillation will lead to large localization error, varying from several meters to several kilometers.



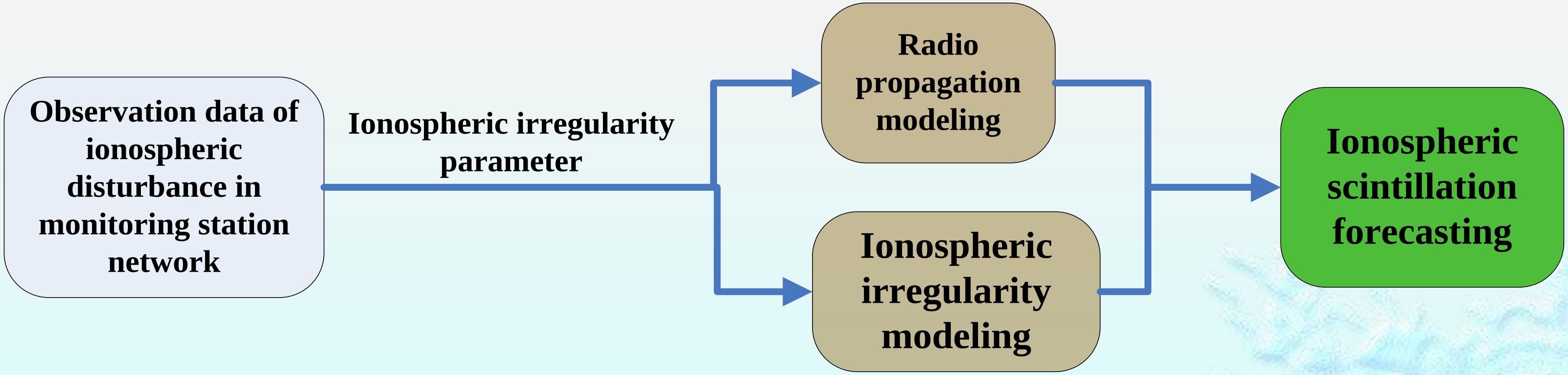


（2） Ionospheric Scintillation detection techniques

1） The establishment of ionospheric irregularity model and signal propagation model;

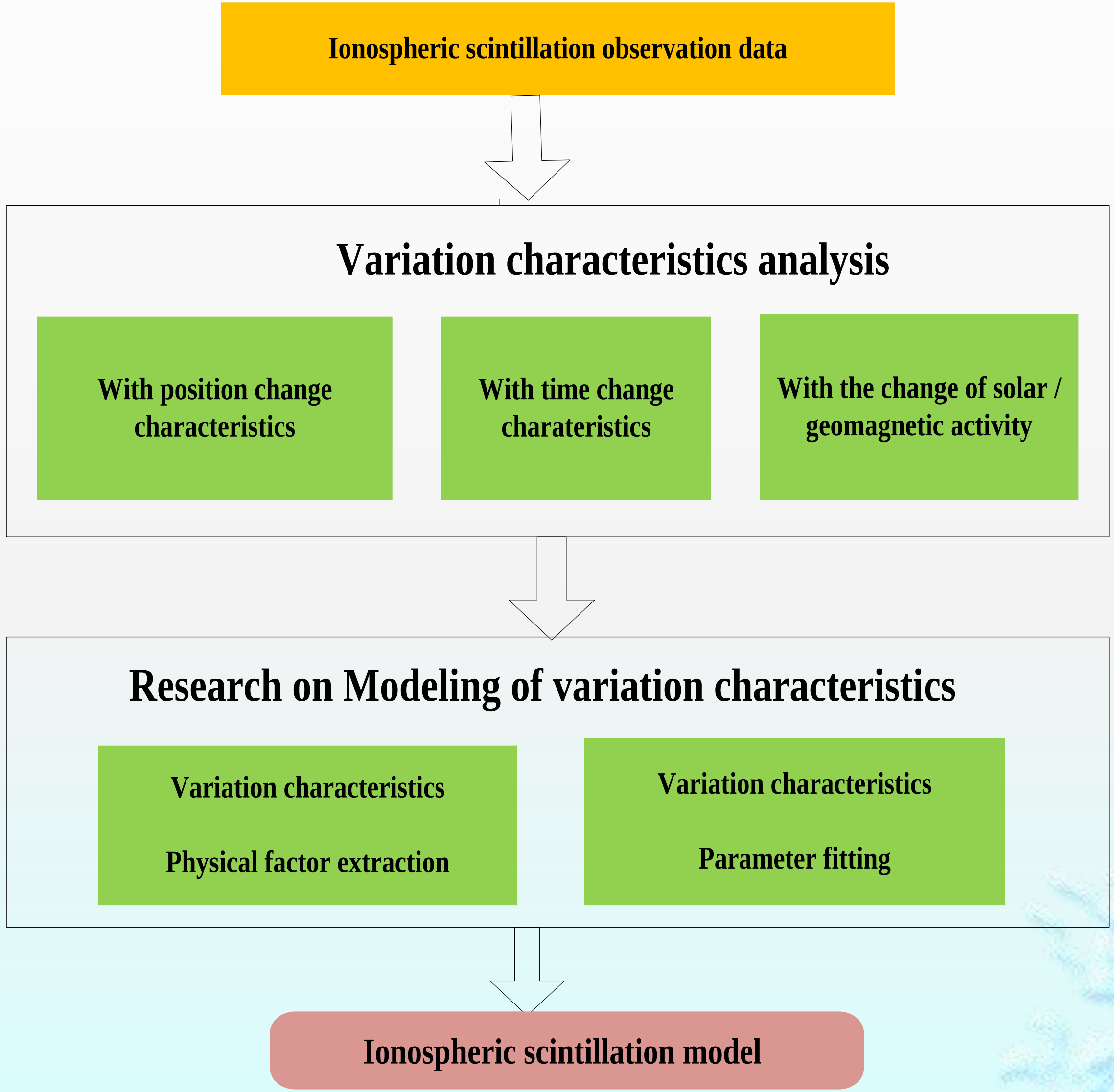
2) The obtaining of ionospheric irregularity body parameters based on the measured data inversion ;

3) The realization of short-term forecasting of ionospheric scintillation



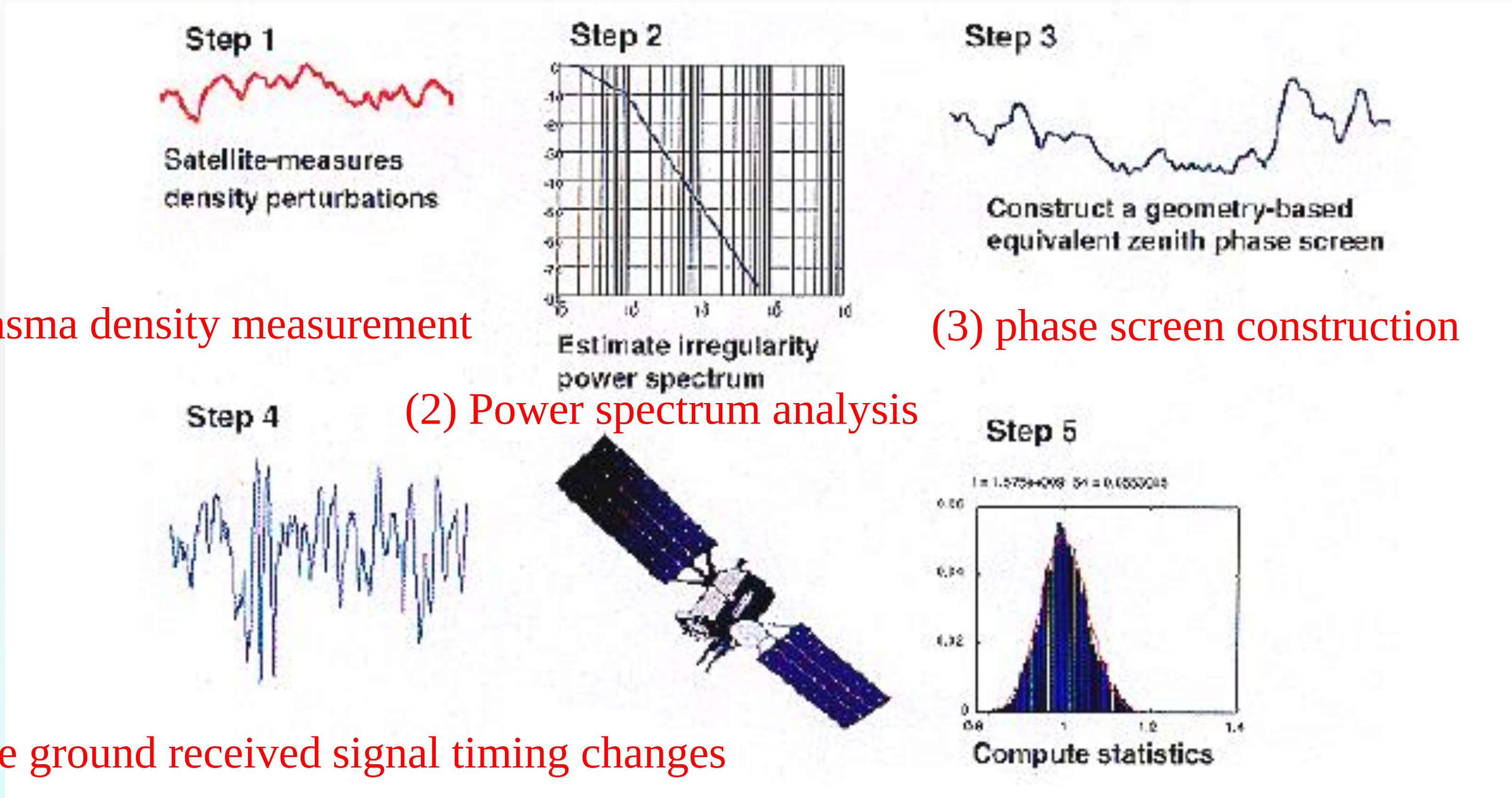
Short-term prediction process of ionospheric scintillation

1）Establishment of ionospheric irregularity model and signal propagation model



process of ionospheric irregularity modeling

The signal propagation model is based on the phase screen theory, which is the most classical method of ionospheric scintillation calculation and widely be used.



(1) Plasma density measurement

(2) Power spectrum analysis

(3) phase screen construction

(4) The ground received signal timing changes

(5) Scintillation index calculation

2）obtaining of ionospheric irregularity parameters based on the measured data inversion

The ionospheric irregularity model contains the following parameters:

- Ionospheric irregularity drift velocity;
- Ionospheric irregularity spectral index;
- Ionospheric irregularity strength;
- The outer scale of the ionosphere irregularity body;
- The range of ionospheric irregularities ;
- The direction of the ionospheric irregularities ;
- Etc,

Among them, the modeling of ionospheric irregularity drift velocity, spectral index and strength are very important .

Obtaining ionospheric irregularity parameters based on the measured data inversion.

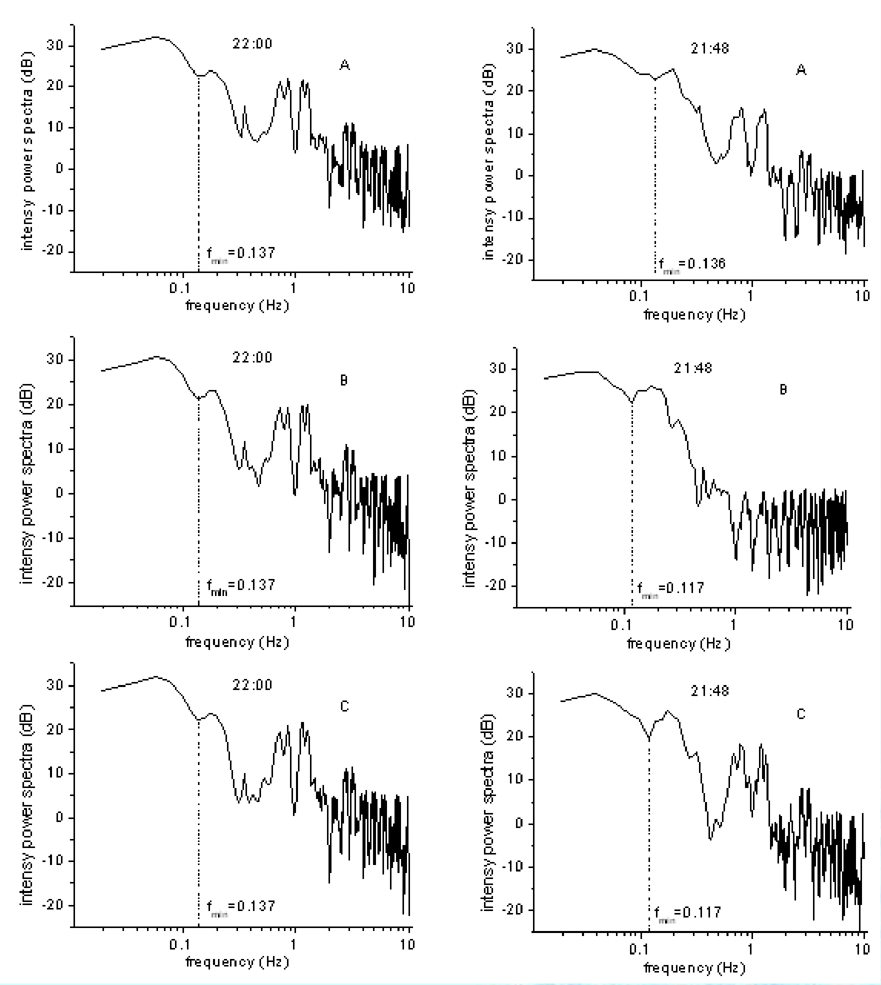
——drift velocity

Based on the signal power spectral analysis, the Ionospheric irregularity drift velocity can be calculated

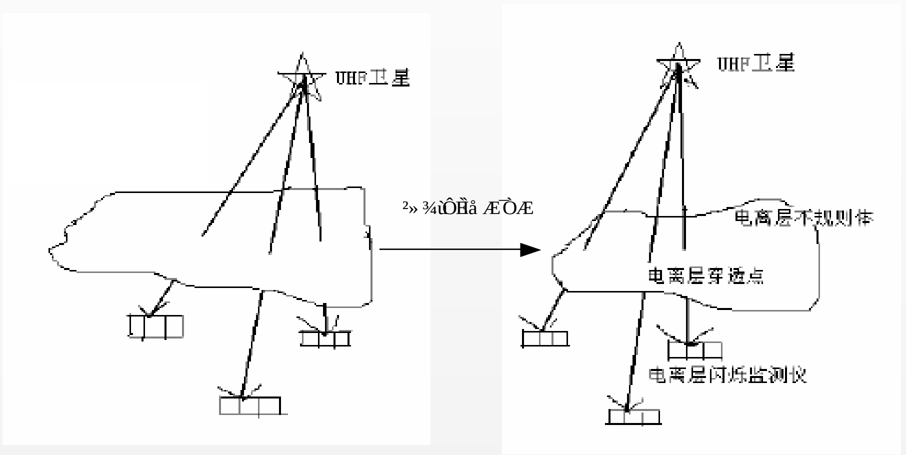
The estimation of the drift velocity of the ionosphere irregularity can be calculated using the Fresnel frequency:

$$v \approx \sqrt{\lambda z}\, f_{\min}$$

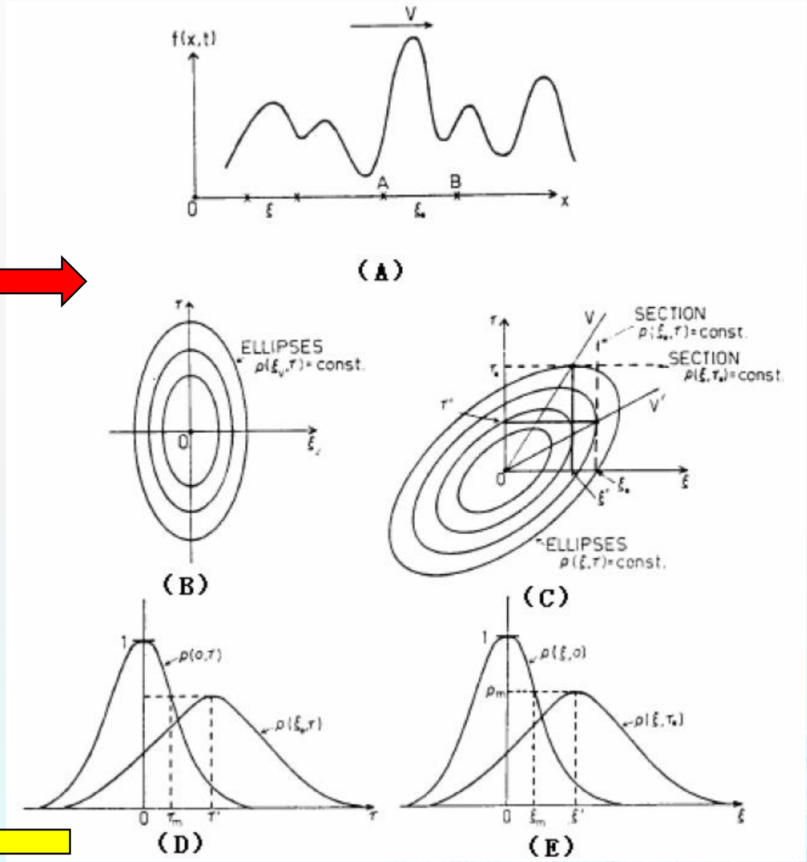
Where v is the drift velocity, λ is the signal wavelength, z is related to the signal propagation elevation angle, fmin is the Fresnel frequency, and can be approximated as the frequency value corresponding to the first minimum value of the signal power spectral curve.

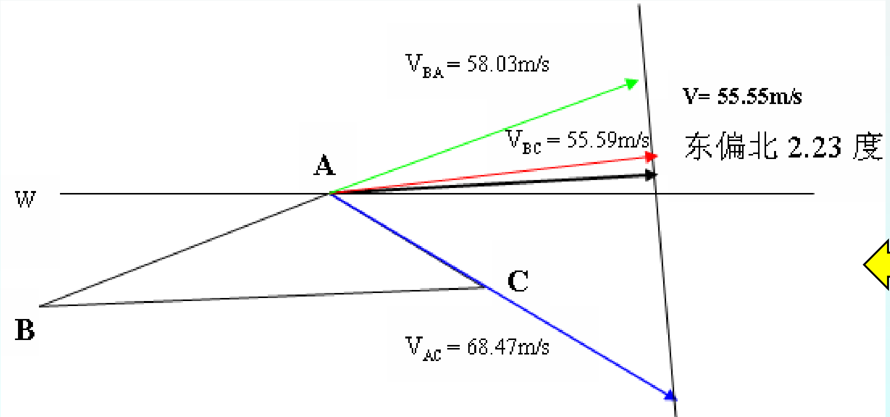


Based on the signal correlation analysis of the short baseline receiver array, it is also possible to calculate the drift velocity of the ionosphere irregularity.



Three stations measurement diagram





Examples of measurement results

Analysis principle

Obtaining of ionospheric irregularity parameters based on the measured data inversion.

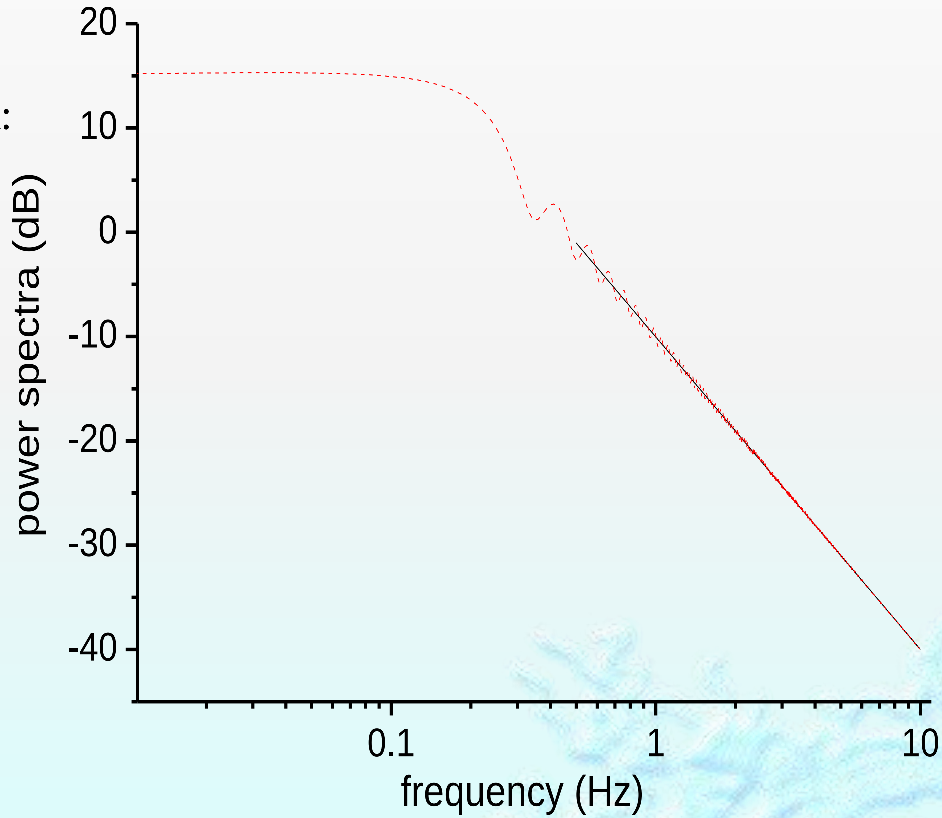
——spectral index

Based on the signal power spectral analysis method, the ionospheric irregularity spectral index can be calculated.

In the high frequency part, the signal power spectral curve can be written as an exponential function form:

$$\Phi_I = Af^{-(p-1)}$$

A is the amplitude of the exponential function, interrelated with signal wavelength, spectral index and other factors, p is the spectral index. After taking the logarithm at both ends, the least squares fitting can be used to obtain the irregularity spectral index.



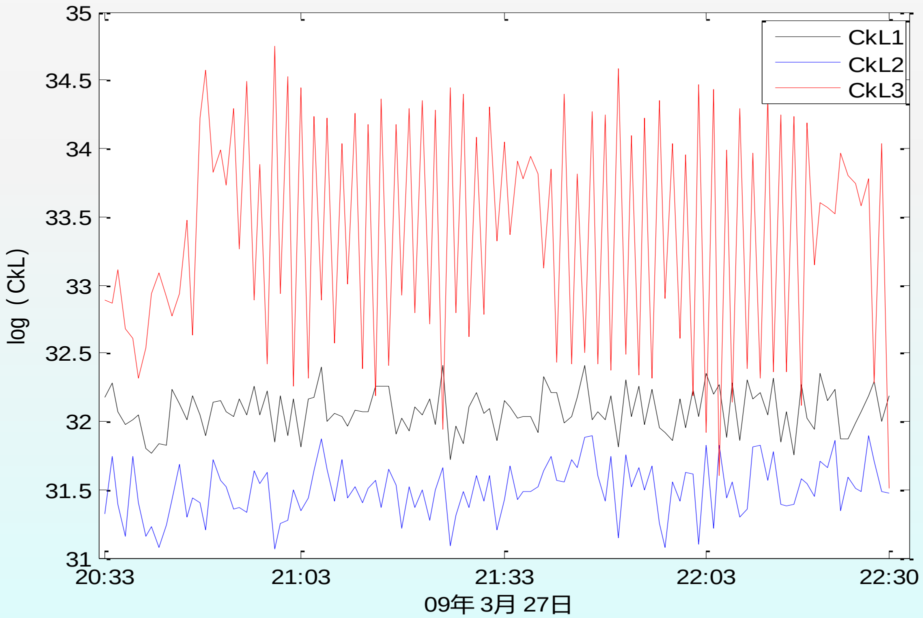
Obtaining of ionospheric irregularity parameters based on the measured data inversion.

——strength

The strength of the ionospheric irregularity can be calculated from the signal phase spectral analysis, phase scintillation index and amplitude scintillation index.

$$S_4 = \sqrt{\frac{<P^2> - <P>^2}{<P>^2}}$$

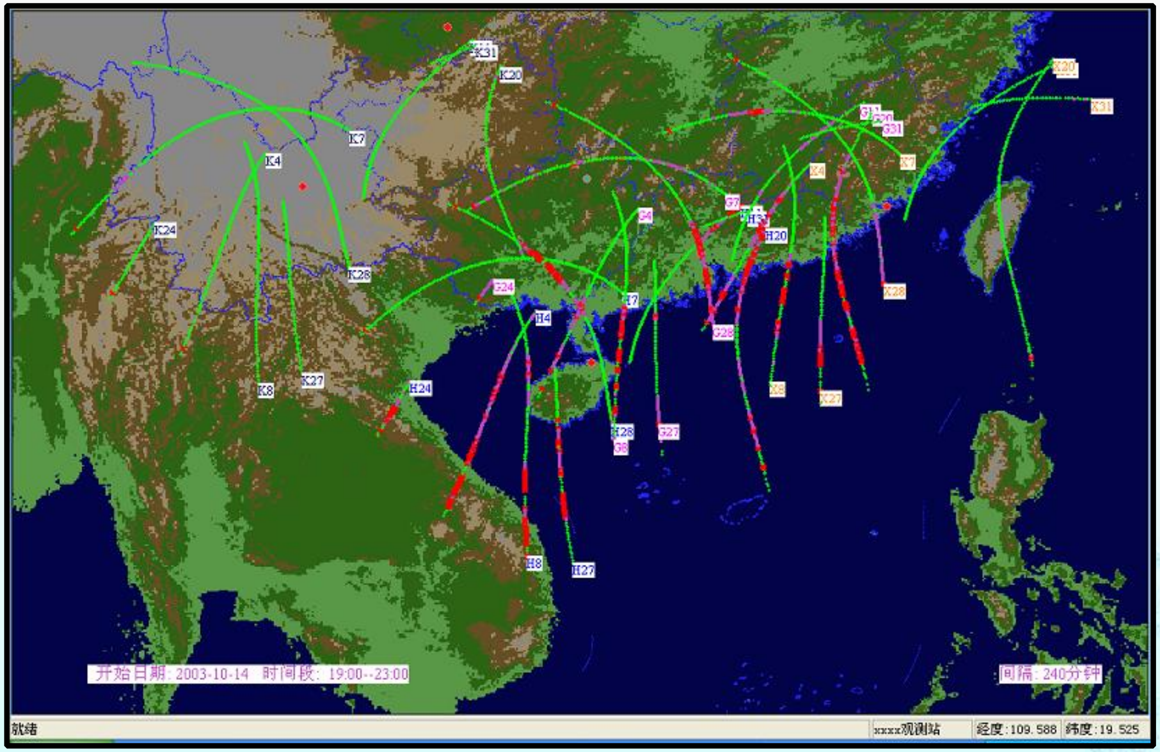
$$\sigma_\phi = \sqrt{<\phi^2> - <\phi>^2}$$



The results of the three different approaches are roughly the same. The results obtained by the amplitude sctillation index are larger, possibly due to the assumption that some of the parameter values are different from the actual.

（3）The realization of short-term forecasting of ionospheric scintillation

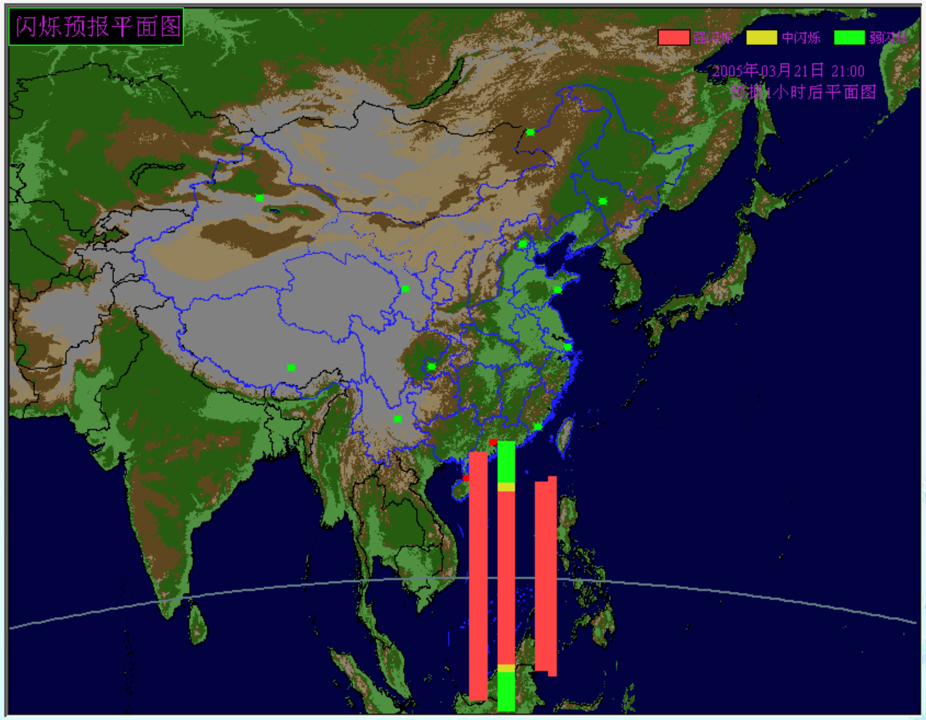
Gound-based short-term forecasting of ionospheric scintillation will be achieved by the inversion of the ionospheric irregularity parameters, the ionospheric irregularity model and the signal propagation model.



Example of short - term forecastingof regional ionospheric scintillation in China based on ground observation data

The spring up of GNSS detection technology has brought a great development of the ionospheric research. In recent years, the study of ionospheric scintillation is gradually showing the trend of the combination of space and ground.

The design and operation of aerospace systems have raised higher requirements for ionospheric scintillation forecasting.



4、Summary

1) Spoofing and ionospheric scintillation affect GNSS positioning and timing, posing a serious threat to GNSS applications for critical infrastructures；
2) A variety of methods can be used to detect spoofing, each with advantages and disadvantages. The conjunction of some methods will achieve more effective spoofing detection;
3) Through the establishment of the ionospheric irregularity modeling and the signal propagation modelling, the parameters of ionospheric irregularity can be obtained based on the measured data;
4) Ionospheric scintillation forecasting can provide better protection for GNSS applications.
5) It is very necessary to strengthen the research on anti-spoofing and ionospheric scintillation correction model to improve the positioning and timing accuracy of the receiver .

Thank you