# A Fundamental Architecture of Anti-spoofing GNSS Receiver

**Li He, Hong Li and Mingquan Lu**

**Abstract** Spoofing attack is growing into a great potential menace to future GNSS systems and related applications, featured by its stealth. Spoofing signal can deceive victim receivers by changing ranging observables covertly, leading to wrong positioning or timing solutions. It is reasonable to keep the power of spoofing signal similar to the power of authentic signal, in addition to its signal structure and navigational data. Therefore, there still are chances to track authentic signal along with received signal. Changing transmit time observables is essential to a successful spoofing attack. Based on this fact, we propose an acquisition and tracking framework in which transmit time plays a core role. This framework combines several algorithms, namely multi-peak acquisition algorithm, multiple tracking algorithm and repetitive signal cancelation regime. A receiver, equipped with the proposed framework, can continuously acquire all existing signals and then tracks them, regardless of their authenticity. Moreover, experiments on GPS simulator attack and meaconing spoofing signal are shown.

**Keywords** Software receiver · Anti-spoofing · Multiple peak acquisition · Multiple peak tracking

## 1 Introduction

GPS system and its vast application have achieved such a great success that almost every sector of today's society relies on its functionality. Therefore, criminals would be more motivated to sabotage it. Recent years have witnessed a rapid rise of

L. He (✉) · H. Li · M. Lu
Department of Electronic Engineering, Tsinghua University,
100084 Beijing, China
e-mail: heliosthu@163.com

H. Li
e-mail: lihongee@mail.tsinghua.edu.cn

M. Lu
e-mail: lumq@mail.tsinghua.edu.cn

J. Sun et al. (eds.), *China Satellite Navigation Conference (CSNC) 2017 Proceedings: Volume I*, Lecture Notes in Electrical Engineering 437,
DOI 10.1007/978-981-10-4588-2_76

incidents caused by GPS interference both unintentionally and intentionally. Amongst these interferences, a method named spoofing has drawn large attention because of stealth and dangerous potential. Spoofing is able to covertly coerce a GPS receiver to output incorrect timing and positioning solution. Spoofing device transmits signals that resemble true GPS signal in vicinity of intended victim, in order to disturb victim's tracking of authentic signal, finally capture its tracking loop.

No concern on GPS security was spent during construction, especially the C/A signal on GPS L1 frequency. Most civilian receivers have no precautions against spoofing. They would utilize any signal available to estimate observables in purpose of positioning. This straightforward but fragile logic leaves a backdoor to various spoofing and interference.

Many methods have been proposed to tackle with malicious interference and spoofing against GPS. Some of them need modification to hardware of existing receivers, such as adding AGC monitor [2] (to monitor signal power), or adding more antenna or cooperation between receiver [3] (to estimate direction of arrival). However, the expense makes updating hardware of existing receivers impossible. Some papers propose single-antenna receiver defence method based on baseband signal processing, requiring no modification to hardware of receivers and signal regime.

Reference [4] proposes that, anomaly occurred during the capture of tracking loop can be detected by monitoring the symmetry of triangular-shaped correlation function of ranging code. This method has high false alarm rate in strong multipath environment, and its transient nature easily confuses with false alarm. Reference [6] points out that monitoring abnormal changes in carrier to noise ratio ($C/N_0$) has potential to detect spoofing. Meanwhile, reference [6] also points out this method is limited without hardware modification. Reference [7] uses cross-correlation of in-phase component of correlation value to discriminate whether the received signals are transmitted from one antenna. But this requires receiver moving in a shading-variation scenario. Reference [1] intensively reviews this type of defence methods.

In summary, methods based on signal feature are somewhat flawed, leading to limited effectiveness in actual use. Considering these facts, this paper proposes a fundamental framework supported by a novel running logic. This framework converts extra computation capability in a receiver into the ability of anti-spoofing. By acquiring and tracking all signals regardless of authenticity, this framework enables defence against various spoofing methods (including simulator attack, meaconing attack and intermediate spoofing attack) after knowing signal characteristics.

This rest part is arranged as follow. The second section characterizes the assumptions and features of spoofing signal, and roughly analyses viable defence. The third and fourth sections introduce the proposed mechanism for the acquisition and tracking of spoofing signal. The fifth section shows experimental results on over-the-air GPS signal. The sixth section comprises conclusion and discussion.

# 2 Analysis of Spoofing Attack

## *2.1 Assumptions and Premises*

According to their nature, attacks on GPS receivers can be roughly categorized into two types, i.e., jamming and spoofing. Jamming refers to attack in which transmission of interference signal disrupts tracking or acquisition of satellite signal. Some jamming signal suppresses the amplifier of victim receiver into non-linear state, blocking receiver baseband processing away from true signal. Some jamming triggers loss of lock in tracking loop. Nonetheless, this type of attack will raise alarm by disrupting normal working of receiver, thus preventing further damage. On the contrary, spoofing signal needs infiltration into baseband and capture of tracking loop. This precludes extremely large signal power. Spoofing signal with power larger than true signal can be detected by power monitoring [2].

All spoofing methods mentioned above are coarse and primitive, especially compared to the novel and inexpensive spoofing method proposed by [5]. The most advantage of this method is stealth. It does not cause any loss of lock and cannot be detected by power monitoring. Concerning its characteristic, we make several assumptions as follow:

1. The low noise amplifier (LNA) of receiver still works in linear state;
2. Spoofing signal has similar power with authentic signal;
3. No nulling or shading of true signal transmitted from GPS satellites.

The assumptions of spoofing signal are reasonable. We only focus on advanced and cost-limited spoofing approaches, not those can be defeated by simple defense methods such as power monitoring. Therefore, these assumptions agree with the capability of existing spoofing techniques, and suffice to circumvent simple anti-spoofing methods.

## *2.2 Characteristics of Spoofing Signals*

Several premises about spoofing and authentic signal have been previously assumed. In this section, characteristics of the signal under assumptions above will be analyzed:

Assumption 1 guarantees that the receiver still is able to receive and acquire GPS signal (no matter of the authenticity);

Assumption 2 ensures that spoofing signal neither does not simply suppress true signal under noise floor, nor the inter-address interference is large enough to prevent acquiring the true ones;

Assumption 3 guarantees the availability of true signal, which means true signal still can be acquired.

With these assumptions, the received signal is the mixture of spoofing signals and authentic ones, and both can be acquired and tracked steadily. As we can see from Sect. 1, most spoofing techniques (ranging from simplest simulator attack to sophisticated spoofing) aiming at civilian receivers need "drag" the timing and positioning solution of a victim from its real time-space point, while a GPS receiver resolves by measuring the transmit time of present signal. Consequently, most spoofing attempts necessarily deviate from true signal in transmit time observables.

This mixed signal appears more than one recognizable peak in the correlation domain used in acquisition. This phenomenon differentiates itself from the single peak scene under normal circumstance. Therefore, this mixed signal could be named as "multi-peak signal". In next section we propose an acquisition algorithm in purpose of acquiring multi-peak signal.

# 3 Multi-peak Acquisition

From the analysis of the characteristic in previous section, it could be seen that the multi-peak signal can be discriminated by the multiple peaks in the correlation domain.

## *3.1 Recognition and Acquisition of Multi-peak Signal*

In the discrete code phase-Doppler frequency domain used in acquisition stage, a correlation peak comprises several relatively large values on adjacent grids. True signal only contains one correlation peak, if no strong multipath or spoofing signal imposed. Whereas the mixed signal shows multiple correlation peaks (when transmit time or Doppler frequency differs from each other), meaning that there would be several areas containing relatively large correlation values in the mentioned domain.

The acquisition algorithm of a normal receiver often searches for the maximum of correlation values and corresponding code phase and Doppler frequency, or find the correlation value larger than a preset threshold in a sequential search. The naivety of this strategy incapacitates acquiring all correlation peaks stemming from mixed signal. Thus, some modifications to the traditional acquisition strategy are necessary. Existing acquisition algorithm can be modified to output information about multiple correlation peaks rather than only one peak. Maximum search method should be changed into multiple maxima search method; threshold method should find all correlation points exceeding the threshold as output. Thus, multi-peak acquisition algorithm outputs several code phase and Doppler frequency pairs that can initialize tracking channels.

However, one correlation peak always causes several relatively large correlation values (or larger than preset threshold) on code phase-Doppler frequency grids.

Hence, if these acquisition results are directly utilized to initialize tracking channels, there would be a great waste in computation resources. By analyzing the structure of correlation peak, we could cluster these raw results to reduce computing consumption.

Correlation peak clustering exploits the structure of correlation peak, and these raw results originated from a single correlation peak are contiguous. This fact facilitates the clustering and recognition algorithm based on comparing the code phases and Doppler frequencies of raw results. The procedure can be listed as:

(1) Clustering the raw results according to their code phases and Doppler frequencies. Ensures that within same correlation peak set the range of code phase does not exceed one code chip, and the range of Doppler frequency does not exceed coherence bandwidth;
(2) The number of points accumulated in a correlation peak set is marked as "support" of the correlation peak set;
(3) In high C/N0 scenario, delete all the correlation peak set with support of 1, and the rest is remained as initial values for tracking channels, which would reduce computation burden largely. In low C/N0 scenario, all the raw results are needed to prevent missing any potential signal (Fig. 1).

## 3.2 Parameters and Performance

For multi-maxima method, the only configurable parameter is the number of multi-maximum. Since one correlation peak causes several maxima according to the configuration of acquisition, and the number of correlation peaks have linear impact on the multiplicity of maxima as long as the overlapping of different correlation peak is limited. Therefore, to set the number of maxima, parameters of acquisition and the expected number of correlation peaks have to be taken into

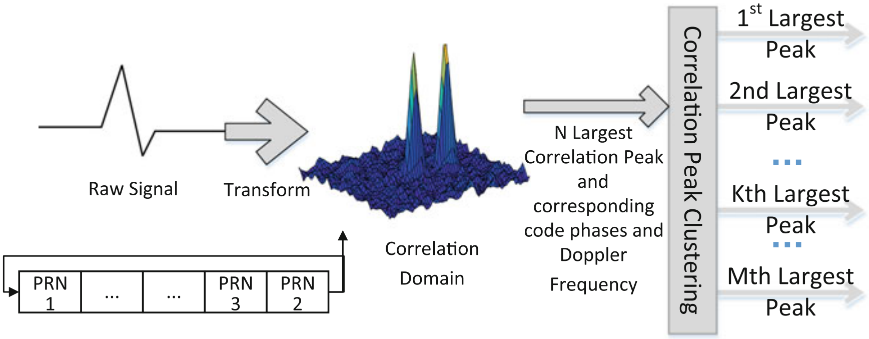


**Fig. 1** Acquisition of multi-peak signal

consideration. If the parameter N is set too low, there probably would be miss detection of possible correlation peaks; if too large, it would aggravate computation burden.

The threshold decision method only relies on the threshold itself. If the threshold is set too low, there would more false alarm due to the increased noise; if too high, there would be more miss detection.

Usually, in complex signal environment, any fixed parameter has its failure area. In fact, the optimal parameter setting is to change it dynamically considering signal environment fluctuation. Unlike normal acquisition, the mathematics behind multi-peak acquisition is a ternary hypothesis test, which requires further analysis. Further mathematical derivation is omitted for the brevity of this paper.

# 4 Multiple Tracking Strategy

Multi-peak signal acquisition can only detect the presence of spoofing signals, but what is more desirable is the ability to distinguish the authenticity of the signal. The foundation of further discrimination and mitigation of spoofing signal is the tracking of all possible signals.

## *4.1 Logic and Procedure of Tracking*

The computation resource of civilian GNSS receiver is structured as channels, and the identification of a specific channel is the PRN code it tracks. In premise of multi-peak signal, however, PRN number does not suffice to identify different channels clearly. Consequently, the tracking logic and procedure of receiver call for modification.

First of all, how to uniquely identify different signals. As previously analysed, the transmit time of spoofing signal should deviate from the authentic ones, then the PRN and transmit time pair is sufficient to uniquely identify the signal being tracked. Therefore, the channel-based architecture still works, only with little change of identifying channels by the mentioned pair.

The most resource consumed in multi-peak tracking is computation capacity. So, a receiver with multi-peak tracking ability inevitably requires more computation capacity, leading to more power consumption. Thus receivers with configurable channels are more suitable for multi-peak signal tracking (Fig. 2).

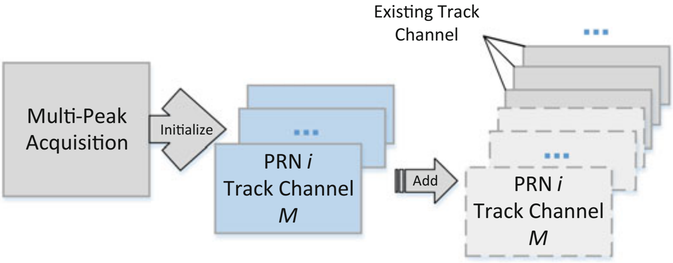


**Fig. 2** Tracking of multi-peak signal

### 4.2 *Repeating Acquisition and Duplicate Signal Cancellation*

The acquisition strategy of normal civilian receiver only tries to acquire the PRN that is not under tracking, rather than those already under tracking. The reason behind is that receiver has no prior knowledge of emerging satellite (because of satellite position and signal fading environment), while those already in tracking require no more acquisition attempts.

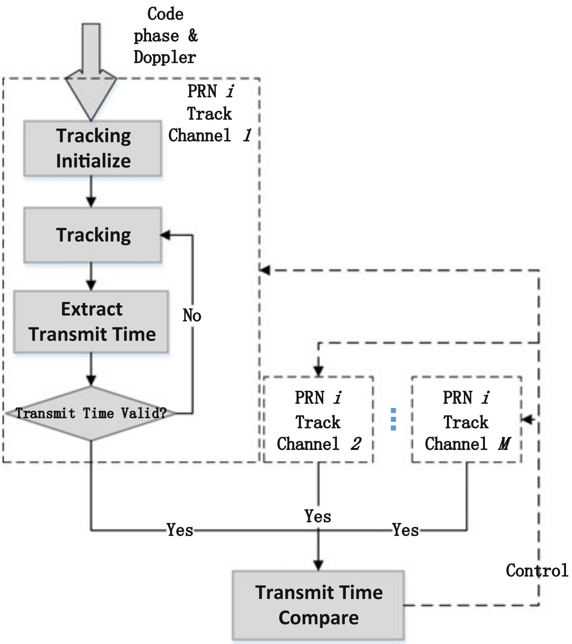
Similarly, we possess no prior knowledge about when spoofing begins, when the spoofing signal captures tracking loop, or when the transmit time of spoofing signal deviates. In a word, we have no idea about when the normal signal becomes multi-peak signal. Consequently, existing acquisition strategy cannot timely counter spoofing signal in long-term operation.

Accordingly, to detect spoofing signal in time, multi-peak acquisition process needs to be repeated for all PRN codes (whether or not a channel is assigned for it). However, this repetition will certainly cause re-acquisition of same signal and its redundant tracking as a consequence. It is obviously not reasonable to assign two channel to track one replica of same signal, while missing an existing signal is more undesirable.

The "PRN-Transmit Time" pair can uniquely determine the signal represented by a single correlation peak in multi-peak signal. Therefore, by comparing the transmit times with same PRN, if the difference of transmit times is smaller than the error performance of tracking loop (typical tracking error performance is around 10 ns), they can be identified as signal represented by a single correlation peak; if the transmit time difference exceeds the error of tracking loop, then we believe that the signals compared originate from different correlation peaks.

But the repeating acquisition leads to re-entry of the signal from the same correlation peak, then there would certainly be two channels with transmit time difference less than tracking error. The extra channels tracking same correlation peak need to be cancelled in purpose of saving resources. To avoid the confusion about cancelling which channel, another feature is necessary for discriminating the channels. The duplicate channels tracking same correlation peak can only stem

**Fig. 3** Recursive acquisition and cancellation of multi-peak signal



from successive multi-peak acquisitions, because of correlation peak clustering. Thus the channel of which the tracking duration is longer should outlive the others. Then through comparing PRN number, transmit time and tracking duration of channels, the repeating multi-peak acquisition can work along with the multi-peak tracking. This mechanism satisfies both the purpose of saving computation resource and missing no possible signal (Fig. 3).

## 5 Experimental Results

After establishing experimental platform, we have conducted experiments both on GPS simulator signal and receiver-spoofer meaconing live signal. The configuration of platform is depicted in Fig. 4. To test the function of the proposed architecture, we can send spoofing signal (at similar power as true signal) into the receiver by adjusting the attenuator.

Figures 5 and 6 shows actual results on the multi-peak signal formed by true signal and spoofing signal transmitted from simulator and receiver-spoofer, respectively.

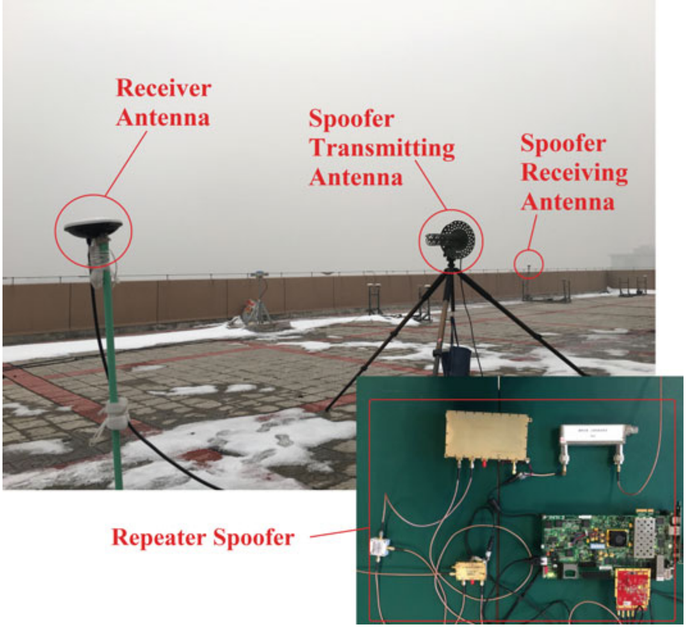
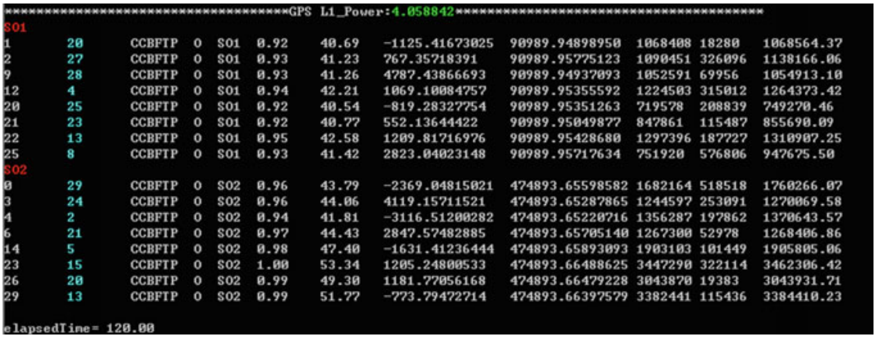


**Fig. 4** Meaconing spoofing platform

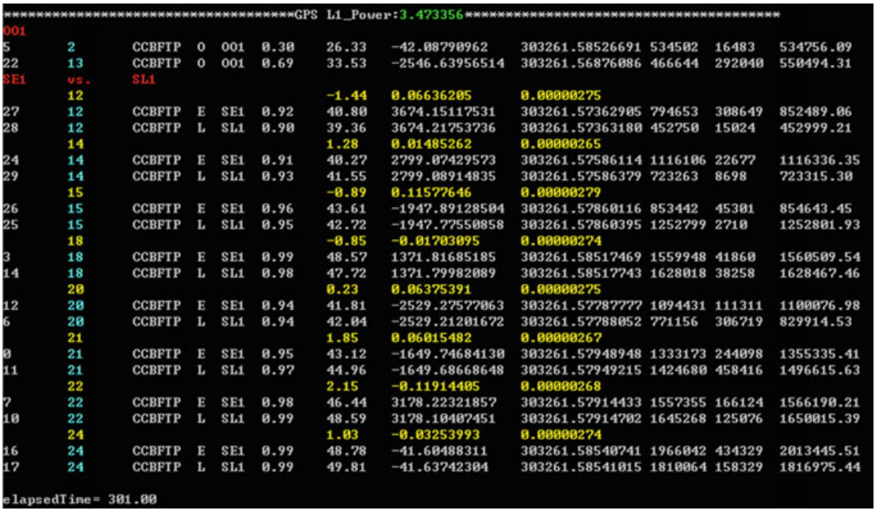


```
************************************GPS L1_Power:4.058842****************************************
S01
1       20      CCBFTP  O  S01  0.92    40.69   -1125.41673025  90989.94898950  1068408 18280   1068564.37
2       27      CCBFTP  O  S01  0.93    41.23   767.35718391    90989.95775123  1090451 326096  1138166.06
9       28      CCBFTP  O  S01  0.93    41.26   4787.43866693   90989.94937093  1052591 69956   1054913.10
12      4       CCBFTP  O  S01  0.94    42.21   1069.10084757   90989.95355592  1224503 315012  1264373.42
20      25      CCBFTP  O  S01  0.92    40.54   -819.28327754   90989.95351263  719578  208839  749270.46
21      23      CCBFTP  O  S01  0.92    40.77   552.13644422    90989.95049877  847861  115487  855690.09
22      13      CCBFTP  O  S01  0.95    42.58   1209.81716976   90989.95428680  1297396 187727  1310907.25
25      8       CCBFTP  O  S01  0.93    41.42   2823.04023148   90989.95717634  751920  576806  947675.50
S02
0       29      CCBFTP  O  S02  0.96    43.79   -2369.04815021  474893.65598582 1682164 518518  1760266.07
3       24      CCBFTP  O  S02  0.96    44.06   4119.15711521   474893.65287865 1244597 253091  1270069.58
4       2       CCBFTP  O  S02  0.94    41.81   -3116.51200282  474893.65220716 1356287 197862  1370643.57
6       21      CCBFTP  O  S02  0.97    44.43   2847.57482885   474893.65705140 1267300 52978   1268406.86
14      5       CCBFTP  O  S02  0.98    47.40   -1631.41236444  474893.65893093 1903103 101449  1905805.06
23      15      CCBFTP  O  S02  1.00    53.34   1205.24800533   474893.66488625 3447290 322114  3462306.42
26      20      CCBFTP  O  S02  0.99    49.30   1181.77056168   474893.66479228 3043870 19383   3043931.71
29      13      CCBFTP  O  S02  0.99    51.77   -773.79472714   474893.66397579 3382441 115436  3384410.23

elapsedTime= 120.00
```

**Fig. 5** Result on GPS simulator attack

In Fig. 5, the simulator-generated signal is readily separated by transmit time clustering algorithm (in the upper part). There are 8 replayed satellites in Fig. 6 that are discriminated from their authentic counterparts. In summary, the receiver equipped with the proposed architecture can readily defence the spoofing attacks with reasonable power that is launched by simulator and receiver-spoofer.



```
**************************************GPS L1_Power:3.473356****************************************
001
5       2       CCBFTP  O  001  0.30    26.33   -42.08790962     303261.58526691 534502  16483   534756.09
22      13      CCBFTP  O  001  0.69    33.53   -2546.63956514   303261.56876086 466644  292040  550494.31
SE1     vs.     SL1
        12                              -1.44   0.06636205       0.00000275
27      12      CCBFTP  E  SE1  0.92    40.80   3674.15117531    303261.57362905 794653  308649  852489.06
28      12      CCBFTP  L  SL1  0.90    39.36   3674.21753736    303261.57363180 452750  15024   452999.21
        14                              1.28    0.01485262       0.00000265
24      14      CCBFTP  E  SE1  0.91    40.27   2799.07429573    303261.57586114 1116106 22677   1116336.35
29      14      CCBFTP  L  SL1  0.93    41.55   2799.08914835    303261.57586379 723263  8698    723315.30
        15                              -0.89   0.11577646       0.00000279
26      15      CCBFTP  E  SE1  0.96    43.61   -1947.89128504   303261.57860116 853442  45301   854643.45
25      15      CCBFTP  L  SL1  0.95    42.72   -1947.77550858   303261.57860395 1252799 2710    1252801.93
        18                              -0.85   -0.01703095      0.00000274
3       18      CCBFTP  E  SE1  0.99    48.57   1371.81685185    303261.58517469 1559948 41860   1560509.54
14      18      CCBFTP  L  SL1  0.98    47.72   1371.79982089    303261.58517743 1628018 38258   1628467.46
        20                              0.23    0.06375391       0.00000275
12      20      CCBFTP  E  SE1  0.94    41.81   -2529.27577063   303261.57787777 1094431 111311  1100076.98
6       20      CCBFTP  L  SL1  0.94    42.04   -2529.21201672   303261.57788052 771156  306719  829914.53
        21                              1.85    0.06015482       0.00000267
0       21      CCBFTP  E  SE1  0.95    43.12   -1649.74684130   303261.57948948 1333173 244098  1355335.41
11      21      CCBFTP  L  SL1  0.97    44.96   -1649.68668648   303261.57949215 1424680 458416  1496615.63
        22                              2.15    -0.11914405      0.00000268
7       22      CCBFTP  E  SE1  0.98    46.44   3178.22321857    303261.57914433 1557355 166124  1566190.21
10      22      CCBFTP  L  SL1  0.99    48.59   3178.10407451    303261.57914702 1645268 125076  1650015.39
        24                              1.03    -0.03253993      0.00000274
16      24      CCBFTP  E  SE1  0.99    48.78   -41.60488311     303261.58540741 1966042 434329  2013445.51
17      24      CCBFTP  L  SL1  0.99    49.81   -41.63742304     303261.58541015 1810064 158329  1816975.44

elapsedTime= 301.00
```

**Fig. 6** Result on meaconing attack

## 6 Conclusions

In this paper, we propose a fundamental receiver architecture and its supporting algorithms. This architecture can be utilized to acquire and track the multi-peak signal that is often encountered in spoofing scenario. The proposed architecture exploits the extra computation resource, and has no requirements of modifying existing RF frontend or IF device.

It is worth mentioning that the proposed architecture cannot discriminate and mitigate spoofing signal. However, the capability of acquiring and tracking multi-peak signal endowed by this architecture lays a cornerstone for further discrimination, mitigation and localization of spoofing signal.

The comparison of signal features enables discrimination of spoofing signal from the true one. For example, the transmit times of signal from GPS simulator always cluster in a small range, while separated from the transmit times of true signal. Meaconing signal does also show a strong pattern. The transmit time extracted from meaconing signal is earlier than true signal, and the differences equal over all satellites. On a receiver in motion, the time history of signal features (such as carrier Doppler frequency and carrier phase) can lend a hand in discrimination.

After distinguishing the spoofing signal, their observables will be excluded from position calculation. This mitigates the impact of spoofing signal, boosts the robustness of receiver. Conversely, the feature and observable of spoofing signal facilitate the localization of spoofer.

In summary, the architecture proposed in this paper exchange extra computation resource for capability of acquiring and tracking multi-peak signal. This architecture lays foundation for detection, discrimination, mitigation and localization of spoofing signal.

**Acknowledgements** This work was supported by the National Natural Science Foundation of China (Grant No. 61571255).

## References

1. Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G (2012) GPS vulnerability to spoofing threats and a review of antispoofing techniques. Int J Navig Obs
2. Akos DM (2012) Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). Navigation 59(4):281–290
3. Borio D, Gioia C (2016) A sum-of-squares approach to GNSS spoofing detection. IEEE Trans Aerosp Electron Syst 52(4):1756–1768
4. Manfredini EG, Motella B, Dovis F (2015) Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests. Proc ION GNSS+, Tampa, FL
5. Humphreys TE, Ledvina, BM, Psiaki ML, O'Hanlon BW, Kintner Jr PM (2008, September) Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: Proceedings of the ION GNSS international technical meeting of the satellite division, vol 55, p 56
6. Jafarnia Jahromi A, Broumandan A, Nielsen J, Lachapelle G (2012) GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. Int J Satell Commun Network 30(4):181–191
7. Nielsen J, Broumandan A, Lachapelle G (2011) GNSS spoofing detection for single antenna handheld receivers. Navigation 58(4):335–344