ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, *25-27 June*, *2017*, *pp. 1134-1138*
doi: 10.18178/wcse.2017.06.198

Beidou Signal Acquisition and Tracking Based on HackRF One

Jian Song [1, 2], Yun-Yao Zhou [1 +], Wei-Ye Tian [1] and Zhen Chen [1, 2]

[1] School of Information Engineering, Wuhan University of Technology, Wuhan, China

[2] Key Laboratory of Fiber Optic Sensing Technology and Information Processing (Wuhan University of Technology), Ministry of Education, Wuhan, China

Abstract. With the development of software defined radio (SDR) technologies, an increasing number of scientific research institutions and companies have started to use software receiver receiving satellite signals. However, the existing software receiver used the dedicated hardware devices to complete data collection. The existing problem of software receiver collection platform concerns a lack in versatility. This paper uses the Beidou signal as an example, proposing a method that used general software radio equipment to receiver satellite signals and giving an improved method. For Zero-IF signal features to design achieved Zero-IF signal digital track loop structure, used plural cross phase-frequency detector to completed phase identification. Simulation results show that compared the traditional method, the improved method improves detection veracity, more Beidou satellites data can be acquired.

Keywords: software defined radio (SDR), Zero-IF, pseudo-code, acquisition, tracking

1. Introduction

For many scientific research institutes, radio researching is conducted using a dedicated hardware device. It is difficult to personal fans have access to this special equipment. But with the emergence of the software radio platform, such as the RTL-SDR USRP and HackRF, BladeRF, and so on, it makes software defined radio appear more applicable. Dr. Alan designed a new type of small radio telescope in 2013 [1], it only used a RTL2832U Demodulator chip and R820T Tuner chip from Realtek as the signal receiving and processing unit, costing only a few dollars. Under his inspiration, a HackRF One was used as a receiving apparatus of the radio signal, completing the Beidou navigation system B1I signal reception, and use HackRF One receiving and tracking the satellite signals to determine the possible problems, proposing solutions.

2. Signal Processing

2.1. Design of a Digital Receiver

HackRF One [2] is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation. It is a SDR peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz. HackRF One on the received signal processing mainly uses the MAX2837 [3] chip to complete. The complete receiver can divide into several functional modules, RF front-end, acquisition module, and tracking module. This design might look similar to that shown in figure 1.

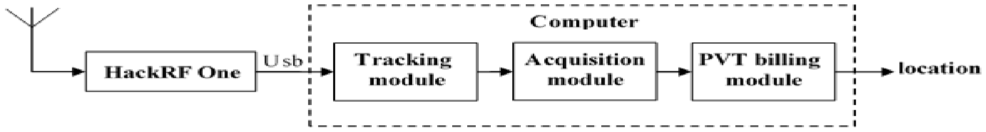

Fig. 1: Receiver structure.

[+] Corresponding author. Tel.: +8618671302334.
E-mail address: songjian0103@163.com.

Connection of equipment used as shown in figure 2.

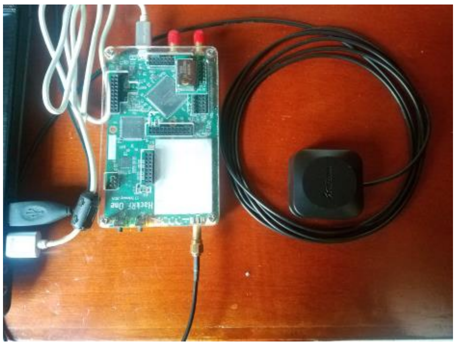

Fig. 2: HackRF one and the microstrip antenna.

2.2. HackRF One Data Structure

HackRF use a quadrature down-conversion mixer to complete signals acquisition. After signal acquisition completed, signal is a sequence as follow. It is important to note that HackRF One with other RF front-end equipment is different, it generates Zero if data. We needs to use other methods when we deal with these data, it will be discussed later.

$$S = I_1, Q_1, I_2, Q_2 ... I_{n,} Q_n$$

In the above formula, n is the data length, it depends on working time of equipment and sampling frequency. For example, we set the sampling frequency is 5.2 MHz, the device generated 5200 data in 1 millisecond.

$$n = f_s / t$$

where, f_s is the sampling frequency, t is the sampling time.

2.3. Beidou Signal Structure

The Beidou B1 signals are the sum of channel I and Q which are inphase quadrature of each other [4].B1I signal is a public signal, its expression is as follow:

$$S(t) = \sum_{k=1}^{N} AC(t)D(t)cos\left[2\pi\left(f + f_d\right)t + \varphi\right]$$

where, t is the receiving time; A is signal amplitude; C is the ranging pseudo-code; D is data modulated on ranging pseudo-code; f is carrier frequency; f_d is Doppler shift; φ is carrier initial phase, and N is the serial number of satellites.

2.4. The Traditional Signal Acquisition Method

The basic principle of satellite signal acquisition is to compare the correlation between the generated local satellite signals and received signals. If they are correlational, it means that the signal is successfully captured. The similarity comparison is done through mathematical operations. One of the methods to have a fast acquisition of satellite signals is to implement the parallel code-phase search [5], which uses the fast Fourier transform (FFT) to perform the correlation. The basic steps of signal acquisition are as follows.

Step 1: Data needs to be converted to another structure based on Beidou signal structure. It is as follow:

$$S = I_n + Q_n j$$

Step 2: Pseudo-code generation, generates native code referring to BeiDou Navigation Satellite System Signal in Space Interface Control Document (Version 2.1), it is a sequence as follow:

$$C = 0,1,1,0,1,0...1$$

Step 3: Convert these points to -1 and 1 (0 → -1) and resample them. The *C* will be converted into discrete code, its length and *n* are equal.

Step 4: In this step, the discrete C is converted into frequency domain by discrete Fourier transform. Then take its complex conjugate.

$$C^* = \text{Conj}\left(FFT\left(C\right)\right)$$

where, FFT is Fourier transform function, Conj() is complex conjugate function, and * is the complex conjugate of C.

Step 5: This step can use the function *exp( )* to generate the local carrier wave signal.

$$C_{\mathrm{W}} = exp\left(\frac{j*2*\pi*f_d}{f_s}*t\right), t=1\sim n$$

where, the value of Doppler shift is between 10 KHz and -10 KHz. searching step length is 500 Hz.

Step 6: Multiply the carrier wave signal and received signals together, giving the acquiring unit a new discrete sequence. Use the discrete Fourier transform to convert into frequency domain.

$$product{=}FFT\left(S \bullet Cw\right)$$

where, • is peer to peer multiplication.

Step 7: Multiply the carrier wave signal and received signals together, which will be used in the function of inverse Fourier transform to convert it into time domain.

$$result = Abs\left(IFFT\left(product \bullet C^{*}\right)\right)$$

This step used the function Abs( ) to obtain the absolute value. This step may need to run 41 times until the maximum value is found. The result might look like figure 3.

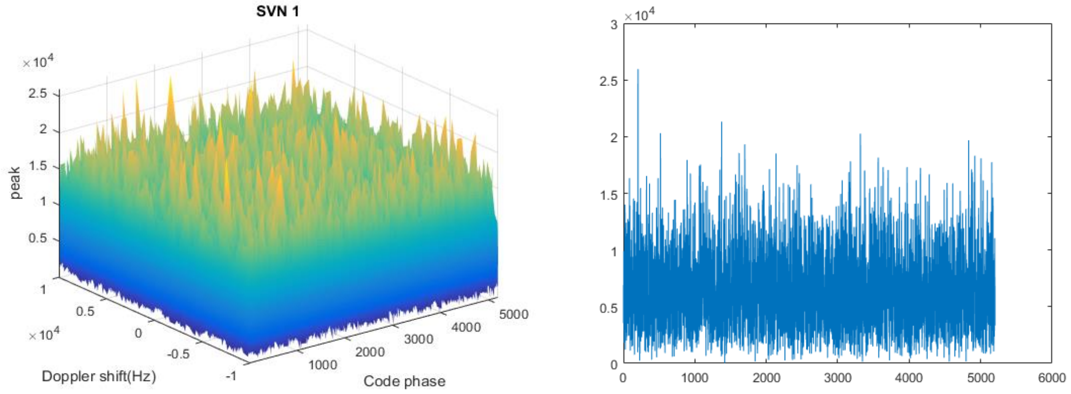

Fig. 3: The result of Beidou-1 acquisition.

2.5. The Improved Signal Acquisition Method

As figure 3 shown, such data cannot help us get the right information because of the actual signals contains noise signals. The easiest way is to take the square of result in the seventh step, because the noise signal is slower than the increased speed of the Beidou signal square. The result look as figure 4, the position of the maximum peak is code phase, the frequency corresponding to this sequence is the Doppler frequency.

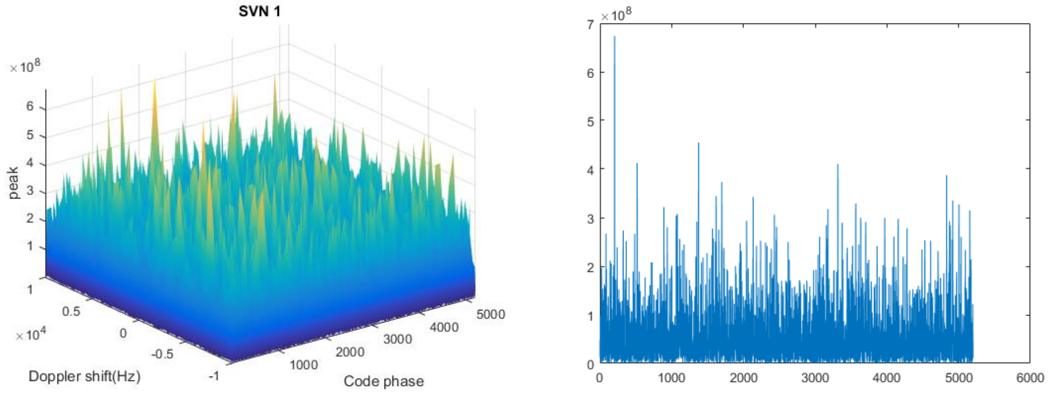

Fig. 4: The result of square.

However, the Beidou signals is weak at times, and contains NH code. We cannot use the traditional methods to judge satellites visibility, it need to use more time data [6]. In this paper, we use 2ms data to complete the acquisition weak signals acquisition. The improved steps are as follows.

Step 1: We need to read the 2ms data, and convert into another structure like the above first step.

Step 2: C needs to be converted into a new sequence in the above fourth step.

$$C' = C,0,0,0,0....0$$

where, compared with the length of C, the length of C' increase 1 times.

By doing so, we can see the maximum value more clearly. Comparison of two methods are as follows.

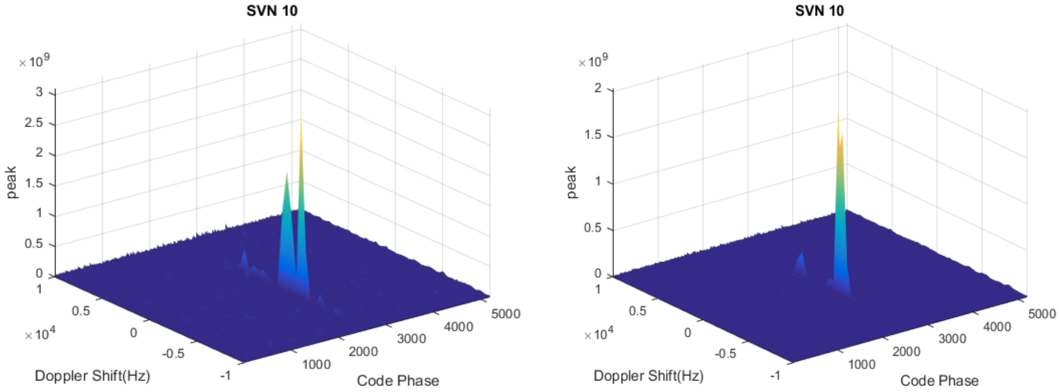

Fig. 5: The comparison of two methods.

where, the left of the graph is the result of the traditional method, and on the right is the result of the improved method. Compared with the traditional method, the improved method improves detection veracity.

2.6. Carrier Phase Tracking Loop

Through the acquisition unit, the tracking unit obtains the signal frequency and code phase. Now, the tracking unit can use the Doppler frequency shift and the code phase to initialize the single-channel tracking unit. In the tracking signal process, the tracking unit generally uses two loops: the code tracking loop and carrier tracking loop. Code phase tracking loop is generally achieved by the use of delay lock loop (DLL), when tracking the intermediate frequency signal or zero-IF signal, its implementation is similar, then carrier tracking loop is not similar. The tracking unit generates a local signal, then it is mixed with the received signal. This step will generate a high frequency signal and low frequency signal. The high frequency signal can be removed by correlation operation in the IF Receiver, this is equivalent to a filter. However, this process is very difficult in Zero-IF receivers, it needs a new method, such as reference [7]. This is shown in figure 6.

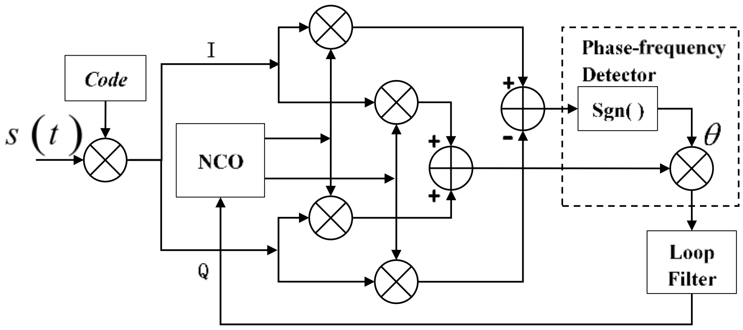

Fig. 6: Carrier Phase Tracking Loop.

In this figure:

$$\theta = p_{cross} sign(p_{dot})$$
$$p_{dot} = C_P * I * cos(t) - C_P * Q * sin(t)$$
$$p_{cross} = C_P * I * sin(t) + C_P * Q * cos(t)$$
$$phase\_error = sin(p_{cross} sign(p_{dot}))$$

where, Phase-frequency Detector used the function sign() to get acquire the symbolic of Pdot, cos(t) is the real part of local signal, sin(t) is the imaginary part of local signal. Cp is local Pseudo-code. The picture of phase_error might look like figure 7.

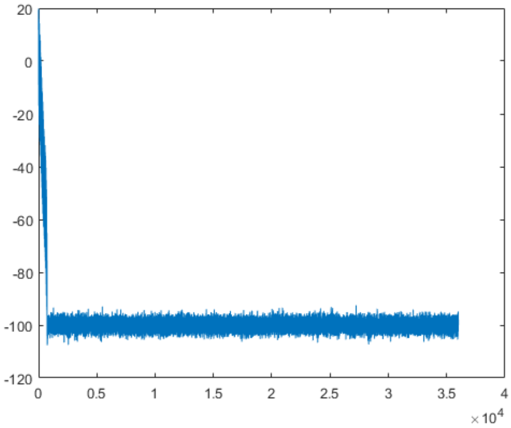

Fig. 7: The result of tracking loop.

3. Conclusions

In this work, we present a novel method for studying satellite signal processing. We designed the signal processing method and provided the main steps. Experimental results show that this method can achieve remarkable stability and sensitivity. Moreover, this method is different from the common method in that it used general equipment, not dedicated equipment, possibly allowing people to be more interested in this field.

4. Acknowledgements

I would like to thank the authors of these references, their work helped me understand the basic principles better. Thank my adviser and schoolmates for helping me to complete these experiments.

5. References

[1] M. Higginsonrollins, A.E. Rogers. Development of a Low Cost Spectrometer for the Small Radio Telescope (SRT), Very Small Radio Telescope (VSRT), and Ozone spectrometer. *American Astronomical Society*, 2014, pp.223.

[2] T.D. Vo-Huu, T.D. Vo-Huu, G. Noubir. Interleaving Jamming in Wi-Fi Networks. *ACM Conference on Security & Privacy in Wireless and Mobile Networks,* 2016, pp.31-42.

[3] K.B. Wu, L. Chen; C. Lv. Design and implementation of the verification platform for WBAN Baseband. *Application of Electronic Technique*, 2016, **42**(6):71-73, 80.

[4] F. Xie, J.Y. Liu, R.B. Li, S. J. Feng. A simultaneous multiple BeiDou signal acquisition algorithm for a software-based GNSS receiver. *Optik - International Journal for Light and Electron Optics*.2015, **127** (4):1607-1614.

[5] J. Leclere, C. Botteron, P.A. Farine. Improving the Performance of the FFT-based Parallel Code-phase Search Acquisition of GNSS Signals by Decomposition of the Circular Correlation. *International Technical Meeting of the Satellite Division of the Institute of Navigation*. 2012, **137**(1):1406-1416.

[6] Z. L. REN, C.Y. Chun, J. L. NIU. Research on BeiDou B1I Weak Signal Acquisition Algorithm Based on PMF-FFT. *Measurement & Control Technology*, 2015, **34**(10):15-18.

[7] Y.C. Deng, Q.Y. Chen, M.A. Lu, L.G. Shi, ZG Wang. Design of BPSK/QPSK Demodulator Based on Direct-conversion Zero-IF RF Integrated Chip. *Video Engineering*, 2015, **39**(1):54-59.