Realization of GPS Dynamic Hijacking Based on Software Radio

Zhihui Wang* and Fan Yang
School of physics and electronic information, Inner Mongolia Normal University, Hohhot, China

*Corresponding author: 20181102646@mails.imnu.edu.cn

Abstract. GPS positioning technology has a wide range of use scenarios, but due to the known characteristics of GPS signal open reception and modulation methods, many solutions can easily deceive GPS signals. Once this technology is abused in violation of regulations, it may cause major safety and property losses. In order to better study the anti-hijacking technology of PGS signals, this article starts with the generative dynamic hijacking of PGS, gives the implementation method based on software radio, and further learns the code phase and dopper between asynchronous hijacking and synchronous hijacking through software radio. The compensation calculation method of Leer frequency shift parameters, and verified the effect of the software radio's GPS dynamic hijacking implementation method through examples, and provide theoretical support for the design and improvement of future anti-hijacking systems.

Keywords: GPS, Dynamic hijacking, C/A code.

1. Introduction
The initial GPS was managed by the US Air Force for the US government. Although the military P code and the civilian C/A code were distinguished to meet both military and commercial needs, the initial GPS was mainly used in the military field [1]. In 2001, the U.S. military department first raised concerns about the possible deception of satellite navigation and began to pay attention to the insecurity of civil encryption [2], and proposed to change the existing GPS receiver to realize the identification of hijacked signals [3] Jon S. Warner et al. proved in 2002 that civilian receivers can be easily deceived by analog signals [4]. In 2018, Kexiong (Curtis) Zeng designed a deception system that can control the normal movement of vehicles at low cost. Facts have proved that the anti-interference problem needs to be solved urgently. Of course, some people in China have realized this problem a few years ago. In 2012, He Liang researched the design and implementation of GNSS deceptive jamming simulation system [5]. In 2013, Yan Zhanjie calculated the relevant parameters and mathematical models of retransmission GPS interference [6]. In 2019, Gao Yangjun and others summarized the development process of retransmission GPS deception and generative deception, and compared the data to draw a point of view: domestic retransmission The technical difficulty of GPS spoofing is lower than that of generative GPS spoofing, so the current level of development of forwarding GPS spoofing is better [7].
Nowadays, the emergence of problems such as the hijacking of drones, the disruption of normal driving routes of unmanned vehicles, and the interruption of the normal working status of some other GPS-based self-cruising devices have reminded us of the necessity of studying anti-hijacking technology. This is of great significance for protecting personal privacy and strengthening military technology research. Military p-code encryption performance is good, and civilian GPS does not involve the transmission of p-code, so this article only involves the hijacking of civilian C/A codes.

2. Dynamic hijacking realization process

2.1. The principle of hijacking

2.1.1. GPS signal composition. GPS operating satellites will send a spread spectrum ranging signal L1 modulated by Binary Phase Shift Keying (BPSK). The working frequency band is 1575.42MHz. Under the premise of ensuring sufficient power transmission, the smallest signal received on the surface of the earth is ensured. The signal power level is -160dbW. As well as the second ranging signal L2, the working frequency band is 1227.60MHz, and the minimum signal power level received on the earth's surface is -166dbW, which is used to support the user's dual frequency correction. In addition to the carrier, the GPS signal consists of two parts: pseudo-random noise code and navigation message data code.

2.1.2. Pseudorandom code. Pseudo-random code spread spectrum technology is the key technology of GPS signals, which has the advantages of improving the navigation and positioning accuracy of the system, enhancing the ability to resist electronic interference and extremely strong confidentiality. Pseudo-random codes have good autocorrelation characteristics and periodicity and cannot be copied.

2.1.3. Navigation message. Navigation message refers to a data code containing navigation information, which is the data basis for users to use GPS for navigation and positioning. Navigation information includes: P code exchange code determined by C/A code, time system, satellite ephemeris, satellite working status, satellite almanac, etc. The navigation message is a binary coded file, which composes a data frame according to a prescribed format and broadcasts it outwards according to the frame. Each frame of text is 1500 bits, and the transmission speed is 50 bits per second, so the propagation time of one frame of text is 30 seconds.

2.1.4. C/A code. The C/A code is used for coarse ranging and code division multiple access. Since the base code rate of the C/A code is 1.023MHz, the repetition period of the pseudo-random sequence can be calculated. \[ T = \frac{1023}{1.023 \times 10^6} = 1\text{ms} \]. The C/A code is a combined code obtained by multiplying two m-sequences with the same code length and code rate but different structures. It is also called a Gold sequence. As shown in the formula: \[ \frac{C}{A(t)} = G_1(t) \cdot G_2(t) \cdot (t + it_0) \]. Where \( G_1(t) \) and \( G_2(t) \) are two m-sequences with a period of 1ms and a code length of \( N = 2^{10} - 1 = 1023 \) bit generated by two shift registers.

Using different \( it_0 \) values corresponds to different \( G(t) \) codes, from which 32 codes are selected to name various GPS satellites as PRN1, PRN2...PRN32. The C/A code has good auto-correlation and cross-correlation characteristics, that is, when the phases are completely aligned, obvious correlation peaks can be generated. But there are some shortcomings. The C/A code has a short code length and is easy to capture. It can also be used to determine the propagation delay of satellite signals. For the C/A code with only 1023 symbols, if searching at a speed of 52 symbols per second, the search time only needs 20.5s.
2.2. Software radio realizes the advantages of each part of the function

Software radio takes digital signal processing as the core, hardware equipment as the platform, and realizes the process of radio sending and receiving, processing and communication through software programming. The calculation of related parameters and the switch between GPS static hijacking and dynamic hijacking can be easily realized by only modifying the corresponding commands. The software radio hardware backplane used in this solution is LimeSDR. The core part of LimeSDR is the LMS7002 chip, which is a programmable radio frequency integrated circuit that can support almost all communication standards.

The American scientist Conley rob proposed that in the GPS standard positioning service signal specification, the SPS receiver is used to compensate the Doppler effect of the C/A code and the phase of the nominal SPS ranging signal. In the implementation of the software radio platform, these configuration files can be used to generate analog pseudorange and Doppler parameters for the GPS satellites in the field of view, and the analog range data can be used to generate digital I/Q samples of the GPS signal. Whether it is a real satellite signal or a spoofed signal, the synchronization accuracy depends on the calculation and control accuracy of related signal parameters, as well as the accuracy of the time when the interference source controls the signal. The use of software radio greatly simplifies this process.

Compared with the primary interference, the satellite position and ephemeris data structure during the realization of the software radio platform are similar to the real satellite signal structure. After data compensation for Doppler shift and code phase, the deception signal is The correlation peaks of the real signal are approximately aligned, and the spoofing signal continuously strips off the correlation peaks of the real signal, and the probability of causing the satellite alarm to be locked is greatly reduced, so the deception effect is better.

By running LimeGPS written in C language, it can receive program input parameters, configure LimeSDR, start GPS simulation and launch tasks. Through the GPS_task configuration file, the navigation message is updated every 30 seconds, and the user parameters and channel allocation are read. Start GPS simulation task program gps_task and start data sending task program tx_task to open two important functions: read data and send to Lime device and realize the synthesis of baseband data. The GPS-SDR-SIM program generates a GPS baseband signal data stream, which can be converted to RF using a software-defined radio (SDR) platform.

3. C/A code Matlab simulation

In order to further prove the practicability of this experiment and related principles, the basic process design of GPS signal modulation and C/A code are used to verify the MATLAB tool. The relevant results are shown in the figure below.

Figure 1. M code auto-correlation and cross-correlation.
4. **Actual test and result analysis**

The location of the experimenter is the Shengle campus of Inner Mongolia Normal University. First complete the static hijacking test: when the mobile phone is in the real signal tracking state, the search threshold will become higher, so first, the mobile phone should be interfered with the normal reception of the satellite positioning signal by transmitting the interference source to make it enter the unlocked state. From the change from 3D fix to NO fix displayed in the GPS test, it can be known that the first step of GPS deception has been completed, that is, the phone successfully loses lock and enters the recapture state. Then use the software radio device LimeSDR to transmit the forged GPS signal, and observe that the 3D fix is redisplayed on the GPS test page, indicating that the mobile phone has successfully captured and sent the forged positioning signal. Switch to Baidu map to observe the location of the forged signal.

**Figure 2.** Sequence code to be sent after spreading.

**Figure 3.** Generated C/A code.

**Figure 4.** The display of the real GPS signal on the Baidu map and GPS test on the mobile phone.
Figure 5. The result of GPS hijacking.

It can be clearly seen that the GPS signal received by the mobile phone was successfully deceived in just over a minute. Through repeated experiments, it is believed that when the mobile phone is in flight state and WLAN positioning is disabled, the GPS dynamic deception effect is better and the time-consuming is shorter.

On the basis of static testing, we selected small drones as a means of displaying the effect of dynamic hijacking. In order to make the effect more intuitive, we added an LCD screen on the drone to display the latitude and longitude of the current position, and the continuity of the dynamic hijacking effect was displayed through the time parameter.

5. Conclusion
This article introduces the composition of GPS signals, uses Matlab tools to design the basic process of GPS signal modulation, masters the PRN sequence generation method and its basic characteristics, masters the basic principles and implementation methods of DSSS modulation and BPSK modulation, and successfully completed C/A code simulation. The static hijacking of PGS is realized through software radio, and generative dynamic hijacking is realized on the basis of static hijacking. The example verifies the effect of the GPS dynamic hijacking method of software radio, and provides theoretical support for the design and improvement of future anti-hijacking systems.

References
[1] Conley R ob. An Overview of the GPS Standard Positioning Service Signal Specification [C] // Proceedings of the 7th.
[2] Volpe J A. Vulnerability Assessment of the Transportation Infrastructure R elying on GPS [J]. International Workshop.
[3] on Algorithms Forwireless Mobile Ad Hoc & Sensor Net- works, 2001.
[4] Jos S.Warner, Ph.D. and Roger G. Johnston, Ph.d, cpp. GPS Spoofing Countermeasures.
[5] Warner J S, Johnston R G. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing [J]. Journal of Security Administration, 2002, 25 (2):19-27.
[6] He Liang. Design and implementation of GNSS deceptive jamming simulation system [D]. University of Electronic Science and Technology, 2016.
[7] Yan Zhanjie, Wu Dewei, Liu Haibo, et al. GPS forwarding deception jamming delay analysis [J]. Journal of Air Force Engineering University: Natural Science Edition, 2013, 14 (4): 67-70.
[8] Gao Yangjun, Lu Zhiwei, Zhou Pengjin, Jia Zhengyang, Zhang Lundong, Cong Dianwei. Status and prospects of satellite navigation deceptive jamming [J] Surveying and Mapping and
Spatial Geographic Information, Vol. 42 No. 10.

[9] Mark, Sun Xun, Nie Yuping. The key technology of GPS generative deception jamming [J]. Aerospace Electronic Warfare, 2014, 30 (6): 24-26.