Analysis of Spoofing Influence of GNSS

Jing Pang[1,a] , Shaojie Ni[1,b], Junwei Nie[3,c]

[1] College of Electronic Science and Engineering, National University of Defense Technology, Changsha, China

[a]pangjing@sina.com, [b]n_s_j@sina.com, [c]njw_nnc@126.com

Keywords: GNSS; spoofing; induction; anti-spoofing

Abstract. Spoofing is an important threat to present satellite navigation equipment; and the research on spoofing technology is the basis of the anti-spoofing technology. According to the principle of spoofing, this paper analyzes constraints on timing receivers and navigation receivers. The analysis results show that spoofing sources cannot spoof the timing and navigation receivers at the same time.

Introduction

Global Navigation Satellite System (GNSS) has been widely used in the civil-military fields. However, because signals reaching the ground are weak and the civilian signal format is open, GNSS is susceptible to spoofing [1].

Spoofing is a human intervention; it let the receiver trace spoofing signals by launching ones, which are same or similar with real satellite signals, resulting in wrong information on time or location [2]. Compared with the traditional suppressed spoofing which mainly is power covering type, the spoofing has greater harm. To successfully suppress spoofing will lead failures in attacked targets' positioning or timing; and then alternate navigation methods will be enabled. The target receivers attacked by spoofing are often unaware of being attacked, and they continuously output wrong positioning or timing results, thus leading missiles to attack incorrect targets, or causing paralysis on social and civil infrastructures, such as power systems, bank systems and finance systems, wireless communication systems etc. [3].

Spoofing has gradually become a potential threat to satellite navigation equipment; therefore, research on spoofing protection schemes of navigation equipment has become a hotspot. Research on spoofing mechanism helps to understand vulnerabilities of navigation equipment and develop anti-spoofing policies, which are the foundation of research on anti-spoofing technology.

This paper analyzes the influence of spoofing on a receiver, so as to realize constraints in spoofing on navigation or timing receivers.

Principle of spoofing

Location principle of a GNSS receiver is to also receive signals from four or over four satellites' signals, combining and solving formulas are made by measuring the pseudo-distance of every satellite signal to a receiver; positioning coordinates (x, y, z) and clock offsets information of a receiver can be obtained. Error pseudo-distance is measured by spoofing GNSS receivers, and then the wrong positioning or timing results are obtained.

This paper describes the principle of typical spoofing; if taking 4-satellite location for example, spoofing schematic is as shown in Figure 1, because the spoofing source located at point S transmits spoofing signals, which cheat the target receiver located at point A to a virtual point B [4]. In the conditions of spoofing, the target receiver receives signals from satellites and sources of interference simultaneously; however, interference signals play a dominant role, the influence of satellite signals is ignored when analyzing.

Spoofing is performed as follows:

(1). The interference source located at point S receives signals from 4 real satellites (G1, G2, G3 G4), and pseudo-distance (r_{S1} , r_{S2} , r_{S3} , r_{S4}) can be obtained;

(2). The interference source separates each channel's signals by spatial filtering or related methods; time delay adjustment can be made to signals of each channel according to the appropriate algorithm, and then these signals are emitted by antennas;

(3). The target receiver is located at point A receives spoofing signals, and obtains pseudo-distance-distance (r_{B1} , r_{B2} , r_{B3} , r_{B4}), which is used to calculate positioning results, serving as the coordinate (x_B,y_B,z_B) of point B.

It can be seen that spoofing lies in the channel separation and calculation of time delay adjustment of every channel signal.

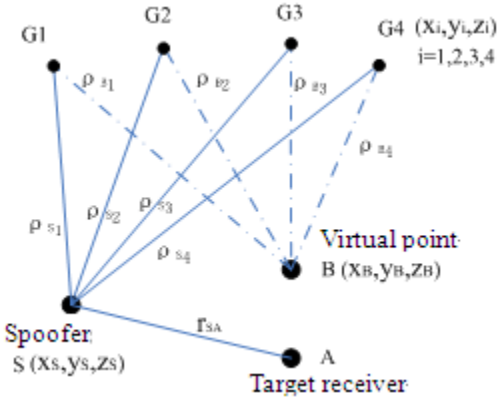

Figure 1 Block diagram of the spoofing system

Theoretical analysis

Pseudo-distance adjustments of every channel are set as $(\Delta r_1 , \Delta r_2 , \Delta r_3 , \Delta r_4)$; the distance between a jammer and a target receiver is r_{SA}, and their timing results are τ_S and τ_A respectively; the timing result of the receiver after being spoofed is τ_B. Pseudo-distance measured by the target receiver can be expressed as the follows according to Figure 1:

$$r_{Bi} = r_{Si} + \Delta r_i + r_{SA}, i=1,2,3,4 \quad (1)$$

Pseudo-distance adjustment is calculated by:

$$\Delta r_i = r_{Bi} - r_{Si} - r_{SA}, i=1,2,3,4 \quad (2)$$

Positioning formulas (3) and (4)

$$r_{Bi} = \sqrt{(x_B - x_i)^2 + (y_B - y_i)^2 + (z_B - z_i)^2} + Ct_B, \ i=1,2,3,4 \quad (3)$$

$$r_{Si} = \sqrt{(x_S - x_i)^2 + (y_S - y_i)^2 + (z_S - z_i)^2} + Ct_S, \ i=1,2,3,4 \quad (4)$$

(4) are substituted into the formula (2), it can obtain:

$$\Delta r_i = \sqrt{(x_B - x_i)^2 + (y_B - y_i)^2 + (z_B - z_i)^2} - \sqrt{(x_S - x_i)^2 + (y_S - y_i)^2 + (z_S - z_i)^2} - r_{SA} + C(t_B - t_S), \ i=1,2,3,4 \quad (5)$$

Where C is the velocity of light; coordinates of the spoofing source S and the virtual point B are known, the coordinates of all satellites are transferred to the users' receivers via satellite signals in the form of navigation message. Therefore, coordinates are known to receivers. It is given in the condition of normal position, timing results of the interference source and the receiver are $\tau_S=\tau_A$,, and then the timing result is changed to $\Delta t = t_B - t_A$, the formula (5) is expressed as:

$$\Delta r_i - C\Delta t = r_{BGi} - r_{SGi} - r_{SA}, \ i=1,2,3,4 \quad (6)$$

Where r_{BGi} is the distance between the virtual point B and the satellite G_i, and r_{SGi} is the distance between the interference source S to the satellite G_i; the distance between the point S and the point A is unknown.

It can be seen from the formula, if there are no constraints on the pseudo-distance adjustment and the timing result change $\Delta\tau$, there will be infinite number of solutions, which can satisfy the formula. If

the timing result changes need to be calculated, coordinates of the interfered target point A must be obtained.

Analysis of the spoofing conditions

In the actual spoofing scenarios, the formula solutions need to be restricted according to physical realizability and some anti-spoofing test measures, which may be adopted by receivers. The following is the analysis of realizability under various constrain conditions.

The transmitting spoofing doesn't do code-related process on signals, only make delayed forwarding on them; negative delay is physically impossible. Therefore, the constraint condition to realize transmitting spoofing is $(\Delta r_i)_{min} > CT$, where T is the processed time delay of the signal transmitting, substituted into the formula (6) to get:

$$\Delta t > T + \frac{r_{SA}}{C} + r_{SGi} - r_{BGi} \quad (7)$$

, i=1,2,3,4

It can be seen from the formula (7) that the timing errors are related with the transmitting process time delay T, the transmitting distance r_{SA} and the layout of the spoofing system. Although the appropriate satellite can be chosen to reduce the timing error when transmitting [5], the timing results will have greater jumping, which is inevitable to the transmitting spoofing. It is known the spoofing method of signal pseudo-code, interference signals can be reconstructed based on signal parameters, and the process of negative time delay of signal channel can be realized.

Timing and navigation receivers are the major objects to spoofing targets; they correspond to static and dynamic goals respectively. Most timing receivers are installed in fixed positions and have known accurate coordinates; receivers will adopt means to monitor signal integrity for position verifying, namely comparing real-time positioning results of receivers with the known coordinates. If obvious position drift is founded, the current received signals can be judged to be abnormal, and the autonomous timekeeping mode can be transferred [6]. Hence, aiming at the spoofing of the timing receiver, the constraint condition is the positioning result is unchanged after being deceived, namely the point A has same coordinates with those of the point B.

Coordinates of the interfered target point A need to know at first when spoofing, which means interference can be conducted only to a single target. The A coordinate is substituted into the formula (6), because the straight line distance between the satellite G_i and the interfered target point A is smaller than the distance, from the satellite to the point S interference source and then being transmitted, the result of the formula (8) is less than zero.

$$\Delta r_i - C\Delta t = r_{AGi} - r_{SGi} - r_{SA} < 0 \quad , \text{ i=1,2,3,4} \quad (8)$$

Drift begins from $\Delta\tau = 0$ gradually when spoofing, the sole solution of Δr_i can be obtained according to the value of $\Delta\tau$. The interference source is laid out in the distance, and the spoofing effect is the positioning results of the timing receiver remain the same; the timing results are drifted gradually from the true values. It is not easy to be detected.

Generally, the navigation receiver is in motion, there are infinite number of solutions to every channel's pseudo-distance adjustments and changes of the timing results according to formula (6). If considering assistant anti-spoofing measures of inertial sensors etc., changes in positioning and timing results after spoofing are in a smaller range, in order not to alert the target receiver; it requires exerting interference to a single target. There are two kinds of principles, one is to get three dimensional location coordinates and speed of the interfered target antenna in far distance, detect aircraft tracks through a radar system as literature [7], as well as carefully calculate and adjust spoofing PVT calculation results; another is to cheat the interference source to adjoin the interfered target, even directly be placed on the target receiver antenna in card like size, using the received satellite signals for location calculation and pseudo-distance adjustment [8].

Analysis of spoofing influence

Researches on GPS spoofing in China mainly focus on the spoofing based on signal transponders. Forward spoofing does not need to know signals' format and pseudo code; its biggest advantage is to avoid decrypting the military codes. Due to sensitivity of the technique, few literatures on forward spoofing have been published abroad.

Literature [9] presented a time delay control of interference signals on distributed transponders, decoying the forward spoofing system of GPS-guided weapons. Literatures [10-12] researched some topics, including decoy-delay algorithm, regional mapping influence factors, inducing performance and system platform optimization array etc. However, these researches are still in the theoretical and simulation stages.

Because the forward spoofing amplifies and forwards, and does not need to know pseudo codes; the time delay for signals reaching the target receiver must be greater than that of the true signals to reach the target receiver; therefore, there are some inherent problems.

(1). Receiving antennas need to adopt smart antenna array or directional antennas which can automatically track satellite signals; separate several satellites' signals via spatial filtering techniques; moreover, restrict application of price and volume;

(2). Received satellite signals are of low power, and transmitted signals are of high power and with exactly same signal format; transmitting and isolation are the difficulties;

(3). Signals are magnified and transmitted along with the receiving noise when forwarding, noise base of the target receiver will be raised, easy for detecting;

(4.) The attacked target timing results will jump based on the preceding analysis, easy for detecting;

(5). The time delay is difficult to be controlled in a chip time, and it is not easy to penetrate the tracking loop of attacked targets; so that time delay needs to be used together with suppress interference.

Conclusions

In summary, spoofing is easy to implement for receivers without adopting anti-spoofing measures. There are a number of successful samples. If considering receivers' anti-spoofing measures, there are some restrict conditions imposed on spoofing conditions; spoofing has many technical difficulties. Spoofing and anti-spoofing is a pair of "spear" and "shields"; good spoofing means can improve the anti-spoofing cost of receivers.

References

[1]. GAO Yang, LI Hong, LU Mingquan , FENG Zhenming ,. Intermediate Spoofing Strategies and Countermeasures[J], TSINGHUA SCIENCE AND TECHNOLOGY 2013, 18(6): 599-605.

[2]. AliJafarnia-Jahromi, AliBroumandan, JohnNielsen,G´erardLachapelle. Gps Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques[J], International Journal o fNavigation and Observation 2012, 2012: 1-16.

[3]. Daniel P.Shepard, Jahshan A.Bhatti, Todd E.Humphreys. Evaluation of Smart Grid and Civilian Uav Vulnerability to Gps Spoofing Attacks [C]//ION GNSS,2012.

[4]. WANG Wei, Tao Yie-rong, WANG Guo-yu, CHEN Yong-guang Study and Simulation of GPS Deception Jamming[J], Fire Control & Command Control 2009, 34(6): 115-118.(in Chinese)

[5]. YAN Zhanjie, WU Dewei, LIU haibo, MAO hu Analysis of Time-delay in GPS repeater Deception Jamming[J], Journal of Air Forece Engineering University 2013, 14(4): 67-70. .(in Chinese)

[6]. HUANG Long , GONG Hang , ZHU Xiangwei , WANG Feixue,Research of re-radiating spoofing technique to GNSS timing receiver[J], Journal of National University of Defense Technology, 2013, 35(4): 93-96. (in Chinese)

[7]. ZHANG Huisuo , GAOGuangen , KOULei , GU Chao, Deceptive Jamming Technology of GPS Based on the Track Induction Method[J], Journal of Projectiles , Rockets , Missiles and Guidance ,2013, 33(3): 149-152. (in Chinese)

[8]. Todd E. Humphreys, Brent M. Ledvina, Mark L.Psiaki, Brady W.O'Hanlon, Paul M.Kintner. Assessing the Spoofing Threat [C]//ION GNSS,Savannah,2008: 2314-2325.

[9]. A Jamming System Through Section Mapping for GPS Navigation[J], Acta Electronica Sinica, 2005, 33(6): 1036-1038. (in Chinese)