Position and time deception based on satellite navigation technology and experimental verification

Zongmin Liu¹, Guangming Wang¹, Jun Yang¹, Chao Zhou¹) and Chao Ma¹

Abstract Due to the characteristics of open system and weak signal power of satellite navigation signal, it is very easy to be affected by navigation deception and other interference. At present, most studies divide the influence of deception signal on the receiver into two independent aspects: positioning and timing. There is a lack of research on accurately controlling the positioning and timing of the receiver in the process of deception. In this paper, the principle of accurately controlling positioning and timing in navigation deception are analyzed, three deception scenarios are proposed and verified by experiments. The experiments show that: 1) it is feasible to introduce a step or linear position deviation to the receiver without excessively affecting the timing results; 2) it is feasible to introduce a step or linear time deviation to the receiver without excessively affecting the positioning results; 3) it is feasible to perform position spoofing and time spoofing on the receiver at the same time, the positioning results of the receivers were successfully pulled off by 1.5m. 

key words: Navigation spoofing, commercial receiver, position deception, time deception

Classification: Circuits and modules for electronic instrumentation

1. Introduction

With the construction of global navigation satellite system and the great progress of receiver technology in low cost and low power consumption[1-4], the all-weather and high-precision positioning and timing services are widely used in production and life[5,6]. However, due to the weakness of satellite navigation signal and the disclosure of data format, the receiver is vulnerable to jamming and spoofing [7-10]. In order to improve the anti-interference performance of the receiver, many researchers have given solutions by different technical means, such as adding array antenna[11], integrated circuit design[12], and et.al[13]. Compared with the jamming effect that making the receiver unable to work, spoofing can make the receiver output wrong positioning and timing results, which is more threatening and harmful[14-17]. At present, there are many researches in the field of anti-spoofing, which are conducive to improve the security of the receiver[18-21]. This paper focuses on navigation spoofing.

In the previous study, the impact of spoofing signals on receivers is divided into two independent aspects: position and time, which are mainly for position sensitive devices: UAV[16], car[22] and ship[23], and time sensitive systems such as smart grid and financial transaction system[24-26].

As a navigation receiver manufacturer, it is necessary to have a deeper understanding of the navigation spoofing position and time mechanism to provide users with better and intact navigation and positioning services. This paper analyzes the principle and possibility of precise control of position and time in navigation spoofing, and conducts experimental verification of the theory. The experimental results show that it is possible to accurately control the position and time of the receivers.

2. Navigation deception principle and system model

2.1 Receiver positioning and timing principle

Pseudorange is one of the most basic measurements in GNSS, and the pseudorange measurement of multiple visible satellites is the key to realize receiver positioning and timing [27]. The process for the navigation receiver is shown in Fig. 1. Take GPS as an example, the digital signal processing unit in the receiver carries out the process of capture, tracking, word and frame synchronization. We can get the launch time of the navigation signal \( t_i(\text{m} - \tau_i(t)) \) (The subscript i represents the clock time of satellite i, \( \tau_i(t) \) represents the propagation delay), satellite orbit parameter, satellite clock error and atmospheric delay (including ionospheric delay \( I_n(t) \) and tropospheric delay \( T_n(t) \)). The reception time \( \tau_n(t) \) can be obtained by multiplying the difference between the signal transmitting time \( t_i \) and receiving time \( t_n \) and the speed of light \( c \).

---

¹ College of Intelligence Science and Technology, National University of Defense Technology, No. 109, Deya Road, Changsha 410073, China
a) zhouchaowhu@126.com

DOI: 10.1587/elex.18.202010366
Received August 28, 2021
Accepted September 21, 2021
Publicized October 04, 2021

IEICE Electronics Express, Vol. xx, No. xx, xx-xx
Because the satellite clock and receiver clock are not consistent with the system time (GPST), there are ionospheric error, tropospheric error, multipath effect, receiver noise and other factors, the pseudorange observation equation is as follows:

$$\rho_i = c(t_i - t_0) = \tau_i + c(\delta t_s - \delta t_i) + I_{on} + T_{ro} + \varepsilon_\rho$$ \hspace{1cm} (1)

Where \(\tau_i\) represents the true geometric distance between satellite \(i\) and the receiver, \(\delta t_s\) and \(\delta t_i\) represent the clock difference of satellite \(i\) and receiver clock relative to system time (GPST), respectively. \(c\) is the speed of light. \(I_{on}\) and \(T_{ro}\) represent ionospheric and tropospheric errors, and \(\varepsilon_\rho\) is for the other unconsidered error terms. Among the error terms of the pseudorange observation equation, satellite clock error \(\delta t_s\), atmospheric delay parameter \(I_{on}\) and \(T_{ro}\) can be obtained by navigation message and mathematical model, and the corrected pseudorange measurement value can be expressed as:

$$\rho_{ei} = \rho_i + c \cdot \delta t_s - I_{on} - T_{ro}$$ \hspace{1cm} (2)

According to the above equation, except for error term \(\varepsilon_\rho\), the corrected pseudorange measurement value \(\rho_{ei}\) only includes the geometric distance \(\tau_i\) between the satellite and the receiver and the clock difference \(\delta t_i\) of the receiver. Satellite position \(p_i(t)\) can be obtained by calculating orbit parameters, so there are only four unknown parameters in the pseudorange equation, namely the three-dimensional position \(p_i(t) = (x, y, z)^T\) and the clock difference \(\delta t_i\). When no less than four sets of pseudoranges can be obtained, positioning and timing can be achieved by solving the pseudorange equations. Taking four visible satellites as an example, the pseudorange equations are shown as follows:

$$\begin{bmatrix}
\rho_{1}(t) \\
\rho_{2}(t) \\
\rho_{3}(t) \\
\rho_{4}(t)
\end{bmatrix} = 
\begin{bmatrix}
p_{1}(t) - p_{1}(t - \tau_{1}(t)) \\
p_{2}(t) - p_{2}(t - \tau_{2}(t)) \\
p_{3}(t) - p_{3}(t - \tau_{3}(t)) \\
p_{4}(t) - p_{4}(t - \tau_{4}(t))
\end{bmatrix} + c
\begin{bmatrix}
\delta t_s \\
\delta t_s \\
\delta t_i \\
\delta t_i
\end{bmatrix} +
\begin{bmatrix}
\varepsilon_1 \\
\varepsilon_2 \\
\varepsilon_3 \\
\varepsilon_4
\end{bmatrix} \hspace{1cm} (3)$$

2.2 Principles of Navigation Spoofing

Navigation spoofing principle is that the spoofing signals occupy the tracking loop of receiver by power advantage, which makes the receiver carry out position and timing calculation corresponding to the spoofing signals[28]. According to the way of signal generation, navigation spoofing can be divided into generative spoofing and meaconing[17,29]. We only discuss generative spoofing in this article.

The core of the navigation spoofing device is the GNSS simulator[30], which can generate high fidelity spoofing signals. The general composition of the generative spoofer is shown in Fig. 2, including the receiving antenna, embedded receiver, navigation signal simulator, power amplifier and transmitting antenna. The receiving antenna and embedded receiver are used to synchronize the real-time ephemeris and time so that the spoofer is synchronized with the current navigation constellation. Under the guidance of the spoofing strategy, the navigation signal simulator generates spoofing signals according to the ephemeris and time reference information calculated by the embedded receiver, and then the spoofing signals are amplified by the power amplifier and transmitted by the directional transmitting antenna.

The working principle of the spoofer is shown in the Fig. 2, which including three main modules: time synchronization module, delay calibration module and signal generation module. The time synchronization module refers to the clock taming unit that can output a high-precision time reference, the main purpose of which...
is to synchronize the spoofing device with the GPS time [27]. In addition, it also takes on the functions of navigation message resolution and ephemeris acquisition. The function of the delay calibration module is to ensure that the phase of the transmitted spoofing signal is consistent with the real signal at the spoofing target, so as to improve the spoofing success rate [31]. The function of the signal generation module is to generate spoofing signals consistent with real signals through mathematical simulation and digital signal generation [32]. The following will be analyzed around mathematical simulation.

Because the pseudorange measurement determines the positioning and timing results of the receiver, accurate imitation of the pseudorange is the key to navigation spoofing. Under the condition that the satellite ephemeris is not changed, the pseudorange simulation process for a given spoofing position is as follows:

The spoofing location is \( p_s(t) = (x_s', y_s', z_s')^T \). The position \( p_i(t) = [x_i(t), y_i(t), z_i(t)]^T \) of satellite \( i \) can be calculated by ephemeris, ionospheric delay \( I_{in}(t) \) and tropospheric delay \( T_{tn}(t) \), then the corresponding pseudorange \( \rho_i(t) \) and modified pseudorange \( \rho'_i(t) \) can be expressed as [27]:

\[
\rho'_i(t) = \|p'_i(t) - p_i(t - \tau'_i(t))\|_2 + c \cdot [\delta I_i(t) - \delta t_i(t)] + T_{tn}(t) + \varepsilon_i \quad (6)
\]

\[
\rho_i(t) = \|p'_i(t) - p_i(t - \tau'_i(t))\|_2 + c \cdot \delta I_i(t) + \varepsilon_i
\]

The propagation delay \( \tau'_i(t) \) can be calculated by the receiving time \( t \) and spoofing position \( p'_i(t) = (x_s', y_s', z_s')^T \) inversely:

\[
\tau'_i(t) = \frac{\|p'_i(t) - p_i(t - \tau'_i(t))\|_2}{c} + [I_i(t) + T_{tn}(t) + \varepsilon_i(t)] \quad (7)
\]

The ionospheric and tropospheric delay are relatively stable, and the receiving time can be calculated directly. We only need to iteratively solve the geometric distance \( \|p'_i(t) - p_i(t - \tau'_i(t))\|_2 \) and the specific steps are as follows ([k] is the number of iterations, \( k = 0,1,2,\ldots \)) [32]:

The first iteration, the propagation delay \( \tau'_i(t)[0] \) is assumed to be zero, that is, the position of the satellite at the time of signal transmitting is the position at the time of signal receiving, then the initial geometric distance can be expressed as \( r_i(t)[0] \):

\[
r_i(t)[0] = \|p'_i(t) - p_i(t)\|_2 \quad (8)
\]

\( \tau'_i(t)[k] \) iteration:

\[
\tau'_i(t)[k] = r_i(t)[k-1]/c \quad (9)
\]

\( \tau'_i(t)[k] \) iteration:

\[
r_i(t)[k] = \|p'_i(t) - p_i(t - \tau'_i(t)[k])\|_2 \quad (10)
\]

Repeat steps (2) and (3) until

\[
|r_i(t)[k] - r_i(t)[k-1]| < \varepsilon_i \quad (11)
\]

The determination of the iterative convergence threshold \( \varepsilon_i \) can be selected according to the accuracy requirements. Meanwhile, the iterative process also requires the backtracking of the satellite position and ionospheric and tropospheric delay models. Due to the relative motion of satellite and the spoofing target, the carrier frequency of the actually received navigation signal will have a certain deviation. Therefore, besides the calculation of the pseudorange of the signal, it is also necessary to calculate the carrier doppler [33].

3. Experimental platform construction

Based on the establishment of the indoor navigation environment, which can complete the amplification and real-time forwarding of the outdoor real signal, we combined the existing equipment to build a complete set of spoofing experiment platform indoors, which is shown in Fig. 3. The Receive antenna 1 provides the satellite ephemeris and time reference for the deception device, and the Receive antenna 2 provides the real navigation signal for the receiver under test (from the indoor transponder); The PC communicates with the deception device through the network port to set the deception strategy (such as position deviation and time deviation) and control the deception signal, at the same time connect with the receiver through the serial port to record the observation data; The output of the spoofing signal and the input of the receiving antenna 2 are combined first, and then output to the receiver after the power divider (when the spoofing signal switch is turned off, it is the normal positioning state, when the spoofing signal is turned on, it is the spoofing state); different receivers The 1PPS output and the time reference (provided by the timing receiver of the time synchronization unit in the spoofing device) are input to the oscilloscope for real-time detection of the influence of the spoofing signal on the time output of the receiver.

The receivers tested are u-blox-LEA-M8T, Unicorecomm-UB4B0 and NovAtel-OEM628LE, the oscilloscope used is KeySight's DSO4404A, and the connection diagram of each channel is shown in Fig.

\[
\tau'_i(t)[k] = r_i(t)[k-1]/c \quad (9)
\]

\( \tau'_i(t)[k] \) iteration:

\[
r_i(t)[k] = \|p'_i(t) - p_i(t - \tau'_i(t)[k])\|_2 \quad (10)
\]

Repeat steps (2) and (3) until

\[
|r_i(t)[k] - r_i(t)[k-1]| < \varepsilon_i \quad (11)
\]

The determination of the iterative convergence threshold \( \varepsilon_i \) can be selected according to the accuracy requirements. Meanwhile, the iterative process also requires the backtracking of the satellite position and ionospheric and tropospheric delay models. Due to the relative motion of satellite and the spoofing target, the carrier frequency of the actually received navigation signal will have a certain deviation. Therefore, besides the calculation of the pseudorange of the signal, it is also necessary to calculate the carrier doppler [33].

3. Experimental platform construction

Based on the establishment of the indoor navigation environment, which can complete the amplification and real-time forwarding of the outdoor real signal, we combined the existing equipment to build a complete set of spoofing experiment platform indoors, which is shown in Fig. 3. The Receive antenna 1 provides the satellite ephemeris and time reference for the deception device, and the Receive antenna 2 provides the real navigation signal for the receiver under test (from the indoor transponder); The PC communicates with the deception device through the network port to set the deception strategy (such as position deviation and time deviation) and control the deception signal, at the same time connect with the receiver through the serial port to record the observation data; The output of the spoofing signal and the input of the receiving antenna 2 are combined first, and then output to the receiver after the power divider (when the spoofing signal switch is turned off, it is the normal positioning state, when the spoofing signal is turned on, it is the spoofing state); different receivers The 1PPS output and the time reference (provided by the timing receiver of the time synchronization unit in the spoofing device) are input to the oscilloscope for real-time detection of the influence of the spoofing signal on the time output of the receiver.

The receivers tested are u-blox-LEA-M8T, Unicorecomm-UB4B0 and NovAtel-OEM628LE, the oscilloscope used is KeySight's DSO4404A, and the connection diagram of each channel is shown in Fig.
7(b): channel 1 is connected to the reference clock output (yellow line), channel 2 is connected to u-blox-LEA-M8T (green line), channel 3 is connected to Unicorecomm-UB4B0 (blue line), and channel 4 is connected to NovAtel-OEM628LE (red line). The time deviation of the receiver is obtained by using oscilloscope to measure the phase difference between the 1PPS rising edge of the receivers (from channel 2,3,4) and the reference clock (channel 1, which is considered relatively stable), the position deviation of the receivers are obtained by the differences between the positioning data reported from the receivers and their position results in the first second of the experiment.

![Fig. 3 Photos of the experimental platform. (a) The physical connection diagram of the field experiment. (b) Connection of each channel of the oscilloscope.](image)

4. Experimental verification

4.1 Experiment of Position Deception under Time Invariant Condition

There are two methods for position deception: step position deviation (SPD) and linear position deviation (LPD). SPD means applying an instantaneous position offset to receiver by directly transmitting the deception signal corresponding to the preset deception position, while LPD refers to the method that deviating the position of the receiver in a constant speed from its original position to the preset deception position. We release the spoofing signal at the 40s and keep it on until the end in all experiments this paper.

We conducted experiments with position deviation value of 15m through SPD and deviation speed of 1m/s through LPD, which are shown in Fig. 4. The curves of different colors with circle markers respectively represent the location shift and time shift of different receivers during the whole experiment; the dotted line indicates the location shift corresponding to the selected deception method (Subsequent experiments all use this representation).

![Fig. 4 Experiment of position deception under time invariant condition. (a-b) The location/time shift of receivers under a position deviation value of 15m. (c-d) The location/time shift of receivers under a position deviation speed of 1m/s.](image)

The above experiment shows that the receivers’ location shift can always converge to their ideal curves, though Unicorecomm-UB4B0 and u-blox-LEA-M8T acted slowly in Fig. 4(a). However, it’s worth noting that the timing result of the receiver hardly changed, which shows that position deception under time invariant condition is feasible.

4.2 Experiment of time deception under position invariant condition

Similar to the methods of position deception, there are also two methods for time deception: step time deviation (STD) and linear time deviation (LTD). STD means
applying an instantaneous time offset to receiver by adding a step delay to all signal channels in the spoofing device, while LTD refers to the method that deviating the time of the receiver in a constant speed by adding a linear delay. We conducted experiments with time deviation value of 50ns through STD and deviation speed of 30ns/s through LTD in Fig. 5, the dotted lines indicate the ideal time shift of receivers under selected time deception method.

The above experiment shows that the receivers can always converge to their ideal curves in a short time (less than 20s) under a time deviation value of 50ns, the position result of the receivers hardly changed (less than 8m); their time shift fit well around the ideal curves under a time deviation speed of 30ns/s. while the receivers’ positioning result produced a change with an amplitude less than 20m, but it stabilized in the subsequent process. The above experiment also proved that receiver can be introduced into an arbitrary time shift without obviously affecting its position output in the position deception method of LTD.

4.3 Experiment of position deception under time variant condition

On the basis of 4.1 and 4.2, the position deception under the condition of time invariance and the time deception under the condition of position invariance have been strongly confirmed. In fact, it is also possible to control the deception of both at the same time.

Taking the simultaneous SPD and STD on the receiver as an example, we have carried out the corresponding experimental verification, as shown in Fig. 6(a-b). In the 40s of the experiment, a spoofing signal with a position deviation of 15m and a time deviation of 50ns was introduced, and it was maintained until the end of the experiment. It can be seen that the positioning and timing results of the three receivers were successfully deceived in the final stage of the experiment, which proves that position deception under time variant condition is feasible.

In order to make the receivers’ positioning and timing results produce a larger-scale deviation at the same time, we synchronously carried out experiment with position deviation speed of 1m/s in LPD and time deviation speed of 10ns/s through LTD in Fig. 6(c-d), both the Location Shift curves and Time Shift curves are quickly converged to their corresponding ideal curves, and maintain good linear trend. Finally, the positioning results of the receivers were successfully pulled off by 160m, and their timing results were pulled off by 1.5μs at the same time. The experimental results in this section show that it is feasible and controllable to perform time spoofing and position spoofing on the receiver at the same time.

5. Conclusions

Aiming at the problem of insufficient research on the relationship between position deception and time deception and lack of experimental verification, theoretical analysis and experimental verification are carried out in this paper. An experimental platform was built and the theoretical part was verified. The experimental results show that: Under the proposed deception strategy, our deception equipment successfully achieved the ideal deception effect in three spoofing
scenarios.

Since the focus of this paper is to analyze the effect of deception on the positioning and timing results of the receiver, it weakens the analysis of the deception success conditions. In fact, this is affected by many factors, such as deception signal power, receiver type, etc. In the next step, we will consider how to conduct integrated controllable deception research based on location and time on the basis of ensuring the success rate of deception.

References

[1] Y. L., et al.: “Development of a GNSS-IR instrument based on low-cost positioning chips and its performance evaluation for estimating the reflector height,” GPS Solutions, vol. (2021) Vol.25, no. No.4 (DOI: 10.1007/s10291-021-01163-6).

[2] Y. Wang, et al.: “A RF CMOS GNSS receiver with a passive mixer for GPS L1/Galileo E1/Compass B1 band,” IEICE ELECTRONICS EXPRESS, vol. 15 (2018) 20180551 (DOI: 10.1587/exle.15.20180551).

[3] Y. Yin, et al.: “A 48-dB precise decibel linear programmable gain amplifier for GNSS receivers,” IEICE ELECTRONICS EXPRESS, vol.11 (2014) (DOI: 10.1587/exle.11.20140940).

[4] X. Qi, et al.: “A novel CMOS active polyphase filter with wideband and low-power for GNSS receiver,” IEICE Electronics Express, vol. Vol.13, no. No.7 (2016) (DOI: 10.1587/exle.13.20160158).

[5] David Pallier, et al.: “Energy-Efficient GPS Synchronization for Wireless Nodes,” IEEE Sensors Journal, vol. Vol.21, no. No.4 (2021) 5221-5229 (DOI: 10.1109/jsen.2020.3031350).

[6] J. B. Zielinski, et al.: “High precision GNSS—prospects for science and applications(Conference Paper),” Lecture Notes in Geoinformation and Cartography (2018) 5-13 (DOI: 10.1007/978-3-319-6218-6_1).

[7] C. Bonebrake, et al.: “Attacks on GPS Time Reliability,” IEEE Security & Privacy, vol. 12, no. 3 (2014) 82-84 (DOI: 10.1109/MSP.2014.40).

[8] W. Kasper, et al.: “GPS Vulnerability Testing: Jamming and Interference,” GPS World, vol. Vol.15, no. No.5 (2004) 20-27.

[9] T. Otsuama, et al.: “A study of evaluation method for GPS-L5 signal environment during flight experiments,” IEICE Communications Express, vol. Vol.2, no. No.7 (2013) 313-318 (DOI: 10.1587/comex.2.313).

[10] J. Jiang, et al.: “Analysis of global navigation satellite system position deviation under spoofing,” IET Radar Sonar and Navigation, (2009) 1-7 (DOI: 10.1049/iet-rsn.20070153).

[11] W. Chen, et. al.: “A Broadened and Deepened Anti-Jamming Technology for High-Dynamic GNSS Array Receivers,” IEICE TRANSACTIONS ON COMMUNICATIONS, vol. E99B, no. No.9 (2016) 2055-2061 (DOI: 10.1587/transcom.2015EBP5493).

[12] Y. Yang, et al.: “An architecture design for anti-jamming circuit with low power and low area cost in high-precision GNSS receiver chip,” IEICE Electronics Express, vol. Vol.16, no. No.10 (2019) 20190179 (DOI: 10.1587/exle.16.20190179).

[13] G. Jin, et al.: “A stable and two-step settling digital controlled AGC loop for GNSS receiver,” IEICE ELECTRONICS EXPRESS, (2014) (DOI:10.1587/exle.11.20140738).

[14] D. P. Shepard, et al.: “Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks,” International Journal of Critical Infrastructure Protection, vol. 5, no. 3 (2012) 146-153 (DOI: https://doi.org/10.1016/j.ijcip.2012.09.003).

[15] D. P. Shepard, et al.: “Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks,” ION GNSS 2012 (2012) 3591-360 (DOI:10.1109/iuscse.2009.5286378).

[16] A. J. Kerns, et al.: “Unmanned Aircraft Capture and Control Via GPS Spoofing,” Journal of Field Robotics, vol. 31, no. 4 (2014) 617-636 (DOI: 10.1002/rob.21513).

[17] T. E. Humphreys, et al.: “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,” in International Technical Meeting of the Satellite Division of the Institute of Navigation (2008).

[18] T. E. Humphreys: “Detection Strategy for Cryptographic GNSS Anti-Spoofing,” IEEE Transactions on Aerospace and Electronic Systems, vol. Vol.49, no. No.2 (2009) 1073-1090 (DOI: 10.1109/taes.2013.6494400).

[19] S. Siamak, et al.: “Dynamic GPS Spoofing Attack Detection, Localization, and Measurement Correction Exploiting PMU and SCADA,” IEEE Systems Journal (2020) 1-10 (DOI: 10.1109/jsyst.2020.3001016).

[20] X. Zhu, et al.: “Detection of Spoofing Medium Contours for Face Anti-Spoofing,” IEEE Transactions on Circuits & Systems for Video Technology (2021) (DOI: 10.1109/tcsvt.2019.2949868).

[21] J. Kwon, et al.: “An incrementally deployable anti-spoofing mechanism for software-defined networks,” Computer Communications, vol. Vol.64, no. No.C (2015) (DOI: 10.1016/j.comcom.2015.03.003).

[22] J. Petri: “Can GPS 'Spoofing' Send Your Car Into a Tree?,” Bloomberg.com (2019).

[23] M. L. Psaki, et al.: “Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies,” IEEE Spectrum, vol. Vol.53, no. No.8 (2016) (DOI: 10.1109/nmspec.2016.7524168).

[24] P. Risbud, et al.: “Vulnerability Analysis of Smart Grids to GPS Spoofing(Article),” IEEE Transactions on Smart Grid, vol. Vol.10 (2019) 3535-3548 (DOI: 10.1109/tsg.2018.2830118).

[25] E. Falletti, et al.: “Synchronization of Critical Infrastructures Dependent upon GNSS: Current Vulnerabilities and Protection Provided by New Signals(Article),” IEEE Systems Journal, vol. 13, no. 3 (2019) 2118-2129 (DOI: 10.1109/jsyst.2018.2883752).

[26] B. Moussa, et al.: “Security Assessment of Time Synchronization Mechanisms for the Smart Grid(Article),” IEEE Communications Surveys and Tutorial (2016) 1952-1973 (DOI: 10.1109/comst.2016.2525014).

[27] Gang Xie: Principles of GPS and Receiver Design (PUBLISHING HOUSE OF ELECTRONICS INDUSTRY, BEIJING, 2009).

[28] C. Ma, et al.: “Effects of a navigation spoofing signal on a receiver loop and a UAV spoofing approach,” GPS Solutions, vol. 24, no. 3 (2020) (DOI: 10.1007/s10291-020-00986-z).

[29] J. Z, et al.: “Efficient Signal Separation Method Based on Antenna Arrays for GNSS Meaconing,” Tsinghua Science and Technology, vol. 24, no. 2 (2019) 216-225 (DOI: 10.26599/tst.2018.9010125).

[30] S. F. Systems.: “Sprink Federal Announces New Enhanced GSS9000 Series GNSS Constellation Simulator,” Business Wire (English) (2019).

[31] W. Jian, et al.: “On the Requirements of GNSS Intermediate Spoofing,” in The 5th China Satellite Navigation Academic Annual Conference (2014) 1.

[32] Jun Yang: Theory and Technology of Satellite Navigation Signal Simulator (National Defense Industry Press, BEIJING, 2015).

[33] Y. SONG Yu-lan, et al.: “Satellite Signal Doppler Simulation Provided by New Signals(Article),” IEEE Systems Journal, vol. Vol.21, no. No.4 (2019) 2055-2061 (DOI: 10.1587/transcom.2015EBP5493).

[34] Y. Yang, et al.: “An architecture design for anti-jamming circuit with low power and low area cost in high-precision GNSS receiver chip,” IEICE Electronics Express, vol. Vol.16, no. No.10 (2019) 20190179 (DOI: 10.1587/exle.16.20190179).

[35] G. Jin, et al.: “A stable and two-step settling digital controlled AGC loop for GNSS receiver,” IEICE ELECTRONICS EXPRESS, (2014) (DOI:10.1587/exle.11.20140738).

[36] D. P. Shepard, et al.: “Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks,” International Journal of Critical Infrastructure Protection, vol. 5, no. 3 (2012) 146-153 (DOI: https://doi.org/10.1016/j.ijcip.2012.09.003).