Experimental Study on the Influence of Satellite Spoofing on Power Timing Synchronization

Jianwu Zhang[1], Xinyu Luo[1], Xingbing Fu[2], Xuxu Wang[1], Chunsheng Guo[1], and Yanan Bai[3]
(Corresponding author: Xingbing Fu)

School of Communication Engineering, Hangzhou Dianzi University[1]
Hangzhou, Zhejiang Province, China
School of Cyberspace, Hangzhou Dianzi University[2]
Hangzhou, Zhejiang Province, China
Chongqing Key Laboratory of Automated Reasoning and Cognition,
Chongqing Institute of Green and Intelligent Technology[3]
Chinese Academy Sciences, Chongqing, China
(Email: fuxbuestc@126.com)
(Received July 3, 2019; Revised and Accepted Dec. 3, 2019; First Online Feb. 3, 2020)

Abstract

The accuracy of time source in power system is required to be high, and the time benchmark of ground usually synchronizes with satellite time. The experimental environment is operated in the open outdoor area. SMBV100A is used as the pseudo Beidou signal transmitter and ATGM332D-5N is used as the Beidou signal receiving chip. The experiment changes the power of pseudo-Beidou satellite signal to explore the influence of spoofing jamming on satellite-ground time synchronization of a single receiving module, and changes the relative position of two receiving modules to study the influence of spoofing jamming on satellite common-view time synchronization. The experimental results show that in the case of deceptive jamming, the greater the power of pseudo-Beidou signal, the shorter the time interval between the receiving module and pseudo-Beidou; when the dual receiving module uses satellite common-view synchronization, there is a large time difference in a period of time. Experiments directly show that time-service time in power system is susceptible to spoofing interference

Keywords: Beidou Spoofing Jamming; Satellite Common View; Time Synchronization between Satellite and Ground; Time Synchronization in Smart Grid

1 Introduction

In the power system, each power automation device, microcomputer monitoring device, and safety automatic protection device are highly dependent on clock synchronization [7, 12]. In order to ensure the accuracy of clock synchronization, the timing clock in the power system is mostly synchronized with the satellite clock by means of satellite synchronization [11,19]. However, due to the navigation message format of the civilian part of the satellite signal including Beidou and GPS, the code modulation mode, carrier frequency and other information are all public. It is easy to use this information to design the Beidou satellite simulator to deceive the satellite receiver,which makes the timing clock of the ground having an error [2, 15, 17].

There are two main ways of time synchronization in the power system:master-slave time synchronization and satellite common-view time synchronization [9, 18]. Master-slave clock synchronization relies on the accuracy of single receiver satellite time synchronization. Satellite common-view time synchronization relies on time synchronization accuracy between multiple satellite receivers [5, 6, 10]. In the case of deception jamming, this work studies the change of the satellite synchronization time of the single Beidou receiver and the change of the satellite synchronization time synchronization of the dual receiver.

2 Experimental Principle

2.1 Satellite-Ground Time Synchronization

Satellites in space continuously transmit satellite signals to the ground by broadcasting, and the ground receiver can resolve the position of the satellite and the time stamp of transmitting signal from the satellite signals.

In theory, when four satellites are used, the ground time and satellite time can be synchronized by Formu-

las (1), (2), (3), and (4) [13].

$$\begin{aligned}
\rho_1 &= c(t_1 - t) && (1)\\
&= \sqrt{(x-x_1)^2 + (y-y_1)^2 + (z-z_1)^2} + cb\\
\rho_2 &= c(t_2 - t) && (2)\\
&= \sqrt{(x-x_2)^2 + (y-y_2)^2 + (z-z_2)^2} + cb\\
\rho_3 &= c(t_3 - t) && (3)\\
&= \sqrt{(x-x_3)^2 + (y-y_3)^2 + (z-z_3)^2} + cb\\
\rho_4 &= c(t_4 - t) && (4)\\
&= \sqrt{(x-x_4)^2 + (y-y_4)^2 + (z-z_4)^2} + cb.
\end{aligned}$$

In Formulas (1), (2), (3) and (4), the subscripts 1, 2, 3 and 4 represent the satellite signal sequence number, ρ_i is the pseudo range of the transmitting satellite to the receiver, t_i is the time stamp of the transmission, and t is local time. c is the speed of light , (x, y, z) is the local location, (x_i, y_i, z_i) is the location where the satellite is launched, and b is the deviation of local time from standard satellite time. It is known that (x_i, y_i, z_i) , t_i and t can find four unknown quantities x , y , z and b , and find $(t - b)$ is the synchronization time between the receiver and the satellite.

2.2 Deception Interference Time Synchronization Principle

When the ground satellite receiver performs the satellite time synchronization normally, it will first capture the signals of different satellite serial numbers from the received signals, and then keep track of the satellite signals. However, the power of the satellite signal received by the ground receiver is relatively small, only about -160dBW [8, 14].

If a pseudo-satellite signal with a relatively large power is transmitted near the receiving module, the pseudo-satellite signal will mask the real satellite signal. The receiving module thereby captures the tracking pseudo lite signal and synchronizes the pseudo lite time according to the navigation message of the pseudo lite signal [3, 4, 16].

2.3 Satellite Common-view Time Synchronization Principle

Satellite common view is a method of time synchronization between devices based on satellite time. Figure 1 shows the schematic diagram of satellite common-view time synchronization.

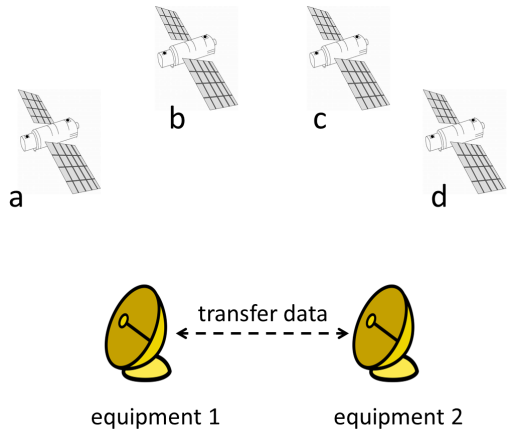

Figure 1: Satellite common view

In Figure 1, device A and device B simultaneously receive satellite signals for satellite time synchronization. Since the durations of the signal processing and data transmitting of device A are different from those of device B, there is a relatively fixed time offset between A and B [1].

3 Experimental Equipment and Experimental Environment

3.1 Experimental Equipment

The main equipment of this experiment is GPS/BD dual-mode receiver module and pseudo-Beidou signal simulator equipment. The GPS/BD dual-mode receiving module includes three parts: Receiving antenna, signal processing chip and serial interface tool. The GPS/BD dual-mode receiving module is shown in Figure 2.

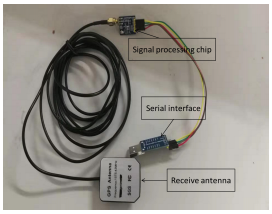

Figure 2: GPS/BD receiving module

The receiving antenna is an ordinary GPS/BD antenna for receiving signals; The signal processing chip is ATGM332D-5N, which is used to capture, track, and analyze satellite signals, and calculates local position and time information; The serial interface tool is CP 2102 USB- TTL BOARDV4.0, used to transfer chip processing data to a computer. Among them, ATGM332D-5N is a key part of the receiving module. Its positioning accuracy is 2.5m, cold-start capture accuracy is -148dBm and tracking capture sensitivity is -162dBm.

The pseudo-Beidou signal simulator is SMBV100A, which is a vector signal generator produced by ROHDE & SCHWARZ. It can simulate the transmission of 12 Beidou

satellite signals, and can set the power of pseudo-satellite signals, UTC, and the location of pseudo-satellite signals.

This experiment records the processing data of the receiving module through the serial port assistant on the computer.

3.2 Experimental Environment Construction

The system block diagram of this experiment is shown in Figure 3. The receiving module receives the real GPS/BD satellite signal during normal operation; when the receiving module is deceived, it receives the real GPS/BD signal and the pseudo-high-pitched signal with high power. The received satellite signal is processed by the serial port tool on the computer.

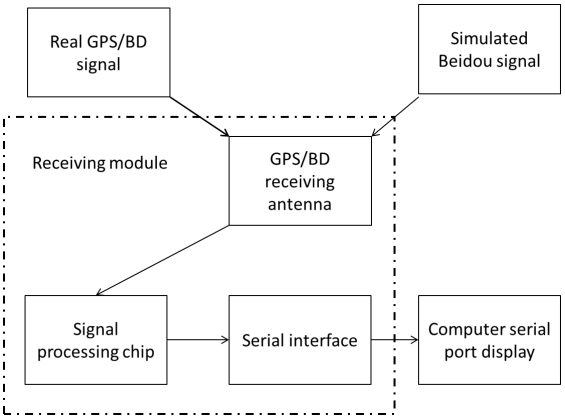

Figure 3: The block diagram of deception interference experiment system

This experiment is carried out in an outdoor open environment to ensure that the receiving module can receive more satellite signals. The transmitting antenna of the pseudo-Beidou signal simulator is placed on a higher floor, ensuring that the pseudo-Beidou signal can cover a larger area. The experimental scene of the BD/GPS receiving module is shown in Figure 4.

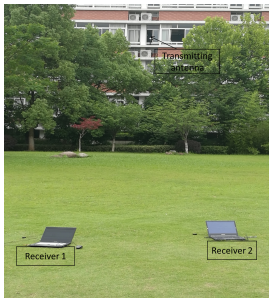

Figure 4: The experimental site map of BD/GPS receiver module

The pseudo-Beidou signal simulator SMBV100A (Figure 5) placed on the upper floor simulates the pseudo-Beidou signal transmitted to the receiving module by a non-omnidirectional antenna with a small beam angle.

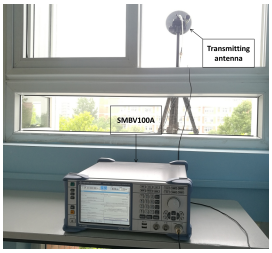

Figure 5: Pseudo-beidou signal simulator and signal transmitting antenna

4 Experimental Steps

This experiment separately studies the effect of deception jamming on the time synchronization of the single receiver module and the effect of deception jamming on the satellite synchronization time synchronization of the dual receiver module. The experimental steps are as follows:

1) Turn off the signal transmission switch of the pseudo-Beidou signal simulator, the receiving module normally receives the real GPS, BD satellite signal and records the signal processing data for 5 minutes through the serial port assistant of the computer after the data is stable.

2) Set the transmission power of the pseudo signal to -20dBm; set the pseudo positioning position of the Beidou signal to be (30°18'53"N, 120°22'23"E), which is about 2' difference from the longitude of the real position; The UTC of the interference source is set to 08:00:00, which is about 12 hours from the real time; the pseudo satellite signal number is 01, 02, 03, 04, 05, 06. Turn on the pseudo-Beidou signal simulator signal emission switch.

3) The serial port assistant records 5 minutes of signal processing data. Turn off the signal transmission switch of the pseudo-Beidou signal simulator.

4) Study the effect of deception jamming on the time synchronization of the single receiver module. Ensure that the experimental environment is unchanged, set the UTC to 04:00:00, change the power of the pseudo-Beidou signal to -20dBm, -15dBm, -10dBm and -5dBm, and repeat the experimental steps from a to c.

5) The effect of deception jamming on the dual-receiving module on satellite common-view time synchronization is studied. Ensure that the experimental environment is unchanged, set the UTC to 07:00:00, the power of the pseudo-Beidou signal to -5dBm, and change the relative distance between the dual receivers to 5m, 10m, 15m and 20m. Experimental steps from a to c were repeated in sequence.

5 Experimental Results and Analysis

5.1 Deception of the Receiving Module

The receiving module normally receives the BD/GPS data, and the GNRMC data read by the computer serial port is shown in Figure 6.

```
$GPGSV,3,3,09,30,19,089,25*4D
$BDGSV,3,1,10,02,,,20,03,,,29,04,,,23,05,,,22*63
$BDGSV,3,2,10,06,72,232,26,08,78,098,30,09,47,224,27,11,21,158,19*65
$BDGSV,3,3,10,13,75,337,29,14,45,036,34*63
$GNRMC,104937.000,A,3018.8702,N,12020.3913,E,0.00,20.86,170718,,,A*42
$GNVTG,20.86,T,,M,0.00,N,0.00,K,A*1F
$GNZDA,104937.000,17,07,2018,00,00*4A
$GPTXT,01,01,01,ANTENNA OK*35
$GNGGA,104938.000,3018.8702,N,12020.3913,E,1,14,0.9,29.0,M,0.0,M,,*4C
$GNGLL,3018.8702,N,12020.3913,E,104938.000,A,A*4E
$GPGSA,A,3,02,06,30,13,05,15,07,29,,,,,1.5,0.9,1.2*34
$BDGSA,A,3,06,08,13,14,11,09,,,,,,,1.5,0.9,1.2*2D
$GPGSV,3,1,09,02,70,083,40,05,61,353,25,06,24,115,32,07,12,060,24*78
$GPGSV,3,2,09,13,59,184,43,15,25,216,20,19,05,161,,29,34,308,32*7C
$GPGSV,3,3,09,30,19,089,25*4D
$BDGSV,3,1,10,02,,,20,03,,,29,04,,,23,05,,,25*64
$BDGSV,3,2,10,06,72,232,26,08,78,098,31,09,47,224,27,11,21,158,19*64
$BDGSV,3,3,10,13,75,337,31,14,45,036,34*6A
$GNRMC,104938.000,A,3018.8702,N,12020.3913,E,0.00,20.86,170718,,,A*4D
$GNVTG,20.86,T,,M,0.00,N,0.00,K,A*1F
```

Figure 6: Serial GNRMC data under normal conditions

The serial port results show that the UTC is 10:49:37 and the local location is (3018.8702N, 12020.3913E), which is (30°18'87.02"N, 120°20'39.13"E). The synchronization time and the positioning position are consistent with the local time and local location, indicating that the receiving module has not received fraudulent interference.

After about 5 minutes of transmitting the pseudo Beidou signal, the GNRMC data read by the serial port is shown in Figure 7. The result shows that the UTC is 08:56:33, and the positioning position is (3018.8835N, 12022.3833E), which is consistent with the parameters set by the Beidou simulator, and is inconsistent with the local time and position. The receiving module is deceived.

```
$BDGSV,3,2,10,05,31,242,54,06,44,266,53,07,26,170,53,08,25,285,52*6C
$BDGSV,3,3,10,13,30,285,53,14,34,223,53*66
$GNRMC,085633.000,A,3018.8835,N,12022.3833,E,0.00,20.86,160718,,,A*4A
$GNVTG,20.86,T,,M,0.00,N,0.00,K,A*1F
$GNZDA,085633.000,16,07,2018,00,00*48
$GPTXT,01,01,01,ANTENNA OK*35
$GNGGA,085634.000,3018.8835,N,12022.3833,E,1,10,1.3,-0.7,M,0.0,M,,*53
$GNGLL,3018.8835,N,12022.3833,E,085634.000,A,A*4F
$GPGSA,A,3,,,,,,,,,,,,,2.7,1.3,2.4*33
$BDGSA,A,3,03,07,05,04,13,06,08,01,02,14,,,2.7,1.3,2.4*2D
$GPGSV,3,1,12,02,50,328,35,04,,,26,05,46,252,16,06,52,051,*40
$GPGSV,3,2,12,09,33,059,26,12,29,267,,13,06,190,36,15,00,212,28*77
$GPGSV,3,3,12,17,33,145,27,19,57,142,28,23,08,039,29,25,11,308,29*71
$BDGSV,3,1,10,01,36,123,54,02,47,219,54,03,54,164,54,04,19,108,53*67
$BDGSV,3,2,10,05,31,242,54,06,44,266,53,07,26,170,53,08,25,285,52*6C
$BDGSV,3,3,10,13,30,285,53,14,34,223,53*66
$GNRMC,085634.000,A,3018.8835,N,12022.3833,E,0.00,20.86,160718,,,A*4D
$GNVTG,20.86,T,,M,0.00,N,0.00,K,A*1F
$GNZDA,085634.000,16,07,2018,00,00*4F
$GPTXT,01,01,01,ANTENNA OK*35
```

Figure 7: Serial GNRMC data in case of fraudulent interference

5.2 Satellite-Ground Time Synchronization under Deception

When the receiving module receives the real Beidou signal, the transmission power of the pseudo Beidou signal is changed to -20dBm, -15dBm, -10dBm and -5dBm, and the experimental data simulation results are shown in Figures 8–11.

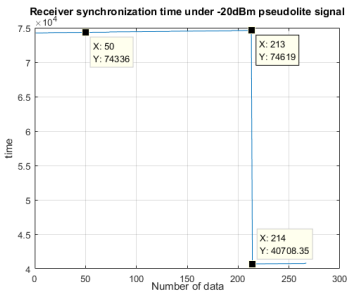

Figure 8: Receiver synchronization time under -20dBm pseudo lite signal

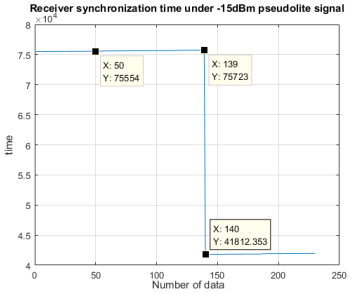

Figure 9: Receiver synchronization time under -15dBm pseudo lite signal

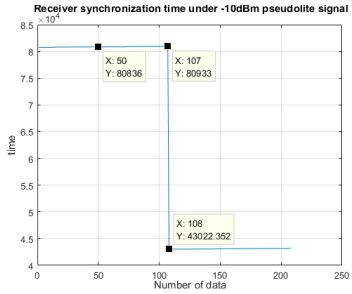

Figure 10: Receiver synchronization time under -10dBm pseudo lite signal

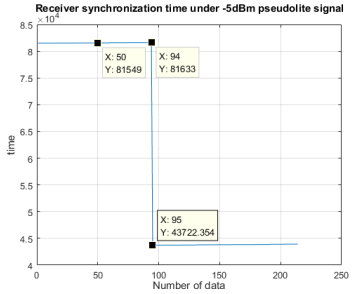

Figure 11: Receiver synchronization time under -5dBm pseudo lite signal

In Figures 8–11, the abscissa is the number of data frames received by the serial port, and 1 s corresponds to one data point. The ordinate is the UTC resolved by the receiving module and is represented by scientific notation.

In Figures 8–11, the UTC line starts from the left and the first black point indicates the moment when

the pseudo-beidou signal is transmitted, the second black point indicates the last moment of the synchronized real satellite time, and the third black point indicates the first moment of time of the synchronous pseudo-beidou. It can be seen that after the pseudo-Beidou signal is transmitted, the UTC parsed by the receiving module does not immediately synchronize the pseudo-dipper time, and still maintains the real satellite time before the interference.

The time interval between the first black point and the second black point indicates the time required for synchronizing the satellite time and the pseudo-beidou signal in the case of fraudulen interference. According to Figures 8–11, the length of time required for synchronizing the UTC of the receiving module and the pseudo Beidou signal is recorded in the case of pseudo-Beidou signal fraud interference of different powers, as shown in Table 1.

Table 1: Time required for synchronizing pseudo-beidou signals

Pseudo-Beidou Signal Power/dBm	-20	-15	-10	-5
Synchronized Pseudo-beidou Signal Time/s	163	89	57	44

It can be seen from Table 1 that the greater the power of the pseudo-Beidou signal, the shorter the time that the UTC resolved by the receiving module is synchronized to the pseudo-Beidou signal.

5.3 Satellite Common Time Synchronization under Deception Jamming

The power of the pseudo-Beidou signal is kept at -5dBm, and the relative distance between the two receivers is changed, which is 5m, 10m, 15m and 20m, respectively, and the experimental data simulation results are obtained (Figures 12–15). In Figures 12–15, it is ensured that the two receiver modules have the same abscissa of the UTC at the same moment. The significance of the three black points on the two UTC lines in the figure is still the pseudo-Beidou signal transmitting time, the last moment of the synchronized real satellite time, and the first moment of time of the synchronous pseudo-beidou is analyzed.

In Figures 12–14, both the receivers 1 and 2 have a UTC hopping condition, and in Figure 15, the receiver 1 always maintains the true UTC, indicating that it is not subject to spoofing interference.

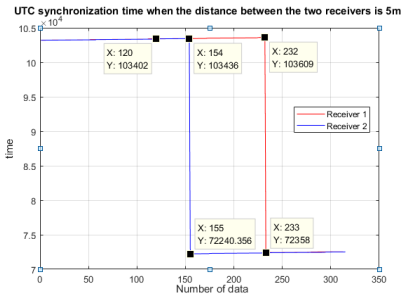

Figure 12: UTC synchronization time when the distance between the two receivers is 5m

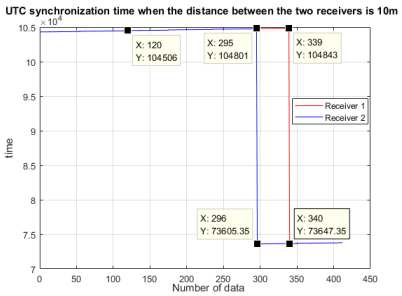

Figure 13: UTC synchronization time when the distance between the two receivers is 10m

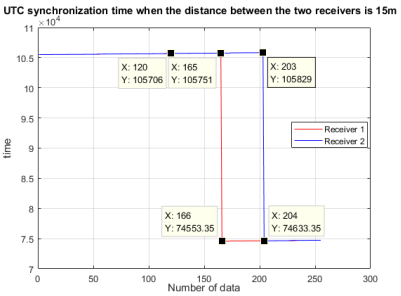

Figure 14: UTC synchronization time when the distance between the two receivers is 15m

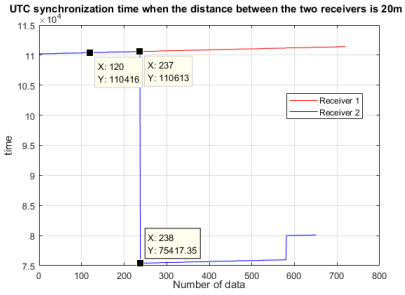

Figure 15: UTC synchronization time when the distance between the two receivers is 20m

As can be seen from Figure 12 to Figure 15, in the case of fraudulent interference, the dual-receiving module satellite common-view synchronization time has a large time difference over a period of time. Record the length of time when the synchronization time of the two receivers

is different under different relative distances. The results are shown in Table 2.

Table 2: Dual receiver satellite common-view synchronous UTC deviation duration

Relative Distance Between Two Receivers/m	5	10	15	20
Satellite Common-view Time Deviation Duration/s	78	44	38	–

It can be seen from Table 2 that when the relative distance between the receivers is too large, the time deviation between the two receiving modules is always large because the pseudo-Beidou signal cannot cause deception to interfere with one of the receiving modules. When the relative distance between the receiving modules is less than 20m, the time deviation between the two receiving modules will be relatively large during a period of time, about 40s to 80s.

6 Conclusion

In this work, based on two time synchronization methods of timing time source in the power system: Satellite-Ground Time Synchronization and Satellite Common Time Synchronization, experiment changes the transmission power of the pseudo-Beidou time signal and the distance between the two receivers to explore the satellite fraudulent interference. The following conclusions are obtained:

1) After being deceived, the time of synchronization of the satellite will jump to the pseudo-Beidou signal time.

2) The greater the power of the pseudo Beidou signal, the shorter the time that synchronizes the receiving module and the pseudo Beidou signal.

3) When the distance between two receivers based on satellite common view synchronization is too large, the pseudo-Beidou signal transmitted by the Beidou simulator may not be able to successfully deceive one of the receivers. The time offset between the two receivers is kept large.

4) When the relative distance of the receiver is within 20m, the dual receivers based on the satellite common view synchronization are deceptively interfered, and the synchronization time will have a large deviation during a period of time, about 40s to 80s.

Acknowledgments

The authors would like to thank the Joint Funds of Smart Grid of the National Natural Science Foundation of China (No.U1866209) for providing the project foundation.

References

[1] D. W. Allan and M. A. Weiss, "Accurate time and frequency transfer during common-view of a GPS satellite," in *The 34th Annual Symposium on Frequency Control*, pp. 334–346, May 1980.

[2] C. Bonebrake and L. Ross O'Neil, "Attacks on GPS time reliability," *IEEE Security Privacy*, vol. 12, pp. 82–84, 2014.

[3] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low-complexity GNSS spoofing mitigation technique using a double antenna array," *GPS World Magazine*, vol. 22, pp. 44–46, 2011.

[4] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS'12)*, pp. 1233–1243, Sep. 2012.

[5] Y. J. Huang, J. D. Fu, H. Takiguchi, W. H. Tseng, and H. W. Tsao, "Stability improvement of an operational two-way satellite time and frequency transfer system," *Metrologia*, vol. 53, pp. 881–890, 2016.

[6] J. F. Li, H. Li, C. X. Peng, J. Wen, and M. Lu, "Research on the random traversal raim method for anti-spoofing applications," in *China Satellite Navigation Conference (CSNC'19)*, pp. 593-605, May 2019.

[7] B. F. Liu, Z. Q. Ji, and Z. X. Xie, "The application analysis of IEEE 1588 in smart substation," in *The International Conference on Advanced Power System Automation and Protection (APAP'11)*, pp. 309–395, Oct. 2011.

[8] B. F. Liu, Z. Q. Ji, and Z. X. Xie, "GPS anti-spoofing technology based on RELAX algorithm in smart grid," in *Proceedings of the 10th International Conference on Communications and Networking in China Chinacom*, pp. 637–642, Aug. 2015.

[9] H. P. Liu, F. Yang, J. Zhou, and H. S. Zhao, "Application of time synchronization technology of beidou navigation system in power system," *East China Electric Power (in Chinese)*, vol. 39, pp. 489–491, 2011.

[10] Z. Y. Chen, H. Li; M. Q. Lu, "GNSS spoofing detection with single moving antenna based on the correlation of satellite transmit time residual," in *China Satellite Navigation Conference (CSNC'18)*, pp. 978–981, May 2018.

[11] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Communications Surveys Tutorials*, vol. 18, pp. 1952–1973, 2016.

[12] F. Ramos, J. L. Gutierrez-Rivas, J. Lopez-Jimenez, B. Caracuel, and J. Diaz, "Accurate timing networks for dependable smart grid applications," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 2076–2084, 2018.

[13] N. O. Tippenhauer, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *ACM Conference on Computer and Communications Security*, pp. 75–86, Oct 2011.
[14] F. Wang, H. Li, and M. Lu, "GNSS spoofing countermeasure with a single rotating antenna," *Journals & Magazines*, vol. 5, pp. 8039–8047, 2017.
[15] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation-Journal of The Institute of Navigation*, vol. 59, pp. 177–193, 2012.
[16] Y. T. Zhang, L. Wang, W. Y. Wang, D. Lu, and R. B. Wu, "Spoofing jamming suppression techniques for GPS based on DOA estimating," in *China Satellite Navigation Conference (CSNC'14)*, pp. 683–693, May 2014.
[17] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, pp. 87–98, 2013.
[18] S. Zhao, "Measurement and synchronization technology based on satellite common view method," *Computer Measurement and Control (in Chinese)*, vol. 12, pp. 49–52, 2016.
[19] T. Zhao, Z. W. Li, and B. Zou, "Wide-area time synchronization method for satellite clock and network clock equipment," *Automation of Electric Power System (in Chinese)*, vol. 14, pp. 202–207, 2017.

Biography

Jianwu Zhang is a professor at Hangzhou Dianzi University, and he received a Ph.D. from Zhejiang University in 1999. His research interests include mobile communication and image processing.

Xinyu Luo is currently pursuing his master's degreee in electronics and communication engineering, Hangzhou Dianzi University. Her research interests include Beidou fraud detection, and image processing.

Xingbing Fu is a lecturer, and he received the Ph.D. degree from University of Electronic Science and Technology of China (UESTC) in 2016. His research interests include cloud computing, cryptography and information security.

Xuxu Wang is currently pursuing his master's degreee in electronics and communication engineering, Hangzhou Dianzi University. His research interests Beidou fraud detection.

Chunsheng Guo received a B.Sc.in Radio Engineering from the Northeastern University (NEU), Shenyang, China, and received a Ph.D. in Communication and Information System from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 1993 and 2002 respectively. He is currently an associate professor at the School of Communication Engineering, Hangzhou Dianzi University, China. His research involves image segmentation, video moving objects detection, Video action recognition and Video anomaly detection.

Yanan Bai is a Ph.D. candidate from Chongqing Institute of Green and Intelligent Technology, Chinese Academy Sciences. Her research interests are homomorphic encryption and applications, big data privacy protection and Cryptography theory.