Analysis and Evaluation of Spoofing Effect on GNSS Receiver

Xiaofeng Ouyang, Fangling Zeng
Hefei Electronic Engineering Institute
Hefei, 230026, China

Pan Hou, Ruizhi GUO
Troops 61251
Qinhuangdao, 066102, China

***Abstract*—Spoofing can effectively attack the GNSS receiver in better ways than normal interference method and it is becoming a main jamming mode to the GNSS. With the rapid development of GNSS spoofing and anti-spoofing, a supporting evaluation system feasible to assess the spoofing effect on receiver appears essential. The paper proposed a new evaluation mechanism and also set up an analysis platform to evaluate the spoofing effect in communication, acquisition and ranging domain. The work presented here can also be generalized to evaluate other GNSS jamming effectiveness.**

Keywords-component; GNSS; spoofing; spoofing effectiveness; evaluation mechanism;

In GNSS (Global Navigation Satellite System) countermeasures fields, jamming and spoofing are the major interference means. Jamming is nothing more than bombarding the receiver with noises, while spoofing is to purposefully mislead the GNSS receiver with a mimic satellite signal [1], which can achieve effective interfering purpose with lower power, smarter mode, and minor error but hazardously misleading information.

GNSS spoofing tends to induce the receiver to track a mimic spoofing signal instead of the original satellite signal. Spoofer changes the GNSS signal with minor but significant PVT (Position Velocity and Time) errors, amplifies and re-broadcasts it to deceive a particular victim [2]. Due to the higher power and mature technique, the target receiver is easily deceived to capture the spoofing. For example, current sophisticated and widely used technique--- Meaconing, claims to be able to spoof the position of a GPS (Global Positioning System) receiver approximately 100 meters [3].Moreover, other theoretical research on simulation-based or repeater-based spoofing is focused on the destruction of the GPS code tracking loop and differential corrections link attacks[4][5][6]. Although spoofing has been covered extensively in the technical literature, an effective evaluation method aims at assessing the spoofing effect on the target receiver has received scant coverage and little attention.

On one hand, since novel modulation types like BOC have been utilized in both civil and military field, the spoofing targets are turn to attacks both traditional BPSK (Binary Phase Shift Keying) signal and the new modulated signal, including BOC (Binary Offset Carrier), MBOC (Multiplexed Binary Offset Carrier) and other new modulation type [7]. New challenges have arisen in the spoofing effectiveness monitoring and evaluating area. On the other hand, with the continuous upgrading of GNSS technique, complex defensive maneuvers of spoofing and anti-spoofing, building an integrated evaluation system including signal simulation, collecting and analyzing under spoofing become essential.

The remainder of this paper is organized as follows. Section I introduces the general background about GNSS spoofing taxonomy and the main principle of spoofing attack. Section II introduces methods of spoofing effectiveness evaluation and key parameters in communication, acquisition and ranging domain. Section III presents the mechanism of spoofing effect evaluation system and the test result based on the system. Conclusions are provided in Section IV.

I. GNSS SPOOFING SCENARIOS

A. Spoofing Taxonomy

Spoofing attacks include simulation-based spoofing and repeater-based spoofing:

1) Simulation-based spoofing is produced by the resource with an mimic GNSS signal, which provides the target receiver with a falsified position and/or time [8]. This method needs to know the exact pseudo-code sequence and satellite message data for each channel. As to the GPS P (Y) / M military code [7], this method cannot be effectively implemented.

2) Repeater-based spoofing does not involve signal simulation, but involves the delay and relay of GNSS authentic signal. Without knowing the actual signal generation parameters, repeater-based spoofing could deceive both the civil and military receivers in an easier way. Therefore, the spoofing method discussed and evaluated in the sections below is mainly about repeater-based spoofing method.

B. Repeater-based Spoofing Mechanism

The spoofing mechanism based on repeater is illustrated in Fig.1. A GNSS signal duplexer (receive-transmit) antenna receives the signal from the actual constellation and sends it to the spoofer. Then the spoofer copies and modifies the original signal with little but important changes. The repeater transmits the spoofing signal to the target receiver in a gradually increasing power without target recognition. During this process, the target receiver receives both the original in-orbit signal and the malicious repeater signal. However, with the time accumulating and power increasing, the synchronization between the original constellation and local receiver is broken. Without being detected, the original

978-1-4673-7211-4/15 $31.00 © 2015 IEEE
DOI 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.250

GNSS signal will be treated as the noise, while the spoofing as the "real" [9].

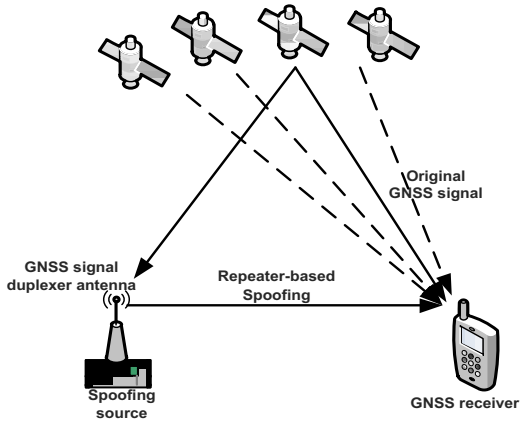


Figure 1. Block diagram of GNSS spoofing.

This paper use GNSS signal source and signal recorder & playback device (Fig.2) to generate a repeater-based spoofing. Be based on this repeater-based spoofing, effectiveness evaluation parameters, mechanism and the whole evaluation system is implemented.

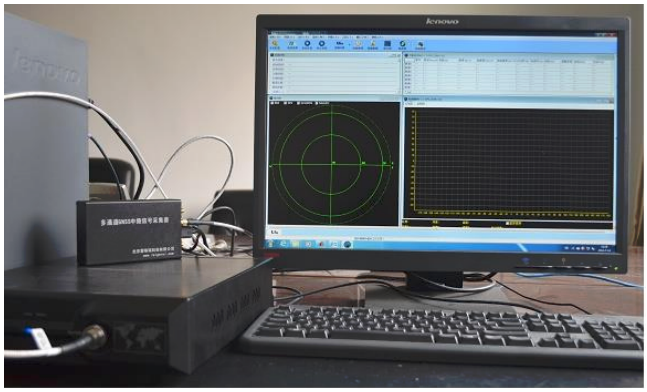


Figure 2. Photo of the GNSS signal & spoofing devices.

II. EVALUATION OF SPOOFING EFFECTIVENESS

A. Communication Effectiveness

The negative influence of spoofing on the communication effectiveness can be evaluated with equivalent carrier-to-noise ratio (CNR) and bit-error-rate (BER). The receiver carrier-to-noise ratio for both non-spoofing (C/N_0) and spoofed ($[C/N_0]_{eq}$) can be represented by (1) and (2), respectively.

$$C/N_0 = S_r + G_\alpha - 10\lg(kT_0) - N_f - L \quad (1)$$

Where S_r indicates the received signal power, G_α indicates antenna gain in the direction of the satellite, K represents Boltzmann constant and T_0 represents the thermal noise temperature. N_f includes noise figure of antenna and line loss. L is the loss of A/D converter (ADC).

The receiver with spoofed GNSS signal would report C/N_0 measurement decreased to equivalent carrier-to-noise $[C/N_0]_{eq}$, which is described as (2).

$$[C/N_0]_{eq} = S_r + G_\alpha - 10\lg[10^{-\frac{\frac{C}{N_0}}{10}} + 10^{\frac{\frac{J}{S}}{10}}/QR_c \quad (2)$$

Where, J and S represent the spoofing and the original signal power respectively, J/S is jam-to-signal ratio. The average bandwidth of spoofing signal is given by $Q = B \cdot R_c$ where Q stands for gain adjustment coefficient and R_c stands for data rate.

Additive white Gaussian noise is assumed in GNSS signal simulation as the environment interference. Thus, the relationship of bit error rate P_e, and $[C/N_0]_{eq}$ is given as (3).

$$P_e = erfc(\sqrt{\frac{[C/N_0]_{eq}}{R_c}}/2 \quad (3)$$

B. Acquisition Effectiveness

As to the acquisition algorithmic in mass-market GNSS receivers, the massive-parallel approach is the most common and comparatively straight forward (it can simply be derived from standard tracking channel architectures in common receivers) [10]. In this paper, we take the parallel method as the acquisition strategy. The receiver correlates the original and spoofed signal respectively with early-prompt-late code. The correlation results explained the acquisition process (Fig.3)

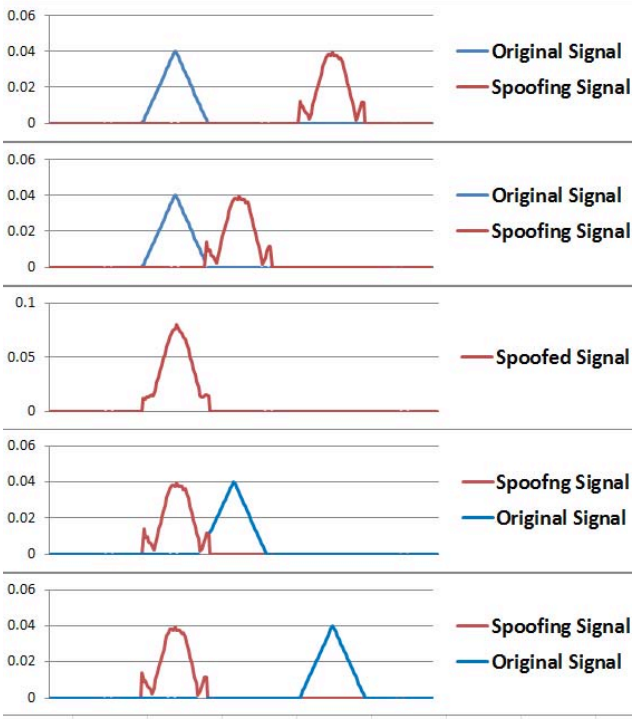


Figure 3. Traction procedure of the spoofing signal .

As shown in Fig.3, Repeater-base spoofing source relayed the GNSS signal and amplified it into a faked version of the original one. Thus, the receiver will try to capture the original signal and the spoofing one with significantly higher

signal power simultaneously. Due to the higher correlation peak, it will continuously deviate its correlation traction from the original state, lead the receiver to lose tracking with the original signal. When the receiver retries acquisition processing, it treat the spoofing as a "real" one, and gradually adjust its local code generator to align with the spoofing. To evaluating this spoofing process and influence, we take acquisition time as a real-time monitoring parameter, which will be explained in section IV and Fig.6.

C. Ranging Effectiveness

1) Code tracking performance

Parameters of the correlation accuracy are important to the receiver raging effectiveness. Particularly, the difference between the ideal correlation peak and the output position of the tracking loop determines the code tracking accuracy. Thus, the correlation peak is an important and effective parameter for evaluating. It produces a pseudo-range error due to the distortion, one of the most important errors.

Besides, using of S-curve bias and correlation loss together analyze the spoofed receiver ranging performance. The GNSS receiver obtains the code delay by the zero-crossing of the code discriminator function——S-curve, based on the CCF (Cross-Correlation Function) [11], which can be used to evaluate the correlation peak performance.

$$S_{curve}(\tau,\delta) = |CCF\left(\tau - \frac{\delta}{2}\right)|^2 - |CCF(\tau + \frac{\delta}{2})|^2 \qquad (4)$$

With its lock-pint (S-curve bias $\tau_{bias}(\delta)$) defined by

$$S_{curve}(\tau_{bias}(\delta),\delta) = 0 \qquad (5)$$

Where δ is the early-late spacing,τ is the code delay.

Within IS-GPS-200D [12], correlation loss (CL) is the difference between the SV (Satellite Vehicle) power received and the signal power recovered in an ideal correlation receiver of the same bandwidth. CL is also based on the output of CCF and the CL under spoofing ($CL_{spoofed}$) is calculated as (6)(7):

$$P_{CCF}[dB] = \max_{\substack{over \\ alls}}(20 \cdot log_{10}(|CCF(\varepsilon)|)) \qquad (6)$$

$$CL_{spoofed}[dB] = P_{\substack{CCF \\ ideal}}[dB] - P_{\substack{CCF \\ spoofed}}[dB] \qquad (7)$$

By comparing assessment results in the follow section, we will know that the correlation peak is intuitional and explicit, but quantizing is shortcoming. S-curve bias and correlation loss can evaluate the ranging performance quantifiably but not accurately enough under spoofing.

2) Carrier tracking performance

PLL (Phase Locking Loop) error is mainly derived from thermal noise error, phase jitter and dynamic stress error. For GNSS receiver, other factors mostly are seen not as a staying or significant error source, but as thermal noise that call for carrier phase tracking performance. Based on arc-tan carrier PLL, the thermal noise is described as:

$$\sigma_{PLLt} = \frac{360}{2\pi}\sqrt{\frac{B_n}{C/N_0}(1 + \frac{1}{2TC/N_0})} \quad (^\circ) \qquad (8)$$

Where B_n is the carrier loop noise bandwidth, C/N_0 is carrier noise ratio, T is time of detection integral beforehand.

III. Test & Analysis of Spoofing Effectiveness

As described in former introduction, multi-modulation such as BOC is new trends of GNSS development and without doubt the new spoofing target. Considering the research application in future navigation countermeasures, tests and analysis in this section are implemented both on BPSK signal and BOC signal.

A. Test & Envaluation Environment

In order to verify the proposed evaluation method of spoofing effectiveness, the test platform is implemented by combining hardware and software. The GNSS signal generator is used to generate authentic RF signal. According to the spoofing parameters setting, the spoofing generator receives the authentic signal and mimics it to relay to the signal processing unit, which is just like a Software-Defined GNSS receiver. Data collection and spoofed signal collection is done by a high speed data recorder. The whole experiment operates on PC equipped with the software receiver and spoofing effect evaluation system. The basic configuration is shown in Fig. 4.

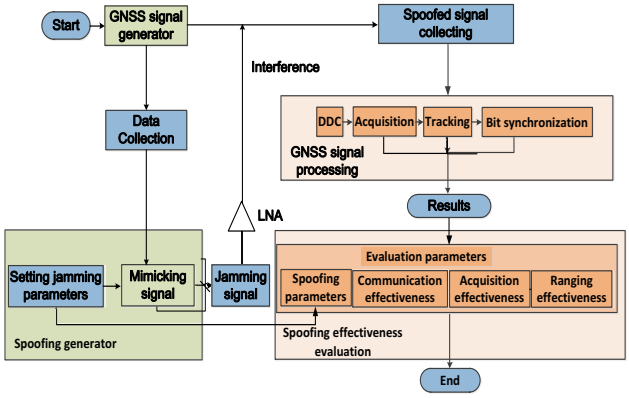


Figure 4. Flowchart of spoofing effect evaluation.

The spoofed signal processing includes several steps, namely DDC (Digital Down Converter), acquisition, tracking, bit synchronization. This paper used a software-defined receiver, which is visible to output raw measurements needed for the following spoofing effect assessment. According to the conventional software-defined receiver, the signal processing unit also has some spoofing detection and anti-spoofing capability. The parallel acquisition function involves coarsely estimating the Doppler offset and code phase for each channel. If signals in more than two time-frequency cell exceed a threshold, jamming signal will be detected. Furthermore, the carrier tracking loop (Costas loop) and code tracking loop (DLL) are designed in second-order loop filter, which is sensitive to the acceleration-pressure and unconditionally stable to any noise bandwidth. The spoofing effectiveness evaluation system is designed with one parameter setting module and three other modules to calculate evaluation parameters in communication, acquisition and ranging domain. The following subsections briefly provide test results of spoofing

on the authentic signals and the effectiveness evaluation results.

Furthermore, considering the modernism of the GNSS signal and research application for both civil and military use, spoofing targets on both traditional BPSK and BOC modulation signal.

B. Communication Effectiveness Analysis

Assuming that the power of the authentic signal is -110dBw; the jam-to-signal ratio is from 20dB to 40dB; receiver bandwidth is $B_n = 30MHz$, time of detection integral beforehand 30ms. TATLE.I illustrates the results of a series of spoofed communication effectiveness.

TABLE I. THE EVALUATION RESULTS OF SPOOFED COMMUNICATION EFFECTIVENESS

	J/S	$[C/N0]_{eq}$
Authentic signal	---	80 dB-Hz
Spoofing	20 dB	57.69 dB-Hz
Spoofing	30 dB	39.47 dB-Hz
Spoofing	40 dB	19.27 dB-Hz

As the results in TABLE.I indicate that, under the spoofing attacks, the receiver's channel is deteriorated. The $[C/N0]_{eq}$ decreases as J/S increases. Alternatively, the Bit flip probability could illustrate the relationship between CNR with BER (Fig.5). .It can be observed that, the decrease of the CNR is able to cause the bit flip to occur and is bound to affect the bit synchronization. Thus, CNR is a key parameter for evaluating the communication effectiveness under spoofing.

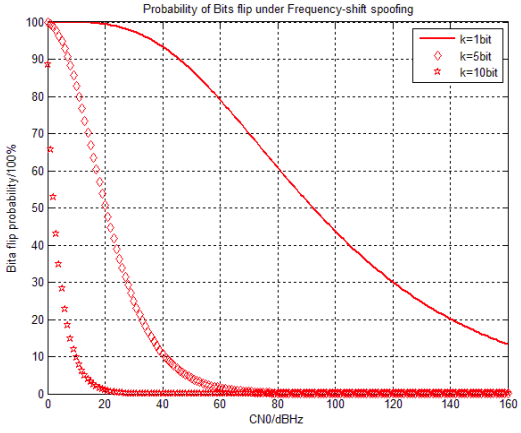
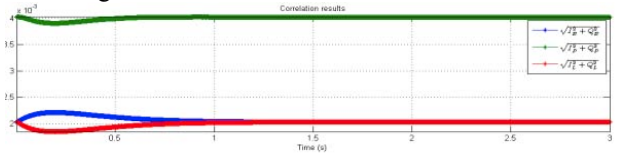


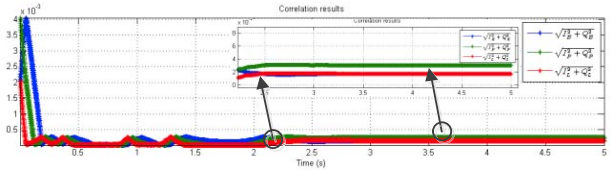
Figure 5. Photo of the test & envaluation devices.

C. Acquisition Effectiveness Analysis

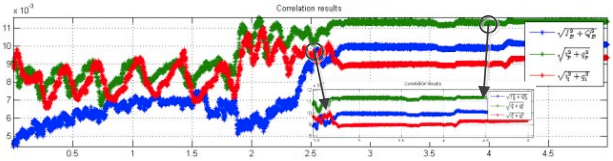
After outputting the raw measurements for communication effectiveness evaluation, the signal processing unit correlates the spoofed signal with early-prompt-late code ($\sqrt{I^2_{(E,P,I)} + Q^2_{(E,P,I)}}$), separated in code phase by 1/2 chip. Fig.6 (a) shows that the local code and the authentic C/A signal are completely synchronized before spoofed. When the spoofer launches a mimic signal, the interrupt of spoofing causes the receiver to lose track at first. Then the receiver tries to re-carry out the acquisition, the spoofing signal will be treated as true signal and adjusted to until it is in phase. As shown in Fig.6 (b) (c), consequently, the receiver will capture and track the spoofed signal just as a "real" signal.



(a) Acquisition time of the authentic C /A signal



(b) Acquisition time of the spoofed BPSK(1) signal



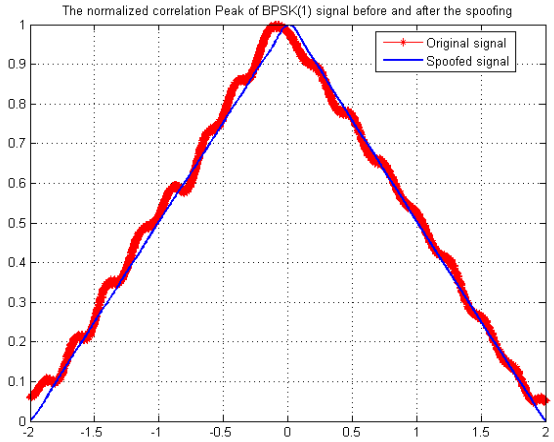
(c) Acquisition time of the spoofed BOC(10,5) signal

Figure 6. Acquisition time of the authentic and spoofed signal.

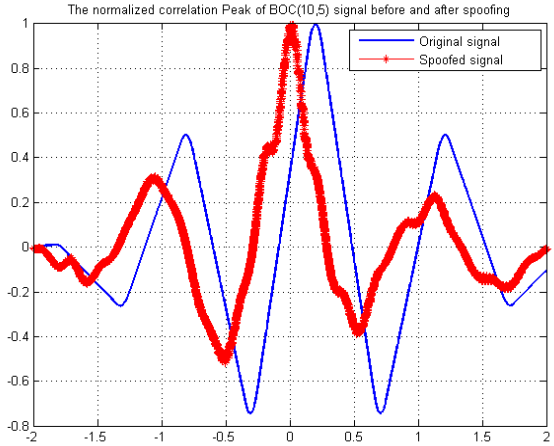
BOC(10,5) is modulation of GPS and GALLILEO military code. Fig.6 (b)(c) respectively indicate the acquisition time of BPSK(1) and BOC(10,5) simulation signal under the spoofing (J/S as 20dB). The test results illustrate that acquisition time can briefly indicate the attacking process of spoofed BPSK and BOC signal.

D. Ranging Effectiveness Analysis

Based on the acquisition effectiveness evaluated above, we already knew some parameters sensitive to the spoofing in communication and acquisition process. We focus on the error of ranging in this subsection. As the spoofed receiver is manipulated by the spoofing signal induced in and verify the performance of receiver, the output of DLL cannot accurately represent pseudo-range bias. However, distortion on the correlation peak of non-spoofing and spoofed (J/S=20dB) BPSK/BOC signal can directly illustrate the ranging effectiveness (As shown in Fig.7). What's more, to quantifiably evaluate the ranging effectiveness, correlation loss (CL) and S-curve bias are obtained to analyze (As shown in TATLE II).



(a). BPSK(1)



(b). BOC(10,5)

Figure 7. The normalized correlation peak before and after spoofing.

Fig.7 indicates that the correlation peak is obscured under spoofing, which indicates a tracking error and consequently an alteration of positioning results. Besides the correlation peak, other evaluation result of quantized parameters is illustrated in TABLE.II, including CL, S-curve bias.

TABLE II. RANGING EFFECTIVENESS PARAMETERS OF CL, S-CURVE BIAS

	CL/dB	**S-curve bias (0.2/0.5)**
Authentic Signal	3.43	0
Spoofing (J/S=20dB)	26.33	2.7062
Spoofing (J/S=30dB)	26.96	1.3039
Spoofing (J/S=40dB)	27.01	2.3657

The CL measures the channel-related losses and the signal power usable within in the correlation-process. As the result in TABLE.II, when spoofed by the malicious interference signal, CL values and S-curve offset magnified due to the distortion of correlation and the relative power loss. Thus, CL and S-curve can directly and quantitatively indicate the spoofing effectiveness.

IV. CONCLUSION

In this paper, we have built a through effectiveness evaluation mechanism for GNSS spoofing, including evaluation parameters, evaluating system and analysis/test platform. Key parameters for evaluating the spoofing effects on GNSS receiver is extracted and calculated in three domains: communication, acquisition and ranging. The experiment results of BPSK and BOC signal demonstrate the effectiveness of the proposed evaluation mechanism and key parameters. The work presented here can be applied to GNSS countermeasure, which covers the void of current research on spoofing effectiveness evaluation.

REFERENCES

[1] J. A. Larcom and H. Liu, "Modeling and Characterization of GPS Spoofing" . Technologies for Homeland Security, 2013 IEEE submitted for publication, Waltham,Massachusetts,USA,November 12-14,2013.

[2] Antonio Cavaleri. " Detection of Spoofed GPS Signal at Code and Carrier Tracking Level", NAVITEC 2010

[3] Green Bay, "Professional Packet Radio (GBPPR) GPS delay spoofing experiments". The Monthly Journal of the American Hacker, 53 (Sept.2008).

[4] J.S. "Warner and R.G.Johnston, GPS Spoofing Countermeasures". Homeland Security Journal,2003

[5] Scott L. Anti-spoofing & authenticated signal architectures for civil navigation systems." In: Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigatio, Portland, 2003. 1543–1552

[6] S.Gong, Z.Zhang, M.Trinkle,et al. GPS Spoofing Based Time Stamp Attack on Real Time Wide Area Monitoting in Smart Grid. IEEE SmartGridComm 2012 Symposium-Cyber Security and Privacy,Tainan City,Taiwan,Novemver 5-8,2012

[7] Jose Angel Avila Rodriguez, "On Generalized Signal Waveforms for Satellite Navigation",University FAF Munich,2008

[8] Yawen Fan, Zhenghao Zhang, Matthew Trinkle, Aleksandar D. Dimitrovski, Ju Bin Song, and Husheng Li, "A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids ," Smart Grid, IEEE Transactions, August 2014.

[9] C. J. Wullems," A spoofing detection method for civilian L1 GPS and the E1-B galileo safety of life service", IEEE Transactions on Aerospace and Electronic Systems, vol. 48, no. 4, pp. 2849-2864, Oct. 2012.

[10] L. Kurz, G. Kappen, T. Coenen, T. G. Noll ,Comparison of Massive-Parallel and FFT-Based Acquisition Architectures for GNSS Receivers,23rd International Technical Meeting of the Satellite Division ofThe Institute of Navigation, Portland, OR, September 21-24, 2010,page 2874-2883

[11] M.Soellner, C.Kurzhals, G.Hechenblaikner, et al. GNSS offline signal quality assessment. In Proceedings of ION GNSS 2008. Savannah, GA(USA), 2008, p.909-920

[12] Aring, NAVSTAR GPS Space Segment/Navigation User Interfaces, IS-GPS-200D, ARINC Engineering Services, LLC, El Segundo, CA, 7 March 2006.