A Gaussian Mixture Model Based GNSS Spoofing Detector using Double Difference of Carrier Phase

Nguyen Van Hien, Nguyen Dinh Thuan, Hoang Van Hiep, La The Vinh*

Hanoi University of Science and Technology, No. 1, Dai Co Viet, Hai Ba Trung, Ha Noi, Viet Nam

Received: February 06,2019; Accepted: June 22, 2020

Abstract

In this paper, we propose a novel method to effectively detect GNSS (Global Navigation Satellite Systems) spoofing signals. Our approach utilizes mixtures of Gaussian distributions to model the Carrier Phase's Double Difference (DD) produced by two separated receivers. DD calculation eliminates measurement errors such as ionosphere error, tropospheric error and clock bias. DD values contain the angle of arrival (AOA) information and a small amount of Gaussian noise. The authentic GNSS signals come from different directions, therefore AOA values are different for each satellite. In contrast, spoofing signals from one broadcaster should always have the same direction. Therefore, DD values of authentic satellites contain mainly the double difference of AOA values, while DD of spoofing satellites contains only an insignificant amount of Gaussian noise. That rough observation is the theoretical basis for our proposal in which we use Gaussian Mixture Models (GMMs) to learn the distribution of DD values calculated for both kinds of satellites. The pre-trained GMMs are then utilized for detecting non-authentic signals coming from spoofing satellites.

Keywords: GMM, AOA, spoofing detector, GNSS

1. Introduction

Nowadays, GNSS has become the core technology for many applications from civilian to military services. Besides providing location for many applications, GNSS services also provide highly accurate time to synchronize systems such as telecommunications and networks. Although there are many benefits, GNSS signal may be affected by intentional and unintentional interferences such as ionospheric delay, jamming, spoofing, TV broadcasted signal, etc. Among these interferences, spoofing can be considered as one of the most dangerous attack because it generates fake signals, having exactly the same format and structure as those of the authentic one, to mislead the position or the time information of the victim GNSS receiver. There are some major types of spoofing attacks in the GNSS literature: simplistic, intermediate, and sophisticated [1-3].

In the simplistic spoofing attack, a GNSS signal simulator is usually connected to a Radio Frequency (RF) front-end and is used to mimic the actual GNSS signal. The spoofer can generate counterfeit GNSS signals, but in general it is unable to synchronize its time with the real GNSS constellation. Therefore, it is quite trivial to detect by simple countermeasures [1].

Intermediate spoofing attack is more complicated and more dangerous than the simplistic attack. In this case, the spoofer is coupled with a real GNSS receiver. The GNSS receiver is used to extract time, position and observation data from the real satellite constellation. After that, the spoofer synchronizes the time from the GNSS receiver with its local code and carrier phase to generate counterfeit signals [1].

Sophisticated spoofing attack is a network of broadcasters with multiple phase-locked portable spoofers. It is the most complicated and effective spoofing method. Furthermore, it can defeat complicated countermeasures (such as the angle-of-arrival defense) by relying on the constructive properties of their RF signals [1].

There are several techniques for spoofing detection based on the characteristics and parameters of the signal. In [3] the authors describe some typical techniques to detect GNSS spoofing: amplitude discrimination, time of arrival discrimination, cross-checking based on navigation inertial measurement unit (IMU), polarization discrimination, angle of arrival discrimination, cryptographic authentication discrimination. The detection techniques based on amplitude and signal's time of arrival can be implemented on a GNSS software-based receiver. However, those methods can only detect the simplest spoofing attacks. IMU based cross-checking detection requires the integration of additional modules into the receiver, which increases the receiver's cost. Signal encryption technique can be used to protect the real signal against the spoofing one. It however breaks the

* Corresponding author: Tel.: (+84) 985290681
Email: vinh.lathe@hust.edu.vn

GNSS receiver rule because this method adds digital signatures to the positioning messages making civilian receivers unworkable. Angle-of-arrival (AOA) based detection uses two or more antennas. In the usual cases, the GNSS signals are transmitted by different satellites and arrive at the receiver from different directions. On the contrary, counterfeit signals from one broadcaster are broadcasted from a single antenna and thus share a common AOA [5]. Therefore, we propose to use AOA to detect fake GNSS signals. We, however, enhance the approach by using an automatic detection threshold instead of using manually tuned value as can be seen in existing works [5, 9].

From the above analysis, this article focuses on the implementation of spoofing signal detection using the AOA measurement. In our proposal, we use a dual-antenna system to verify if some of the received signals have the similar AOA or not. Theoretically, DD values of fake signals from one broadcaster distribute densely around the zero point, because all the AOA-related terms are eliminated in the subtractions. Authentic signals have DD values diversely distributed due to the difference of AOA among satellites. Existing works [2, 5, 9-15] manually tune thresholds to distinguish those two distributions. However, the threshold is strongly affected by several factors like signal-to-noise ratio, elevation angle of satellites, ionospheric and tropospheric condition, etc. Therefore, we propose to use Gaussian Mixture Models to objectively learn parameters of the distributions over a large amount of training data. The trained GMMs later can well recognize authentic and spoofing distributions without any manually tuned parameters. In the remaining part of this paper, section 2 describes how we compute the double difference of the GNSS measurement, section 3 shows how we setup our experiment, section 4 presents the spoofing detection result in different scenarios, and finally we conclude our paper in section 5.

2. Carrier phase model and Double carrier phase model

The carrier phase measurement in the output of a receiver is determined as follows [5-6]:

$$\phi_i = d_i + N_i\lambda + c(dt_i - dT) - I_i + Tr_i + \varepsilon_i \qquad (1)$$

where:

i = 1, 2, 3 … denotes measurements from the i^{th} satellite,

ϕ_i is the carrier phase measurement, expressed in meters,

d_i is the geometric distance between the GNSS receiver and the i^{th} satellite,

N_i is the integer ambiguity,

λ is the wavelength of the carrier signal (approximately 0.19m for the GPS L1 frequency and 0.244m for the GPS L2 frequency),

c is the speed of light (approximately 3x108 m/s),

dt_i is the satellite clock error,

dT is the receiver clock error,

I_i is ionospheric error,

Tr_i is tropospheric error,

ε_i is unmodeled errors.

When two receivers are available and are synchronized on time, we can form a single carrier phase difference measurement [6]:

$$\Delta\phi = \Delta\phi_i^1 - \Delta = (d_i^1 - d_i^2) + \Delta N_i\lambda + c(dT^2 - dT^1) + \Delta\varepsilon_i \qquad (2)$$

where the superscript symbols [1] and [2] respectively, denote measurements from the receiver 1 and receiver 2. Two antennas are located at a distance which is small enough so that the ionospheric and tropospheric errors are mitigated in the above subtraction. Moreover, because the distance between satellites and receivers (~ 20,000km) is much greater than the distance between the two receivers, so the radio frequency (RF) waves are assumed to be in parallel as depicted in Fig.1. The distance between satellites and receivers can be expressed as:

$$d_i^1 - d_i^2 = Dcos\alpha_i \qquad (3)$$

where:

D is the distance between the two antennas,

α_i is the angle of arrival of the i^{th} satellite's signal. We can model the carrier phase single difference in units of cycles as:

$$\Delta\phi_i = \frac{\Delta\phi}{\lambda} = \frac{D}{\lambda}cos\alpha_i + \Delta N_i + \frac{c}{\lambda}(dT^2 - dT^1) + \frac{1}{\lambda}\Delta\varepsilon_i \qquad (4)$$

$\frac{c}{\lambda}(dT^2 - dT^1)$ is zero when two receivers are connected to the same oscillator (so they are suffered from the same clock bias). In our case, two receivers operate independently without sharing a common oscillator. Therefore, we have to construct the double carrier phase difference (DCPD) between satellite i^{th} and satellite j^{th} to remove the clock bias terms:

$$\Delta\nabla\varphi_{i,j} = \frac{D}{\lambda}\left(cos\alpha_i - cos\alpha_j\right) + \Delta\nabla N_{i,j} + \frac{1}{\lambda}\Delta\nabla\varepsilon_{i,j} \qquad (5)$$

(5) is used in the next section to implement our detector.

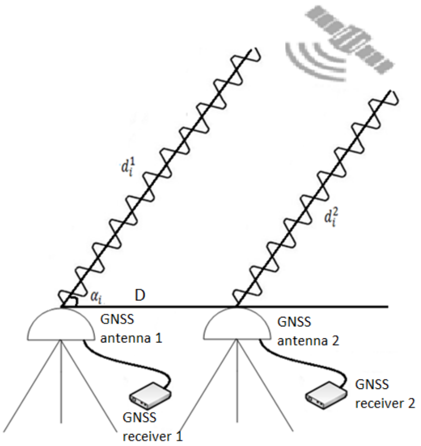

Fig. 1. Received signals from two closely spaced antennas of GNSS receivers.

3. System and setup

In our experiment, we simulate a simplistic spoofing attack where we attach a power amplifier and an antenna to a GNSS signal simulator, and we radiate the RF signal toward the target receivers. This experiment is carried out indoor in order to avoid the difficulty of synchronizing a simulator's output with the real GNSS signals. We use the IFEN NavX-NCS Essential one to generate and broadcast GNSS signals and Septentrio AsteRx4 OEM modules to receive signals. An example of system set up is reported in [2].

From Fig.2 (b), it is possible to see that the spoofer is located on a mezzanine at ISMB premises and comprises of a hardware simulator, a PC laptop running the SW part of the GNSS simulator and a choke ring passive Novatel antenna transmitting the amplified GNSS-like signals. In Fig.2(a) and (c), we can see the spoofing signal is received by a set of three antennas (forming two baselines) that are connected to two multi-constellation dual-antenna Septentrio receivers. It is important to stress that only one baseline would be necessary to detect the spoofing attack.

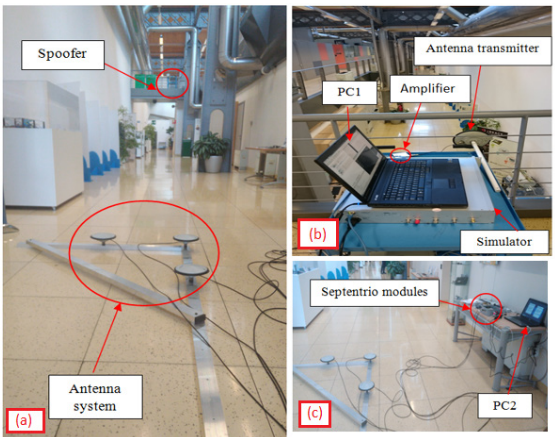

Fig. 2. System set up of a simplistic spoofing attack. The spoofer location (a), a view of the spoofer (b) and of the target receivers (c)

4. GMM classification result

The Gaussian distribution (or normal distribution) is defined by the below probability density function:

$$f(x|\mu,\sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \qquad (6)$$

Gaussian Mixture Model (GMM) [16] is a probabilistic model which assumes that every data point is generated from a linear combination of several Gaussian distributions. By using GMM, we can obtain a probability density function of a given dataset in the form of a single density function:

$$p(x) = \sum_{k=1}^{K} w_k f(x|\mu_k,\sigma_k^2) \qquad (7)$$

w_k is the weight factor of the k^th distribution (μ_k, σ_k).

In our work, we first build two datasets of DCPD values (illustrated in Fig.3a and 3c) for training Gaussian mixture models (or learning the density function in the form eq.7). Two models are trained on the two DCPD datasets corresponding to authentic and spoofed signals.

The difference of the two distributions is presented clearly in Fig.3b and Fig.3d. With the two models, we are able to decide if a set of GNSS data is spoofed or not depending on whether the value of the spoofed density function is higher or smaller than the one of the authentic density functions.

Using the GMM PDFs illustrated in Fig.3, we successfully detect 1921/1967 (97.66 %) authentic signal points and 8442/8586 (98.32%) spoofed patterns in our experiment. More detail about the experiment is described below.

We use the well-known cross validation testing method (*k*-fold with $k = 10$) to measure the performance of the proposed method. In 10-fold cross validation, the whole dataset is randomly shuffled and divided into 10 subsets, 9 sets are used to train the GMMs and the remaining is used for testing. Table 1 shows the results of the ten folds.

Table 1. The result of cross validation testing

Fold	#Training data points	#Testing data points	#Correctly classified points	Accuracy (%)
1	7643	848	835	98.46
2	7643	848	837	98.70
3	7643	848	834	98.34
4	7643	848	838	98.82
5	7643	848	834	98.34
6	7643	848	831	97.99
7	7643	848	831	97.99
8	7643	848	838	98.82
9	7643	848	840	99.05
10	7643	848	834	98.34
				98.52 (σ^2=0.1)

From table 2, we see the effect of cycle slips on the results is relatively large, since the average accuracy decreases to 93.25%. To overcome this problem, we use a Doppler shift monitor to detect and eliminate cycle slips as in [9].

Table 2. The testing result with cycle slips

Fold	#Training data points	#Testing data points	#Correctly classified points	Accuracy (%)
1	7643	848	785	92.57
2	7643	848	791	93.27
3	7643	848	779	91.86
4	7643	848	791	93.27
5	7643	848	790	93.16
6	7643	848	789	93.04
7	7643	848	795	93.75
8	7643	848	800	94.33
9	7643	848	790	93.16%
10	7643	848	798	94.10%
Total				93.25% (σ^2=0.5%)

To further investigate the effect of antenna distance on the classification result, we implement different experiments using a range of distance values. Result in Table 3 shows that antenna distance has almost no effect on the classification accuracy.

Table 3. The result of the difference of distance two antennas (λ = 19cm)

Length	#Training data points	#Testing data points	#Correctly classified points	Accuracy (%)
1λ	9398	1044	1033	98.94
2λ	8190	910	900	98.90
4λ	9038	1004	996	99.20
8λ	9492	1054	1038	98.48
				98.85 (σ^2=0.05)

5. Conclusion

A civil GPS spoofing is a pernicious type of intentional interference whereby a GPS receiver is fooled into tracking counterfeit GPS signals. One of the most promising techniques is the angle-of-arrival discrimination, which exploits differential carrier-phase measurements taken between multiple antennas. However, in existing work, manually tuned classification thresholds lead to dataset-dependent classification error rates making the detection less universal. Therefore, in this paper we propose a more robust approach to detect these spoofers using GMM. Our method still leverages the concept of AOA and requires multiple antennas. However, since the classification threshold is automatically learnt by GMMs, the algorithm can easily adapt to different antenna geometries and satellite conditions. Our classification success rate is about 98.5% for both fake and authentic signal patterns.

Acknowledgment

This work has been partly supported by the Vietnamese government in the framework of the bilateral project GILD Italia-Vietnam 2017–2019, NĐT.38.ITA/18. This work is also partially supported by the Domestic Master/ PhD Scholarship Programme of Vingroup Innovation Foundation.

The datasets in this paper were supported by Navigation Signal Analysis and Simulation (NavSAS) is a joint research group between LINKS Foundation, an R&D foundation, and Politecnico di Torino.

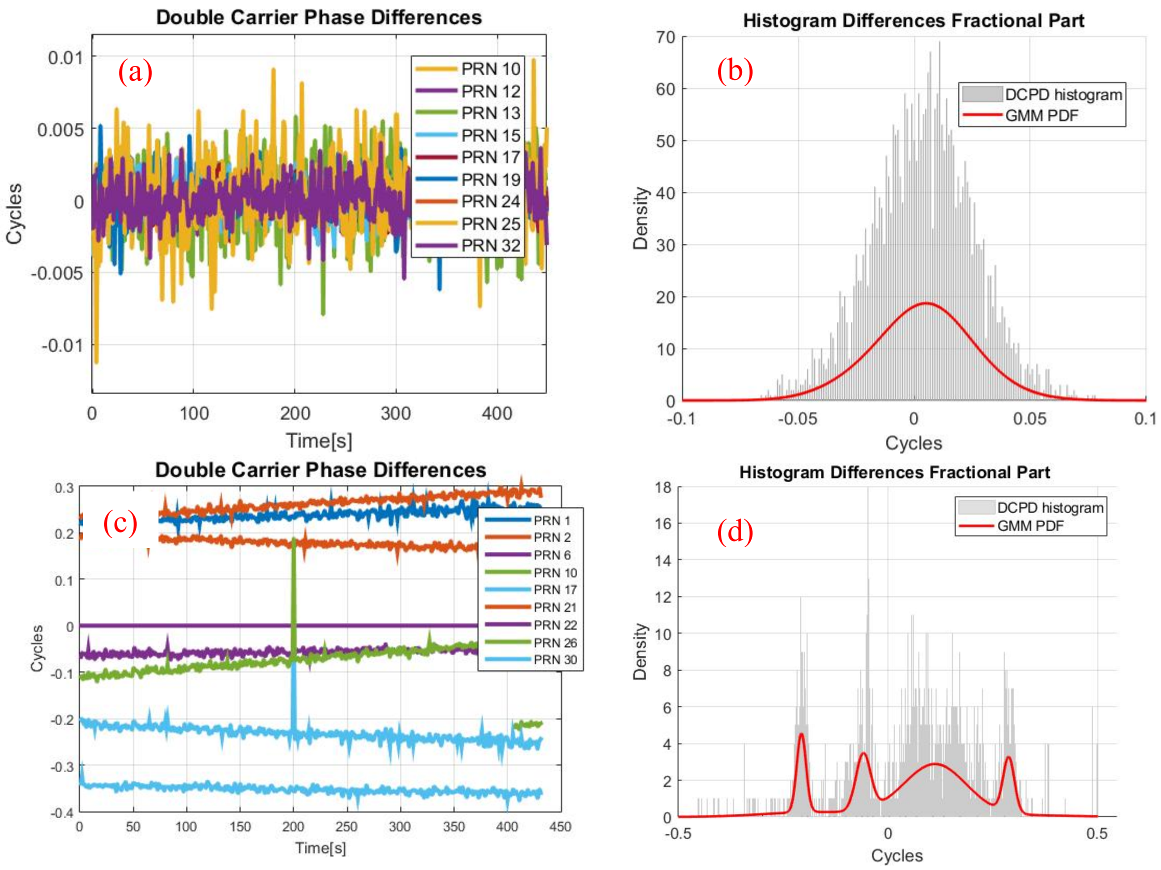

Fig. 3. Double carrier phase difference and GMM density functions of spoofed signals and authentic signals

References

[1] F. Dovis, Ed., GNSS Interference Threats and Countermeasures. Norwood, MA, USA: Artech House, 2015.

[2] Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O' Hanlon, B. W, and Kintner, Jr., P. M., Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer, Proceedings of ION GNSS 2008, Institute of Navigation, Savanna, GA, 2008.

[3] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer, in Proc. of the International Technical Meeting of the Institute of Navigation, (Anaheim, CA), pp. 124 – 130, Jan. 2009.

[4] Key, E. L., Techniques to Counter GPS Spoofing, Internal memorandum, MITRE Corporation, Feb. 1995.

[5] Borio, D., and Gioia, C. A dual-antenna spoofing detection system using GNSS commercial receivers. In Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS +), Tampa, FL, Sep. 2015, 1–6.

[6] Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System, Tech. rep., John A. Volpe National Transportation Systems Center, 2001.

[7] IFEN NavX-NCS Essential Simulator website: https://www.ifen.com/products/navx-ncs-essential gnss-simulator/

[8] https://www.septentrio.com/products/gnss-receivers/rover-base-receivers/oem-receiver-boards/asterx4-oem

[9] V. H. Nguyen, G. Falco, M. Nicola, E. Falletti, A Dual Antenna GNSS Spoofing Detector Based on the Dispersion of Double Difference Measurements, NAVITEC, Noordwijk, The Netherlands (2018).

[10] Rui Xu, Mengyu Ding, Ya Qi, Shuai Yue, Jianye Liu, Performance Analysis of GNSS/INS Loosely Coupled Integration Systems under Spoofing Attacks Sensors 2018 DOI:10.3390/s18124108.

[11] Y.F.Hu, S.F. Bian, B. Ji, J. Li, GNSS spoofing detection technique using fraction parts of double-difference carrier phases, J. Navig. 2018, 71, 1111–1129.

[12] Li He, Hong Li, Mingquan Lu, Dual-antenna GNSS spoofing detection method based on Doppler frequency difference of arrival, GPS Solutions July 2019.

[13] Y. Hu, S. Bian, K. Cao, B. Ji, GNSS spoofing detection based on new signal quality assessment model, GPS Solutions, vol. 22, pp. 28, Jan. 2018.

[14] Esteban Garbin Manfredini, Dennis M. Akos, Yu-Hsuan Chen, Sherman Lo, Todd Walter, and Per Enge, Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers, Proceedings of the Institute of Navigation International Technical Meeting, Reston, VA January 2018.

[15] G. Caparra, J.T. Curran, On the Achievable Equivalent Security of GNSS Ranging Code Encryption, in IEEE/ION Position, Location and Navigation Symposium (PLANS) 2018, (Monterey, California), 2018.

[16] Douglas Reynolds, Gaussian Mixture Models, Encyclopedia of Biometrics, pp. 659—663, Springer, ISBN: 978-0-387-73003-5.