Light-Weight GPS Spoofing Detection for Synchrophasors in Smart Grids

Xiao Wei
Electrical and Computer Engineering
National University of Singapore
Singapore
weixiao@u.nus.edu

Muhammad Naveed Aman
Computer Science
National University of Singapore
Singapore
naveed@comp.nus.edu.sg

Biplab Sikdar
Electrical and Computer Engineering
National University of Singapore
Singapore
bsikdar@nus.edu.sg

***Abstract*—The reliable operation of modern power grids depends on the accuracy of the synchrophasors produced by phasor measurement units (PMUs). However, PMUs rely on location and time information obtained from global positioning systems (GPS) which are vulnerable to spoofing attacks. This paper proposes a light-weight threshold-based GPS spoofing detection technique for synchrophasors. The proposed technique is based on the statistical runs test. The experimental evaluation shows that the proposed technique not only detects GPS spoofing attacks with high accuracy but is also efficient in terms of detection latency and can be used for real time applications in modern power systems.**

***Index Terms*—GPS spoofing detection, synchrophasors, Runs Test, phasor measurement units, power grid**

I. Introduction

A synchrophasor represents a complex phasor of an alternating current (AC) power system at the nominal system frequency synchronized to UTC (coordinated universal time) [1]. PMUs measure highly accurate synchrophasors for voltage and current at different buses of the electric power grid [2]. Any glitch in PMU data may lead to stability issues and even black outs, therefore, time synchronization is critical for the correct operation of PMUs. Thus, global positional systems (GPS) are used to provide the reference for time synchronization in PMUs.

The feasibility of GPS spoofing attacks was researched in many works. The present GPS spoofing methods can be classified into two categories, the GPS satellite position information is spoofed by ephemerides data manipulation or inserting a delay to shift the GPS signal time. Jiang et al. presented a problem formulation and simulation results to confirm the feasibility of GPS ephemerides spoofing in [3]. However, this method is not feasible in the physical real-life environments because it is not efficient enough and the spoofing attack in this way is restricted to statistic locations. Moreover, the GPS satellite information is designed to exist both in the almanacs and ephemerides, which make the long-distance position spoofing only through fake ephemerides is impossible. In contrast, the spoofing attacks by inserting delays, also known as the replay attack, are easier to implement. GPS spoofing by time-shifting is theoretically introduced by Tippenhauer et al. in [4]. In [5], a software defined radio (SDR) receiver platform is introduced by Humphreys et al., the platform is designed for GPS spoofing via inserting delays. In [5], a change in the victim receiver's tracking point can be successfully observed by gradually manipulating the signal delay and signal power. Recently, the simplest method for GPS spoofing is presented by Lin et al. [6] and Wang et al. [7]. In their works, the authentic ephemerides data and the intended spoofing location or time are fed into an open source code, GPS-SDR-SIM, to generate the fake GPS signal. Then the fake GPS signal is transmitted via a low-cost SDR device, such as BladeRF, HackRF or USRP. The use of GPS-SDR-SIM software and SDR devices gives attackers the convenience of carrying out low cost GPS spoofing attacks. Thereby increasing the probability of GPS receivers being attacked.

In view of the importance of GPS data and the harmful effects of GPS spoofing attacks, GPS spoofing detection is of utmost importance. The existing detection methods can be categorized into three types: external assistance, signal statistics, and cryptographic authentication. Many sensors or systems can be used as external assistance to provide additional information, such as jamming and noise sensors [8], inertial measurement unit (IMU) [9], cellular networks, and Internet or high-stability clocks [10]. The limitation of these methods is that the external helpers require additional hardware or the ability to access other systems. Conversely, the detection methods can only rely on the features inherent in the GPS signal. Typical examples are using the angle-of-arrival [11] [12] [13], signal quality [14] or signal power [15] [16] as detection statistic. Cryptographic authentication methods can be classified into two categories. The first is based on inserting some special information to the current GPS signal for verification at the GPS receiver such as the public key infrastructure (PKI) [17], signal authentication sequence (SAS) [18] or navigation message authentication (NMA) [19] [20]. The second category relies on the unpredictable cryptographic information carried by the GPS signal, such as the correlation distortion [21] [22] or the encrypted military P(Y) code authentication [23] [24]. These authentication methods have the advantage of higher confidence and robustness. Moreover, they do not require additional hardware or any changes to the current scheme. However, the authentication process increases the complexity of GPS signal processing and increases the

latency.

However, the studies on GPS spoofing mainly focus on GPS location spoofing, there are few works on the GPS time spoofing attacks. Only simulations are exhibited by Jiang et al [3] to show the feasibility of GPS time spoofing. [25] demonstrated a GPS spoofing attack to maximize the clock offset while maintaining a minimal location error. In [26], professional equipment, including RF front-end and back-end, DSP broad, and a single board computer are employed to introduce an experiment on GPS time spoofing attack. Besides these demonstrations, the existing detection methods all rely on external assistance, such as the reference synchronized clock or additional hardware support. Garofalo et al. [27] verified compromised GPS signals by using Network Time Protocol (NTP) as an alternative time reference. Zhang et al. [28] proposed a method of detecting clock synchronization attacks by monitoring the standard deviation of the differences in the signal-to-noise ratio from two GPS receiving antennas. A generalized likelihood ratio test of the time errors among different PMUs was introduced in [29]. [30] employed distributed multiple directional antennas with a common clock to detect spoofing. Signal correlation and power spectral density at multiple receivers are used in [22]. These techniques rely on multiple receivers or antennas which leads to higher complexity and may not be feasible for time-sensitive synchrophasors. To solve these issues, this paper proposes a light weight threshold based mechanism to detect GPS spoofing attacks in synchrophasors. The proposed technique is based on a statistical test called the Runs test.

The rest of the paper is organized as follows: Section II describes the system model and the proposed technique is presented in Section III. Simulation results are discussed in Section IV and the paper conclusions are given in Section V.

II. System Model

Let us consider the system model shown in Figure 1. In this model we have GPS satellites sending authentic signals to a PMU. However, an attacker eavesdrops on the signals. The attacker generates fake signals based on the eavesdropped signals and the position of PMU, then broadcasts them to the PMU. The signal received by PMU at GPS civil frequency is a mixture of authentic GPS signals and fake signals.

III. Proposed Technique

Let us denote the authentic signal sent by the GPS satellite by $x(t)$, and the signal received by the PMU as $y(t)$. In the absence of any adversary [31]:

$$y(t) = H * x(t) + \eta, \tag{1}$$

where H represents the wireless channel coefficients, and η is the additive white Gaussian noise (AWGN) [32]. The adversary can also receive $y(t)$ and produce a spoofed signal as follows:

$$y'(t) = H * x'(t) + \eta, \tag{2}$$

where $x'(t)$ is the tampered GPS signal. Using a high powered software defined radio, the adversary can cause the authentic

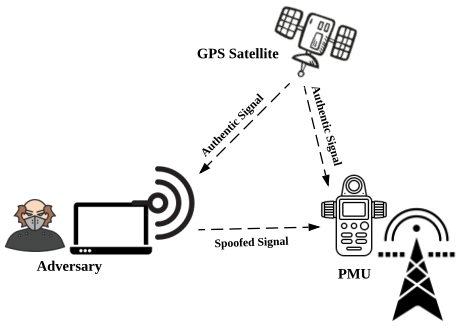
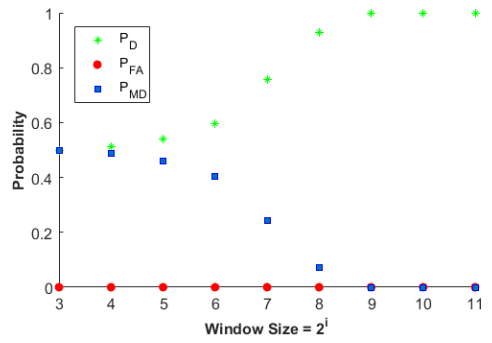


Fig. 1: System Model.

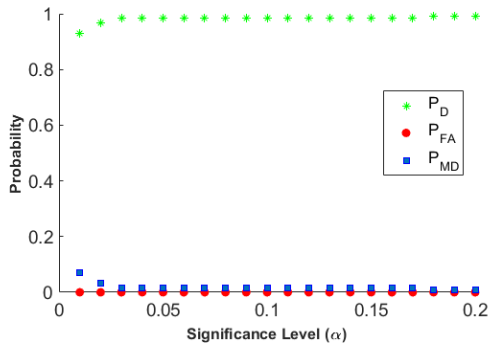
signal sent by the GPS satellite to weaken and therefore, the PMU will consider $y'(t)$ as the authentic signal received from the GPS satellite. However, to produce a spoofed signal and disturb the synchronization of the PMU clock, the adversary replays a previously captured signal. Thus, we expect some degree of auto-correlation in $y'(t)$ for different sampling instants. Thus, to detect this correlation among different received signals we use a windowed approach, i.e., we combine multiple received signals over a time period to create a GPS window. However, to capture correlation among different received signals we take the power spectral density (PSD) of the received signal instead of the signal itself. For example, consider a series of received signals $y(t_i)$, $y(t_i+1)$, $\cdots$, $y(t_i+T-1)$, where t_i is the current time instant and T is the window size. Let us denote the PSD for these signals as P_0, P_1, $\cdots$, P_{T-1}, then a GPS window is defined as a vector $\mathbf{W}_{t_i} = [P_0, P_1, \cdots, P_{T-1}]^T$. Thus, we compare the current window $\mathbf{W}_{t_i}$ with the previous window $\mathbf{W}_{t_i-1}$ to detect any correlation, this is done using the well-known runs test, i.e., we perform a hypothesis test as follows:

$$\begin{aligned} H_0 &: \text{The elements of } \mathbf{W} \text{ are } \textbf{not} \text{ correlated,} \\ H_1 &: \text{The elements of } \mathbf{W} \text{ are correlated,} \end{aligned}$$

where H_0 is the null hypothesis representing no GPS spoofing attack. Note that $y(t)$ and $y'(t)$ are independent but drawn from the same distribution. The runs test checks the PSD distribution consistency between the current and previous windows. Since the samples on the two signals' PSD are independent and drawn from the same distribution, the purpose of runs test is to check if the distributions of the two windows are consistent or not. If the distributions are consistent then runs test rejects the null hypothesis and we can assume there is an attack on the GPS signal. Otherwise, if the distributions are not consistent then the null hypothesis is accepted and the system is considered secure. The runs test outputs a quantitative measure called *run* r which represents the level of correlation present between two vectors. Thus, a higher value of r means the null hypothesis can be rejected. In this paper, we use a threshold approach to detect GPS spoofing attacks such that if $r \leq \gamma$, then we reject the null hypothesis and



(a)



(b)

Fig. 2: Affect of window size and runs test significance level on the proposed technique.

raise an alarm to flag an attack. The value of the threshold γ is determined empirically using experiments.

IV. Experimental Evaluation

To evaluate the effective of the proposed technique, we conducted experiments using equipment from National Instruments (NI). A GPS antenna was connected to a NI USRP-2943R software defined radio re-configurable device to receive signals at GPS L1 frequency. The configuration parameters of for the experimental setup are listed in Table Ia. LabView and Matlab were used to process the received GPS signals. We collected a total of 13864 signal samples. To generate the spoofed signals we used the gps-sdr-sim software to spoof the location and time. The spoofed signals were then broadcasted at GPS L1 frequency via BladeRF x115 to overlap the actual GPS signals sent by the GPS satellite. The configuration parameters for BladeRF are listed in Table Ib.

TABLE I: The configuration parameters

(a) NI USRP - 2943R

Parameters	Carrier Frequency	IQ rate	Gain	Active Antenna
Values	1575.42M	1M	25	RX1

(b) BladeRF X115

Parameters	Frequency	Sample rate	Bandwidth	txvga
Values	1575.42M	2.6M	2.5M	-25

The performance of the proposed technique is evaluated on the bases of probability of detection P_D, probability of false alarm P_{FA} (i.e., the ratio of the number of times the proposed technique inferred an attack while there was no attack) and probability of missed detection P_{MD} (i.e., the ratio of number of times the proposed technique inferred no attack while there was an attack). To study the affect of window size on the proposed technique, Figure 2(a) shows the three performance metrics as the window size is increased from 2^3 to 2^{11}. We observe that P_{FA} is negligible while P_D increases with window size and P_{FA} is reduced with window size. We observe that P_D is above 90% for a window size of 256 samples. Moreover, to study the affect of the significance level α of the runs test on the proposed technique, Figure 2(b) show the three performance metrics as the significance level in the runs test is increased from 0 to 0.2, i.e., 0 to 20% significance level with a fixed window size of 256 samples. We observe that the accuracy of the proposed technique increases with the increase in significance level. From Figure 2 we observe the optimal values for window size and significance level to be 256 samples and 0.05, respectively. Note that a larger window size and higher significance level lead to higher computational complexity which is translated to higher latency to detect attacks. However, using the optimal parameters, i.e., $T = 256$ and $\alpha = 0.05$, the latency to detect attacks for the proposed technique on an intel core-i5 7th generation processor was 10 μ-seconds on the average, i.e., well below the 26.5 μ-seconds standard defined by the IEEE-C37.118 standard for PMUs.

V. Conclusion

This paper presented a light-weight GPS spoofing detection technique for synchrophasors. The PSD of the received signals is used to detect any correlation in the previously recorded GPS readings and the current readings using the runs test which is an indication of a GPS spoofing attack. Experiments using a realistic scenario using actual GPS hardware shows that the proposed technique can detect attacks with an accuracy of approximately above 99% and negligible miss-classification rates with a detection latency of less than 10 μ-seconds.

References

[1] A. Rashid, M. N. Aman, M. Ullah, and B. Sikdar, "Detecting data tampering in synchrophasors using power flow entropy," in *IEEE PES ISGT-Asia*, 2018, pp. 850–855.

[2] M. N. Aman, K. Javed, B. Sikdar, and K. C. Chua, "Detecting data tampering attacks in synchrophasor networks using time hopping," in *IEEE PES ISGT-Europe*, 2016, pp. 1–6.

[3] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, A. D. Domı *et al.*, "Spoofing gps receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253–3262, 2013.

[4] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, pp. 75–86.

[5] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Radionavigation laboratory conference proceedings*, 2008.

[6] L. Huang and Q. Yang, "Gps spoofing: Low-cost gps simulator," *DEF CON*, vol. 23, 2015.

[7] K. Wang, S. Chen, and A. Pan, "Time and position spoofing with open source projects," *black hat Europe*, vol. 148, 2015.

[8] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," in *2015 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2015, pp. 1–6.

[9] N. A. White, P. S. Maybeck, and S. L. DeVilbiss, "Detection of interference/jamming and spoofing in a dgps-aided inertial system," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 34, no. 4, pp. 1208–1217, 1998.

[10] Y. Bardout, "Authentication of gnss position: An assessment of spoofing detection methods," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 2011, pp. 436–446.

[11] E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge, "Single antenna gps spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications," in *Proceedings of the 27th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2014), Tampa, FL*. Citeseer, 2014, pp. 2233–2242.

[12] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses raim," in *proceedings of the 25th international technical meeting of the satellite division of the Institute of Navigation (ION GNSS 2012)*, 2012, pp. 3007–3016.

[13] 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 *Proceedings of the 2009 International Technical Meeting of The Institute of Navigation*, 2009, pp. 124–130.

[14] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal quality monitoring applied to spoofing detection," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 2011, pp. 1888–1896.

[15] D. M. Akos, "Who's afraid of the spoofer? gps/gnss spoofing detection via automatic gain control (agc)," *NAVIGATION: Journal of the Institute of Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[16] P. Vahid, J. Nielsen, and G. Lachapelle, "Gnss spoofing detection based on receiver c/n0 estimates," in *Proc. ION GNSS12 Conf.*, 2012, pp. 2878–2884.

[17] L. Scott, "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 Navigation (ION GPS/GNSS 2003)*, 2003, pp. 1543–1552.

[18] O. Pozzobon, L. Canzian, M. Danieletto, and A. Dalla Chiara, "Anti-spoofing and open gnss signal authentication with signal authentication sequences," in *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*. IEEE, 2010, pp. 1–6.

[19] O. Pozzobon, "Keeping the spoofs out: Signal authentication services for future gnss," *Inside GNSS*, vol. 6, no. 3, pp. 48–55, 2011.

[20] M. N. Aman, K. C. Chua, and B. Sikdar, "Physically secure mutual authentication for iot," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017, pp. 310–317.

[21] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for gnss-signal authentication," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 1, pp. 469–475, 2018.

[22] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "Gnss signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 739–754, 2017.

[23] L. Heng, D. Chou, and G. X. Gao, "Cooperative gps signal authentication from unreliable peers," in *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014)*, 2014, pp. 2801–2809.

[24] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Gps spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

[25] X. Wei and B. Sikdar, "Impact of gps time spoofing attacks on cyber physical systems," in *IEEE ICIT*, 2019, pp. 1155–1160.

[26] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[27] A. Garofalo, C. Di Sarno, L. Coppolino, and S. D'Antonio, "A gps spoofing resilient wams for smart grid," in *European Workshop on Dependable Computing*. Springer, 2013, pp. 134–147.

[28] Z. Zhang, M. Trinkle, A. D. Dimitrovski, and H. Li, "Combating time synchronization attack: A cross layer defense mechanism," in *2013 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2013, pp. 141–149.

[29] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "Gps spoofing attack characterization and detection in smart grids," in *2016 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2016, pp. 391–395.

[30] S. Bhamidipati, K. J. Kim, H. Sun, and P. V. Orlik, "Gps spoofing detection and mitigation in pmus using distributed multiple directional antennas," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–7.

[31] M. N. Aman, W. K. Chan, and B. Sikdar, "Collision detection in ieee 802.11 networks by error vector magnitude analysis," in *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 5218–5223.

[32] M. N. Aman and B. Sikdar, "Distinguishing between channel errors and collisions in ieee 802.11," in *2012 46th Annual Conference on Information Sciences and Systems (CISS)*, 2012, pp. 1–6.