Impact of GPS Time Spoofing Attacks on Cyber Physical Systems

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

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

***Abstract*—The development of software defined radio platforms and related open source software have made it possible to generate and broadcast global positioning system (GPS) signals easily and at low cost. Since GPS time is widely used in time sensitive systems for time reference, any attack on GPS can have serious consequences. This paper evaluates GPS time spoofing attacks in cyber physical systems. We explore methods to spoof the GPS time by manipulating the GPS timestamp or the signal propagation time of GPS satellite signals. In our experiments, the impact of GPS time spoofing attacks on the pseudorange, receiver location, and time errors is investigated. Our results show that when only the GPS timestamp is changed or the same delay is introduced to all signals, the resulting location error and pseudorange error can be very small, making it difficult to detect. In particular, the attacks achieved by inserting the same delay have constant location error and negligible pseudorange error. Conversely, the attacks that insert different delay to each signal or change the GPS timestamp at the same time usually lead to large location error and pseudorange error that are easy for attack detection. Moreover, the attacks that change the propagation time are difficult to distinguish irrespective of whether it can cause enough damage to violate the IEEE C37.118 standard or not.**

***Index Terms*—GPS time spoofing attack, cyber-physical systems, power grids**

I. Introduction

Besides its well-known precise positioning service, the GPS can also provide exact time synchronizing with the accuracy of a few nanoseconds [4], since the GPS signals have time accuracy within 10 billionths of a second with the use of atomic clocks. Many time-sensitive systems rely on GPS signals for timing information. Humphreys et al. have shown that electric power grids are vulnerable to the GPS time spoofing attack since they require accurate time synchronization for measurement and state estimation [6]. A large time error at the phasor measurement units (PMUs) may have serious consequences, including a black-out. Moreover, GPS time is used as transaction timestamp in financial exchanges, and even nanoseconds time error may lead to serious consequences for global markets. Major communications networks (e.g. Long Term Evaluation (LTE)), banking systems, etc. depend heavily on GPS for precise time synchronization as well.

However, the GPS civilian signal is easy to capture, process and generate. With the improvement of radio frequency hardware and the software defined radio (SDR) platform, it is not difficult to find a device which can receive and transmit signals in GPS civilian frequency. The attacks can also take advantage of the unencrypted GPS civilian signals to extract the GPS information. In addition, due to the long distance attenuation, ionospheric interference and other effects, the received carrier power is around -158.5 dBw [3] and the signal to noise ratio (SNR) is a small value. This makes the authentic GPS signal susceptible to interference from other signals with greater signal power. All of these factors make a GPS receiver vulnerable to GPS spoofing attacks.

GPS spoofing attacks aim to fool the victim receiver to a false position or time by broadcasting a fake signal. According to Humphreys et al., existing spoofing attacks can be classified into three categories: simplistic attack, intermediate attack and sophisticated attack [1]. A simplistic attack broadcasts GPS signals without taking into account any information specific to the victim receiver. The intermediate attack is based on the GPS signal received by the victim receiver. The attacker generates the fake GPS signal using the information extracted from the authentic signal. By processing this fake signal, the GPS receiver can be spoofed to a false location and time. The sophisticated attack employs several coordinated antennas to emulate the spatial signal domain, which reduces the pseudorange and Doppler variation correlation, and makes the attack difficult to detect. Since GPS spoofing attacks not only affect the operation of navigation systems or transportation system but also bring serious safety issues in a number of cyber-physical systems, a detailed analyses of GPS time spoofing attacks and the development of effective and accurate spoofing detection techniques are desirable. This paper focuses on GPS time spoofing attacks. Two variables, the GPS timestamp and the signal propagation time were manipulated to carry out GPS time spoofing attacks and we investigated the relationship between pseudorange error, location error and the receiver time error under different spoofing scenarios. In addition, our simulation results showed the possibility of conducting a GPS time spoofing attack with low pseudorange error and receiver location error.

The main contributions of this paper are as follows:

1. We investigate various time spoofing methods by generating fake GPS signals.

2. We demonstrate the possibility of conducting a GPS time

spoofing attack with low error in pseudorange and receiver location.

3. We investigate whether it is possible to distinguish attacks that break the IEEE C37.118 standard from attacks that do not.

The rest of the paper is organized as follows. In Section II we provide a survey of existing studies on GPS spoofing attacks, including the spoofing methods and detection methods. We introduce the spoofing environment, the composition of GPS receiver time and observation aspects in Section III. Section IV describes the methods used in this paper to spoof GPS time. The simulation results are presented in Section V. Finally, Section VI concludes the paper.

II. Related Work

The existing GPS spoofing methods mainly focus on changing the GPS satellite position information by manipulating the ephemerides data or shifting the GPS signal time through a delay. Jiang et al. investigated the influence of fake ephemerides in the positioning and timing process in [2]. The authors presented a problem formulation and simulation results to confirm the feasibility of GPS ephemerides spoofing. However, this method may not be feasible in the physical real-life environments. Firstly, it is not efficient enough since it requires at least 30 seconds to transmit the fake ephemerides data. Secondly, the spoofing attack in this way is restricted. The changes on the GPS satellite information is fixed during a period of time due to which it cannot spoof the victim receiver on a dynamic route. Additionally, the long-distance position spoofing is impossible since the GPS satellite information exists both in the almanacs and ephemerides. In contrast, it is easier to carry out multiple spoofing attacks by shifting the time, which are usually called replay attacks. Tippenhauer et al. [7] theoretically formulated the GPS spoofing problem. Humphreys et al. detailed the development of a SDR receiver platform for GPS spoofing in [1]. In their scheme, by gradually changing the delay, a change in the victim receiver's tracking point can be successfully observed in an intermediate spoofing attack. A simple way for GPS spoofing is presented by Lin et al. [5] and Wang et al. [8]. They use the ephemerides data and the intended spoofing location or time to generate the fake GPS signal through an open source code: GPS-SDR-SIM. Then the fake GPS signal is transmitted via a low-cost SDR device, such as BladeRF, HackRF or USRP.

Among existing studies, only a few focus on the time spoofing attack. Shepard et al. introduced a GPS time spoofing attack experiment with professional equipment, RF front-end and back-end, DSP broad and a single board computer [6]. Jiang et al. only exhibited the feasibility of GPS time spoofing by simulations [2].

III. Problem Definition

In this paper, we explore the possible GPS time spoofing attacks under the environment of power grids. The impact of different GPS time spoofing attacks is evaluated using simulations. In the scenario of power grids, the GPS receivers which are equipped in the Phasor Measurement Units have the property of fixed location. Thus, the attacker conducts GPS spoofing attacks by generating and broadcasting fake GPS signals.

According to the GPS positioning principle, the parameters, including GPS satellite positions, GPS receiver location, GPS receiver time, GPS signal timestamp, should satisfy Equation (1):

$$\sqrt{(x_s^i - x_r)^2 + (y_s^i - y_r)^2 + (z_s^i - z_r)^2} = c(t_r - t_{GPS}^i) \quad (1)$$

where $\left(x_s^i, y_s^i, z_s^i\right)$ represents the position of the i-th visible GPS satellite, (x_r, y_r, z_r) refer to the position of the GPS receiver, t_r is the GPS receiver time, and t_{GPS}^i is the timestamp of the i-th GPS satellites signal.

The time difference between the i-th GPS satellite and the GPS receiver is equal to the signal propagation time (Δt_i) plus clock error (τ) as shown in Equation (2). Since all GPS satellites are equipped with an atomic clock, the GPS satellites are time synchronized. Hence, the clock error between satellites and a receiver is same.

$$t_r - t_{GPS}^i = \tau + \Delta t_i. \quad (2)$$

Since Equation (2) can be written as

$$t_r^i = \tau + \Delta t_i + t_{GPS}^i, \quad (3)$$

we can see that the receiver time is dependent on the time deviation, signal propagation time and the signal transmitting timestamp. Theoretically, there are three ways to spoof the time of the victim GPS receiver: changing the propagation time, changing the GPS timestamp, and changing both of them. These methods for GPS time spoofing will be discussed in Section IV.

In our experiments, the GPS timestamp and signal propagation time are manipulated to conduct a time spoofing attack. At the same time, the receiver location error and pseudorange error are observed. As observed in [2], the time spoofing attack may also affect the calculated receiver location. Hence, the location error caused by GPS spoofing for a fixed location receiver in power grids is more sensitive and obvious than that in other location unknown systems. Moreover, the pseudorange is closely related to the receiver time. The pseudo distance from the satellite to the receiver is marked by pseudorange:

$$\rho_i = c(t_r - t_{GPS}^i) \quad (4)$$

As shown in Equation (4), the pseudorange is obtained by multiplying the speed of light by the time that the signal has taken from the satellite to the receiver, including the time deviation caused by the atmospheric delay or other bias. Therefore, our objective is to investigate the location changes and pseudorange changes that result from various GPS time spoofing attacks.

IV. Possible GPS Time Spoofing Methods

In this section, we analyze the GPS time spoofing methods in detail and we introduce algorithms to simulate each attack method. Since a clock error greater than 36.5 μs breaks IEEE

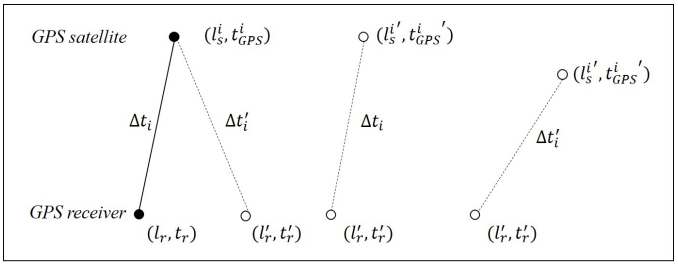

Fig. 1. Illustration of satellite position and receiver location and time: (a) changing the signal propagation time (b) changing the GPS timestamp (c) simultaneous change of GPS timestamp and propagation time.

Algorithm 1: Only change the GPS timestamp

Input: l_i^{GPS}, ρ_i, i= 1 to 4; t^{GPS}; l^r; τ; eph
Output: δ_t; δ_l; δ_i^ρ

for $\delta_t^{GPS} \leftarrow -53\mu s$ *to* $53\mu s$ *step 265ns* **do**
  $t^{GPS'} \leftarrow \delta_t^{GPS} + t^{GPS}$;
  $l_i^{GPS'} \leftarrow f(t^{GPS'}, eph)$;
  $(l^{r'}, \tau') \leftarrow g(t^{GPS'}, l_i^{GPS'}, \rho_i)$;
  $\delta_t \leftarrow \tau' - \tau + \delta_t^{GPS}$;
  $\delta_l \leftarrow norm(l^{r'} - l^r)$;
  $\delta_i^\rho \leftarrow abs(c(\tau' - \tau))$;
end

C37.4 standards and may lead to disruption of power grids, we manipulated the GPS timestamp and signal propagation time with errors (Δt^{GPS} and d_i^{GPS}) from -53 μs to 53 μs in order to conducting time spoofing attacks that can result in time errors of around two times 36.5 μs for observation. In addition, a negative GPS timestamp error leads the calculated receiver time to be earlier than the actual time while a positive GPS timestamp error causes the calculated receiver to be later than the actual time.

A. Changing the GPS timestamp

In this method, we change the GPS timestamp (t_{GPS}^i) to a spoofed timestamp ($t_{GPS}^{i\,'}$) while keeping the signal propagation time Δt_i unchanged. As shown in Figure 1(b), the signal propagation time is unchanged while the timestamp at a GPS satellite is changed which causes the receiver to make an error in positioning and timing. From the GPS positioning principle in Equation (1), the receiver's calculated location (x_r', y_r', z_r') and time (t_r^i) should satisfy the following equation:

$$\sqrt{(x_s^{i\,'} - x_r')^2 + (y_s^{i\,'} - y_r')^2 + (z_s^{i\,'} - z_r')^2} = c(t_r^{i\,'} - t_{GPS}^{i\,'}). \tag{5}$$

According to the Equation (3), the spoofed time is

$$t_r^{i\,'} = \tau^{'} + \Delta t_i + t_{GPS}^{i\,'}, \tag{6}$$

where the $\tau^{'}$ is a new clock error between GPS receiver and the i-th satellite.

The spoofed pseudorange is

$$\rho_i{}' = c(t_r^{i\,'} - t_{GPS}^{i\,'}) = c(\tau^{'} + \Delta t_i). \tag{7}$$

To conduct this attack, the fake GPS signals are generated with a timestamp which is different from the genuine timestamp. Moreover, the spoofed signal is transmitted later than the original one, to keep the propagation time unchanged. In this paper, the attack is simulated in Matlab using Algorithm 1.

The GPS timestamp error (δ_t^{GPS}) is increased from -53μs to 53μs while keeping the signal delay unchanged. The spoofed GPS time stamp ($t^{GPS'}$) is equal to the timestamp error plus the original timestamp (t^{GPS}). Thus, the spoofed GPS position (l^{GPS}) is calculated according to the timestamp and the GPS ephemerides (eph) by GPS position function $f(\cdot)$. The provided GPS location and timestamp (l^{GPS} and t^{GPS}) are used to calculate the location (l^r) and clock offset (τ') of the GPS receiver by function $g(\cdot)$ (Equation (5)). According to Equations (3) and (6), the receiver time error is the difference between the calculated clock offset and the real clock offset (τ) plus the GPS timestamp error:

$$\delta_t = t_r^{i\,'} - t_r^i = \tau^{'} - \tau + \delta_t^{GPS}. \tag{8}$$

The receiver location error is the distance between the calculated location l^r and the real location l^r. From Equations (4) and (7), the pseudorange error is equal to the speed of light (c) multiplied with the clock offset difference:

$$\delta_i^\rho = \rho' - \rho = c(\tau' - \tau). \tag{9}$$

B. Changing the GPS signal propagation delay

In this method, we change the signal propagation time by inserting a delay (Δt_i) while keeping (t_{GPS}^i) unchanged. As shown in Figure 1(a), the GPS satellite position is authentic during attack, but the manipulated propagation time causes location and time errors at the receiver side.

As we insert a delay for each signal, from Equation (1), the parameters should satisfy:

$$\sqrt{(x_s^i - x_r')^2 + (y_s^i - y_r')^2 + (z_s^i - z_r')^2} = c(t_r^{i\,'} - t_{GPS}^i). \tag{10}$$

According to Equation (3), the received time is

$$t_r^{i\,'} = \tau' + \Delta t_i' + t_{GPS}^i \tag{11}$$

Moreover, from Equation (4), the spoofed pseudorange is

$$\rho_i{}' = c(t_r^{i\,'} - t_{GPS}^i) = c(\tau' + \Delta t_i + d_i^{GPS}) \tag{12}$$

For conducting an attack, the spoofed GPS signal is generated with the original GPS time stamp and transmitted later or before the authentic GPS signal to change the propagation time.

Since the GPS positioning and timing calculations require at least four GPS satellites and each GPS satellite is located differently in space, the signal propagation time from each satellite to a receiver is different. The propagation time of each signal can be changed by the same amount or by a different amount.

Algorithm 2: Only change the propagation time by the same amount

Input: l_i^{GPS}, ρ_i, i= 1 to 4; t^{GPS}; l^r; τ; eph
Output: δ_t; δ_l; δ_i^ρ

for $d^{GPS} \leftarrow -53\mu s$ *to* $53\mu s$ *step 265ns* **do**
  $(l^{r'}, \tau') \leftarrow g(t^{GPS}, l_i^{GPS}, \rho_i)$;
  $\delta_t \leftarrow \tau' - \tau$;
  $\delta_l \leftarrow norm(l^{r'} - l^r)$;
  $\delta_i^\rho \leftarrow abs(c(\tau' - \tau + d^{GPS}))$;
end

1) Same delay for all satellite signals: To change the propagation time for different satellites by the same amount, a delay is inserted to all signals. Algorithm 2 is used to simulate this scenario. A delay (d^{GPS}) is generated by increasing linearly from -53μs to 53μs while the GPS timestamp has not been tampered with. The false GPS signal propagation time is equal to the real propagation time plus the provided delay. The victim receiver computes a fake location and clock offset, using the fake propagation time and the real GPS timestamp and location as input to Equation (10). Since the GPS timestamp is unchanged, the clock error is equal to the difference between the actual and calculated clock offset:

$$\delta_t = \tau' - \tau. \tag{13}$$

The pseudorange error is computed by multiplying the speed of light with the sum of clock error and inserted delay:

$$\delta_i^\rho = c(\tau' - \tau + d_i^{GPS}). \tag{14}$$

2) Different delay for each satellite signal: Alternatively, the propagation time can be manipulated differently for each satellite by inserting different delays. As shown in Algorithm 3, the delay for each satellite (d_i^{GPS}) is randomly generated between -53μs and 53μs and n is used as the iteration index. In our simulations, we used $n = 400$ and obtained 400 samples. As in Algorithm 2, the victim receiver uses these signal propagation times and the authentic GPS position to calculate its location and clock offset which leads to the location and clock errors. The pseudorange error of each satellite is calculated respectively according to the inserted delay.

Algorithm 3: Only change the GPS timestamp

Input: l_i^{GPS}, ρ_i, i= 1 to 4; t^{GPS}; l^r; τ; eph
Output: δ_t; δ_l; δ_i^ρ

for $n \leftarrow$ *1 to 400* **do**
  $d_i^{GPS} \leftarrow random(-53\mu s \text{ to } 53\mu s)$;
  $(l^{r'}, \tau') \leftarrow g(t^{GPS}, l_i^{GPS}, d_i^{GPS}, \rho_i)$;
  $\delta_t \leftarrow \tau' - \tau$;
  $\delta_l \leftarrow norm(l^{r'} - l^r)$;
  $\delta_i^\rho \leftarrow abs(c(\tau' - \tau) + d_i^{GPS})$;
  $n \leftarrow n + 1$;
end

C. Simultaneous change of GPS timestamp and signal propagation time

In this method, we change the signal propagation time Δt_i and GPS timestamp t_{GPS}^i at the same time. As shown in Figure 1(c), the calculated GPS position is changed since the GPS timestamp is different, and the propagation time has been modified.

According to the GPS positioning principle, the parameters fulfill the following Equation:

$$\sqrt{(x_s^{i'} - x_r')^2 + (y_s^{i'} - y_r')^2 + (z_s^{i'} - z_r')^2} = c(t_r^{i'} - t_{GPS}^{i\,'}) \tag{15}$$

The spoofed time is

$$t_r^{i'} = \tau' + \Delta t_i' + t_{GPS}^{i\,'} \tag{16}$$

and the spoofed pseudorange is

$$\rho_i' = c(t_r^{i'} - t_{GPS}^{i\,'}) = c(\tau' + \Delta t_i + d_i). \tag{17}$$

To conduct this kind of spoofing attack, the fake GPS signal is generated with a GPS timestamp $t_{GPS}^{i\,'}$ that is different from the authentic one. At the same time, the faked GPS signal for the i-th satellite is transmitted with a delay d_i.

Algorithm 4 shows the simulation methodology. The GPS timestamp error and the delays that are inserted to each satellite signal are generated randomly from -53μs to 53μs. The GPS position is calculated using the provided GPS timestamp and the received authentic ephemerides via GPS satellites position function $f(\cdot)$. The receiver location and clock offset are calculated by the provided GPS position information and the false propagation times via Equation (15). The receiver clock error and pseudorange error are calculated using Equations (8) and (14), respectively.

Algorithm 4: Only change the GPS timestamp

Input: l_i^{GPS}, ρ_i, i= 1 to 4; t^{GPS}; l^r; τ; eph
Output: δ_t; δ_l; δ_i^ρ

for $n \leftarrow$ *1 to 400* **do**
  $d_i^{GPS} \leftarrow random(-53\mu s \text{ to } 53\mu s)$;
  $\delta_t^{GPS} \leftarrow random(-53\mu s \text{ to } 53\mu s)$;
  $t^{GPS'} \leftarrow \delta_t^{GPS} + t^{GPS}$;
  $(l^{r'}, \tau') \leftarrow g(t^{GPS'}, l_i^{GPS'}, d_i^{GPS}, \rho_i)$;
  $\delta_t \leftarrow \tau' - \tau + \delta_t^{GPS}$;
  $\delta_l \leftarrow norm(l^{r'} - l^r)$;
  $\delta_i^\rho \leftarrow abs(c(\tau' - \tau) + d_i^{GPS})$;
end

V. Simulation Results

Our simulations consider a scenario with four satellites and one receiver. The simulations use the GPS navigation toolbox from MathWorks. The actual GPS signal transmission time is at GPS epoch time 247079.926271138 while the actual GPS signal received time is at epoch time 247080. The GPS ephemerides record the GPS satellites navigation

TABLE I
POSITIONS OF GPS SATELLITES AND RECEIVER IN ECEF

Name	*X*	*Y*	*Z*
Sat. 1	16126524.5052064	-15547762.6633447	14383520.4858258
Sat. 2	12603610.5415753	12117327.4879380	20031907.9625531
Sat. 3	25942474.2728668	-4759620.41858934	4338909.54401078
Sat. 4	21058564.0351066	16301904.2272398	2284049.46872917
Rcvr.	3894192.03660674	318961.824436966	5024275.88464529

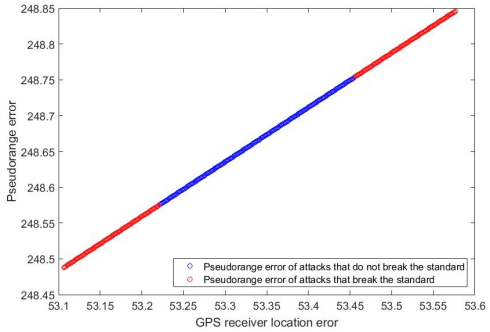

Fig. 2. Relationship between location error and pseudorange error when only the GPS timestamp is changed.

messages of this day. The actual positions of the four GPS satellites and the GPS receiver are listed in Table V in ECEF (earth-centered, earth-fixed) coordinates in meters. The actual pseudorange values for each satellite are 22112811.5587781, 20982905.7182692, 22636015.7464408, 23613050.5864770 meters.

A. Impact of changing GPS timestamp

The relationship between pseudorange error and location error is displayed in Figure 2. The red data points represent attacks that break the IEEE C37.118 standard for power grids (i.e., where the error is larger than 26.5 μs) while the blue data points represent attacks that do not cause enough error to break the standard. Our results show that standard-break attacks can have pseudorange error lower than 248.6m and location error lower than 53.2m, which are less than standard-not-break attacks. Since these errors are not very significant, it is difficult to distinguish this kind of attacks from normal interference only by considering the pseudorange error and receiver location error.

B. Impact of changing the propagation time by the same amount

The receiver location error and pseudorange error of attacks where the signal propagation time is changed by the same amount are shown in Figure 3. The red data points and lines indicate attacks that break the IEEE C37.118 standard with time error larger than 26.5μs, and the blue data points and lines represent attacks that are not large enough to break the standard. In the simulations, the receiver location errors stay constant at 283.6m, irrespective of the receiver time error, while changing the inserted delay. The pseudorange

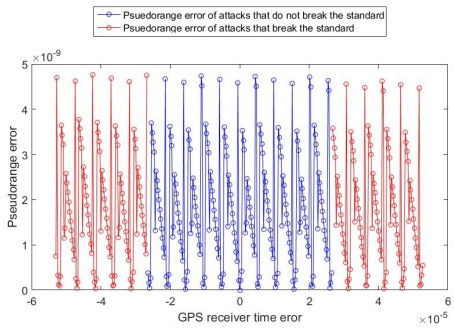

Fig. 3. The pseudorange error along time error when the propagation time is changed by the same amount.

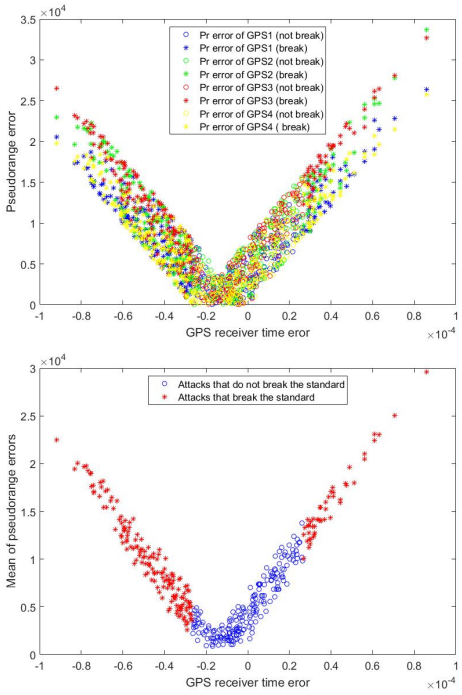

Fig. 4. The pseudorange error and location error as a function of receiver time error when the propagation time is changed differently for each satellite.

error for different receiver time errors is shown in Figure 3. The pseudorange error fluctuates between zero and 5nm. In particular, the pseudorange error for a standard-break attack can be as small as 28.44pm. Moreover, the standard-break attacks experience the same fluctuation trend as the standard-not-break attacks. Due to the negligible pseudorange error and similar fluctuation trend, the GPS time spoofing attack conducted by inserting same delay to all GPS signals is difficult to perceive when only considering the pseudorange error.

C. Impact of changing propagation time for each satellite signal differently

The pseudorange and receiver location error of each signal as a function of the receiver time error are shown in Figure 4.

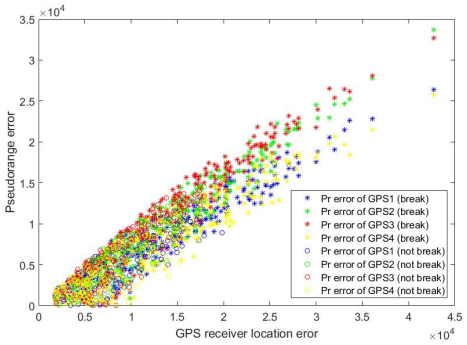

Fig. 5. The pseudorange error for different receiver location error when the propagation time is changed differently for each satellite.

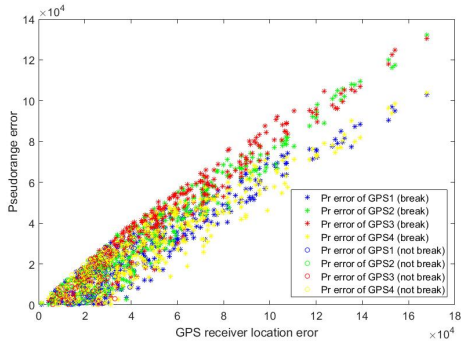

Fig. 6. The pseudorange error for different receiver location error when both the GPS timestamp and the propagation time are changed.

The circles represent the pseudorange error of standard-not-break attacks while stars represent that of standard-break attacks. The result for each satellite is colored in blue, green, red and yellow, respectively. The pseudorange errors have a distinct trend along the receiver time error. They decease in the range -90μs to -15μs and increase in the range -15μs to 90μs. The pseudorange errors can be up to 35km which is quite large for detecting. The receiver location errors have a similar trend with the pseudorange error. The location error of standard-not-break attacks can be up to 20km. Since the GPS receivers in power grids have a fixed location, these location errors are large enough for detection. Figure 5 plots the relationship between the pseudorange error and receiver location error. The distribution of circles overlaps with that of stars. The pseudorange error and location error of a standard-break attack can be smaller than that of a standard-not-break attack. Although both errors have large values, it is difficult to identify whether the attack is standard-break or not only via the pseudorange error and location error.

D. Impact of changing both the GPS timestamp and each signal's propagation time

The simulation results have similar trend with the case where the attacks are conducted via only changing the propagation time of each signal differently. Although the GPS timestamp is changed as well, it does not help in reducing the resulting errors. Both the pseudorange and location errors for an attack that does not break the standard can be up to 40km, which are much larger than the results that are shown in Section V.C. Thus, it is much easier for detecting this kind of attack. The relationship between pseudorange error and location error is displayed in Figure 6. In the area where the location error is smaller than 45km and pseudorange error is smaller than 40km, the data points of standard-break attacks overlap with the standard-not-break attack. Therefore, although the large errors make it easy to detect this time spoofing attack, it is difficult to distinguish whether an attack is serious enough to break the power grid or not from pseudorange error and location error.

VI. Conclusion

While generating a fake GPS signal, the GPS timestamp and the GPS signal propagation time of each satellite may be manipulated by the attacker to conduct GPS time spoofing attacks. We observed the resulting pseudorange, receiver location, and time errors while changing these two parameter individually or simultaneously. Our results show that serious GPS time spoofing can be conducted with low pseudorange error (248.6m) and low location error (53.2m) by only forging the GPS timestamp. Attacks can also be achieved with negligible pseudorange error lower than 5nm and constant location error of 283.6m via only inserting the same amount of delay to all GPS signals. Compared to the GPS positioning accuracy, these low error attacks are difficult to be detected just from the location error or calculated pseudorange. Conversely, when random delay is inserted into each signal to manipulate the propagation time, the pseudorange error and receiver location error can be thousands of meters which are quite large and obvious for detection.

References

[1] Todd E. Humphreys, Brent M Ledvina, Virginia Tech, Mark L Psiaki, Brady W O Hanlon, and Paul M Kintner. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation*, (September 2008):2314–2325, 2008.

[2] Xichen Jiang, Jiangmeng Zhang, Brian J. Harding, Jonathan J. Makela, and Alejandro D. Dominguez-Garcia. Spoofing GPS Receiver Clock Offset of Phasor Measurement Units. *IEEE Transactions on Power Systems*, 28(3):3253–3262, aug 2013.

[3] Elliott D. Kaplan and Christopher J. Hegarty. *Understanding GPS/GNSS : Principles and Applications, Third Edition*.

[4] Wlodzimien Lewandowski, Gcrard Petit, and Claudine Thomas. Precision and Accuracy of GPS Time Transfer. *IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT*, 42(2), 1993.

[5] Huang Lin and Yang Qing. GPS SPOOFING Low-cost GPS simulator. 2015.

[6] Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3-4):146–153, 2012.

[7] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. *ACM conference on Computer and communications security, CCS*, page 75, 2011.

[8] Kang Wang, Shuhua Chen, and Aimin Pan. Time and position spoofing with open source projects. *Black Hat Europe*, 148, 2015.