SPOOFING GPS RECEIVER CLOCK OFFSET OF PHASOR MEASUREMENT UNITS

BY

XICHEN JIANG

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2012

Urbana, Illinois

Adviser:

Assistant Professor Alejandro D. Domínguez-García

ABSTRACT

We demonstrate the feasibility of a spoofing attack on the GPS receiver of a phasor measurement unit (PMU). We formulate the attack as an optimization problem where the objective is to maximize the difference between the time offset of the PMU's receiver clock before and after the attack. Since the PMU uses this clock offset to compute a time-stamp for its measurements, an error in the receiver clock offset introduces a proportional phase error in the voltage or current phase measurements provided by the PMU with a phase-wrap of 2π (in practice, the computed maximum receiver clock offset error is never large enough to induce a phase error that requires a phase-wrap of 2π) . The decision variables in the optimization problem are the satellites' ephemerides, pseudoranges, and the receiver coordinates. The constraints are cast such that the receiver and satellite positions computed from the solution of the optimization problem will be close to their pre-attack values to avoid detection. We show that the spoofing attack is feasible for any number of visible satellites. Simulation results, in which four and seven satellites are spoofed, are presented to illustrate the effect of the attack on the phase measurements provided by a PMU.

To my parents, Xiaoyun and Haiming

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to Professor Alejandro Domínguez-García for his encouragement, guidance, and support throughout this research process, without which this work would not have been possible. Always teeming with brilliant ideas and witty comments, Alejandro has been a phenomenal collaborator and an inspirational mentor. He is someone special to my heart. In addition, I would like to thank Professor Jonathan Makela for his invaluable advice and insights throughout this project.

Lastly, words alone simply cannot express the thanks I owe to my parents, Xiaoyun and Haiming, for their patience and much-needed support throughout the last two years. I thank them for providing me comfort whenever the research is not going smoothly. I am forever grateful for their unconditional love.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The motivation behind this work stems from the current trend of increasing deployment of phasor measurement units (PMUs) across the power grid. While the integration of this new technology has brought about significant advances in the stability monitoring and state estimation capabilities for the power system, it has also been a source of security concern. Specifically, as these PMUs depend on GPS signals to synchronize their measurements, they are also susceptible to spoofing attacks. A method for spoofing PMU receivers that results in maximal phase error while evading detection is formulated and simulated. This introductory chapter provides the background on PMUs and how they utilize the GPS signals for time synchronization. A review of relevant research is presented along with the main contributions of this thesis.

1.1 Background

Under the US-DOE Smart Grid vision and its European counterpart, electric power systems are undergoing radical transformations in structure and functionality. As such, these transformations are enabled by the integration of new technologies. One such technology that has received considerable attention is the PMU, which provides synchronized positive sequence voltage and phase measurements of a power system in real-time [3]. These devices enable the power system engineers to directly measure the power system state, allowing for real-time control and monitoring of power flows in the power grid. While the many applications of PMUs are still under research, some of them include [4]:

- verification of voltage transformers in a substation
- verification of current transformer polarity and phase

- verification of state estimator results
- verification of system models, where PMU measurements are used to obtain system dynamic equivalent models, estimate model parameters, and analyze wide-area transient stability [5]
- synchronization of fault and disturbance records

Therefore, incorporation of PMUs into the power grid results in more efficient distribution of power and better fault detection in transmission lines.

1.2 Problem Statement

PMUs use a GPS receiver front-end to derive a time stamp in Coordinated Universal Time (UTC) for their phase measurements. As such, they are vulnerable to spoofing attacks. The GPS receiver acquires signals transmitted by satellites, decodes each satellite's navigation data, and estimates the receiver position and the current time. A spoofing attack on the GPS receiver can cause a faulty time stamp, which introduces errors in the PMU's phase measurements. This thesis focuses on one particular method of data-level spoofing that introduces the maximal phase error in the PMUs' measurements. However, assessing the impact of phase error on PMU applications is beyond the scope of this thesis.

1.3 Related Work

The first comprehensive assessment of the vulnerabilities in the civilian GPS infrastructure was published a decade ago in a report prepared by the Volpe National Transportation Systems Center [6]. This report concluded that among the different types of attacks, GPS spoofing is the most pernicious and difficult to detect. Generally speaking, spoofing attacks fall under two categories: signal-level and data-level. Signal-level spoofing focuses on causing the receiver to lose lock to the real GPS signal by overpowering it with the spoofed signal. One method is to use a GPS simulator to generate a rogue GPS signal matching the genuine signal's phase, code delay, and encoded data. The spoofer gradually increases its transmission power until the GPS receiver locks onto the malicious signal, at which point the victim receiver is fully under the spoofer's control [7]. It was shown that such an attack causes significant errors in the phase measurements provided by the PMUs. In data-level GPS spoofing, the data of the GPS signals, namely the ephemerides, are altered in such a way that the receiver using the spoofed data computes the incorrect location, velocity, or clock offset. The problem is to determine how to manipulate these data in order to cause interference while evading detection. This type of spoofing is the focus of this thesis.

The absence of effective countermeasures against civilian GPS receiver spoofing has been made known to major manufacturers, but little has been done to address such deficiencies in security [7]. Only recently, research into GPS spoofing have resulted in several recommendations to counteract such attacks [8], [9]:

1. Amplitude discrimination
2. Time-of-arrival discrimination
3. Polarization discrimination
4. Angle-of-arrival discrimination
5. Cryptographic authentication
6. Signal strength discrimination

The first two methods can be implemented in software but provide only a rudimentary defense against spoofing attacks. Polarization and angle-of-arrival discrimination require multiple antennas to implement and are ineffective against sophisticated coordinated attacks involving multiple rogue GPS transmitters. An extensive review of cryptographic techniques is made in [10]. However, cryptographic methods require significant changes to the current GPS signal coding scheme, which is unlikely to happen in the short term [7]. Recent developments in cryptographic methods that allow for minimal modifications to the current system include navigation message authentication (NMA) and signal authentication sequences (SAS) [11], [12], [13]. These schemes are robust against signal spoofing but provide no security for unauthorized signal access. Furthermore, to the author's best knowledge, civilian

GPS receivers have not implemented these techniques at the time this thesis was written.

In [14], the authors demonstrated a spoofing attack on a PMU and reported constraints on the velocity and acceleration with which the GPS clock can be manipulated. The attack hijacks the receiver's tracking loops and steers them to modify the receiver's clock offset as desired. They found that if the tracking loops are steered too aggressively, the receiver loses lock and the spoof is readily detected. While the work in [14] employed an attack based on advancing or delaying each satellite signal, we propose an attack based on modifying the encoded data without modifying the underlying signal characteristics. As such, we do not expect to be bound by the bandwidth of the receiver tracking loops, only by the rate at which the GPS receiver incorporates new ephemerides and the rate at which the PMU updates its time stamp based on the GPS receiver. The impact of GPS receiver spoofing on the frequency monitoring network of the power grid is demonstrated in [15]. The authors showed that alterations to the PMUs' receiver clock offset can hamper determination of fault locations and introduce erroneous oscillation modes in the power system. However, methods to introduce errors in the receiver clock offsets of the PMUs were not discussed.

1.4 Contribution of Thesis

We investigate the feasibility of a simple data-level attack on the GPS receiver of a PMU using a GPS simulator. Most of the civilian GPS receivers on the market today do not have the capability of detecting such an attack. In addition, the price of a GPS simulator has dropped significantly from as high as $400,000 ten years ago to around $20,000 today, greatly reducing the barrier to GPS spoofing [7]. These GPS simulators have also seen significant miniaturization during this period, which makes a spoofer difficult to locate.

To demonstrate the feasibility of a GPS spoofing attack, we formulate the attack as an optimization problem where the objective is to maximize the difference between time offsets of the PMU's receiver clock before and after the attack while maintaining the computed receiver location close to its pre-attack value. We perform the optimization for a given instant in time, which is when the spoof will be applied. The decision variables in the problem are the satellite ephemerides, pseudoranges, and receiver position. The ephemerides are a set of values broadcast by the GPS satellite that allow the receiver to compute the satellite position at a particular time. The pseudorange is the measured distance from the satellite to the receiver and is computed by multiplying the signal propagation velocity, $c = 299792458$ m/s, by the signal transit time, which is derived from the nonsynchronized satellite clock and receiver clock. Because of the receiver clock offset (which is responsible for the nonsynchronization), the pseudoranges measured by the receiver all deviate from the true range by a common amount. In the optimization problem, the constraints are placed on the decision variables as required in order to avoid spoofing detection. Methods of attack are presented for four-satellite and seven-satellite cases. For the specific spoofing attack simulation presented in this thesis, it is shown that the error introduced in the receiver clock offset can be as high as 2.3 ms, which corresponds to 14% of a cycle in a 60-Hz signal.

The remainder of this thesis is organized as follows. In Chapter 2, we describe the algorithm that a GPS receiver uses to compute its position and time offset. In Chapter 3, we formulate the attack as an optimization problem for finding the maximum receiver clock offset for an arbitrary number of visible satellites. Chapter 4 presents the results of two simulated spoofing attacks for the four-satellite and seven-satellite cases. Chapter 5 describes ideas for designing systems to detect and hinder such attacks. Finally, concluding remarks are made in Chapter 6.

CHAPTER 2

CALCULATION OF RECEIVER POSITION

In this chapter, we explain how a GPS receiver computes its position and clock offset given the satellite ephemerides and pseudoranges. The relation between the satellite ephemerides and satellite position is also explained. In subsequent developments, an overline above a symbol denotes vectors and a superscript star denotes the pre-attack value of some real-valued variable; i.e., $\overline{\delta}$ is a vector and x^* is the pre-attack value of x.

2.1 GPS Receiver Position and Time Synchronization Error Calculation

A GPS receiver determines its distance from a satellite by measuring the time of signal transmission from the satellite to the receiver and multiplying that by the speed of the signal propagation, which is assumed to be the speed of light. Given the satellites' positions and their ranges from the receiver, the receiver location could be computed through a process known as trilateration [1]. In three dimensions, three satellites are needed to determine the receiver's exact location, provided that there is no noise in the measurements and the time between the satellites' clocks and the receiver clock are perfectly synchronized. However, in reality the receiver clock has an offset t_u from the GPS time t_E of the satellites that arise from internal hardware bias in the local clock oscillator (note that we use t_E to denote the GPS system time at *any particular time*). For solvability, it is safe to assume that the receiver clock offset is constant across all receiver channels [2]. Therefore, we can express the GPS time as:

$$t_E = t_r - t_u, \tag{2.1}$$

where t_r denotes the receiver clock time. The coordinated universal time (UTC), t_{UTC}, is offset from GPS time t_E by an integer number of leap seconds

Δt_{UTC}, which is 15 s as of 1 January 2010 [1]. Therefore, t_{UTC}, which is used for PMU time synchronization [16], is computed as follows:

$$t_{UTC} = t_E - \Delta t_{UTC}. \tag{2.2}$$

Figure 2.1 shows a general three bus system with PMUs dispatched at each bus. A voltage phasor is measured at each bus and time-stamped using the reference time signal t^*_{UTC}. This time-stamp is common to all three buses and provides the synchronization of the PMUs' phasor measurements.

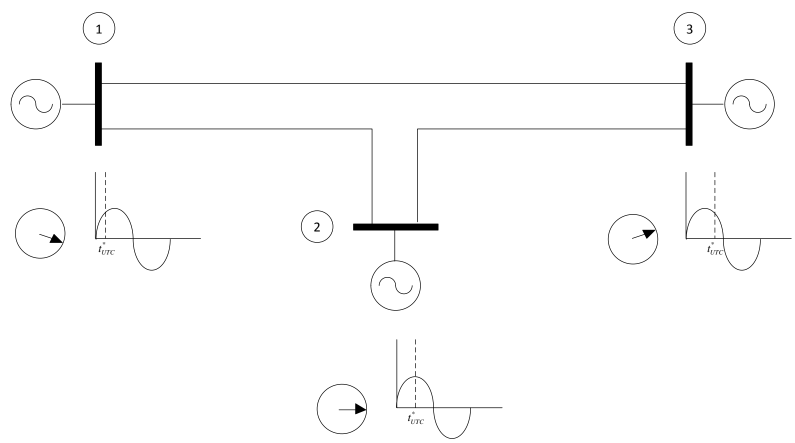


Figure 2.1: PMU and Associated Phasor Measurements.

With the addition of the receiver clock offset as a variable, at least four satellites are needed in order to determine the receiver's Earth-Centered Earth-Fixed (ECEF) coordinates and the clock offset. The satellite-to-receiver distance, which is computed by taking the time difference between the satellite clock t_e and the receiver clock t_r and multiplying by the propagation speed, does not yield the true range between the satellite and the receiver because of the receiver clock offset. Instead, this measurement is called the *pseudorange*, which can be expressed as a linear function of the true range and the receiver clock offset.

2.2 Four Visible Satellites

For a given time, let ρ_i and r_i be the i^{th} satellite's pseudorange and true range; x_i, y_i, and z_i be the i^{th} satellite's ECEF coordinates; x_u, y_u, z_u, be the receiver's ECEF coordinates; $c = 299792458$ m/s, and t_u be the receiver clock offset. Then,

$$\rho_i = r_i - ct_u, \quad i = 1, 2, 3, 4 \tag{2.3}$$

$$r_i = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2}. \tag{2.4}$$

The satellite coordinates x_i, y_i, and z_i are computed by the receiver through a set of parameters contained in the GPS signal known as the ephemerides (described in detail below). In the four-satellite case and assuming no noise in the measurements, the receiver location and the clock offset can obtained by solving (2.3)-(2.4) directly, as the number of unknowns is equal to the number of equations. This system of nonlinear equations is solved by the GPS receiver through a nonlinear solution method, e.g., Newton-Raphson.

2.3 More Than Four Visible Satellites

It is almost always the case that more than four satellites are visible at a particular instant of time. Then in (2.3)-(2.4), $i > 4$, which results in an overdetermined system. In this scenario, the solution x_u, y_u, z_u, and t_u is obtained by solving a least squares errors estimation (LSE) problem of the form:

$$\min \quad f_0 = \sum_{i=1}^{n} (\rho_i - r_i + ct_u)^2, \quad n > 4, \tag{2.5}$$

where n denotes the number of visible satellites. The GPS receiver solves the LSE problem in (2.5), which can be solved numerically using the Gauss-Newton method [17].

2.4 GPS Ephemerides

The ephemerides are a set of parameters that allow the receiver to compute a satellite's position at any time. Up-to-date ephemerides are uploaded from the GPS control segment to the satellites once per day and then broadcast to the receiver as part of the navigation data signal. A detailed description of

Table 2.1: Keplerian Elements

a	semimajor axis of ellipse
e	eccentricity of ellipse
τ	time of perigee passage
i	inclination of orbit
Ω	longitude of ascending node
ω	argument of perigee

the ephemerides and their role in calculating a satellite's position is presented next.

The accurate characterization of the GPS satellites' orbits is essential for determining the receiver's position. In the absence of external perturbations, the trajectory of a satellite is solely governed by the gravitational force of Earth and can be described by

$$\frac{d^2\overline{s}_i}{d\overline{s}_i^2} + \frac{G}{s_i^3}\overline{s}_i = 0, \tag{2.6}$$

where $\overline{s}_i = [x_i,\ y_i,\ z_i]^T$ is the position vector of the i^{th} satellite, $G = 3986005 \times 10^8\ \text{m}^3/\text{s}^2$ is the product of the universal gravitation constant and the mass of the Earth [1], and s_i is defined as:

$$s_i = \sqrt{x_i^2 + y_i^2 + z_i^2}.$$

The solution of (2.6) is characterized by six constants of integration known as *Keplerian elements* (listed in Table 2.1), which result from solving (2.6) with the initial conditions $\overline{s}(0)$ and $\frac{d\overline{s}(0)}{dt}$. These six parameters allow the receiver to compute the position and velocity vectors of the satellite at any point in time given the initial conditions. In order to describe a satellite's orbit even more accurately, the additional forces acting on the satellite must be considered. These forces include the so-called third-body gravitation from the Sun and the Moon, solar radiation pressure, and the Earth's tidal variations, among others. Table 2.2 lists some of the major perturbing forces and their effects on the satellites. Although the accelerations from the other perturbing forces are small compared to the gravitational acceleration of the Earth, their effects do add up to significant changes over an extended period of time.

It is still possible to completely characterize the satellite's motion under

Table 2.2: Forces on GPS Satellites and Resultant Accelerations [1].

Force	Acceleration (m/s^2)
Earth Gravity	0.56
Equatorial bulge	5×10^{-5}
Lunar/Solar Gravity	5×10^{-6}
Solar radiation	1×10^{-7}

full perturbation with the Keplerian elements; however, these parameters will no longer be constants. A reference time known as the *epoch* (denoted by t_{0e} in Table 2.3) is established to characterize the time-dependent integrals of motion. At the exact reference time, the six Keplerian elements in Table 2.1 describe the position and velocity vectors of the satellite exactly, but as time progresses the true position and velocity vectors of the satellite will deviate from the position and velocity vectors computed by the six integrals. In order to account for these deviations, parameters that characterize how the Keplerian elements change over time are added to the satellite's navigation signal. This expanded parameter set which contains the Keplerian elements is known as the satellite's ephemerides and is updated by the satellite every two hours. The information contained in the ephemerides is summarized in Table 2.3. A full specification of the ephemerides can be found in [18], which describes the interface between the GPS space segment and the GPS user segment.

For completeness, Table 2.4 provides the algorithm by which a GPS receiver computes the position of a satellite in ECEF coordinates from the GPS ephemerides. The parameter t used in step (3) of Table 2.4 is the time at which the GPS signal was transmitted from the satellite. The subscript k appearing in the computations signifies that the variable is measured at time t_k, the time (in seconds) from epoch t_{0e} to time of transmission t.

To ease notation in subsequent developments, we denote by $\delta_i(j)$ the j^{th} ephemeride of satellite i and define $\overline{\delta}_i = [\delta_i(1),\ \delta_i(2),\ \ldots,\ \delta_i(m)]^T$ as the vector that contains the ephemerides broadcasted by the i^{th} satellite. Using this notation, we can express the ECEF position of the satellite as a function

Table 2.3: GPS Ephemeris Data Definitions [2].

t_{0e}	Reference time of ephemeris
$\sqrt{a}$	Square root of semimajor axis
e	Eccentricity
i_0	Inclination angle
Ω_0	Longitude of ascending node
ω	Argument of perigee
M_0	Mean anomaly
$\frac{di}{dt}$	Rate of change of inclination angle
Ω	Rate of change of longitude of ascending node
Δn	Mean motion correction
C_{uc}	Amplitude of cosine correction to argument of latitude
C_{us}	Amplitude of sine correction to argument of latitude
C_{rc}	Amplitude of cosine correction to orbital radius
C_{rs}	Amplitude of sine correction to orbital radius
C_{ic}	Amplitude of cosine correction to inclination angle
C_{is}	Amplitude of sine correction to inclination angle

Table 2.4: Computation of Satellite's ECEF Coordinates [2].

(1)	$a = (\sqrt{a})^2$	Semimajor axis
(2)	$n = \sqrt{\frac{\mu}{a^3}} + \Delta n$	Corrected mean motion
(3)	$t_k = t - t_{0e}$	Time from ephemeris epoch
(4)	$M_k = M_0 + n t_k$	Mean anomaly
(5)	$M_k = E_k - e \sin E_k$	Eccentric anomaly
(6)	$\sin \nu_k = \frac{\sqrt{1-e^2} \sin E_k}{1 - e \cos E_k}$ $\cos \nu_k = \frac{\cos E_k - e}{1 - e \cos E_k}$	True anomaly
(7)	$\phi_k = \nu_k + \omega$	Argument of latitude
(8)	$\Delta \phi_k = C_{us} \sin(2\phi_k) + C_{uc} \cos(2\phi_k)$	Argument of latitude correction
(9)	$\Delta r_k = C_{rs} \sin(2\phi_k) + C_{rc} \cos(2\phi_k)$	Radius correction
(10)	$\Delta i_k = C_{is} \sin(2\phi_k) + C_{ic} \cos(2\phi_k)$	Inclination correction
(11)	$u_k = \phi_k + \Delta \phi_k$	Corrected argument of latitude
(12)	$r_k = a(1 - e \cos E_k) + \Delta r_k$	Corrected radius
(13)	$i_k = i_0 + (di/dt) t_k + \Delta i_k$	Corrected inclination
(14)	$\Omega_k = \Omega_0 + (\Omega - \dot{\Omega}_e) t_k - \dot{\Omega}_e t_{0e}$	Corrected longitude of node
(15)	$x_p = r_k \cos \mu_k$	In-plane x position
(16)	$y_p = r_k \sin \mu_k$	In-plane y position
(17)	$x_s = x_p \cos \Omega_k - y_p \cos i_k \sin \Omega_k$	ECEF x-coordinate
(18)	$y_s = x_p \sin \Omega_k + y_p \cos i_k \cos \Omega_k$	ECEF y-coordinate
(19)	$z_s = y_p \sin i_k$	ECEF z-coordinate

$\overline{\delta}_i$ such that

$$\begin{aligned} x_i &= f(\overline{\delta}_i, t), \\ y_i &= g(\overline{\delta}_i, t), \\ z_i &= h(\overline{\delta}_i, t), \end{aligned} \tag{2.7}$$

where the functions $f(\cdot)$, $g(\cdot)$, and $h(\cdot)$ can be defined using Table 2.4.

CHAPTER 3

MATHEMATICAL FORMULATION OF ATTACK

In this chapter, we provide the mathematical formulation of the spoofing attack such that the receiver clock bias offset is maximized. The problem is cast as an optimization problem where the objective function is the phase error of the PMU measurements.

3.1 GPS Receiver Spoofing and Impact on the Phase Information Provided by PMUs

Time synchronization across PMUs is crucial for maintaining an accurate measurement of phase angles. In the following developments, we assume that the maximum receiver clock offset from its pre-attack value is not large enough to cause a phase-wrap in the phase measurement from the PMU. Therefore, for demonstrating the feasibility of an attack on PMU time synchronization (and phase measurements), we simply seek to maximize the difference of the receiver clock offset t_u (post-attack) with respect to its pre-attack value t_u^*. A GPS simulator can simulate a rogue GPS navigation data signal and cause simple receivers to latch onto the new signal by gradually overpowering the true GPS signal, thus forcing the receiver to compute an incorrect receiver clock offset. For a 60-Hz signal, the PMU's phase measurement error ε_θ is related to the receiver clock offset error through the linear relationship

$$\varepsilon_\theta = [60 \times (t_u - t_u^*) \times 360°] \bmod 360. \tag{3.1}$$

Figure 3.1 shows the result of a GPS spoofing attack on bus 2 (red) of the general three bus system. The receiver clock offset t_u is shifted from its pre-attack value of t_u^*, causing a proportional error in the estimate of t_{UTC}. Consequently, the erroneous time-stamp $\tilde{t}_{UTC}$ used by the PMU of bus 2 results in an incorrect phase estimate, which causes the PMU to lose synchronization from the rest of the system.

We are interested in determining the maximum phase shift error that can be introduced in a PMU's phase measurement by spoofing the GPS signal. Though many commercial GPS receivers are not secured against spoofing, we nevertheless employ the following constraints to demonstrate the feasibility of an attack under simple spoofing detection schemes: i) The difference between the true receiver location and the location calculated by the spoofed receiver should be small, and ii) The difference between the true ephemerides and the spoofed ephemerides should be small. The difference between the pre-attack clock offset and the spoofed clock offset is maximized. In the optimization problem, the decision variables are the satellites' ephemerides.

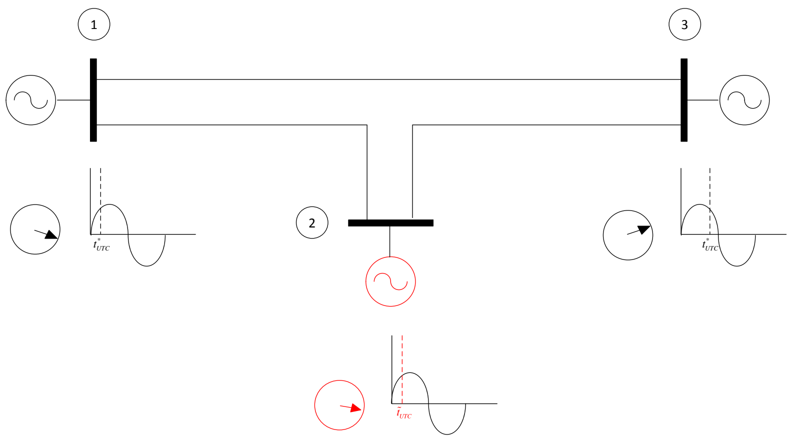


Figure 3.1: PMU and Associated Phasor Measurements Post-Attack.

3.2 Four Visible Satellites

In this case, the problem can be formulated as an optimization of the maximum clock offset error as follows:

$$
\begin{aligned}
\max \quad & (t_u - t_u^*)^2 \\
\text{subject to} \quad & \rho_i = r_i - ct_u, \quad \forall i = 1,2,3,4 \\
& |x_u - x_u^*| \le \varepsilon_{x_u} \\
& |y_u - y_u^*| \le \varepsilon_{y_u} \\
& |z_u - z_u^*| \le \varepsilon_{z_u} \\
& |\delta_i(j) - \delta_i^*(j)| \le \varepsilon_{\delta_i}(j), \quad j = 1,2,\ldots,m \\
& x_i = f(\overline{\delta}_i, t) \\
& y_i = g(\overline{\delta}_i, t) \\
& z_i = h(\overline{\delta}_i, t)
\end{aligned}
\tag{3.2}
$$

where x_u, y_u, z_u are the receiver's ECEF coordinates, $\overline{\delta}_i$ are the i^{th} satellite's ephemerides. The difference between the decision variables and their pre-attack values (denoted by *) is bounded by ε_{x_u}, ε_{y_u}, ε_{z_u} and $\varepsilon_{\delta_i}(j)$. As discussed above, these bounds are specified to demonstrate that the spoofing can still succeed even if the receiver checks for abrupt changes to these parameters from their pre-attack values as a possible countermeasure to detect spoofing (to the author's best knowledge, there are currently no commercial products that implement these countermeasures). If the receiver does not check for abrupt changes in the receiver and satellite positions and the ephemerides as a way to detect data spoofing, then these bounds can be relaxed to positive infinity. In addition, equation (2.3) must also be satisfied as constraints to the optimization problem so that the solutions found are valid. The expression for t_u in the objective function is obtained by summing the expressions in (2.3) and solving for t_u, which results in

$$
t_u = \frac{-1}{4c} \sum_{i=1}^{4} (\rho_i - r_i). \tag{3.3}
$$

3.3 More Than Four Visible Satellites

In this case, the system is overdetermined and, assuming noise in measurements, an exact solution to (2.3) no longer exists. Therefore, the constraints arising from (2.3) are replaced by the LSE condition in (2.5). Since (2.5) itself is an optimization problem, it cannot be readily stated as a regular constraint. However, we can exploit the convexity of the LSE problem [19], and use the fact that the first-order optimality conditions that the solution of (2.5) must satisfy are also sufficient conditions, i.e.,

$$\begin{aligned} \frac{\partial f_0}{\partial x_u} &= 0, \\ \frac{\partial f_0}{\partial y_u} &= 0, \\ \frac{\partial f_0}{\partial z_u} &= 0, \\ \frac{\partial f_0}{\partial t_u} &= 0, \end{aligned} \tag{3.4}$$

where

$$\begin{aligned} \frac{\partial f_0}{\partial x_u} &= 2\sum_{i=1}^{n}\left[\frac{(\rho_i - r_i + ct_u)(x_i - x_u)}{r_i}\right], \\ \frac{\partial f_0}{\partial y_u} &= 2\sum_{i=1}^{n}\left[\frac{(\rho_i - r_i + ct_u)(y_i - y_u)}{r_i}\right], \\ \frac{\partial f_0}{\partial z_u} &= 2\sum_{i=1}^{n}\left[\frac{(\rho_i - r_i + ct_u)(z_i - z_u)}{r_i}\right], \\ \frac{\partial f_0}{\partial t_u} &= 2c\sum_{i=1}^{n}(\rho_i - r_i + ct_u). \end{aligned} \tag{3.5}$$

The optimization for the maximization of the receiver clock offset when more than four satellites are visible becomes

$$\begin{aligned} \max \quad & (t_u - t_u^*)^2 \\ \text{subject to} \quad & \frac{\partial f_0}{\partial x_u} = \frac{\partial f_0}{\partial y_u} = \frac{\partial f_0}{\partial z_u} = \frac{\partial f_0}{\partial t_u} = 0 \\ & |x_u - x_u^*| \le \varepsilon_{x_u} \\ & |y_u - y_u^*| \le \varepsilon_{y_u} \\ & |z_u - z_u^*| \le \varepsilon_{z_u} \\ & |\delta_i(j) - \delta_i^*(j)| \le \varepsilon_{\delta_i}(j), \quad j = 1, 2, \ldots, m \\ & x_i = f(\overline{\delta}_i) \\ & y_i = g(\overline{\delta}_i) \\ & z_i = h(\overline{\delta}_i). \end{aligned} \tag{3.6}$$

The variable t_u in the objective function can be solved from any of the expressions in equation (3.5). Solving for t_u using the equation $\frac{\partial f_0}{\partial t_u} = 0$ yields

$$t_u = \frac{-1}{nc} \sum_{i=1}^{n} (\rho_i - r_i). \tag{3.7}$$

Note that in the formulation of the optimization problem for more than four satellites, the constraint (2.3) is replaced by the first order optimality conditions of (3.4) so as to satisfy the LSE conditions.

CHAPTER 4

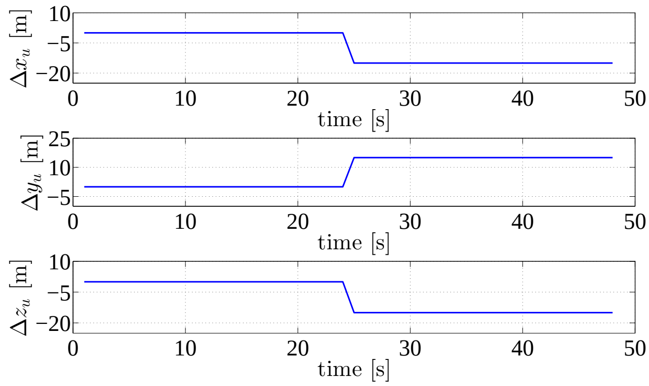
CASE STUDIES

In this chapter, we illustrate the concepts developed in this paper by presenting the results of spoofing a simulated GPS receiver that is receiving signals from four and seven satellites. The optimization problem described in Chapter 3 has been implemented in the MATLAB environment with the perturbation of each of the satellites' ephemerides limited to $\pm 2\%$ of their pre-attack values. The pre-attack values (nominal values) of the satellite ephemerides are presented in Tables A.1 and A.2 of Appendix A. The GPS receiver location is also restricted to vary at most 15 m from its pre-attack position (see Table A.3 of Appendix A).

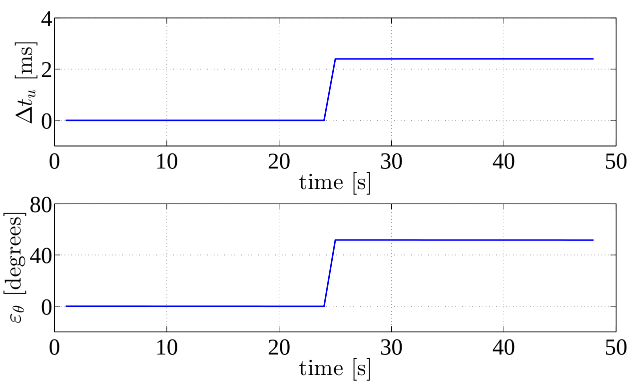
4.1 Simulations

For the four-satellite case, the optimization problem in (3.2) is computed for 24 time instances. The solutions for position and clock offset of the spoofed receiver are plotted along with the corresponding pre-attack solutions in Fig. 4.1. The attack occurs 24 seconds into the simulation. In Fig. 4.1(a), it is observed that the jumps in the ECEF coordinates of the receiver due to the spoofed ephemerides are indeed within the 15 m bounds specified by the constraints. Therefore, if the threshold for detecting an attack is greater than 15 m, then such spoofing would not be noticed. Figure 4.1(b) shows the change in the receiver clock offset from the spoofing attack and the resulting PMU phase angle error corresponding to the attack.

The optimization problem in (3.6) is computed for the seven-satellite case using the same bounds on the ephemerides, pseudoranges, and receiver locations as the four-satellite case. The results from the simulation are shown in Fig. 4.2. The phase angle error resulting from these attacks can be as high as $52°$, which corresponds to 14 percent of a full cycle for a 60-Hz system.



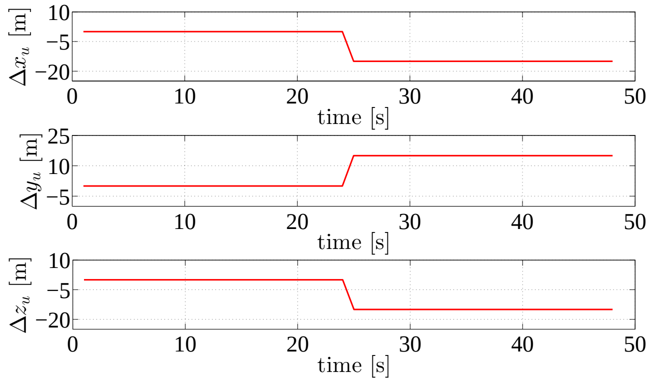
(a) Receiver ECEF Coordinates.



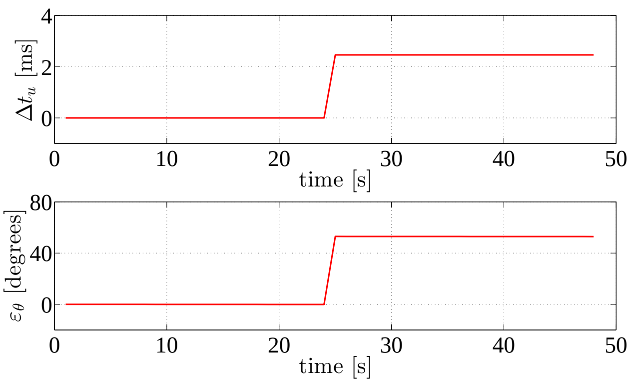
(b) Receiver clock offset and phase angle.

Figure 4.1: Receiver Position, Clock Offset, and PMU Phase Error for Spoofing Four Satellites.

Figure 4.3 shows the receiver clock offset and the resulting PMU phase error for both the four-satellite and seven-satellite spoofing on the same plot. Comparing the two plots, it can be seen that the maximum phase errors that can be introduced under the same constraints for each satellite are nearly the same.



(a) Receiver ECEF Coordinates.



(b) Receiver clock offset and phase angle.

Figure 4.2: Receiver Position, Clock Offset, and PMU Phase Error for Spoofing Seven Satellites.

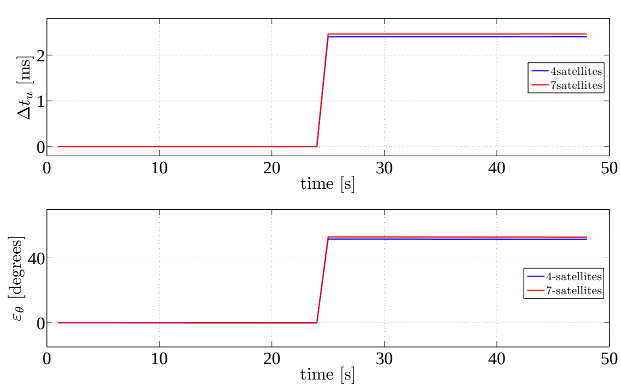


Figure 4.3: Clock Offset and PMU Phase Error for Spoofing Four and Seven Satellites.

CHAPTER 5

COUNTERMEASURES

In this chapter, some possible countermeasures for GPS receiver spoofing are described. The methods presented here are by no means comprehensive and as the receiver technology evolves, more sophisticated attacks and countermeasures are expected to be developed.

5.1 Possible Countermeasures

The simplicity and effectiveness of the attack demonstrated in this thesis suggest that spoofing detection needs to be employed by PMUs in the power grid, and in general any high-reliability system using a GPS time stamp. As described in the Introduction, such detection schemes include [8], [9]:

1. Amplitude discrimination
2. Time-of-arrival discrimination
3. Polarization discrimination
4. Angle-of-arrival discrimination
5. Cryptographic authentication
6. Signal strength discrimination

The attack proposed in this thesis would be easily detected by 4 or 5, but 4 requires multiple networked antennas, and 5 requires changes to the GPS signal architecture.

Several other simple spoofing detection schemes would readily detect the attack proposed in this paper. If a receiver is connected to the Internet, it could download the most recent ephemerides from the GPS control segment to validate the received navigation data. Since the proposed attack relies on spoofing the ephemerides, a cross-check would reveal tampering. Of course, the spoof would not be revealed until the online ephemeris data were updated, creating a window of opportunity for the spoofer to cause damage.

Instead of checking against published ephemeris data, the receiver could compare the received navigation data with the almanac, a reduced-resolution but multi-satellite version of the ephemerides that is continually broadcast by every satellite along with its own navigation data. Receivers typically use stored almanac data upon startup to obtain a quicker fix on all visible satellites. By comparing a computed satellite position with the position expected from the almanac, an aggressive spoof could be detected. However, conservative spoofers could stay below any particular threshold by tightening the constraints on the optimization problem.

Most GPS clocks do not use the receiver clock offset measurement directly, but rather use it to guide an independent crystal-controlled oscillator. Monitoring the discrepancy between the oscillator and the computed GPS time could reveal tampering.

Another spoofing detection scheme takes advantage of the fact that the genuine satellite signals, while less powerful than the spoofed signals, are still present. Exact cancellation of the genuine signals would require a complicated spoofer. This technique is known as vestigial signal defense (VSD) and is described in detail in [20]. VSD is software-based, requiring no extra hardware. A spoof is detected if additional GPS signals are present in addition to the most powerful ones. The drawback of VSD is that the buried signals are hard to distinguish from multipath interference, but if the GPS receiver is in a static environment (as is the case for PMUs), then multipath effects could be measured and accounted for.

Finally, the proposed spoof would be easily detected in real time if the victim receiver were networked to a trusted GPS receiver at another location, assuming that the trusted receiver is not being spoofed. The victim receiver need only validate the navigation data, the current GPS time estimate, or other signal characteristics such as the P(Y) code. The work in [21] shows that spoofing could be revealed by comparing the P(Y) code on the trusted and victim receivers. The P(Y) code is an encrypted military code that is transmitted in quadrature with the civilian GPS code. A spoofed signal could not contain the genuine P(Y) code.

CHAPTER 6

CONCLUSIONS

PMUs provide synchronized real-time measurements of voltage and current phasors across the power system. They rely on GPS signals to time stamp their measurements. As such, these devices are vulnerable to spoofing attacks. One method of spoofing is to introduce an error in the receiver clock offset, which introduces a proportional phase estimation error from the PMU.

This thesis demonstrates the feasibility of an attack on PMU phase measurements through spoofing the ephemerides' data on the GPS signal. An optimization algorithm that maximizes the error in the receiver clock offset while maintaining the receiver position close to its pre-attack value is proposed. The bounds placed on the maximum receiver position change due to the attack are to ensure that the spoofing avoids detection. When four satellites are visible and no noise is in the measurements, an exact solution to the optimization problem can be found. In the case of more than four satellites, a LSE solution to the optimization problem is formulated with the least squares condition recast into a first order optimality constraint. The feasibility and effectiveness of the proposed spoofing method is demonstrated through simulations of four- and seven- satellite cases.

Future plans involve extending the domain of optimization from an instant in time to a duration over which the PMU can be potentially spoofed. Subsequent experimental work includes a demonstration of this attack on a PMU by building a GPS spoofer (hardware demonstration). The optimization algorithm will be used to compute the optimal spoofing method for a particular time well in advance of the spoofing attack. The solution of the optimization problem will then be downloaded onto the GPS simulator for execution at a later time. Given the feasibility of such an attack, the effects of erroneous phase measurements on state estimation and stability analysis must be assessed and countermeasures developed.

APPENDIX A

PRE-ATTACK EPHEMERIDE AND RECEIVER POSITION VALUES

In Tables A.1 and A.2, we present the pre-attack (nominal values) of the ephemerides for the four-satellite and seven-satellite spoofing case studies and the nominal receiver position. For the seven-satellite spoofing case study, satellites 1-4's nominal ephemerides are the same as those of the four-satellite spoofing case study. Table A.3 presents the nominal receiver position before the spoofing attack.

Table A.1: Nominal Ephemeride Values for Four-Satellite Spoofing.

	Satellite			
	1	2	3	4
t_{0e}	259200	259200	259184	259200
$\sqrt{a}$	5.15363×10^3	5.15371×10^3	5.15354×10^3	5.15308×10^3
e	0.011830	0.005979	0.005346	0.005578
i_0	0.925918	0.933421	0.968260	0.957126
Ω_0	-1.43155	-1.36401	-2.34350	-1.24484
ω	0.90023	-1.37025	-0.36405	-0.36441
M_0	-0.360673	2.106577	2.118746	0.394096
$\frac{di}{dt}$	-0.4753×10^{-9}	-0.5003×10^{-9}	-0.0617×10^{-9}	-0.4846×10^{-9}
Ω	-0.8712×10^{-8}	-0.8269×10^{-8}	-0.8274×10^{-8}	-0.8089×10^{-8}
Δn	0.54709×10^{-8}	0.51577×10^{-8}	0.48512×10^{-8}	0.45341×10^{-8}
C_{uc}	-0.1814×10^{-5}	-0.2183×10^{-5}	-0.0430×10^{-5}	-0.1622×10^{-5}
C_{us}	0.83204×10^{-5}	0.86668×10^{-5}	0.52582×10^{-5}	0.95609×10^{-5}
C_{rc}	1.978437×10^2	1.905625×10^2	2.819687×10^2	1.927187×10^2
C_{rs}	-35.2812	-41.9687	-14.5937	-26.3125
C_{ic}	-0.0502×10^{-6}	0.0707×10^{-6}	0.1396×10^{-6}	0.0856×10^{-6}
C_{is}	0.17136×10^{-6}	-0.03166×10^{-6}	0.13224×10^{-6}	-0.00372×10^{-6}

Table A.2: Additional Nominal Ephemeride Values for Seven-Satellite Spoofing.

	Satellite		
	5	6	7
t_{0e}	259200	259200	259184
$\sqrt{a}$	5.153657×10^3	5.153611×10^3	5.153715×10^3
e	0.0497098	0.00608376	0.0070581
i_0	0.940222	0.9702241	0.972953
Ω_0	0.811398	1.829237	2.8690143
ω	-1.879963	2.882563	-1.140461
M_0	1.2627788	-0.1488341	-1.899143
$\frac{di}{dt}$	0.055002×10^{-9}	-0.077503×10^{-9}	0.37287×10^{-9}
Ω	-0.872000×10^{-8}	-0.808105×10^{-8}	-0.78260×10^{-8}
Δn	0.524486×10^{-8}	0.42926×10^{-8}	0.43191×10^{-8}
C_{uc}	0.11064×10^{-5}	-0.30063×10^{-5}	0.066682×10^{-5}
C_{us}	0.30100×10^{-5}	0.81341×10^{-5}	0.96298×10^{-5}
C_{rc}	3.085625×10^2	2.2546875×10^2	2.0253125×10^2
C_{rs}	21.4375	-57.625	9.37500
C_{ic}	$-0.0689179 \times 10^{-6}$	0.0745058×10^{-6}	$-0.10430812 \times 10^{-6}$
C_{is}	$-0.0204891 \times 10^{-6}$	$-0.0111758 \times 10^{-6}$	0.1341104×10^{-6}

Table A.3: Nominal Receiver Clock Offset and Position

X_r	Y_r	Z_r	t_0
4.9522459×10^6	-3.9473904×10^6	-0.7579975×10^6	-0.0029999

REFERENCES

[1] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*. Lincoln, Massachusetts: Ganga-Jamuna, 2011.

[2] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications*. Boston, Massachusetts: Artech House, 2006.

[3] A. G. Phadke and J. Thorp, *Synchronized Phasor Measurements and Their Applications*. New York: Springer, 2008.

[4] H. J. A. Ferrer and I. E. O. Schweitzer, *Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems*. Pullman, WA: Schweitzer Engineering Laboratories, Inc., 2010.

[5] A. Chakrabortty, J. Chow, and A. Salazar, "A measurement-based framework for dynamic equivalencing of large power systems using wide-area phasor measurements," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 68 –81, Mar. 2011.

[6] "IEEE standard for synchrophasors for power systems," IEEE Standard C37.118, Tech. Rep., 2005.

[7] T. Humphreys, P. Kintner Jr., M. Psiaki, B. Ledvina, and B. O'Hanlon, "Assessing the spoofing threat," *GPS World*, Jan. 2009.

[8] E. Key, "Techniques to counter GPS spoofing," Feb. 1995, internal memorandum, MITRE Corporation.

[9] J. Warner and R. Johnston, "GPS spoofing countermeasures," Dec. 2003, Los Alamos Research Paper LAUR-03-6163.

[10] L. Scott, "Anti-spoofing and authenticated signal architecture for civil navigation systems," in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation*, 2003, pp. 1543–1552.

[11] O. Pozzobon, "Keeping the spoofs out signal authentication services for future GNSS," *Inside GNSS*, pp. 48 –55, May 2011.

[12] O. Pozzobon, C. Wullems, and M. Detratti, "Security considerations in the design of tamper resistant gnss receivers," in *Proc. Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, Dec. 2010, pp. 1–5.

[13] O. Pozzobon, L. Canzian, M. Danieletto, and A. Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," in *Proc. Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, Dec. 2010, pp. 1–6.

[14] D. Shepard and T. Humphreys, "Characterization of receiver response to spoofing attacks," in *Proc. of ION GNSS*, Sep. 2011.

[15] Z. Zhang, S. Gong, H. Li, C. Pei, Q. Zeng, and M. Jin, "Time stamp attack on wide area monitoring system in smart grid," in *Computing Research Repository*, Feb. 2011.

[16] "Vulnerability assessment of the transportation infrastructure relying on the global position system," John A. Volpe National Transportation Systems Center, Tech. Rep., 2001.

[17] V. Pereyra, "Iterative methods for solving nonlinear least squares problems," *SIAM Journal on Numerical Analysis*, vol. 4, no. 1, pp. 27–36, Mar. 1967.

[18] IS-GPS-200D. Interface Specification IS-GPS-200, Revision D, Navstar GPS Space Segment/Navigation User Interfaces, Navstar GPS Joint Program Office, 2004.

[19] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2009.

[20] K. Wesson, D. Shepard, J. Bhatti, and T. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proceedings of ION GNSS*, Portland, Oregon, 2011.

[21] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Proceedings of ION GNSS*, Portland, Oregon, 2011.