ROBUST GPS-BASED TIMING FOR PHASOR MEASUREMENT UNITS BASED ON SINGLE-RECEIVER AND MULTI-RECEIVER POSITION-INFORMATION-AIDED VECTOR TRACKING

BY

DANIEL CHOU

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, 2015

Urbana, Illinois

Adviser:

Assistant Professor Grace Xingxin Gao

ABSTRACT

In recent years there has been a major push by the power industry to utilize phasor measurement units (PMUs) for wide area monitoring and control. PMUs are considered to be one of the most critical technologies for the future and modernization of the power grid. This technology produces time-stamped voltage and current phasor measurements, allowing measurements from any point in the power infrastructure to be synchronized. Widely regarded as one of the most vital devices in monitoring and control for the future of power systems, PMUs rely on the Global Positioning System (GPS) to provide the absolute time reference necessary to synchronize phasor measurements. The security and reliability of PMUs are essential to the future of the power grid and so in this work we aim to provide robust GPS timing for PMUs.

Since power systems are considered part of the civil sector, PMUs must utilize the civil GPS signals to obtain the time reference. However, the low received signal strength and unencrypted nature of the civil GPS signal leaves PMU reliability susceptible to both non-malicious and malicious interference. Most notably, jamming and spoofing attacks on PMU GPS receivers can pose a risk to the position, velocity, and timing (PVT) solutions.

Our goals are to provide robust GPS time transfer for PMUs and to rapidly detect malicious spoofing attacks. We achieve these goals by leveraging the inherent properties of PMU GPS receivers. We propose and implement the position-information-aided (PIA) vector tracking loop and the multi-receiver PIA vector tracking loop. To evaluate the effectiveness of the algorithms presented in this thesis, we also conduct field experiments which showed improve tracking capabilities and continued operation through various attacks of both algorithms. Our experiments show that the proposed PIA and multi-receiver PIA vector tracking approaches 1) improve the robustness of GPS receivers used in PMUs against jamming and interference; 2) are robust against spoofing attacks; and 3) can detect various spoofing attacks. Finally, we conducted tests using a real-time digital simulator (RTDS) which demonstrate the impacts of an attack on a PMU's time source.

ACKNOWLEDGMENTS

First and foremost I would like to express my sincerest gratitude to my advisor, Prof. Grace Gao, for the continuous encouragement, support, and patience she provided throughout the course of my graduate studies.

I thank my labmates at the UIUC GPS group for the relaxing environment, invaluable assistance, and great discussions over the last two years. Also I would like to thank all the friends at UIUC, both new and old, for all the good times amidst the stress and deadlines. I also thank TCIPG and all the members of TCIPG for all their support and assistance in my graduate research endeavors.

Finally I would like to thank my family for their unconditional love and support.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Global Positioning System Background

The Global Positioning System (GPS) was developed by the United States Air Force in the early 1970s, at the height of the Cold War, as a means to quickly determine the location of military assets. In 1978, the first GPS Block-I satellite was launched and 15 years later, 1993, GPS achieved initial operational capability with a constellation of 24 satellites in Medium Earth Orbit. While GPS was originally developed for U.S. military use only, after a tragedy in 1983 where a civilian airplane carrying 269 passengers was shot down after accidentally entering Soviet airspace, President Ronald Reagan issued a directive that allowed unrestricted global access to GPS technology once the system was operational.

When the GPS system was proposed, the U.S. military predicted that upon completion GPS could potentially have tens of thousands of users. Today, GPS has evolved into an indispensable infrastructure with billions of receivers world-wide. Many critical sectors such as energy, finance, transportation, and communications are increasingly reliant on positioning, navigation, and timing (PNT) services provided by GPS. This thesis will focus on the use of GPS in the energy sector, the vulnerabilities GPS introduces, and a novel tracking method to mitigate potential vulnerabilities.

1.2 Phasor Measurement Unit Introduction

The generation, transmission, and distribution of electrical power over wide area is accomplished through the use of an interconnected infrastructure known as the power grid. Many industrialized countries have recognize the necessity of power grid security and advancement on a national scale. In the United States, a presidential policy directive (PPD-21) identifies the power grid as an critical infrastructure and executed a policy that aims to strengthen and secure the power grid [1]. The last two decades have shown that the power grid is vulnerable to intentional, unintentional, and natural disruptions. While past disruptions have merely resulted in small-scale losses, the power community has recognized the necessity for a more resilient infrastructure. In an effort to increase the resiliency and response time of power systems, new physical and cyber infrastructure, also known as the "smart grid," is in the process of being installed. One of the most important components of the smart grid infrastructure is the phasor measurement unit (PMU), which is a device that allows for synchronous phasor measurements by using GPS to supply a time reference.

Current power systems employ the supervisory control and data acquisition (SCADA) system for the purposes of collecting and monitoring the electrical wave observations in the power grid. This system operates without the use of an external time reference but has also been proven to have limited robustness and significant delayed event detection times. In SCADA, the state of the power grid is estimated using legacy sensors and transmitted to control stations via a communication system; the state information is then used in making decisions on the operation of the power grid [2]. The SCADA system generally polls for information from remote sites once every few seconds for critical systems and up to a few minutes for non-critical systems [3]; however, due to transmission delays and the asynchronous nature of the wave measurement tools, the information displayed by SCADA is delayed and out of phase. During typical steady-state conditions, delays in measurement are not of major concern. However, during system disturbances the information collected by SCADA does not accurately represent the system and the states cannot be precisely estimated [4].

While the current power grid relies on SCADA, the upcoming smart grid requires significantly improved state estimations and sampling rates. PMUs, also known as synchrophasors, are devices that provide precise electrical wave measurements at frequencies up to 60 Hz. The high speed measurements generated by PMUs are capable of providing the control stations with information at subsecond time frames, allowing dynamic state measurements of the power system. Additionally, since PMUs across the country use the

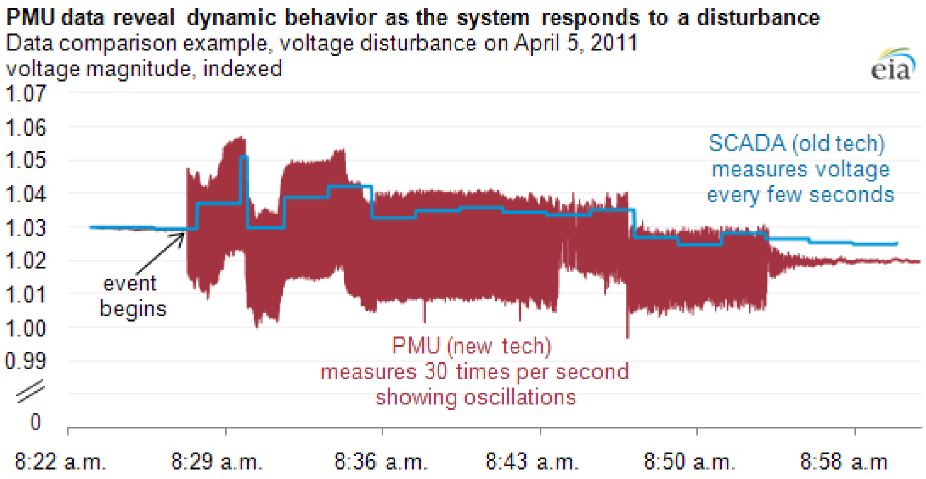

Figure 1.1: Disturbance in the power grid: SCADA and PMU comparison [5]. SCADA measurements show a significant delayed detection time compared with PMU measurements.

GPS system as a common time source, the phasor measurements collected by individual units can be placed onto the same phasor diagram without regard to distance or transmission times. This information allows for fine-tuning of the power system that was previously unattainable using the SCADA system. The near real-time measurements collected by PMUs would allow for adaptive and robust state adjustments to account for any changes in the system.

Figure 1.1 illustrates the difference between measurements collected by the SCADA system and a PMU during disturbance in a power grid in Oklahoma [5]. For this disturbance, the SCADA system displayed a delayed detection time of around 30 seconds and only updates the states once every few minutes. These numbers may change depending on the system and the collection points but even the most ideal SCADA system can only collect a single sample in the time a PMU can collect hundreds. Figure 1.2 simplifies the basic operations of a PMU in the power grid.

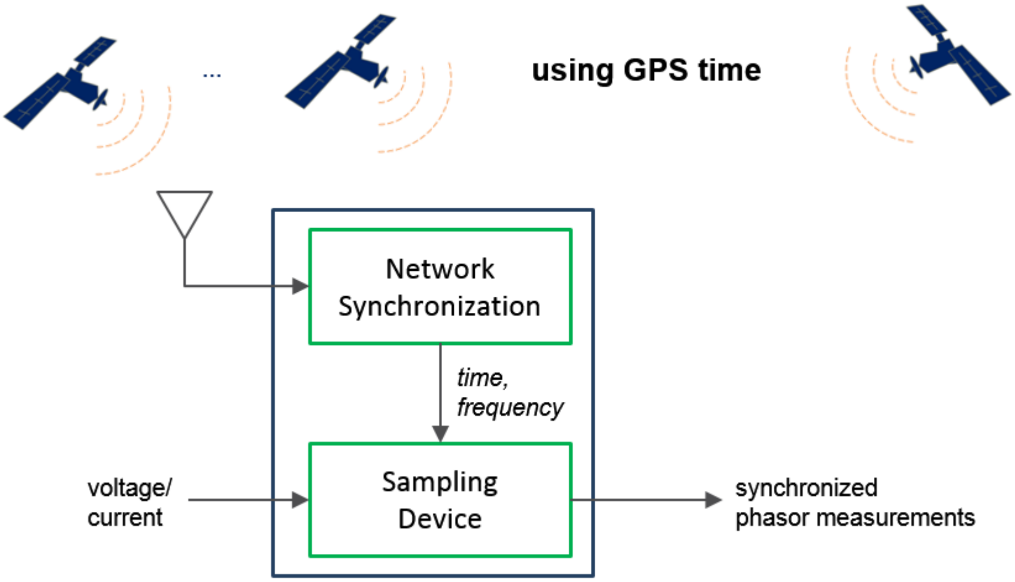

Figure 1.2: The basic operation of a PMU. By time-stamping measurements to GPS time, we can effectively synchronize phasor measurements among any set of PMUs.

CHAPTER 2

BACKGROUND

In this chapter we discuss the background behind PMUs, a few fundamental concepts of GPS, and GPS vulnerabilities specific to PMUs.

2.1 PMU Applications

The concept of PMUs was first developed in 1988 by Dr. Arun G. Phadke and Dr. James S. Throp at Virginia Tech; PMUs were designed to produce time-stamped phasor measurements of AC waveforms at rates up to 60 samples per second [6]. While this technology has been around for nearly three decades, PMU usage has only skyrocketed in the last few years when the U.S. Department of Energy committed a sizable amount towards the development of the smart grid in 2009. In 2010, the North American SynchroPhasor Initiative (NASPI) estimated that there were around 200 PMUs spread across the United States and Canada, the majority being research-grade units [7]. By 2012, that number had increased to 500 [5]; and by the end of 2014, NASPI estimated that there were over 1,700 production grade PMUs deployed across the U.S. and Canada [7]. This network now provides near 100-percent visibility of the major power systems and many companies have already begun to integrate PMU measurements into their monitoring systems.

PMUs are generally installed at critical substations, strategically placed such that the states of an entire area can be monitored for shifts in grid stability at any time. Since PMU measurements are synchronized to a common time reference, absolute comparisons between PMU measurements are possible allowing system operators to accurately assess system conditions and make control decisions [8, 9].

There are many benefits to utilizing PMUs, a few are listed below.

1. Automatic control: This includes, for example, balancing supply and demand in the power grid. Due to safety concerns, current transmission lines operate under the worst-case limit which restricts power flow far beneath the ideal dynamic limit. PMU technology has the potential to change the economics of power delivery by automatically balancing supply to demand, allowing power to flow up to the line's dynamic limit instead of its worst-case limit [10].

2. Fault detection: In 2003, a widespread blackout in the Northeast U.S. illustrated how PMU technology could have been used to detect and mitigate the effects of the blackout [11].

3. Wide area monitoring and analysis: WAM can reveal patterns, trends, and abnormalities in the power system.

4. Event analysis: Post-event analysis will benefit significantly from the data gathered by PMUs.

In North America alone there are currently over a thousand PMUs networked into the power grid. However, the measurements collected by these PMUs have yet to replace those of the SCADA system in their roles for automatic control of the power systems. This is largely due to the fact that PMUs are not yet secure devices given their dependence on GPS. It has been demonstrated that attacks on PMUs can induce timing errors leading to the destabilizing or unnecessary control responses from an automated system [4].

2.2 Global Positioning System

The Global Positioning System is designed as a satellite-based radio navigation system that provides position, velocity, and time (PVT) information to any GPS receiver given that the signals from four or more satellites are received. GPS utilizes a network of 24 to 32 satellites orbiting the Earth twice a day at approximately 20,200 km above the surface of the earth. Each satellite is equipped with multiple network-synchronized atomic clocks, enabling a user receiver to effectively synchronize to the satellites' atomic clocks for near atomic accuracy, without the cost of owning an atomic clock. Each GPS satellite continuously broadcasts several signals at various frequencies.

For the purposes of this thesis, we will only discuss the signals broadcast at the GPS L1 frequency (1575.42 MHz). GPS signals are transmitted at a power equivalent to a 50 watt light bulb and by the time they reach a GPS receiver on the Earth's surface, the GPS signals are buried beneath the thermal noise floor. Fortunately, GPS signals can still be decoded due to the pseudo-random noise (PRN) codes that the satellites use. Each satellite transmits two unique spread spectrum pseudo-random ranging signals: a civil Coarse/Acquisition (C/A) code and a Precision encrypted (P(Y)) code. The C/A code is unencrypted and readily available to the public whereas the P(Y) code is reserved for military use. Navigation messages are further modulated onto the signals which, once decoded, are used to calculate the satellite positions and the satellite clock bias [12].

Once the pseudorange, satellite positions, and satellite clock biases are known we use basic trilateration to determine the user location:

$$\begin{aligned}\rho_r^{(i)} = \sqrt{(x_s^{(i)} - x_r)^2 + (y_s^{(i)} - y_r)^2 + (z_s^{(i)} - z_r)^2} \\ + c(b_r - b_s^{(i)}) + \epsilon^{(i)}\end{aligned}$$

where $x_s^{(i)}$ is the position of the ith satellite, x_r is the position of the user receiver, $\rho_r^{(i)}$ is the pseudorange between the user receiver and the ith satellite, b_r is the receiver clock bias, $b_s^{(i)}$ is the satellite clock bias, and $\epsilon^{(i)}$ is the range measurement error. Given that we have 4 or more satellites, the unknowns (x_r, y_r, z_r, and b_r) can be solved for by minimizing $\epsilon^{(i)}$.

2.2.1 GPS Vulnerabilities Affect PMUs

As with all GPS dependent systems, GPS vulnerabilities are included in PMU vulnerabilities. Other PMU vulnerabilities include physical and cyber vulnerabilities. However, both the physical security and cyber security aspects of PMUs are more readily dealt with since cyber security flaws can quickly be patched and physical security is easily upgraded. GPS vulnerabilities, on the other hand, are much more difficult to mitigate since GPS satellite-receiver communication only flows one way and the structures of GPS civil signals are readily available for public use. As a result, PMU reliability is limited by GPS reliability.

The weak signal strength and unencrypted nature of the civil GPS signals leave receivers at risk for unintentional interference, jamming [13, 14], and spoofing attacks [15, 16, 17]. Each of these threats can potentially alter the position and time solutions generated by the receivers.

Threats to PMUs considered in this thesis:

1. Unintentional interference: There are many sources of unintentional interference to GPS signals. In recent years, the GPS community was engaged in a struggle in order to prevent high-powered radio signals from being broadcast near the GPS L1 frequency [18]. While the high-powered signals would only be broadcast in their allocated band, studies on the subject revealed that the low-powered GPS signals would be overwhelmed by the high-powered signals, forcing millions of existing GPS users to upgrade their devices or accept degraded service [19]. Unintentional interference can also come from naturally occurring electromagnetic (EM) fields [20, 21] and solar flares [22]; and even common electronic devices have been reported to produce interference.

2. Jamming: In a jamming attack, a jammer transmits high-powered signals in the GPS frequency band which effectively raises the noise floor and prevents a user receiver from acquiring and tracking the GPS signal. Due to its simplicity, a jamming attacks is perhaps the most common attack faced by GPS receivers.

3. Spoofing: Since the structure of the civil GPS signals is publicly known, a spoofer can generate falsified GPS signals in order to mislead the target receiver as shown in Figure 2.1. There are many types of spoofing attacks [23, 16]; in this thesis we will focus on meaconing attacks, also known as bent-pipe spoofing and record-and-replay attacks. A spoofer employing meaconing attacks records authentic GPS signals in one location and rebroadcasts (with a delay τ) them towards the target receiver. The navigation processing of a receiver affected by a meaconing attack will produce a PVT solution with the position of the spoofer's recording antenna and a time solution that is delayed by tau.

PMU-based control of the power grid is being pushed for by both the power industry and the U.S. Energy Information Administration (EIA) [5]. Reliable PMU measurements can pave the way to efficient energy distribution,

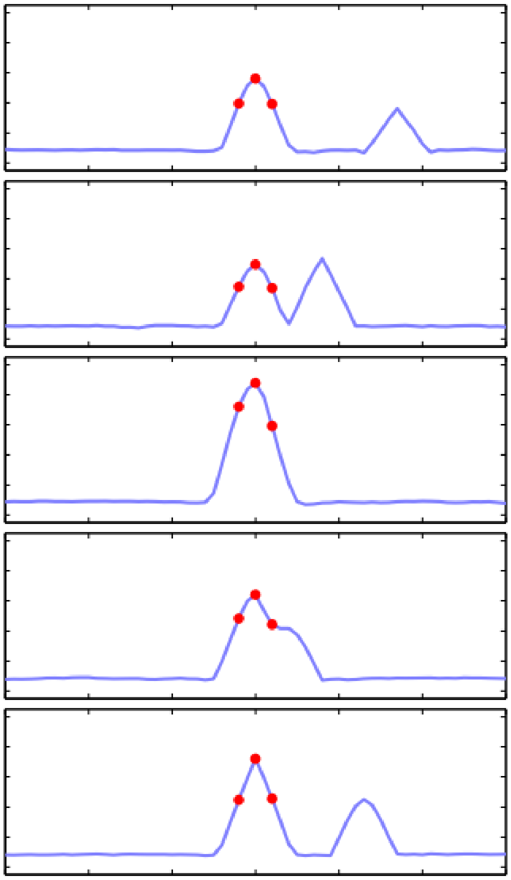

Figure 2.1: A spoofing attack in progress. In the first frame, the tracking loop is locked onto the legitimate GPS signal. In the second frame, the spoofer matches the amplitude of the legitimate GPS signal. In the third frame, the legitimate signal and the spoofed signal overlap. In the 4th frame the tracking loop locks onto the spoofed signal. In the 5th frame, the spoofed signal draws the tracking loop away from the legitimate signal, successfully spoofing the signal. [15]

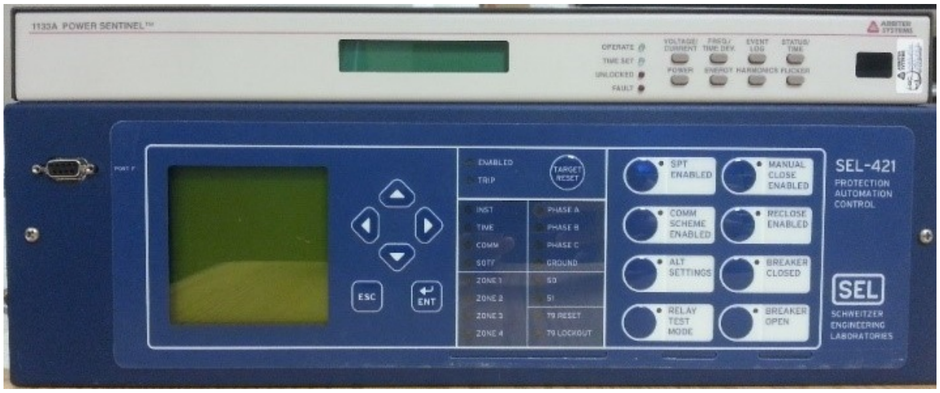

Figure 2.2: Two phasor measurement units from the TCIPG testbed at University of Illinois at Urbana-Champaign.

increase grid resistance and robustness to disturbances, and increase event response times. However, the security and stability of the power grid supersedes the improved efficiency and control. The security risks introduced by utilizing GPS-based devices prevent PMUs from being fully integrated into the power system. Since we aim to provide robust GPS-based timing to PMUs, our goals are to:

1. Improve PMU GPS receiver robustness against interference and jamming attacks.
2. Increase receiver robustness against spoofing attacks.
3. Detect spoofing attacks.

2.3 Our Testbed

To fully understand the real-life impacts of a spoofed or jammed GPS signal on the PMU, and by extension the power grid, we must be able to test its effects in a controlled environment. At the University of Illinois at Urbana-Champaign, the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) has built a testbed specifically for emulating large-scale power systems using high-end simulation equipment. The testbed currently contains 10 PMUs, two of which are shown in Figure 2.2, which are used to control and monitor high fidelity simulations and equipment such as the real-time digital simulator (RTDS) shown in Figure 2.3.

Figure 2.3: A real-time digital simulator of power systems at the University of Illinois at Urbana-Champaign. The RTDS is capable of simulating large-scale power systems in order to test the effects of disturbances on the power grid.

2.4 Contents of this Thesis

The remainder of this thesis discusses a novel type of tracking loop, the PIA vector tracking loop, our approach to implementing the algorithm, and results from field tests designed to test the PIA vector tracking loop. Then another chapter will discuss the multi-receiver PIA vector tracking loop and test results from this algorithm. Finally, we will present the test results from our RTDS simulations and give the conclusions.

CHAPTER 3

POSITION-INFORMATION-AIDED VECTOR TRACKING

3.1 Concepts of PIA Vector Tracking

In order to accomplish the goals set, we proposed and implemented the Position-Information-Aided (PIA) vector tracking loop which utilizes the static nature of the GPS receivers used in PMUs to enhance tracking performance. The concept of the PIA vector tracking loop was first developed by Heng et al. [24]. The basic idea behind the PIA vector tracking loop is that by leveraging the knowledge of the true position of GPS receivers used in PMUs, we can accurately predict the code and carrier measurements used in tracking the signal. By projecting the relative position and velocity between satellites and the receiver on the line-of-sight (LOS) direction, the tracking parameters can be precisely estimated. This type of receiver architecture is a subset of the vector tracking architecture which has been shown to increase immunity to interference and jamming [25, 26, 27]. Vector tracking combines signal tracking and position/velocity estimation into one algorithm, allowing information from one channel to aid in the tracking of another. The main downside to vector tracking is the high computation time required; however, for the purposes of this work, processing power is not of major concern.

Tracking robustness is also improved through the use of Kalman filtering and since the receivers in a PMU must remain static, the parameters of the tracking loops can be adaptively chosen to narrow the loop filter bandwidth. The narrowband tracking loop limits receiver noise, which reduces the effective radius of any jamming attacks. Additionally, the PIA vector tracking approach allows for a natural defense against meaconing attacks. Since the PIA vector tracking approach is dependent on the true position of the GPS receiver, the proposed tracking loop will fail to converge in the case of a meaconing attack, therefore enabling the detection of meaconing.

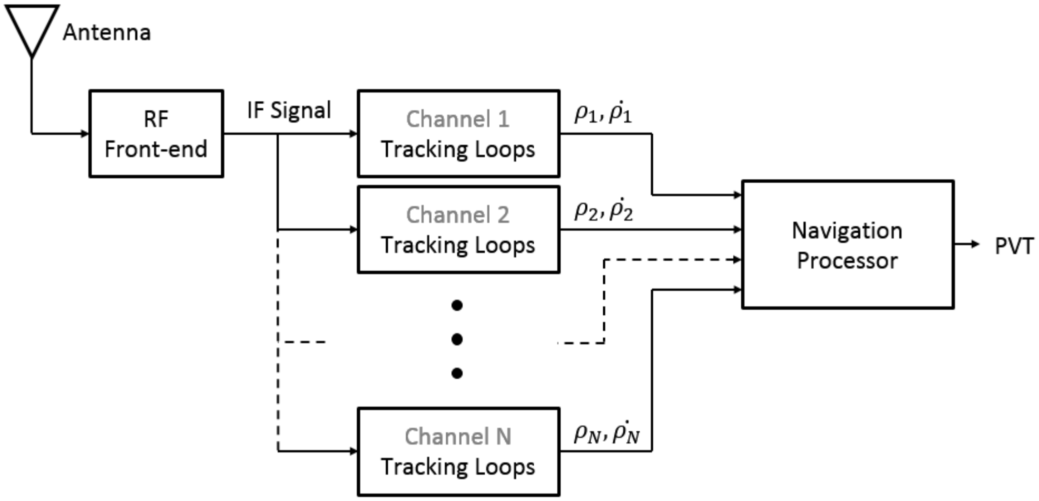

Figure 3.1: Scalar tracking architecture. The incoming signal is processed by N independent tracking loops, where N is the number of visible satellites.

3.2 Background on Traditional Tracking Methods

3.2.1 Scalar Tracking

Tracking loops are among the most critical components of a GPS receiver. These loops process received signals with an ultimate goal of a position, velocity and time (PVT) solution. However, the code and carrier tracking loops are vulnerable to low signal-to-noise ratio and high dynamics [28]. Based on the principles of calculating navigation solutions, at least 4 satellites are needed to provide 3-dimensional positions and clock bias [24]. Therefore, when the number of available satellites drops below 4 due to interference or blockage, the receiver will fail to navigate.

In a traditional GPS receiver, tracking loops work independently [25]. The inherent connections based on the same user position and velocities between channels are neglected [26]. Thus, there is no information exchange between channels, which makes it impossible for channels with strong signals to aid those with weak signals. Figure 3.1 shows the scalar architecture and Figure 3.2 breaks down the operation of the scalar tracking loop.

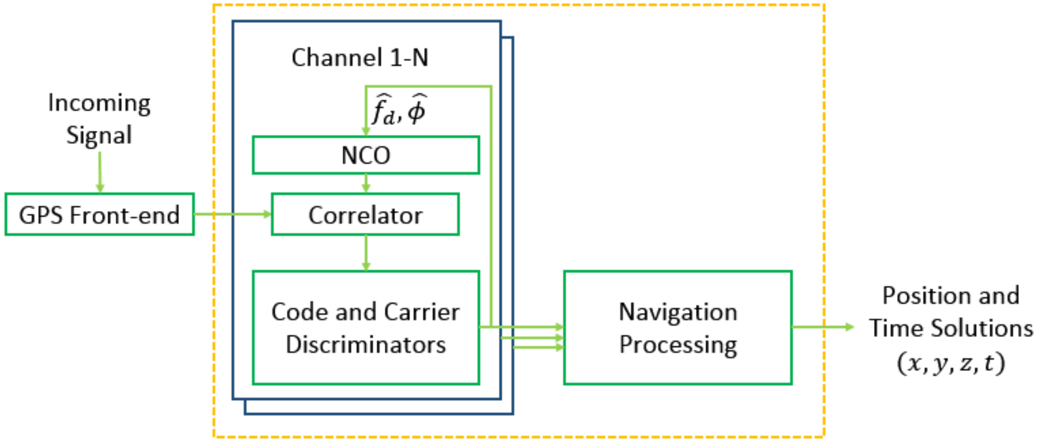

Figure 3.2: Simplified scalar tracking loop operation. In scalar tracking, the GPS signal is collected by the front end and used to generate correlations with the replicas from the NCO. The correlations are used to calculate the discriminators, which are then used to derive the next Doppler and phase estimates.

3.2.2 Vector Tracking

The concept behind vector tracking loops was first introduced by Spilker in 1996 [29]. While scalar loops function independently for all channels, a vector tracking loop simultaneously processes signals from all channels and calculates navigation solutions based on the code and carrier measurements. Vector tracking enhances performance by enabling information to be exchanged between channels, which enables channels with strong signals to aid those with weak signals [25]. Current PMU GPS receivers employ traditional scalar tracking loops for the purposes of a PVT solution [23]. However, scalar tracking loops neglect the inherent relations between each channel and the same static PMU receiver position. Figure 3.3 shows the basic architecture of a standard scalar tracking loop.

3.3 Architecture and Overall Flow

The structure of the PIA vector tracking loop is shown in Figure 3.4. In PIA vector tracking, information from the navigation filter and the known true position is fed back into the tracking loop and used to control the numerically controlled oscillator (NCO). As a result, the channels share information with

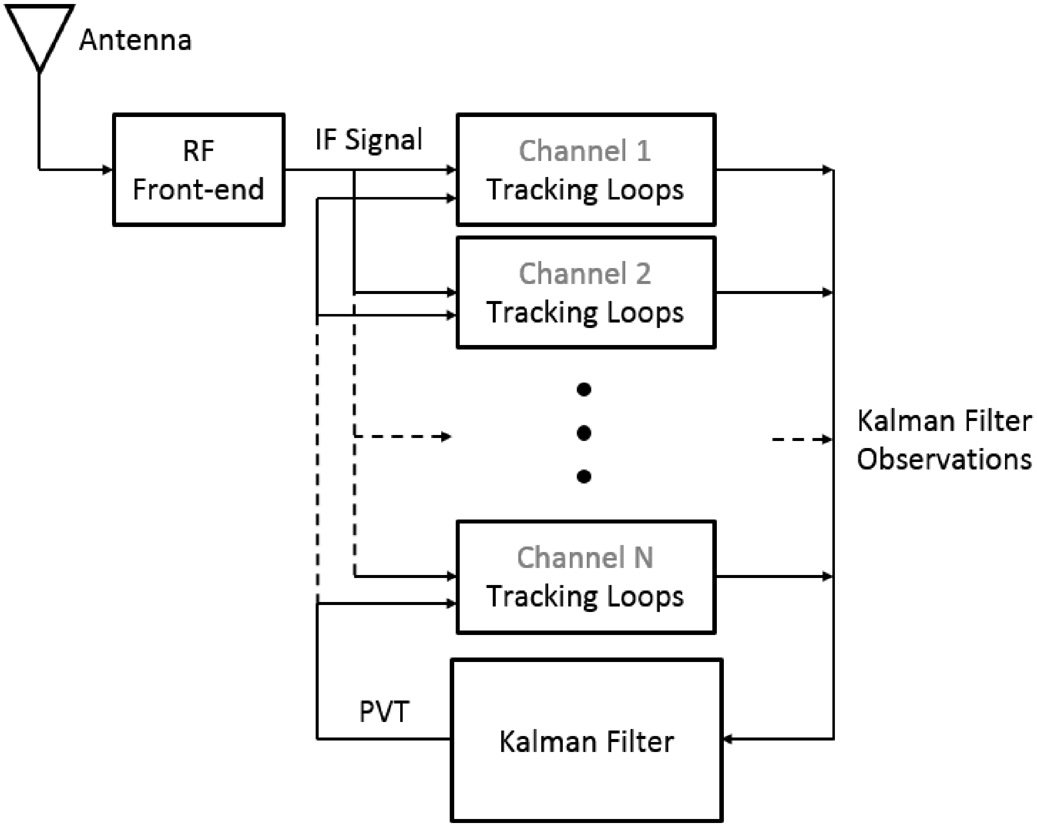

Figure 3.3: Vector tracking architecture. All of the channels are linked by the same user position, velocity, and time solutions. By feeding back the PVT solution into the tracking loop, the vector tracking architecture can improve tracking results.

one another and are able to aid channels with weak signal-to-noise ratios through the use of a common static receivers position, velocity, and clock bias.

In comparison to our PIA vector tracking approach, traditional scalar tracking processes each channel independently, and there is no feedback of information between the navigation filter and the tracking loops. As such, scalar tracking neglects to take into account the relations between satellites and the user position and velocity. By leveraging this information in our PIA vector tracking algorithm, the search space is narrowed considerably in the (x,y,z) dimensions.

In implementing the position-information-aided vector tracking algorithm, we actively drew on the previous vector tracking research completed by Zhao and Akos [26] as well as the open source MATLAB SDR code created by

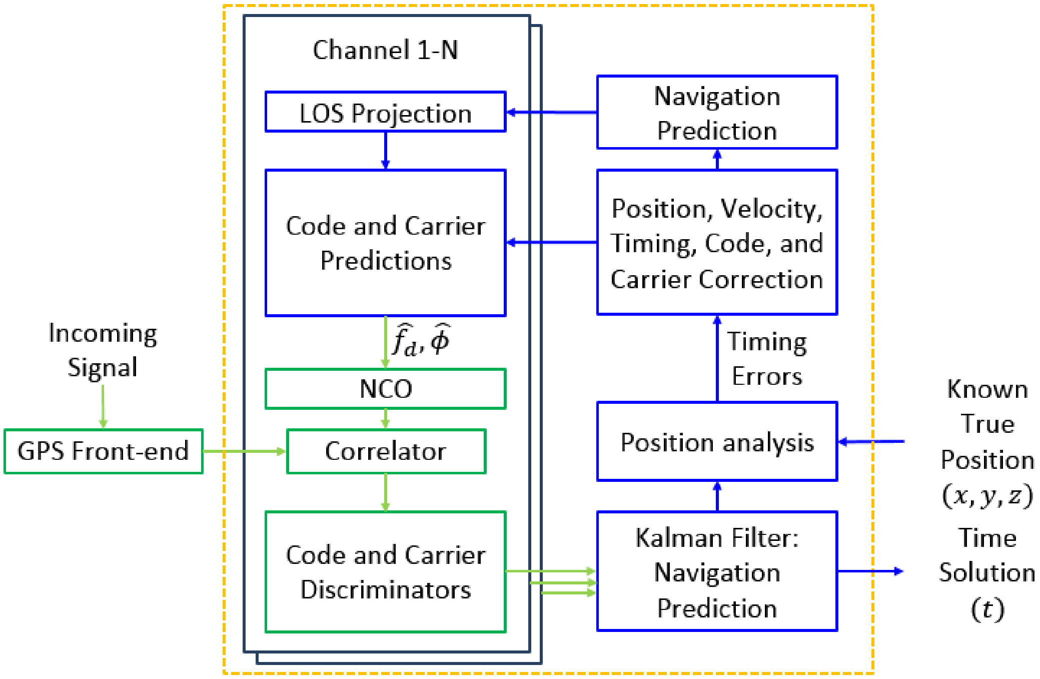
Channel 1-N
LOS Projection
Code and Carrier Predictions
$\hat{f}_d, \hat{\phi}$
NCO
Correlator
Code and Carrier Discriminators
Incoming Signal
GPS Front-end
Navigation Prediction
Position, Velocity, Timing, Code, and Carrier Correction
Timing Errors
Position analysis
Kalman Filter: Navigation Prediction
Known True Position (x, y, z)
Time Solution (t)

Figure 3.4: Position-Information-Aided vector tracking loop operation. By assisting the tracking loop with the known location, the PMU GPS receiver increases its robustness against interference.

Borre et al. [30]. The open source vector tracking code designed by Zhao and Akos was designed to operate under high dynamics and low signal-to-noise environments. For the purposes of implementing the PIA vector tracking, we have extensively modified the existing vector tracking code for operation under no dynamics and low signal-to-noise situations.

PIA vector tracking loops are meant to be used in conjunction with the existing scalar loops. At a specific time epoch, the following are extracted from the scalar tracking results and used to initialize the PIA vector tracking loop: code phase ($\phi_{j,k}$), code frequency ($f_{code,j,k}$), carrier frequency ($f_{j,k}$), signal transmit time ($t_{trans,j,k}$), clock bias ($t_{b,k}$), and clock drift ($t_{d,k}$). The subscript j represents the jth satellite and k represents the kth epoch. Since the PIA vector tracking is loosely dependent on these initial values, we choose to initialize our tracking loop after the scalar loop has gained a strong fix on the signal.

After initialization, the PIA vector tracking loop first predicts the navigation solution and errors for the next time epoch. Then early, late, and prompt code replicas are generated using the LOS projections to calculate the predicted Doppler and phase terms. The code replicas are then used to create correlations with the signal from the GPS front end which is then used generate the code and carrier discriminators. The discriminators from each channel contain the code and carrier errors, which are then projected onto the LOS vectors and used to generate the Kalman filter measurement matrix. The Kalman filter then estimates the new errors and, based on the updated errors, we can estimate the new navigation solution and create a prediction for the next time epoch. Since we know the true position of the GPS receiver, we then correct the prediction and create a closed feedback loop using the corrected predictions.

3.4 Detailed Flow

The process for the PIA vector tracking algorithm can be broken down into 4 main groups: 1. Estimation of the NCO parameters, 2. Discriminator calculation and processing, 3. Navigation error estimation and navigation prediction, 4. Navigation correction and error correction using the true position and feedback. In the next section, we will discuss each of these groups in greater detail.

3.4.1 Estimation of the NCO Parameters

The NCO uses carrier frequency and phase estimates to generate code replicas used for correlation. Since the carrier frequency and phase terms are directly influenced by the geometry and movement of the satellites with respect to the PMU GPS receiver, we simply need to use the satellite positions and velocities to estimate these terms.

We assume that the ephemeris values are known from either scalar tracking results or external sources. Then the satellite positions from the kth epoch can be generated and the satellite positions and velocities are then used to estimate the pseudorange, the LOS unit vector, and find the relative velocity between the satellite and the PMU receiver. The code phase and carrier frequencies can then be calculated based on the previous estimated terms. The true position of the receiver is assumed to be known, and therefore the predicted position and velocity are given by the following equations:

$$\hat{X}_{k+1} = X_{true} \tag{3.1}$$

$$\hat{V}_{k+1} = V_{true} \tag{3.2}$$

where X_{true} is the PMU receiver position and V_{true} is the PMU receiver velocity. We denote position and velocity predictions for the next time epoch as $\hat{X}_{k+1}$ and $\hat{V}_{k+1}$. Once the position and velocity projections are calculated the code phase/frequency, carrier frequency, and clock drift prediction equations are given in equations 5-8 of Zhao and Akos [26].

From the estimated code phase and carrier frequencies, replicas of the code are generated and used to create correlations with the received GPS signal at the corresponding time epoch.

3.4.2 Discriminator Calculation and Processing

The NCO generates early, prompt, and late replicas which are used to create correlations with the incoming signals. We will denote the in-phase early, prompt, and late correlations as I_E, I_P, and I_L. Similarly, quadrature correlations will be denoted as Q_E, Q_P, and Q_L.

In this work, we chose to only use carrier frequency discriminators since carrier phase tracking is not suited for low signal-to-noise environments, as is the case during interference or jamming attacks.

For the code phase discriminator, we chose to use:

$$\frac{1}{2}\frac{E-L}{E+L}$$

where

$$E = \sqrt{I_E^2 + Q_E^2} \quad \text{and} \quad L = \sqrt{I_L^2 + Q_L^2}$$

This discriminator, described in [31], is a noncoherent early minus late envelope normalized by E+L to remove amplitude sensitivity.

We chose to use a normalized decision directed frequency discriminator as described in table 5.4 of [31]:

$$\frac{(\text{cross}) \times \text{sign}(\text{dot})}{2\pi(t_2 - t_1)(I_{P2}^2 + Q_{P2}^2)}$$

where

$$\begin{aligned} \text{cross} &= I_{P1}Q_{P2} - I_{P2}Q_{P2} \\ \text{dot} &= I_{P1}I_{P2} - Q_{P2}Q_{P2} \end{aligned}$$

and the $P1$ and $P2$ subscripts represent the results over current epoch and the previous epoch. The discriminator outputs are then used to generate the Kalman filter measurement matrix.

3.4.3 Navigation Error Estimation and Navigation Prediction

The discriminators output the code phase errors and carrier frequency errors which contain the corresponding LOS projections of the discrepancies between the estimated position and velocity and the known true position and velocity. The relationship between the code phase error and carrier frequency errors with the user position error can be modeled as:

$$e_{code,k} = \hat{\phi}_{j,k} - \phi_{j,k} \tag{3.3}$$

$$e_{carr,k} = \hat{f}_{j,k} - f_{j,k} \tag{3.4}$$

where e_{code} and ϕ are in meters, and e_{carr}, and f are in meters/sec. By using the calculated LOS projections $(a_{j,k})$, we can rewrite (3.3) and (3.4) as functions of the clock bias and change in clock drift:

$$e_{code,k} = t_{b,k} + (X_k - \hat{X}_k)^T a_{j,k} \tag{3.5}$$

$$e_{carr,k} = \Delta t_{d,k} + (V_k - \hat{V}_k)^T a_{j,k} \tag{3.6}$$

The position and velocity errors can be modeled as the difference between the true PMU receiver position and the calculated position and velocity:

$$\delta X_k = X_{true} - X_k \tag{3.7}$$

$$\delta V_k = X_{true} - V_k \tag{3.8}$$

In each of the equations above, there is an implied error term that has not been included.

We can see from the error analysis that, if the position and velocity errors can be estimated, the navigation solution can also be calculated. Therefore in implementing the PIA vector tracking, we chose the position errors, velocity errors, clock bias error, and clock drift error as the states of the Kalman filter. Since we know the initial position, velocity, clock bias, and clock drift values from the scalar tracking results, the navigation solution can be estimated through the errors.

Then δX, δV, δt_b, and δt_d are the states of our system and the discrete process equation is given by

$$\begin{bmatrix} \delta X_{k+1} \\ \delta V_{k+1} \\ \delta t_{b,k+1} \\ \delta t_{d,k+1} \end{bmatrix} = F_{k,k+1} \begin{bmatrix} \delta X_k \\ \delta V_k \\ \delta t_{b,k} \\ \delta t_{d,k} \end{bmatrix} \tag{3.9}$$

where

$$F_{k,k+1} = \begin{bmatrix} 0 & \Delta t & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \Delta t \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

where Δt is given by the time difference between the kth and $k+1$ time epoch. The Kalman filter measurement equation is then given in equation 10 of Zhao and Akos [26]:

$$\begin{aligned} Z_k =& HX_k + V_k \\ =& [z_{code,1,k} \quad z_{carrier,1,k} \quad \cdots \quad z_{code,n,k} \quad z_{carrier,n,k}]^T_{1\times 2n} \end{aligned}$$

where the terms of the H matrix are determined by the following equations:

$$\begin{aligned} z_{code,j,k} &= a_{j,k}\delta X + t_{b,k} \\ z_{carrier,j,k} &= a_{j,k}\delta V + \Delta t_{d,k} \end{aligned}$$

where $\Delta t_{d,k}$ is the change in the clock drift error.

Since the states of the Kalman filter were chosen to be error of the position, velocity, clock bias, and clock drift, we can then correct our predictions as:

$$\begin{aligned} X_{k+1} &= \hat{X}_{k+1} + \delta X_{k+1} \qquad (3.10) \\ &= X_{true} + \delta X_{k+1} \\ V_{k+1} &= \hat{V}_{k+1} + \delta V_{k+1} \qquad (3.11) \\ &= V_{true} + \delta V_{k+1} \\ t_{b,k+1} &= \hat{t}_{b,k+1} + \delta t_{b,k+1} \qquad (3.12) \\ t_{d,k+1} &= \hat{t}_{d,k+1} + \delta t_{d,k+1} \qquad (3.13) \end{aligned}$$

where the 'hat' indicates the predictions from the previous time epoch. The corrected predictions shown here are then output as our navigation solutions.

In the PIA vector tracking loop, the bandwidth is controlled by the Kalman filter, which makes it difficult to pinpoint the exact bandwidth that is being used as the adaptive Kalman filter gain, K, is proportional to the bandwidth. Thus, in this work, the bandwidth was set empirically by controlling the Kalman filter Q and R matrices which represent the uncertainty in the dynamics of the user and the noise in the discriminator outputs. More detailed explanations can be found in [26]. However, to compare the scalar and PIA vector tracking results, the tracking loop bandwidths should be relatively similar. Therefore, we empirically adjusted the Q and R matrices such that the basic vector tracking loop's performance closely matched that of the scalar tracking loop using a 5 Hz bandwidth, due to the receiver being static, and we used the same Q and R values in our P.I.A vector tracking loop.

3.4.4 Navigation Correction and Error Correction Using the True Position and Feedback

Once the position and velocity predictions have been corrected by the Kalman filter, we then compare the corrected predictions with our known true position and velocity. By taking into account the true position, we can estimate the errors for the next time epoch using (3.7) and (3.8) and feed back the predicted errors into the tracking loop to form a closed loop.

Then the code frequency, code phase, and carrier frequency can be corrected as:

$$
\begin{aligned}
f_{code,j,k+1} &= \hat{f}_{code,j,k+1} \\
&\quad + (t_{d,k+1} + \delta V_{k+1} a_{j,k}) \\
&\quad f_{code}/c & (3.14) \\
\phi_{j,k+1} &= \hat{\phi}_{j,k+1} + \delta X_{k+1}^T a_{j,k} + t_{b,k} & (3.15) \\
f_{carrier,j,k+1} &= \hat{f}_{carrier,j,k+1} \\
&\quad + (t_{d,k+1} + \delta V_{k+1} a_{j,k}) \\
&\quad f_{carrier}/c & (3.16)
\end{aligned}
$$

3.4.5 Calculating GPS Receiver Clock Bias

Since we know the true position of the receiver, we can accurately calculate the clock bias of the receiver as a weighted average of the difference between the calculated pseudorange and actual range. Equation 4.7 from Heng [32]:

$$
t_b = \frac{1}{\sum_{j=1}^{J} \omega_j} \sum_{j=1}^{J} \omega_j (\tilde{\rho}^{(j)} - |x^{(j)} - x|) \tag{3.17}
$$

3.5 Experimental Setup and Results

In order to determine the performance of the PIA vector tracking algorithm compared with the traditional tracking algorithm, we conducted field tests using an off-the-shelf GPS receiver. For the receiver, we chose the SiGe GN3S GPS sampler, which is essentially an A/D converter with a bandpass filter, to collect raw GPS signals. The SiGe front-end is a thumb-sized USB device designed to operate in conjunction with a software-defined receiver (SDR), shown in Figure 3.5. It uses a sampling frequency from 4 MHz to 16 MHz and a quantization resolution of 2 bits. Since the quality of the GPS receivers used in PMUs is generally higher than that of a SiGe sampler, the results we obtain using data collected with the low-cost SiGe will provide a conservative lower-bound estimate of results collected using PMU receivers.

The antenna used in this experiment was a fixed-reference choke ring antenna (pictured in Figure 3.6) in conjunction with the SiGe sampler. Dur-

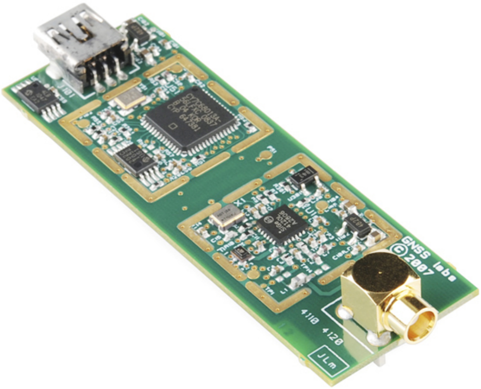

Figure 3.5: Low cost receiver - SiGe sampler.

ing data collection the antenna had full view of the open sky with up to 10 satellites with clear LOS. The data was then post-processed using the software-defined-receiver (SDR) for both scalar and PIA vector tracking.

After processing the collected data, the acquisition module of our SDR was able to acquire 9 of the 10 satellites in view. Then the data was processed using the scalar tracking loop and navigation module. The scalar tracking results were then used to initialize the PIA vector tracking loop.

When compared with scalar tracking results, the PIA vector tracking loop is expected to more accurately predict the code and carrier frequencies needed to track the signal, and as a result we obtain more accurate PVT solutions. Results over a 50 second time span are shown in Figures 3.7-3.15. Figures 3.7-3.9 show the code frequency difference from the GPS code frequency ($1.023e6$ MHz). From these figures, we can clearly observe the benefits of the PIA vector tracking algorithm. The PIA results are far less noisy than the scalar results due to the reduced uncertainty through fixed position feedback. Figures 3.10-3.12 show the Doppler frequencies for the first 3 channels. From the figures, we can see that the code and carrier frequencies calculated in the PIA vector tracking loop are more accurate and precise than the frequencies from the scalar counterparts.

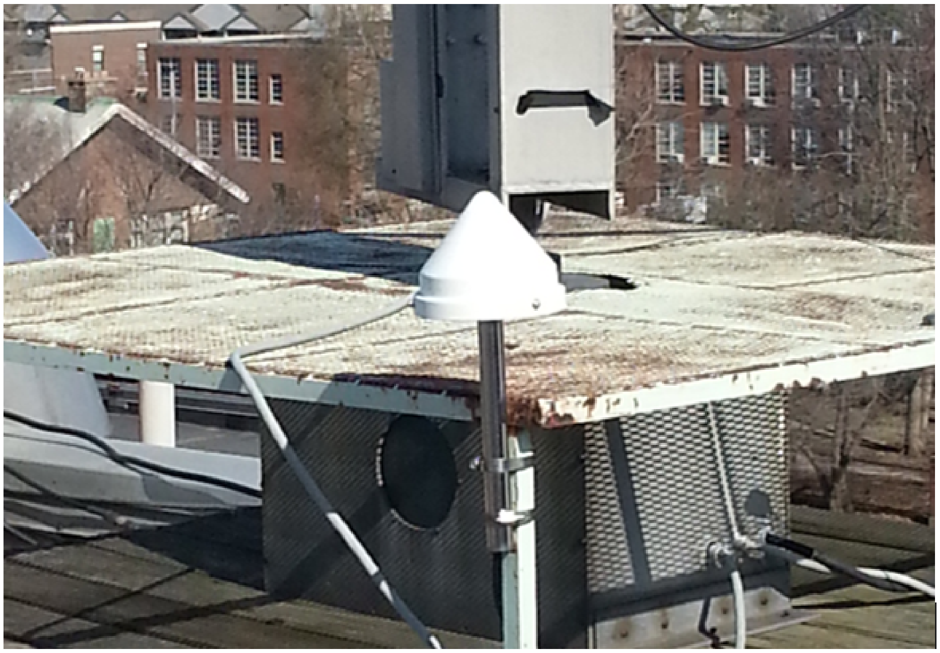

Figure 3.6: Fixed reference antenna with full access to the open sky.

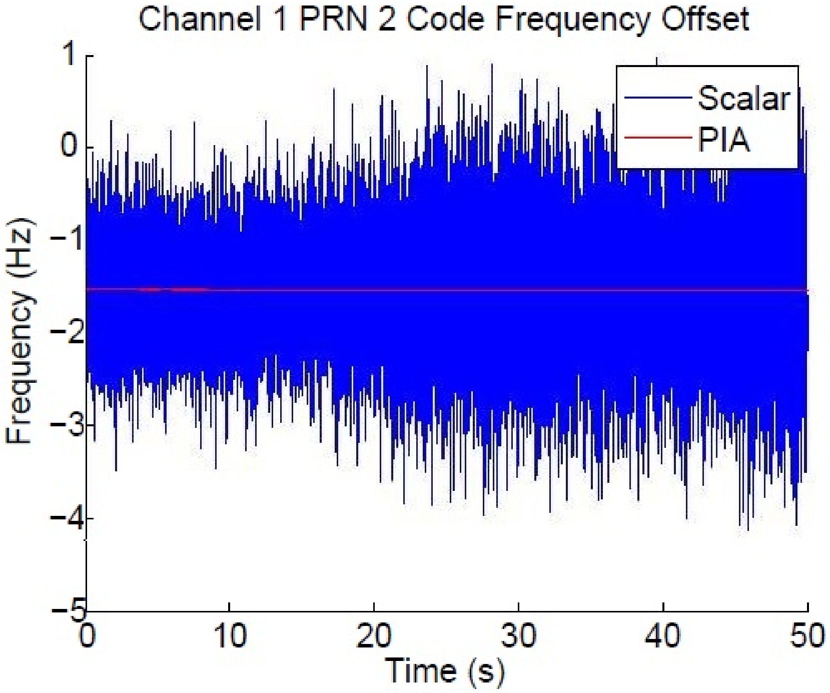

Figure 3.7: Code frequency results from PRN 2.

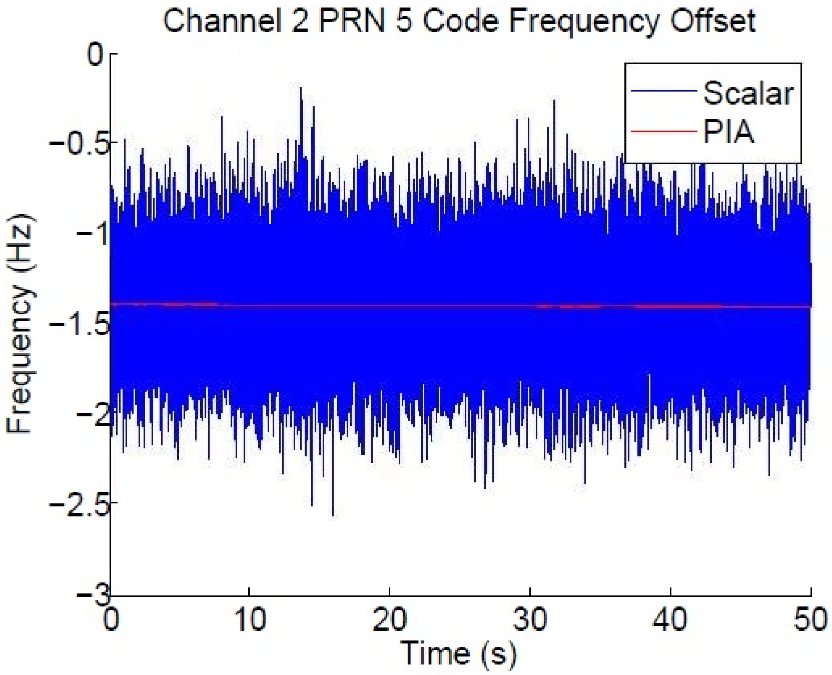

Figure 3.8: Code frequency results from PRN 5.

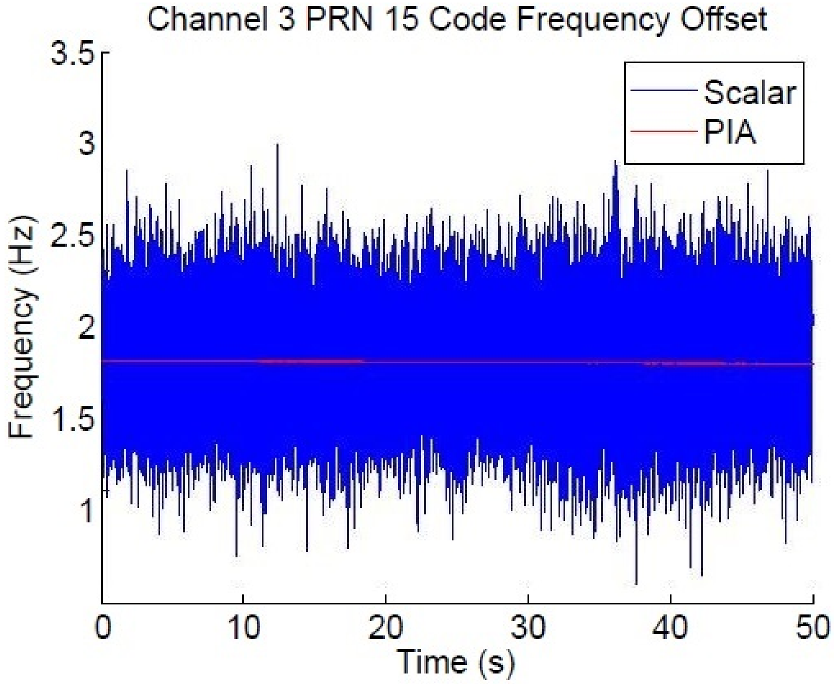

Figure 3.9: Code frequency results from PRN 15.

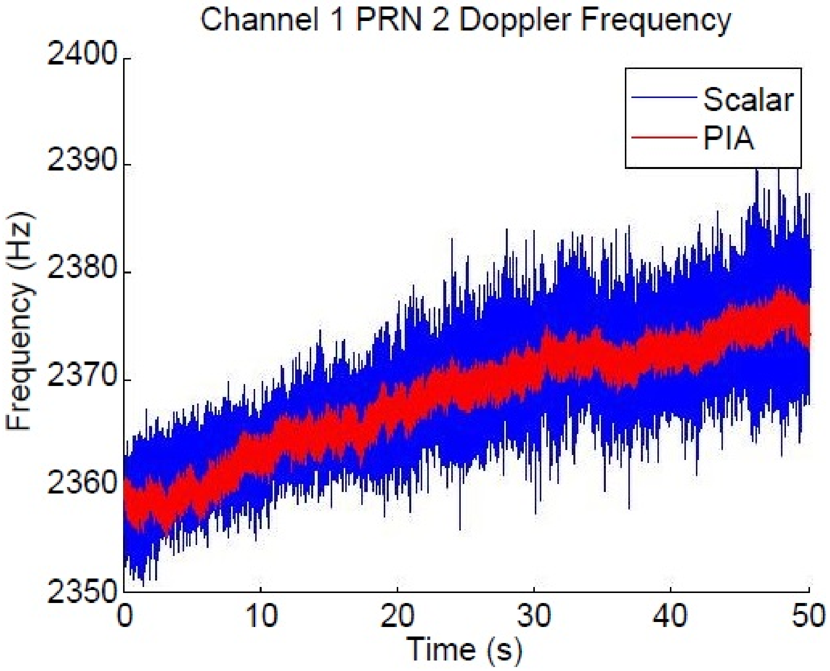

Figure 3.10: Code frequency results from PRN 2.

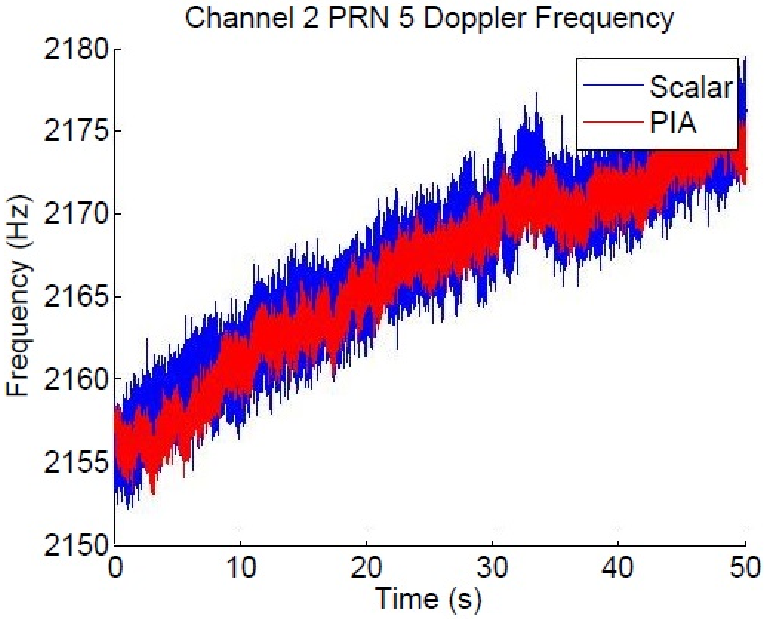

Figure 3.11: Code frequency results from PRN 5.

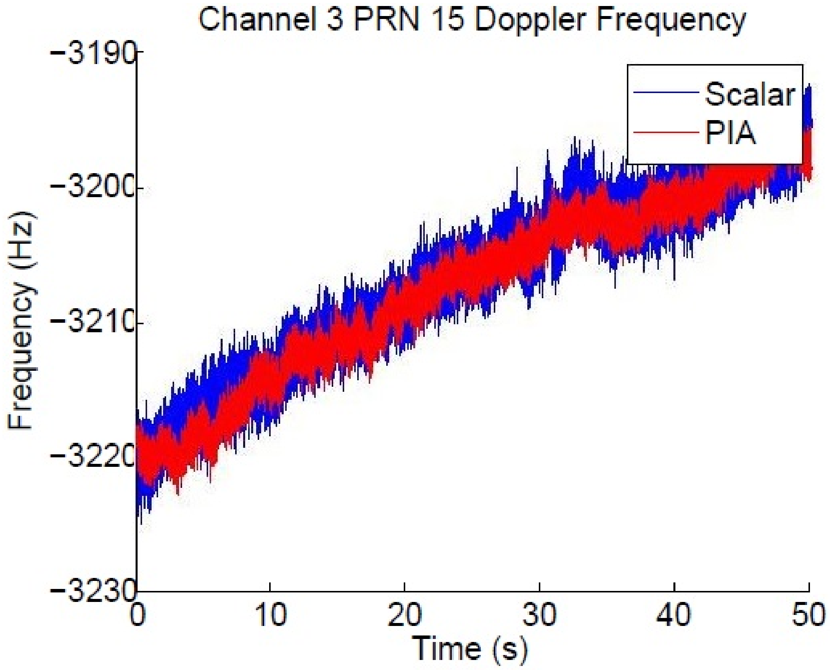

Figure 3.12: Code frequency results from PRN 15.

3.5.1 Noise Tolerance and Anti-Jamming Performance

To determine the noise tolerance and anti-jamming performance of the PIA vector tracking algorithm, we purposely added 1-10 dB of simulated Gaussian noise to the raw GPS signal and processed the resulting data. Figures 3.13-3.15 show the time error results for varying levels of added noise. With no added noise, the maximum time errors for the scalar results were close to 45 ns, whereas the time errors for the PIA results were around 10 ns.

Scalar tracking was able to produce decodable navigation bits up until we increased the noise past 4 dB. However, with every dB of additional noise, the number of channels that experienced a loss-of-lock increased. At 4 dB of additional noise, the scalar tracking loop was only able to lock onto 4 satellites while the original data could lock onto all 9. The time errors also increased as the noise increased: scalar results showed close to 60 ns of maximum errors and PIA results showed maximum errors of 13 ns.

The PIA vector tracking loop continued operating until we increased the noise past 9 dB, at which point the maximum time errors were close to 20 ns.

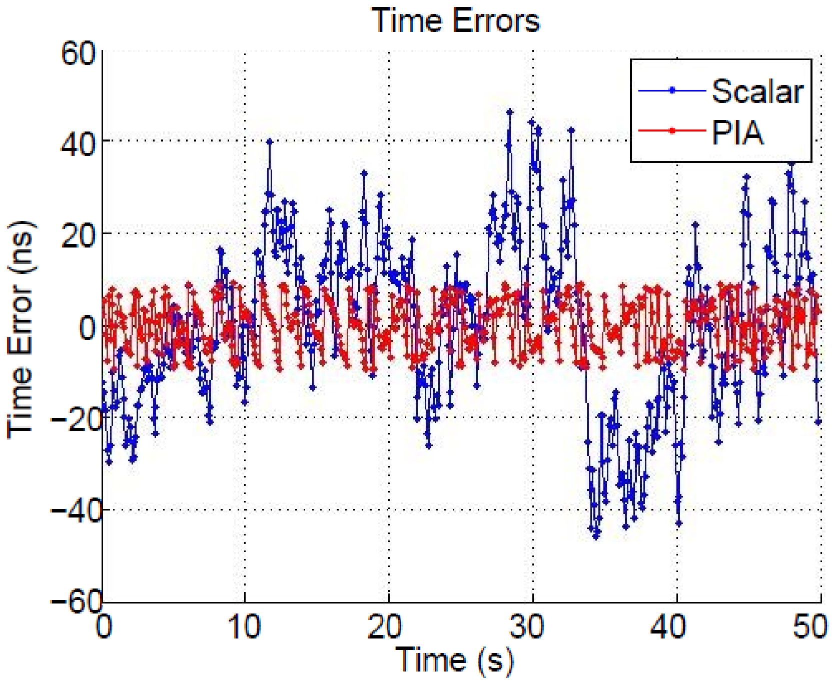

Figure 3.13: Time errors with no added noise.

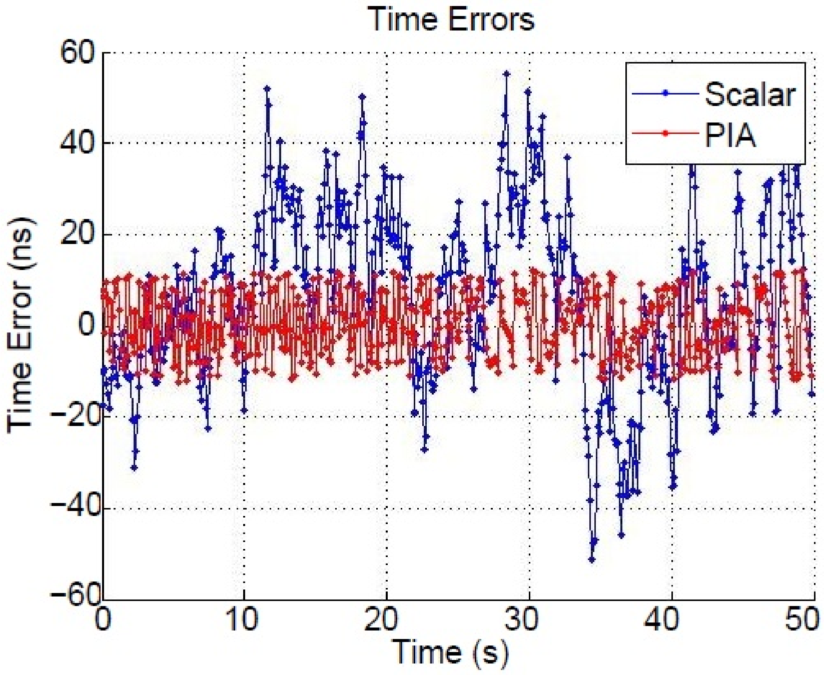

Figure 3.14: Time errors with 4 dB of added noise.

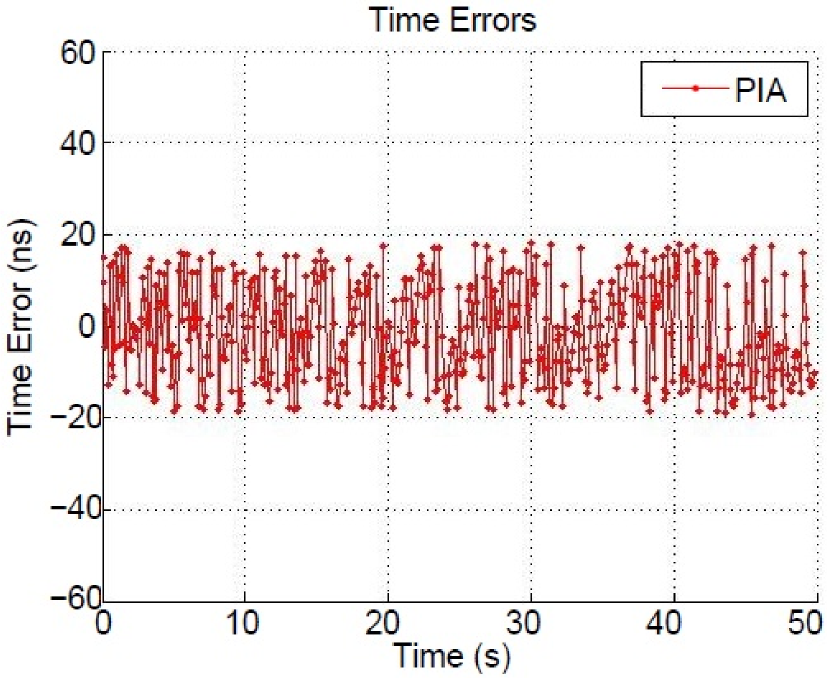

Figure 3.15: Time errors with 9 dB of added noise.

3.5.2 Meaconing Attack Simulation

The PIA vector tracking algorithm is designed to function with the known true position as the reference point. In a meaconing attack, also known as the record-and-replay attack, the GPS signal is first received by the attacker and then broadcast at a higher signal-to-noise ratio than the signals received from the satellites, causing the GPS receivers to lock onto the meaconed signal. A traditional scalar tracking loop would continue to operate during a meaconing attack; however, the PVT solution calculated would be equal to the PVT solution of the attacker, plus a delay, thus providing wrong and misleading timing information. Figure 3.16 shows the results of a meaconing attack simulation. Due to the fixed-position nature of the PIA vector tracking loop, the algorithm fails to converge as soon as the meaconing attack begins. Therefore, our proposed PIA vector tracking is able to successfully detect the meaconing attack.

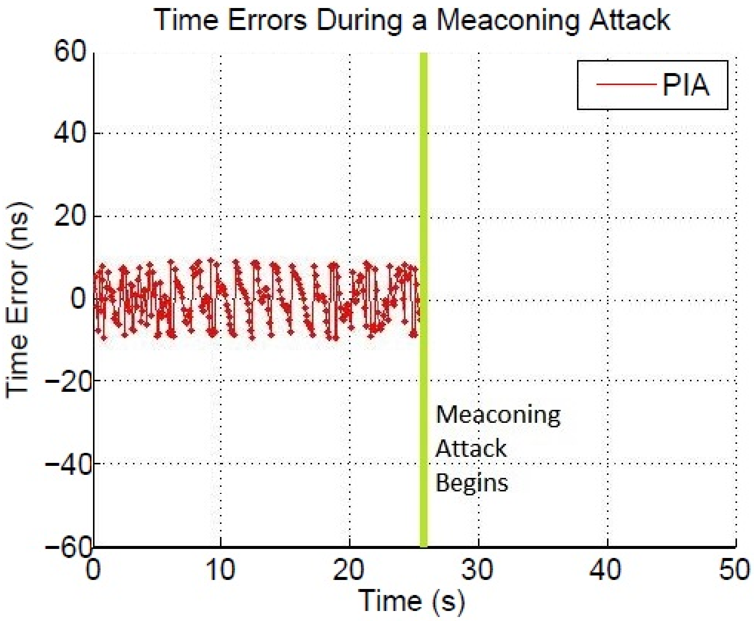

Figure 3.16: Time errors during a simulated meaconing attack with a 200m separation between the spoofer and the PMU GPS receiver.

CHAPTER 4

MULTI-RECEIVER POSITION-INFORMATION-AIDED VECTOR TRACKING

4.1 Concepts of Multi-Receiver PIA Vector Tracking

To meet the goals set in Chapter 2, we further propose the multi-receiver position-information-aided vector tracking loop which collaboratively processes the signals from multiple receivers which are connected by a common time source. This is an extension of the single-receiver PIA vector tracking loop that was proposed and implemented in a previous paper [33]. In this countermeasure, we deploy multiple receivers in close vicinity synchronized to a common clock as shown in Figure 4.1. By tracking each receiver in a multi-receiver PIA vector tracking loop, we will show that every threat can be either reduced (jamming) or detected (spoofing and receiver errors) by our countermeasure.

In traditional GPS receivers, scalar tracking loops are used to track GPS signals from each satellite in view. Each satellite's tracking loop operates independently and the results from the processed data are used to decode the satellite ephemeris data and calculate the navigation solution. In our multi-receiver PIA vector tracking loop, the receiver's navigation solution is set as the states of a Kalman filter, allowing information from all satellites to be shared by combining signal tracking and position/velocity estimation into one algorithm.

There are several aspects of our multi-receiver architecture that can be leveraged when designing spoofing detection algorithms. First, every receiver is static, which allows us to predict the expected code and carrier elements for all receivers by using the known baseline and the signal from a single receiver. The expected elements can then be compared with the actual measurements to detect inconsistencies. Secondly, each receiver will be connected by a common clock and therefore the data collected by each receiver should

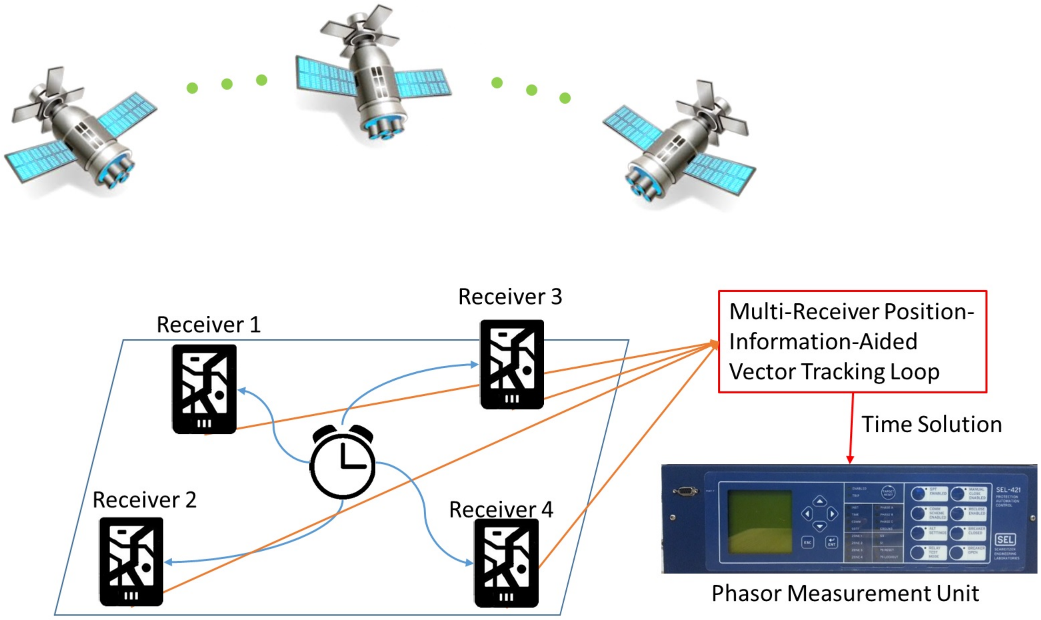

Figure 4.1: Multi-receiver architecture.

produce the same clock bias and clock drift. Finally, since the receivers are in close proximity to each other, we can compare their decoded navigation data as well as that of external sources.

By tracking the multi-receiver signals in a single algorithm, we can precisely calculate the clock solution and absolute GPS time while greatly increasing receiver resistance to jamming through redundancy. While single receiver PIA vector tracking algorithms have been shown to be capable of detecting meaconing attacks, multi-receiver PIA vector tracking can be used to detect and combat data-level spoofing and meaconing attacks. Additionally, multi-receiver processing can help in detecting receiver errors by cross checking the navigation message for consistency.

4.2 Threat Detection Capabilities

In the case of a single PMU GPS receiver, in order to avoid detection a spoofer will likely attempt to maximize the clock error while minimizing the position error. This can be done in data-level spoofing by modifying the ephemeris parameters such that the receiver sees each in-view satellite shifted by a certain distance along the line-of-sight vector (Figure 4.2). If done

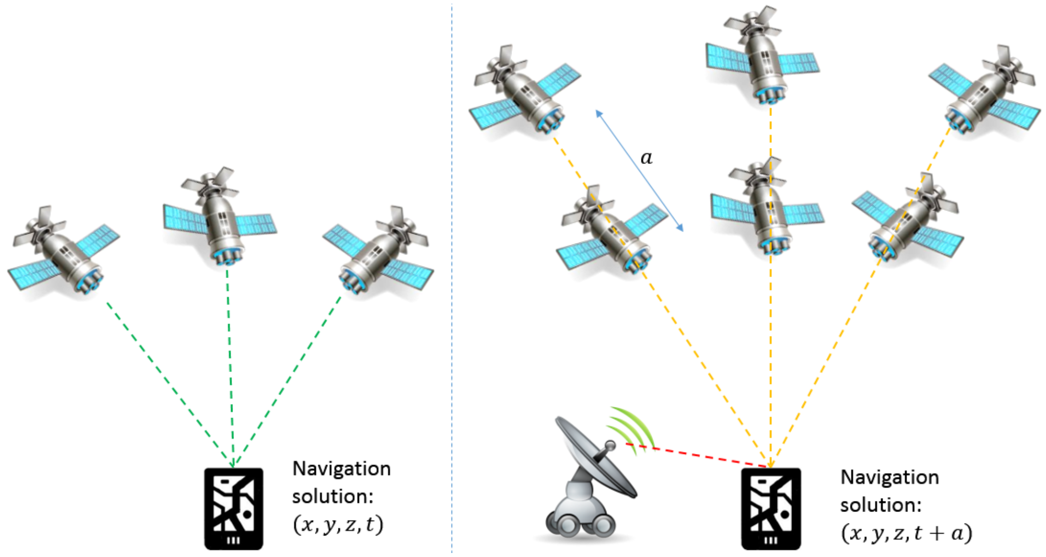
a
Navigation solution: (x, y, z, t)
Navigation solution: $(x, y, z, t + a)$

Figure 4.2: Spoofing attack designed to shift calculated satellite positions in such a way that the position solution remains the same but the clock bias is offset.

properly, both spoofing attacks can remain undetected by a single PMU GPS receiver. However, by deploying several clock synchronized GPS receivers in close proximity to create our multi-receiver architecture, we argue that every type of threat can be alleviated or detected.

In the case of a spoofing attack with a single attacker, there are three possibilities to consider: (1) none of the receivers are spoofed, (2) a partial number of receivers are being spoofed, and (3) all of the receivers are being spoofed. Since the majority of power system substations are fairly small (approximately 20m by 20m) and the receivers are restricted to this area, we can assume that either none (1) or all (3) of the receivers are spoofed.

If all of the receivers are subject to the spoofing attack, the position solutions for all receivers will be identical, causing significant errors to build up in the position-information-aided algorithms, and thus the attack can be detected. The only way to successfully spoof the multi-receiver architecture is to spoof each receiver in the network using multiple spoofers with carefully tuned transmit power to only spoof a single receiver. Each spoofer would be required to be time-synchronized to simultaneously adjust the perceived satellite positions or pseudoranges to manipulate the clock solution. While this spoofing attack is possible, it is highly unlikely that such a complex attack could be employed without severely compromised physical security.

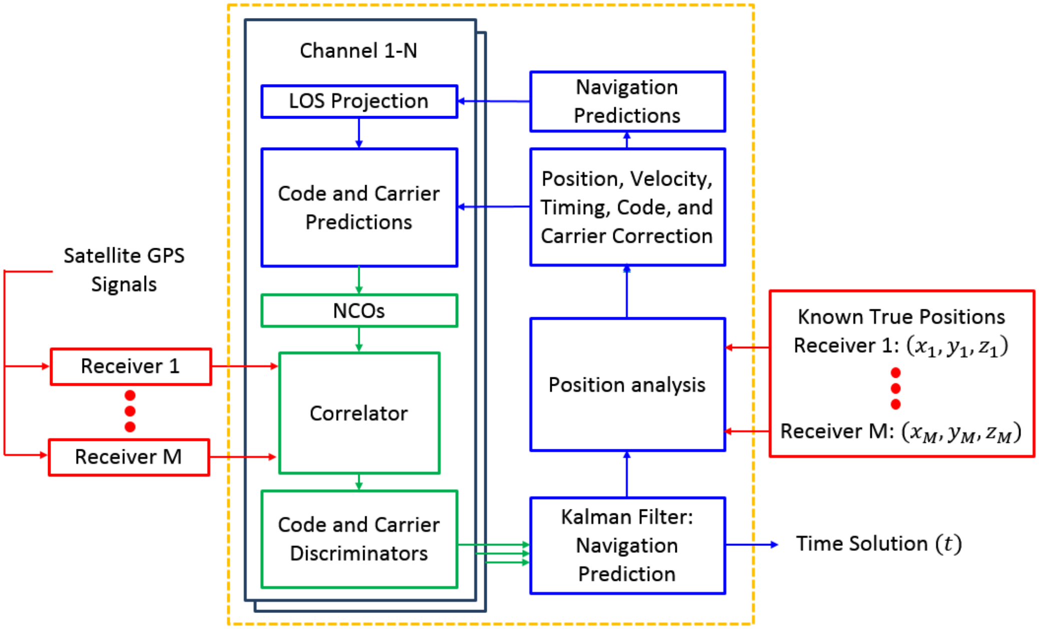
Channel 1-N
LOS Projection
Code and Carrier Predictions
NCOs
Correlator
Code and Carrier Discriminators
Navigation Predictions
Position, Velocity, Timing, Code, and Carrier Correction
Position analysis
Kalman Filter: Navigation Prediction
Time Solution (t)
Satellite GPS Signals
Receiver 1
Receiver M
Known True Positions
Receiver 1: (x_1, y_1, z_1)
Receiver M: (x_M, y_M, z_M)

Figure 4.3: Multi-receiver PIA vector tracking loop.

4.3 Architecture and Flow

The structure of the multi-receiver PIA vector tracking loop is shown in Figure 4.3. In multi-receiver PIA vector tracking, information from the navigation filter and the known true positions is fed back into the tracking loop and used to control the numerically controlled oscillator (NCO). As a result the channels share information with one another and channels with weak signal-to-noise ratios can be aided through the use of a common static receiver's position, velocity, and clock bias.

In comparison to our multi-receiver PIA vector tracking approach, traditional scalar tracking processes each channel independently, and there is no feedback of information between the navigation filter and the tracking loops. As such, scalar tracking neglects to take into account the relations between satellites and the user positions and velocities. By leveraging this information in our multi-receiver PIA vector tracking algorithm, the search space is narrowed considerably in the (x,y,z) dimensions.

Similarly to the single-receiver PIA vector tracking loop, the multi-receiver PIA vector tracking loop is meant to be used in conjunction with the existing scalar loops rather than as a replacement. At a specific time epoch, several scalar tracking loop values are extracted and used to initialize the multi-receiver PIA tracking loop. Since the multi-receiver PIA vector tracking is loosely dependent on these initial values, we choose to initialize our tracking loop after the scalar loop has gained a strong fix on the signal.

After initialization, the multi-receiver PIA vector tracking loop generates early, late, and prompt code replicas with the NCO for each of the receivers using LOS projections from receivers to the satellites. The satellite ephemeris is assumed to be known from the scalar initialization of the tracking loop, which is then used to generate a satellite constellation at a specific time epoch. Using the geometry and change in geometry of the satellites to receivers, we can predict the Doppler and phase terms for the NCO. The code replicas are then used to create correlations with the signal from the GPS front ends, which are then used generate the code and carrier discriminators. The discriminators from each channel contain the code and carrier errors, which are then projected onto the LOS vectors and used to generate the Kalman filter measurement matrix. The Kalman filter then estimates the new navigation solution and creates a prediction for the next time epoch, and since we know the true positions of the GPS receivers, we correct the prediction and create a closed feedback loop using the corrected predictions.

While the basic idea behind the multi-receiver PIA vector tracking algorithm is similar to the single-receiver version, there are a few key differences which we will now discuss. The first major difference is the structure of the state transition matrix in the Kalman filter, and the second major difference is the receiver clock estimation. For single receiver vector tracking, the states of the Kalman filter were chosen to be the ECEF position, ECEF velocity, clock bias, and clock drift. For multiple receivers that are connected to a common clock, the states become $N\times$ECEF position, $N\times$ECEF velocity, clock bias, and clock drift, where N is the number of receivers in the receiver-clock network. The receiver elements of the state transition matrix are then given by:

$$A_{i,k} = \begin{bmatrix} 1 & 0 & 0 & \Delta T & 0 & 0 \\ 0 & 1 & 0 & 0 & \Delta T & 0 \\ 0 & 0 & 1 & 0 & 0 & \Delta T \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.1}$$

$$\begin{bmatrix} x_{i,k} \\ y_{i,k} \\ z_{i,k} \\ v_{x,i,k} \\ v_{y,i,k} \\ v_{z,i,k} \end{bmatrix} \tag{4.2}$$

where i indicates the different receivers, ΔT is the time step between update cycles, and k represents the kth epoch. For each receiver's A_i, the next predicted positions are given by a linear combination of the previous position and velocity. Since the receivers in the network are stationary and the time step between update cycles is relatively short, the velocity can be modeled as a constant. Then the state transition matrix when $N = 4$ is given by:

$$F_k = \begin{bmatrix} A_{1,k} & 0 & 0 & 0 & 0 & 0 \\ 0 & A_{2,k} & 0 & 0 & 0 & 0 \\ 0 & 0 & A_{3,k} & 0 & 0 & 0 \\ 0 & 0 & 0 & A_{4,k} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \Delta T \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.3}$$

$$\begin{bmatrix} X_{1,k} \\ X_{2,k} \\ X_{3,k} \\ X_{4,k} \\ t_b \\ t_d \end{bmatrix} \tag{4.4}$$

Then the discrete process equation can be written as:

$$X_{k+1} = F_{k+1}X_k + W_k \tag{4.5}$$

where W_k is the process noise matrix.

The key concept behind the multi-receiver PIA vector tracking is that by leveraging the known positions and velocities of the receivers, we can better predict the terms in our tracking loop. In order to obtain the known locations, we can either utilize external ground truth mechanisms or simply average GPS navigation solutions over an extended period. Once the true positions and velocities of each of the receivers are known, we can correct our Kalman filter position and velocity estimates.

While the clock bias and clock drift in the above equations are modeled as common terms for all receivers, there is always slight clock difference between receivers. Even though we use a single common clock to synchronize the receivers, due to differences in cable length, connector delays, and internal receiver clocks, the clock solutions for each of the receivers will be slightly different. In order to use the common clock model, we manually tune each receiver's clock bias by a certain constant offset:

$$t_{b,i,k} = t^*_{b,i,k} + a_i \tag{4.6}$$

where t^* is the uncorrected clock term and a_i is the clock correction term which can be obtained through extended observation of clock differences in scalar tracking.

4.4 Experimental Setup and Results

In field experiments, the goal is to emulate real world scenarios as closely as possible. Given that the majority of networked PMUs are located within power system substations, we chose our hardware such that the results collected would be applicable to every substation with access to the open sky.

To evaluate the effectiveness of the countermeasure presented in this thesis, we deployed four USRPs connected to a common chip-scale atomic clock (CSAC) as shown in Figure 4.4. Each USRP is connected to an active GNSS antenna powered by onboard 3.3V bias tees. As mentioned previously, the majority of power system substations are not very large, around 20 m by 20 m. Since we want our receiver-clock network to be contained within the confines of the substation, but not so close that the errors are correlated, we chose to separate the antennas using 10 m long coaxial cables (Figure 4.5).

The purpose of the CSAC as the common time source instead of a less stable alternative is two-fold. First, by using the CSAC we can expect the time solutions of our receivers to be very stable, which is essential for reliable PMU measurements. Second, in the event of temporary GPS unavailability the CSAC can potentially be used as a temporary timing source.

There are also several reasons we chose the USRPs instead of an off-the-shelf alternative. First we needed receivers that could output the raw GPS signals rather than post-processed navigation data. Secondly, the receivers needed to accept an external common clock source. And finally, we needed a receiver with flexible bandwidths and center frequency settings. Out of all the receivers we considered, only the USRP N210 fulfilled all of these requirements.

Using the USRPs, we collected GPS signals at 2 MHz sampling frequency. During data collection, the receivers had a clear view of the open sky, up to 8 satellites with clear LOS and good DOP.

After collecting data using our multi-receiver set-up, we processed the signals using the Python SDR using scalar tracking, single-receiver PIA vector tracking, and multi-receiver PIA vector tracking. We then added noise to the GPS signals and simulated several spoofing scenarios to show that our algorithm can be used to mitigate or detect the attack. Even though a couple receivers could acquire up to 8 satellites, we only performed tracking using the 6 satellites acquired by all 4 receivers. Figure 4.6 shows the clock error

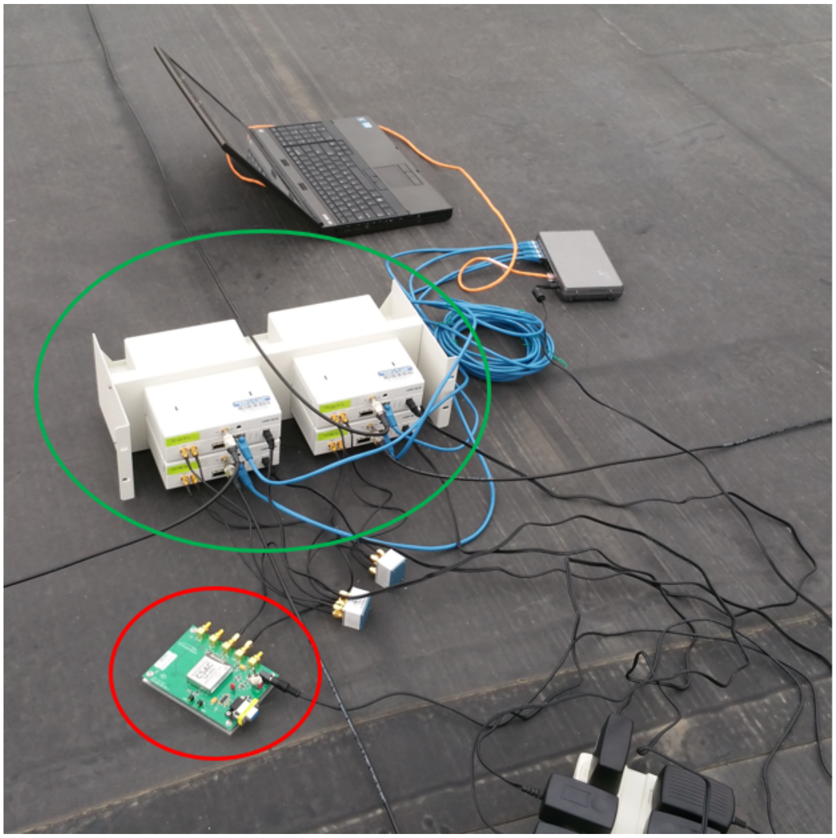

Figure 4.4: Hardware set up. CSAC is shown circled in red and the USRPs circled in green.

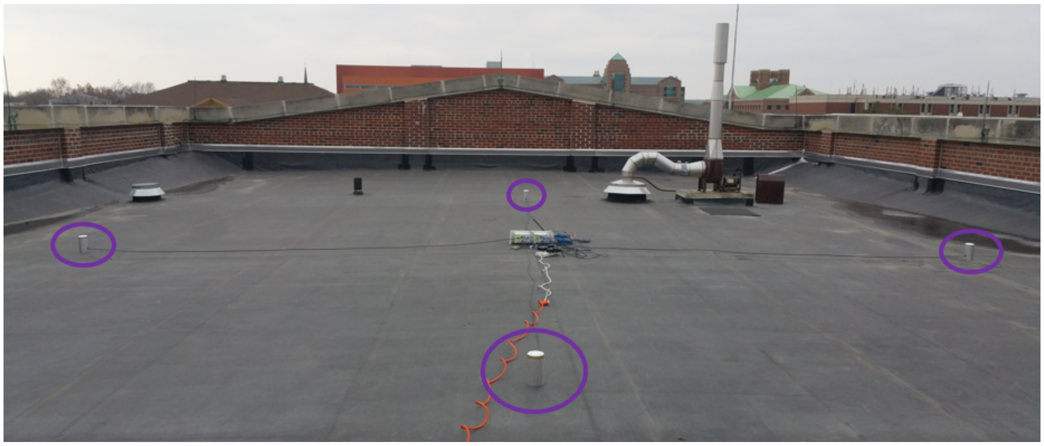

Figure 4.5: The antennas are placed at an approximately 10 m radius.

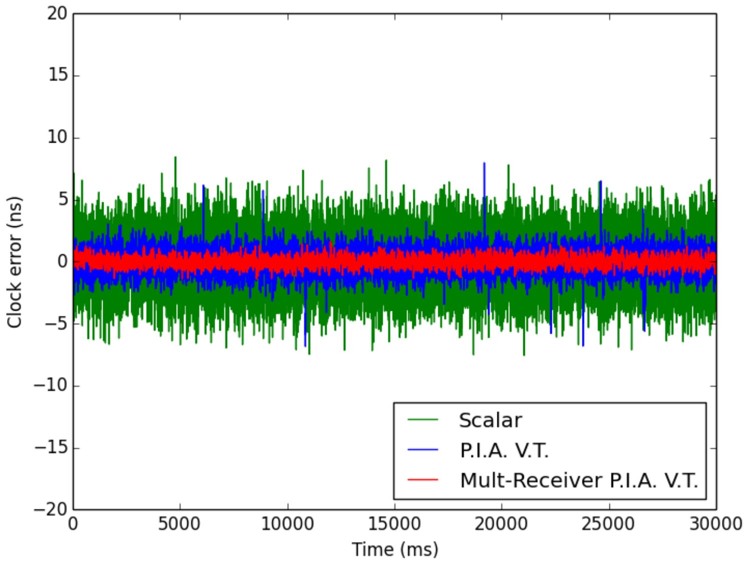

Figure 4.6: Time errors under open sky conditions.

results for scalar, PIA vector tracking, and multi-receiver PIA vector tracking under open sky conditions. From these results, we can see that by leveraging the known position, the PIA vector tracking reduces the clock errors when compared to scalar tracking, and multi-receiver PIA vector tracking again reduces the clock errors even further.

4.4.1 Performance of Anti-Jamming and Noise Tolerance

To determine the anti-jamming and noise tolerance capabilities of the multi-receiver PIA vector tracking algorithm, we added Gaussian noise at 1 dB increments and processed the full dataset using all 3 tracking methods. As the noise increased, each tracking method's clock errors increased with scalar trackings being the most drastic as shown in Figure 4.7.

After the noise was increased past 4 dB, the number of channels that could remain locked during tracking fell below 4, which was consistent with our previous findings using the MATLAB SDR. Single-receiver PIA vector tracking could track the signal until we increased the noise past 8 dB (Figure 4.8), and multi-receiver PIA vector tracking continued operating until we increased the noise past 11 dB. From Figure 4.6 and Figure 4.9, we can see that even at 11 dB of additional noise, the clock error of the multi-receiver PIA vector

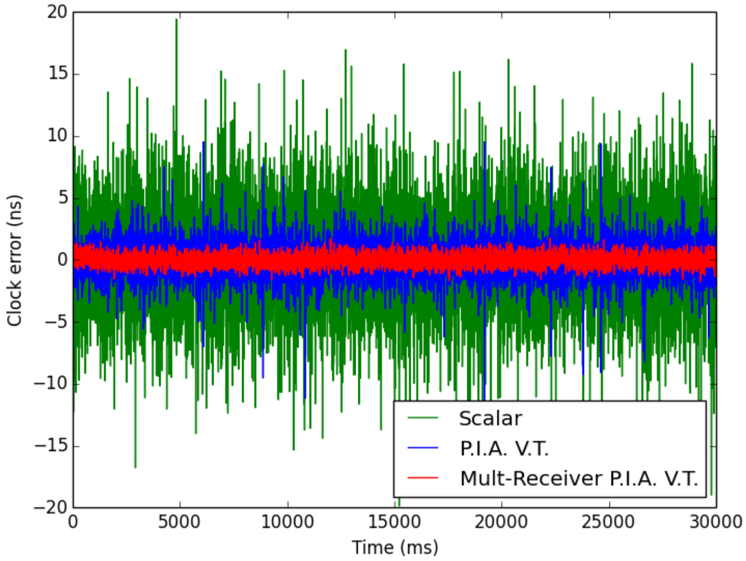

Figure 4.7: Time errors when 4 dB of additional noise is added.

tracking rivaled that of scalar tracking under open sky conditions. Since for every 3dB loss, the signal strength received is roughly halved, we can see that the multi-receiver PIA vector tracking algorithm is very robust against jamming and environmental noise. Table 4.1 lists the peak clock errors for each of the tracking methods as the added noise is increased.

Added Noise and Peak Errors				
Tracking Method	0 dB	4 dB	8 dB	11 dB
Scalar Tracking	7 ns	20 ns		
PIA Vector Tracking	7 ns	10 ns	15 ns	
Multi-Receiver PIA Vector Tracking	1.5 ns	2 ns	3 ns	7 ns

Table 4.1: Peak clock error for each of the tracking methods as the added noise is increased.

4.4.2 Spoofing Attack Simulations

The threat of spoofing attacks is arguably the biggest impediment to the use of PMUs to control the power grid. Fortunately, the vast majority of

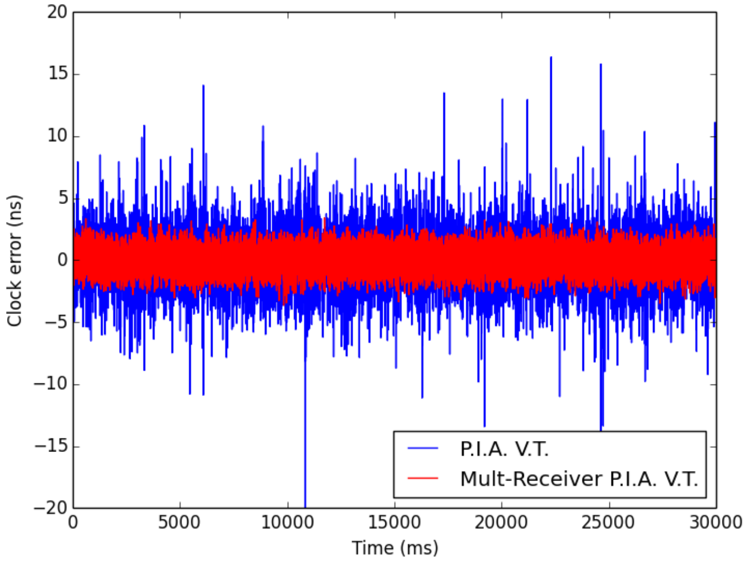

Figure 4.8: Time errors when 8 dB of additional noise is added. Scalar tracking has stopped working.

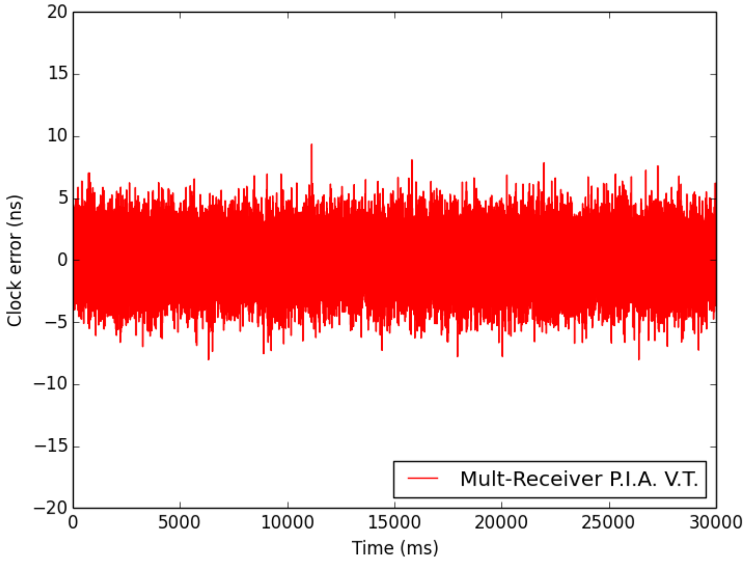

Figure 4.9: Time errors when 11 dB of additional noise is added. Scalar and single-receiver PIA vector tracking have both stopped tracking.

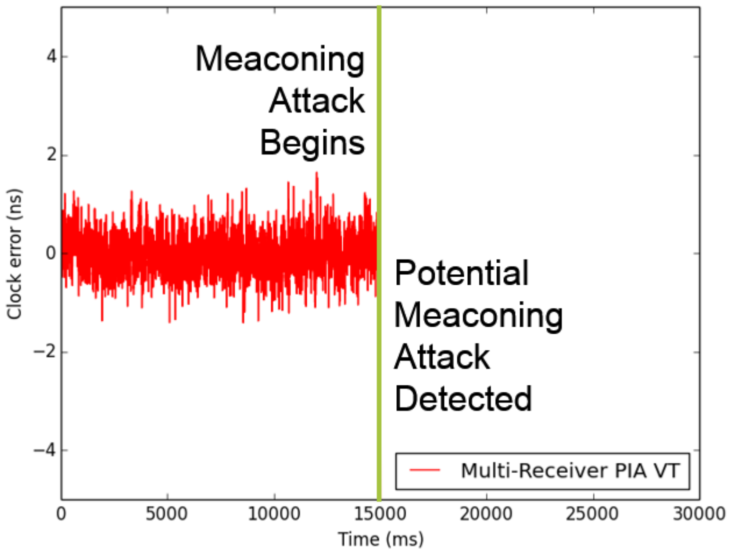

Figure 4.10: Time errors during a simulated meaconing attack with a 100 m separation between the spoofer and the PMU GPS receivers.

possible spoofing attacks have several common elements which the multi-receiver PIA vector tracking architecture is designed to combat. By placing multiple receivers in close proximity (within the 20 m by 20 m area) we can assume that the spoofing signal is either received by all receivers or by none.

During a meaconing attack, legitimate GPS signals are first received by the spoofer and then broadcast towards the victim receivers at a higher power than the signals from the GPS satellites. When this attack is directed at a receiver running a standard scalar tracking algorithm, the victim receiver will calculate the same PVT solution as the attacker with an additional delay, thus causing the receiver to output incorrect timing information. Since the multi-receiver PIA vector tracking algorithm is dependent on the true positions and velocities, the difference between the known position/velocity and the spoofed signals position/velocity causes significant errors, leading to the failure of the multi-receiver PIA vector tracking loop as shown in Figure 4.10. Thus, the meaconing attack can be detected.

As discussed previously, for a data-level spoofing attack, a spoofer could modify the ephemeris parameters of the signals in such a way that the position solution calculated by the victim receivers remains the same but the timing solution would be incorrect. Figure 4.11 shows the results of our data-level spoofing simulation. Once the spoofing attack began, the errors in the Kalman filter quickly accumulated, ultimately resulting in the failure of

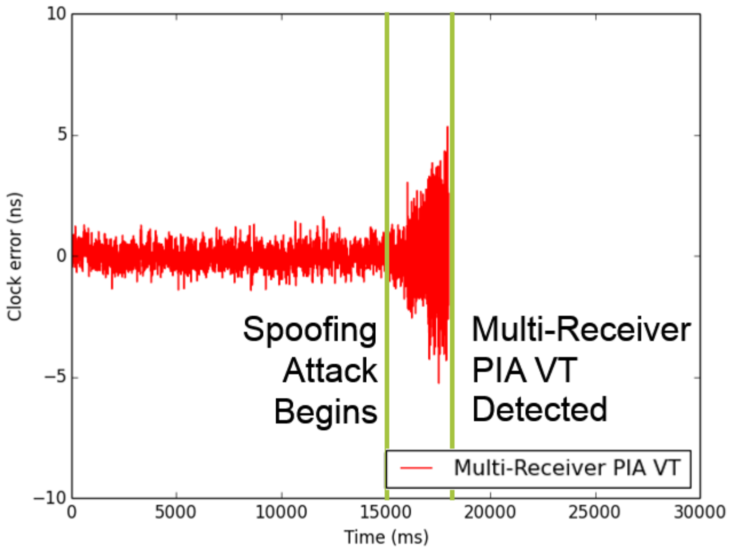

Figure 4.11: Time errors during a simulated data-level spoofing attack.

the multi-receiver PIA vector tracking loop. By simply observing the clock error, we can see that prior to the failure of the tracking loop the clock errors drastically increased from the previous open sky errors. This increase in error can potentially be used as an additional spoofing detection metric.

Therefore our proposed multi-receiver PIA vector tracking algorithm is able to successfully detect meaconing and data-level spoofing attacks.

CHAPTER 5

REAL-TIME DIGITAL SIMULATOR FOR POWER SYSTEMS

This chapter will discuss the tests that we performed with the real-time digital simulator, the results of the tests, and the implications of the results.

5.1 Testing Environment

A power grid is comprised of thousands of power generators, transmission lines, and distribution centers. Power generators are often interconnected for improved reliability and economic benefits. By interconnecting power suppliers, energy can be purchased from multiple sources and customers can draw power from generators in different regions in order to ensure reliable power. For example, one region may be producing cheap hydro power during high water seasons, but in low water seasons, another area may be producing cheaper power through wind, allowing both regions to access cheaper energy sources from one another during different times of the year. Neighboring generators help others to maintain the overall system frequency and also help manage tie transfers between generator regions.

In order to demonstrate the impacts of a spoofed GPS signal on a PMU we chose to use Kundur's four-machine two-area power system case. The basic structure of the case is shown in Figure 5.1 and the system contains 11 buses, four generators, and two areas. Kundur's case is commonly used in power simulations for studies on dynamic stability, power interexchange, and oscillation damping. In this case, we simplify our problem into two areas with four generators and two loads. The ideal case for this system is when each area's generator generates just enough power to supply its respective load, thus eliminating transmission losses. Over-generation of power is also undesirable as it leads to economic losses. Therefore, in order to ensure reliable power supply for the two areas, we interconnect them so that the

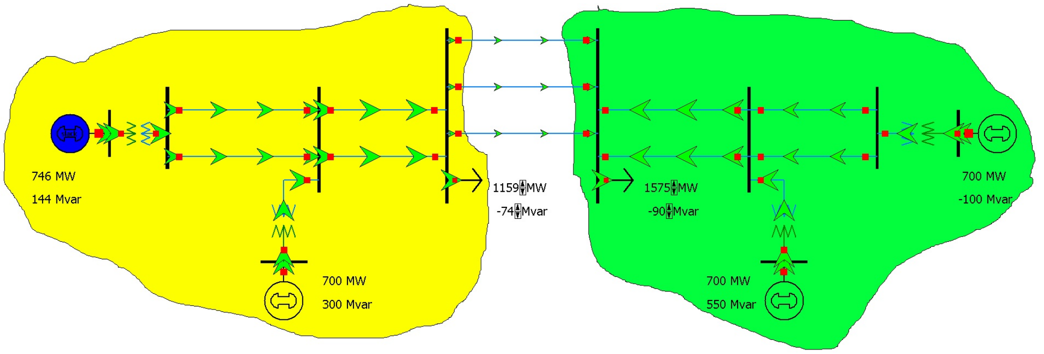

Figure 5.1: Two-area Kundur power system case.

generation responsibility is distributed among the four generators.

However, in order to ensure interconnected compatibility between two areas, the phase angle difference between them must not exceed a certain regulatory amount. This value is closely monitored by power system controllers and incorrect or falsified values could lead to disastrous results.

5.2 Equipment and Software Setup

The hardware used to implement this test consisted the RTDS shown previously in Figure 2.3, a function generator, a GPS receiver, and a physical PMU; the equipment was then connected as shown in Figure 5.2. The equipment was connected in this way ensure that under the unspoofed scenario, both the physical and virtual PMU (generated by the RTDS) would be synchronized to the same timing signal.

The RTDS test case was implemented using RSCAD shown in Figure 5.3. Figure 5.3 sections different blocks in the RSCAD test case together in a more intuitive manner. Each blue block represents a generator with its respective power stabilizers, excitation systems, and governors. The brown blocks represent short transmission lines designed to provide power to the load contained by the red blocks. The loads in this case could represent two cities separated by some distance which are then connected by transmission lines in the green block. We also inserted a fault scenario, where one of the loads could be shorted to ground - which would be equivalent to having a city-wide blackout. In this test case, we set up the virtual and physical PMUs to collect measurements at the load (cities) of each of the two areas.

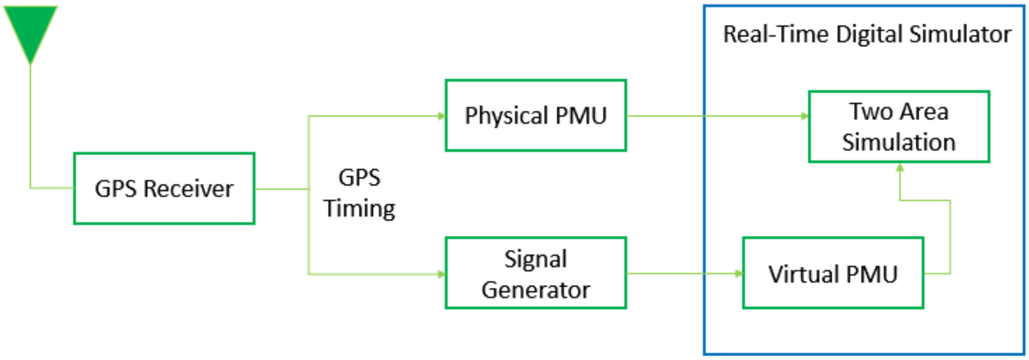

Figure 5.2: Equipment physical set-up. The timing solution from the GPS receiver is used as an input to the physical PMU and the signal generator. The signal generator then generates a synchronized timing signal which is fed into the virtual PMU. The two PMUs are then used to measure the phasor elements of the two areas.

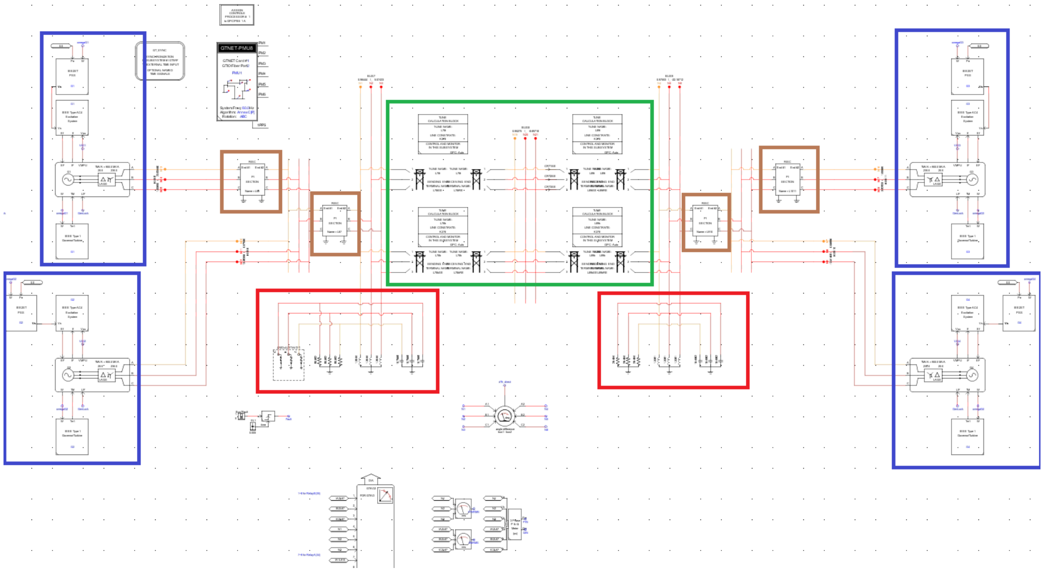

Figure 5.3: Kundur's four-machine two-area case implemented in RSCAD. Each blue block represents a generator with its respective power stabilizers, excitation systems, and governors. The brown blocks represent short transmission lines designed to provide power to the load contained by the red blocks. The loads in this case could represent two cities separated by some distance which are then connected by transmission lines in the green block.

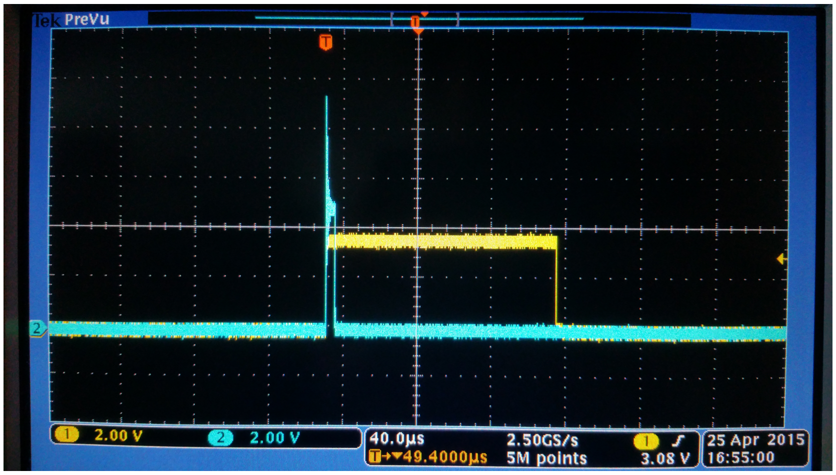

Figure 5.4: Synchronized timing pulses. The blue signal is the timing signal from the GPS receiver and the yellow is the synchronized timing pulse generated by the signal generator. Time-scale is 40 μs.

5.3 Experimental Results

The purpose of this experiment is to demonstrate how a spoofed PMU could be used to lead a control system to falsely assume that another area is out of sync, which could lead to unnecessary overcompensation from one or more of the generators, causing grid instability. In order to show this, we produced slightly unsynchronized clock solutions and fed the value into the virtual PMU and observed the system response over the span of several minutes.

In the unspoofed case, the timing signals for the two PMUs are shown in Figure 5.4, and Figure 5.5 shows an enlarged version of the same signals. Since the times noted by the PMUs are generated based on the rising edge of the pulse signal, both signals produce the same timing solution. In both cases, we trigger the fault scenario to determine the response of the system.

In order to simulate a spoofing attack, we slowly unsynchronize the timing signals as shown in Figures 5.6, 5.7, and 5.8. The final difference in the two timing signals was roughly 4 ms.

After running the tests for both the spoofed and unspoofed case, we then analyzed the data collected by the two PMUs. This section presents the plots for the voltage magnitude, voltage phase, and phase difference between the two PMUs.

Figure 5.9 shows the voltage response in the system under standard operating conditions (without GPS spoofing) and Figure 5.10 enlarges the system

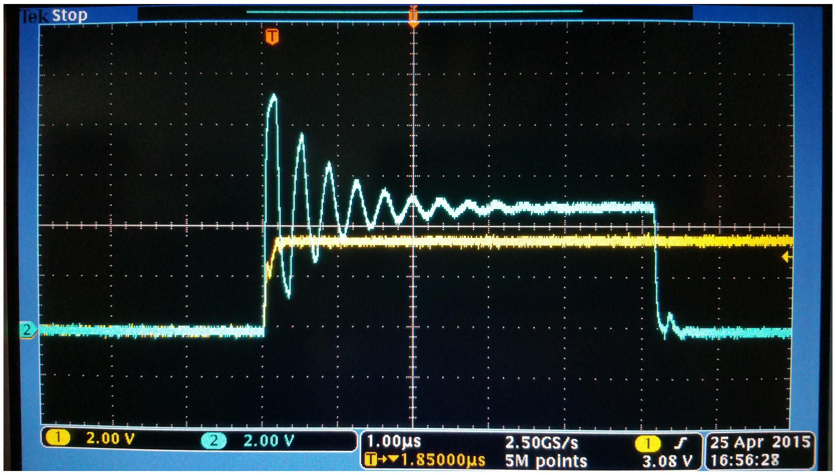

Figure 5.5: An expanded view of the timing pulses. Time-scale is 1 μs.

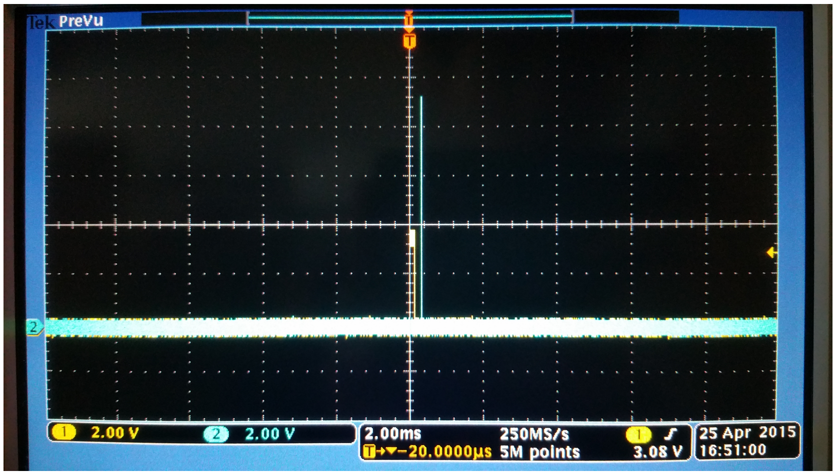

Figure 5.6: Simulated spoofing attack resulting in unsynchronized timing signals. Time-scale is 2 ms.

response to the triggering of the fault scenario. From these two figures, we can see that the system quickly recovers back into steady state in the span of a couple seconds.

Figure 5.11 shows the voltage phase response of the two PMUs and Figure 5.12 shows the phase difference between the two PMUs. The information contained in Figure 5.12 is what we are mainly interested in since the phase difference between the two areas is crucial for maintaining generator synchronization. From this figure, we can see that even when the fault scenario is triggered, the phase difference between the two PMUs never exceeds ± 4 degrees.

For the spoofed case, we repeated the test while using the spoofed timing

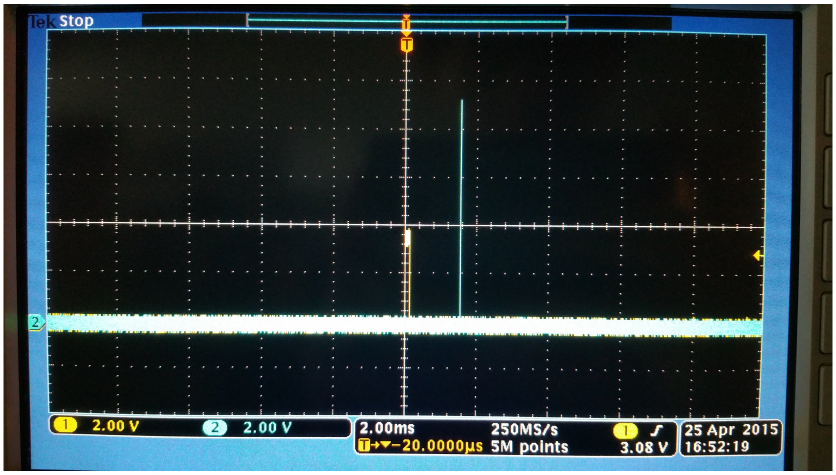

Figure 5.7: The timing signals are moved further apart. Time-scale is 2 ms.

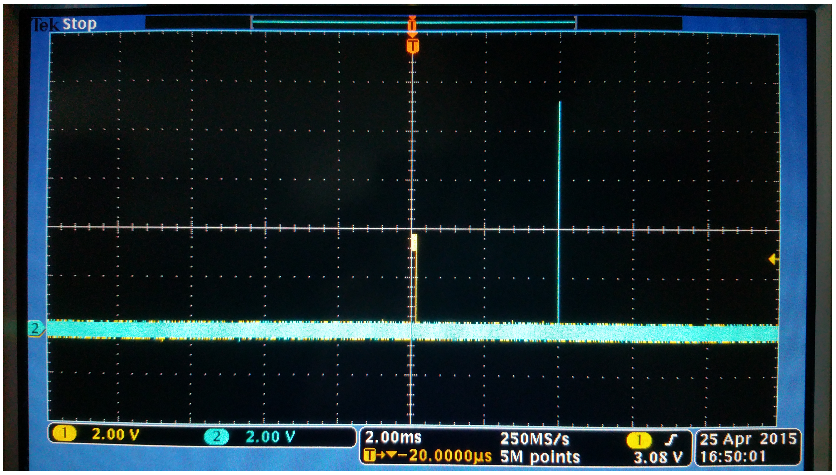

Figure 5.8: There is a 4 ms discrepancy between the real and simulated timing signals. Time-scale is 2 ms.

in the virtual PMU. Figure 5.13 and Figure 5.14 show the voltage magnitude and phase of the two PMUs. Over the 8 minute time-span of the experiment, we were able to bring the phase difference (shown in Figure 5.15) between the two PMUs up to 140 degrees. We can also see in this figure that the impact of the fault is magnified by the phase difference. If only a small phase difference is needed, an attacker could potentially increase the perceived phase difference between the two PMUs a certain amount and then initiate a fault in the grid causing severe fluctuations in the phase difference measurements.

As the demand for energy grows, PMUs will be increasingly used for control purposes to reduce stability margins and increase distribution capabilities. The most basic PMU control simply checks the difference between the phase

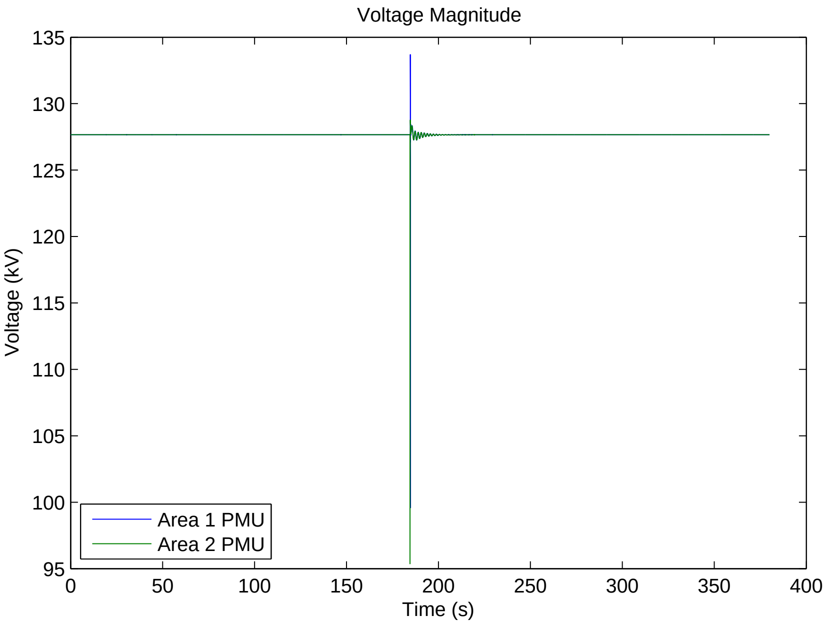

Figure 5.9: Voltage magnitude of the unspoofed case. The fault causes the magnitude to briefly drop down to 95 kV but the system quickly returns to steady-state.

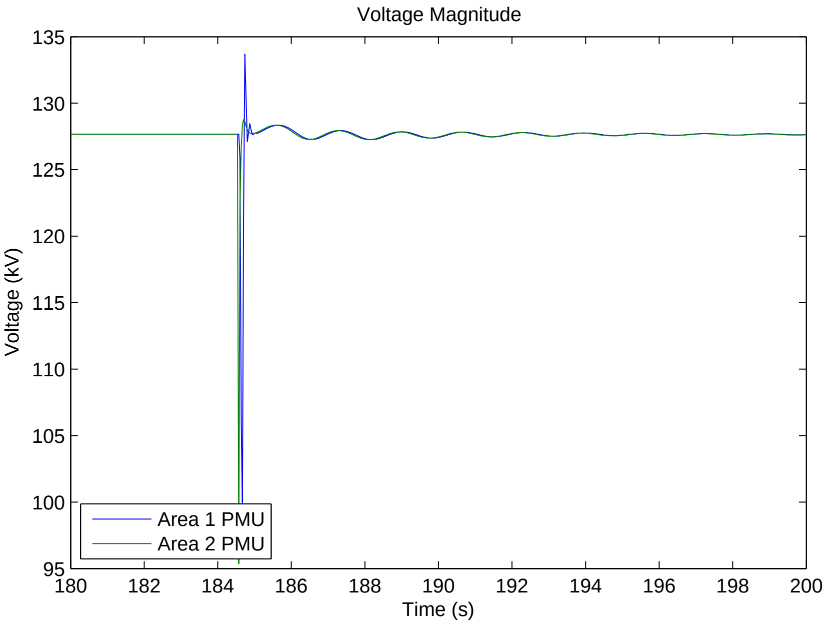

Figure 5.10: An enlarged view of the fault response in the voltage magnitude.

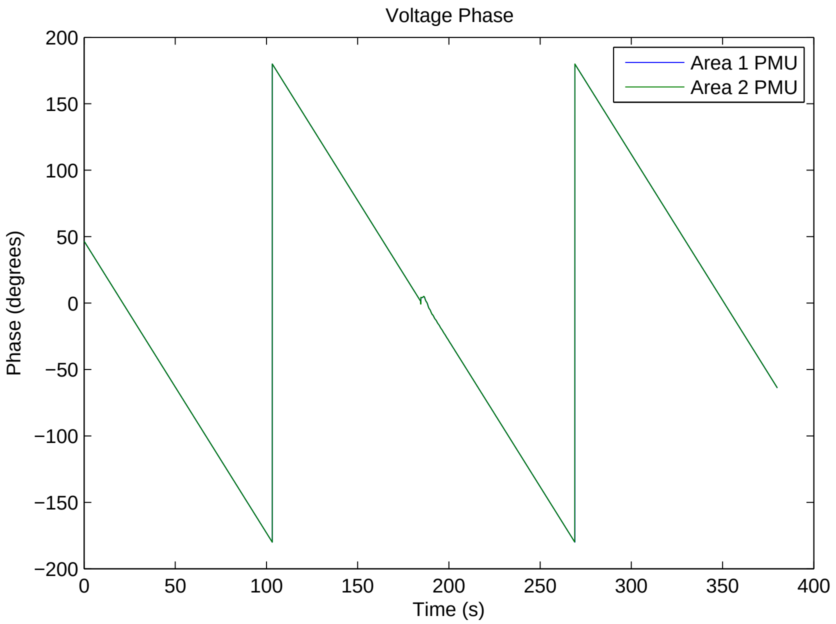

Figure 5.11: Voltage phase of the unspoofed case. The two areas are well synchronized.

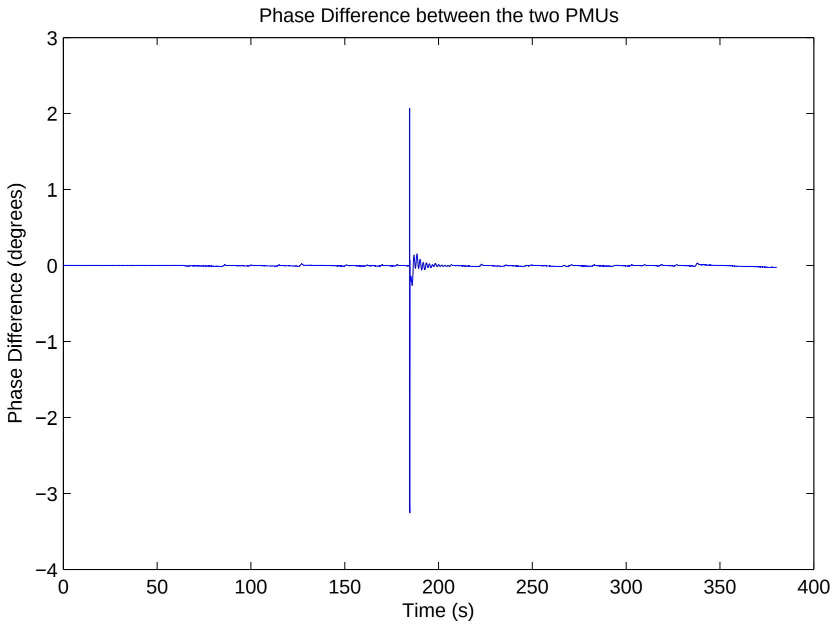

Figure 5.12: Phase difference during the unspoofed case. The fault causes a phase difference of ±4 degrees.

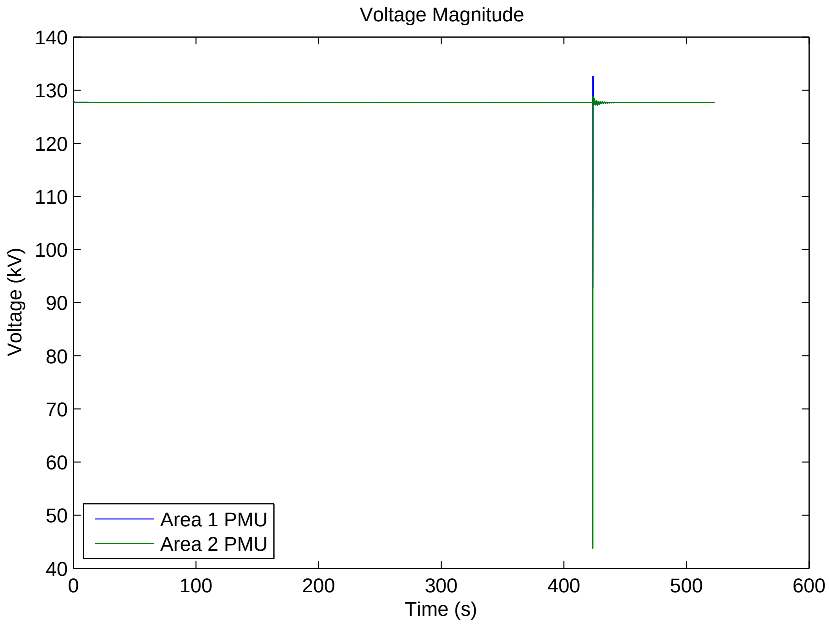

Figure 5.13: Voltage magnitude of the spoofed case. The fault causes the magnitude to briefly drop down to 40 kV which is significantly more drastic than the unspoofed case.

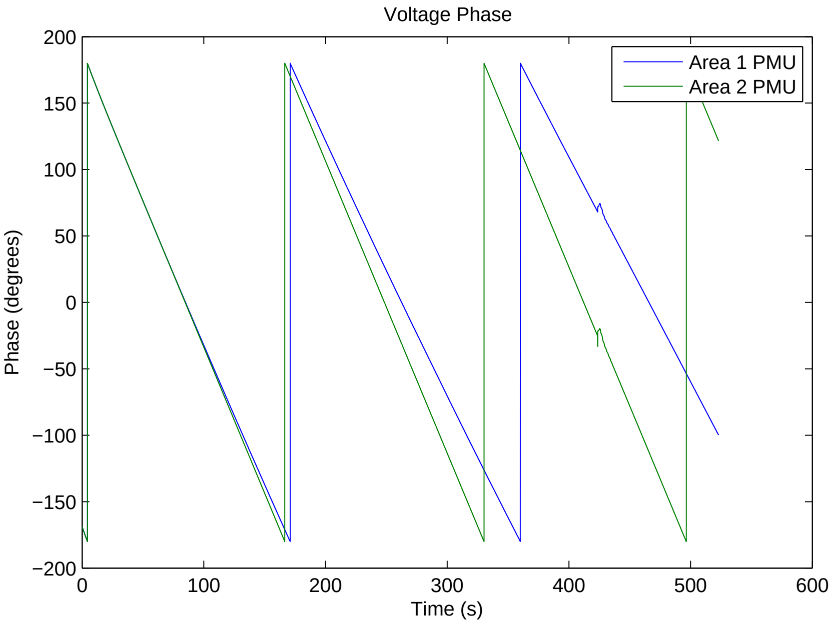

Figure 5.14: Voltage phase of the spoofed case. We can see the two areas slowly becoming increasingly unsynchronized.

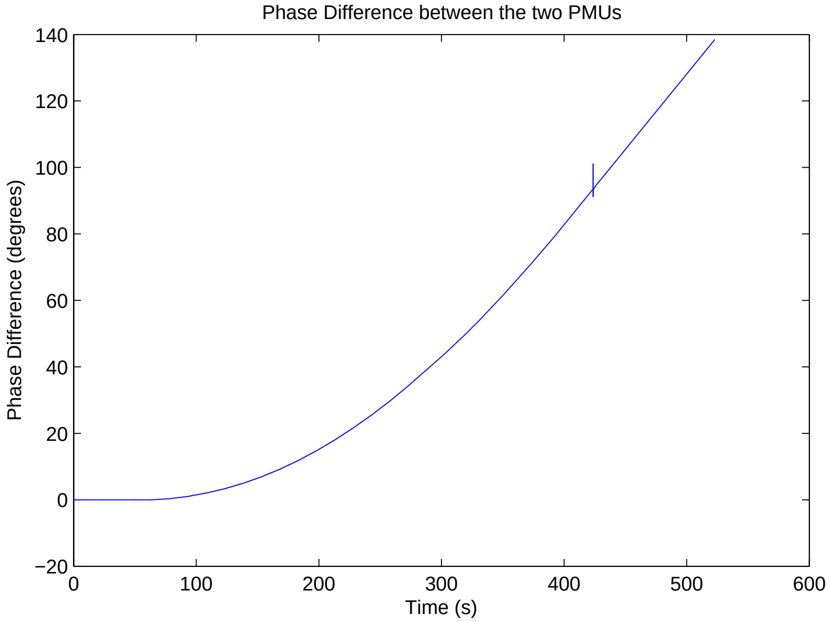

Figure 5.15: Phase difference during the spoofed case. The phase difference drastically increases the longer the spoofing attack is in place.

angles of two PMUs. If the phase angle difference exceeds a certain value, the respective generators will be tripped to prevent grid instabilities.

From the results shown in this chapter, we can see how disastrous a spoofed timing signal can be on the power grid. If the PMUs in the network were used as feedback sensors in a generator control system, an attacker could lead the generator to believe that the system was unstable; and the generator, in the process of adjusting its outputs, could be tripped. If properly planned, several tripped generators have the potential to cause severe grid instabilities, leading to wide-area cascading blackouts.

CHAPTER 6

CONCLUSION

Security and reliability of PMU measurements are vital to the development of power systems. Currently, PMUs are mainly used for grid monitoring. As PMU usage continues to grow, automatic grid control via PMU measurements will become increasingly common. In order to ensure the integrity of GPS-based timing for PMUs, we proposed and implemented the PIA and multi-receiver PIA vector tracking loops. We have discussed the underlying concepts, modeled and implemented the proposed tracking loops in a software-defined-receiver, and conducted field experiments to evaluate the performance of the algorithms.

The field experiments showed that by utilizing the static nature of the GPS receivers used in PMUs, we are able to reduce the search space of the vector tracking loops and improve the accuracy of time solutions generated by the static receivers. We have demonstrated that the PIA and multi-receiver PIA vector tracking loops improve the robustness against interference and jamming, have the ability to detect various spoofing attacks, and also increase the accuracy of the timing solutions.

We also conducted several experiments using the RTDS and found that by attacking a PMU's timing source, we could induce significant phase difference between two PMUs' measurements. Since phase difference between two areas is often used as an indication of fault or potential instabilities, an attacker could lead the system to believe that its current power generation is either insufficient or saturated; and in the process of correcting for the believed deficiency, the system could trip the generators or activate other unnecessary protection mechanisms. If the GPS timing used in the PMUs were generated utilizing our proposed tracking algorithms, the timing solutions could be protected from the spoofing attack.

REFERENCES

[1] Office of the Press Secretary, "Presidential policy directive – critical infrastructure security and resilience," https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, February 2012.

[2] B. Naduvathuparambil, M. C. Valenti, and A. Feliachi, "Communication delays in wide area measurement systems," in *Proceedings of the Thirty-Fourth Southeastern Symposium on System Theory*, 2002.

[3] D. Hart, "Use of SCADA data for failure detection in wind turbines," in *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, July 2008.

[4] H. Bentarzi, "Improving monitoring, control and protection of power grid using wide area synchro-phasor measurements," in *Proceedings of the 12th WSEAS international conference on Automatic control, modelling & simulation.* World Scientific and Engineering Academy and Society (WSEAS), 2010, pp. 93–98.

[5] United States Energy Information Administration, "Today in energy," http://www.eia.gov/todayinenergy/detail.cfm?id=5630, March 2012.

[6] A. Phadke, B. Pickett, M. Adamiak, M. Begovic, G. Benmouyal, R. Burnett Jr, T. Cease, J. Goossens, D. Hansen, M. Kezunovic et al., "Synchronized sampling and phasor measurements for relaying and control," *Power Delivery, IEEE Transactions on*, vol. 9, no. 1, pp. 442–452, 1994.

[7] A. Silverstein, "An update on synchrophasor tech across America," *Intelligent Utility Magazine*, November 2014.

[8] M. Patel, S. Aivaliotis, E. Ellen et al., "Real-time application of synchrophasors for improving reliability," NERC Report, October 2010.

[9] A. G. Phadke and J. S. Thorp, *Synchronized phasor measurements and their applications.* Springer Science & Business Media, 2008.

[10] J. Giri, D. Sun, and R. Avila-Rosales, "Wanted: A more intelligent grid," *Power and Energy Magazine, IEEE*, vol. 7, no. 2, pp. 34–40, 2009.

[11] B. Liscouski and W. Elliot, "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations," US Department of Energy, Tech. Rep. 4, 2004.

[12] G. Wing, *Interface Specification IS-GPS-200E*, June 2010.

[13] J. Warburton and C. Tedeschi, "GPS Privacy Jammers and RFI at Newark: Navigation Team AJP-Results," in *12th International GBAS Working Group Meeting (I-GWG-12), Atlantic City, New Jersey*, November 2011.

[14] C. Tedeschi, "The Newark Liberty International Airport (EWR) GBAS Experience," in *12th International GBAS Working Group Meeting (I-GWG-12), Atlantic City, New Jersey*, November 2011.

[15] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS international technical meeting of the satellite division*, vol. 55, 2008, p. 56.

[16] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, p. 32533262, 2013.

[17] J. S. Warner and R. G. Johnston, "A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing," *Journal of Security Administration*, vol. 25, no. 2, pp. 19–27, 2002.

[18] N. D. Pham, "The economic benefits of commercial GPS use in the US and the costs of potential disruption," NDP Consulting, Tech. Rep., June 2011.

[19] S. Burgett and B. Hokuf, "Experimental Evidence of Wide Area GPS Jamming That Will Result from LightSquareds Proposal to Convert Portions of L Band 1 to High Power Terrestrial Broadband," Garmin International, Tech. Rep., 2011.

[20] GPS.gov, "GPS spectrum and interference issues," http://www.gps.gov/spectrum/, March 2012.

[21] Federal Communications Commission, "Deere submission: LightSquared Interference to GPS and StarFire," May 2011.

[22] R. B. Langley, "GPS, the Ionosphere, and the Solar Maximum," *GPS World*, vol. 11, no. 7, pp. 44–49, 2000.

[23] 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, pp. 146–153, 2012.

[24] L. Heng, J. J. Makela, A. D. Dominguez-Garcia, R. B. Bobba, W. H. Sanders, and G. X. Gao, “Reliable GPS-based timing for power systems: A multi-layered multi-receiver architecture,” in *Power and Energy Conference at Illinois (PECI), 2014*. IEEE, 2014, pp. 1–7.

[25] M. Lashley, D. M. Bevly, and J. Y. Hung, “Performance analysis of vector tracking algorithms for weak GPS signals in high dynamics,” *Selected Topics in Signal Processing, IEEE Journal of*, vol. 3, no. 4, pp. 661–673, 2009.

[26] S. Zhao and D. Akos, “An open source GPS/GNSS vector tracking loop-implementation, filter tuning, and results,” in *Proceedings of the 2011 International Technical Meeting of The Institute of Navigation*, January 2011, pp. 1293–1305.

[27] M. Lashley, D. M. Bevly, and J. Y. Hung, “A valid comparison of vector and scalar tracking loops,” in *Position Location and Navigation Symposium (PLANS), 2010 IEEE/ION*. IEEE, 2010, pp. 464–474.

[28] V. A. Dierendonck, P. Fenton, and T. Ford, “Theory and performance of narrow correlator spacing in a gps receiver,” *Navigation*, vol. 39, no. 3, pp. 265–283, 1992.

[29] B. W. Parkinson and J. J. Spilker, *Progress In Astronautics and Aeronautics: Global Positioning System: Theory and Applications*. AIAA, 1996.

[30] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach (Applied and Numerical Harmonic Analysis)*. Birkhuser, 2007.

[31] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications*, 2nd ed. Artech House Inc, MA, 2006.

[32] L. Heng, “Safe satellite navigation with multiple constellations: global monitoring of GPS and GLONASS signal-in-space anomalies,” Ph.D. dissertation, Stanford University, 2012.

[33] D. Chou, L. Heng, and G. X. Gao, “Robust GPS-Based Timing for Phasor Measurement Units: A Position-Information-Aided Approach,” in *Proceedings of Institute of Navigation GNSS+ 2014 Conference*, September 2014.