ATTACK RESILIENT GPS BASED TIMING FOR PHASOR MEASUREMENT UNITS USING MULTI-RECEIVER DIRECT TIME ESTIMATION

BY

SRIRAMYA BHAMIDIPATI

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Aerospace Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2017

Urbana, Illinois

Adviser:

Assistant Professor Grace Xingxin Gao

ABSTRACT

Modern power distribution systems are incorporating Phasor Measurement Units (PMUs) to measure the instantaneous voltage and current phasors at different nodes in the power grid. These PMUs depend on Global Positioning Systems (GPS) for precise time and synchronization. However, GPS civil signals are vulnerable to external attacks because of its low power and unencrypted signal structure. Therefore, there is a need for the development of attack resilient GPS time transfer techniques to ensure power grid stability.

To counteract these adverse effects, we propose an innovative Multi-Receiver Direct Time Estimation (MR-DTE) algorithm by utilizing the measurements from multiple GPS receivers driven by a common clock. The raw GPS signals from each receiver are processed using a robust signal processing technique known as Direct Time Estimation (DTE). DTE directly correlates the received GPS signal with the corresponding signal replica for each of the pre-generated set of clock states. The optimal set of clock candidates is then determined by maximum likelihood estimation. We further leverage the known geographical diversity of multiple receivers and apply Kalman Filter to obtain robust GPS timing.

We evaluate the improved robustness of our MR-DTE algorithm against external timing attacks based on GPS field experiments. In addition, we design a verification and validation power grid testbed using Real-Time Digital Simulator (RTDS) to demonstrate the impact of jamming, meaconing (i.e., record-and-replay attack) and satellite data-level anomalies on PMUs. Later, we utilize our power grid testbed to validate the attack-resilience of our proposed MR-DTE algorithm in comparison to the existing techniques such as traditional scalar tracking and Position-Information-Aided Vector Tracking.

ACKNOWLEDGMENTS

First and foremost, I would like to express my sincere gratitude to my advisor, Prof. Grace Xingxin Gao, for her continuous encouragement, support, and patience. I would also like to thank Cyber Resilient Energy Delivery Consortium (CREDC) team members at University of Illinois: Alfonso Valdes, Prosper Panumpabi, Jeremy Jones, David Emmerich for helping me in setting up the power grid testbed and also in collecting and analyzing the data. In addition, I would also like to thank all the members of our research group: Derek Chen, Akshay Shetty, Hsi-Ping Chu, Craig Babiarz, Enyu Luo, Matt Peretic, Yuting Ng and Shubhendra Chauhan for the insightful discussions and helping me during various stages of my research work. Finally, I am extremely grateful to my parents and friends for their continued emotional support and words of encouragement.

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

Disclaimer

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Synchronized phasor measurements when incorporated into the real-time control of power grids, will play an important role in maintaining the overall stability of the network power system [1, 2, 3]. Thus, the voltage and current phasor measurements are required to be monitored at high frequency and precision to ensure power grid stability.

Modern power systems deploy Phasor Measurement Units (PMUs) as they provide highly synchronized measurements in regard to the current state of the system [4]. Improving the security of smart grid against cyber attacks has become an important research topic in the power community [5]. In addition to cyber dependency, the operation of PMUs greatly relies on precise time-keeping sources, such as Global Positioning Systems (GPS) signals for timing and synchronization [6].

However, traditional GPS signals are unencrypted and susceptible to external interference [7], either natural or man-made, such as multipath, jamming and spoofing attacks [8]. Therefore, there is a need for the development of robust GPS time transfer techniques to ensure power grid stability.

Most of the timing systems output either a 1-PPS (pulse per second) signal or an IRIG-B (Inter Range Instrumentation Group) time code. 1-PPS signal provides a precise reference timing at the start of every second and an IRIG-B time code provides both time and date information [9]. Phasor measurements are recorded for stability analysis using the corresponding timing signal generated from Coordinated Universal Time (UTC) time obtained from the GPS receivers.

The IEEE C37.118 Standard, “Synchrophasors for Power Systems” is for evaluating the robustness and stability of the power grid setup [10]. This standard evaluates the Total Vector Error (TVE) which can be defined as the vectorial difference between the measured and expected values of the phasor for any measurement at any given instant. The quantity TVE depends on three parameters: magnitude, timing and phase angle. In accordance with the IEEE C37.118 Standard, without any timing and magnitude errors, phase angle error of 0.573° which corresponds to a 1% TVE, is the maximum allowable TVE. This phase angle error is equivalent to a timing error of 26.5 μs which is used as a benchmark in significant number of studies on stability analysis [11, 12].

The hazardous impact of GPS timing attacks has recently gained worldwide attention due to the successful spoofing of an $80 million yacht, demonstrated in [13, 14]. Furthermore, real-time tests have been conducted to demonstrate the vulnerability of PMUs to GPS spoofing attacks [15] and corresponding detection of presence of attacker using antenna arrays [16].

Atomic clock is one of the alternate sources for supplying timing to PMUs essentially due to its high precision and low drifting rate. However, a regular atomic clock is costly and large in size and weight. A more affordable option is to combine GPS with a chip scale atomic clock (CSAC) as implemented in [17]. CSAC provides stable timing with drifting rate less than 30 ns/hr, is light weight and compact in size [18]. However, CSAC combined with GPS can only address jamming attacks which cause low signal-to-noise ratios of satellites or loss of satellite lock. However, during a more sophisticated timing attack such as spoofing, this approach fails to provide required protection.

In addition, an active research area is in developing a low-cost record and replay prototype using Universal Software Radio Peripheral (USRP) for use in academia as an experiment platform [19, 20]. One of the important aspects of our work involves offline experimental verification and validation of our robust time transfer technique using USRP by introducing emulated timing attacks in the signals transmitted by the device [21].

There have been a variety of algorithms developed to enhance the GPS timing robustness. Previously developed techniques in our group include Position-Information-Aided Vector Tracking (PIAVT), which was proven to be effective in detecting external malicious attacks like jamming, spoofing, etc. [22]. In addition, Multi-Receiver Position-Information-Aided Vector Tracking (MR-PIAVT) was developed and discussed in [23] which improves the robustness of the system by taking into account additional baseline information.

Our current work is an extension of our earlier work on single receiver Direct Time Estimation (DTE), whose ability to detect meaconing attacks at an early stage and greater tolerance for higher noise levels, such as those during a jamming attempt, has been presented and verified in prior publications [24]. We propose a Multi-Receiver Direct Time Estimation (MR-DTE) architecture, as each receiver is affected differently by the timing attacker when deployed at different locations [25]. Therefore, achieving geometric diversity.

1.1 Wide Area Monitoring Systems

The power grid accomplishes the tasks of generation, transmission and distribution of electricity to designated locations through a well established network architecture. The supply and demand of electricity need to be balanced at all times to maintain power grid stability. Nowadays, the nature of power grid infrastructure is undergoing rapid changes, such as switching to renewable sources, utilizing digital technology for grid operations and automating the grid for improved grid resiliency [26].

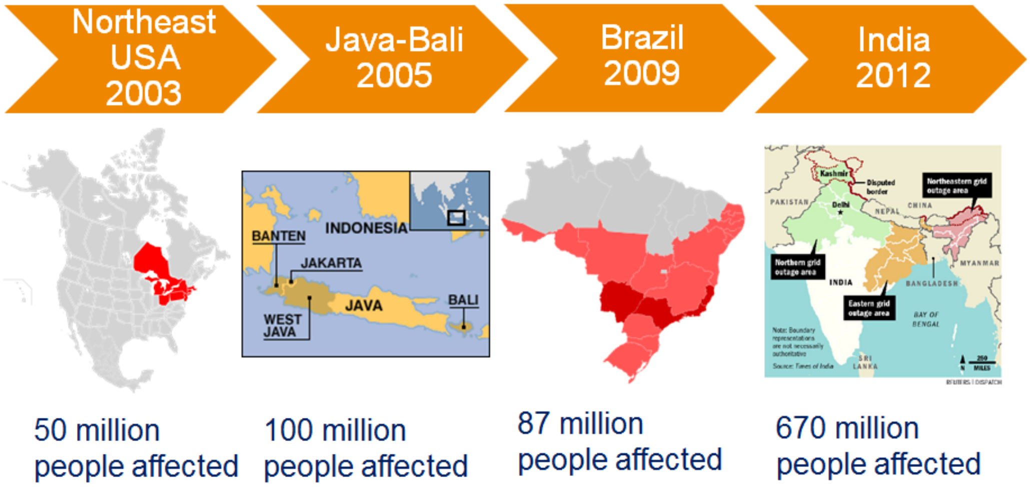


Figure 1.1: Noted power outages in the past that affected millions of people.

The impact of external factors on the stability of power grids may range from small local perturbations to large scale blackouts. Fig. 1.1 describes some of the most noted power outrages in recent history. The first one is the north east USA and Canada blackout that occurred due to a software bug in an Ohio power substation [27]. About 50 million people were affected and the entire region remained in darkness for 2 days. The second one occurred in Indonesia due to a transmission line failure affecting 100 million people [28]. In 2009, another major power black out occurred in Brazil that affected 87 million people [29]. This was due to heavy rains and winds that led to a short-circuit. The power blackout in India during July 2012 affected around 670 million people [30]. The weak interlinking power lines and the increased power demand from some regions resulted in this largest power outrage in the word history. Therefore, we can observe that with time, there is an increase in the population affected by power outages.

In the light of these wide-scale blackouts, Office of Electricity Delivery and Energy Reliability (OE) has come up with a set of goals [31] aiming to improve the reliability and robustness of the future power grid. The set of goals are as follows:

1. Providing synchronized phasor measurements
2. Establishing reliable communication network
3. Monitoring the grid in real-time
4. Automating the power grid control operations
5. Improving the security margins

The focus of this thesis is to obtain synchronized phasor measurements required to establish reliable real-time network monitoring across various nodes in the power grid. The term "phasor" refers to a complex quantity representing the magnitude and phase angle of the voltage and current measurements. Wide Area Monitoring Systems (WAMS) rely on the modern data acquisition technology of phasor measurements to monitor the transmission system conditions at various crucial nodes across the grid [32]. The goal of WAMS is to efficiently detect the system anomalies and take countermeasures to prevent grid instabilities [33].

Currently, the power system functions are regulated using a control system known as Supervisory Control and Data Acquisition (SCADA) [34]. SCADA monitors the phasors across the power grid by polling the measurements once every few seconds for critical systems and once every few minutes for non-critical ones. The state of the power grid is measured through sensors at various nodes of power grid that are later transmitted to a master control station for stability analysis. Due to the lack of a precise time reference and transmission delays, SCADA outputs unsynchronized measurements, thereby increasing the complexity of data analysis and reducing the reliability and robustness of the electricity grid [35].

With the recent development in the technology, advanced devices i.e., PMUs are being employed for grid monitoring as in Fig. 1.2. PMUs were invented in 1988 by Dr. Arun G. Phadke and Dr. James S. Thorp at Virginia Tech [36]. PMUs are capable of polling up to 60 observations per second. WAMS depends on synchronized phasor measurements from distributed PMUs. These precise phasor measurements are required for high-resolution grid state estimation and potential early-stage detection of destabilizing conditions [37]. PMUs are critical for providing quick response to emergencies, preventing disturbance propagation across grid, limiting the possibility of load shedding and improving the system restoration time in the event of an instability.

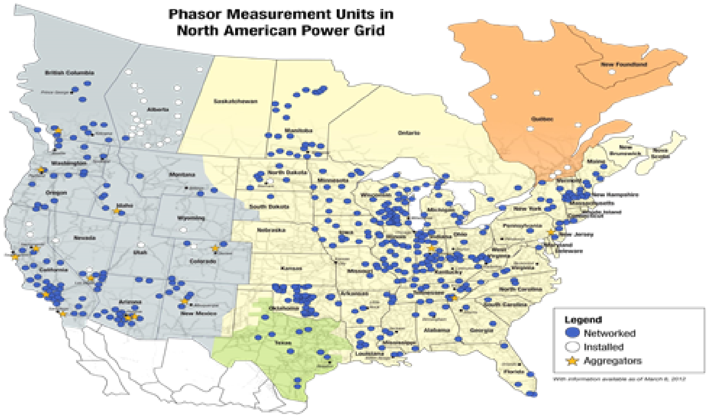


Figure 1.2: Map showing the widespread distribution of PMUs across US.

Due to the high sampling frequency, the PMUs are capable of providing the control monitoring stations with measurements at subsecond time frame. The precise PMU measurements are thereby used for real-time state estimation and control operations required to analyze the stability of the power system. Fig. 1.3 shows the performance comparison of PMU and SCADA devices in the event of voltage disturbance in a power grid in Oklahoma that occurred on April 5, 2011 [38]. We observe that the PMU provides high precision measurements and detects the anomaly approximately 30 *s* prior to the SCADA systems.

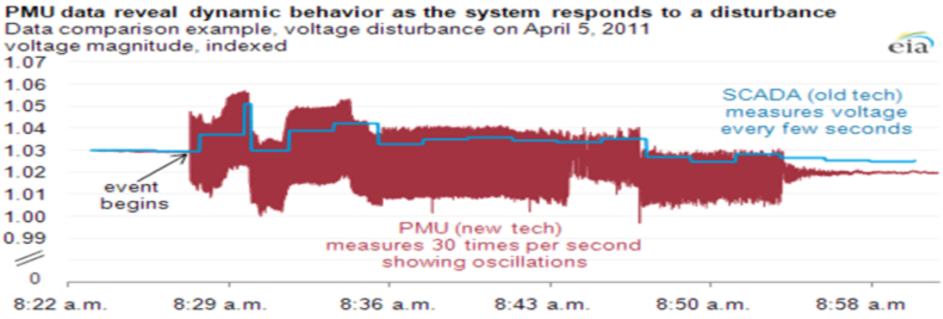


Figure 1.3: PMU measurements are denoted by the red line while the SCADA measurements are denoted by the blue line. In the event of voltage disturbance, PMU detects anomaly approximately 30 *s* prior to SCADA.

PMUs measure current, voltage, frequency and phase angle measurements at certain given nodes in the power system which are recorded in a data concentrator at an interval of 100 *ms*. The dynamic state of critical and non-critical nodes in transmission and distribution networks is monitored by comparing the PMU measurement data across the grid. Therefore, a closed loop dynamic monitoring of critical nodes in power systems is achieved in near future using these high precision devices.

1.2 GPS timing for PMUs

Given that the power community is transitioning to an automated smart grid in future, synchronized phasor measurements from PMU are extremely essential for automated control and stability monitoring. In typical applications, phasor measurement units are sampled from widely dispersed locations in the power system network and synchronized from the common time source of a GPS radio clock. Table 1.1 compares the advantages and disadvantages of using GPS for obtaining precise measurements. GPS provides up to μs-level accurate timing and is free to all users. In addition, GPS constellation has global coverage, which enables network-wide stability monitoring of the grid.

Table 1.1: Characteristics of GPS.

Advantages	**Disadvantages**
Global coverage	Un-encrypted signal structure
Freely available	Low signal power
$\mu s-$level accurate time	Vulnerable to attacks

On the other hand, given the unencrypted nature and low signal power, GPS signals are vulnerable to external interference either natural or man-made. The susceptibility of GPS signals to jamming and spoofing leads to potential vulnerabilities in WAMS [39, 40].

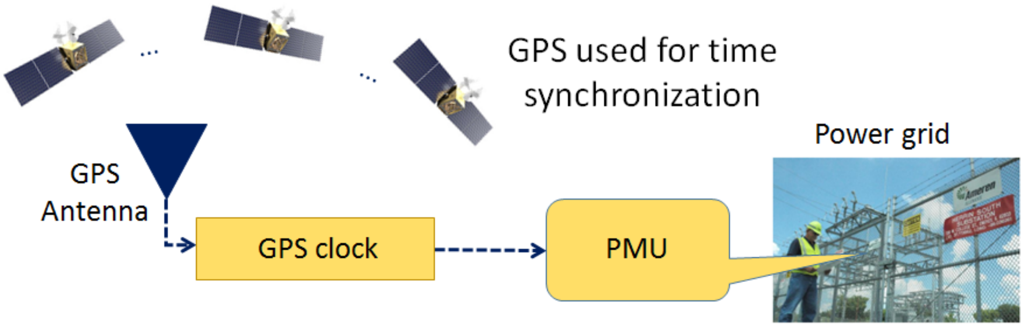
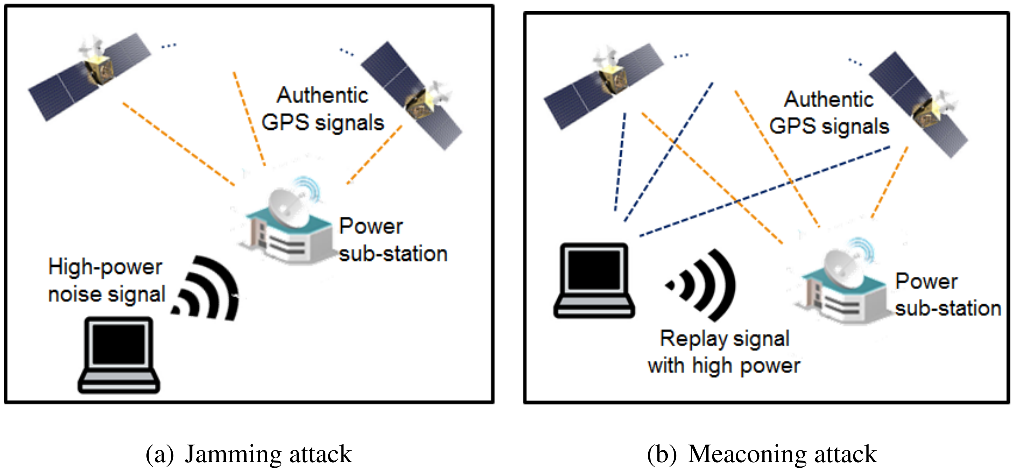


Figure 1.4: GPS timing in PMUs.

1.3 GPS timing attacks and error sources

We classified the sources of GPS threats and errors that affect the accuracy and reliability as follows: atmosphere (ionosphere and troposphere), user clock errors, satellite clock bias errors, number of satellites, satellite geometry, multipath and non-line of sight signals, intentional/unintentional GPS transmission anomalies, intentional degradation of the satellite signal (such as spoofing, jamming) etc.. Due to the vulnerabilities of the GPS signals explained in Section 1.2, our current focus is on jamming, spoofing attacks, satellite broadcast data anomalies and unwanted external interference.



(a) Jamming attack

(b) Meaconing attack

Figure 1.5: Types of timing attacks that affect the robustness; (a) broadcast high power noise signals in $L1$ frequency range; (b) record-and-replay of high power spurious GPS signals.

1.3.1 Jamming

Jamming is one of the most common mode of GPS timing attack that involves broadcasting a high-power noise signal in the GPS frequency band as in Fig. 1.5(a). Jamming causes the GPS receiver to lose track of the signal acquired [41, 42], and ultimately makes the timing information unavailable for the PMUs.

1.3.2 Spoofing

In spoofing, spurious counterfeit GPS signals are transmitted with high power so as to manipulate the GPS receiver with wrong data as shown in Fig. 1.5(b). In our work, we focus on a type of spoofing attack known as meaconing, or record and replay attack. The standard meaconing attack involves collecting the GPS signals at a different place and different time, and replaying them with increased power [43, 44]. However, a sophisticated attack involves collecting the signals at the same place but at a different time. This sophisticated attack deceives the algorithms that implement a position check.

1.3.3 Satellite broadcast data anomalies

According to GPS design specifications: GPS time is automatically steered to UTC on a daily basis by the ground control station to keep system time within one microsecond of UTC time. On a few occasions such as software bugs or wrong calculations, erroneous data have been transmitted by the GPS satellites and affected the GPS position and timing accuracy [45, 46].

1.3.4 Unwanted external interference

The GPS community is actively working to prevent the broadcast of high-powered radio signals in or near $L1$ GPS frequency band [47]. In addition, the other sources of external interferences are due to electromagnetic waves [48], solar flares [49] and certain electronic devices. Since the received GPS signals are of very low power, the presence of these external unwanted disturbances degrades the GPS signal-to-noise ratio (SNR) and deteriorates the accuracy.

1.4 Contribution and outline of this thesis

The contribution of this thesis is in three major aspects:

1. We proposed a novel MR-DTE architecture that utilizes the information from spatially dispersed receiver locations to improve resilience to noise and external timing attacks. MR-DTE is an extension of DTE, a robust signal processing technique that directly operates with timing parameters and performs non-coherent vector correlation across satellites to improve the SNR. In addition, we enhanced the computational efficiency of DTE by incorporating an adaptive covariance based Gaussian search space.

2. We demonstrated the impact of timing attacks and GPS satellite data anomalies on the stability of power grid using Real-Time Digital Simulator (RTDS) based virtual power grid testbed.

3. We validated the increased robustness of our MR-DTE algorithm as compared to scalar tracking, PIAVT and single-receiver DTE (SR-DTE).

The rest of the thesis is organized as follows: Chapter 2 covers the basics of GPS and provides an overview of the existing GPS algorithms, namely scalar tracking and PIAVT. Chapter 3 describes the importance of GPS timing in PMUs and the associated GPS timing attacks and other significant error sources. Chapter 4 describes the underlying concept of our efficient DTE based signal processing technique and our novel MR-DTE architecture. This chapter also provides details in regard to its initialization and Kalman Filter design to account for multiple receivers. Chapter 5 outlines the experimental setup for validating our multi-receiver DTE algorithms. In Chapter 6, we present the impact of GPS satellite data anomaly, jamming and meaconing attacks on stability of the power grid. Chapter 7 validates the increased resilience of our MR-DTE algorithm using both a GPS experimental setup and a virtual power grid testbed. Chapter 8 concludes the thesis and describes the future direction of our research.

CHAPTER 2

BACKGROUND OF GPS

Global Navigation Satellite Systems (GNSS) is an integral part of commercial navigation based applications to estimate the global Position, Velocity and Time (PVT) information at any location on Earth. In this thesis, we utilize the civilian $L1$ signals (carrier frequency of 1575.42 MHz) of the operational GNSS system of the United States known as GPS [50].

GPS has 3 segments: space segment, user segment and control segment. The space segment comprises of 24 to 32 satellites in medium Earth orbit at an altitude of $20,200$ km. GPS satellites are strategically placed in 6 orbital planes, such that a minimum of 4 satellites are available to calculate the navigation solution at any time and location [51]. The control segment consists of a master control station (MCS), an alternate master control station, ground antennas and monitor stations. The user segment includes GPS receivers that utilize the signals broadcast from GPS satellites to calculate their corresponding locations.

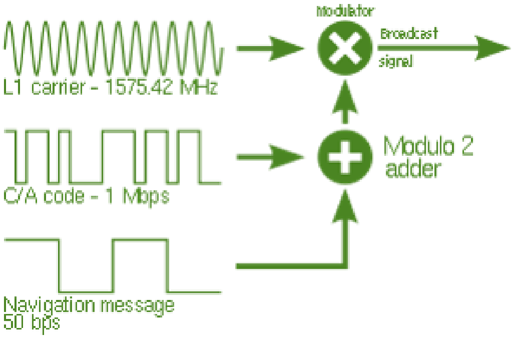


Figure 2.1: GPS signal structure.

GPS satellites broadcast a modulated signal (over a carrier wave) as in Fig. 2.1 which consists of:

1. Pseudorandom code: this is a satellite specific code used to distinguish the individual satellite signals. It is also used for estimating the time of ar-

rival (TOA) of the signal in the receiver time scale. They are unencrypted Coarse/Acquisition (C/A) code which chip rate of 1.023 MHz.

2. Navigation message: this includes the satellite position, satellite clock corrections, UTC corrections, time of transmission (TOT) of the signal, etc. Each GPS satellite continuously broadcasts a navigation message at a rate of 50 $bits/s$.

2.1 Defining the parameters

We consider N satellites in view. The GPS signal replica Y given by Eq. (2.2) can be represented by 4 signal parameters as follows: carrier frequency $f_{carr}^{(i)}$ and carrier phase $\phi_{code}^{(i)}$ which characterizes the underlying Doppler carrier wave; code frequency $f_{code}^{(i)}$ and code phase $\phi_{code}^{(i)}$ which represent the i^{th} satellite specific C/A code. In addition, these GPS parameters are also a function of the 3D position and velocity X, clock parameters T and 3D satellite position and velocity, $S^{(i)}$.

$$\begin{aligned}
X &: \text{Position and velocity of the receiver} \\
&= [x, y, z, \dot{x}, \dot{y}, \dot{z}] \\
T &: \text{Clock states of the receiver} \\
&= [c\delta t, c\delta \dot{t}] \\
S^{(i)} &: \text{Position and velocity of the } i^{th} \text{ satellite} \\
&= [x_s^{(i)}, y_s^{(i)}, z_s^{(i)}, \dot{x}_s^{(i)}, \dot{y}_s^{(i)}, \dot{z}_s^{(i)}]
\end{aligned} \tag{2.1}$$

$$\begin{aligned}
Y &: \text{signal replica of the GPS signal} \\
&= \sum_{i=1}^{N} Y^i \\
Y &: \text{signal replica corresponding to } i^{th} \text{ satellite} \\
Y^i &= D^i(t) G^i(f_{code}^i(t) + \phi_{code}^i) e^{j2\pi(f_{carr}^i(t) + \phi_{carr}^i)}
\end{aligned} \tag{2.2}$$

$$\begin{aligned}
t &: \text{time instant being considered} \\
D^i(t) &: \text{Navigation databit from } i^{th} \text{ satellite} \\
G^i(t) &: \text{L1 C/A code chip from } i^{th} \text{ satellite} \\
f^i_{code} &: \text{Code frequency of the } i^{th} \text{ satellite signal} \\
\phi^i_{code} &: \text{Code phase of the } i^{th} \text{ satellite signal} \\
f^i_{carr} &: \text{Carrier frequency of the } i^{th} \text{ satellite signal} \\
\phi^i_{carr} &: \text{Carrier phase of the } i^{th} \text{ satellite signal}
\end{aligned} \tag{2.3}$$

$$\begin{aligned}
f_{C/A} &: \text{Chiprate of C/A code, } 1.023\ MHz \\
f_{L1} &: \text{Frequency of L1 signal carrier, } 1575.42\ MHz \\
f_{IF} &: \text{Intermediate frequency (IF), } Hz \\
ECI &: \text{Earth-Centered-Inertial}
\end{aligned} \tag{2.4}$$

2.2 Traditional approach

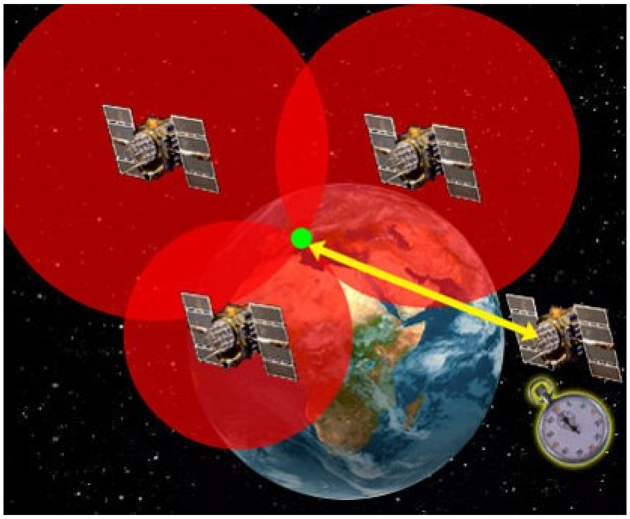


Figure 2.2: GPS Trilateration. Reference image taken from [53].

2.2.1 Trilateration

Commercial GPS receivers rely on a technique known as *trilateration*. In simplest terms, trilateration involves calculating the intersection point of 3 circles given the center and radius as shown in Fig. 2.2. The center of the red circles correspond to the satellite position S^i, the radius corresponds to the distance between the satellite and the receiver ρ^i, and the intersection point is the position of GPS receiver X. The onboard GPS satellite clocks are not synchronized to the GPS receiver clocks, because of which there is an associated 4^{th} unknown parameter known as the clock bias $(c\delta t)$. Therefore, at least 4 satellites are required to estimate the navigation solution.

The pseudo distance known as pseudorange $\rho^{(i)}$ is calculated based on the difference in the transmit time of the signal from the i^{th} satellite and the received time at the GPS receiver represented below.

$$\begin{aligned}
\rho^{(i)} &: \text{Pseudorange corresponding to the } i^{th}\text{satellite} \\
&= c * t^{(i)}_{travel} \\
t^{(i)}_{travel} &: \text{Signal time of flight corresponding to the } i^{th}\text{satellite} \\
&= c(t^{(i)}_{tx} - t_{rx}) \\
t^{(i)}_{tx} &: \text{Transmit time of the signal from } i^{th}\text{satellite} \\
t_{rx} &: \text{Receive time of the signal at the receiver}
\end{aligned}$$

Pseudorange is theoretically estimated by modeling the satellite clock errors, receiver clock bias, atmospheric delays and Gaussian noise as in Eq. (2.5).

$$\rho^{(i)} = \sqrt{((x^{(i)}_s - x)^2 + (y^{(i)}_s - y)^2 + (z^{(i)}_s - z)^2} + c(T_{c\delta t} - T^{(i)}_{c\delta t,s}) + c(T^{(i)}_T + T^{(i)}_I) + \varepsilon^{(i)}, \tag{2.5}$$

where $\varepsilon^{(i)}$ is the Gaussian measurement error, $cT^{(i)}_T$ is the tropospheric error and $cT^{(i)}_I$ is the ionospheric error.

The information related to satellite position, satellite clock corrections $T^{(i)}_{c\delta t,s}$, transmit time of the signal are encoded in the navigation message. The decoding of the navigation message requires the receiver to track the GPS parameters listed in Eq. (2.3). Once the pseudorange, satellite positions, and satellite clock biases are known we implement trilateration using least-squares method to determine the user position and velocity.

Similarly, this can be extended to the velocity domain of the receiver. Here the pseudorate $\dot{\rho}^{(i)}$ is calculated from the Doppler shifts or the time difference in the carrier phase measurements. Finally, a complete navigation solution consisting of 8 (X,T) unknown parameters are estimated with a minimum of 4 satellites in view [52]. These unknowns are estimated using least-squares technique whose equations are formulated by linearizing the Eq. (2.6).

$$\begin{bmatrix} \delta\rho_1 \\ : \\ \delta\rho_j \\ \delta\rho_N \\ \delta\dot{\rho}_1 \\ : \\ \delta\dot{\rho}_j \\ \delta\dot{\rho}_{\dot{N}} \end{bmatrix} = H \begin{bmatrix} \Delta x \\ \Delta y \\ \Delta z \\ \Delta c\delta t \\ \Delta\dot{x} \\ \Delta\dot{y} \\ \Delta\dot{z} \\ \Delta c\delta\dot{t} \end{bmatrix}, \tag{2.6}$$

where geometry matrix is given by

$$H = \begin{bmatrix} los_{x,k}^{(1)} & los_{y,k}^{(1)} & los_{z,k}^{(1)} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & los_{x,k}^{(1)} & los_{y,k}^{(1)} & los_{z,k}^{(1)} & 0 & 1 \\ : & : & : & : & : & : & : & : \\ : & : & : & : & : & : & : & : \\ los_{x,k}^{(N)} & los_{y,k}^{(N)} & los_{z,k}^{(N)} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & los_{x,k}^{(N)} & los_{y,k}^{(N)} & los_{z,k}^{(N)} & 0 & 1 \end{bmatrix}, \tag{2.7}$$

where

$los_{x,y,z}^{(i)}$: ECI line of sight vector for i^{th}satellite

$$= \frac{-(X_{x,y,z,ECI} - S_{x,y,z,ECI}^{i})}{||X_{x,y,z,ECI} - S_{x,y,z,ECI}^{i}||}.$$

2.2.2 Scalar Tracking

Tracking loops play a critical role in continuously tracking the dynamically changing code and carrier parameters of the incoming GPS signal. However, the code and carrier tracking loops of traditional scalar tracking are vulnerable to low SNR and high dynamics [54].

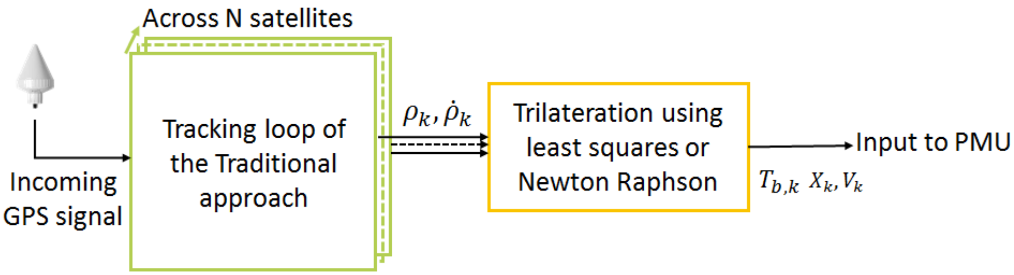

Across N satellites
Incoming GPS signal
Tracking loop of the Traditional approach
$\rho_k, \dot{\rho}_k$
Trilateration using least squares or Newton Raphson
Input to PMU
$T_{b,k}$ X_k, V_k

Figure 2.3: Flow chart for scalar tracking.

In a traditional GPS receiver, acquisition is done first to determine the satellites in view and their corresponding initial code phase and carrier doppler frequency [55]. After the initial acquisition, the scalar tracking loops track the satellite signals and independently estimate the corresponding pseudoranges. These pseudoranges are then collectively processed to obtain the PVT solution as in Fig. 2.3. We can observe that in scalar tracking there is no information exchange between tracking loops and navigation block. Also the conventional scalar tracking neglects the dependencies between the channels based on the same user position and velocities.

The Numerically Controlled Oscillator (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. Given the prior information about the low dynamic nature of our power grid system, we opted for carrier frequency and code phase discriminators that are well suited for low SNR environments, such as interference or jamming [57].

For the code phase discriminator, we opted for the non-coherent early minus late discriminator, which is given by:

$$\frac{1}{2}\frac{E-L}{E+L} \tag{2.8}$$

where $E = \sqrt{I_E^2 + Q_E^2}$ and $L = \sqrt{I_L^2 + Q_L^2}$. This discriminator is normalized to remove amplitude sensitivity.

We chose to use a normalized decision directed frequency discriminator, which is described as follows:

$$\frac{cross \times sign(dot)}{2\pi(t_k - t_{k-1})(I_k^2 + Q_k^2)} \tag{2.9}$$

where $cross = I_{k-1}Q_k - I_kQ_{k-1}$ and $dot = I_{k-1}I_k - Q_{k-1}Q_k$. The error values obtained as outputs from the above discriminators are then used to generate the Kalman filter measurement matrix.

2.3 Position-Information-Aided Vector Tracking

Unlike scalar tracking, a vector tracking loop combines the tracking and PVT estimation blocks into a single loop. Vector tracking enhances performance by enabling closed loop information flow among satellite channels [56]. For timing applications, since the receivers are static, receiver position information is provided to vector tracking, called PIAVT [57].

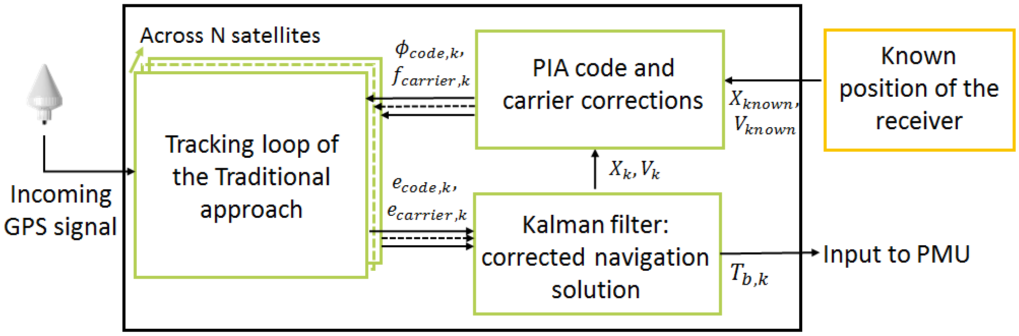

Across N satellites
$\phi_{code,k}$, $f_{carrier,k}$
PIA code and carrier corrections
X_{known}, V_{known}
Known position of the receiver
Tracking loop of the Traditional approach
X_k, V_k
$e_{code,k}$, $e_{carrier,k}$
Kalman filter: corrected navigation solution
$T_{b,k}$
Input to PMU
Incoming GPS signal

Figure 2.4: Flow chart for PIAVT.

As shown in Fig. 2.4, the process for the PIAVT contains 3 main blocks [22] as follows:

1. Scalar tracking: predict the GPS signal parameters using NCO and employs discriminators to track the code and carrier offsets as explained in Section 2.2.
2. Kalman Filtering based measurement update: obtain corrected timing parameters which are given as input to the PMU.
3. PIA and Kalman Filtering based time update: incorporate the known position information to correct for the GPS signal parameters, and then predicts

the timing parameters for the next instant.

2.3.1 Kalman Filtering based measurement update

The code phase and carrier frequency errors are obtained as output from discriminators explained in Section 2.2. The relationship between the code phase and carrier frequency errors in terms of user position and velocity are written as follows:

$$\begin{aligned} e^{(i)}_{code,k} &= \hat{\phi}^{(i)}_k - \phi^{(i)}_k \\ &= T_{b,k} + (X_{x,y,z,k} - \hat{X}_{x,y,z,k})^T los^{(i)}_k \end{aligned} \tag{2.10}$$

$$\begin{aligned} e^{(i)}_{carrier,k} &= \hat{f}^{(i)}_{carrier,k} - f^{(i)}_{carrier,k} \\ &= \Delta T_{d,k} + (X_{\dot{x},\dot{y},\dot{z},k} - \hat{X}_{\dot{x},\dot{y},\dot{z},k})^T los^{(i)}_k, \end{aligned} \tag{2.11}$$

where $e^{(i)}_{code,k}$ and $\phi^{(i)}_k$ are in m, and $e^{(i)}_{carrier,k}$, and $f^{(i)}_{carrier,k}$ are in m/s. Therefore, in our PIAVT approach, we set the states of the Kalman Filter to be 3D position error (ΔX), velocity error(ΔV), clock bias $(T_{b,k})$ and clock drift error$(\Delta T_{d,k})$.

Kalman Filter is initialized through the scalar tracking results. Kalman Filter equations for this case is written as follows:

$$\begin{bmatrix} \Delta X_{x,y,z,(k+1)} \\ \Delta X_{\dot{x},\dot{y},\dot{z},(k+1)} \\ T_{b,(k+1)} \\ \Delta T_{d,(k+1)} \end{bmatrix} = F \begin{bmatrix} \Delta X_{x,y,z,(k+1)} \\ \Delta X_{\dot{x},\dot{y},\dot{z},(k+1)} \\ T_{b,k} \\ \Delta T_{d,k} \end{bmatrix}, \tag{2.12}$$

where the state transition matrix F is

$$F = \begin{bmatrix} 0 & 0 & 0 & \Delta t & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \Delta t & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \Delta t & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{2.13}$$

The Kalman Filter measurement matrix is then given by

$$Z_k = \left[e^1_{code,k} \quad e^1_{carrier,k} \quad ..e^i_{code,k} \quad e^i_{carrier,k} .. \quad e^N_{code,k} \quad e^N_{carrier,k} \right], \tag{2.14}$$

where the measurement matrix H is defined as Eq. (2.7).

The corrected predictions are then obtained as output of our vector tracking loop. Based on this, we calculate the clock bias of the receiver as a weighted average of the difference between the pseudorange calculated and the range [58]:

$$t_b = \frac{1}{\sigma^N_{i=1} \omega_i} \sum_{i=1}^{N} \omega^{(i)} (\rho^{(i)} - |S^{(i)} - X_{known}|), \tag{2.15}$$

where $\omega^{(i)}$ is the weighting term calculated by $\omega^{(i)} = \frac{1}{var(\varepsilon^{(i)})}$, where $\varepsilon^{(i)}$ is the noise in the channel corresponding to i^{th} satellite, and $\rho^{(i)}$ is the calculated pseudorange between the PMU receiver and the i^{th} satellite. $var(\varepsilon^{(i)})$ is obtained from the carrier-to-noise density ratio (C/N_o) of a particular i^{th} satellite. This corrected clock bias is then obtained as an output from PIAVT loop, which is then given as input to the PMUs in power grid.

2.3.2 PIA and Kalman Filtering based time update

Once the position and velocity predictions have been corrected by the Kalman filter, these corrected predictions are compared with the pre-determined known 3D position and velocity. By taking into account the true position, we can estimate the corrected signal parameters for the same time epoch using Eq. (2.16).

$$\begin{aligned} \phi^{(i)}_k &= \hat{\phi}^{(i)}_k + \Delta X_{x,y,z,k} \,.\, los^{(i)}_k + c\Delta t + T_{b,k} \\ f^{(i)}_{code,k} &= \hat{f}^{(i)}_{code,k} + (T_{d,k} + \Delta X_{\dot{x},\dot{y},\dot{z},k} \,.\, los^{(i)}_k) f_{C/A}/c \\ f^{(i)}_{carrier,k} &= \hat{f}^{(i)}_{carrier,k} + (T_{d,k} + \Delta X_{\dot{x},\dot{y},\dot{z},k} \,.\, los^{(i)}_k) f_{L1}/c \end{aligned} \tag{2.16}$$

After this step, these corrected values are used to calculate the timing parameters for the next time epoch. These predicted timing parameters are sent back into the loop to predict the signal parameters using NCO of scalar tracking loop for the next time epoch and the loop continues.

CHAPTER 3

MULTI-RECEIVER DIRECT TIME ESTIMATION

3.1 Overview of our algorithm

Our proposed MR-DTE algorithm employs multiple receivers to establish geographical diversity enabled by the infrastructure of the grid. Fig. 3.1 shows an electrical power substation in Champaign, Illinois. Given that the power grid is a static system, the 3D position and velocity of the receivers are surveyed ahead of time and later used for aiding the fine solution. Unlike scalar tracking, DTE directly operates with the timing parameters and does not require the estimation of intermediate pseudorange measurements.

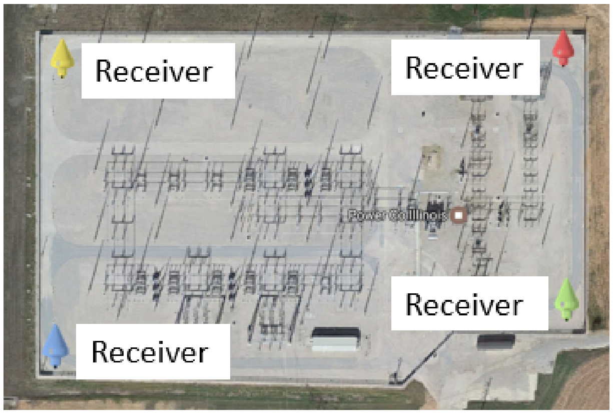


Figure 3.1: Illinois Power Substation, Champaign IL.

All the receivers in the MR-DTE setup are triggered by a common external clock. Difference in cable lengths introduces a bias across the receivers that needs be pre-determined. In our setup, the cable length difference across the receivers is between $1-2$ m. The cable delay difference is much less than the C/A chip width, thus considered negligible [59]. All the above aspects are adopted to reduce the search space from $8L$ $(X_{t,k}, T_{t,k})$ to 2 $(T_{t,overall})$, thereby decreasing the computational complexity.

3.2 Architecture of MR-DTE

In our MR-DTE architecture [25], there are L different receivers that receive GPS signals from N visible satellites at time instant t. The complete state of any k^{th} GPS receiver is represented by X_k (3D position and velocity) and T_k (clock parameters). As shown in Eq. (3.1), the corrected overall clock state vector $T_{t,overall}$ is obtained as the output from MR-DTE. This is used to estimate the absolute UTC time that is used as reference time in PMUs.

$$\begin{aligned} L &: \text{Number of receivers in MR-DTE setup} \\ k &: 1,.., \text{L subscript to denote the } k^{th} \text{ receiver} \end{aligned}$$

$$\begin{aligned} X_{t,k} &: \text{3D Position and velocity of the } k^{th} \text{ receiver at} \\ &\quad t^{th} \text{ time instant} \\ &= [x_k, y_k, z_k, \dot{x}_k, \dot{y}_k, \dot{z}_k]_t \\ T_{t,k} &: \text{Clock states of the } k^{th} \text{ receiver at } t^{th} \text{ time instant} \\ &= [c\delta t_k, c\delta \dot{t}_k]_t \end{aligned}$$

The high level architecture of MR-DTE described in Fig. 3.2 consists of two major steps. The first step involves applying DTE in parallel to estimate the maximum likelihood timing parameters for each of the k^{th} receiver. The corresponding error residuals e_k computed from the first step are considered as input for next step. The second step is the MR-DTE filter. We jointly process the error residuals from different receivers in an overall filter to account for individual receiver errors and mitigate the effect of localized malicious signals if any. We define:

$$\begin{aligned} T_{t,overall} &: \text{Overall clock state of the MR-DTE setup} \\ &: \text{Input to the PMUs in power grid, } 2 \times 1 \\ &= [c\delta t_{overall}, c\delta \dot{t}_{overall}], \\ \text{where} & \\ c\delta t_{overall} &: \text{Overall clock bias of the clock (m)} \\ c\delta \dot{t}_{overall} &: \text{Overall clock drift of the clock (m/s).} \end{aligned} \tag{3.1}$$

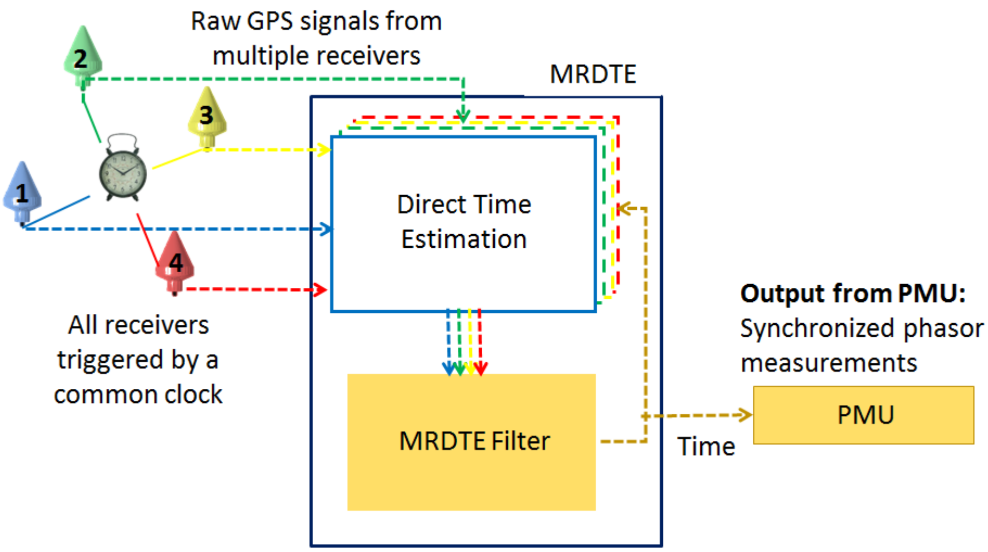

Raw GPS signals from multiple receivers
MRDTE
2
3
1
4
Direct Time Estimation
All receivers triggered by a common clock
Output from PMU: Synchronized phasor measurements
PMU
MRDTE Filter
Time

Figure 3.2: Architecture of MR-DTE.

3.2.1 Characteristics of DTE

DTE which is the first step of MR-DTE, estimates the cumulative satellite vector correlation of the raw received GPS signal with the signal replica produced for each grid point g_j from a pre-generated 2D-search space consisting of G grid points [24]. As shown in Eq. (3.2), correlating the incoming GPS signal with a cumulative satellite signal replica is equivalent to first correlating the incoming signal with the individual satellite replicas and then summing across the satellites. For each clock candidate set, we execute the per satellite computations in parallel which are later aggregated together to establish the final correlation value.

$$\begin{aligned}
&\text{corr}_j : \text{DTE correlation for the } j^{th} \text{ clock candidate set}\\
&\quad = corr(R, \sum_{i=1}^{N} Y^i(c\delta t_j, c\delta \dot{t}_j))\\
&\quad = \sum_{i=1}^{N} corr(R, Y^i(g_j)) \qquad (3.2)\\
&R : \text{Raw received GPS signal}\\
&g_j : j^{th} \text{ grid point in 2-D search space}\\
&\quad = [c\delta t_j, c\delta \dot{t}_j]\\
&j : 1.. \text{ G subscript denote the } j^{th} \text{ grid point}
\end{aligned}$$

$$\text{corr-overall} = \max_{j=1}^{G} \text{corr}_j \tag{3.3}$$

$$G: \text{Number of grid points in search space}$$

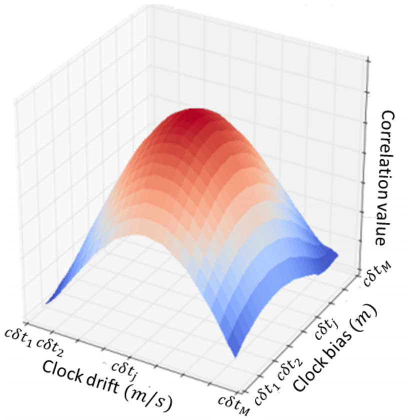


Figure 3.3: Vector correlation weights corresponding to the 2-D clock state search space with G grid points. Peak of the bell curve estimated using MLE.

Taking 3D position and velocity of the static receiver as aprior information, the most plausible clock state of the receiver represented by the peak of the bell curve in Fig. 3.3, is evaluated using maximum likelihood estimation (MLE) [60].

In the case of weak signal environment, DTE directly focuses on the combined satellite signal correlation rather than tracking satellite channels independently. Therefore, DTE is more robust [62] in degraded signal environment and in the presence of multipath or external timing attacks. DTE achieves equal or better accuracy compared to scalar tracking. Mathematically, this is justified because the variance of a one-step estimator is lower than the variance of an estimator involving multiple steps [61].

3.3 Detailed flow of MR-DTE

The flow chart explaining the first step i.e., DTE is shown in Fig. 3.4 and each block is explained in the subsequent steps:

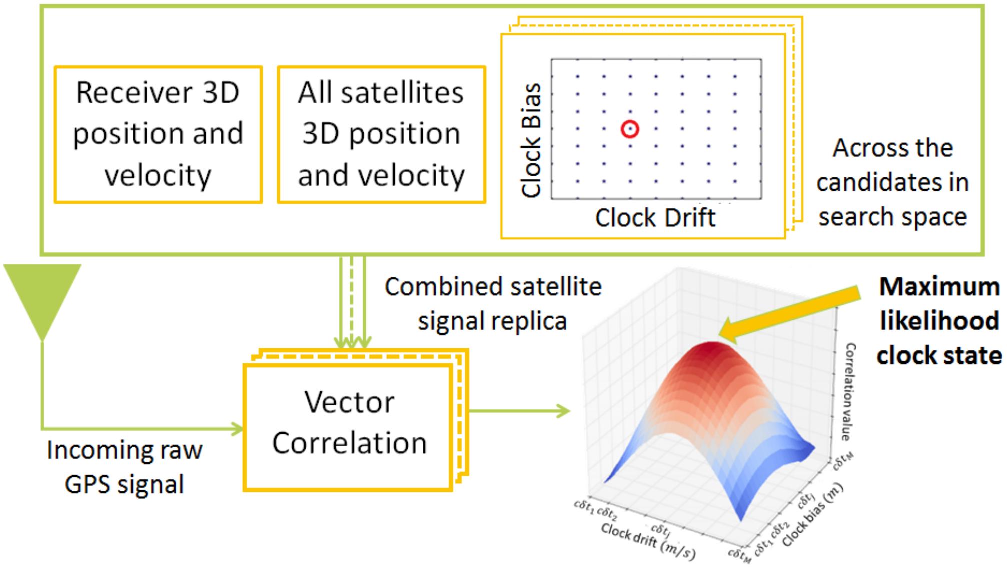

Receiver 3D position and velocity
All satellites 3D position and velocity
Clock Bias
Clock Drift
Across the candidates in search space
Combined satellite signal replica
Maximum likelihood clock state
Vector Correlation
Incoming raw GPS signal
Correlation value
$c\delta t_1$ $c\delta t_2$ $c\delta t_j$ $c\delta t_M$
Clock drift (m/s)
$c\delta t_1$ $c\delta t_2$ $c\delta t_j$ $c\delta t_M$
Clock bias (m)

Figure 3.4: DTE.

3.3.1 Vector correlation

Based on the predicted clock state estimate, N satellite positions and 3D position and velocity of the k^{th} receiver, a composite signal replica is generated for each of the G grid points considered. First step in the DTE process is to carry out vector correlations on a per satellite channel basis.

Correlations are performed by correlating the incoming signal with the carrier signal replica to obtain the variation of correlation amplitude against the code phase residuals as depicted in Fig. 3.5.

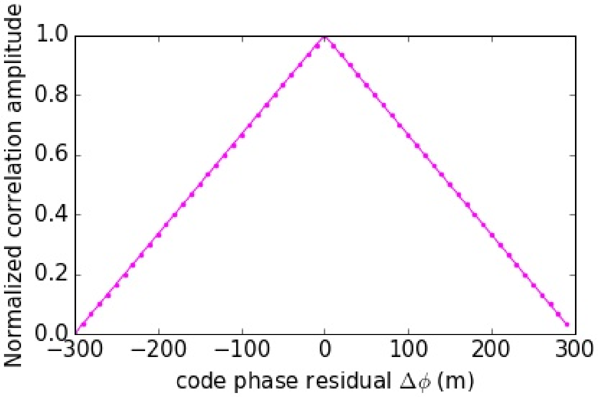


Figure 3.5: Correlation amplitude plotted against the code phase residual.

Similarly, Fourier transforms are computed by correlating the incoming signal with the generated code replica and then plotting variation of the spectrum magnitude table as shown in Fig. 3.6.

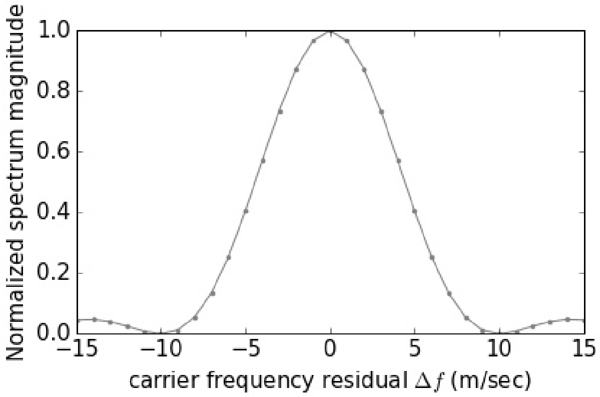


Figure 3.6: Spectrum magnitude against carrier doppler frequency residual.

The above computations are carried out in two parallel threads as in Fig. 3.7: one for correlations and other for the Fourier transforms.

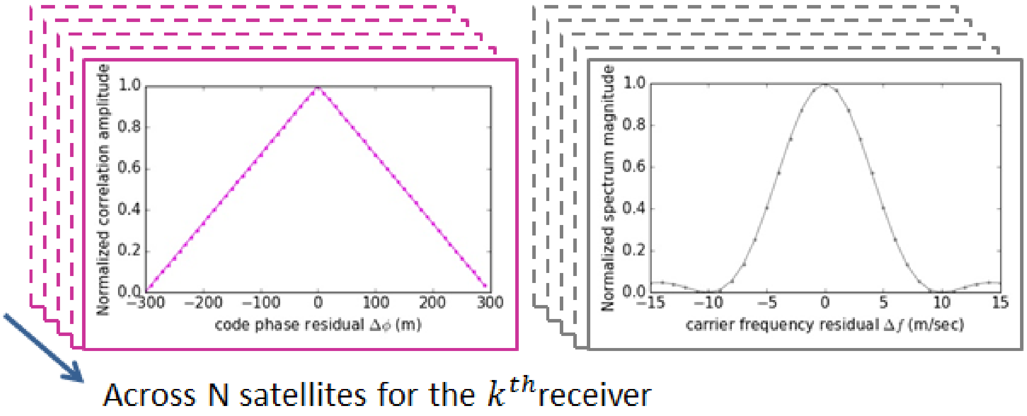
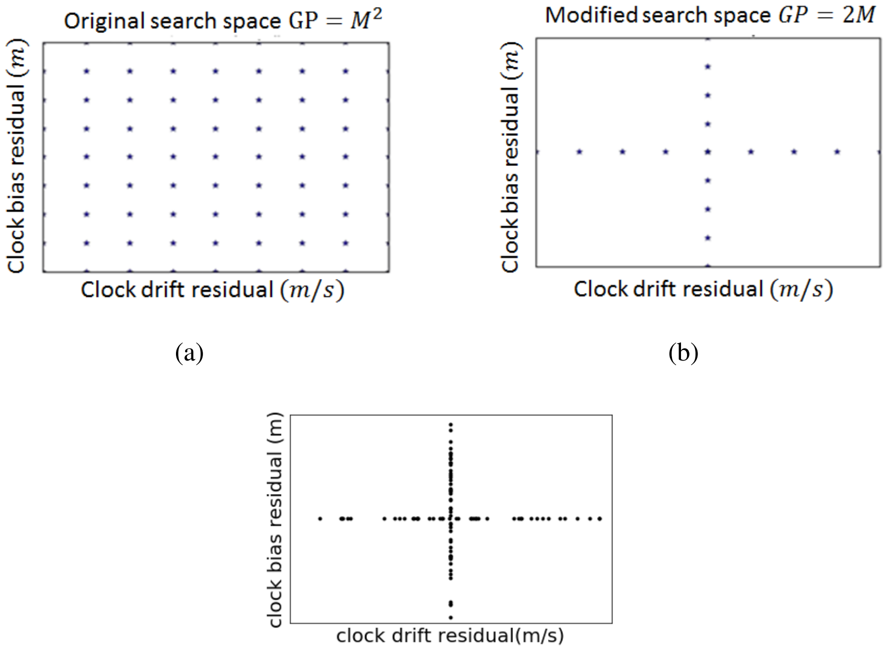

Normalized correlation amplitude
1.0
0.8
0.6
0.4
0.2
0.0
−300
−200
−100
0
100
200
300
code phase residual Δφ (m)
Normalized spectrum magnitude
1.0
0.8
0.6
0.4
0.2
0.0
−15
−10
−5
0
5
10
15
carrier frequency residual Δf (m/sec)
Across N satellites for the k^{th}receiver

Figure 3.7: Correlation amplitude and Spectrum magnitude across satellites

3.3.2 Candidate selection

DTE is computationally expensive given that search space at each time instant involves $G = M^2$ number of computations, where M denotes the number of pregenerated clock bias and clock drift candidates each. In order to reduce the complexity, we carry out the search process independently and in two parallel threads. Keeping the current predicted estimate of the clock drift as constant, clock bias residual candidates are evaluated through the first thread. Similarly, second thread considers candidates of clock drift residuals keeping the current predicted estimate of the clock bias as constant. As shown in Fig. 3.8(a) and 3.8(b), for each time instant, the number of computations are effectively reduced from $G = M^2$ to $G = 2M$.

The accuracy of the solution estimated using DTE depends on the resolution of the grid points considered. To further improve the computational efficiency and precision of the clock parameters estimated, we incorporated an adaptive covariance based Gaussian search space as seen in Fig. 3.8(c). The search space is designed based on the predicted covariance values estimated by the time update of Kalman Filter.


Original search space GP = M^2
Clock bias residual (m)
Clock drift residual (m/s)
Modified search space $GP = 2M$
Clock bias residual (m)
Clock drift residual (m/s)
clock bias residual (m)
clock drift residual(m/s)

(a)

(b)

(c)

Figure 3.8: (a) The original search space for a pre-generated $G = M^2$ grid points; (b) The modified $G = 2M$ uniform search space; (c) The adaptive Gaussian search space for computational efficiency.

This split is justified because channel delay is proportional to clock bias and

Doppler frequency is proportional to clock drift as described in Eq. (3.4)-(3.5).

$$\begin{aligned} f^{(i)}_{code} &= f_{C/A} + \frac{f_{C/A}}{f_{L1}} \times f^{i}_{dcarr} \\ \phi^{(i)}_{code} &= -\frac{f_{C/A}}{c}(||X_{x,y,z,ECI} - S^{i}_{x,y,z,ECI}||) \\ &\quad + (T_{c\delta t} - T^{i}_{c\delta t}) \end{aligned} \tag{3.4}$$

$$\begin{aligned} f^{(i)}_{carr} &= f_{IF} + f^{i}_{dcarr} \\ f^{(i)}_{dcarr} &: \text{carrier doppler frequency of the } i^{th}\text{satellite} \\ &= -\frac{f_{L1}}{c}(-los^{i}_{x,y,z}.(X_{\dot{x},\dot{y},\dot{z},ECI} - S^{i}_{\dot{x},\dot{y},\dot{z},ECI}) \\ &+ (T_{c\delta\dot{t}} - T^{i}_{c\delta\dot{t}})) \end{aligned} \tag{3.5}$$

To reduce the computational load, computations of DTE are separated into two parallel thread. The sets of clock candidates are given below.

$$\Delta T_{c\delta t} = \begin{bmatrix} \Delta c\delta t_1 & 0 \\ : & : \\ \Delta c\delta t_j & 0 \\ \Delta c\delta t_M & 0 \end{bmatrix},$$

$$\Delta T_{c\delta\dot{t}} = \begin{bmatrix} 0 & \Delta c\delta\dot{t}_1 \\ : & : \\ 0 & \Delta c\delta\dot{t}_j \\ 0 & \Delta c\delta\dot{t}_M \end{bmatrix}.$$

For each candidate residual $\Delta T_{c\delta t,j}$, we compute the corresponding code residual and map it to the correlation table in Section 3.3.1. The correlation amplitude corresponding to the code residual is computed for the j^{th} set and for each of the N satellites. In parallel, spectrum magnitude corresponding to the carrier residual is generated from the $\Delta T_{c\delta\dot{t},j}$.

3.3.3 Non-coherent summation

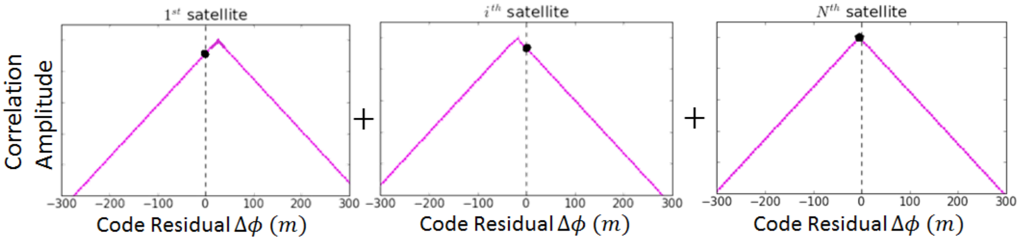


Figure 3.9: Non-coherent summation of the correlation amplitude $c_{i,j,k}$ across N satellites to compute the correlation weight $w_{c\delta t,j,k}$ corresponding to j^{th} clock bias candidate $\Delta T_{c\delta t,j}$ and k^{th} receiver.

For each j^{th} candidate set, non-coherent summation (i.e., amplitude summation without considering the phase) of correlation amplitudes $c_{i,j,k}$ and spectrum magnitudes $s_{i,j,k}$ is evaluated respectively across the N visible satellites.

In ideal conditions, the correlation peaks across the satellites should correspond to the same code and carrier residual. However, given the measurement noise, we observe difference in location of the maximum correlation peak for correlation amplitude plots in Fig. 3.9 and for spectrum magnitude plots in Fig. 3.10. By adopting the non-coherent summation based vector correlation, we are essentially employing a voting scheme wherein each i^{th} satellite votes for the likelihood of a particular j^{th} candidate error residual set.

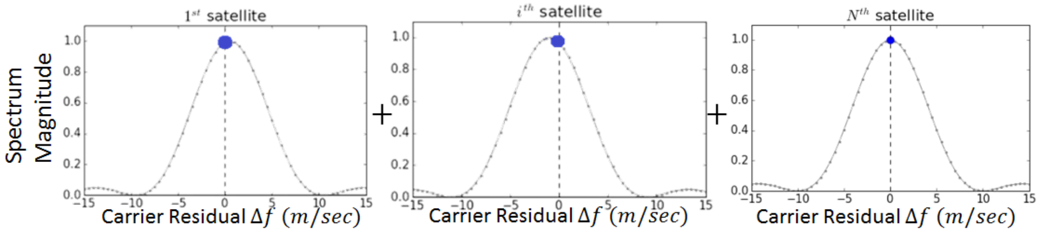


Figure 3.10: Non-coherent summation of the spectrum magnitude $s_{i,j,k}$ across N satellites to compute the correlation weight $w_{c\delta t,j,k}$ corresponding to j^{th} clock drift candidate $\Delta T_{c\delta i,j}$ and k^{th} receiver.

The obtained summation of correlation values are allocated as weights for the next step that performs maximum likelihood estimation.

The weights obtained for each of the clock bias candidates is as follows:

$$w_{c\delta t,j,k} = \sum_{i=1}^{N} c_{i,j,k}, \tag{3.6}$$

where $c_{i,j,k}$ denotes the correlation amplitude obtained for i^{th} satellite, j^{th} clock candidate and k^{th} receiver.

The weights obtained for each of the clock drift candidates is as follows:

$$w_{c\delta\dot{t},j,k} = \sum_{i=1}^{N} s_{i,j,k}, \tag{3.7}$$

where $s_{i,j,k}$ denotes the correlation amplitude obtained for i^{th} satellite, j^{th} clock candidate and k^{th} receiver.

3.3.4 MLE

The steps in Sections 3.3.1-3.3.3 are for a particular receiver and candidate set. In this step for each receiver, MLE is applied across the M candidate sets to estimate the most likely set of clock residuals.

After obtaining the weights corresponding to the clock candidate sets, a weighted average as in Eq. (3.8) is performed to come up with the best estimate of the clock parameters. The measurement error residual obtained in Eq. (3.9) is given as input to MR-DTE filter.

$$T_{t,k,MLE} = \left[\frac{\sum_{j=1}^{M} w_{c\delta t,j,k} c\delta t_{j,k}}{\sum_{j=1}^{M} c\delta t_{j,k}}, \quad \frac{\sum_{j=1}^{M} w_{c\delta\dot{t},j,k} c\delta\dot{t}_{j,k}}{\sum_{j=1}^{M} c\delta\dot{t}_{j,k}} \right], \tag{3.8}$$

where

$T_{t,k,MLE}$: maximum likely estimate of the clock state

$$\begin{aligned} e_{t,k} &: \text{Measurement residual for the } k^{th}\text{receiver} \\ &= T_{t,k,MLE} - T_{t,overall} \\ &= [\Delta c\delta t_k, \Delta c\delta\dot{t}_k] \end{aligned} \tag{3.9}$$

3.3.5 Individual measurement update

After obtaining the measurement error vectors e_k for each of the individual receivers, Kalman Filter is implemented to estimate the individual corrected clock bias and clock drift represented by $T_{t,k}$. The measurement noise covariance matrix is evaluated by considering the covariance of the last 20 individual measurement residuals.

The measurement update for k^{th} receiver at any instant t:

$$\begin{aligned}
H_k &: \text{Observation matrix, } 2 \times 2 \\
&= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
\hat{P}_{t,k} &: \text{Predicted state error covariance matrix} \\
R_{t,k} &: \text{measurement noise covariance matrix} \\
&= \sum_{i=t}^{t-19} e_{t,k} \\
K_{t,k} &: \text{Kalman gain matrix} \\
&= \hat{P}_{t,k} H_k^T (H_k \hat{P}_{t,k} H_k^T + R_{t,k})^{-1} \\
\Delta T_{t,k} &: \text{State error vector} \\
&= K_{t,k} e_{t,k}
\end{aligned} \tag{3.10}$$

$$\begin{aligned}
T_{t,k} &: \text{Corrected state vector of the } k^{th} \text{ receiver} \\
&= \hat{T}_{t,k} + \Delta T_{t,k} \\
P_{t,k} &: \text{Corrected state error covariance matrix} \\
&= (I - K_{t,k} H_k) \hat{P}_{t,k}
\end{aligned} \tag{3.11}$$

3.3.6 Overall measurement update

In this step, the measurements obtained from individual receivers are processed using an overall Kalman Filter to account for spurious signals. The measurement residual vector $e_{t,overall}$ is obtained by computing the difference between individual corrected clock parameters $T_{t,k}$ and the predicted reference state vector $\hat{T}_{t,overall}$.

The overall measurement update equations at instant t are listed as follows:

$$
\begin{aligned}
e_{t,overall} &= \begin{bmatrix} T_{t,1} - \hat{T}_{t,overall} \\ : \\ T_{t,k} - \hat{T}_{t,overall} \\ T_{t,L} - \hat{T}_{t,overall} \end{bmatrix} \\
H &: \text{Observation matrix, } (L+1) \times (L+1) \\
&= \begin{bmatrix} 1 & 1 & 0 & .. & 0 \\ 0 & 1 & 1 & .. & 0 \\ : & : & : & .. & : \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}
\end{aligned}
\tag{3.12}
$$

$$
\begin{aligned}
\hat{P}_t &: \text{Predicted state error covariance matrix} \\
R_t &: \text{measurement noise covariance matrix} \\
&= \begin{bmatrix} R_{t,1} & .. & 0 & .. & 0 \\ : & : & R_{t,k} & : & : \\ 0 & .. & 0 & .. & R_{t,L} \end{bmatrix} \\
K_t &: \text{Kalman gain matrix} \\
&= \hat{P}_t H^T (H \hat{P}_t H^T + R_t)^{-1}
\end{aligned}
\tag{3.13}
$$

$$
\begin{aligned}
\Delta T_{t,overall} &: \text{State error vector} \\
&: K_t e_{t,overall} \\
T_{t,overall} &: \text{Corrected state vector of the } k^{th} \text{ receiver} \\
&= \hat{T}_{t,overall} + \Delta T_{t,overall} \\
P_t &: \text{Corrected state error covariance matrix} \\
&= (I - K_t H) \hat{P}_t
\end{aligned}
\tag{3.14}
$$

The corrected clock parameters $(T_{t,overall})$ obtained as output from MR-DTE is given as input to the PMU. Later, we update the clock parameters of individual receivers to have same values as the overall state vector.

$$
\overline{T}_{t,k} = T_{t,overall}, \;\; k = 1,..,L \tag{3.15}
$$

3.3.7 Time update

We linearly propagate the clock parameters based on the first order state transition matrix to predict the overall and individual receiver states for the next time instant $t+1$. The predicted covariance matrix obtained is used for designing the grid points of clock candidate search space for the next time instant.

The time update equations for the k^{th} receiver are:

$$\begin{aligned}
\Delta T &: \text{Update interval} \\
F_k &: \text{State transition matrix, } 2 \times 2 \\
&= \begin{bmatrix} 1 & \Delta T \\ 0 & 1 \end{bmatrix} \\
Q_{t,k} &: \text{State process noise covariance matrix} \\
&= F_k \begin{bmatrix} 0 & \Delta T \\ 0 & (c \times \sigma_\tau)^2 \end{bmatrix} F_k^T \qquad (3.16) \\
\sigma_\tau &: \text{allan deviation of the front-end oscillator, (s)} \\
\hat{T}_{t+1,k} &: \text{Predicted state vector for the } (t+1)^{th} \text{ instant} \\
&= F_k \overline{T}_{t,k} \\
\hat{P}_{t+1,k} &: \text{Predicted state error covariance matrix} \\
&= F_k P_{t,k} F_k^T + Q_{t,k}
\end{aligned}$$

The overall time update equations are given by:

$$\begin{aligned}
\hat{T}_{t+1,overall} &: \text{Predicted state vector} \\
&= F T_{t,overall} \qquad (3.17) \\
\hat{P}_{t+1,overall} &: \text{Predicted state error covariance matrix} \\
&= F P_t F^T + Q_t
\end{aligned}$$

F : Overall state propagation matrix

$$= \begin{bmatrix} F_1 & .. & 0 \\ : & F_k & \\ 0 & .. & F_L \end{bmatrix}$$

Q_t : state process noise covariance matrix

$$= F \begin{bmatrix} Q_{t,1} & .. & 0 \\ : & Q_{t,k} & \\ 0 & .. & Q_{t,L} \end{bmatrix} F^T$$

3.4 Initialization of MR-DTE

Accuracy and convergence of MR-DTE depend on the reliability of known static position and velocity of receivers, which is computed through the existing GPS algorithms averaged over time. The static information obtained is used for the initialization of MR-DTE. In high noise levels conditions, where the position coordinates obtained are not accurate enough, 3D position and velocity of individual receivers are included in the state vector and simultaneously estimated.

CHAPTER 4

EXPERIMENTAL SETUP

Our experimental setup consists of two parts: the first part involves collecting raw GPS signals using multiple receivers. The raw GPS signals are processed to evaluate the increased robustness of our advanced algorithms namely SR-DTE and MR-DTE. The second part analyzes the stability of the grid when subjected to timing attacks using our proposed algorithm in Section 3 as compared to scalar tracking explained in Section 2.2 and PIAVT described in Section 2.3.

4.1 GPS experimental setup

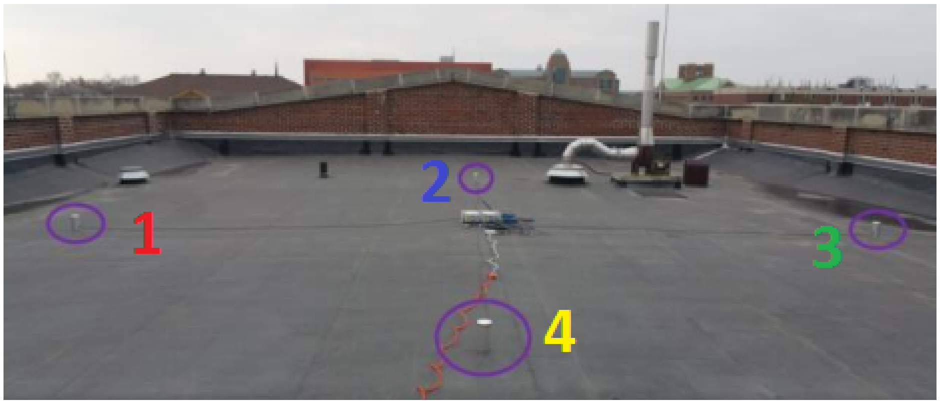


Figure 4.1: Four GPS antennas located on roof of Talbot Laboratory, University of Illinois at Urbana-Champaign (UIUC). Reference image taken from [23].

Our proposed algorithms are validated using AntCom 3GNSSA4-XT-1 GNSS antennas [63] mounted onto the roof of Talbot Laboratory, Urbana, Illinois as shown in Fig. 4.1. They are connected to a common Microsemi Quantum SA.45s CSAC [64], chosen for its low drift rate.

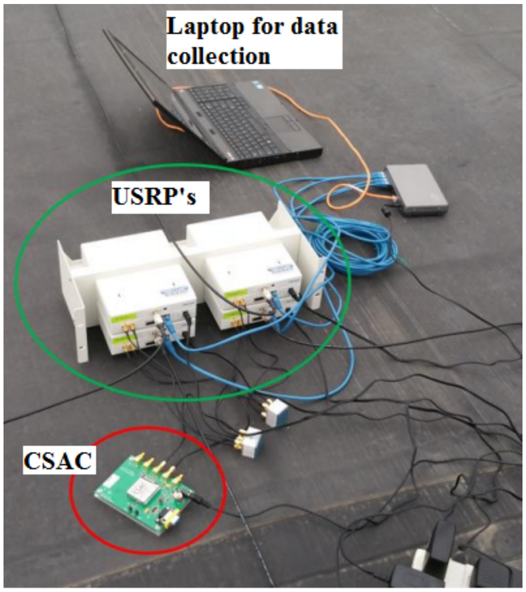


Figure 4.2: Data collection for GPS experiments.

The raw voltage data is logged using respective Universal Software Radio Peripherals (USRP-N210) [65] each equipped with a DBSRX2 daughterboard as shown in Fig. 4.3. GNUradio [66] was used for collecting the raw GPS $L1$ signal samples from USRP at a sampling rate of 5 MHz.

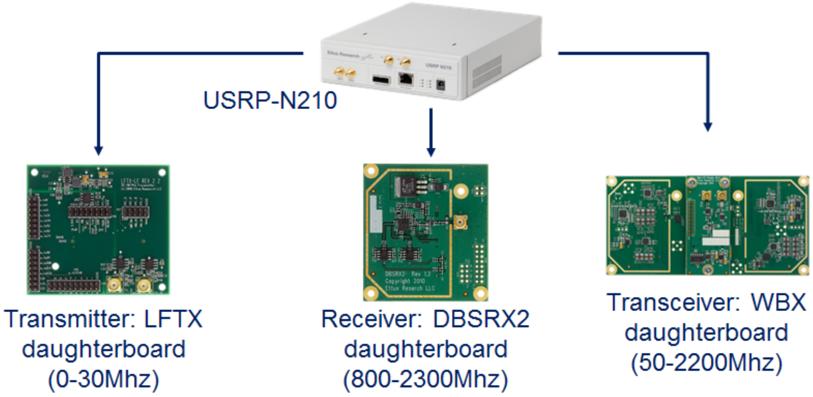

USRP-N210
Transmitter: LFTX daughterboard (0-30Mhz)
Receiver: DBSRX2 daughterboard (800-2300Mhz)
Transceiver: WBX daughterboard (50-2200Mhz)

Figure 4.3: Specifications of the daughter boards used with USRP-N210.

Virtual timing attacks are generated and mixed with the signal collected to simulate timing attack scenarios as in Fig. 4.4. We chose to implement this technique in the Python based Software Defined Radio (SDR) developed in our lab known as pyGNSS [67], given its flexible and object oriented framework. In our case, the 3D position and velocity of the receivers are calculated using Multi-Receiver Vector Tracking (MRVT) [68]. For the vector correlation, we opted a coherent integration time of $\Delta T = 20\ ms$.

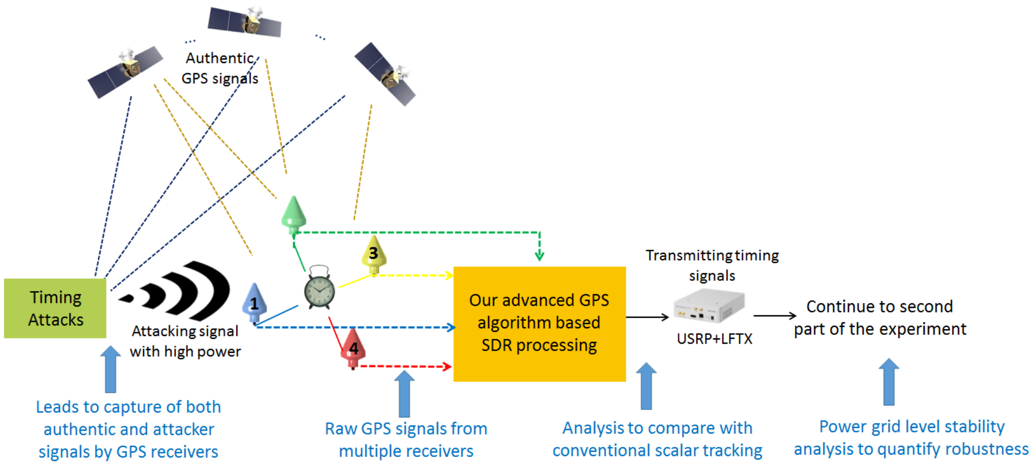

Authentic
GPS signals
Timing Attacks
Attacking signal with high power
1
3
4
Our advanced GPS algorithm based SDR processing
Transmitting timing signals
USRP+LFTX
Continue to second part of the experiment
Leads to capture of both authentic and attacker signals by GPS receivers
Raw GPS signals from multiple receivers
Analysis to compare with conventional scalar tracking
Power grid level stability analysis to quantify robustness

Figure 4.4: Flow chart explaining the first part of experimental validation. Raw GPS signals are collected using multiple receivers and processed through SDR based pyGNSS to generate the corresponding timing signals.

4.2 Power grid testbed

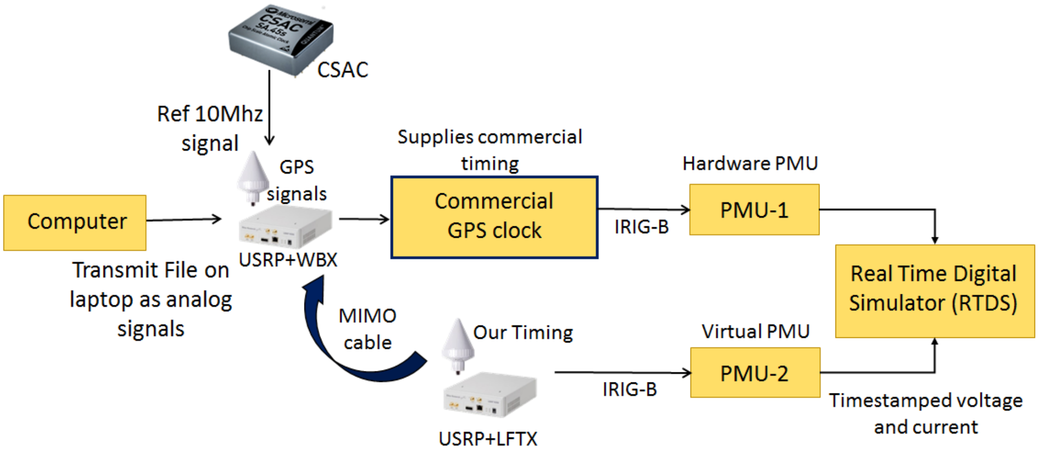
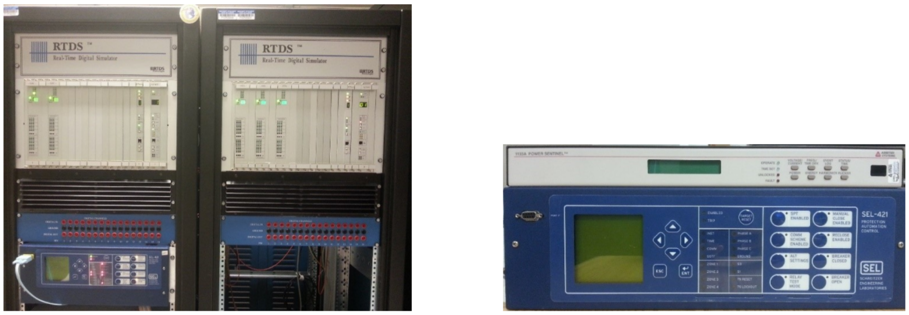


Figure 4.5: Flow chart explaining our power testbed at UIUC. Raw GPS signals and the corresponding MR-DTE based timing signals are simultaneously transmitted to analyze the recorded PMU data.

The second part of our experimental validation involves performing offline stability analysis of the grid, in the presence of timing attacks using our setup shown in Fig. 4.5. The upper thread sends the GPS signals to a commercial clock that in turn supplies the timing signals to a hardware PMU. The lower thread triggers another hardware PMU using our SR-DTE/MR-DTE based timing. We use Real-

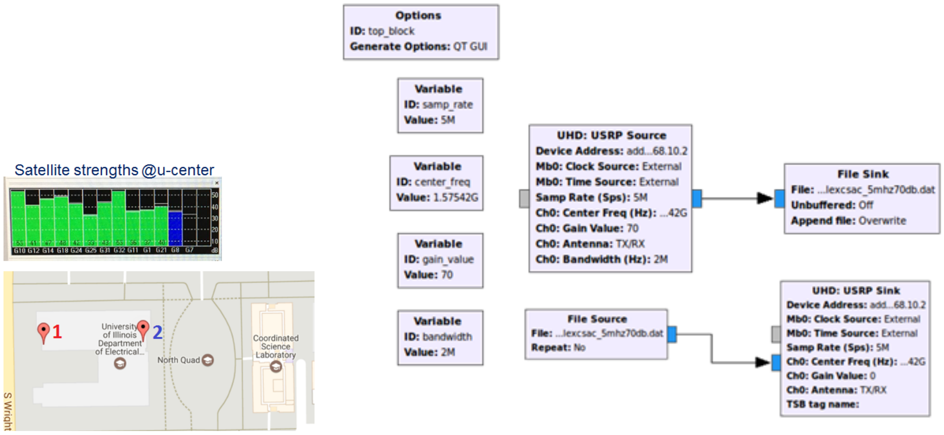
Time Digital Simulator (RTDS) in Fig. 4.6(a) for simulating wide network power system.



(a) (b)

Figure 4.6: (a) RTDS; (b) hardware PMU used for the experiments.

Second set of GPS signals are collected on the rooftop of Electrical and Computer Engineering (ECE) building using two receivers as in Fig. 4.7(a). The datasets analyzed are different from that used in Section 6.1. The collected GPS signals are re-transmitted as either authentic or malicious signals using the USRP with WBX daughter board, which is a wide bandwidth transceiver.


Satellite strengths @u-center
55
41
47
48
42
33
43
53
36
37
40
G10 G12 G14 G18 G24 G25 G31 G32 G11 G1 G21 G8 G7
50
40
30
20
10
dB
1
2
University of Illinois Department of Electrical...
North Quad
Coordinated Science Laboratory
S Wright

Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 5M

Variable
ID: center_freq
Value: 1.57542G

Variable
ID: gain_value
Value: 70

Variable
ID: bandwidth
Value: 2M

UHD: USRP Source
Device Address: add...68.10.2
Mb0: Clock Source: External
Mb0: Time Source: External
Samp Rate (Sps): 5M
Ch0: Center Freq (Hz): ...42G
Ch0: Gain Value: 70
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 2M

File Sink
File: ...lexcsac_5mhz70db.dat
Unbuffered: Off
Append file: Overwrite

File Source
File: ...lexcsac_5mhz70db.dat
Repeat: No

UHD: USRP Sink
Device Address: add...68.10.2
Mb0: Clock Source: External
Mb0: Time Source: External
Samp Rate (Sps): 5M
Ch0: Center Freq (Hz): ...42G
Ch0: Gain Value: 0
Ch0: Antenna: TX/RX
TSB tag name:

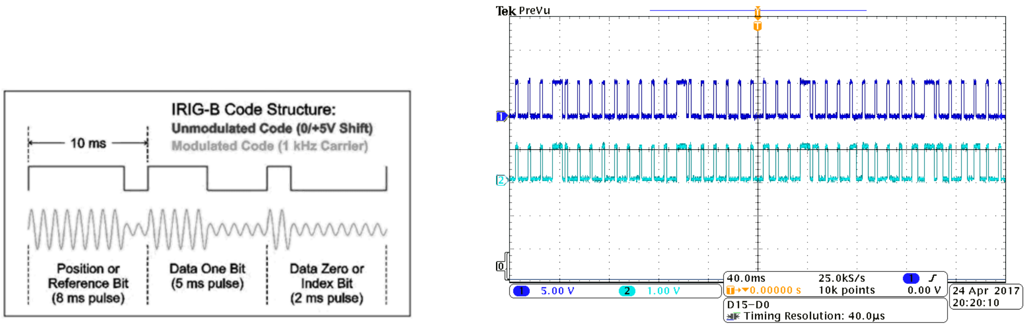
(a) (b)

Figure 4.7: (a) GPS antenna setup on ECE building and the satellite signal strengths; (b) GNURadio software used for record and replay of GPS signals.

Recording and replaying the collected GPS signals cause an additional unknown frequency offset that is dependent on the accuracy of the reference oscillator. USRP-N210 has a Temperature Compensated Crystal Oscillator (TCXO) on-board which provides upto 2.5 ppm^3 accuracy [65]. However, this is not sufficient to trigger the SEL-2488 satellite synchronized network clock used in our experiments. To account for this, we aid the USRP+WBX with an external 10 MHz reference clock signal supplied by the CSAC.

These re-transmitted GPS signals are given as input to the commercial GPS clock (SEL-2488) that provides the corresponding timing signals as output. The output from the commercial clock is used to trigger the hardware PMU (SEL-421 protection, automation and control system) as shown in Fig. 4.6(b).

The USRP with LFTX daughter board ($0-30$ MHz transmitter) transmits the timing signals produced using MR-DTE. The timing signals follow a standard protocol for transferring timing information known as IRIG time codes as shown in Fig 4.8(a). We designed a parser to convert the time obtained from our GPS algorithms to IRIG-B004 protocol. Manual zero padding is done at the start to align the raw GPS signals. The output from USRP+LFTX is of $0-1$ V, while the PMU is configured to operate with $0-5$ V input. Therefore, a voltage shifter is designed to amplify the signal as shown in Fig. 4.8(b).


IRIG-B Code Structure:
Unmodulated Code (0/+5V Shift)
Modulated Code (1 kHz Carrier)
10 ms
Position or Reference Bit (8 ms pulse)
Data One Bit (5 ms pulse)
Data Zero or Index Bit (2 ms pulse)
Tek PreVu
1
2
0
5.00 V
1.00 V
40.0ms
0.00000 s
25.0kS/s
10k points
0.00 V
D15–D0
Timing Resolution: 40.0μs
24 Apr 2017
20:20:10

(a) (b)

Figure 4.8: (a) Basic IRIG-B signal bits; (b) cyan line represents the output from the commercial clock before voltage shifting, and blue line denotes the output after voltage shifting.

A MIMO expansion cable is used to synchronize both the USRPs, thereby enabling an exchange of clock and time information. GNURadio software is used for transmitting the synchronized signals in Fig. 4.9 to the USRPs as shown in Fig. 4.10.

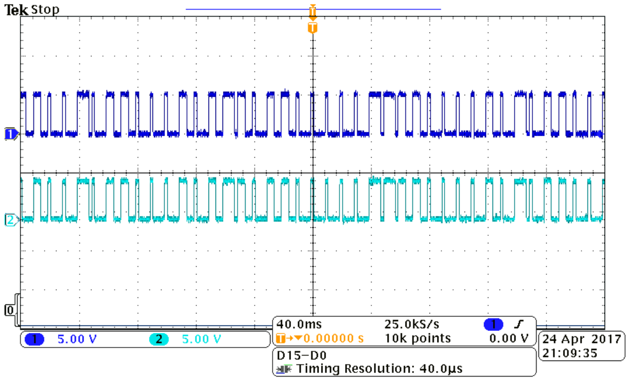
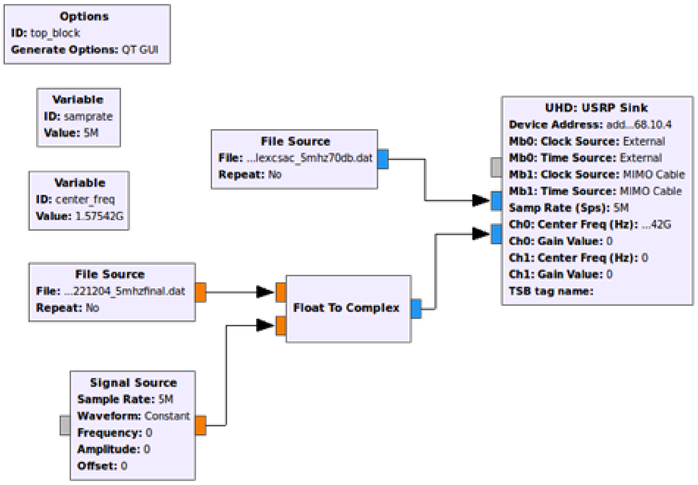


Figure 4.9: Blue signals represents the timing signals from USRP+LFTX setup while cyan signals represent the timing signals from USRP+WBX setup.



Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samprate
Value: 5M

Variable
ID: center_freq
Value: 1.57542G

File Source
File: ...lexcsac_5mhz70db.dat
Repeat: No

File Source
File: ...221204_5mhzfinal.dat
Repeat: No

Signal Source
Sample Rate: 5M
Waveform: Constant
Frequency: 0
Amplitude: 0
Offset: 0

Float To Complex

UHD: USRP Sink
Device Address: add...68.10.4
Mb0: Clock Source: External
Mb0: Time Source: External
Mb1: Clock Source: MIMO Cable
Mb1: Time Source: MIMO Cable
Samp Rate (Sps): 5M
Ch0: Center Freq (Hz): ...42G
Ch0: Gain Value: 0
Ch1: Center Freq (Hz): 0
Ch1: Gain Value: 0
TSB tag name:

Figure 4.10: GNURadio program for MIMO setup.

Our hardware equipment with their respective connections is shown in Fig. 4.11.

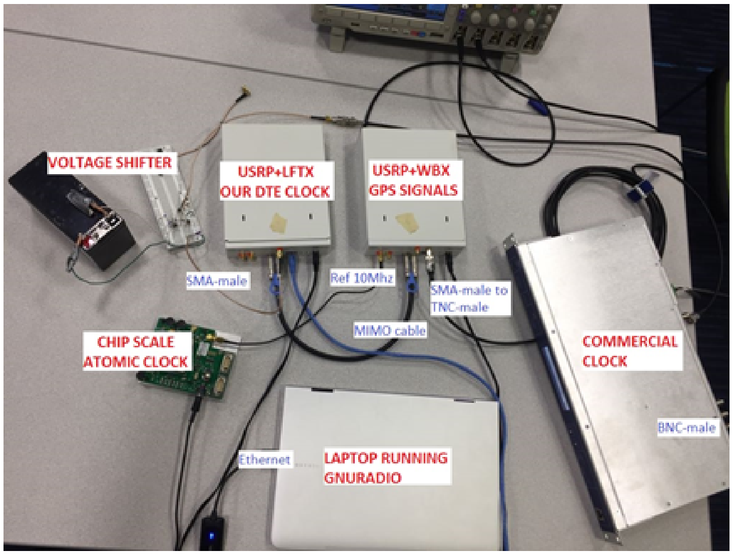
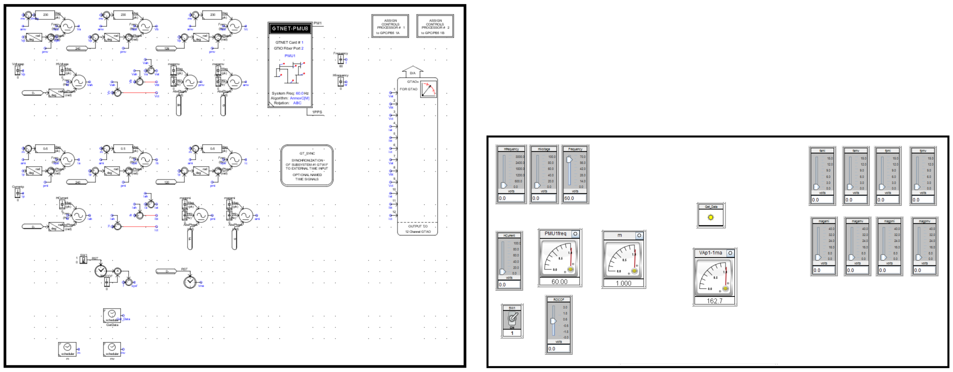


Figure 4.11: Our hardware power testbed.

The virtual test case is designed using PMU performance analyzer (PPA) [69] as shown in Fig. 4.12. PPA is a tool developed for analyzing the performance of PMU during steady-state and dynamic conditions. Step inputs of 16 units is given to voltage and 23 units is given to current, while maintaining a constant phase angle of $-89.5°$. The data is collected using OpenHistorian trending tool [70] and processed in MATLAB [71] to generate the results corresponding to different experiments.



(a)

(b)

Figure 4.12: (a) Underlying virtual circuit to generate the linear step based PMU testcase; (b) settings for PMU testcase.

CHAPTER 5

IMPACT OF TIMING ATTACKS AND ANOMALIES ON POWER GRID

In this section, we demonstrate the impact of timing attacks and GPS satellite broadcast data anomalies on the grid. According to the IEEE standard for PMU measurements, without any timing and magnitude errors, the max allowable phase angle error between two PMUs should not exceed 0.573° [11].

5.1 Jamming attacks

To test and quantify the impact of jamming and meaconing on commercial clocks (in this case, SEL-2488), we conducted experiments using our power testbed. We supplied one of the PMUs with authentic signals and the other with emulated malicious signals as shown in Fig. 5.1. Our setup is triggered using RTDS.

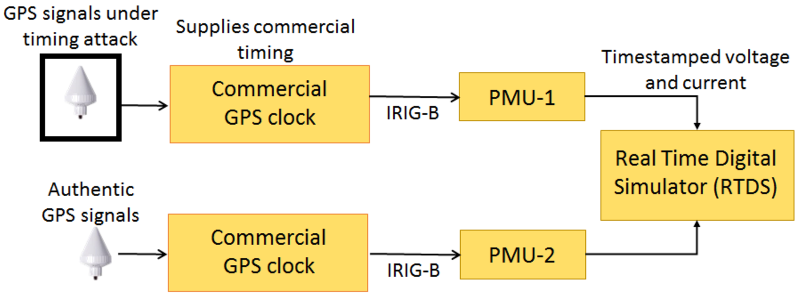

GPS signals under timing attack
Supplies commercial timing
Commercial GPS clock
IRIG-B
PMU-1
Timestamped voltage and current
Real Time Digital Simulator (RTDS)
Authentic GPS signals
Commercial GPS clock
IRIG-B
PMU-2

Figure 5.1: Setup to demonstrate the impact of timing attacks on the grid. One PMU is supplied with authentic GPS timing signals, and the other is supplied with emulated malicious signals.

To evaluate the effect of jamming, we design a GNURadio block code shown in Fig. 5.3, with a variable noise voltage to be introduced. Fig. 5.2 shows decrease in satellite signal strengths with increase in noise voltage of the jamming signal introduced.

Commercial clocks require to detect and track a minimum of 4 satellites with signal strength more than 30 *dB* above the noise floor. Based on these conditions, a jamming threshold of 11.2 V added noise voltage is computed, above which sufficient number of strong satellite signals can no longer be tracked and therefore the GPS timing is no longer available.

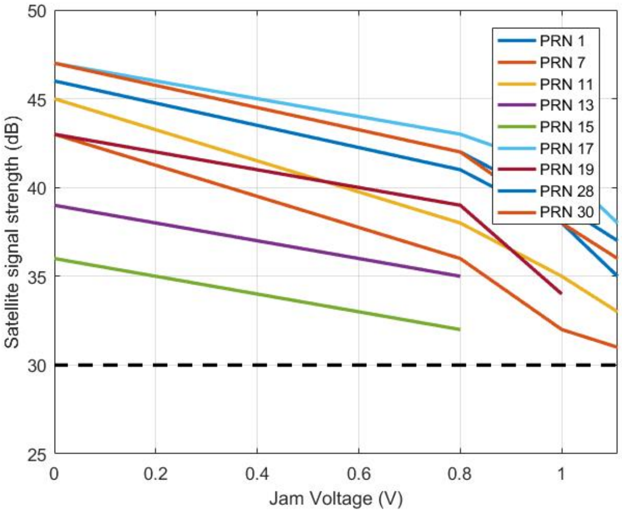
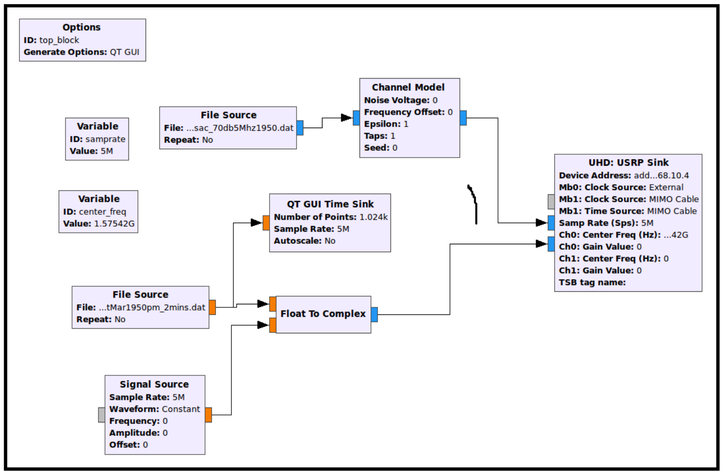


Figure 5.2: Variation of satellite signal strength with jamming. The black dotted line represents the threshold for scalar tracking as it requires a minimum of 4 satellites.



Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samprate
Value: 5M

Variable
ID: center_freq
Value: 1.57542G

File Source
File: ...sac_70db5Mhz1950.dat
Repeat: No

Channel Model
Noise Voltage: 0
Frequency Offset: 0
Epsilon: 1
Taps: 1
Seed: 0

QT GUI Time Sink
Number of Points: 1.024k
Sample Rate: 5M
Autoscale: No

UHD: USRP Sink
Device Address: add...68.10.4
Mb0: Clock Source: External
Mb1: Clock Source: MIMO Cable
Mb1: Time Source: MIMO Cable
Samp Rate (Sps): 5M
Ch0: Center Freq (Hz): ...42G
Ch0: Gain Value: 0
Ch1: Center Freq (Hz): 0
Ch1: Gain Value: 0
TSB tag name:

File Source
File: ...tMar1950pm_2mins.dat
Repeat: No

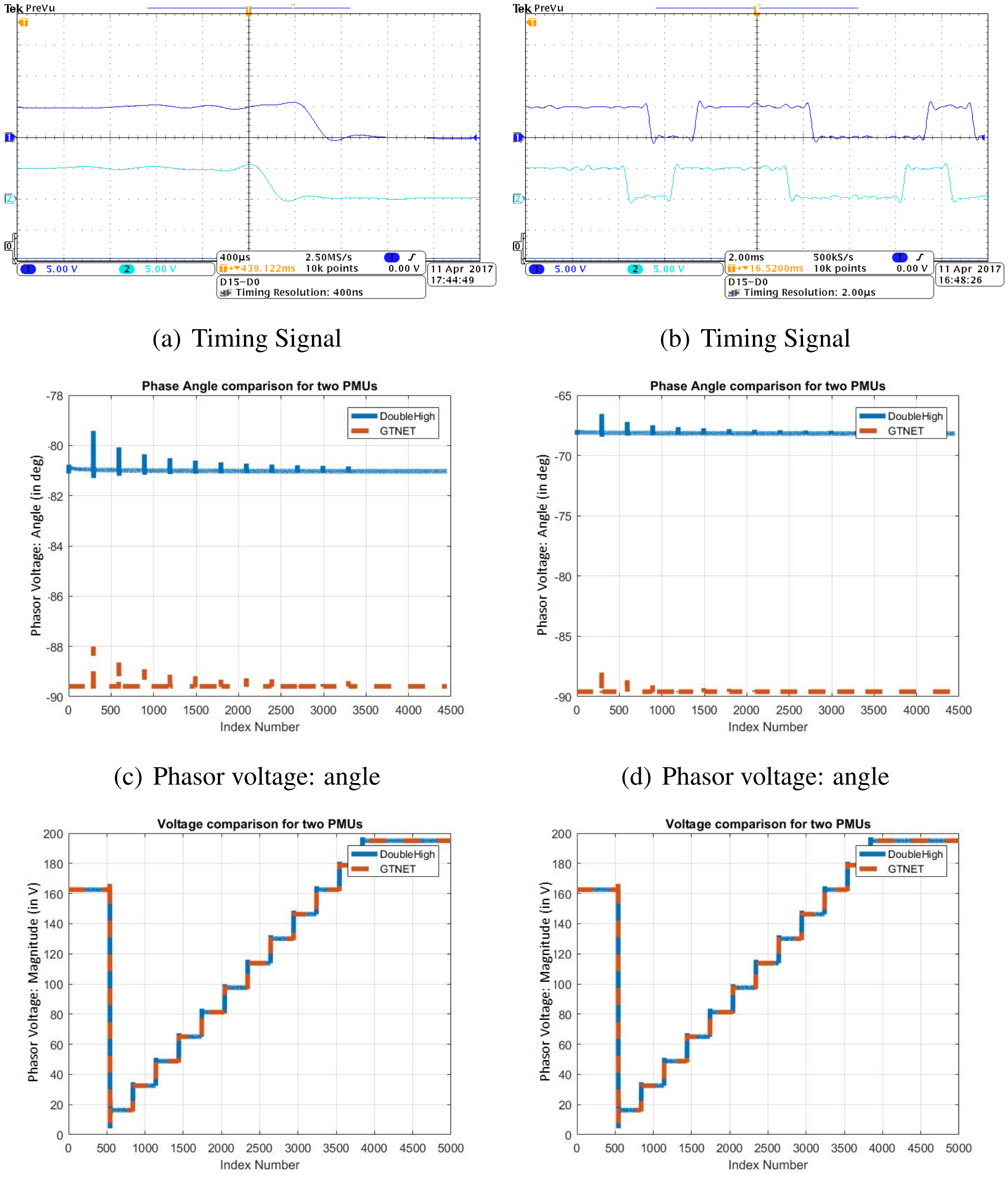
Float To Complex

Signal Source
Sample Rate: 5M
Waveform: Constant
Frequency: 0
Amplitude: 0
Offset: 0

Figure 5.3: GNURadio code to generate added jamming based GPS signal.

5.2 Meaconing attacks

Compared to jamming, meaconing is a more sophisticated and dangerous attack as it manipulates the PMU with wrong time. To illustrate the impact of meaconing attack, we introduce meaconing signals with varying delay and signal strength as shown in Fig. 5.4.



(a) Timing Signal

(b) Timing Signal

(c) Phasor voltage: angle

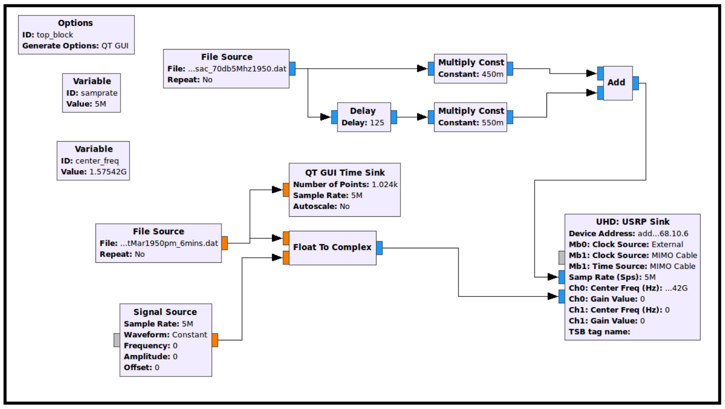
(d) Phasor voltage: angle

(e) Phasor voltage: magnitude

(f) Phasor voltage: magnitude

Figure 5.4: (a), (c), (e) plots represent meaconing attack with 4 dB higher power than authentic signals and a delay of 400 μs; (b), (d), (f) represent meaconing attack with 4 dB higher power than authentic signals and a delay of 1000 μs.

To compute the dependency of delay introduced by meaconing attack on PMU phase angle, we designed GNURadio block code to simulate meaconing attacks as shown in Fig. 5.5. We observe a linear increase in phase angle difference observed by PMUs, with increase in the delay introduced in Fig. 5.6. Therefore, when the current power system is transferred to an automated smart grid in future, GPS timing attacks will be of high threats to the power grid stability.



Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samprate
Value: 5M

Variable
ID: center_freq
Value: 1.57542G

File Source
File: ...sac_70db5Mhz1950.dat
Repeat: No

Delay
Delay: 125

Multiply Const
Constant: 450m

Multiply Const
Constant: 550m

Add

QT GUI Time Sink
Number of Points: 1.024k
Sample Rate: 5M
Autoscale: No

File Source
File: ...tMar1950pm_6mins.dat
Repeat: No

Float To Complex

Signal Source
Sample Rate: 5M
Waveform: Constant
Frequency: 0
Amplitude: 0
Offset: 0

UHD: USRP Sink
Device Address: add...68.10.6
Mb0: Clock Source: External
Mb1: Clock Source: MIMO Cable
Mb1: Time Source: MIMO Cable
Samp Rate (Sps): 5M
Ch0: Center Freq (Hz): ...42G
Ch0: Gain Value: 0
Ch1: Center Freq (Hz): 0
Ch1: Gain Value: 0
TSB tag name:

Figure 5.5: GNURadio code for generating the meaconing signal.

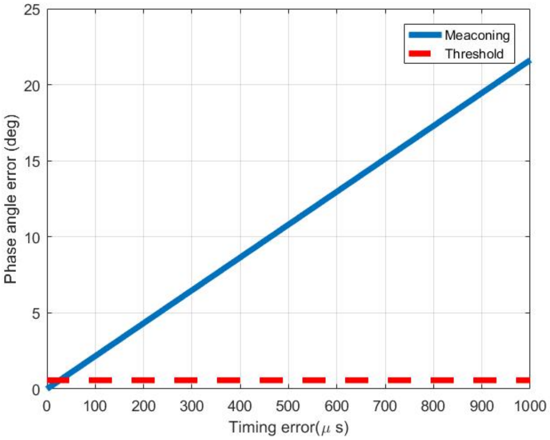


Figure 5.6: Variation of phase angle difference with delay introduced by meaconing attack. A linear increase in the phase angle difference is observed with increase in delay introduced.

5.3 GPS satellite data anomaly: a case study on January 26, 2016

In addition to the timing attacks namely jamming and meaconing, GPS satellite broadcast data anomalies also affect the robustness of the WAMS. The impact of the data anomalies on the stability of the grid is discussed in this section.

5.3.1 Causes of the anomaly

On January 26, 2016, a temporary error was triggered in the data upload system of GPS due to the decommissioning of the GPS satellite SV-23 [72]. This anomaly caused incorrect data to be transmitted from the satellites on the commercial $L1$ band used by most of the commercial GPS receivers. Satellites reportedly transmitting the erroneous parameters were PRN: 2, 6, 7, 9 and 23.

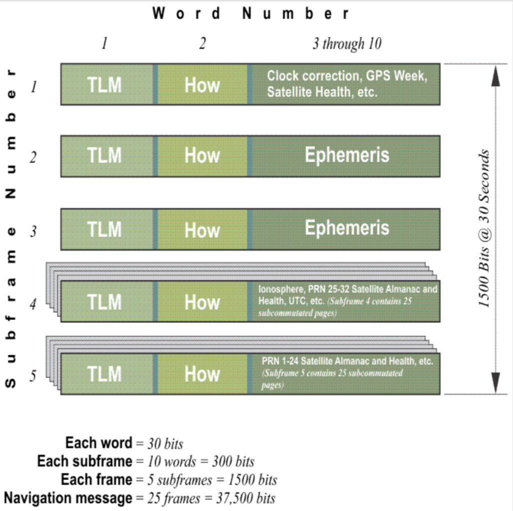
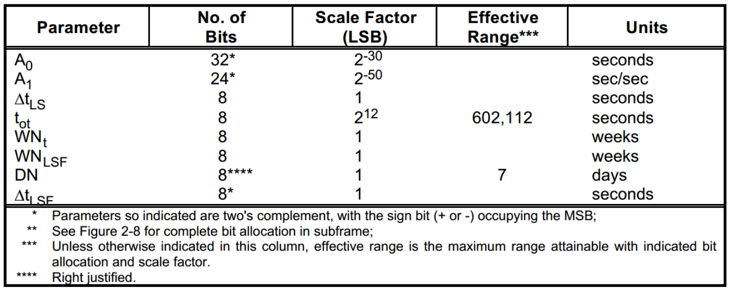

Word Number
1
2
3 through 10
Subframe Number
1
TLM
How
Clock correction, GPS Week, Satellite Health, etc.
2
TLM
How
Ephemeris
3
TLM
How
Ephemeris
4
TLM
How
Ionosphere, PRN 25-32 Satellite Almanac and Health, UTC, etc. (Subframe 4 contains 25 subcommutated pages)
5
TLM
How
PRN 1-24 Satellite Almanac and Health, etc. (Subframe 5 contains 25 subcommutated pages)
1500 Bits @ 30 Seconds
Each word = 30 bits
Each subframe = 10 words = 300 bits
Each frame = 5 subframes = 1500 bits
Navigation message = 25 frames = 37,500 bits

Figure 5.7: Navigation message structure of GPS signals showing the information broadcast by GPS satellites.

GPS navigational message as shown in Fig.5.7 contains information of satellite time of transmission, ephemeris, satellite health, satellite clock correction, propagation delay effects (due to signal propagation in ionosphere and troposphere), time transfer to UTC, GPS satellite constellation health status. The subframe 4 of the navigation message as shown in Fig. 5.8 transmits the ionospheric correction parameters, UTC parameters and the almanac data. During the anomaly, the UTC parameters (t_{ot}, WN_t, A_0) decoded from specific affected satellites mentioned above were wrong.



Parameter	No. of Bits	Scale Factor (LSB)	Effective Range***	Units
A_0	32*	2^{-30}		seconds
A_1	24*	2^{-50}		sec/sec
Δt_{LS}	8	1		seconds
t_{ot}	8	2^{12}	602,112	seconds
WN_t	8	1		weeks
WN_{LSF}	8	1		weeks
DN	8****	1	7	days
Δt_{LSF}	8*	1		seconds

* Parameters so indicated are two's complement, with the sign bit (+ or -) occupying the MSB;
** See Figure 2-8 for complete bit allocation in subframe;
*** Unless otherwise indicated in this column, effective range is the maximum range attainable with indicated bit allocation and scale factor.
**** Right justified.

Figure 5.8: UTC parameters broadcast by GPS satellites.

The UTC parameters are useful for applications in which synchronization of time is essential such as in power grids. The relation between UTC and GPS time is computed as follows:

$$\begin{aligned}
t_{UTC} &= mod((t_E - \Delta t_{UTC}), 86400) \\
\Delta t_{UTC} &= \Delta t_{LS} + A_0 + A_1(t_E - t_{ot} + 604800(WN - WN_t)) \\
t_E &: \text{GPS time as estimated by the user} \\
\Delta t_{LS} &: \text{delta time due to leap seconds} \\
A0, A1 &: \text{constant and first order terms of polynomial} \\
t_{ot} &: \text{reference time for UTC data} \\
WN &: \text{current week number (derived from subframe 1)} \\
WN_t &: \text{UTC reference week number}
\end{aligned} \tag{5.1}$$

5.3.2 Results and analysis

In this section, different GPS receivers across America are analyzed and the broadcast satellite data are compared with the correct ephemeris data to understand the impact of the GPS satellite data anomaly on different users.

A high-end GPS receiver :

A high-end trimble GPS receiver is mounted on the rooftop of Talbot Laboratory at UIUC. This is a highly precise instrument and can give an accuracy of upto centimeter level. In the table below, the data files of Trimble receiver on January 26, 2016 are compared with that of February 22, 2016.

Table 5.1: UTC parameters decoded by the Trimble receiver on the rooftop of Talbot Laboratory at UIUC. The parameters decoded on January 26, 2016 show an error of 13.7 μs

Date	**UTC.A0**	**UTC.A1**	T_{ot}	WN_t
February 23, 2016	0	-5.3291e-15	319488	1881
February 22, 2016	3.7253e-09	8.8818e-15	319488	1881
January 22, 2016	**-13.696e-06**	**1.2434e-14**	**0**	**0**

We observe from Table. 5.1, that an error has been detected by the Trimble receiver similar to the error reported by various GPS receivers across the world.

This shows that UTC parameters being transmitted were indeed corrupted.

Continuously Operating Reference Station (CORS):

We considered the stations in Colorado, given that the Master Control Station (MCS) is located in Colorado Springs. For comparison, the closest CORS network station (ILUC) to UIUC is also listed [73]. Unlike the broadcast data received by the Trimble receiver, CORS receivers are referenced to the correct navigation parameters obtained from International GNSS Service (IGS) network [74]. Instead of an error of 13.7 μs in timing parameters, we see from Table. 5.2, that the CORS network is not affected.

Table 5.2: UTC Parameters decoded by CORS receivers. CORS receivers are referenced to the correct navigation data obtained from IGS network and hence do not show the anomaly.

Location	**UTC.A0**	**UTC.A1**	T_ot	WN_t
Cannon City, Colorado	9.3132e-10	5.3291e-15	319488	1881
Pueblo, Colorado	9.3132e-10	5.3291e-15	319488	1881
Urbana, Illinois	9.3132e-10	5.3291e-15	319488	1881

5.3.3 Impact on Power grid

Fig. 5.9 depicts the difference in the position between the case when corrupted UTC parameters were used to the case when actual UTC parameters were used. We observe that no significant effect on the navigation solution can be seen. Thus, the normal commercial users did not face any problem.

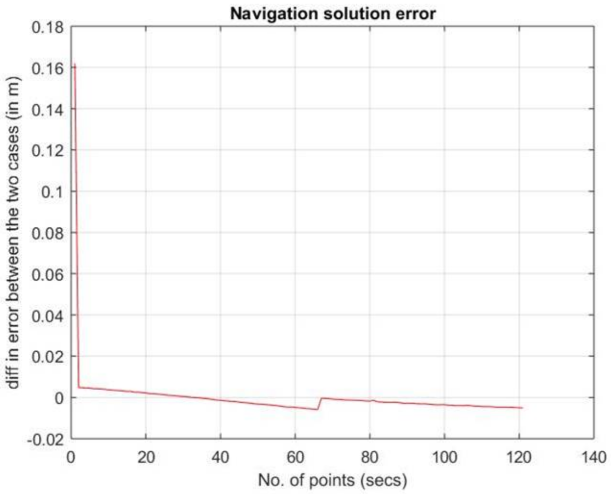


Figure 5.9: Negligible error in navigation solution. GPS satellite data anomaly does not affect the position calculated. However, we will show in Fig. 5.10 that a significant error of 13.7 μs is observed in the calculation of UTC time.

The Fig. 5.10 shows the comparison between the two scenarios: One where the time difference is computed between the original UTC of London and user calculated UTC from GPS time using correct UTC parameters and the second case where this difference is calculated using corrupted UTC parameters.

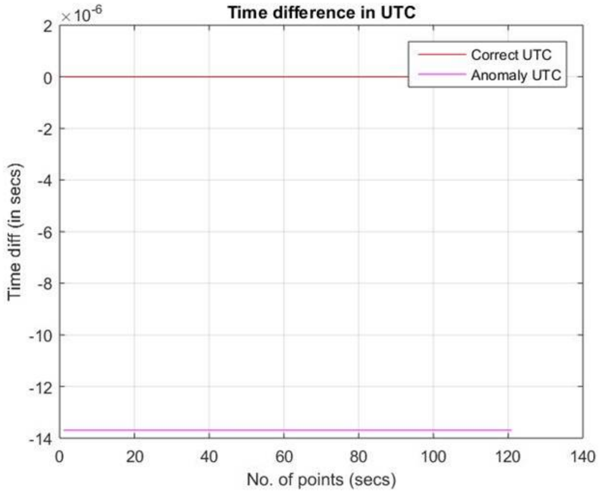


Figure 5.10: Significant error of 13.7 μs in the calculation of UTC time.

To summarize, we see that an error of 13.7 μs does not affect the position accuracy to a great extent. However, in the case of power grid an error in 13.7 μs results in a phase angle difference of 1° which is a significant error according to the IEEE C37.118 standard.

CHAPTER 6

RESULTS AND ANALYSIS

In our verification and validation experiments, attack resiliency of our proposed GPS algorithms is compared to the existing techniques, such as PIAVT and scalar tracking. Our analysis is categorized into 3 sections of experiments as follows:

1. GPS field experiments conducted using the setup described in Section 4.1 to analyze the robust competency of our SR-DTE and MR-DTE algorithms in tracking the GPS signal parameters correctly.

2. Our power testbed experiments to analyze the improved stability of power grid at the PMU level.

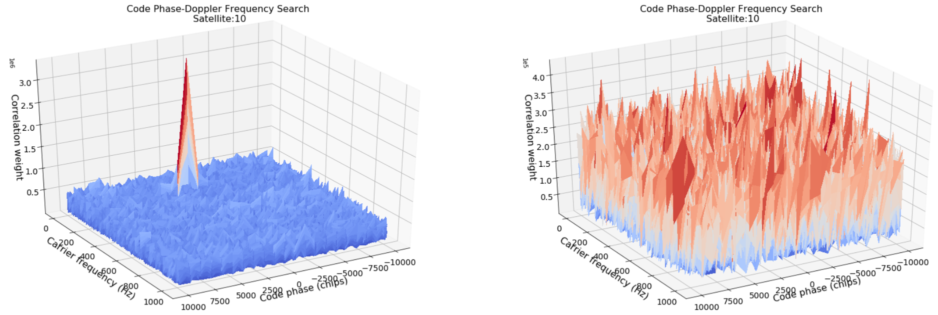
6.1 GPS Robustness Analysis

6.1.1 Single-Receiver Direct Time Estimation (SR-DTE)

We test the performance of SR-DTE as compared to scalar tracking while subjected to external timing attack scenarios.

Jamming

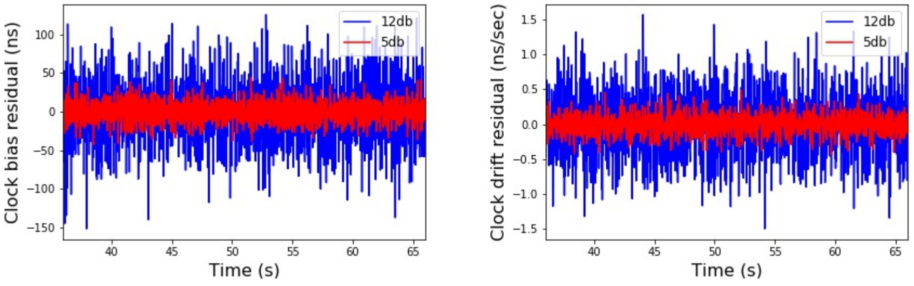
The conditions of jamming are generated by adding an additional white Gaussian noise $Ae^{j2\pi\phi t}$ to the incoming received signal as shown in Fig. 6.1(a). The noisy jamming signal includes two components: amplitude A which is a measure of the strength of the noise being introduced and random phase ϕ. Before the addition of noise, there is a clear peak as shown in Fig.6.1(a) but after the addition of 12 dB noise, the peak falls below the noise floor as shown in Fig. 6.1(b).



(a) (b)

Figure 6.1: Jamming attack effect: (a) Authentic case with distinct peak above noise floor; (b) 12*dB* of added jamming case with no distinct peak above noise floor.

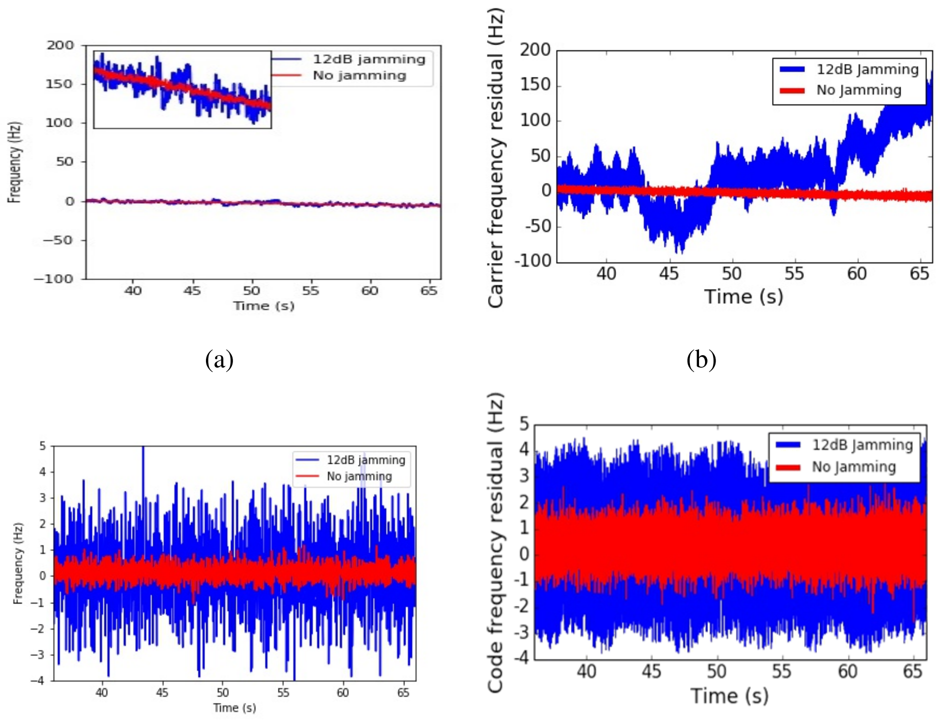
The clock bias and clock drift residuals of SR-DTE are compared with scalar tracking in Fig. 6.7. For 5 *dB* of added jamming, the clock bias is less than 25 *ns* and clock drift residual of 0.25 ns/s. Furthermore, we observe that even under 12 *dB* of added jamming, the clock bias residual is less than 150 *ns* and the clock drift residual of less than 1.5 ns/s.



(a) (b)

Figure 6.2: Resiliency of SR-DTE with 5 *dB* and 12 *dB* added jamming; (a) clock bias residual; (b) clock drift residual. Even with 12 *dB* of added jamming, clock bias residual is within 150 *ns* and clock drift residual within 1.5 ns/s.

Under an added jamming attack of 12 *dB*, Fig. 6.3 shows that the scalar tracking lost the lock while SR-DTE still maintains robust tracking. Additional offline experiments verified that the SR-DTE algorithm remains robust till 14.2 *dB* of added jamming thereby providing 2.2 *dB* of increased noise tolerance.



(a)

(b)

(c)

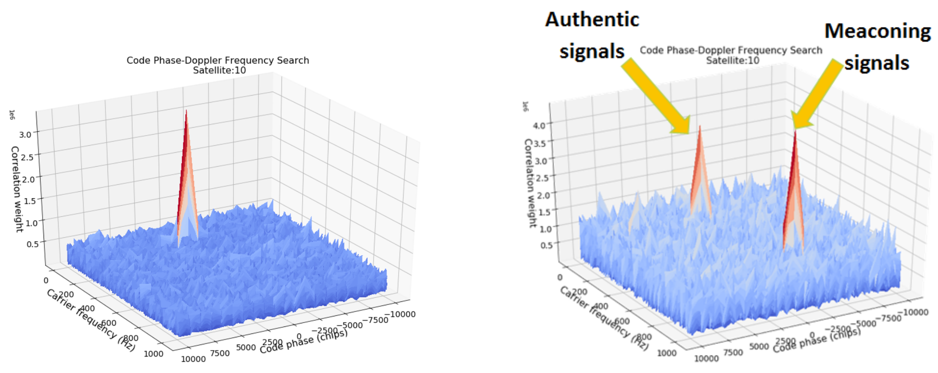
(d)

Figure 6.3: (a) Carrier doppler frequency residual using SR-DTE; (b) carrier Doppler residual using scalar tracking; (c) code frequency residual using SR-DTE; and (d) code frequency residual using scalar tracking. Scalar tracking loses track at 12 *dB* of added noise, whereas SR-DTE still remains robust.

Meaconing

In this case, a replay signal with similar GPS signal structure and signal power 2.3 *dB* greater than the authentic signal is added to the incoming GPS signal. The first 36 *s* uses scalar tracking, after which the spurious signal is introduced. At this point we turn on the SR-DTE algorithm and compare its performance to that of scalar tracking for the next 30 *s*.

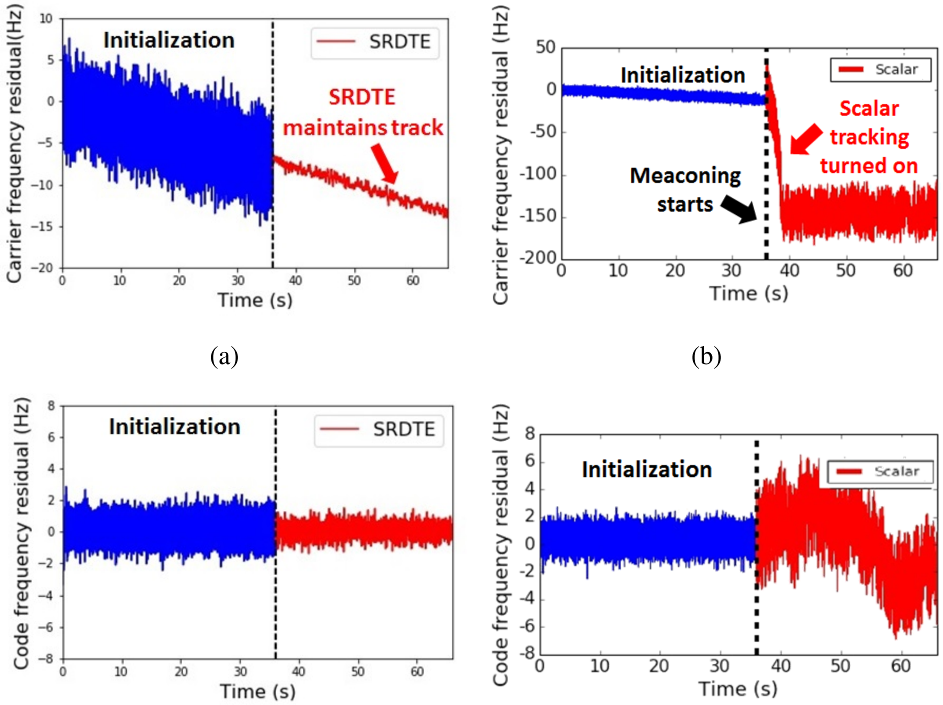
The correlation plots in Fig. 6.4(b) show the presence of both meaconing and authentic signals. The meaconing signals which is of higher power than the authentic signals is tracked by scalar tracking thereby estimating wrong time information.



(a)

(b)

Figure 6.4: Meaconing attack effect: (a) Authentic case with distinct peak above noise floor; (b) meaconing case with two distinct peaks above noise floor: one corresponds to the authentic signals, while the other stronger peak corresponds to meaconed signal.



(a)

(b)

(c)

(d)

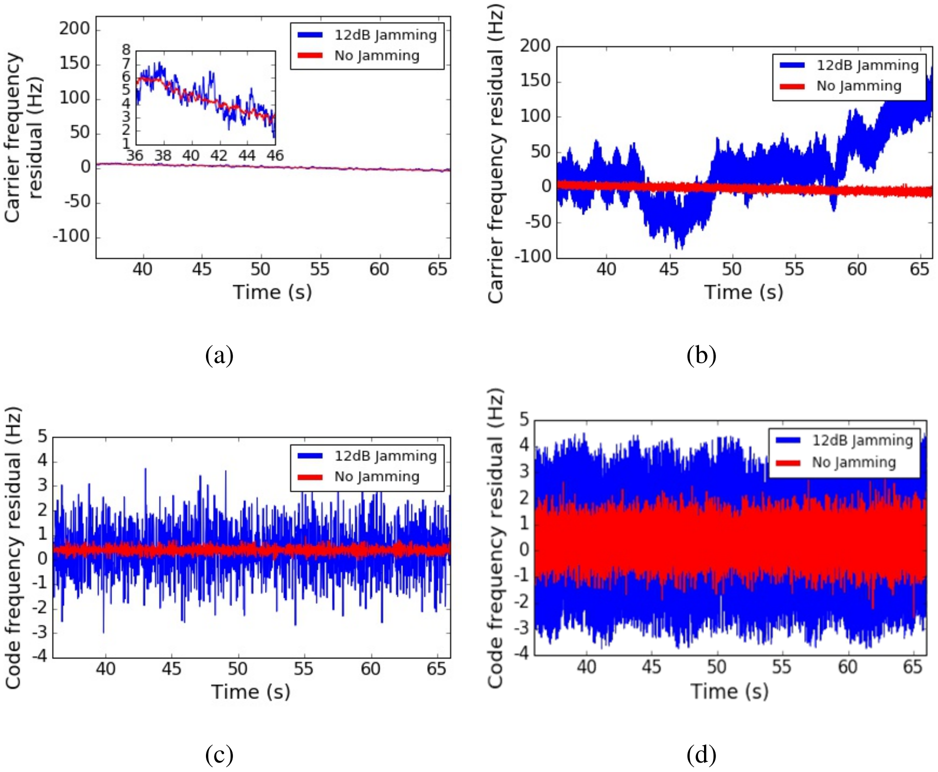
Figure 6.5: (a) Carrier Doppler frequency residual for SR-DTE; (b) carrier Doppler frequency residual for scalar tracking; (c) code frequency residual for SR-DTE; and (d) code frequency for scalar tracking. Scalar tracking locks onto the meaconed signal whereas SR-DTE maintains lock onto the legitimate one.

We observe in Fig. 6.5 that scalar tracking locks on the meaconing signal and continues to track the malicious signal while the SR-DTE tracks the authentic signal. Our SR-DTE algorithm is able to sustain a meaconing signal with 1.3 *dB* higher power than the authentic signals.

6.1.2 MR-DTE

Jamming

In the case of jamming, Fig. 6.6 is indicative of the robustness of the MR-DTE algorithm. In the presence of 12 *dB* added noise, the scalar tracking loses track. However, the MR-DTE continues to track the authentic signal accurately.



(a)

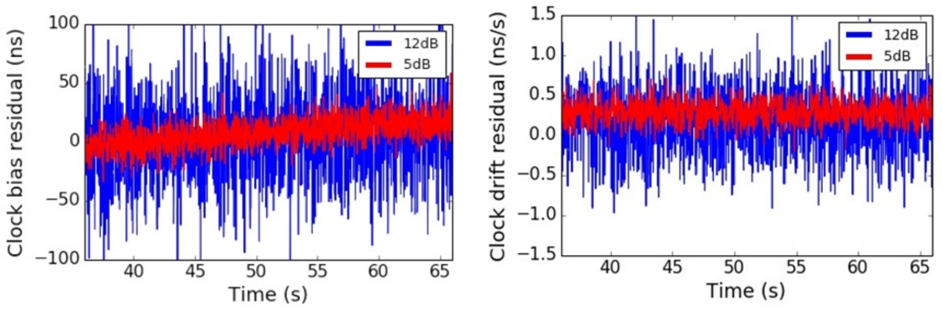
(b)

(c)

(d)

Figure 6.6: (a) Carrier Doppler frequency residual using MR-DTE; (b) carrier Doppler residual using scalar tracking; (c) code frequency residual using MR-DTE; and (d) code frequency residual using scalar tracking. Scalar tracking loses track at 12 *dB* of added noise, whereas MR-DTE still remains robust.

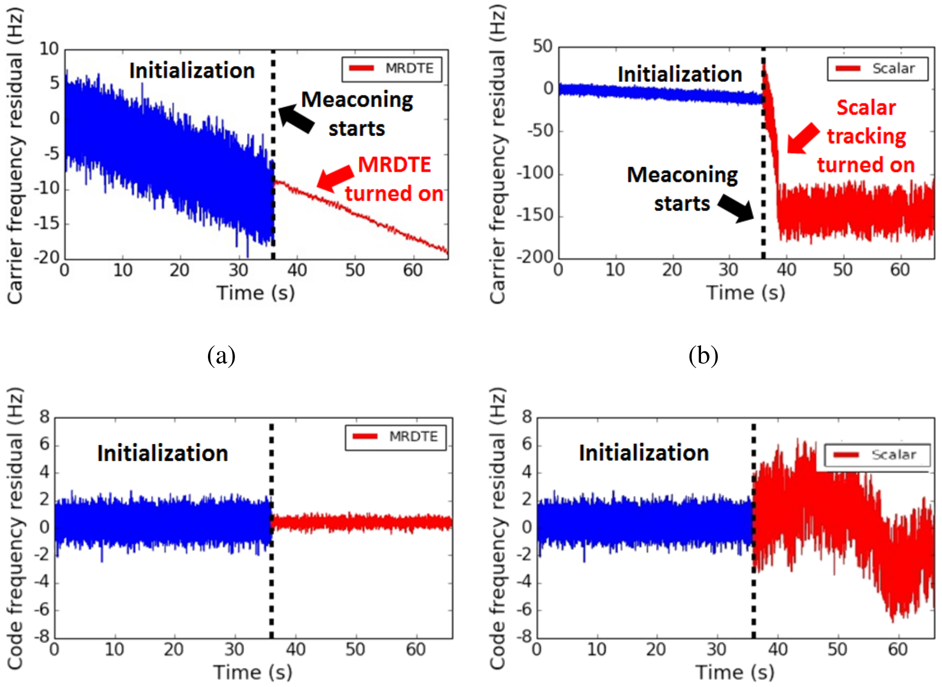
In Fig. 6.7, the clock bias and clock drift residuals are compared for added noise with respect to the signal noise floor. In the presence of 5dB added noise, the clock bias is estimated with an error of within 10 *ns* and in case of 12 *dB* added noise within an error of 100 *ns*. The jamming threshold for MR-DTE is calculated as 17 *dB* which is 5 *dB* higher than traditional scalar tracking. Thus a more robust clock state is estimated by implementing MR-DTE algorithm.



(a) (b)

Figure 6.7: (a) Clock bias residual comparison for 5 *dB* and 12 *dB* of added noise; and (b) clock drift comparison for 5 *dB* and 12 *dB* of added noise. Even with 12 *dB* of added jamming, clock bias residual is within 100 *ns* and clock drift residual within 1.5 *ns*/*s*.

Meaconing



(a) (b)

(c) (d)

Figure 6.8: (a) Carrier Doppler frequency residual for MR-DTE; (b) carrier Doppler frequency residual for scalar tracking; (c) code frequency residual for MR-DTE; and (d) code frequency for scalar tracking. Scalar tracking locks onto the meaconed signal whereas MR-DTE maintains lock onto the legitimate one.

When meaconing signal of 3 *dB* higher power than authentic signals is added, the scalar tracking locks onto the counterfeit signal as shown in Fig. 6.8 whereas the MRDTE still consistently tracks the authentic signal and mitigates the effect of meaconing attack.

In accordance with the experimental results shown in Table. 6.1, MR-DTE has a higher threshold to both jamming and meaconing attacks. Under added jamming, MR-DTE has 2.8 *dB* higher tolerance than SR-DTE and 5 *dB* higher tolerance than scalar tracking. In the presence of meaconing attack, MR-DTE offers 0.7 *dB* more tolerance than SR-DTE and 2 *dB* more tolerance than the scalar tracking.

Table 6.1: Threshold of various GPS algorithms to timing attacks. Here, the timing attacks are emulated in pyGNSS. MR-DTE offers higher tolerance to jamming and meaconing attacks than SR-DTE, PIAVT and scalar tracking.

Algorithm	**Jamming (in *dB*)**	**Meaconing (in *dB*)**
Scalar	12	1
SR-DTE	14.2	2.3
MR-DTE	**17**	**3**

6.2 Stability analysis of the Power Grid

To validate attack resilience of our multi-receiver setup at the power grid level, we analyzed the TVE error of PMU by recording the voltage, current and phase angle measurements. The power testbed described in Section 4.2 is used for conducting the experiments. In the experiments below, the PMU labelled "GTNET" is the reference one which always supplies the authentic signals and the PMU labelled "Double High"is the one attacked by the malicious GPS signals. The experiments are conducted using GPS signals collected on the rooftop of ECE building and are different from the GPS signals analyzed in Section 6.1

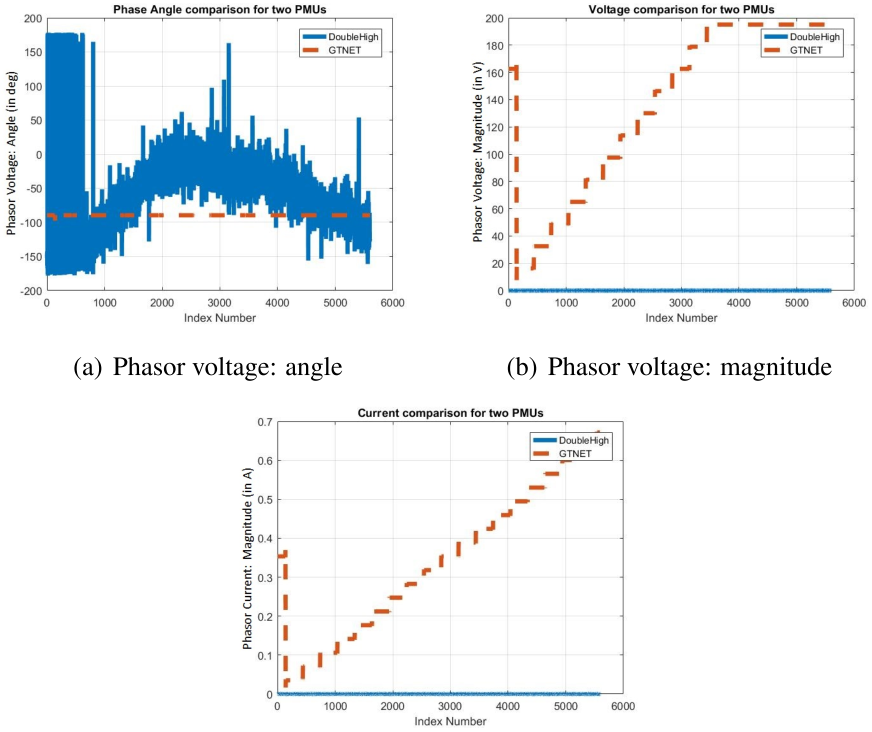
We calibrated the PMUs to account for any initial offsets in the measurements recorded. One of the PMUs receives the IRIG-B timing signals generated by supplying authentic GPS signals (using USRP+WBX). Similarly, the other PMU is triggered using the USRP+LFTX that supplies the authentic pyGNSS based scalar tracking signals. Based on this, the PMU measurements are calibrated to an accuracy of around 0.005°.

Table 6.2: Threshold of various algorithms to external attacks. Here, the timing attacks are emulated in GNURadio. MR-DTE offers higher tolerance to jamming and meaconing attacks than SR-DTE, PIAVT and scalar tracking.

Algorithm	**Jamming (in V)**	**Meaconing (in dB)**
Scalar	1.12	1
PIAVT	1.6	1.4
SRDTE	2.1	2.01
MRDTE	3.4	4.2

Jamming

For the jamming case, a 11.2 V added noise voltage is mixed with authentic signals and the results are analyzed. We observe from Table. 6.2 that MR-DTE has higher threshold to jamming which can be verified through Fig. 6.9. In the case of jamming, the GPS timing information is unavailable for one of the PMUs because of which the voltage and current measurements recorded are zero while the phase angle fluctuates randomly.

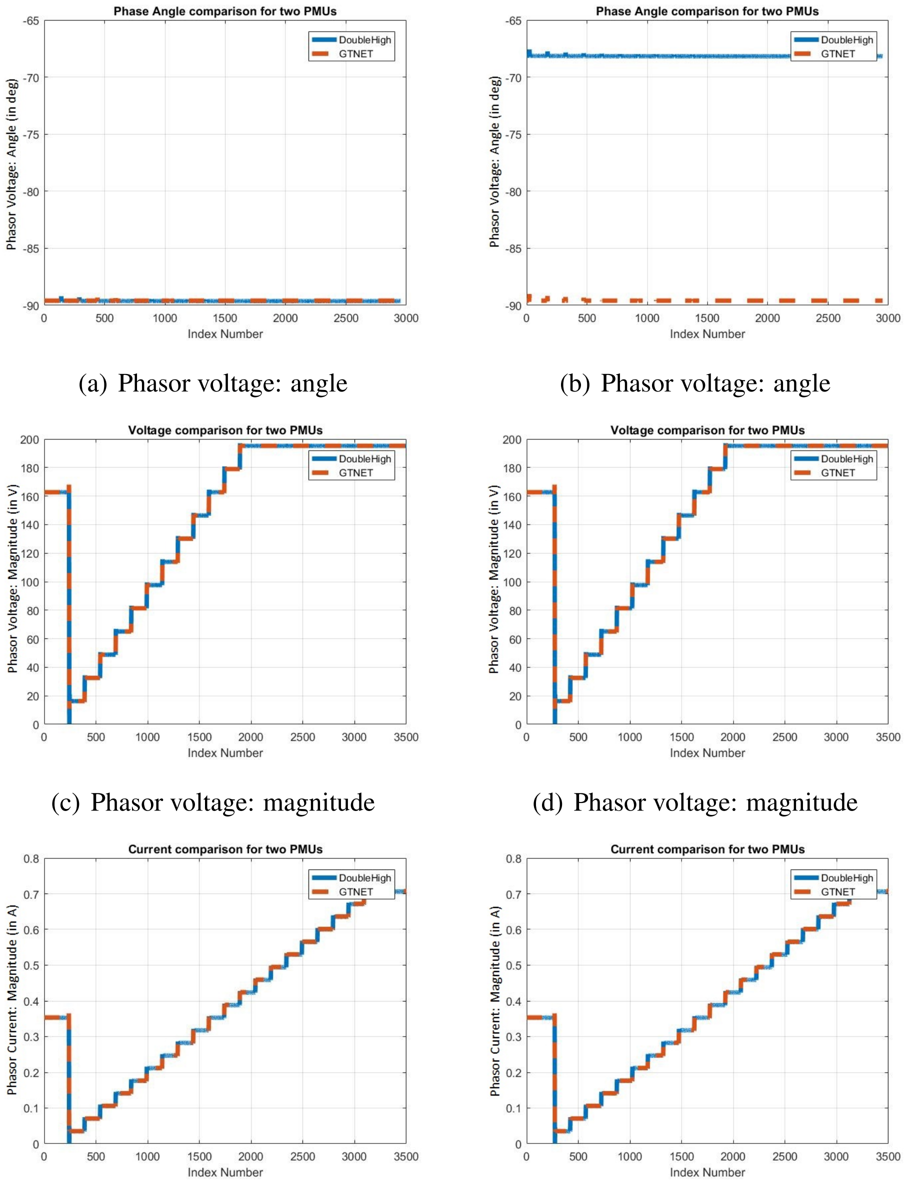


(a) Phasor voltage: angle

(b) Phasor voltage: magnitude

(c) Phasor current: magnitude

Figure 6.9: Phasor measurements under jamming attack. The red dotted line corresponds to the unjammed GTNET PMU, while the blue solid line represents the jammed Double High PMU. The phase angle difference is 21° which violates th IEEE C37.118 standard for PMU measurements.



(a) Phasor voltage: angle

(b) Phasor voltage: angle

(c) Phasor voltage: magnitude

(d) Phasor voltage: magnitude

(e) Phasor current: magnitude

(f) Phasor current: magnitude

Figure 6.10: (a), (c), (e) denote measurements for the authentic case without meaconing; (b), (d), (f) denotes the measurements for the case where one of the PMU experiences external timing attacks. The IEEE C37.118 standard is violated in phase angle measurements of (b) as compared to (a).

Meaconing

We introduced a meaconing signal with delay of 1000 μs as compared to the authentic signal. The strength of the meaconing signal is varied and the Table. 6.2 shows the thresholds of various algorithms. We observe that the MR-DTE can sustain 4.2 dB of higher powered meaconing signal followed by SR-DTE which sustains 2.01 *dB* and lastly PIAVT and scalar tracking which can sustain 1.4 *dB* and 1 *dB* respectively. Fig. 6.10 shows the current, voltage and phase angles for both cases. The plots on left shows the accurate synchronization between PMUs under non-timing attack conditions whereas the plots on the right depicts the timing attack case where unsynchronized PMU data is observed with a phase angle error of 20° thereby violating the IEEE C38.117 standard for synchrophasors.

CHAPTER 7

SUMMARY AND FUTURE WORK

To summarize, we have proposed MR-DTE, a robust GPS algorithm to improve the resiliency of the power grid against external timing attacks. We implement DTE based signal processing technique. DTE directly correlates the incoming GPS signal with the cumulative satellite signal replica for a pre-generated set of clock candidates, and compute the maximum likelihood timing parameters.

MR-DTE utilizes multiple static receivers sharing a common clock. We leverage the geographical diversity and information redundancy of the multiple receivers to improve the inherent robustness of the system. Our multi-receiver protection scheme enables higher tolerance levels for WAMS thereby allowing continued operation in the presence of 17 *dB* of added jamming and meaconing attack of 3 *dB*.

We designed a virtual power grid test platform using RTDS, USRP, PMU and a commercial GPS clock to showcase the impacts of satellite broadcast data anomalies, jamming and meaconing attacks. Through the emulated timing attacks to the GPS signals collected, we demonstrated the increased resilience of MR-DTE both at the GPS level by tracking the signal parameters correctly and at the power grid level by analyzing the power grid stability. The results of these experiments highlight the attack resilience of our proposed MR-DTE algorithms, while simultaneously maintaining GPS timing with accuracy that satisfies the IEEE C37.118 standards.

For future work, we propose to improve the robustness of PMUs against meaconing attack by incorporating new protective measures to our existing MR-DTE platform. We plan to further design and develop a spoofer localization scheme to counteract these attacks, thereby advancing the resiliency of power grids.

REFERENCES

[1] J. Hazra, R.K. Reddi, K. Das, P. Seetharam, “Power Grid Transient Stability Prediction Using Wide Area Synchrophasor Measurements”, 3rd IEEE PES Innovative Smart Grid Technologies, 2012.

[2] R.O. Burnett, M.M. Butts, P.S. Sterlina, “Power system applications for phasor measurement units”, IEEE Computer Applications in Power, 1994.

[3] P. Kundur, N. J. Balu, and M. G. Lauby, “Power system stability and control”, McGraw-hill New York, 1994, vol. 7.

[4] Schweitzer Engineering Laboratories, “Improve Data Analysis by TimeStamping Your Data, The Synchrophasor Report, May 2009, vol. 1, no. 3. Retrieved June 14, 2015 from https://www.selinc.com/issue3/.

[5] S. Sridhar, A. Hahn, M. Govindarasu, “Cyber-Physical System Security for the Electric Power Grid”, in Proceedings of the IEEE, 2012.

[6] Y. Ota, H. Ukai, K. Nakamura, H. Fujita, “Evaluation of Stability and Electric Power Quality in Power System by using Phasor Measurements”, in Proceedings 2000 International Conference Power System Tecnology (PowerCon2000), vol.3, December 2000, pp.1335-1340.

[7] P. Misra and P. Enge, “Global Positioning System: Signals, Measurements and Performance”, Second Edition. Lincoln, MA: Ganga-Jamuna Press, 2006.

[8] Sam Pullen and Grace Xingxin Gao, “GNSS Jamming in the Name of Privacy: Potential Threat to GPS Aviation”, Inside GNSS Magazine, March-April 2012.

[9] J. Huang, L. Du, Q. Liu, “Application of IRIG-B Code in Phase Measurement Unit”, in Power and Energy Engineering Conference (APPEEC), 2012.

[10] “IEEE Standard for Synchrophasors for Power Systems,” IEEE Std C37.118-2005 (Revision of IEEE Std 1344-1995) , vol., no., pp.0_1-57, 2006.

[11] K.E Martin, D.Hamai, M.G Adamiak, S. Anderson, M. Begovic, G. Benmouyal, G. Brunello, J. Burger, J. Y. Cai, B. Dickerson, V. Ghapure, B. Kennedy, D. Karlsson, A.G. Phadke, J. Salj, V. Skendizic, J. Sperr, Y. Song,

C. Huntley, B. Kastenny and E. Price, “Exploring the IEEE Standard C37.118-2005 Synchrophasors for Power Systems, IEEE Trans. on Power Del.,Vol. 23, no. 4, pp 1805-1811, Oct, 2008.

[12] M. Lixia, C. Muscas, and S. Sulis, “On the accuracy specifications of phasor measurement units, in Proc. IEEE I2MTC, May 2010, pp. 14351440.

[13] J. Bhatti, T. Humphreys, “Hostile control of ships via false GPS signals: Demonstration and detection”, Navigation, 2016.

[14] M. L. Psiaki and T. E. Humphreys, “GNSS Spoofing and Detection”, in Proceedings of IEEE, 2016, 104, 1258-1270.

[15] D. P. Shepard and T. E. Humphreys, “Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks”, in International Journal of Critical Infrastructure Protection, 5(3-4), 146153.

[16] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, “Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer, in Proceedings of the Institute of NavigationInternational Technical Meeting (ITM ’09), pp. 124130, Anaheim, Calif, USA, January 2009.

[17] L. Zhan, Y. Liu, W. Yao, J. Zhao and Y. Liu, “Utilization of Chip-Scale Atomic Clock for Synchrophasor Measurements”, in IEEE Transactions on Power Delivery, 2016.

[18] C. T.-C. Nguyen, J. Kitching, “Towards chip-scale atomic clocks”, in Proceedings of IEEE International Solid-State Circuits Conference, 2005.

[19] W. Blass, A. Hennigar and S. Mao, “Implementation of a Software-Defined Radio based Global Positioning System Repeater”, in ASEE Southeast Section Conference, 2015.

[20] R. Di, “A USRP-Based Flexible GNSS Signal Recording and Playback System: Performance Evaluation and Study.” (Electronic Thesis or Dissertation). Retrieved from https://etd.ohiolink.edu/, 2013.

[21] S. Z. Jian Chen and H. Wang, “Practicing a Record-and-Replay System on USRP, IEEE Trans. Wireless Commun., May 2013.

[22] D. Chou, L. Heng, and G. X. Gao, “Robust GPS-Based Timing for Phasor Measurement Units: A Position-Information-Aided Vector Tracking Approach, in Proceedings of the ION GNSS+ conference, Tampa, 2014.

[23] D. Chou, Y. Ng, and G. X. Gao, “Robust GPS-Based Timing for PMUs Based on Multi-Receiver Position-Information-Aided Vector Tracking”, in Proceedings of the ION ITM conference, Dana Point, 2015.

[24] Y. Ng and G. X. Gao, "Robust GPS-Based Direct Time Estimation for PMUs" in Proceedings of the IEEE/ION PLANS conference, Savannah, 2016.

[25] S. Bhamidipati, Y. Ng and G. X. Gao, "Multi-Receiver GPS-based Direct Time Estimation for PMUs", in Proceedings of the ION GNSS+ conference, Portland, 2016.

[26] National Electric Sector Cybersecurity Organization Resource (NESCOR), "Electric Sector Failure Scenarios and Impact Analyses", 2013

[27] "New York Times", [Online]. Available: http://www.nytimes.com/2003/08 /15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html, 2003.

[28] "Sun Daily News", [Online]. Available: http://www.thesundaily.my/node /176940, 2005.

[29] "New York Times", [Online]. Available: http://www.nytimes.com/2009/11 /12/world/americas/12brazil.html, 2009.

[30] "New York Times", [Online]. Available: http://www.nytimes.com/2012/08 /01/world/asia/power-outages-hit-600-million-in-india.html, 2012.

[31] "Energy.gov", [Online]. Available: https://energy.gov/oe/services/technolog y-development/smart-grid, 2007.

[32] 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 and simulation, 2010, pp. 93-98.

[33] Energy.gov, "Roadmap to Achieve Energy Delivery Systems Cybersecurity, Energy Sector Control Systems Working Group", 2011.

[34] D.G. Hart, D. Uy, V. Gharpure, D. Novosel, D. Karlsson, M. Kaba, "PMUs A new approach topower network monitoring", ABB Review, 2001.

[35] 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, 2008.

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

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

[38] "United States Energy Information Administration", [Online]. Available: http://www.eia.gov/todayinenergy/detail.cfm?id=5630, 2012.

[39] X. Jiang, J. Zhang, B. J. Harding et al., “Spoofing GPS receiver clock offset of phasor measurement units,” IEEE Transactions on Power Systems, vol. 28, no. 3, p. 3253-3262, 2013.

[40] L. Heng, J. J. Makela, A. D. Dominguez-Garcia et al., ”Reliable GPS-based timing for power systems: A multi-layered multi-receiver architecture,” in Power and Energy Conference at Illinois (PECI), 2014. pp. 1-7.

[41] 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, 2011.

[42] C. Tedeschi, “The Newark Liberty International Airport (EWR) GBAS Experience,” in 12th International GBAS Working Group Meeting (IGWG-12), Atlantic City, New Jersey, 2011.

[43] 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.

[44] G. X. Gao, H. Denks, A. Steingassnd et.al., “DME Interference Mitigation Based on Flight Test Data Over European Hot Spot”, GPS Solutions, vol. 17, issue 1, January 2013.

[45] L. Heng, G. X. Gao, T. Walter and P. Enge, “GPS Signal-in-Space Performance Evolution: Data Mining 400 Million Navigation Messages of the Last Decade from a Global Network of 360 receivers”, IEEE Transactions on Aerospace and Electronic Systems, vol. 48, no. 4, 2012.

[46] L. Heng, G. X. Gao, T. Walter and P. Enge, “GLONASS signal-in-space anomalies since 2009”, in Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, 2012.

[47] 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.

[48] S. Storm van Leeuwen, ”Electromagnetic Interference on Low Cost GPS Receivers”, National Aerospace Laboratory, 2008.

[49] E. L. Afraimovich, E. I. Astafyeva, A. V. Oinats, et al., “Global electron content: A new conception to track solar activity”. Ann Geophys, 2008, 26: 335344

[50] B. W. Parkinson, J. J. Spilker, P. Axelrad, P. Enge, “Global Positioning System Theory and Applications”, DC, Washington:Amer. Inst. Astron. Aero., vol. 163, 1996.

[51] J. J. Spilker Jr., “GPS signal structure and performance characteristics”, Navigation: J. Inst. Navigation, vol. 25, no. 2, pp. 121-146, June 1978.

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

[53] “GPS Spotlight”, [Online]. Available: http://xenon.colorado.edu/spotlight/index.php?action=kbpage=42

[54] 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.

[55] 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.

[56] B. W. Parkinson and J. J. Spilker, “Progress In Astronautics and Aeronautics: Global Positioning System: Theory and Applications”, in American Institute of Aeronautics and Astronautics, 1996.

[57] 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.

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

[59] R. F. Vangen, “Time synchronization master station and remote station system”, US4337463 A, issued Jun 29, 1982.

[60] P. Closas, C. Fernandez-Prades, J. Fern andez-Rubio et al., Maximum likelihood estimation of position in GNSS, Signal Processing Letters, IEEE, vol. 14, no. 5, pp. 359362, 2007.

[61] Closas, P., Fernandez-Prades, C.: Direct position estimation approach outperforms conventional two-steps positioning. Proc. XVII European Signal Processing Conf. (EUSIPCO), Glasgow, Scotland, August 2009, pp. 19581962

[62] P. Axelrad, J. Donna, and M. Mitchell, Enhancing GNSS acquisition by combining signals from multiple channels and satellites, in Proceedings of the 22nd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2009), 2001, pp. 26172628.

[63] “Antcom”, [Online]. Available: http://www.antcom.com/documents/catalogs/Page/3GNSSA4-XT-1GNSSAntennas1.pdf

[64] “Microsemi”, [Online]. Available: https://www.microsemi.com/document-portal/docview/133305-quantum-sa-45s-csac

[65] ”Ettus Research”, [Online]. Available: ”https://www.ettus.com/content/files/ 07495EttusN200-210DSFlyerHR1.pdf”

[66] ”GNURadio”, [Online]. Available: https://www.gnuradio.org/

[67] E.Wycoff, Y.Ng and G.X.Gao, “Python GNSS Receiver: An Object-Oriented Software Platform Suitable for Multiple Receivers”, GPS World Magazine, February 2015.

[68] Y.Ng and G. X. Gao,” Advanced Multi-Receiver Vector Tracking for Positioning a Land Vehicle”, in Proceedings of the Institute of Navigation GNSS+ conference (ION GNSS+ 2015), Tampa, 2015.

[69] S. Biswas, A. K. Srivastava, J. S. Park, J. Castaneda, “Tool for testing of phasor measurement units: PMU performance analyser”, IET Gener. Transmiss. Distrib., vol. 9, no. 2, pp. 154-163, Aug. 2014.

[70] ”OpenHistorian 2.0”, [Online]. Available: https://github.com/ GridProtectionAlliance/openHistorian

[71] ”MathWorks”, [Online]. Available: https://www.mathworks.com/products/ matlab.html

[72] K. Kovach, P. J. Mendicki, E. D. Powers, B. Renfro, “Impact from the UTC Offset (UTCO) Anomaly of 25-26 January 2016”, in Proceedings of the ION GNSS+ conference, Portland, 2016.

[73] ”National Geodetic Survey”, [Online]. Available: https://www.ngs.noaa. gov/CORS/

[74] ”International GNSS Service”, [Online]. Available: http://www .igs.org/