Robust GPS-Based Timing for PMUs Based on Multi-Receiver Position-Information-Aided Vector Tracking

Daniel Chou, Yuting Ng and Grace Xingxin Gao,
University of Illinois Urbana-Champaign

BIOGRAPHIES

Daniel Chou is a Master's student in the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign. He received his B.S. in Electrical Engineering from Arizona State University in 2013. His current research projects include designing and implementing countermeasures against malicious attacks on civilian grade GPS receivers utilized in phasor measurement units.

Yuting Ng is a Master's student in the Aerospace Engineering Department at the University of Illinois at Urbana-Champaign. She received her Bachelor's degree, graduating with university honors, from the Electrical Engineering Department also from the University of Illinois at Urbana Champaign in 2014.

Grace Xingxin Gao is an assistant professor in the Aerospace Engineering Department at University of Illinois at Urbana-Champaign. She received her B.S. degree in Mechanical Engineering in 2001 and her M.S. degree in Electrical Engineering in 2003, both at Tsinghua University, China. She obtained her Ph.D. degree in Electrical Engineering at Stanford University in 2008. Before joining Illinois at Urbana-Champaign as an assistant professor in 2012, Prof. Gao was a research associate at Stanford University. Professor Gao has won a number of awards, including RTCA William E. Jackson Award, Institute of Navigation Early Achievement Award, 50 GNSS Leaders to Watch by GPS World Magazine, and multiple best presentation awards at ION GNSS conferences.

ABSTRACT

Reliable and precise electrical wave measurements are essential to the stability and efficiency of a power system. Phasor Measurement Units (PMUs), also known as synchrophasors, are devices that provide precise synchronized voltage magnitude and phase measurements at a high sampling frequency. Widely regarded as one of the most vital devices in monitoring and control for the future of power systems, PMUs rely on the Global Positioning System (GPS) to provide the absolute time reference necessary to synchronize phasor measurements. The dependence of PMUs on GPS introduces new vulnerabilities to a power system utilizing PMUs. The unencrypted nature and low received signal-to-noise ratio (SNR) of civil GPS signals opens risks for malicious parties to broadcast falsified civil GPS signals with the intentions of altering the position or time solutions generated by the GPS receivers [1].

Our goals are to provide robust GPS time transfer for PMUs and to rapidly detect malicious spoofing attacks. Given that the GPS receivers used by PMUs are static, we employ position-information-aided (PIA) vector tracking loops which have been shown to improve the accuracy of the time solutions, robustness against noise and jamming, as well as the ability to detect meaconing attacks [2]. In this paper we extend the single-receiver PIA vector tracking to the multi-receiver case by connecting each of the receivers to the same stable atomic clock and processing the data in a multi-receiver PIA vector tracking loop. Our tests show that this countermeasure can successfully detect meaconing and data-level spoofing. Our approach also significantly improves robustness against jamming and accidental receiver errors.

INTRODUCTION

In the power system, phasor measurement units (PMUs) are GPS based high fidelity state measurement devices which have the potential to significantly enhance system monitoring, control, and protection functions. Current power system functions are regulated by the supervisory control and data acquisition (SCADA) system. However, the SCADA system is comprised of a network of unsynchronized periphery measurement devices which are only polled for measurements once every few seconds. The limitations of the SCADA system prevent more efficient power transmission and distribution.

The near real-time GPS-synchronized state measurements provided by PMUs have the potential to enable effective real time system monitoring and control when placed at key locations across a power grid. This information allows for fine-tuning of the power system that was previously unattainable using the SCADA system. The near real-time measurements collected by PMUs would allow for adaptive and robust state adjustments to account for any changes in the system. Figure 1 illustrates the difference between measurements collected by SCADA and a PMU during disturbance in a power grid in Oklahoma [3]. From the figure, we can see that PMU measurements were able to detect the disturbance several seconds in advance compared with the SCADA measurements.

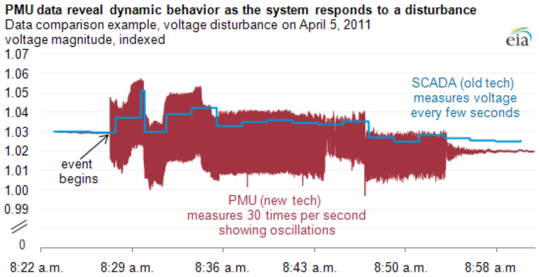

Figure 1: Disturbance in the power grid: SCADA and PMU comparison [3].

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

Types of attacks

Due to the weak signal strength and unencrypted nature of the civil GPS signals, interference and attacks on a GPS receiver can potentially alter both position and time solutions generated by the receivers. In this paper, we consider four types of threats:

- Jamming: an attacker broadcasts a high-powered signal in the GPS frequency band to prevent receivers from locking and tracking the GPS signals.
- Data-level spoofing: an attack where the spoofer broadcasts counterfeit GPS signals with modified ephemeris data.
- Bent-pipe spoofing: An attack where the spoofer records authentic GPS signals in one location and broadcasts them in another. Also known as meaconing and record-and-replay attack.
- Accidental receiver errors: receiver malfunctions can lead to incorrect navigation solutions.

During a jamming attack, our goal is the continued operation of the receivers and the reduction of the jammer's effective range. For the remaining threats, we aim to quickly detect the attack with high probability of success.

OUR APPROACH: MULTI-RECEIVER POSITION-INFORMATION-AIDED (PIA) VECTOR TRACKING

To meet these goals, we propose the multi-receiver position-information-aided vector tracking loop which collaboratively processes the signals from multiple receivers which are connected by a common time source. This is an extension of the single-receiver PIA vector tracking loop that was proposed and implemented in a previous paper [1]. In this countermeasure, we deploy multiple receivers in close vicinity synchronized to a common clock as shown in Figure 2. By tracking each receiver in a multi-receiver PIA vector tracking loop, we will show that every threat can be either reduced (jamming) or detected (spoofing and receiver errors) by our countermeasure.

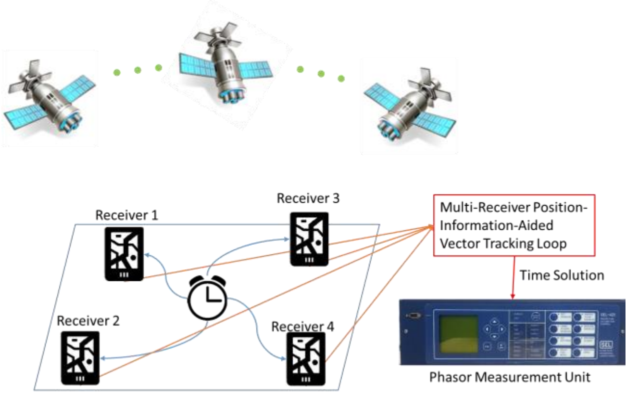

Figure 2: Multi-Receiver Architecture

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

There are several aspects of our multi-receiver architecture that can be leveraged when designing spoofing detection algorithms. First, every receiver is static which allows us to predict the expected code and carrier elements for all receivers by using the known baseline and the signal from a single receiver. The expected elements can then be compared with the actual measurements to detect inconsistencies. Secondly, each receiver will be connected by a common clock and therefore the data collected by each receiver should produce the same clock bias and clock drift. Finally, since each of the receivers are in close proximity we can compare the decoded navigation data of each receivers as well as to external sources.

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

Multi-receiver PIA vector tracking threat detection

In the case of a single PMU GPS receiver, in order to avoid detection a spoofer will likely attempt to maximize the clock error while minimizing the position error. This can be done in data-level spoofing by modifying the ephemeris parameters such that the receiver sees each in-view satellite shifted by a certain distance along the line-of-sight vector (Figure 3). If done properly, both spoofing attacks can remain undetected by a single PMU GPS receiver. However, by deploying several clock synchronized GPS receivers in close proximity to create our multi-receiver architecture, we argue that every type of threat can be alleviated or detected.

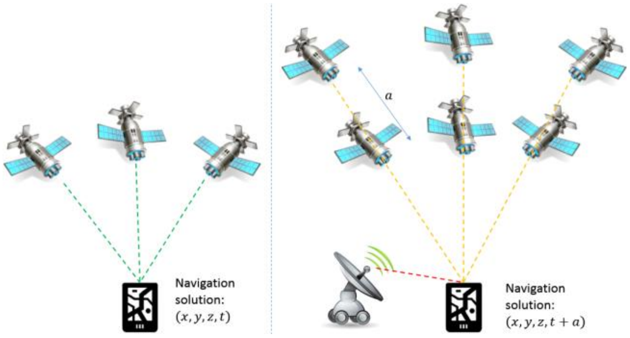

Figure 3: Spoofing attack designed to shift calculated satellite positions in such a way that the position solution remains the same but the clock bias is offset

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

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

For the remainder of this paper, we will first discuss the structure of the multi-receiver PIA vector tracking loop and our approach to implementing the algorithm. We will discuss equipment and location of the field experiment in section “Experimental Setup”. Section “Test Results” presents the performance of the multi-receiver PIA vector tracking loop as well as the results of simulated spoofing attacks.

Multi-receiver PIA vector tracking architecture

The structure of the multi-receiver PIA vector tracking loop is shown in Figure 4. In multi-receiver PIA vector tracking, information from the navigation filter and the known true positions is fed back into the tracking loop and used to control the numerically controlled oscillator (NCO). As a result the channels share information with one another and are able to aid channels with weak signal-to-noise ratios through the use of a common static receivers’ position, velocity, and clock bias.

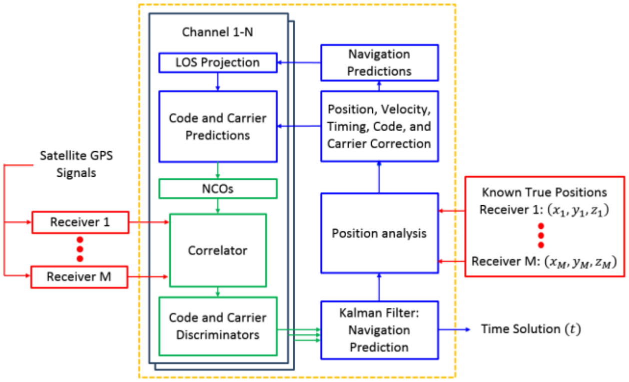
Channel 1-N
LOS Projection
Code and Carrier Predictions
NCOs
Correlator
Code and Carrier Discriminators
Navigation Predictions
Position, Velocity, Timing, Code, and Carrier Correction
Position analysis
Kalman Filter: Navigation Prediction
Satellite GPS Signals
Receiver 1
Receiver M
Known True Positions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

Figure 4: Multi-Receiver PIA Vector Tracking Loop

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

Python Software-Defined-Receiver (SDR)

In order to implement the multi-receiver PIA vector tracking algorithm, we needed a flexible platform and a reliable SDR. In our previous paper on single-receiver PIA vector tracking, we designed our tracking loops on the open source MATLAB SDR developed by Zhao and Akos [4]. Even though the MATLAB SDR worked well, there was limited documentation and we found the MATLAB platform to be very restricting due to its numerous licensing conditions. Additionally, the existing SDR was designed to process data for a receiver using a procedural coding design which is a good solution for a single receiver, but does not adapt well to processing multiple receiver concurrently. For these reasons we chose to develop our SDR in Python which is well suited to process multiple receivers simultaneously due to its object oriented programming design. The framework for the Python SDR was first designed by Wycoff [6] and since then further iterations and a multi-receiver vector tracking loop was developed by Ng [7].

Implementation

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

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

While the basic idea behind the multi-receiver PIA vector tracking algorithm is similar to the single-receiver version there are a few key differences which we will now discuss. The first major difference is the structure of the state transition matrix in the Kalman filter and the second major difference is the receiver clock estimation.

For single receiver vector tracking, the states of the Kalman filter were chosen to be the ECEF position, ECEF velocity, clock bias, and clock drift. For multiple receivers that are connected to a common clock, the states become $N \times$ ECEF position, $N \times$ ECEF velocity, clock bias, and clock drift. Where N is the number of receivers in the receiver-clock network. Equations 1-2 are then the receiver elements of the state transition matrix.

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

$$X_{i,k} = \begin{bmatrix} x_{i,k} \\ y_{i,k} \\ z_{i,k} \\ v_{x,i,k} \\ v_{y,i,k} \\ v_{z,i,k} \end{bmatrix} \tag{2}$$

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

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

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

Then the discrete process equation can be written as:

$$X_{k+1} = F_{k+1} X_k + W_k \tag{5}$$

where W_k is the process noise matrix.

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

$$\delta X_{k+1} = X_{True} - (X_k + V_k \Delta t) \quad (6)$$
$$\delta V_{k+1} = V_{True} - V_k \quad (7)$$

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

$$t_{b,i,k} = t_{b,i,k}^{*} + a_i \quad (7)$$

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

EXPERIMENTAL SETUP

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

To evaluate the effectiveness of the countermeasure presented in this paper, we deployed four USRPs connected to a common chip-scale atomic clock (CSAC) as shown in Figure 5. Each USRP is connected to an active GNSS antenna powered by onboard 3.3V bias tees. As mentioned previously, the majority of power system substations are not very large, around 20m by 20m. Since we want our receiver-clock network to be contained within the confines of the substation but not so close such that the errors are correlated, we chose to separate the antennas using 10m long coaxial cables (Figure 6).

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

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

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

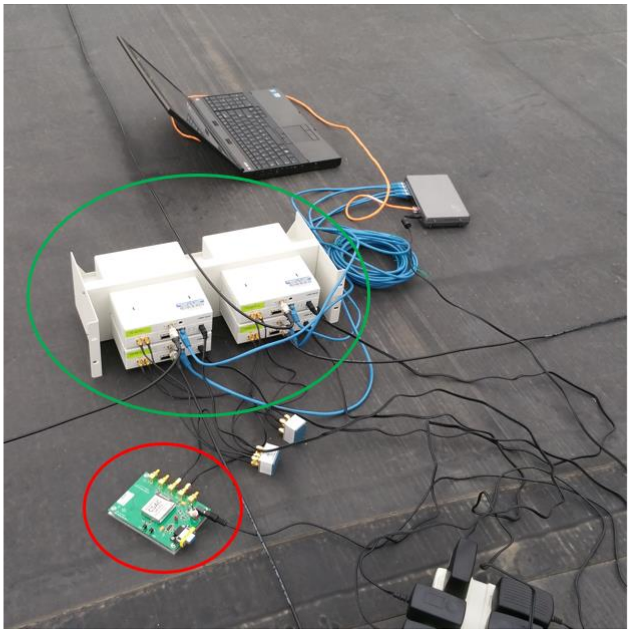

Figure 5: Hardware set up. CSAC is shown circled in red and the USRPs circled in green

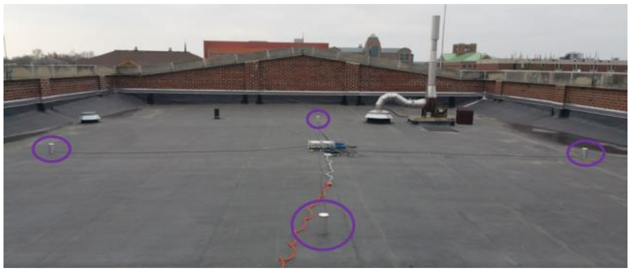

Figure 6: The antennas are placed at an approximately 10m radius.

TEST RESULTS

After collecting data using our multi-receiver set-up, we processed the signals using the Python SDR using scalar tracking, single-receiver PIA vector tracking, and multi-receiver PIA vector tracking. We then added noise to the GPS signals and simulated several spoofing scenarios to show that our algorithm can be used to mitigate or detect the attack.

Even though a couple receivers could acquire up to 8 satellites, we only performed tracking using the 6 satellites acquired by all 4 receivers. Figure 7 shows the clock error results for scalar, PIA vector tracking, and multi-receiver PIA vector tracking under open sky conditions. From these results, we can see that by leveraging the known position, the PIA vector tracking reduces the clock errors when compared to scalar tracking and multi-receiver PIA vector tracking again reduces the clock errors even further.

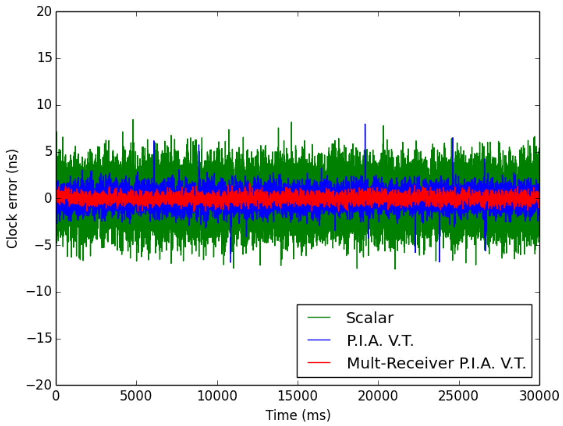

Figure 7: Time errors under open sky conditions

Anti-jamming and noise tolerance

To determine the anti-jamming and noise tolerance capabilities of the multi-receiver PIA vector tracking algorithm, we added Gaussian noise at 1dB increments and processed the full dataset using all 3 tracking methods. As the noise increased, each tracking method's clock errors increased with scalar tracking's being the most drastic as shown in Figure 8.

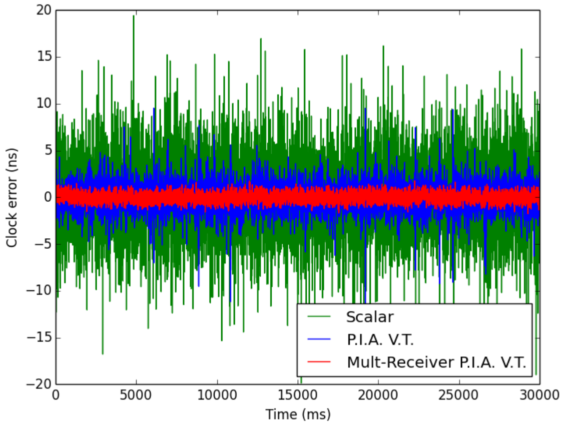

Figure 8: Time errors when 4dB of additional noise is added

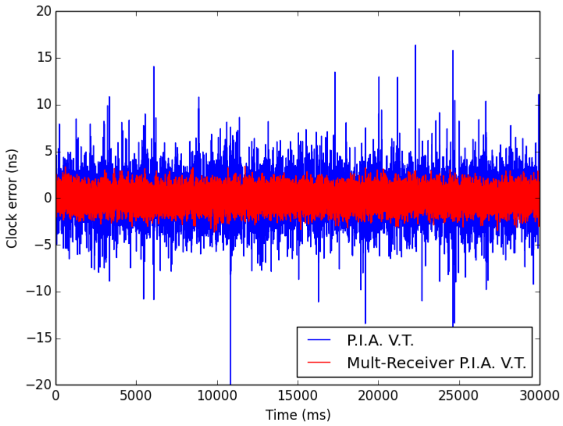

Figure 9: Time errors when 8dB of additional noise is added. Scalar tracking has stopped working.

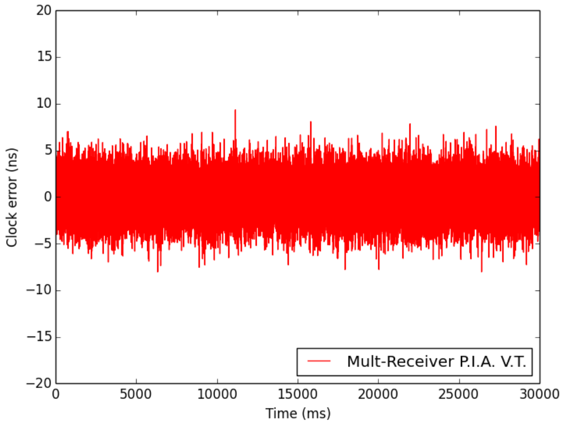

Figure 10: Time errors when 11dB of additional noise is added. Scalar and single-receiver PIA vector tracking have both stopped tracking.

After the noise was increased past 4dB, the number of channels that could remain locked during tracking fell below 4 which was consistent with our previous findings using the MATLAB SDR. Single-receiver PIA vector tracking could track the signal until we increased the noise past 8dB and multi-receiver PIA vector tracking continued operating until we increased the noise past 11dB. From Figure 7 and Figure 10, we can see that even at 11dB of additional noise, the clock error of the multi-receiver PIA vector tracking rivaled that of scalar tracking under open sky conditions. Since for every 3dB loss, the signal strength received is roughly halved, we can see that the multi-receiver PIA vector tracking algorithm is very robust against jamming and environmental noise. Table 1 lists the peak clock errors for each of the tracking methods as the added noise is increased.

Tracking	0dB	4dB	8dB	11dB
Scalar	7ns	20ns		
PIA Vector	7ns	10ns	15ns	
Multi-receiver PIA Vector	1.5ns	2ns	3ns	7ns

Table 1: Peak clock error range for each of the tracking methods as the added noise is increased

Spoofing attack simulations

The threat of spoofing attacks is arguably the most limiting factor towards the use of PMUs to control the power grid. Fortunately, the vast majority of possible spoofing attacks have several common elements which the multi-receiver PIA vector tracking architecture is designed to combat. By placing multiple receivers in close proximity (within the 20m by 20m area) we can assume that the spoofing signal is either received by all receivers or by none.

During a meaconing attack, legitimate GPS signals are first received by the spoofer and then broadcast towards the victim receivers at a higher power than the signals from the GPS satellites. When this attack is directed at a receiver running a standard scalar tracking algorithm, the victim receiver will calculate the same PVT solution as the attacker with an additional delay. Thus causing the receiver to output incorrect timing information. Since the multi-receiver PIA vector tracking algorithm is dependent on the true positions and velocities, the difference between the known position/velocity and the spoofed signal's position/velocity causes significant errors leading to the failure of the multi-receiver PIA vector tracking loop as shown in Figure 11. Thus, the meaconing attack can be detected.

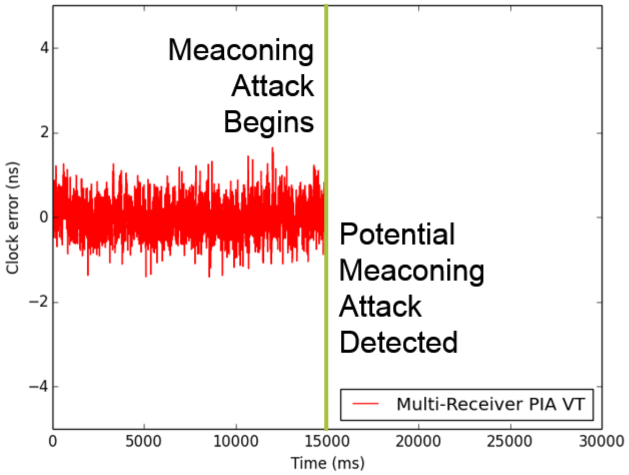

Figure 11: Time errors during a simulated meaconing attack with a 100m separation between the spoofer and the PMU GPS receivers.

As discussed previously, for a data-level spoofing attack, a spoofer could modify the ephermis parameters of the signals in such a way that the position solution calculated by the victim receivers remains the same but the timing solution would be incorrect. Figure 12 shows the results of our data-level spoofing simulation. Once the spoofing attack began, the errors in the Kalman filter quickly accumulated ultimately resulting in the failure of the multi-receiver PIA vector tracking loop. By simply observing the clock error, we can see that prior to the failure of the tracking loop the clock errors drastically increased from the previous open sky errors. This increase in error can potentially be used as an additional spoofing detection metric.

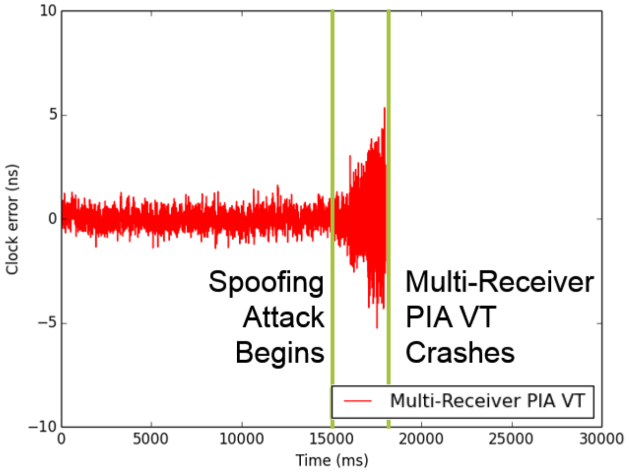

Figure 12: Time errors during a simulated data-level spoofing attack.

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

Accidental receiver errors

While no field tests were performed for this threat, the multi-receiver architecture is well suited for detecting accidental receiver errors. Under normal operating conditions, each receiver will generate a set of ephemeris values from each satellite which can be compared with the values from other receivers. This provides an extra layer of redundancy allowing the multi-receiver architecture to potentially operate properly even when faced with receiver malfunctions.

CONCLUSION

Security and reliability of PMU measurements are vital to the development of power systems. Currently, PMUs are mainly used for grid monitoring. As PMU usage continues to grow, automatic grid control via PMU measurements will become increasingly common. In order to ensure the integrity of GPS-based timing for PMUs, we proposed and implemented the multi-receiver position-information-aided vector tracking loop on the our software receiver using Python.

The field experiments showed that the proposed multi-receiver architecture improves the accuracy of the time solutions generated by the receivers by leveraging the known static receivers' locations in our tracking algorithm. The results show that our proposed tracking algorithm significantly decreases the effectiveness of a jammer by reducing the jammer's effective range. We also simulated several spoofing attacks to show that the multi-receiver PIA vector tracking is capable of detecting various types of threats presented in this paper.

ACKNOWLEDGEMENTS

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000097.

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.

REFERENCES

[1] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," IEEE Transactions on Power Systems, Vol. 28, No. 3, pp. 3253-3262, 2013.

[2] Daniel Chou, Liang Heng, and Grace Xingxin Gao, “Robust GPS-Based Timing for Phasor Measurement Units: A Position-Information-Aided Vector Tracking Approach,” ION GNSS+ 2014, Tampa FL, Sep 2014.

[3] U.S. Energy Information Administration, “Today in Energy”, Retrieved from: http://www.eia.gov/todayinenergy/detail.cfm?id=5630

[4] Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler, “Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks”, International Journal of Critical Infrastructure Protection, Volume 5, Issues 3-4, December 2012, p. 146-153

[5] Zhao and Akos, “An Open Source GPS/GNSS Vector Tracking Loop – Implementation, Filter Tuning, and Results”, International Technical Meeting of the Institute of Navigation, San Diego, CA, January 2011, pp. 1293-1305.

[6] Eliot Wycoff and Grace Xingxin Gao, “A Python Software Platform for Cooperatively Tracking Multiple GPS Receivers,” ION GNSS+ 2014, Tampa FL, Sep 2014.

[7] Yuting Ng and Grace Xingxin Gao, “Multi-Receiver Vector Tracking Based on a Python Platform”, International Technical Meeting of the Institute of Navigation, Dana Point, CA, Jan 2015.