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

Daniel Chou and Grace XingXin Gao,
University of Illinois Urbana-Champaign

BIOGRAPHIES

Daniel Chou is a graduate 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.

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 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].

In this work, our goals are to provide robust GPS time transfer for PMUs and to rapidly detect malicious interference. Given that the GPS receivers used by PMUs are static, we employ position-information-aided (P.I.A.) vector tracking loops which have been shown to improve the accuracy of the time solutions, improved robustness against noise and jamming, as well as the ability to detect meaconing attacks [2]. In this paper we extend the P.I.A. 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 P.I.A vector tracking loop. Our tests show that this countermeasure can successfully detect meaconing, data-level spoofing, and signal-level spoofing attacks. 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 [1]. From the figure, we can see that PMU measurements were able to detect the disturbance several

seconds in advance compared with the SCADA measurements.

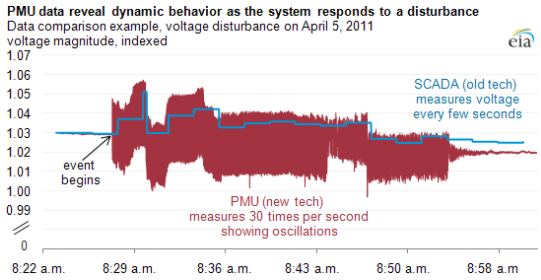

Figure 1: Disturbance in the power grid: SCADA and PMU comparison [1].

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. This is largely due to the fact that PMUs are not secure devices given their dependence on GPS.

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 five 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.
- Signal-level spoofing: The spoofer generates counterfeit GPS signals with carefully tuned code delays.
- 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. For the remaining threats, we aim to quickly detect the attack with high probability of success.

OUR APPROACH: MULTI-RECEIVER POSITION-INFORMATION-AIDED (P.I.A.) 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 P.I.A. 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 P.I.A. vector tracking loop, we will show that every threat can be either reduced (jamming) or detected (spoofing and receiver errors) by our countermeasure.

In traditional GPS receivers, scalar tracking loops are used to track GPS signals from each satellite in view. Each satellite's tracking loop operates independently and the results from the processed data is used to decode the satellite ephemeris data and calculate the navigation solution. In our multi-receiver P.I.A. 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.

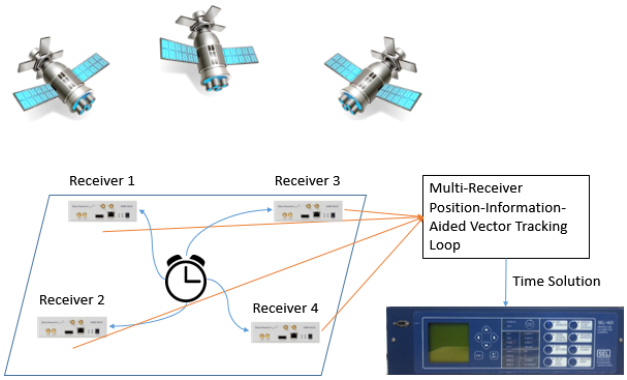

Figure 2: Multi-Receiver Architecture

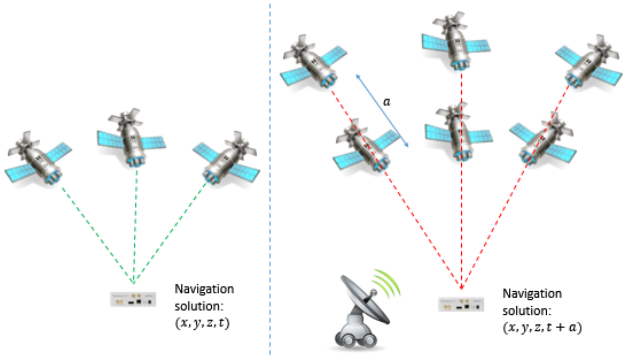

Figure 3: Spoofing attack designed to shift calculated satellite positions in such a way that the position solution remains the same but the clock bias is offset

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 P.I.A. vector tracking algorithms have been shown to be capable of detecting meaconing attacks, multi-receiver P.I.A. vector tracking can be used to detect and combat data-level spoofing, signal-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 P.I.A 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 both data-level and signal level spoofing by either modifying the ephemeris parameters or code delays 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.

In the case of a spoofing attack with a single attacker, there are three possibilities that we 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. If none of the receivers are subject to the spoofing attack, each receiver will output the same clock bias. If a partial number of the receivers are spoofed, then the spoofed receivers will output a different clock bias than the unspoofed receivers. Finally 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 P.I.A. 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 P.I.A. vector tracking loop as well as the results of simulated spoofing attacks.

Multi-receiver P.I.A. vector tracking architecture

The structure of the multi-receiver P.I.A. vector tracking loop is shown in Figure 4. In multi-receiver P.I.A. 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.

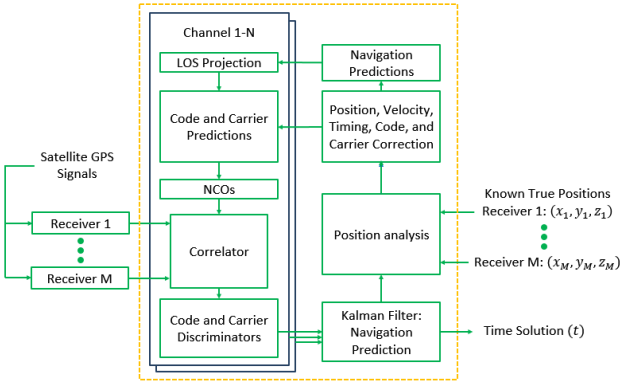

Figure 4: Multi-Receiver P.I.A. Vector Tracking Loop

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

Implementation

The multi-receiver P.I.A. vector tracking loop is meant to be used in conjunction with the existing scalar loops rather than a complete replacement. At a specific time epoch, several tracking loop values are extracted and used to initialize the multi-receiver P.I.A. tracking loop. Since the multi-receiver P.I.A. 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 P.I.A. vector tracking loop first predicts the navigation solution and errors for the next time epoch. Then early, late, and prompt code replicas are generated using the LOS projections for each receiver to calculate the predicted Doppler and phase terms. 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. Since we know the true position of the GPS receiver, we correct the prediction and create a closed feedback loop using the corrected predictions.

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 and 10m long coaxial cables. The use of the CSAC as the common time source results in extremely stable time solutions compared with standard GPS receivers. The signals were collected using 2 MHz sampling frequency and during data collection the receivers had full view of an open sky with up to 8 satellites with clear LOS and good DOP.

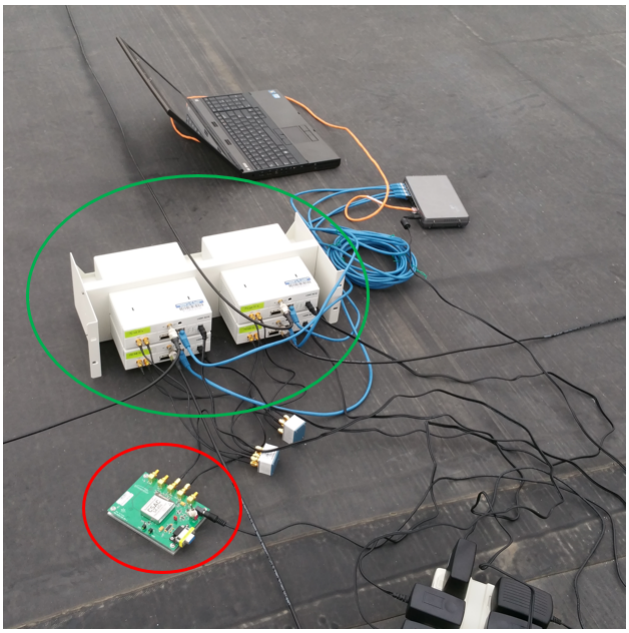

Figure 5: Hardware set up. CSAC is shown circled in red and the USRPs circled in green

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

TEST RESULTS – this section is not yet complete

After collecting data using our multi-receiver set-up, we processed the signals using the python-based software-defined-receiver and our multi-receiver P.I.A. vector tracking loop. We then simulate several spoofing scenarios and show that our algorithm can be used to detect the attack

What we expect to see:

- Case: No receivers spoofed
  - Timing solution errors on the order of 5-10ns
- Case: Partial number of receivers spoofed by the same spoofer
  - Clock biases and navigation data will not match
- Case: All receivers spoofed by the same spoofer
  - The position difference will cause the multi-receiver P.I.A. vector tracking loop to fail

CONCLUSION

The security and reliability of the PMU measurements is vital to the continued development of power systems. In this paper, we propose and implemented the multi-receiver position-information-aided vector tracking loop on the python-based software-defined-receiver. We postulated the multi-receiver algorithm increases the receiver's robustness against jamming attacks as well as strong spoofing detection capabilities. We then conducted field experiments to evaluate the performance of the tracking loop.

The field experiments conducted showed that the proposed multi-receiver architecture and tracking loops improves the accuracy of the time solutions generated by the receivers by leveraging the known static receivers' locations in our tracking algorithm. We also simulated several spoofing attacks to show that the multi-receiver P.I.A. vector tracking is capable of detecting every type of threat 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] L. Heng, J. J. Makela, A. D. Dominguez-Garcia, R. B. Bobba, W. H. Sanders, and G. X. Gao, "Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture," IEEE PECI 2014, Champaign, IL, Feb 2014.

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