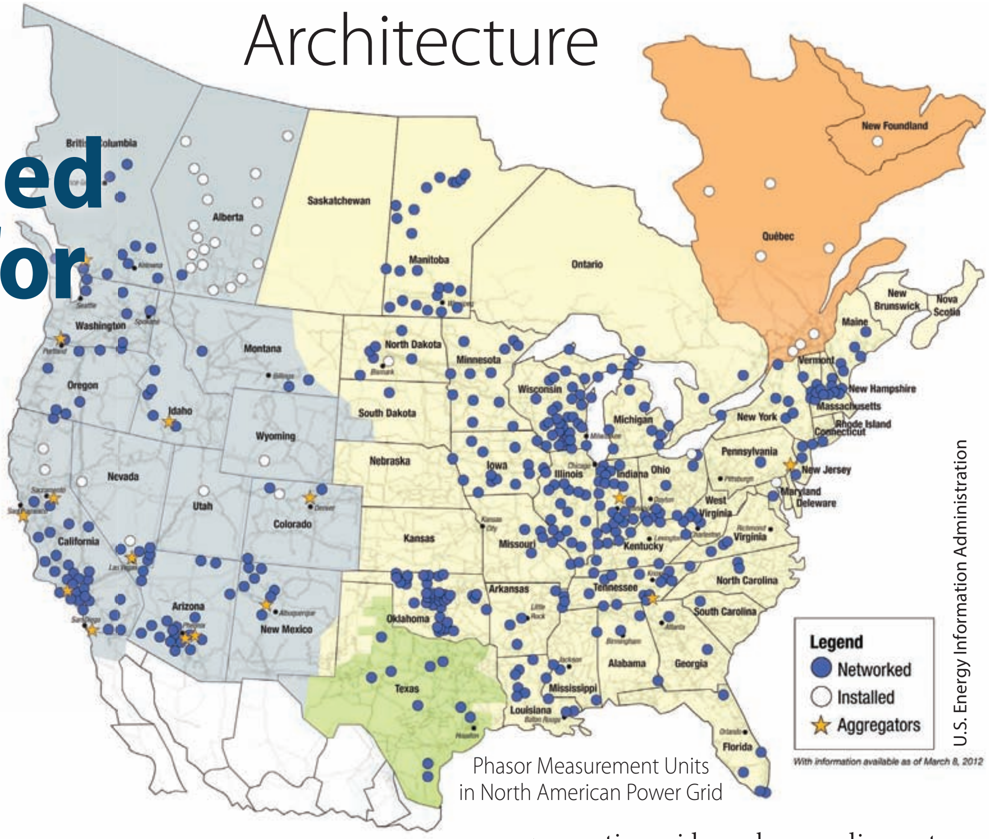
A Multi-Layered, Multi-Receiver Architecture

Reliable GPS-Based Timing for Power Systems



Phasor Measurement Units in North American Power Grid

LIANG HENG, DANIEL CHOU, AND GRACE XINGXIN GAO
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Synchronized voltage and current phasor measurements provided by phasor measurement units (PMUs) can potentially augment power system monitoring, control, and protection functions. PMUs use GPS receivers to synchronize measurements across a wide geographical area. However, GPS signals are vulnerable to jamming, spoofing, and accidental receiver malfunctions. The authors present a multi-layered multi-receiver architecture that hardens GPS-based timing against these hazards. The article describes eight countermeasures that address five known threat models and an experiment to test the viability of this approach. Analysis demonstrates high reliability and robustness for the new architecture.

Efficient power transmission and distribution would benefit from synchronized near–real-time measurements of voltage and current phasors at widely dispersed locations in an electric power grid. Such measurements also could enable effective real-time system monitoring and control, which are considered to be the key to preventing wide-scale cascading outages like the 2003 Northeast Blackout.

A phasor measurement unit (PMU), also known as a *synchrophasor*, is a device capable of measuring power system voltage and current phasors at a rate of thousands of samples per second. The samples are time-stamped with one-microsecond or better accuracy to a common absolute time reference provided by the GPS receivers attached to PMUs.

Unfortunately, low-received-power, unencrypted civil GPS signals have proven to be vulnerable to jamming and spoofing attacks. A jammer emits a high-power interfering signal at the GPS frequency in order to deny nearby GPS receivers access to the GPS signal. A spoofer broadcasts a counterfeit GPS signal that overpowers the authentic signal so as to manipulate a victim receiver's reported position, time, or both.

In a future scenario where PMU data play a significant role in power system operations, an attacker might disturb or bring down the system by attacking the GPS receivers attached to PMUs. In an article listed in the Additional Resources section near the end of this article, D. P. Shepard *et alia* have shown that an attacker could cause a generator trip by spoofing a GPS time reference receiver.

Even without being jammed or spoofed, a GPS receiver does not always yield correct position and time solutions due to accidental receiver malfunctions. In an earlier article, L. Heng *et alia* (2012b) showed that 0.34 percent of the navigation messages collected by the geodetic-grade GPS receivers in the International GNSS Service (IGS) network during the year 2009 were incorrect. Another relevant event occurred on July 31, 2006, when 29 out of 245 GPS receivers in the IGS network missed or misinterpreted a navigation message. As a result, the 29 receivers miscalculated their positions and clocks for more than one hour.

So far, a variety of countermeasures have been proposed to enhance civil GPS receivers' robustness against jamming and spoofing attacks and accidental receiver errors. These methods can be generally categorized into four groups: external assistance, signal features, redundant measurements, and cryptography.

The first group of proposed solutions uses information from sensors external to the GPS subsystem, such as accelerometers, gyroscopes, odometers, and cellular networks. The second group makes use of the features inherent in GPS signals, including angle-of-arrival (spatial sparsity), time-frequency sparsity, signal quality, signal power, and multipath. The third group exploits the redundancy of pseudorange measurements and the correlation among multiple cooperative receivers. The fourth group uses cryptographic, unpredictable information carried by the GPS signal to ensure its authenticity. Some of the key papers and articles describing these various types of spoofing defenses can be found in the Additional Resources section.

Most of these proposed methods were designed for stand-alone kinematic receivers, and their primary objective was reliable positioning but not necessarily reliable timing. There is still a dearth of countermeasures designed for static, networked GPS time reference receivers in power systems.

In this article, we present a multi-layered multi-receiver architecture that hardens GPS-based timing against jamming, spoofing, and receiver errors. Our architecture integrates eight countermeasures in all layers of receiver signal and data processing. Most of the countermeasures exploit the static and networked nature of time reference receivers.

In describing this security architecture, we begin with a formal definition of threat models and design goals. Then, we elaborate on the multi-layered multi-receiver architecture. Finally, we present our implementation of a key countermeasure, a position-information-aiding tracking loop, along with experimental results.

Threat Models and Design Goals

The GPS receiver uses trilateration (also referred to as multilateration) to determine its position and clock bias. A standalone GPS Standard Positioning Service receiver must meet two prerequisites for generating a correct real-time position and time solution: correct pseudorange measurements from at least four satellites and valid navigation messages so that the receiver can correctly calculate satellite positions and clock biases.

This article is concerned with the threats that render any of these two prerequisites unavailable or incorrect. Specifically, we consider the following five threat models:

[J] Jamming:
- high power interfering signal
- deny-of-service attack

[S1] Data-level spoofing (such as the spoofing attack described in the article by X. Jiang *et alia*):
- counterfeit GPS signals with modified navigation data
- carefully tuned delay of each code
- can manipulate time solutions without altering position solutions

[S2] Signal-level spoofing (such the spoofing attack conducted in D. P. Shepherd *et alia*):
- the same navigation data as concurrently broadcast by the GPS satellites
- carefully tuned delay of each code
- can manipulate time solutions without altering position solutions

[S3] Replay spoofing (also referred to as meaconing):
- recording and replaying of authentic GPS signals
- time solution is always delayed, position solution equal to attacker's location

[E] Accidental receiver malfunctions:
- missed or misinterpreted navigation data
- incorrect pseudorange measurements.

Under threat model [J], we want to reduce the jammer's effective range. For the other threat models, our goal is to detect the threat with a high confidence in a timely manner. The next section describes our multi-layered multi-receiver architecture and how it achieves these goals.

Overall Architecture

Figure 1 shows our proposed multi-layered, multi-receiver architecture that enables reliable GPS-based timing. Our architecture employs comprehensive countermeasures in all layers of receiver signal and data processing.

The list below summarizes the main purpose of the countermeasures performed in each layer:
- signal conditioning: early spoofing detection
- tracking loop: continuous operation under jamming;
- navigation data: spoofing detection and receiver malfunction detection;
- position/time calculation: final spoofing detection and receiver malfunction detection.

The remainder of this section will describe the eight countermeasures in detail.

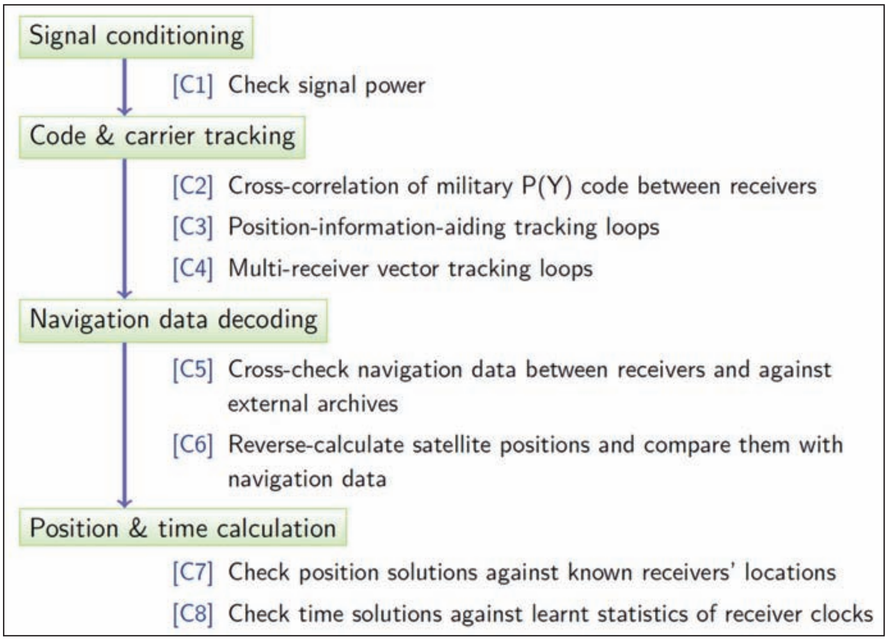

Signal conditioning
[C1] Check signal power
Code & carrier tracking
[C2] Cross-correlation of military P(Y) code between receivers
[C3] Position-information-aiding tracking loops
[C4] Multi-receiver vector tracking loops
Navigation data decoding
[C5] Cross-check navigation data between receivers and against external archives
[C6] Reverse-calculate satellite positions and compare them with navigation data
Position & time calculation
[C7] Check position solutions against known receivers' locations
[C8] Check time solutions against learnt statistics of receiver clocks

FIGURE 1 Our proposed multi-layered multi-receiver architecture for reliable GPS-based timing for power system applications

[C1] Check Signal Power. In a spoofing attack, the counterfeit signal must overpower the authentic signal so that a victim receiver will lock onto the more powerful counterfeit signal. Therefore, an ascent of received signal power implies the possibility of a spoofing attack. In GPS receivers that use two or more bits for sampling, automatic gain control (AGC) is used to adjust the front-end gain to a level suitable for the analog-to-digital converter (ADC). Experiments carried out by D. Akos (see Additional Resources) have shown that AGC level is a low-computational-complexity, low-cost means to detect potential spoofing attacks.

Our architecture integrates the signal-power check as an early spoofing detection. Advantages of this countermeasure include very low computational complexity and independence (not relying on other receivers). A major disadvantage is the low detection confidence due to the stochastic nature of signal power. Therefore, the signal-power check is considered as an auxiliary countermeasure against all spoofing threats [S1]-[S3].

[C2] Cross-Correlation of Military P(Y) Code between Receivers. The GPS signal contains the unencrypted C/A code and the encrypted P(Y) code, which are modulated onto the L1 carrier in-phase and quadrature, respectively. This countermeasure is based on the fact that a spoofer cannot forge the P(Y) code. Here's how it works:

Suppose two receivers are tracking the signal from a satellite visible to both of them. Each receiver uses the C/A-code phase and timing relationships to the P(Y) code to take a snippet of the same part of the received P(Y) code. The spoofing detector correlates the two snippets.

Although the P(Y) code is encrypted and thus unknown to non-military receivers and although its received versions are noisy and may be distorted by narrow-band RF front-ends, when conducting cross-correlation, the P(Y) code components in the two snippets are similar enough to create a high correlation peak if neither receiver is spoofed. A high correlation peak may also appear if both receivers are spoofed by the same spoofer, but this scenario can be precluded by choosing reference receivers far (e.g., at least one kilometer) away from the user receiver.

S. Lo *et alia* and M. L. Psiaki *et alia* (see Additional Resources) have demonstrated the efficacy of this method using one user receiver and one reference receiver. L. Heng *et alia* (2013b) have extended this method to multiple receivers. A key conclusion of this research was that, respectively, the probability of detection errors decreases exponentially with the length of the P(Y)-code snippet (preferably one second or longer) and with the number of reference receivers.

Therefore, this anti-spoofing method has proven effectiveness against synthesized spoofing attacks, including threat models [S1] and [S2]. Unfortunately, it is ineffective against threat [S3] because a replay spoofer rebroadcasts the authentic GPS signals, which contain the correct P(Y) code.

To implement the P(Y)-code cross-correlation countermeasure, the receiver must be able to output baseband samples, and these samples need to be transmitted over a data network. Due to the high sampling rate (usually greater than two Msps), we recommend performing this spoofing detection periodically rather than continuously.

[C3] Position-Information-Aiding (PIA) Tracking Loops. Our proposed approach of PIA tracking loops aims to take advantage of the static nature of GPS receivers used in PMUs to enhance tracking performance. The knowledge of the true position of GPS receivers used in PMUs helps predict the code and carrier phases by projecting the relative position and velocity between satellites and the receiver in the line-of-sight (LOS) direction. This type of receiver architecture is referred to as *vector tracking* and has been shown to increase immunity to interference and jamming.

We can also improve tracking robustness through the use of Kalman filtering. Because the receivers in a PMU must remain static, the parameters of the tracking loops can be adaptively chosen to narrow the loop filter bandwidth. The narrowband tracking loop limits receiver noise, which reduces the effective radius of any jamming attacks (threat [J]).

Additionally, the PIA vector tracking approach allows for a natural defense against threat [S3]. Replayed signals are simply authentic GPS signals being recorded somewhere else. As the PIA vector-tracking approach depends on its knowledge of the true position of the GPS receiver, then the PIA tracking loop will fail to function in the case of a replay spoofing attack, therefore being able to detect meaconing.

[C4] Multi-Receiver Vector-Tracking Loops. In addition to the PIA tracking loops that leverage the static nature of PMU GPS receivers, in the code and carrier tracking layer we use multi-receiver vector tracking loops to explore the benefit from the networked nature of GPS-timed PMUs either within a substation or across an electrical grid.

Multi-receiver vector tracking loops collaboratively process information from multiple receivers. A. Soloviev *et alia* showed that multi-receiver signal accumulation improves acquisition and tracking performance under low signal-to-noise ratio (SNR) conditions. Multi-receiver phased arrays greatly improve the robustness against jamming and spoofing attacks (threat models [J], [S1]-[S3]) by forming beams to satellites and steering nulls in the direction of attacking transmitters. In addition, multi-receiver signal processing helps detect receiver errors (threat model [E]) because a malfunctioning receiver's performance is usually inconsistent with other receivers.

The main downside of multi-receiver vector tracking is the intensive computation that it requires. However, for static receivers in power systems, processing power is not of major concern.

Similar to countermeasure [C2], multi-receiver processing requires receivers to output baseband samples. The high-sampling-rate data need to be continuously transmitted among receivers (or to a central processing server). In practice, we recommend choosing receivers near to one another and transmitting the data over a local area network.

[C5] Cross-Check Navigation Data among Receivers. This countermeasure cross-checks the navigation messages collected by one PMU GPS receiver with those collected by others. This method can easily detect data-level spoofing attacks (threat model [S1]) in which the navigation data are modified. Cross-checking also ensures that a receiver does not miss or misinterpret a navigation message (threat model [E]).

Furthermore, under jamming attacks (threat model [J]), a receiver may be able to track satellites but cannot correctly decode navigation messages. Using navigation data from other receivers helps the receiver under attack continue operating.

[C6] Reverse-Calculate Satellite Positions and Compare Them with Navigation Data. Because the PMU GPS receivers are static and their positions are known, we propose using the pseudorange measurements from multiple receivers to reverse-calculate satellite positions via trilateration.

Reverse-calculated satellite positions match the satellite positions calculated from the navigation data only when both the navigation data and the pseudorange measurements are correct. Therefore, this countermeasure can easily detect replay spoofing attacks (threat model [S3]) and receiver errors (threat model [E]). This countermeasure also makes the synthesized spoofing attacks (threat models [S1] and [S2]) much more difficult because it imposes more constraints on "valid" spoofing signals.

The accuracy of trilateration depends on the satellite-to-users geometry. We recommend choosing receivers at dispersed locations to improve accuracy.

[C7] Check Position Solutions against Receivers' Known Locations. For a single GPS receiver, checking the position solution against its *a priori* known location can detect a replay spoofer (threat model [S3]). Receiver errors (threat model [E]) can also be detected if the errors result in an incorrect position solution. However, this method cannot detect the synthesized spoofing attacks (threat models [S1] and [S2]) because, when formulated properly, these attacks ensure unaltered position solutions.

However, this countermeasure *is* effective against threat models [S1] and [S2] when multiple receivers are deployed in close vicinity and the position solutions from the receivers are cross-checked. **Figure 2** shows three receivers deployed in a substation with a distance of 20 to 50 meters between two neighboring receivers. If no receivers are spoofed, all receivers yield the same time solutions, and each receiver's position solution is close to its actual position. If a fraction of the receivers are spoofed by a spoofer, the victim receivers yield time solutions that are different from those of the innocent receivers.

If all receivers are spoofed by the same spoofer, although they generate the same clock bias, they output identical position solutions despite being at different locations because the position solution is controlled by the spoofer and does not depend on the receivers' locations. In this case, the spoofing attack can also be detected.

The only way to spoof multiple receivers without being detected is to employ multiple spoofers, each of which must fine-tune the transmit power so as to spoof just one receiver. The spoofers would also need to be synchronized to ensure that the clock biases output by all receivers are the same. Generally, this spoofing attack is too complicated and too costly to be practical.

[C8] Check Time Solution against Learned Statistics of Receiver Clocks. Spoofing attacks and receiver errors are rare events. Based on this fact, we propose monitoring the behavior of receiver clocks and learning the statistics. The article by K. Wang *et alia* describes a model for high-stability clocks. When spoofing attacks (threat models [S1]-[S3]) and receiver errors occur (threat [E]), the time solution is unlikely to be consistent with the learnt statistics of receiver clocks. Due to the stochastic volatility of receiver clocks, this countermeasure is considered auxiliary in our architecture.

Comparison and Implementation of Countermeasures

Table 1 summarizes the effectiveness of the countermeasures that we have just described. For each threat model, markers *, o, and • denote whether a countermeasure is effective, auxiliary, or ineffective, respectively.

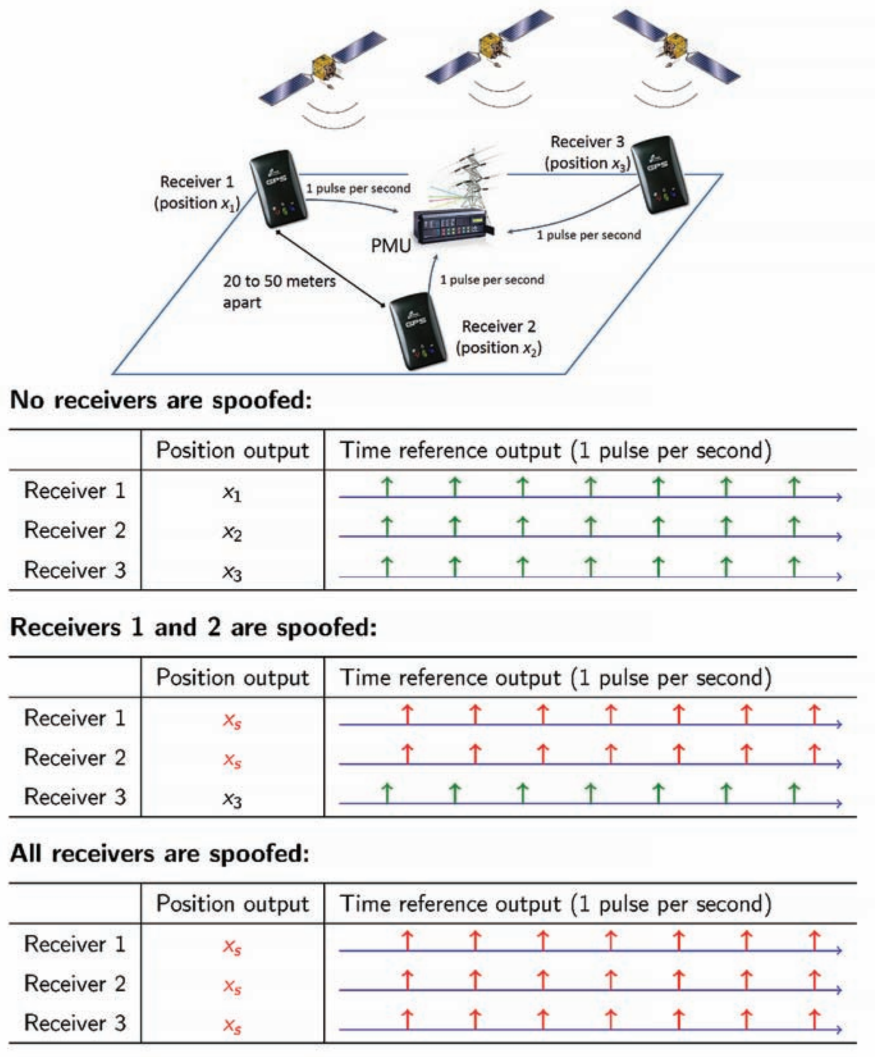
The table shows that our multi-layered multi-receiver approach provides at least two effective countermeasures against each threat. Taking auxiliary countermeasures into account, at least five countermeasures are available against spoofing attacks and receiver errors. The redundancy in countermeasures guarantees highly reliable GPS-based timing even if some of the countermeasures fail.

Countermeasures [C1]-[C4] in the signal conditioning layer and the tracking loop layer require modification of the current GPS time reference receivers used in PMUs. In particular, [C2] and [C4] require output of samples from digital baseband. Thus, these countermeasures are unlikely to be widely implemented in the near future.

Because countermeasures [C5]-[C8] utilize the output already available from current GPS time reference receivers, these can be implemented in current power girds with minimal modification. As can be seen from Table 1, countermeasures [C5]-[C8] still provide redundant protection against spoofing attacks and receiver errors.

Designing a PIA Tracking Loop

The previous section showed that a position-information-aiding tracking loop is an effective countermeasure against jamming and replay spoofing. This sec-



No receivers are spoofed:

	Position output	Time reference output (1 pulse per second)
Receiver 1	x_1	↑ ↑ ↑ ↑ ↑ ↑ ↑ →
Receiver 2	x_2	↑ ↑ ↑ ↑ ↑ ↑ ↑ →
Receiver 3	x_3	↑ ↑ ↑ ↑ ↑ ↑ ↑ →

Receivers 1 and 2 are spoofed:

	Position output	Time reference output (1 pulse per second)
Receiver 1	x_s	↑ ↑ ↑ ↑ ↑ ↑ ↑ →
Receiver 2	x_s	↑ ↑ ↑ ↑ ↑ ↑ ↑ →
Receiver 3	x_3	↑ ↑ ↑ ↑ ↑ ↑ ↑ →

All receivers are spoofed:

	Position output	Time reference output (1 pulse per second)
Receiver 1	x_s	↑ ↑ ↑ ↑ ↑ ↑ ↑ →
Receiver 2	x_s	↑ ↑ ↑ ↑ ↑ ↑ ↑ →
Receiver 3	x_s	↑ ↑ ↑ ↑ ↑ ↑ ↑ →

FIGURE 2 Configuration of multiple receivers. With this configuration, checking position solutions against known PMU locations can effectively detect all spoofing attacks (threat models [S1]–[S3]).

Counter-measures	Threat Models				
	[J] Jamming	[SD] Data-level spoofing	[SS] Signal-level spoofing	[SR] Replay spoofing	[E] Accidental receiver errors
[C1] Check signal power	•	o	o	o	•
[C2] Cross-correlation of P(Y) code between receivers	•	*	*	•	•
[C3] Position-information-aiding tracking	*	•	•	*	•
[C4] Multi-receiver vector tracking	*	o	o	o	o
[C5] Check navigation data	o	*	•	•	*
[C6] Reverse-calculate satellite positions	•	o	o	*	*
[C7] Check position solutions	•	*	*	*	*
[C8] Check time solutions	•	o	o	o	o

* Effective
o Auxillary
• Ineffective

TABLE 1 Effectiveness of countermeasures against threat models

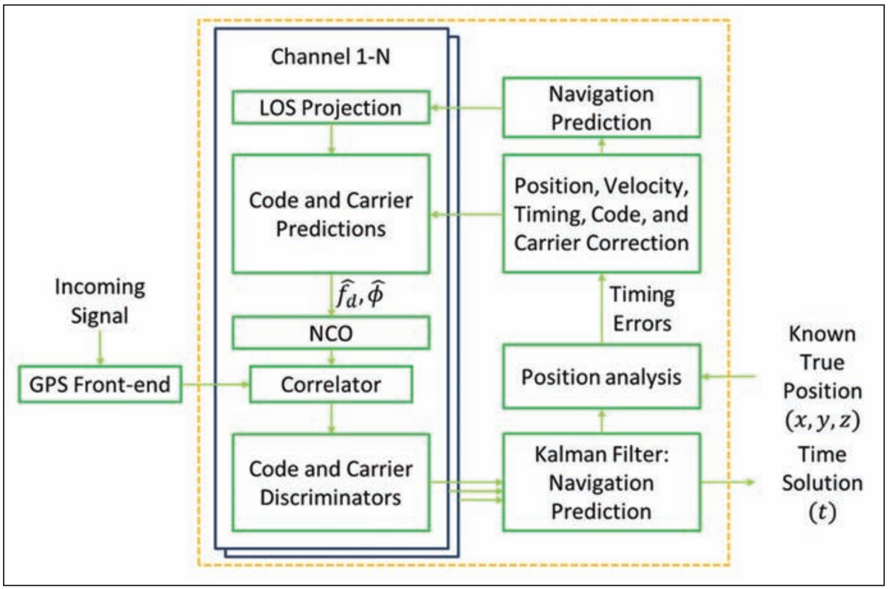

Channel 1-N
LOS Projection
Code and Carrier Predictions
$\hat{f_d}, \hat{\phi}$
NCO
Correlator
Code and Carrier Discriminators
Incoming Signal
GPS Front-end
Navigation Prediction
Position, Velocity, Timing, Code, and Carrier Correction
Timing Errors
Position analysis
Kalman Filter: Navigation Prediction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

FIGURE 3 Block diagram of PIA tracking loops

tion presents one of our designs for a PIA tracking loop along with experimental results.

Structure. Figure 3 shows the structure of the PIA tracking loop. After initialization, the tracking loop first predicts the navigation solution and errors for the next time epoch. The known true position of the GPS receiver greatly simplifies the Kalman filter design. The state equation contains only the receiver clock parameters, as given by

$$\begin{bmatrix} b_{k+1} \\ d_{k+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} b_k \\ d_k \end{bmatrix} + w_k,$$

where b_k is the receiver clock bias at the kth time epoch, d_k is the receiver clock drift rate, Δt is the sample duration, and w_k is the Gaussian noise.

Our PIA tracking loop design incorporates predicted clock bias, together with the known receiver position and satellite positions calculated from broadcast ephemerides, to generate the local code and carrier replicas. The early, late, and prompt code replicas are used to create correlations with the signal from the GPS front-end. We choose to use carrier frequency discriminators from each channel to form the Kalman filter measurement matrix. The Kalman filter then estimates the new errors, and, based on the updated errors, we can estimate the new navigation solution and create a prediction for the next time epoch.

In implementing the PIA vector tracking algorithm, we actively drew on the previous vector tracking research completed by S. Zhao and D. Akos (Additional Resources) as well as the open source software-defined radio (SDR) code created by K. Borre *et alia*. The open source code was designed to operate under high dynamics. We have extensively modified the code for operation under zero dynamics.

Experiment Setup. In the experiments, we used an off-the-shelf low-cost GPS sampler as the front-end to collect raw GPS signals. The front-end is a thumb-sized USB device designed to operate in conjunction with an SDR. It uses a sampling frequency from 4 to 16 megahertz and a quantization resolution of two bits. Because the quality of GPS receivers used in PMUs is generally higher than this kind of front-end, the results we obtain using data collected employing the low-cost sampler will provide a conservative, lower-bound estimate of results produced by PMU receivers applying our PIA tracking loop design.

For this experiment we used a fixed-reference choke ring antenna. During data collection the antenna had full view of an open sky with up to 10 satellites with clear line of sight. We then post-processed the data using the SDR for both scalar and PIA vector tracking.

Jamming Tolerance Performance. To determine the performance of the PIA vector-tracking algorithm, we added 1–10 decibels of simulated Gaussian noise to the raw GPS signal and processed the resulting data. Figures 4 to 6 show the time error results for varying levels of added noise. With no added noise, the maximum time errors for the scalar results were close to 45 nanoseconds whereas the time errors for the PIA results were around 10 nanoseconds.

Scalar tracking was able to produce decodable navigation bits until we increased the noise past four decibels. However, with every decibel of additional noise, the number of channels that experienced a loss-of-lock increased. At four decibels of additional noise (Figure 5), the scalar tracking loop was only able to lock onto four satellites while the original data could lock onto all nine. The time errors also increased as the noise

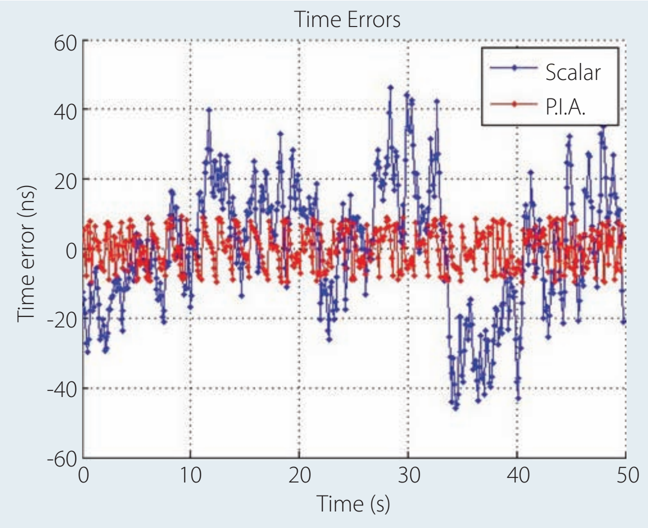


FIGURE 4 Time errors with no added noise

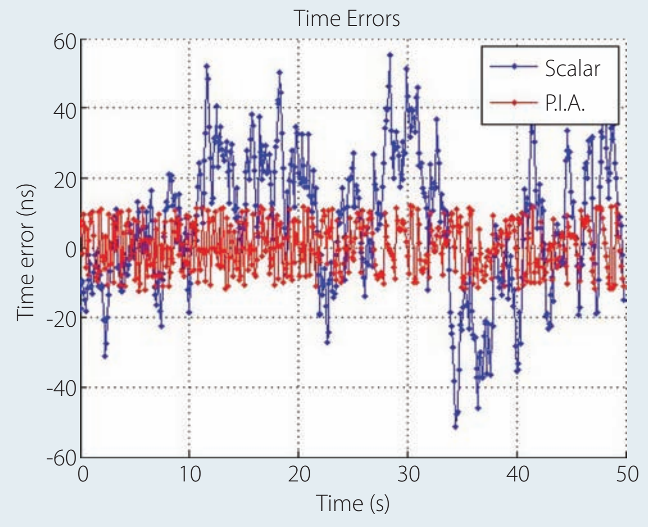


FIGURE 5 Time errors with 4 dB of added noise

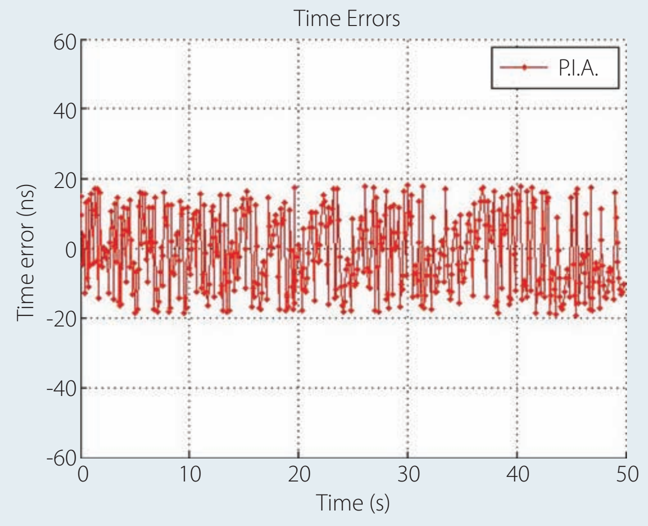


FIGURE 6 Time errors with 9 dB of added noise. Scalar tracking has stopped working.

increased: scalar results showed close to 60 nanoseconds of maximum errors and PIA results showed maximum errors of only 13 nanoseconds.

The PIA vector tracking loop continued operating until we increased the noise past nine decibels (**Figure 6**), at which point the maximum time errors were close to 20 nanoseconds.

The experimental results show that, in comparison to scalar tracking, PIA tracking gains at least a five-decibel advantage in tolerating jamming signals. This is equivalent to reducing the effective area of a jammer by a factor of 3.16.

Replay Spoofing Detection Performance. We designed the PIA vector-tracking algorithm to function with the known true position as the reference point. In a replay spoofing attack, also known as the meaconing attack, the position solution calculated would be equal to the position of the attacker. PIA vector tracking will instantly detect the attack if the attacker is sufficiently far (greater than 10 meters) from the receiver.

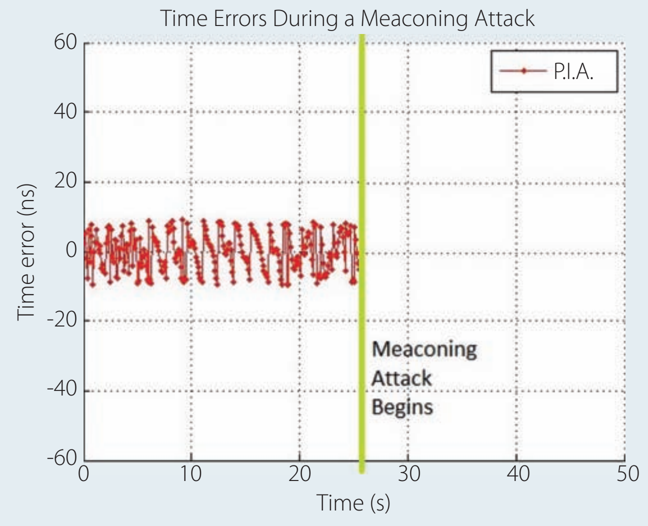


FIGURE 7 Time errors during a simulated meaconing attack with a 200-meter separation between the spoofer and the PMU GPS receiver.

Figure 7 shows the results of a meaconing attack simulation. Due to the fixed-position nature of the PIA vector-tracking loop, the algorithm fails to converge as soon as the meaconing attack begins. Therefore, this shows that our proposed PIA vector tracking is capable of detecting meaconing attacks.

Conclusions

This article presents a reliable and robust GPS-based timing mechanism that supports power system applications such as the PMU. We have designed a multi-layered multi-receiver architecture that incorporates eight countermeasures in all layers of signal and data processing.

Most of the countermeasures exploit the static and networked nature of time reference receivers. We have defined five threat models and qualitatively analyzed the effectiveness of each countermeasure against each threat model. Our analysis demonstrates that the redundant, independent but complementary countermeasures provide high reliability and robustness.

In our discussion in this article, we further implemented one of the countermeasures: the PIA tracking loop. Our experiments show that PIA tracking can improve the receiver's robustness against jamming attack and can detect replay spoofing attacks.

Accurate timing is a critical element for many economic activities around the world, including not only power grids but also communication systems and financial networks. All of these systems rely on static, networked GPS time reference receivers. Our multi-layered multi-receiver architecture, although developed in the context of power systems, is also applicable to these other systems.

Acknowledgments

This work was supported in part by the Trustworthy Cyber

Infrastructure for the Power Grid (TCIPG) under U.S. Department of Energy Award DE-OE0000097.

The authors would like to thank Jonathan J. Makela, Alejandro D. Dominguez-Garcia, Rakesh B. Bobba, and William H. Sanders for their helpful discussions and inputs.

This article is based on two of the authors' papers: "Reliable GPS-Based Timing for Power System Applications: A Multi-Layered Multi-Receiver Approach," in *Proceedings of the 2014 IEEE Power and Energy Conference at Illinois (PECI 2014)*, Champaign, Illinois USA, and "Robust GPS-Based Timing for Phasor Measurement Units: A Position-Information-Aided Approach," in *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014)*, Tampa, Florida USA.

Manufacturers

The front-end used to receive GPS signals was the SiGe GN3S sampler co-developed by the GNSS Lab at the University of Colorado and SiGe Semiconductor, now part of the product lines of **Skyworks Solutions, Inc.**, Woburn, Massachusetts USA.

Additional Resources

[1] Akos, D., "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," *NAVIGATION*, Vol. 59, No. 4, pp. 281–290, Winter 2012

[2] Bardout, Y., "Authentication of GNSS Position: An Assessment of Spoofing Detection Methods," *Proceedings of ION GNSS 2011*, Portland, OR, September 2011

[3] Borre, K., and D. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*, Springer, New York, 2007

[4] Heng, L. (2012a), and G. X. Gao, T. Walter, and P. Enge, "Automated Verification of Potential GPS Signal-in-Space Anomalies using Ground Observation Data," *Proceedings of IEEE/ION PLANS 2012*, Myrtle Beach, SC, April 2012

[5] Heng, L. (2012b), and G. X. Gao, T. Walter, and P. Enge, "GPS Signal-in-Space Integrity Performance Evolution in the Last Decade: Data Mining 400,000,000 Navigation Messages from a Global Network of 400 Receivers," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 48, No. 4, pp. 2932–2946, October 2012

[6] Heng L. (2013a), and T. Walter, P. Enge, and G. X. Gao, "Overcoming RFI with High Mask Angle Antennas and Multiple GNSS Constellations," *Proceedings ION GNSS+ 2013*, Nashville, TN, September 2013, pp. 3433–3442

[7] Heng L. (2013b), and D. B. Work, and G. X. Gao, "Cooperative GNSS Authentication: Reliability from Unreliable Peers," *Inside GNSS*, September/October 2013

[8] Jiang, X., and 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*, January 2013, 28(3):3253-3262. DOI: 10.1109/TPWRS.2013.2240706

[9] Lo, S., and D. D. Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal Authentication: A Secure Civil GNSS for Today," *Inside GNSS*, September/October 2009

[10] Psiaki, M. L., and B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 49, No. 4, pp. 2250–2267, October 2013

[11] Pullen, S., and G. X. Gao, "GNSS Jamming in the Name of Privacy: Potential Threat to GPS Aviation," *Inside GNSS*, March/April 2012

[12] Shepard, D. P., and T. E. Humphreys, and A. A. Fansler, "Going Up Against Time: The power Grid's Vulnerability to GPS Spoofing Attacks," *GPS World*, August 2012

[13] Soloviev, A., and J. Dickman, and J. Campbell, "MUSTER: A Collaborative GNSS Receiver Architecture for Weak Signal Processing," *Inside GNSS*, May 2013

[14] Swaszek, P. F., and R. J. Hartnett, "Spoof Detection using Multiple COTS Receivers in Safety Critical Applications," *Proceedings of ION GNSS+ 2013*, Nashville, TN, September 2013

[15] Wang, K., and M. Rothacher, "Stochastic Modeling of High-Stability Ground Clocks in GPS Analysis," *Journal of Geodesy*, Vol. 87, No. 5, pp. 427–437, 2013

[16] Wilson, R. E., "Uses of Precise Time and Frequency in Power Systems," *Proceedings of the IEEE*, Vol. 79, No. 7, pp. 1009–1018, 1991

[17] Zhao, S., and D. Akos, "An Open Source GPS/GNSS Vector Tracking Loop—Implementation, Filter Tuning, and Results," *Proceedings of ION ITM 2011*, San Diego, CA, January 2011

Authors

Liang Heng is a postdoctoral research associate in the Department of Aerospace Engineering, University of Illinois at Urbana-Champaign. He received the B.S. and M.S. degrees from Tsinghua University, China in 2006 and 2008, and the Ph.D. degree from Stanford University in 2012, each in Electrical Engineering. His research interests are cooperative navigation and satellite navigation. He is a member of the Institute of Electrical and Electronics Engineer (IEEE) and the Institute of Navigation (ION).

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 wngineering from Arizona State University. 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. Prof. 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. IG