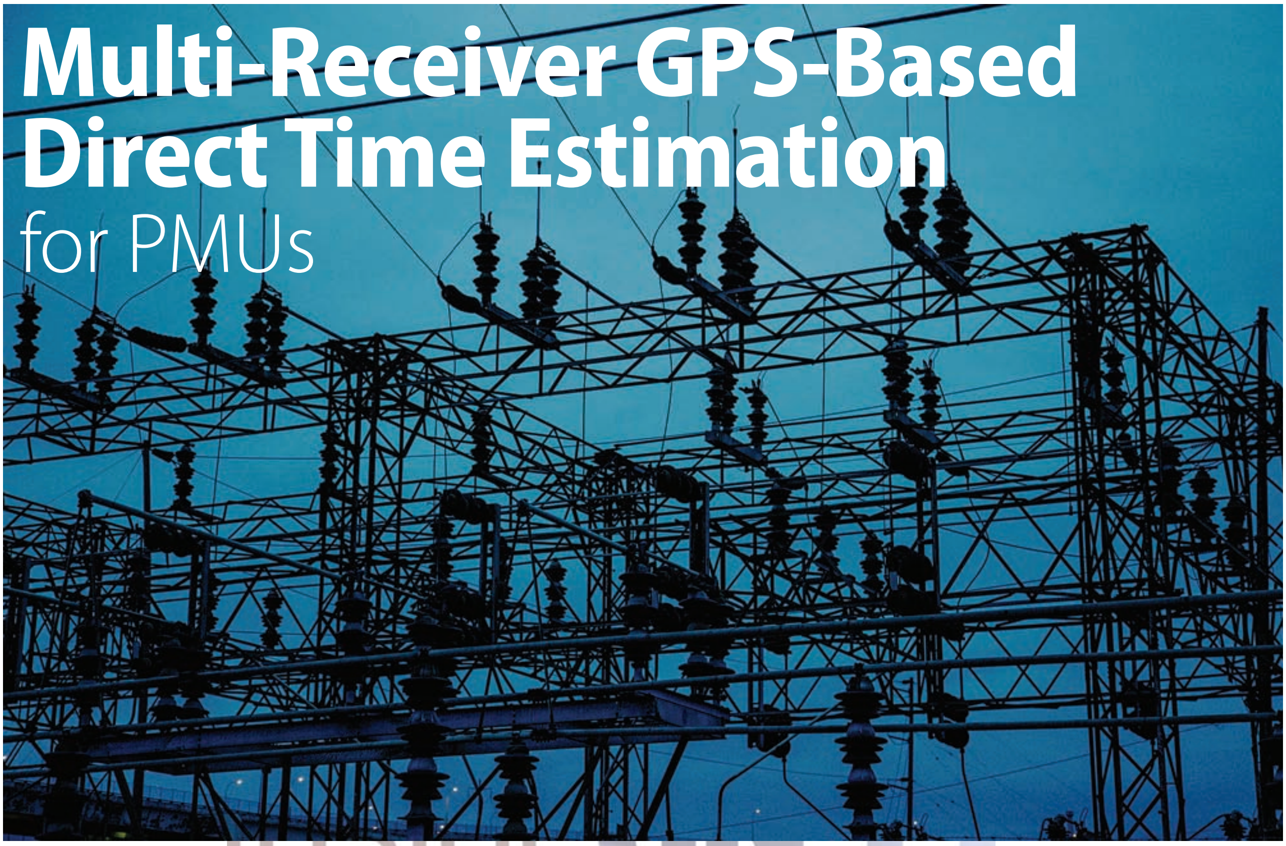
Multi-Receiver GPS-Based Direct Time Estimation for PMUs



Wikipedia Commons

While phasor measurement units depend on GPS for precise time and synchronization, GPS L1 C/A signals are vulnerable to external timing attacks because of their low power and unencrypted signal structure. Here the authors propose a novel multi-receiver direct time estimation algorithm using the measurements from multiple receivers triggered by a common clock. Through outdoor field experiments, they validate the algorithm's increased resilience against malicious timing attacks that include jamming and meaconing.

SRIRAMYA BHAMIDIPATI, YUTING NG, AND GRACE XINGXIN GAO
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Incorporation of real-time synchronized phasor measurements in the control of power grids can play an important role in maintaining the overall closed-loop stability of the power system. In the past, instability in the power grid caused disturbances ranging from small local perturbations to severe large scale blackouts as can be seen from **Figure 1**. Currently, the synchronization achieved in measurements collected using devices known as supervisory control and data acquisition (SCADA) is not robust enough for ef cient monitoring the power grid.

Modern power systems can benefit from deploying phasor measurement units (PMUs) as they provide synchronized measurements of up to 60 observations per second in regard to the current state of the system. The operation of PMUs greatly relies on precise time-keeping sources, such as GPS signals, to obtain absolute time for synchronization.

However, traditional GPS signals are of low power and unencrypted thereby making them susceptible to external timing attacks. In this article, we propose a novel multi-receiver direct time estimation (MRDTE) algorithm which utilizes the concept of maximum likelihood estimation.

This current setup is an extension of our earlier work focusing on single receiver direct time estimation (DTE), described in the paper by Y. Ng and G. X. Gao (2016) listed in Additional Resources near the end of this article. This prior article illustrated and verified the ability of DTE to detect meaconing attacks at an early stage and tolerate high noise levels. This multi-receiver architecture uses the information from spatially dispersed receiver locations to improve noise resilience and reduce the inf uence of external timing attacks.

Multi-Receiver Direct Time Estimation

With an aim to improve the robustness of our time-estimation method, we developed an extension that we named as multi-receiver direct time estimation. We propose the placement of multiple static antennas with pre-evaluated 3D position and velocity at dif erent corners in the same power sub-station. Utilizing the geographical diversity in the receiver locations, the signals from dif erent receivers are collectively analyzed to mitigate the ef ect of localized spurious signals.

In our setup, there are L dif erent receivers that receive GPS signals from N visible satellites at any time instant t. All the receivers are triggered by the same common external clock. Dif erent cable lengths introduce a bias across the receivers that can be pre-accounted for. Thereby, the clock states are considered to be the same across the receivers, as indicated in equation (1).

$X_{t,k}$: 3D Position and velocity of the k^{th} receiver at t^{th} time instant $= [x_k, y_k, z_k, \dot{x}_k, \dot{y}_k, \dot{z}_k]_t$ **(1)**

$T_{t,k}$: Clock states of the k^{th} receiver at t^{th} time instant $= [c\delta t_k, c\delta \dot{t}_k]_t$

The higher level architecture of the MRDTE described in **Figure 2** consists of two major steps. The first step involves applying a novel signal processing technique known as DTE.

In the second step, known as MRDTE filter, the DTE outputs obtained from the receivers are collectively processed through an overall kalman filter. The corrected overall clock vector $T_{t,\,overall}$ at any time instant t obtained as the output from MRDTE, is given as input to the PMUs. This strategy is adopted to reduce the search space from $8L$ $(X_{t,k}, T_{t,k})$ to 2 $(T_{t,overall})$, thereby increasing the robustness and decreasing the computational complexity.

Direct Time Estimation

DTE estimates the cumulative satellite vector correlation of the raw received GPS signal with the signal replica produced from each grid point $g_j = [c\delta t_j, c\delta \dot{t}_j]$ in a pre-generated 2D-search space (total M grid points). Taking the 3D position and velocity of the static receiver as the a priori information, the most plausible clock state of the receiver is evaluated based on the principle of maximum likelihood estimation, as shown in equations (2) through (4).

R: raw received GPS signal **(2)**

Y: signal replica of the GPS signal

$$= \sum_{i=1}^{N} Y^i$$

Y^i: signal replica corresponding to i^{th} satellite

corr_j: DTE correlation for the j^{th} clock candidate set **(3)**

$$= corr\left(R, \sum_{i=1}^{N} Y^i(g_j)\right)$$

$$= \sum_{i=1}^{N} corr\left(R, Y^i(c\delta t_j, c\delta \dot{t}_j)\right)$$

$$\text{corr-overall} = \max_{j=1}^{M} \text{corr}_j \quad (4)$$

The corresponding satellite channel delay residual is directly proportional to the clock bias residual, and the channel doppler residual is proportional to the clock drift residual. Given this, the channel delay and carrier doppler estimation are split into two parallel threads and independently estimated. (See **Figure 3**.)

Correlations are performed on a per satellite channel basis to obtain the correlation amplitude with respect to the code

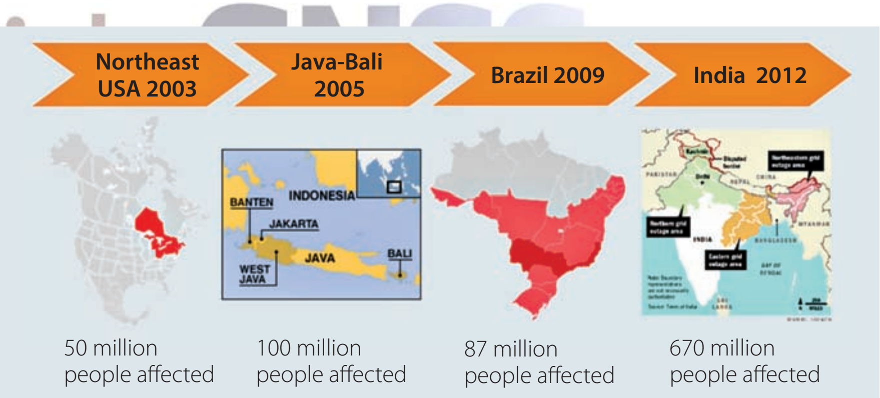


FIGURE 1 Wide-scale power blackouts in the world

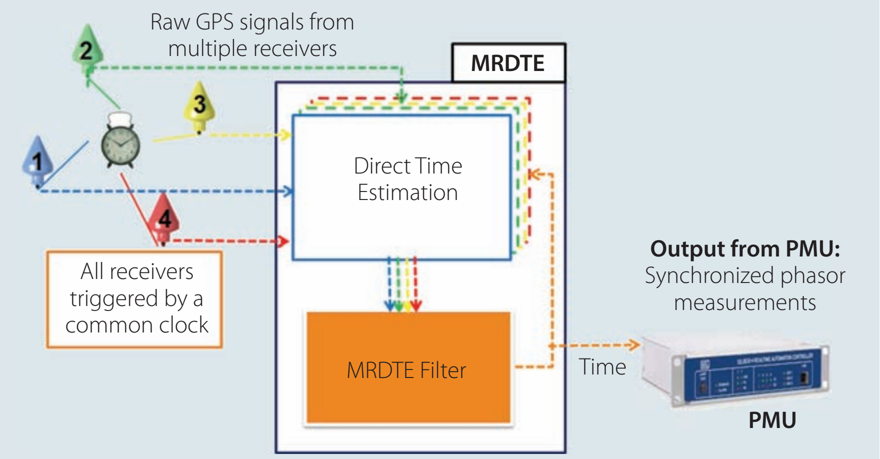


FIGURE 2 Architecture of MRDTE

residual in **Figure 4a** while fourier transforms are carried out in parallel to obtain the spectrum magnitude with respect to the carrier doppler residual as shown in **Figure 4b**.

Non-coherent summation of the correlation amplitudes and spectrum magnitudes is computed respectively across the N visible satellites. These obtained summation of correlation values are allocated as weights that represent the likelihood of a particular g_j in the 2D-search space.

MRDTE Filter. After obtaining, the measurement error vectors e_k for each of the individual receivers, an individual receiver level measurement update $T_{t,k}$ is done using a kalman filter. The next stage involves incorporating the individual receiver corrected clock parameters $T_{t,k}$k into an overall kalman filter to obtain the final corrected clock state $T_{t,overall}$ corresponding to the common shared clock.

The overall measurement update at any instant t is:

$$e_{t,overall} = \begin{bmatrix} T_{t,1} - \hat{T}_{t,\text{overall}} \\ \vdots \\ T_{t,k} - \hat{T}_{t,\text{overall}} \\ T_{t,L} - \hat{T}_{t,\text{overall}} \end{bmatrix} \quad (5)$$

$$H : \text{Observation matrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 & .. & 0 \\ 0 & 1 & 1 & .. & 0 \\ : & : & : & .. & : \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}_{(L+1)\times(L+1)}$$

$$K_t : \text{Kalman gain matrix}$$

$$T_{t,overall} : \text{Corrected state vector of the } k^{th} \text{ receiver}$$

$$= \hat{T}_{t,overall} + K_t e_{t,overall}$$

The prediction of the overall and individual receiver states for the next time instant t+1 is achieved by linearly propagating the clock parameters based on the first order state transition matrix.

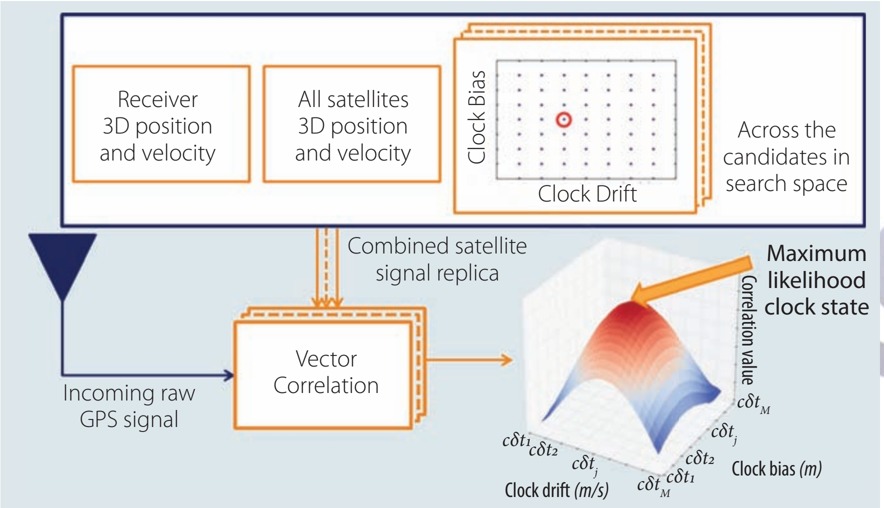


FIGURE 3 Direct Time Estimation

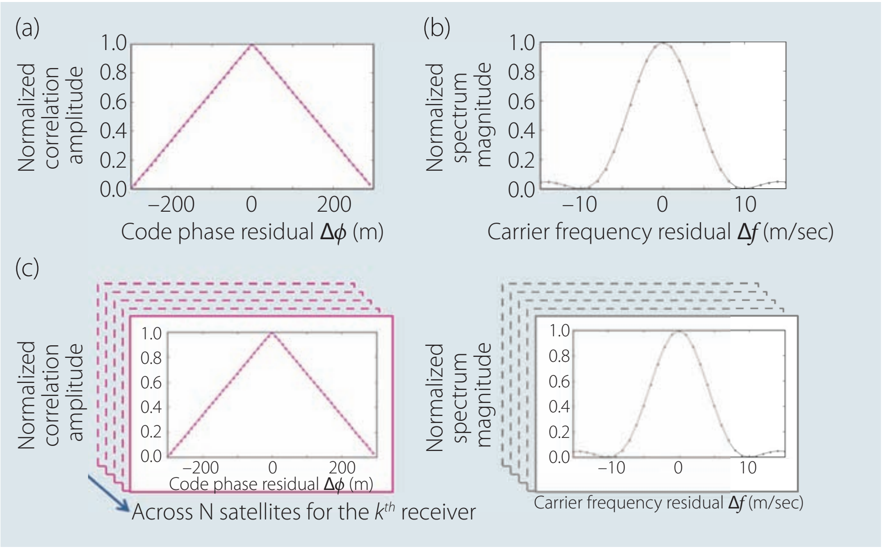


FIGURE 4 (a) shows the correlation amplitude plotted against the code phase residual. (b) shows the spectrum magnitude with respect to the carrier doppler frequency residual. (c) represents the non-coherent summation across satellites.

Initialization of MRDTE. The initialization $T_{0,k}$ for each receiver can be done using any commercial techniques like scalar tracking etc. or by considering an optimum initial search space. Given that power grid is a static system, the receiver locations can be accurately pre-determined using the already available of -the-shelf techniques and averaged over time to get the best 3D position and velocity estimate.

Experimental Setup

To evaluate our MRDTE approach, we set up a field experiment, as described in the following section.

Hardware setup. We validated the robustness of the proposed multi-receiver DTE using four GNSS antennas mounted onto the roof of Talbot Laboratory, University of Illinois at Urbana-Champaign, as shown in **Figure 5**.

The antennas are connected to a common chip scale atomic clock (CSAC), chosen for its low drift rate, to form a receiver network, and the raw voltage data are logged using respective universal software radio peripherals (USRPs) each equipped with a daughterboard as in **Figure 6**.

Software Setup. GNUradio, a free open-source software development toolkit that provides signal processing blocks to implement software radios, was used for collecting the raw GPS L1 signal samples from USRP at a sampling rate of two megahertz. We chose to implement this technique in the python software-defined radio developed in our lab (pyGNSS), given its f ex-

FIGURE 5 Four antennas located on roof of Talbot Laboratory, University of Illinois at Urbana-Champaign.Reference image of the setup taken from the article by D. Chou *et alia* listed in Additional Resources.

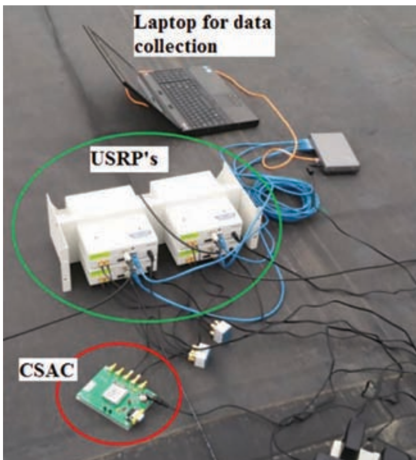


FIGURE 6 Hardware setup used for the experimental testing of MRDTE. Reference image of the setup taken from the article by D. Chou *et alia* listed in Additional Resources.

ible and object-oriented framework. In our case, the 3D position and velocity of the receivers are calculated using *multi-receiver vector tracking* as described in the article by Y. Ng and G. X. Gao (2015) listed in Additional Resources. For the vector correlation, we opted for a coherent integration time of $\Delta T = 20ms$. The measurement noise covariance matrix is evaluated using the covariance of the last 20 individual measurement residuals.

Results and Analysis

Virtual timing attacks, which include jamming and meaconing, are simulated and added onto the field data collected after which they are processed using MRDTE as discussed previously. While subjected to these external attack scenarios, we test the performance of MRDTE to that of conventional scalar tracking.

Jamming. Jamming involves broadcasting a high-power noise signal near the GPS frequency range thereby causing the GPS receivers to lose track of the signal being acquired. The conditions of jamming are generated by adding white Gaussian noise $A^{ej2\pi\Phi t}$ onto the incoming received signal. This noisy signal includes two components: random amplitude A, which is a measure of the strength of the noise being introduced and random phase Φ.

Figure 7 is indicative of the robustness of the MRDTE algorithm. In the presence of 12 decibels added noise, the scalar tracking loses track. However, the MRDTE still successfully tracks the signal accurately.

In **Figure 8**, the clock bias and clock drift residuals are compared for added noise with respect to the signal noise floor. In the presence of 5 decibels of added noise, the clock bias is estimated with an error of within 10 nanoseconds and, in the case of 12 decibels of added noise, within an error of 100 nanoseconds. Thus, a more robust clock state is estimated by implementing MRDTE algorithm.

Meaconing. In this case, a replay signal with similar GPS signal structure and signal power two decibels more than that of the authentic signal is added onto the incoming GPS signal. The first 36 seconds correspond to that of scalar tracking and after which the spurious signal is introduced represented by the thick black dotted line. At this point we turn on the MRDTE algorithm and compare its performance to

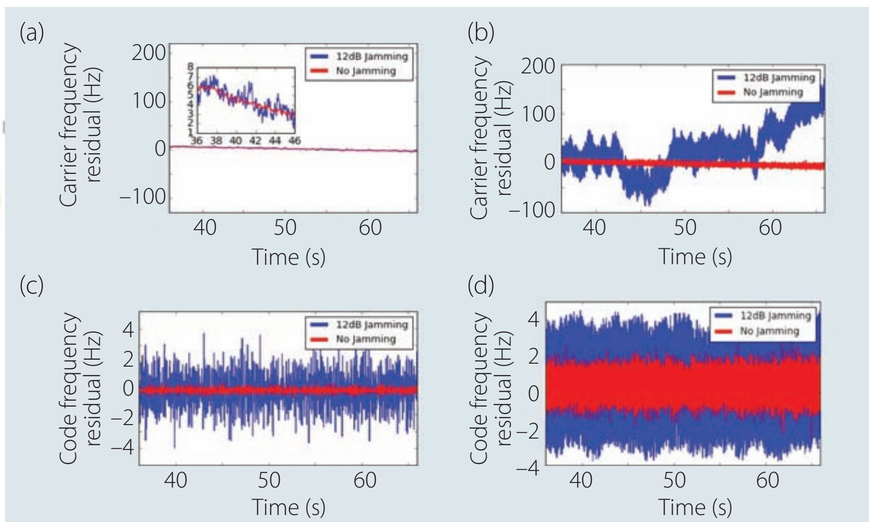


FIGURE 7 (a) carrier doppler frequency residual using MRDTE, (b) carrier doppler residual using scalar tracking, (c) code frequency residual using MRDTE, and (d) code frequency residual using scalar tracking. MRDTE is more robust than scalar tracking to jamming attacks. Under a jamming attack of 12 dB, MRDTE maintained accurate tracking while scalar tracking lost track.

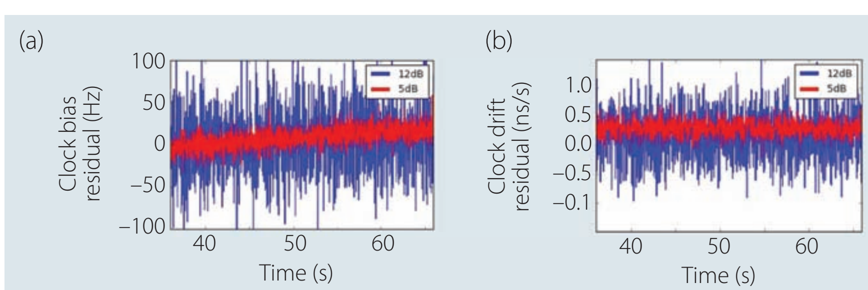


FIGURE 8 (a) clock bias residual comparison for 5 decibels and 12 decibels of added noise, and (b) clock drift comparison for 5 decibels and 12 decibels of added noise. Even with 12 decibels of added jamming, clock bias residual is within 100 nanoseconds and clock drift residual within 1.5ns/s.

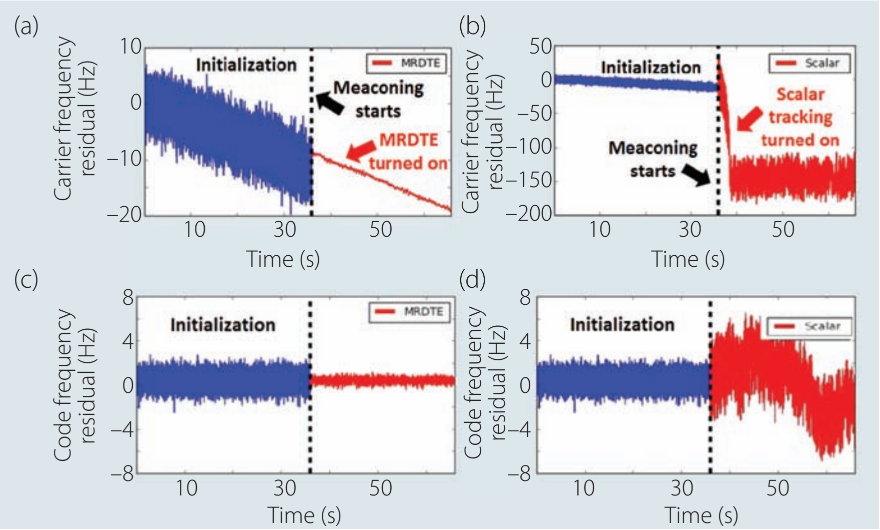


FIGURE 9 (a) carrier doppler frequency residual for MRDTE, (b) carrier doppler frequency residual for scalar tracking, (c) code frequency residual for MRDTE, and (d) code frequency for scalar tracking. Scalar tracking locks onto the meaconed signal whereas MRDTE maintains locking onto the legitimate signal. This demonstrates the robustness of MRDTE against meaconing attacks.

that of scalar tracking for the next 30 secs.

When meaconing starts, the scalar tracking locks onto the counterfeit signal as shown in **Figure 9** whereas the MRDTE still consistently tracks the authentic signal thereby mitigating the ef ect of meaconing attack.

Conclusions

This article proposed a novel MRDTE algorithm for secure and robust GPS time transfer using multiple static receivers sharing a common external clock. We leveraged the information redundancy and the known 3D positions of receivers to improve the robustness of the system. We implemented MRDTE using commercial available front-ends and our software platform PyGNSS. Through simulations of timing attacks based on GPS signals collected in field experiments, we demonstrate MRDTE's increased resilience against jamming and meaconing attacks.

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. 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 ref ect those of the United States Government or any agency thereof.

Manufacturers

The antennas used in the test equipment configuration were 3GNSSA4-XT-1 antennas from **AntCom Corporation**, Torrance, California USA. The CSAC used in this research was the Quantum SA.45s Chip Scale Atomic Clock from **Microsemi Corporation**, Aliso Viejo, California USA. The USRP was the DBSRX2 USRP Daughterboard from **Ettus Research** (a National Instruments company), Santa Clara, California USA.

Additional Resources

[1] Adamiak, M., and R. Hunt, Application of Phasor Measurement Units for Disturbance Recording, *Protection and Control Journal,* Spring 2009

[2] Chou, D., and Y. Ng, and G. Xingxin Gao, Robust GPS-Based Timing for PMUs Based on Multi-Receiver Position-Information-Aided Vector Tracking, ION International Technical Meeting 2015, Dana Point, California, January 2015

[3] Closas, P., and C. Fernandez-Prades, and J. Fernández-Rubio Â´ et al., "Maximum likelihood estimation of position in GNSS," Signal Processing Letters, IEEE, vol. 14, no. 5, pp. 359–362, 2007.

[4] Hart, D.G., and D. Uy, V. Gharpure, D. Novosel, D. Karlsson, and M. Kaba, "PMUs A New Approach to Power Network Monitoring," *ABB Review,* 2001

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

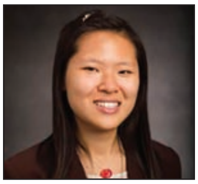
[6] Ng, Y., and G. X. Gao (2016), Robust GPS-Based Direct Time Estimation for PMUs in Proceedings of the IEEE/ION PLANS conference, Savannah, 2016.

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

[8] Schweitzer Engineering Laboratories, "Improve Data Analysis by TimeStamping Your Data," The Synchrophasor Report, May 2009, vol. 1, no. 3. conference (ION GNSS+ 2015), Tampa, 2015

Authors

Sriramya Bhamidipati is a graduate student in the Aerospace Engineering Department at the University of Illinois at Urbana-Champaign. She received her B.Tech. with honors in aerospace engineering and minor in systems and controls engineering from Indian Institute of Technology Bombay, India. Her research interests include GPS, computer vision, unmanned aerial vehicles, robotics, and control systems.



Yuting Ng is a graduate student in the Aerospace Engineering Department at the University of Illinois at Urbana-Champaign. She received her B.S. degree in electrical engineering, graduating with university honors, from the same university. Her research interests are in advanced signal tracking, navigation, control, LiDAR, RADAR, and UAVs.

Grace Xingxin Gao received her B.S. degree in mechanical engineering and her M.S. degree in electrical engineering from Tsinghua University, Beijing, China. She received her Ph.D. degree in electrical engineering from Stanford University. From 2008 to 2012, she was a research associate at Stanford University. Since 2012, she has been an assistant professor in the Aerospace Engineering Department at University of Illinois at Urbana-Champaign. Her research interests are systems, signals, control, and robotics. She is a senior member of IEEE and a member of ION. IG