GPS Spoofer Localization for PMUs using Multi-Receiver Direct Time Estimation

Sriramya Bhamidipati and Grace Xingxin Gao
University of Illinois at Urbana-Champaign

***Abstract*— Our work highlights the improved robustness of Phasor Measurement Units (PMUs) against meaconing i.e., record and replay attack by incorporating new protective measures to our prior work on Direct Time Estimation (DTE). In this paper, we propose a novel GPS spoofer localization based Multi-Receiver Direct Time Estimation (MRDTE) algorithm by leveraging the geometrical diversity of multiple receivers. DTE performs non-coherent summation across the satellites to evaluate the likelihood of the clock candidates considered from a pre-generated search space.**

Firstly, we execute DTE based multiple peak vector correlation to detect the presence of spoofer. Thereafter, we compare the time-delayed similarity in the signal properties across the geographically distributed receivers to distinguish these spoofing signals. Lastly, we perform non-coherent summation across the satellites at individual receiver level and then incorporate a Joint Filter module. This module includes a Particle Filter to estimate the spoofer location and a Kalman Filter to collectively process the maximum likely clock parameters obtained from individual receivers to estimate the precise UTC time.

We validate our algorithm under a complex case of meaconing attack generated by recording the GPS signals in the same place as our multi-receiver setup and later replaying them from a different location with higher power. Our experimental results demonstrate precise localization of the spoofer while simultaneously computing the GPS time to within the accuracy specified by the power community (IEEE C37.118).

I. Introduction and Related Work

Wide Area Monitoring System (WAMS) [1]–[3] depends on synchronized phasor (voltage and current) values obtained from distributed Phasor Measurement Units (PMUs) [4]. When the current power system is transferred to an automated smart grid in the future, these PMU measurements are crucial for high-resolution grid state estimation and early-stage detection of destabilizing conditions.

The IEEE C37.118 Standard for Synchrophasors defines that without any timing and magnitude errors, phase angle error of 0.573° ($\approx$ timing error of 26.5 μs) is the maximum allowable total vector error [5].

In this regard, PMUs maintain their synchronization by obtaining precise time stamps from accurate time keeping sources like GPS. GPS offers μs-level time accuracy and is freely available to users. Due to the global coverage provided by the GPS constellation, network-wide stability monitoring of the power grid is efficiently achieved. However, given that the civilian modulation codes are unencrypted and are of low signal power, GPS signals are vulnerable to external timing attacks.

The susceptibility of GPS signals to timing attacks like spoofing leads to potential threats in the power system. In spoofing, spurious counterfeit GPS signals are transmitted with high power [6] so as to manipulate the time supplied to the PMUs. A type of spoofing attack known as meaconing involves recording the GPS signals at a specified place and later replaying them with increased power.

In our prior work, we proposed our novel Direct Time Estimation (DTE) [7] and Multi-Receiver Direct Time Estimation (MRDTE) [8] architecture to improve the robustness of GPS timing supplied to the PMUs. MRDTE utilizes the known location of the spatially dispersed receivers to improve resilience against noise and external timing attacks.

In the aforementioned, we validated the improved attack-resilience of our MRDTE based timing as compared to the traditional scalar tracking and our prior work on Position-Information-Aided Vector Tracking [9]. Given that spoofing is a complex and sophisticated external timing attack, in our current work, we develop a novel architecture known as Spoofing Localization (LS) based MRDTE. The focus of our LS-MRDTE is to explicitly detect, mitigate and localize the spoofer using multiple peak vector correlation analysis and joint filter architecture.

The rest of the paper is as follows: Section II describes our LS-MRDTE architecture in detail and gives an overview of our Joint Particle and Kalman Filter. Section III validates the performance of our LS-MRDTE in localizing the spoofer through outdoor experiments under different scenarios of GPS meaconing attack. Section IV concludes the paper.

II. GPS Spoofer Localization based MRDTE

Our novel Spoofer Localization (LS) module is used in conjunction with our MRDTE algorithm to provide attack-resilient GPS timing to the PMUs by detecting and localizing the source of spoofing signals. Given that the power substation is a static, we pre-compute the position and velocity ($X_k,\ k = 1,..,L$) of our L spatially dispersed multiple receivers and use that for position aiding. In addition, all the receivers in our setup are synchronized using a common clock.

A. Overview of LS-MRDTE

The underlying principle of our LS-MRDTE algorithm depends on our novel signal processing technique known as the Direct Time Estimation (DTE). Unlike the scalar tracking, DTE directly works in the navigation domain and does not estimate the intermediate pseduorange and pseduorate measurements.

As in Eq. 1, DTE estimates the cumulative satellite vector correlation (N satellites-in-view) of the received raw GPS signal (R) with the signal replica (Y) produced for each grid point g_j from a pre-generated search space that consist of G gridpoints. Later, the principle of maximum likelihood estimation is applied to estimate the maximum likely clock parameters at any instant.

$$\begin{aligned} \text{corr}_j &: \text{vector correlation for the } j^{th} \text{ grid point} \\ &= corr(R, \sum_{i=1}^{N} Y^i(g_j)) \\ g_j &= [c\delta t_j, c\delta \dot{t}_j] \quad , \; j = 1, ..., G \\ \text{corr-overall} &= \max_{j=1}^{G} \text{corr}_j \end{aligned} \tag{1}$$

Our MRDTE algorithm executes DTE algorithm at each individual receiver level and later computes the joint probabilistic distribution across the receivers. Therefore, we leverage the information redundancy and geometrical diversity of the receivers to improve the robustness of the GPS timing given to the PMUs as input.

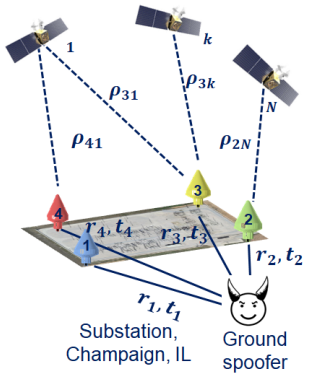


Fig. 1: Multiple receivers considered for our LS-MRDTE algorithm to localize a ground spoofer.

To localize the ground spoofer as seen in Fig. 1, we utilize the concept that this spoofer is relatively in close proximity to the multiple receiver setup as compared to the authentic GPS satellites that are 20200 km.

B. Architecture of LS-MRDTE

In our algorithm, we consider the scenario of an unsynchronized meaconing attack by a single spoofer present in the direct Line-Of-Sight (LOS) of our multi-receiver setup. We also assume that the spoofing signals sent by the attacker effect all the receivers.

Our proposed LS-MRDTE addresses the meaconing attack in four stages as shown in Fig. 2:

1) Firstly, we execute multi-peak vector correlation to detect all the significant peaks found in the pre-generated search space considered.
2) Next, we detect and distinguish the spoofing signals by comparing the time-delayed similarity in the signal properties received across the geographically distributed receivers.

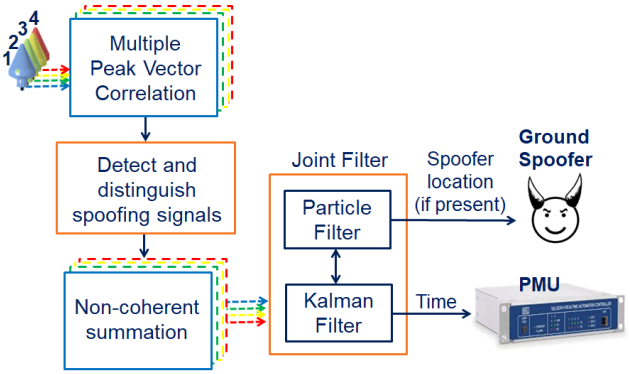


Fig. 2: High level architecture of our LS-MRDTE algorithm.

3) We perform non-coherent summation across the satellites for each receiver to estimate the maximum likely clock parameters in case of authentic signals and to compute the shift in the emulated peak in case of malicious signals.
4) Lastly, we execute our Joint Filter module which consists of a Particle Filter that localizes the spoofer; and a Kalman Filter that collectively processes the maximum likely clock parameters obtained from different receivers to estimate the UTC time that is sent to the PMUs.

C. Our LS-MRDTE Algorithm

In our LS-MRDTE, we consider L receivers (> 3) and N satellites-in-view at any time instant t. The first stage is our multiple peak based vector correlation algorithm. Based on our DTE algorithm, this module estimates all the significant peaks from the considered search space.

1) Spoofer Detection:

By utilizing the known 3D position and velocity of the satellites and receivers, we generate a combined satellite signal replica corresponding to each of the grid points (g_j) as in Fig. 3. Then, multiple peak vector correlation of the incoming raw GPS signal and our combined satellite replica is executed to obtain the likelihood of each of the grid points.

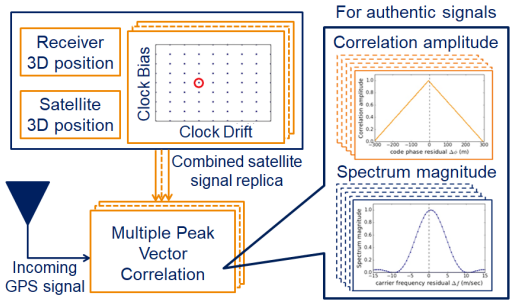


Fig. 3: Detailed flow of vector correlation. Refer to [7].

At the individual receiver level, vector correlation plots the correlation amplitude and spectrum magnitude for each satellite. Correlation amplitude depends on the code phase

residual ($\Delta\phi^i_{code}$) which is proportional to the clock bias candidate ($\Delta c\delta t_j$). Similarly, spectrum magnitude depends on the carrier doppler frequency residual (Δf^i_{carr}) which is proportional to the clock drift candidates ($\Delta c\delta \dot{t}_j$). For authentic signals, the correlation amplitude and spectrum magnitude plots show a single clear peak as in Fig. 3 across the clock candidates considered.

However, under meaconing attack, we observe multiple significant peaks in the correlation amplitude plotted against the clock bias candidates as in Fig. 4. Of these, one peak corresponds to the spoofing signals and the other corresponds to the authentic signals. Across the satellites, we can observe that the peaks occur consistently at around the same clock candidates with a difference in the magnitude of the correlation amplitude values.

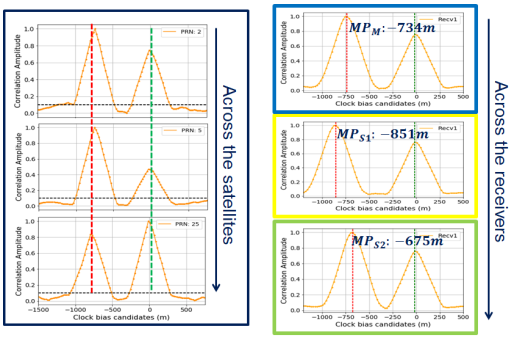


Fig. 4: Under meaconing attack, multiple peaks are detected in the vector correlations plots. The clock bias candidate that correspond to malicious peak passing through the red dotted line is consistent across the satellites and show a significant shift across the receivers.

Similar comparison is conducted across the receivers as in Fig. 4. An important property of the ground spoofer is that due to close proximity, there is a time-delayed similarity in signals properties across the geographically distributed receivers. After this non-coherent summation across the satellites is carried out at the individual receiver level to obtain weights that correspond to the likelihood of the grid point (g_j). For authentic signals, principle of maximum likelihood estimation is carried out to obtain the maximum likely clock parameters.

For spoofing signals, one of the receivers is designated as master ($k = 1$) and the others as slaves ($k = 2,..,L$). We compute the shift in the malicious peak for each master-slave pair which is equivalent to the difference in the range of receivers from the spoofer. This algorithm not only detects the counterfeit signals but also distinguishes them from that of authentic signals.

$$MP_1 - MP_k = r_1 - r_k, \qquad k = 2,..,L \tag{2}$$

Due to position aiding, the unknown spoofer is localized using Particle Filter branch of the Joint Filter module. Simultaneously, the Kalman Filter branch of the Joint Filter collectively processes the maximum likely clock parameters obtained from different receivers to estimate the corrected clock bias and clock drift parameters which are used to estimate the UTC time.

2) Spoofer Localization using Particle Filter:

The first branch of our Joint Filter module implements a Particle Filter to localize the spoofer (X_{sp}) based on the shift in the malicious peaks for each of the master-slave pair.

$$Z_t = \begin{bmatrix} MP_1 - MP_2 \\ \vdots \\ MP_1 - MP_k \\ MP_1 - MP_L \end{bmatrix} = \begin{bmatrix} ||X_1 - X_{sp}|| - ||X_2 - X_{sp}|| \\ \vdots \\ ||X_1 - X_{sp}|| - ||X_k - X_{sp}|| \\ ||X_1 - X_{sp}|| - ||X_L - X_{sp}|| \end{bmatrix} \tag{3}$$

We generate α particles $\hat{X}_{n,sp}$, $n = 1,...,\alpha$ around the initial guess that is assumed to be the centroid of the multiple receiver setup. The geographical area to be spanned, distribution and number of particles are considered based on the receiver setup during the initialization phase.

First, we update the weights of all the α particles based on our measurement model by computing the probability of the given measurement of a particle given the actual measurement obtained:

$$Z_{n,sp} = \begin{bmatrix} ||X_1 - X_{n,sp}|| - ||X_2 - \hat{X}_{n,sp}|| \\ \vdots \\ ||X_1 - X_{n,sp}|| - ||X_k - \hat{X}_{n,sp}|| \\ ||X_1 - X_{n,sp}|| - ||X_L - \hat{X}_{n,sp}|| \end{bmatrix}$$

$$P_{w_n} = \frac{e^{\frac{-(Z_t - Z_{n,sp})^2}{2R_{pf}}}}{\sqrt{2\pi R_{pf}}} \tag{4}$$

$$P_{w_n} = \frac{P_{w_n}}{\sum_{n=1}^{\alpha} P_{w_n}}$$

After obtaining the weights, we randomly (β) re-sample new set of α particles from the cumulative distribution of the weights P_{w_n}. Based on statistical probability, on an average, we obtain the particles with higher probability. Then the mean of these particles is assigned as the estimate of the spoofer at that particular instant.

$$\begin{aligned} X_{n,sp} &= \hat{X}_{n,sp} \qquad \text{if } \beta \leq \text{cumsum}(P_{w_n}) \\ X_{pf,sp} &= \text{mean}(X_{n,sp}) \end{aligned} \tag{5}$$

Finally the state of the particles are estimated for the next instant based on the state transition matrix of a stationary spoofer. The measurement and process noise covariance matrix (R_{pf}, Q_{pf}) are manually tuned during initialization to efficiently localize the spoofer.

3) GPS time using Kalman Filter:

The maximum likely clock parameters obtained from individual receivers are processed using our second branch of Joint Filter module i.e., Kalman Filter to obtain the measurement error vector (e_t).

The measurement update equations are as follows:

$$e_t = \begin{bmatrix} T_{t,1} - \hat{T}_t \\ : \\ T_{t,k} - \hat{T}_t \\ T_{t,L} - \hat{T}_t \end{bmatrix} \tag{6}$$

H : Observation matrix, $(2L) \times (2L)$

$$= \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}^T$$

$\hat{P}_t$: Predicted state error covariance matrix

R_t : measurement noise covariance matrix

$$= \begin{bmatrix} R_{t,1} & .. & 0 & .. & 0 \\ : & : & R_{t,k} & : & : \\ 0 & .. & 0 & .. & R_{t,L} \end{bmatrix} \tag{7}$$

K_t : Kalman gain matrix

$$= \hat{P}_t H^T (H \hat{P}_t H^T + R_t)^{-1}$$

ΔT_t : State error vector

$$: K_t e_t$$

T_t : Corrected state vector of the k^{th} receiver

$$= \hat{T}_t + \Delta T_t \tag{8}$$

P_t : Corrected state error covariance matrix

$$= (I - K_t H) \hat{P}_t$$

We linearly propagate the clock parameters based on the first order state transition matrix to predict the common clock parameters for the next time instant $t+1$. The time update equations are:

F : State transition matrix, 2×2

$$= \begin{bmatrix} 1 & \Delta T \\ 0 & 1 \end{bmatrix}, \quad \Delta T \text{is the update interval}$$

Q_t : State process noise covariance matrix

$$= F \begin{bmatrix} 0 & \Delta T \\ 0 & (c \times \sigma_\tau)^2 \end{bmatrix} F^T \tag{9}$$

σ_τ : allan deviation of the front-end oscillator, (s)

$\hat{T}_{t+1}$: Predicted state vector for the $(t+1)^{th}$ instant

$$= F T_t$$

$\hat{P}_{t+1}$: Predicted state error covariance matrix

$$= F P_t F^T + Q_t \tag{10}$$

III. Results and Analysis

In this section, we validate the accuracy of spoofer location and robustness of GPS timing estimated using our LS-MRDTE algorithm subjected to meaconing attack.

A. Experimental Setup

We installed four AntCom 3GNSSA4-XT-1 GNSS antennas on the rooftop of Talbot Laboratory‘(TL), Urbana, Illinois and the Spoofer is located approximately 300 m away on the rooftop of Electical and Computer Engineering (ECE), Urbana, Illinois as seen in the Fig. 5.

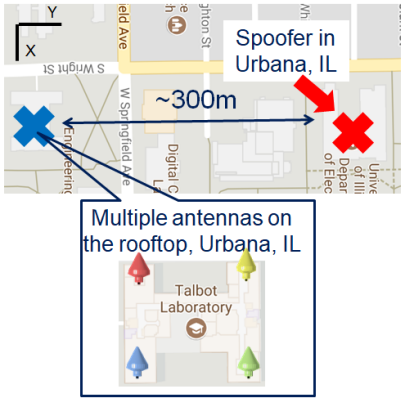


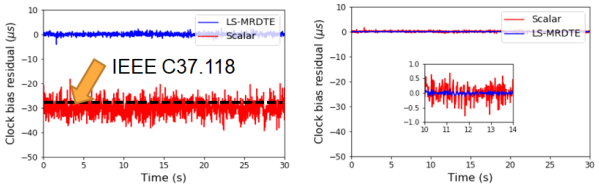
Fig. 5: Experimental setup for validating our LS-MRDTE algorithm. The blue cross corresponds to the known multi-receiver setup and the red cross corresponds to the spoofer position to be localized.

The data is collected using five (four+one) Universal Software Radio Peripherals (USRP-N210's) which are triggered using a Microsemi Quantum SA.45s Chip Scale Atomic clock (CSAC). The raw GPS signals are collected at both the locations and then post-processed using our pyGNSS platform which is a python based object oriented framework.

The 3D position and velocity of the GPS antenna locations are pre-determined using our Multi-receiver Vector Tracking [10] algorithm and used for position aiding. The integration time considered for our LS-MRDTE algorithm is $\Delta T = 20$ ms. In our Particle Filter, we generate 1000 random particles of uniform distribution at every instant. In our Kalman Filter, our measurement noise covariance matrix R_t is estimated by computing the covariance of the past 15 measurement error vector values.

B. Experimental Results

Virtual meaconing attack with 2 dB higher power and which induces a delay of 30 μs is added to the authentic GPS signals collected using our multi-receiver setup. This violates the IEEE.C37.118 standards, according to which the timing error between PMUs should not exceed 26.5μs.



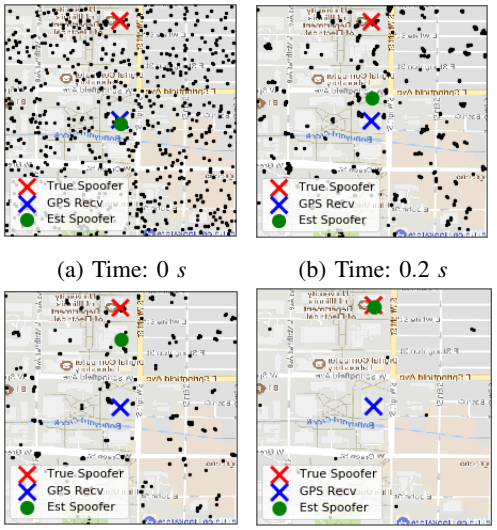
(a) 2 dB added meaconing (b) No meaconing

Fig. 6: Comparison of clock bias residuals; The red line corresponds to scalar tracking and blue line corresponds to our LS-MRDTE; (a) Under 2 dB of added meaconing that induces a delay of 30μs; (b) Under no added meaconing. Our LS-MRDTE estimates GPS time accurately while the conventional scalar tracking shows an error in the clock bias residuals of 30 μs thereby violating IEEE.C37.118.

In the situation, we record GPS signals on the same TL rooftop as our multi-receiver setup and then replay later from the top of ECE building as meaconed signals.

In the Fig. 6, we compare the increased robustness of our LS-MRDTE as compared to the conventional scalar tracking. Under no meaconing, we observe that both scalar tracking and our LS-MRDTE shows μs time accuracy. Under 2 dB added meaconing, the scalar tracking locks to the meaconed signals and thereby computes an error in the clock residual of around 30 μs which is equivalent to the meaconed delay induced. However, our LS-MRDTE accurately detects these spoofing signals and accurately estimates the GPS time to the order of μs.

The Fig. 7 shows the time series convergence of our Particle Filter starting with the initial guess of the spoofer location to be same as the centroid of our multi-receiver setup calculated as $\left(\frac{X_1+X_2+X_3+X_4}{4}\right)$. We observe that our LS-MRDTE accurately converges to the true location of the spoofer in less than 0.25 s thereby demonstrating the robustness of our algorithm.



(a) Time: 0 s (b) Time: 0.2 s

(c) Time: 0.22 s (d) Time: 0.24 s

Fig. 7: Our LS-MRDTE based Spoofer localization using Particle Filter: (a) First iteration; (b) Tenth iteration; (c) Eleventh iteration; (d) Twelfth iteration; Red cross denotes the actual location of the spoofer while blue cross corresponds to the location of our multi-receiver setup. Green blob depicts the estimate of the spoofer at each time instant. We observe that our LS-MRDTE based Particle Filter accurately converges to the true spoofer.

IV. Conclusions

In conclusion, we demonstrated increased resilience of PMUs in the power grid by extending our MRDTE platform to detect and localize the ground spoofer. Our LS-MRDTE algorithm utilizes the geometry of geographically distributed receivers and principle of vector correlation to analyze this GPS vulnerability. Our experimental results validated the precise localization of the spoofer to within 3 m accuracy and the UTC time to μs level which is compliant with the accuracy requirements specified by the power community (IEEE.C37.118).

Acknowledgment

I would like to thank my lab members at University of Illinois: Arthur Chu, Shubhendra Chauhan and James Kok for helping with the data collection and experimental setup.

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

References

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

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

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

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

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

[6] J. S. Warner and R. G. Johnston, "A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing," Journal of Security Administration, vol. 25, no. 2, pp. 19-27, 2002.

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

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

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

[10] Y. Ng and G. X. Gao, "GNSS Multi-Receiver Vector Tracking", IEEE Transactions on Aerospace and Electronic Systems. vol. PP, no.99, doi: 10.1109/TAES.2017.2705338, May 2017.