GPS Multi-Receiver Joint Direct Time Estimation and Spoofer Localization

Sriramya Bhamidipati, Student Member, IEEE and Grace Xingxin Gao, Senior Member, IEEE

Abstract—We propose a novel algorithm on joint estimation of GPS time and spoofer location (LS) using Multi-Receiver Direct Time Estimation (MRDTE). We utilize the geometry and known positions of multiple static GPS receivers distributed within the power substation. DTE directly estimates the maximum likely clock parameters from a pre-generated set of clock candidates by performing multi-peak vector correlation across the satellites. We compare the time-delayed similarity in the signal properties across the geographically distributed receivers to detect and distinguish the spoofing signals. Later, we localize the spoofer using our joint Particle and Kalman Filter.

We validate the robustness of our LS-MRDTE subjected to spoofing attacks such as meaconing and data-level spoofing. Our experimental results demonstrate precise localization of the spoofer while simultaneously estimating GPS time to within the accuracy specified by the power community (IEEE C37.118).

Keywords—GPS, Spoofing, Meaconing, Maximum Likelihood Estimation, Kalman Filter, Particle Filter, Vector Correlation, Phasor Measurement Units, Cramér Rao Lower Bound, Detection, Localization

I. INTRODUCTION

In power grid, Wide Area Monitoring System (WAMS) [1]-[3] depends on synchronized phasor (voltage and current) measurements 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.

A. GPS Timing in PMUs

The IEEE C37.118.1-2011 describes the standarized measures to evaluate the stability of the power grid [5]. This standard evaluates the Total Vector Error (TVE) which depends on three parameters: magnitude, timing and phase angle. With no errors in timing and magnitude, phase angle error of 0.573° which corresponds to a 1% TVE, is the maximum allowable TVE as in Fig 1(a). This phase angle error is equivalent to a timing error of 26.5 µs which is used as a benchmark in our power grid stability analysis [6]-[7].

In this regard, PMUs maintain network-wide synchronization by obtaining precise time stamps from time keeping sources such as GPS, external atomic clocks etc. Civil GPS signals provide µs-level time accuracy and are 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, the power of GPS signals received is as low as 10⁻¹⁶ W, which is below the thermal noise floor. In addition, the GPS civil signals are unencrypted, with their PRN codes explicitly described in publicly available documents [8]. This makes the GPS signal spectrum susceptible to external timing attacks such as jamming [9]-[10], spoofing [11]-[12] etc.

![Fig. 1: (a) IEEE C37.118 standard for synchrophasors. Maximum allowable TVE is 1%; (b) during spoofing, GPS signal acquisition shows two significant peaks one due to authentic signals and other due to spoofing.](image)

B. Impact of spoofing attacks

The susceptibility of GPS signals to spoofing leads to potential threats in the power system. In spoofing, counterfeit signals are transmitted as in Fig. 1(b) to mislead the PMU with incorrect time and thereby disrupt the stability of the grid. A spoofer aims to maximize the time error induced while minimizing the probability of being detected. The various GPS spoofing attacks which threaten the stability of the power systems are as follows:

1) Meaconing: A spoofer executing meaconing attack (also known as record and replay) as seen in Fig. 2(a), records the GPS signals and replays them at a later time to overpower the authentic signals and manipulate the receiver [13]. To execute this attack, the spoofer doesn’t require the knowledge of encryption codes and is thereby capable to spoof even military receivers.

2) Data-level spoofing: In data-level spoofing, a spoofer modifies the ephemeris [14] such that the satellites are shifted in position along their Line-Of-Sight (LOS) to the target receiver as in Fig. 2(b). This causes the receiver to still estimate the correct location but wrong time thereby covertly manipulating the PMUs.

3) Signal-level spoofing: This is a sophisticated three-stage attack as shown in Fig. 2(c). At first, a spoofer generates and broadcasts counterfeit GPS signals identical to the authentic signals received at the target receiver [15]. In the second stage, the power of these malicious signals is slowly increased to mislead the target receiver to lock onto these counterfeit signals. Once locked, the...
spoofing manipulates the time by moving the counterfeit signal away from the true time. Since there is no sudden change in the GPS timing output, this method cannot easily be detected by traditional methods.

![Image](image.png)

(a) Meaconing attack  
(b) Data-level spoofing attack  
(c) Signal-level spoofing attack

Fig. 2: Types of spoofing attacks: (a) meaconing attack involving record and replay of GPS signals; (b) data-level spoofing that transmits incorrect ephemeris; (c) signal-level spoofing that generates spoofing signals to trick the receiver into latching onto the spoofing peak.

C. Related Work

One of the works on spoofing [16] analyzes the requirements for successful spoofing attacks and analytically identifies the location and precision with which the attacker needs to generate the corresponding spoofing signals. This work describes the characteristics of the spoofing attacker and their temporal and spatial effect on the receivers.

The hazardous impact of GPS timing attacks has recently gained worldwide attention due to the successful spoofing of an $80 million yacht, demonstrated in [17]. Furthermore, tests have been conducted to demonstrate the vulnerability of PMUs to GPS spoofing attacks [18].

Various countermeasures have been proposed by researchers [19] to tackle varying complexity of spoofing attacks on civilian GPS signals as seen in Fig. 2. Some of the state-of-the-art techniques deal with analyzing the physical characteristics of the signal such as satellite signal strength, noise floor, automatic gain control (AGC) and angle of arrival (AOA). Also, a simple spoofing detector based on analyzing the position data has been proposed in [20] that employs Gaussian based Neyman-Pearson perspective.

A probabilistic countermeasure has been proposed in [21] that leverages the underlying correlation between the errors at co-located receiver positions to detect the presence of spoofing attacks. The increase in complexity of placing a successful spoofing attack has been demonstrated by observing the $L_1$ carrier differences between multiple receivers in [22]. However, the above mentioned methods are not completely resilient against advanced attacks capable of manipulating the navigation message while maintaining the original signal characteristics or that can perform seamless takeover attack.

In [23] researchers analyze the security of GPS timing in PMUs against spoofing attacks by detecting and localizing the presence of the spoofing source using multilateration techniques. A spoofing resistant GPS receiver known as SPREE has been proposed in [24], that detects the spoofing signals using auxiliary peak tracking technique and analyzes its theoretical and practical bounds within which it successfully tracks the malicious signals.

In our prior work, we proposed our novel Direct Time Estimation (DTE) [25] architecture to improve the robustness of GPS timing supplied to the PMUs. We extended our work to Multi-Receiver Direct Time Estimation (MRDTE) [26] that utilizes the known location of the spatially dispersed receivers to improve resilience against 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 [27].

D. Our work and contribution

To address GPS spoofing, which is a complex and sophisticated external timing attack, we develop a novel algorithm on joint estimation of spoofer location (LS) and GPS time using MRDTE. The focus of our LS-MRDTE is to explicitly detect and distinguish the spoofing signals using multiple peak vector correlation and later mitigate and localize the spoofer using joint Particle and Kalman Filter. In our prior work [26], we described the framework of MRDTE and in [28], we showed the preliminary results of our LS-MRDTE subjected to meaconing. In this paper, we present our new contributions in the following aspects:

1) To analyze the localization accuracy obtained, we theoretically formulated the impact of the geometry and positions of multiple receivers in estimating the Cramér Rao Lower Bound (CRLB).

2) We mathematically estimated the covariance of the measurements obtained by executing multiple peak vector correlation designed to detect and distinguish the spoofing signals. These measurements are given to the joint Particle and Kalman Filter to locate the spoofer.

3) We also estimated the probability of spoofer detection using our LS-MRDTE based on the covariance of the measurements estimated.

4) During spoofing, we demonstrated the increased robustness of our LS-MRDTE in estimating the GPS signal parameters as compared to single receiver DTE (SRDTE) and traditional scalar tracking.
5) We validated the accuracy of estimated GPS time and spoofer location using our LS-MRDTE subjected to different scenarios of spoofing attacks such as meaconing and data-level spoofing.

The rest of the paper is as follows: Section II describes our LS-MRDTE architecture in detail and gives an overview of the Joint Particle and Kalman Filter module. We also theoretically prove the lower bounds of the spoofer localization accuracy obtained using CRLB and estimate the probability of spoofer detection. Section III validates the performance of our LS-MRDTE in localizing the spoofer and estimating the GPS time through outdoor experiments under different scenarios of GPS spoofing attacks. Section IV concludes the paper.

II. JOINT ESTIMATION OF SPOOFER LOCATION AND GPS TIME USING MRDTE

Our novel joint estimation algorithm is used in conjunction with our multiple receiver based DTE to simultaneously localize the source of spoofing signals and provide attack-resilient GPS timing to the PMUs.

A. Background of GPS Signal Parameters

Given that the power substation is static, we pre-compute the position and velocity (\(X_k, \dot{X}_k k = 1, ..., L\)) of our \(L (> 3)\) spatially dispersed multiple receivers [29] and use this information for position aiding. In addition, all the receivers in our setup are synchronized using a common clock.

\[
\begin{align*}
X_k & : \text{Known position of the } k^{th} \text{ receiver} \\
& = [x, y, z]_k \\
\dot{X}_k & : \text{Known velocity of the } k^{th} \text{ receiver} \\
& = [\dot{x}, \dot{y}, \dot{z}]_k \\
T & : \text{Clock state of the receivers} \\
& = [c \delta t, c \delta t_d],
\end{align*}
\]

where \(t\) denotes the time instant, \(c = 299792458 \text{ m/s}\) is the velocity of light, \(c \delta t\) denotes clock bias and \(c \delta t_d\) denotes clock drift.

For L1 frequency, the transmitted GPS civilian signals from the \(i^{th}\) satellite are represented as:

\[
x_i^t = 9\lambda_t \left\{ \sqrt{2P_t} U^i(t) e^{j2\pi f_{L1}t} \right\},
\]

where \(U^i(t) = D^i(t)G^i(t), P_t\) represents the transmitted power of the GPS signal and \(f_{L1} = 1575.42 \text{ MHz}\) is the frequency of L1 GPS signals. \(D^i(t)\) and \(G^i(t)\) denotes the navigation databit and the L1 C/A code chip of the \(i^{th}\) satellite at any time instant \(t\).

The GPS signal replica \((Y)\) given by Eq. (2) depends on 4 signal parameters for each of \(i^{th}\) satellite which include carrier properties denoted by the carrier frequency \((f_{\text{carr}}^i)\) and carrier phase \((\phi_{\text{carr}}^i)\) and C/A code properties denoted by code frequency \((f_{\text{code}}^i)\) and code phase \((\phi_{\text{code}}^i)\).

\[
\begin{align*}
Y & : \text{Signal replica of the GPS signal} \\
& = \sum_{i=1}^{N} Y^i \\
Y^i & : \text{Signal replica corresponding to the } i^{th} \text{ satellite} \\
& = D^i(t)G^i(f_{\text{code}}^i + \phi_{\text{code}}^i)e^{j2\pi(f_{\text{carr}}^i + \phi_{\text{carr}}^i)},
\end{align*}
\]

where \(N\) denotes the total number of satellites-in-view.

\[
\begin{align*}
f_{\text{code}}^i &= \frac{f_{C/A}}{f_{L1}} \\
\phi_{\text{code}}^i &= -\frac{f_{C/A}}{c} \left( |X_{k,y,z} - S_{k,y,z}^i| \right) \\
&\quad + (c \delta t - c \delta t_d) \\
f_{\text{carr}}^i &= f_{L1} + f_D \\
D &: \text{Carrier Doppler frequency of the } i^{th} \text{ satellite} \\
&= -\frac{f_{L1}}{c} \left( -\text{los}_{k,y,z}^i(X_{k,y,z} - S_{k,y,z}^i) \\
&\quad + (c \delta t - c \delta t_d) \right),
\end{align*}
\]

where \(\text{los}_{k,y,z}^i : \text{LOS vector for } i^{th} \text{ satellite} \]
\[
= -\frac{X_{k,y,z} - S_{k,y,z}^i}{||X_{k,y,z} - S_{k,y,z}^i||}
\]

\[
S_{k,y,z}^i : \text{Position and velocity of the } i^{th} \text{ satellite} \\
= [x_i^t, y_i^t, z_i^t, \dot{x}_i^t, \dot{y}_i^t, \dot{z}_i^t]_t.
\]

B. Overview of LS-MRDTE

The underlying principle of our LS-MRDT 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 pseudo-range and pseudo-rate measurements.

As in Eq. (5), DTE estimates the cumulative satellite vector correlation of the received raw GPS signal \((s_R)\) with the signal replica \((Y)\). This vector correlation is produced for each grid point \(g_j\) from a pre-generated search space that consist of \(G\) grid points. Later, the principle of Maximum Likelihood Estimation (MLE) is applied to estimate the maximum likely clock parameters.

\[
\begin{align*}
corr_j & : \text{Vector correlation for the } j^{th} \text{ grid point} \\
& = \Re(s_R, \sum_{i=1}^{N} Y^i(g_j)) \\
g_j & = [c \delta t_j, c \delta t_d] \quad j = 1, ..., G \\
T_{\text{MLE}} : \text{MLE estimated GPS time} \\
& = \arg \max_{j=1}^{G} \Re(c \delta t_{\text{MLE}}, c \delta t_{\text{MLE}})
\end{align*}
\]
Our MRDTE algorithm executes DTE at each individual receiver in parallel and later computes the joint probabilistic distribution across the receivers. 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.

According to the free space path loss model, the received signal $s_{R,k}$ at the $k^{th}$ receiver has two components when subjected to spoofing: one corresponds to the authentic signal ($s_{R,aut,k}$) and the other is the meaconed signal ($s_{R,sp,k}$).

$$s_{R,k} = \sum_{i=1}^{N} \left\{ \frac{\lambda_{d,1}}{4\pi} e^{j2\pi f_{L,1} t} \right\} \left[ \frac{\sqrt{2P_{aut}^i}}{r_{aut,k}^{i}} \left( f_{code,aut}^i + \phi_{code,aut}^i \right) e^{-j2\pi r_{aut,k}^{i}/\lambda_{d,1}} \right] + \left[ \frac{\sqrt{2P_{sp}^i}}{r_{sp,k}^{i}} \left( f_{code,sp}^i + \phi_{code,sp}^i \right) e^{-j2\pi r_{sp,k}^{i}/\lambda_{d,1}} \right]$$

(6)

where $\lambda_{d,1} = \frac{c}{f_{L,1}}$ and $P_{aut}^i$ and $P_{sp}^i$ are the received power levels of authentic and spoofed GPS signals respectively. $r_{aut,k}^{i}$ and $r_{sp,k}^{i}$ are the distances traveled by the authentic and the meaconed signal respectively to reach $k^{th}$ receiver. $r_{sp,0}^{i}$ is the distance between the $i^{th}$ satellite and the spoofer location while $r_k$ is the distance between the spoofer location and the $k^{th}$ GPS receiver.

![Fig. 3: In our LS-MRDTE, time-delayed similarity in the signals received by multiple receivers are utilized to detect and localize the spoofer.](image1)

To localize the ground spoofer as seen in Fig. 3, we utilize the aspect that the spoofer is relatively in close proximity to our multiple receiver setup as compared to the authentic GPS satellites that are at an altitude of 20200 km (12550 miles).

**C. Architecture of LS-MRDTE**

Our proposed LS-MRDTE addresses the spoofing attacks in four stages as shown in Fig. 4:

1) Firstly, we generate a 2-Dimensional (2D) search space consisting of plausible clock bias and clock drift candidates.
2) Later, we execute multi-peak vector correlation to detect all the significant peaks found in the pre-generated search space.
3) Next, we detect and distinguish the spoofing signals by comparing the time-delayed similarity in the signal properties received across the geographically distributed receivers.
4) 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 across the receiver pairs in case of malicious signals.
5) 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 GPS time.

![Fig. 4: High level architecture of our LS-MRDTE algorithm.](image2)

**D. Our LS-MRDTE Algorithm**

In our algorithm, we consider a single spoofer present in the direct LOS of our multi-receiver setup. We assume that the malicious signals sent by the spoofer effect all the receivers.

1) **Spoofing Detection:**

The first stage is our multi-peak vector correlation module. Based on our DTE, this module estimates all the significant peaks from the considered search space. 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. 5. Then, multi-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.
Across the satellites is carried out at the individual receiver.

Correlation amplitude depends on the code phase residual ($\Delta \phi_{\text{code}}^i$) as in Eq. (3). Similarly, spectrum magnitude depends on the carrier Doppler frequency residual ($\Delta f_{\text{carr}}^i$) which is proportional to the clock drift candidates ($\Delta \delta^i_t$) as in Eq. (4). For computational efficiency, we separate our calculations into two independent threads as

$$
\Delta T_{c \delta t} = \begin{bmatrix}
\Delta c \delta t_1 \\
\Delta c \delta t_j \\
\Delta c \delta t_M
\end{bmatrix},
\Delta T_{c \delta t} = \begin{bmatrix}
0 & \Delta c \delta t_1 \\
0 & \Delta c \delta t_j \\
0 & \Delta c \delta t_M
\end{bmatrix}
$$

and therefore,

$$
c \delta_{\text{MLE}} = \arg \max_{j=1}^M \left( \sum_{i=1}^N \mathbb{R} \left( \Delta T_{c \delta t_i}, c \delta t \right) \right) \quad (7)
$$

$$
c \delta_{\text{MLE}} = \arg \max_{j=1}^M \left( \sum_{i=1}^N \mathbb{R} \left( c \delta t, \Delta T_{c \delta t_i} \right) \right) \quad (8)
$$

For authentic signals, the correlation amplitude and spectrum magnitude plots show a single clear peak as in Fig. 5 across the clock candidates considered. However, under spoofing attack, we observe multiple significant peaks in the correlation amplitude plotted against the clock bias candidates as in Fig. 6(a). 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.

Similar comparison is conducted across the receivers as in Fig. 6(b). We compare time-delayed similarity in signals receiver across spatially dispersed receivers to detect and distinguish the spoofing signals. 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 MLE is carried out to obtain the maximum likely clock parameters.

For authentic signals, principle of MLE is

$$
m_{\text{MLE}} = \begin{bmatrix}
\alpha_1 & \alpha_2 & \cdots & \alpha_L
\end{bmatrix}
$$

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. These parameters are used to estimate GPS time that is later given as input to the PMU.

2) Spoofer Localization using Particle Filter:

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

$$
\xi = \begin{bmatrix}
|X_1 - X_{\text{sp}}| - |X_2 - X_{\text{sp}}| \\
|X_1 - X_{\text{sp}}| - |X_k - X_{\text{sp}}| \\
|X_1 - X_{\text{sp}}| - |X_L - X_{\text{sp}}|
\end{bmatrix}
$$

We generate $\alpha$ particles $\hat{X}_{n,\text{sp}}$, $n = 1, ..., \alpha$ 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 $\alpha$ particles based on our measurement model by computing the probability of the
measurement of a particle given the state of a particle \((P_{w_n})\):

\[
\hat{\beta}_{w_n,sp} = \frac{1}{\sqrt{2\pi R_{pf}}} e^{-\frac{(\beta - \hat{\beta}_{w_n})^2}{2R_{pf}}}
\]

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

After obtaining the weights, we randomly \((\hat{\beta})\) re-sample new set of \(\alpha\) 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.

\[
\begin{align*}
X_{n,sp} = \hat{X}_{n,sp} & \quad \text{if } \hat{\beta} \leq \text{cumsum}(P_{w_n}) \\
X_{sp} = \text{mean}(X_{n,sp})
\end{align*}
\]

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 \((R_{sp}, Q_{sp})\) 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 to obtain the measurement error vector \((\epsilon_i)\). This is given as input to the second branch of our Joint Filter module i.e., Kalman Filter. The measurement update equations are as follows:

\[
\begin{align*}
\epsilon_t &= \begin{bmatrix} T_{t,1} - \hat{T}_t \\ T_{t,2} - \hat{T}_t \\ \vdots \\ T_{t,L} - \hat{T}_t \end{bmatrix} \\
H &\colon \text{Observation matrix} \\
&= \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}^T \\
\hat{P}_t &\colon \text{Predicted state error covariance matrix} \\
R_t &\colon \text{Measurement noise covariance matrix} \\
&= \begin{bmatrix} R_{t,1} & 0 & \cdots & 0 \\ 0 & \ddots & \vdots & \vdots \\ 0 & \cdots & R_{t,k} & 0 \\ 0 & \cdots & 0 & R_{t,L} \end{bmatrix} \\
K_t &\colon \text{Kalman gain matrix} \\
&= \hat{P}_t H^T (H \hat{P}_t H^T + R_t)^{-1}
\end{align*}
\]

\[\Delta T_t : \text{State error vector} \] 
\[T_t : \text{Corrected state vector of the } k^{th} \text{ receiver} \] 
\[= \hat{T}_t + \Delta T_t \]
\[P_t : \text{Corrected state error covariance matrix} \] 
\[= (I - K_t H) \hat{P}_t \]

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:

\[
\begin{align*}
F &\colon \text{State transition matrix, } 2 \times 2 \\
&= \begin{bmatrix} 1 & \Delta T \\ 0 & 1 \end{bmatrix}, \ \Delta T \text{is the update interval} \\
Q_t &\colon \text{State process noise covariance matrix} \\
&= F \begin{bmatrix} 0 & \Delta T \\ 0 & (c \times \sigma_c)^2 \end{bmatrix} F^T \\
\sigma_c &\colon \text{allan deviation of the front-end oscillator} \\
\hat{T}_{t+1} &\colon \text{Predicted state vector for the } (t + 1)^{th} \text{ instant} \\
&= FT_t \\
\hat{P}_{t+1} &\colon \text{Predicted state error covariance matrix} \\
&= FP_t F^T + Q_t
\end{align*}
\]

E. Localization accuracy using CRLB

The factors related to receiver setup such as number of receivers, their spatially geometry, distance of these receivers from spoofer affect the localization accuracy of the spoofer. In addition, our GPS signal processing technique namely DTE impacts the covariance of measurements obtained thereby effecting the localization accuracy. To assess the impact of these factors, we evaluate the CRLB that provides a measure on the localization accuracy that is attained based on the incoming measurements.

The CRLB gives a lower bound on the asymptotic covariance that is achievable using any unbiased estimator. This lower bound is defined to be at least as high as the inverse of the Fisher Information (FI). The CRLB and FI are defined as follows:

\[
E \left[ (X_{sp} - \chi)(X_{sp} - \chi)^T \right] = J_{sp}^{-1}
\]

and

\[
J_{sp} = E \left[ \Delta \ln p(\zeta | \chi)(\Delta \ln p(\zeta | \chi))^T \right].
\]

where \(E[\cdot]\) denotes the expectation operator, \(\zeta\) denotes the difference in range measurements for each master-slave receiver pair, \(X_{sp}\) is the estimate of the spoofer from our LS-MRDE while \(\chi\) is the true position of the spoofer.

In our LS-MRDE algorithm, we consider a pre-determined receiver geometry and their positions based on the constraints
of the power substation. Assuming additive Gaussian measurement noise, the variance of the spoofing signals depends on the spoofer characteristics and our LS-MRDTE i.e.,

$$\zeta_{lk} - m_{lk}(\chi) \approx \mathcal{N}(0, \sigma_{lk}^2(\chi)), \quad (20)$$

where $\sigma_{lk}^2(\chi) = \sigma_1^2(\chi) + \sigma_2^2(\chi)$ and $\sigma_k^2(\chi)$, $k = 1, \ldots, L$ is the variance of measurements estimated using our LS-MRDTE and given as input to the Particle Filter.

Based on this assumption, the probability of likelihood function is expressed as

$$p(\zeta | \chi) = \frac{1}{\sqrt{2\pi\Sigma(\chi)}} e^{-\frac{1}{2}(\zeta - m(\chi))^T \Sigma^{-1}(\chi)(\zeta - m(\chi))}, \quad (21)$$

$$\ln p(\zeta | \chi) = \ln \left( \frac{1}{\sqrt{2\pi\Sigma(\chi)}} \right) - \frac{1}{2}(\zeta - m(\chi))^T \Sigma^{-1}(\chi)(\zeta - m(\chi)), \quad (22)$$

where

$$\Sigma(\chi) = \begin{pmatrix} \sigma_1^2 + \sigma_2^2 & \sigma_1^2 & \cdots & \sigma_1^2 \\ \sigma_1^2 & \sigma_1^2 + \sigma_3^2 & \cdots & \sigma_1^2 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1^2 & \sigma_1^2 & \cdots & \sigma_1^2 + \sigma_L^2 \end{pmatrix}.$$

Substituting Eq. (22) into Eq. (19), we obtain the FI matrix in terms of receiver geometry and measurement covariance of size 3 x 3 for 3-Dimensional (3D). For $i, j = 1, 2, 3$, the elements of the FI matrix are represented as:

$$J_{sp,i,j} = \left( \frac{\partial m(\chi)}{\partial \chi_i} \right)^T \Sigma^{-1}(\chi) \left( \frac{\partial m(\chi)}{\partial \chi_j} \right) + \frac{1}{2} \frac{\partial}{\partial \chi_i} \left( \Sigma^{-1}(\chi) \frac{\partial \Sigma(\chi)}{\partial \chi_j} \Sigma^{-1}(\chi) \right), \quad (23)$$

where

$$\frac{\partial m(\chi)}{\partial \chi_i} = \begin{pmatrix} \frac{\partial m_{12}(\chi)}{\partial \chi_i} \\ \frac{\partial m_{13}(\chi)}{\partial \chi_i} \\ \vdots \\ \frac{\partial m_{1L}(\chi)}{\partial \chi_i} \end{pmatrix} = 2 \begin{pmatrix} -\overrightarrow{r}_{1,i} + \overrightarrow{r}_{2,i} \\ -\overrightarrow{r}_{1,i} + \overrightarrow{r}_{3,i} \\ \vdots \\ -\overrightarrow{r}_{1,i} + \overrightarrow{r}_{L,i} \end{pmatrix}.$$

We denote $J_{sp} = J_{wdop} + J_{E}$ where $J_{wdop}$ depends on the geometry of the receiver and $J_{E}$ represents the dependency of the covariance on the spoofer location.

$$\sigma_{sp,x}^2 = (J_{wdop})_{11}^{-1}, \quad \sigma_{sp,y}^2 = (J_{wdop})_{22}^{-1}, \quad \sigma_{sp,z}^2 = (J_{wdop})_{33}^{-1}.$$

$$e_{sp} = \sqrt{\sigma_{sp,x}^2 + \sigma_{sp,y}^2 + \sigma_{sp,z}^2} = WDOP, \quad (24)$$

where $e_{sp}$ is the 3D root-mean-square error in the spoofer location that is attained for the given configuration of receiver geometry and measurements. $\sigma_{sp,x}^2$, $\sigma_{sp,y}^2$ and $\sigma_{sp,z}^2$ are the respective x, y, z covariances.

In Eq. (23), we define the inverse of the first part $(J_{wdop})$ as Weighted Dilution Of Precision (WDOP). WDOP characterizes the spoofer-receiver geometry. The lower is value of WDOP, lower is the error ($e_{sp}$) and thereby better is the estimate of our spoofer location.

The second part of $J_{sp,i,j}$ depicts the influence of the spoofer location in determining the covariance of measurements estimated using our LS-MRDTE. Therefore, we estimate the covariance of the measurements given by $\Sigma(\chi)$ i.e., $\sigma_k^2(\chi)$ to obtain a bound on the localization accuracy $J_{sp}^{-1}$.

Our LS-MRDTE is based on DTE which estimates the maximum likely clock estimates from a pre-generated set of clock candidates considered. Since MLE is asymptotically efficient our measurement covariance of spoofing peak is equal to the inverse of its corresponding FI matrix.

$$\sigma_k^2(c_{\delta t_{MP}}) = \left( \sum_{i=1}^{N} \mathbb{E} \left\{ \frac{\partial^2 p(s_{R,k} | \mu^i_{\rho})}{\partial c \delta t_{MP_k}} \left( \frac{\partial^2 p(s_{R,k} | \mu^i_{\rho})}{\partial c \delta t_{MP_k}} \right)^T \right\} \right)^{-1}, \quad (25)$$

where $\mu^i_{\rho} = [\phi^i_{code}, f^i_{code}]_{sp}$ denotes the code phase and code frequency of GPS spoofing signal. $c_{\delta t_{MP_k}}$ denotes the clock candidate corresponding to the malicious peak of the $k^{th}$ receiver after detecting and distinguishing the spoofing signals.

For $k^{th}$ receiver, the probability of likelihood $\frac{\partial p(s_{R,k} | \mu^i_{\rho})}{\partial c \delta t_{MP_k}}$ following a Gaussian distribution with covariance $(\sigma_{\mu}^2)$ is expressed as

$$p(s_{R} | \mu^i_{\rho}) = \frac{1}{\sqrt{2\pi\sigma_{\mu}^2}} e^{-\frac{1}{2}(s_{R} - \mu)^2} \quad (26)$$

and

$$\frac{\partial p(s_{R,k} | \mu^i_{\rho})}{\partial c \delta t} = \left( \frac{\partial \mu^i_{\rho}}{\partial c \delta t} \right)^T \frac{\partial p(s_{R,k} | \mu^i_{\rho})}{\partial \mu^i_{\rho}} \quad (27)$$

In case of spoofing, we write the Eq. (25) as

$$\sigma_k^2(\chi) = \sigma_k^2(c_{\delta t_{MP}}) = \left[ \sum_{i=1}^{N} \mathbb{E} \left\{ \left( \frac{\partial \mu^i_{\rho}}{\partial c \delta t_{MP_k}} \right)^T \frac{\partial p(s_{R,k} | \mu^i_{\rho})}{\partial \mu^i_{\rho}} \right\} \left( \frac{\partial \mu^i_{\rho}}{\partial c \delta t_{MP_k}} \right)^T \frac{\partial p(s_{R,k} | \mu^i_{\rho})}{\partial \mu^i_{\rho}} \right]^{-1}.$$
where $J_{R,s,p,k}(\mu^i_{sp})$ is the FI matrix of $\mu^i_{sp}$ corresponding to $k^{th}$ receiver and is calculated from Eq. (26) and Eq. (27). As seen from Eq. (6), this matrix depends on the distance of spoofer from receiver, SNR and sampling rate.

From Eq. (3) and Eq. (4), we calculate the derivative of our code phase and carrier frequency with respect to the clock candidate as:

$$\frac{\partial \mu^i_{sp}}{\partial \delta \hat{c} MP} = \left[-\frac{f_{C/A}}{c}\right]^T$$

(29)

Substituting Eq. (29) in Eq. (28), we obtain the covariance $\sigma^2(\chi)$ as

$$\sigma^2(\chi) = \left(\frac{c}{f_{C/A}}\right)^2 \sum_{j=1}^{N} J_{R,s,p,k}(\mu^i_{sp})_{11}^{-1}$$

(30)

The above expression for $\sigma^2(\chi)$ is substituted in Eq. (23) to obtain the lower bound on the localization accuracy for a given configuration of multiple receivers. In addition, the value of $J^{-1}$ can be minimized to compute the optimum locations for the placement of multiple receivers. Thus, we provide mathematical insights into choosing the parameters related to multi-receiver setup by analyzing the corresponding CRLB of localization accuracy attained.

### F. Probability of spoofer detection

Based on Eq. (28), the spoofing peak detected using our multi-peak vector correlation follows a Gaussian distribution given by

$$Y_k = \mathcal{N}\left[c\delta t_{MPk}, \sigma^2(\chi)\right]$$

(31)

We rewrite $Y$ in terms of $Z$ as

$$Z = \frac{X - c\delta t_{MPk}}{\sigma(\chi)} = \mathcal{N}\left(0, 1\right)$$

(32)

Let $H_0$ be the hypothesis that our LS-MRDTE detects spoofing and $V_0$ be the hypothesis that the multi-receiver setup is actually being spoofed. Therefore, we detect the spoofing signal using multi-peak vector correlation with a probability defined as

$$P(H_0|V_0) = P\left(Y > \mathbb{E}_{aut}(c\delta t_j, c\delta i_{aut,k})|j=MPk\right)$$

$$= 1 - P\left(Z \leq \frac{\mathbb{E}_{aut}(c\delta t_j, c\delta i_{aut,k})|j=MPk - c\delta t_{MPk}}{\sigma(\chi)}\right)$$

(33)

$$= 1 - \Phi\left(\frac{\mathbb{E}_{aut}(c\delta t_j, c\delta i_{aut,k})|j=MPk - c\delta t_{MPk}}{\sigma(\chi)}\right)$$

where $\Phi$ is the standard normal distribution.

### III. Experimental Results and Analysis

Our experimental results are divided into two categories: firstly, we compared the improved robustness of MRDTE in estimating the GPS signal parameters as compared to our prior work on SRDTE [25] and conventional scalar tracking. Secondly, we validated the accuracy of spoofer location and robustness of GPS timing estimated using our LS-MRDTE when subjected to spoofing attacks.

We collected our data using four Universal Software Radio Peripherals (USRP-N210) each equipped with a DBSRX2 daughterboard as in Fig. 7. They are connected to a common external atomic clock Microsemi Quantum SA.45s CSAC. The collected raw GPS signals are post-processed using our pyGNSS platform, a python based object oriented framework.

Fig. 7: Our data collection experiments involve 4 USRPs, a CSAC and a laptop for storing data.

The integration time considered for our LS-MRDTE is $\Delta T = 20 ms$. In our Kalman Filter, our measurement noise covariance matrix $R_k$ is estimated by computing the covariance of past 20 measurement error vector values. The position and velocity of multiple static receivers are pre-determined using Multi-Receiver Vector Tracking [30].

#### A. Robustness of MRDTE against spoofing

We analyzed the robustness of MRDTE in estimating the GPS code frequency ($f_{code}$) and carrier frequency ($f_{carr}$) as compared to scalar tracking during meaconing.
1) Experimental setup:
For this experimental analysis, we installed four AntCom 3GNSSA4-XT-1 GNSS antennas on the rooftop of Talbot Laboratory (TL), Urbana, Illinois as in Fig. 8. The receivers are arranged such that they represent the corners of a square of diagonal 10 m.

![Fig. 8: Four GPS antennas located on roof of Talbot Laboratory, University of Illinois at Urbana-Champaign (UIUC). Reference image is taken from [14].](image)

2) Analysis of signal parameters during meaconing:
When meaconing signal of 3 dB higher power than authentic signals is added, the scalar tracking locks onto the counterfeit signal as shown in Fig. 9 whereas MRDTE consistently tracks the authentic signal and mitigates the effect of meaconing attack.

![Fig. 9: Under 3 dB added meaconing: (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 tracks the authentic signal.](image)

In accordance with the experimental results shown in Table I, MRDTE has a higher threshold to meaconing. In the presence of meaconing attack, MRDTE offers 0.7 dB higher tolerance than SRDTE and 2 dB higher tolerance than the scalar tracking.

![TABLE I: Threshold of various GPS algorithms against meaconing. MRDTE offers higher tolerance than SRDTE and scalar tracking.](image)

B. Accuracy analysis of our LS-MRDTE
In the second set of experiments, we validated the accuracy and convergence rate of our LS-MRDTE in computing the location of spoofer and GPS time.

![Fig. 10: 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 determined.](image)

1) Experimental Setup:
We installed four AntCom 3GNSSA4-XT-1 GNSS antennas at each corner on the rooftop of Talbot Laboratory (TL), Urbana, Illinois and the Spoofer is located approximately 300 m away on the rooftop of Electrical and Computer Engineering (ECE), Urbana, Illinois as seen in the Fig. 10. In our Particle Filter, we generate 1000 random particles of uniform distribution every instant.

2) Fixed vs adaptive clock candidate distribution:
To investigate the convergence rate and accuracy of GPS time estimated using our MRDTE, we analyzed different clock candidate distributions. Specifically, we compared the fixed uniform distribution in Fig. 11(a) with respect to adaptive Gaussian distribution as seen in Fig. 11(b). Clock candidates following adaptive Gaussian distribution are generated using the predicted covariance values estimated during the time update of Kalman Filter.

In Fig. 12, the clock bias and clock drift residuals are compared for both above-mentioned candidate distributions. We observed that the clock bias residuals are within 1 µs using adaptive Gaussian and within 3 µs using fixed uniform
distribution. Similarly, in the case of clock drift, the residuals computed are within 0.5 ns/s using adaptive Gaussian and within 1.5 ns/s using fixed uniform. Thus, more precise timing is obtained by implementing an adaptive Gaussian clock candidate distribution.

In Fig. 13, we compared the clock residuals computed using our LS-MRDTE with that of scalar tracking subjected to data-level spoofing attack. We observed that the scalar tracking tracks the malicious signals and thereby shows a clock bias residual of 60 μs whereas our LS-MRDTE maintains a clock bias residual of within 1 μs.

4) Spoofer localization and GPS time during meaconing:
During meaconing, the position calculated by the effected receivers is the same as the position of spoofer’s antenna while recording the GPS signals. We demonstrated the robustness of our LS-MRDTE in computing the GPS time and spoofer location under two different cases of meaconing. 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 26.5 μs.

In our first case, the meaconed signals with above specifications are recorded on the rooftop of ECE building and replayed later in time from the same location.

In the second case of meaconing which is more stealthy, we recorded GPS signals on the same TL rooftop as our multi-receiver setup and later replayed them from the top of ECE building as meaconed signals. By implementing this sophisticated attack, the spoofer surpassed all the position check algorithms with lower probability of being detected.

In Fig. 15, we validated 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 residuals of around 30 μs which is equivalent to the meaconed delay induced. However, our LS-MRDTE accurately detects these spoofing signals and estimates the GPS time with 1.5 μs time accuracy.
Fig. 15: Comparison of clock bias residuals: (a) under 2 dB of added meaconing that induces a delay of 30 \( \mu s \); (b) under no added meaconing. The red line corresponds to scalar tracking and blue line corresponds to our LS-MRDTE. Our LS-MRDTE estimates GPS time with 1.5 \( \mu s \) accuracy while the scalar tracking shows an error in the clock bias residuals of 30 \( \mu s \) thereby violating IEEE.C37.118 standards.

Fig. 16 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. We observe that our LS-MRDTE converges to the true location of the spoofer in as quick as 0.22 s thereby demonstrating the fast convergence rate of our algorithm.

Fig. 16: Our LS-MRDTE based Spoofer localization using Particle Filter: (a),…,(i) show the sequential snapshots of the spoofer location estimated by our Particle Filter. 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 that time instant. We observe that our LS-MRDTE based Particle Filter converges to within 2.85 m the true spoofer.

IV. CONCLUSIONS

In conclusion, we presented our novel joint estimation of GPS time and spoofer location for PMUs using MRDTE. We utilized the geometry of spatially distributed receivers and carried out multi-peak vector correlation to detect and distinguish spoofing attacks. Later, we theoretically estimated the CRLB of the localization accuracy achieved for a given configuration of multi-receiver setup. In addition, we also computed the probability of spoofing detection using our LS-MRDTE algorithm.

Our experimental results obtained from joint Particle and Kalman Filter validated the localization of spoofer to within 3 m and the GPS time to within 1\( \mu s \) accuracy. This is compliant with the IEEE.C37.118 requirements specified by the power community. Our LS-MRDTE estimated the spoofer location in 0.22 s, thereby demonstrating fast convergence of our algorithm.

ACKNOWLEDGMENT

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

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 reflect those of the United States Government or any agency thereof.

REFERENCES


Sriramya Bhamidipati is a graduate student under Prof. Grace Gao in the Department of Aerospace Engineering at the University of Illinois at Urbana-Champaign. She received her M.S degree in Aerospace Engineering from University of Illinois at Urbana-Champaign in 2017. She received her B.Tech. with honors in Aerospace Engineering and minor in Systems and Controls Engineering from Indian Institute of Technology Bombay, India in 2015. Her research interests include GPS, power and control systems, computer vision and UAVs.

Grace Xingxin Gao received the B.S. degree in mechanical engineering and the M.S. degree in electrical engineering from Tsinghua University, Beijing, China in 2001 and 2003. She received the PhD degree in electrical engineering from Stanford University in 2008. From 2008 to 2012, she was a research associate at Stanford University. Since 2012, she has been with University of Illinois at Urbana-Champaign, where she is presently an assistant professor in the Aerospace Engineering Department.