MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

GPS Spoofing Detection and Mitigation in PMUs Using Distributed Multiple Directional Antennas

Bhamidipati, S.; Kim, K.J.; Sun, H.; Orlik, P.V.

TR2019-023 June 04, 2019

Abstract

In power distribution networks, microgrids utilize Phasor Measurement Units (PMUs), to assess the voltage stability at critical nodes in the network. PMUs rely on precise time-keeping sources, such as GPS, to obtain synchronization. However, GPS signals are vulnerable to external spoofing attacks due to their unencrypted signal structure and low received power. To detect the spoofing-induced timing anomaly, an innovative geographically Distributed Multiple Directional Antennas (DMDA) setup is proposed, which is triggered using a common clock. Utilizing the configuration of the proposed DMDA, a Belief-Propagation (BP)-based Extended Kalman Filter (EKF) algorithm is developed to estimate the timing errors caused by spoofing. The BP-EKF algorithm analyzes the single difference pseudorange residuals across each pair of antennas in a probabilistic graphical framework not only to detect the spoofed antennas in the DMDA setup but also to estimate the timing errors associated with the spoofed antennas. Based on the BP estimate of timing error at each antenna and the known baseline distances across antennas, the pseudoranges are corrected, and then adaptive EKF is employed to estimate the GPS timing. The performance of the BP-EKF algorithm is assessed by subjecting the simulated authentic GPS signals to a simulated meaconing attack, which induces a time delay of 60 microseconds. Both successful detection of meaconing, and also accurate estimation of GPS timing that complies with the IEEE-C37.118 standards, is validated using the experimental results. At a critical node in the simulated microgrid, as compared to scalar tracking, an increased voltage stability is demonstrated using the BP-EKF by assessing a metric, namely, voltage stability index.

IEEE International Conference on Communications (ICC)

GPS Spoofing Detection and Mitigation in PMUs Using Distributed Multiple Directional Antennas

Sriramya Bhamidipati, Kyeong Jin Kim, Hongbo Sun, and Philip V. Orlik

***Abstract*—In power distribution networks, microgrids utilize Phasor Measurement Units (PMUs), to assess the voltage stability at critical nodes in the network. PMUs rely on precise time-keeping sources, such as GPS, to obtain synchronization. However, GPS signals are vulnerable to external spoofing attacks due to their unencrypted signal structure and low received power. To detect the spoofing-induced timing anomaly, an innovative geographically Distributed Multiple Directional Antennas (DMDA) setup is proposed, which is triggered using a common clock. Utilizing the configuration of the proposed DMDA, a Belief-Propagation (BP)-based Extended Kalman Filter (EKF) algorithm is developed to estimate the timing errors caused by spoofing. The BP-EKF algorithm analyzes the single difference pseudorange residuals across each pair of antennas in a probabilistic graphical framework not only to detect the spoofed antennas in the DMDA setup but also to estimate the timing errors associated with the spoofed antennas. Based on the BP estimate of timing error at each antenna and the known baseline distances across antennas, the pseudoranges are corrected, and then adaptive EKF is employed to estimate the GPS timing. The performance of the BP-EKF algorithm is assessed by subjecting the simulated authentic GPS signals to a simulated meaconing attack, which induces a time delay of 60 μs. Both successful detection of meaconing, and also accurate estimation of GPS timing that complies with the IEEE-C37.118 standards, is validated using the experimental results. At a critical node in the simulated microgrid, as compared to scalar tracking, an increased voltage stability is demonstrated using the BP-EKF by assessing a metric, namely, voltage stability index.**

***Index Terms*—GPS spoofing, Belief Propagation, Factor Graph, Extended Kalman Filter, Voltage Stability Index**

I. Introduction

Due to the changing dynamics for future electricity demand and supply as well as the increasing complexity of interconnected grids, it is becoming increasingly difficult to reliably control the entire power grid [1]. To improve the grid efficiency and localize disruptions, the concept of microgrid is proposed for the power distribution networks [2]. Microgrid possesses the capability to function both when connected to a traditional grid and also as an independent electrical island. However, unlimited power consumption causes the microgrid to be vulnerable to voltage collapse, which needs to accurately monitored.

With the development of data acquisition technology, Wide Area Monitoring System (WAMS) [3] plays a pivotal role in providing unprecedented situational awareness and real-time system monitoring for the current and future grid. Advanced devices such as Phasor Measurement Units (PMUs) [4] are used in WAMS to record the time-tagged phasor measurements, namely, voltage and current phasors. PMUs rely on precise time-keeping sources, such as GPS, to obtain global timing for synchronization. However, GPS civilian signals are unencrypted and their power is as low as -160 dBW, which makes them vulnerable to external spoofing attacks [5].

With an aim to disrupt the voltage stability of the microgrid via spoofing attacks, the attacker broadcasts malicious look-alike GPS signals to induce timing errors while simultaneously minimizing the detection probability of these attacks. In this work, we focus on a type of spoofing attack, namely, meaconing, which is also known as record-and-replay. In addition, the generalized framework of the proposed algorithm is also directly applicable for the detection and mitigation of other attacks, namely, data-level and signal-level spoofing [6]. An attacker executing meaconing records the authentic GPS signals at a physical location and later broadcasts these recorded signals with higher power towards the target receiver. This attack delays the target receiver's estimated time as compared to the true time [7]. Meaconing is a serious threat to the critical infrastructure, such as microgrids, given the relatively simple hardware involved and minimal knowledge of the GPS tracking loops [8] required to execute this attack.

The IEEE C37.118.1-2011 prescribes a criterion based on Total Vector Error (TVE) [9], according to which we consider 1% TVE equivalent to a timing error of 26.5 μs, as a benchmark in the stability analysis. Prior research on spatial signal processing-based approaches to detect spoofing attacks utilize beamforming antenna arrays [10]-[11] based on phase delays and direction of angle-of-arrival of the satellite signals. Even though effective, these techniques involve in attitude estimation and adaptive steering of antenna to mitigate the spoofing attacks at the sacrifice of high hardware complexity. The authors of [12] analyze the time-difference-of-arrival properties across multiple receivers to authenticate the received satellite signals. However, their practical execution involve significant limitations as they require wide spatial diversity and collective synchronization among the network of considered receivers.

In this work, we propose a geographically Distributed Multiple Directional Antennas (DMDA) setup, such that, each antenna points towards a different section of the sky, thereby, receives GPS satellite signals from only a subset of total visible satellites. In our innovative DMDA setup, the selective visibility of the multiple directional antennas ensures that the external spoofer cannot attack all the antennas

S. Bhamidipati is with the University of Illinois at Urbana-Champaign (UIUC), Urbana, IL, 61801 USA.

K. J. Kim, H. Sun, and P. V. Orlik are with Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, 02139 USA.

This work was done while S. Bhamidipati was working at MERL.

simultaneously. Thereafter, we develop a Belief-Propagation (BP)-based Extended Kalman Filter (EKF) to not only detect the presence of antenna-specific timing anomaly caused by spoofing attacks but also correct for the timing errors to ensure that reliable GPS timing is provided to the PMUs. By utilizing the selective visibility of GPS satellite signals and the known baselines across multiple antennas, our DMDA-based BP-EKF algorithm is resilient against all kinds of spoofing attacks.

II. The Proposed DMDA Setup

In this work, we assume that the attacker broadcasts counterfeit GPS signals corresponding to all the visible GPS satellites so as to execute a successful spoofing attack. In this section, the different advantages of the proposed DMDA setup, seen in Fig. 1, are explained as follows.

A. Directional antenna and static infrastructure of the grid

In authentic conditions, each directional antenna sees satellites that match the expected subset of satellites found in their section of the sky. However, during attack, the spoofed antenna sees equal or more satellites than expected. By utilizing the known satellite ephemeris and static infrastructure of the grid, we pre-determine the expected number of satellites observed at each antenna. We analyze the difference between expected and observed set of satellites to obtain *a prior* regarding the presence or absence of spoofing attacks.

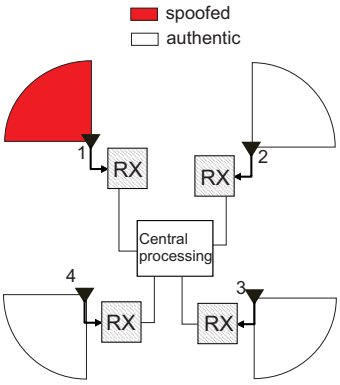

Fig. 1: Configuration of the proposed DMDA setup. Each directional antenna is provided with selective visibility by pointing it towards a different section of the sky, such that, not all the directional antennas can be spoofed simultaneously. Sector of circle represents the field-of-view of each antenna.

B. Geographical diversity of multiple directional antennas

Given that spoofing is a directed attack executed from a near-ground level ($\ll 20,200$ km), the attacker cannot simultaneously be in line-of-sight with all the antennas. In Fig. 2, different spatial configurations of the attacker and their effect on the proposed DMDA setup is shown. When the attacker is not directly overhead as seen in Fig. 2(a) and Fig. 2(b), the number of antennas affected by spoofing are *strictly less* than the total number of antennas. We leverage this information to detect spoofing-induced anomaly in timing and thereafter isolate these spoofing attacks.

Geographical diversity, i.e., spatial separation between antennas, is another crucial aspect of the proposed DMDA setup. Given that the grid is static, we utilize the pre-computed baseline information across antennas to distinguish spoofing attacks affecting multiple antennas, including Fig. 2(c) where the attacker is overhead.

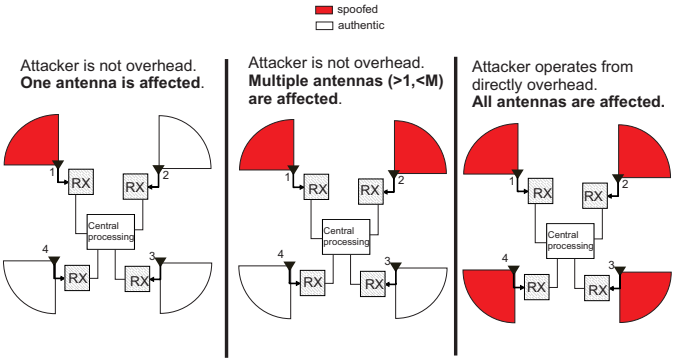

Fig. 2: Different spatial configurations of the attacker with respect to the proposed DMDA setup.

C. Common clock

We trigger all the antennas in the proposed DMDA setup using the same clock. Therefore, in authentic conditions, the pseudoranges received at different antennas exhibit the same receiver timing-based clock bias. However, during spoofing, the affected antennas exhibit different/varying receiver clock bias as compared to non-spoofed antennas, which we leverage to estimate the spoofing-induced timing errors.

III. BP-EKF Algorithm

In this section, based on the configuration of the proposed DMDA setup, we explain the BP-EKF algorithm designed to detect and mitigate GPS spoofing attacks on the microgrid. Using the BP-EKF algorithm, we ensure that reliable GPS timing is provided as input to the PMUs, which is later used to monitor the grid stability via WAMS.

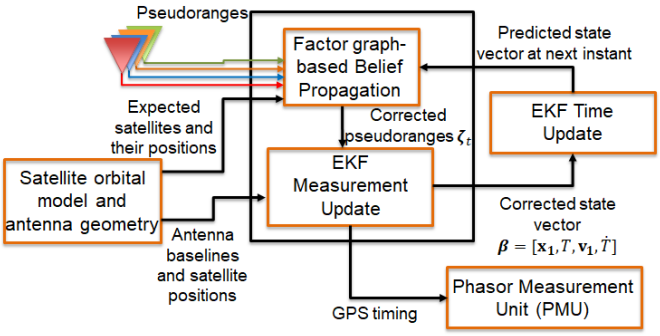

Fig. 3: Architecture of the BP-EKF algorithm.

A. Proposed Architecture

The overall architecture of the proposed BP-EKF algorithm is seen in Fig. 3. Using the DMDA setup described in Section II, we obtain the pseudoranges from different antennas and collectively process them in the Central Processing (CP)

unit. In the CP unit, across each pair of antennas, we compute the *single difference pseudorange residual*, by considering one satellite from each antenna. Later, using factor graph-based BP, we compute the marginal Gaussian distribution of the timing error at each antenna, termed as *belief*, by calculating the product of its own prior distribution and the *incoming message* from other antennas in the proposed DMDA setup. At each instant, the incoming message received from other antennas is calculated from the belief distribution of its own timing error and likelihood of the single difference pseudorange residual. After obtaining BP estimate of timing error at each antenna, we correct the pseudoranges and later adaptively process these corrected measurements via EKF to estimate the GPS timing, which is provided as input to the PMUs for time-tagging the phasor measurements.

B. Proposed Algorithm

The details of the proposed BP-EKF algorithm to detect timing anomaly caused by spoofing attacks and to perform corresponding timing error correction is discussed as follows

1) Conditioned GPS measurements:

We consider the proposed DMDA setup to comprise of M antennas and obtain the pre-computed baseline vectors between these antennas, which is denoted by $\boldsymbol{b}_{kn}$, $k, n \in \{1, \ldots, M\}$. Also, $\boldsymbol{x}_k = [x, y, z]_k$ and $\boldsymbol{v}_k = [\dot{x}, \dot{y}, \dot{z}]_k$ are the three-dimensional (3D) position and 3D velocity of the kth antenna at tth time instant. The pseudorange observed at the kth antenna corresponding to the ith satellite is given by

$$\begin{aligned}\rho^i_{k,t} &= ||\boldsymbol{x}_{1,t} - \boldsymbol{b}_{1k} - \boldsymbol{y}^i_t|| + (T_t + \alpha_{k,t} - c\delta t^i) + I^i_k + \omega^i_k \\ &= h_{k,t}\big(\boldsymbol{x}_{1,t},\, T_t,\, \boldsymbol{b}_{1k}\big) + \alpha_{k,t}, \end{aligned} \tag{1}$$

where i indexes the total visible satellites, $L_{k,t}$, at the kth antenna. In addition, $\boldsymbol{y}^i_t$ and $c\delta t^i$ respectively denote the 3D position and clock bias of the ith satellite. The atmospheric errors, I^i_k, related to ionosphere and troposphere are estimated using existing methods. ω^i_k represents the additive Gaussian noise in the corresponding satellite measurements. Given that the antennas are triggered using same clock, as explained in Section II-C, the corresponding common clock bias, T_t, and clock drift, $\dot{T}_t$, are independent of the antenna considered. The antenna-specific timing errors in pseudorange are denoted by α_k and $h_{k,t}(\cdot)$ denotes the measurement model of the kth antenna, which depends on the reference antenna's 3D position, $\boldsymbol{x}_{1,t}$, receiver clock bias, T_t, and baseline distance, $\boldsymbol{b}_{1k}$. The antenna specified by $k = 1$ is considered as the reference antenna.

Next, for each pair of antennas, we obtain the single difference pseudorange residuals between the ith visible satellite from the kth antenna with that of the jth visible satellite from the nth antenna as

$$\begin{aligned}\gamma^{ij}_{kn,t} = (\rho^i_{k,t} - ||\hat{\boldsymbol{x}}_{k,t} - \boldsymbol{x}^i|| + c\delta t^i) \\ -(\rho^j_{n,t} - ||\hat{\boldsymbol{x}}_{n,t} - \boldsymbol{x}^j|| + c\delta t^j),\end{aligned} \tag{2}$$

where $\hat{\boldsymbol{x}}_{k,t} \triangleq \hat{\boldsymbol{x}}_{1,t} - \boldsymbol{b}_{1k}$, with $\hat{\boldsymbol{x}}_{1,t}$, the prediction of $\boldsymbol{x}_1$ made by the EKF time update at time t.

Based on the known ephemeris and the predicted position, velocity and clock of the antennas, i.e., $\hat{\boldsymbol{x}}_{k,t}$, and $\hat{T}_t$, we calculate the metric $\boldsymbol{\gamma}_{kn,t} = \{\gamma^{ij}_{kn,t}, \forall k, n \in \{1, \ldots, M\}, k \neq n, i \in L_{k,t}, j \in L_{n,t}\}$ across all pairs of antennas and the corresponding satellites observed at the respective antennas. After accounting for atmospheric effects, $\gamma^{ij}_{kn,t}$ is equivalent to

$$\gamma^{ij}_{kn,t} = \alpha_k - \alpha_n + \omega^{ij}_{kn}. \tag{3}$$

In non-spoofed conditions, $\gamma^{ij}_{kn} \approx 0$ due to the presence of only uncorrelated noise observed at the ith and kth antennas. However, in the event of spoofing, when either ith or kth antenna is spoofed, this metric shows significant non-zero errors. Given the directional nature of the DMDA setup, as explained in Section II-B, the attacker can spoof only a subset of antennas simultaneously, which we leverage in the BP-EKF to isolate the spoofed antennas. Across a pair of antennas, the likelihood probability is computed as follows:

$$\begin{aligned}p(\boldsymbol{\gamma}_{kn,t}|\alpha_k, \alpha_n) = \frac{1}{\sqrt{(2\pi\nu^2)^{L_{k,t}L_{n,t}}}} \\ \exp\Bigg\{\frac{-L_{k,t}L_{n,t}}{2\nu^2}\Big(\frac{\mathbf{1}^T\boldsymbol{\gamma}_{kn,t}}{L_{k,t}L_{n,t}} + (\alpha_k - \alpha_n)\Big)^2\Bigg\},\end{aligned} \tag{4}$$

where ν^2 denotes the measurement variance of the summation of single difference residual components which comprises of errors observed due to pseudoranges, satellite ephemeris errors, and errors in predicted position and velocity.

2) Belief Propagation (BP):

To estimate the unknown timing errors at each antenna, the *marginal distribution* is computed by the factor graph-based BP framework. Factor graph is a probabilistic graphical model [13] which consists of two nodes: variable nodes that represent the unknowns to be estimated and factor nodes that represent the relationship between different variable nodes.

Given a network of M antennas, the joint posterior distribution is given by $p(\alpha_1, \ldots, \alpha_M|\boldsymbol{\gamma}_{kn})$, where $\mathcal{B}_k$ denotes the set of all antennas excluding kth antenna and the corresponding marginal distribution $g(\cdot)$ is defined as

$$\begin{aligned}&g(\alpha_k) = \\ &\int_{\alpha_1,\ldots,\alpha_{k-1}} \int_{\alpha_{k+1},\ldots,\alpha_M} p(\alpha_1, \ldots, \alpha_M|\{\boldsymbol{\gamma}_{kn}\}_{k=1,\ldots,M,n\in\mathcal{B}_k}) \\ &\quad d\alpha_1 \ldots d\alpha_{k-1}\, d\alpha_{k+1} \ldots d\alpha_M.\end{aligned} \tag{5}$$

With an increase in the number of antennas, M, in the network, (5) becomes computationally intractable. By utilizing the factor graph framework, for every variable node, α_k, a computationally-efficient marginal distribution can be computed at every time instant t, which is defined as belief $b_t(\alpha_k)$. The belief $b_t(\alpha_k)$ at the kth antenna is computed as the product of its prior distribution and all the *incoming messages* from other antennas in the DMDA setup. In this work, we model the belief as Gaussian [14], as seen in (6), with mean $\mu_{k,t}$ and variance $\sigma^2_{k,t}$. This is justified, given that the attacker transmits GPS look-alike signals and therefore, the corresponding

spoofing-induced timing errors follow a Gaussian distribution. That is,

$$b_t(\alpha_k) = m_{f_k\to\alpha_k}\prod_{n\in\mathcal{B}_k} m_{f_{kn}\to\alpha_k}(\alpha_k) = \mathcal{N}(\alpha_k : \mu_{k,t}, \sigma^2_{k,t}), \tag{6}$$

where the factor node, f_{kn}, connects two variable nodes, α_k and α_n, based on the likelihood probability, $p(\boldsymbol{\gamma}_{kn}|\alpha_k, \alpha_n)$, and the other factor node, f_k, which connects to its corresponding variable node, α_k, and indicates the prior distribution of α_k.

In (6), the message, $m_{f_{kn}\to\alpha_k}$, indicates the belief of nth antenna on the variable node, α_k, based on the factor node, f_{kn}, calculated using (4) as (7) provided at the top of the next page. From the derivation in (7), we represent $m_{f_{kn}\to\alpha_k}$ as a Gaussian distribution given by

$$m_{f_{kn}\to\alpha_k}(\alpha_k) \approx \mathcal{N}(\alpha_k : \mu_{kn,t},\, \sigma^2_{kn,t}), \tag{8}$$

where $\mu_{kn,t} \triangleq \mu_{n,t-1} - \dfrac{\mathbf{1}^T\boldsymbol{\gamma}_{kn,t}}{L_{k,t}L_{n,t}}$ and $\sigma^2_{kn,t} \triangleq \dfrac{\nu^2}{2L_{k,t}L_{n,t}} + \sigma^2_{kn,t-1}$.

Similarly, we also model the prior distribution as Gaussian, i.e., $p(\alpha_k) = \mathcal{N}(\alpha_k : \mu_{pk,t}, \sigma^2_{pk,t})$, where the mean is denoted as $\mu_{pk,t}$ and variance as $\sigma^2_{pk,t}$. Based on this, the message from factor node, f_k, to the variable node, α_k, is computed as:

$$m_{f_k\to\alpha_k} = p(\alpha_k)\int b(\alpha_k)d\alpha_k = p(\alpha_k) = \mathcal{N}(\alpha_k : \mu_{pk,t}, \sigma^2_{pk,t}), \tag{9}$$

where $\mu_{pk,t}$ and $\sigma^2_{pk,t}$ are calculated based on the difference between the observed and the expected set of satellites. At the kth antenna, when the mismatch between the observed and the expected set of satellites, as explained in Section II-A, is ≥ 2, then $\mu_{pk,t} = 0$ and $\sigma^2_{pk,t} = \infty$, thereby representing an approximated uniform distribution. However, if the mismatch between observed and expected set of satellites is ≤ 2, then $\mu_{pk,t}$ and $\sigma^2_{pk,t}$ are computed from the empirical distribution calculated on-the fly by considering the most recent W timing errors $\alpha_{k,t-W:t}, \forall k = 1, \cdots, M$.

Given the product of Gaussian distributions is still Gaussian [15], we compute the belief for time instant t as:

$$b_t(\alpha_k) = \mathcal{N}(\alpha_k : \mu_{pk,t}, \sigma^2_{pk,t})\prod_{n\in\mathcal{B}_k}\mathcal{N}(\alpha_k : \mu_{kn,t}, \sigma^2_{kn,t}) = \mathcal{N}(\alpha_k : \mu_{k,t}, \sigma^2_{k,t}), \tag{10}$$

where

$$\sigma^2_{k,t}(\alpha_k) = \left(\frac{1}{\sigma^2_{pk,t}} + \sum_{n\in\mathcal{B}_k}\frac{1}{\sigma^2_{kn,t}}\right)^{-1} \text{ and}$$
$$\mu_{k,t}(\alpha_k) = \sigma^2_{k,t}(\alpha_k)\left(\frac{\mu_{pk,t}}{\sigma^2_{pk,t}} + \sum_{n\in\mathcal{B}_k}\frac{\mu_{kn,t}}{\sigma^2_{kn,t}}\right). \tag{11}$$

3) Adaptive Extended Kalman Filter (EKF):

After estimating α_k using the factor graph-based BP framework, namely, $\hat{\alpha}_k$ for the kth antenna, a closed-loop adaptive tracking is conducted by using EKF. The EKF has two main steps: measurement and time update. For EKF processing, we first compute the corrected pseudoranges, i.e., $\boldsymbol{\zeta}_t \triangleq [\rho^1_c, \ldots, \rho^L_c]$, where $\rho^i_c \triangleq \rho^i_k - \hat{\alpha}_k$ and $L \triangleq L_1 + \cdots + L_M$ indicates the total number of satellites. Next, we adaptively propagate the 3D position, 3D velocity, clock bias, and clock drift of the reference antenna via EKF and compute the corrected 3D position and 3D velocity of other antennas using the known baseline information $\boldsymbol{b}_{1n} \triangleq \boldsymbol{x}_1 - \boldsymbol{x}_n$.

During measurement update, EKF updates the adaptive measurement noise covariance matrix, $\boldsymbol{R}_t$, the measurement model, $\boldsymbol{H}_t$, the predicted state vector, $\hat{\boldsymbol{\beta}}_t \triangleq [\hat{\boldsymbol{x}}_{1,t}, \hat{T}_t, \hat{\boldsymbol{v}}_{1,t}, \hat{\dot{T}}_t]^T$, and the predicted state covariance matrix, $\hat{\boldsymbol{P}}_t$, as follows:

$$\begin{aligned}
\bar{\boldsymbol{\beta}}_t &= \big(\boldsymbol{I}_{8\times8} - \boldsymbol{K}_t\boldsymbol{H}_t\big)\hat{\boldsymbol{\beta}}_t + \boldsymbol{K}_t\boldsymbol{\zeta}_t,\\
\bar{\boldsymbol{P}}_t &= \big(\boldsymbol{I}_{8\times8} - \boldsymbol{K}_t\boldsymbol{H}_t\big)\hat{\boldsymbol{P}}_t,\\
\boldsymbol{K}_t &= \hat{\boldsymbol{P}}_t\boldsymbol{H}_t^T\Big(\boldsymbol{H}_t\hat{\boldsymbol{P}}_t\boldsymbol{H}_t^T + \boldsymbol{R}_t\Big)^{-1},\\
\boldsymbol{h}_t(\boldsymbol{\beta}_t) &= \begin{bmatrix} h_{1,t}\big(\boldsymbol{x}_{1,t},\, T_t,\, \boldsymbol{b}_{1k}\big)\\ \vdots \\ h_{L,t}\big(\boldsymbol{x}_{1,t},\, T_t,\, \boldsymbol{b}_{1L}\big)\end{bmatrix},\\
\boldsymbol{H}_t &= \left.\frac{\partial\boldsymbol{h}_t(\boldsymbol{\beta}_t)}{\partial\boldsymbol{\beta}_t}\right|_{\hat{\boldsymbol{\beta}}_t},\\
\boldsymbol{\epsilon}_t &= \boldsymbol{\zeta}_t - \boldsymbol{h}_t(\bar{\boldsymbol{\beta}}_t), \text{ and}\\
\boldsymbol{R}_{t+1} &= d\boldsymbol{R}_t + (1-d)(\boldsymbol{\epsilon}_t^T\boldsymbol{\epsilon}_t + \boldsymbol{H}_t\hat{\boldsymbol{P}}_t\boldsymbol{H}_t^T),
\end{aligned} \tag{12}$$

where $\boldsymbol{K}_t$ represents the Kalman gain and $\boldsymbol{I}$ denotes the identity matrix. At time instant t, EKF estimates the corrected receiver state, $\bar{\boldsymbol{\beta}}_t$, and state covariance matrix, $\bar{\boldsymbol{P}}_t$. EKF adaptively estimates the measurement noise covariance matrix, $\boldsymbol{R}_t$, by assessing the post-residual vector, $\boldsymbol{\epsilon}_t$, and considering the forgetting factor as $d = 0.3$ [16]. The EKF-estimated clock bias $\hat{T}_t$ is used to compute the GPS timing, which is provided to the PMUs.

In time update, EKF predicts the next instant state vector using a state transition matrix, $\boldsymbol{F}$, and a static process noise covariance matrix, $\boldsymbol{Q}_t$, as:

$$\hat{\boldsymbol{\beta}}_{t+1} = \boldsymbol{F}\bar{\boldsymbol{\beta}}_t, \text{ and } \hat{\boldsymbol{P}}_{t+1} = \boldsymbol{F}\bar{P}_t\boldsymbol{F}^T + \boldsymbol{Q}_t, \tag{13}$$

where $\hat{\boldsymbol{\beta}}_{t+1}$ and $\hat{\boldsymbol{P}}_{t+1}$ are the predicted state and state covariance, respectively, at next time instant $t+1$, and

$$\boldsymbol{F} = \begin{bmatrix}\boldsymbol{I}_{4\times4} & \delta t\boldsymbol{I}_{4\times4}\\ \boldsymbol{0}_{4\times4} & \boldsymbol{I}_{4\times4}\end{bmatrix} \text{ and } \boldsymbol{Q}_t = \boldsymbol{F}\begin{bmatrix}\boldsymbol{0}_{4\times4} & \delta t\boldsymbol{I}_{4\times4}\\ \boldsymbol{0}_{4\times4} & \boldsymbol{\kappa}\end{bmatrix}\boldsymbol{F}^T,$$

where $\boldsymbol{\kappa} = \begin{bmatrix}\boldsymbol{0}_{3\times3} & 0\\ 0 & c\tau\end{bmatrix}$, with τ representing allan deviation of the front-end oscillator and δt denoting the update interval of the adaptive EKF step.

IV. Experiments

In this section, we validate the proposed BP-EKF algorithm in detecting and mitigating the effect of simulated meaconing

$$
\begin{aligned}
m_{f_{kn}\to\alpha_k}(\alpha_k) &= \int p(\boldsymbol{\gamma}_{kn}|\alpha_k,\alpha_n)\, b_{t-1}(\alpha_n) d\alpha_n \\
&= \int \frac{1}{\sqrt{(2\pi\nu^2)^{L_kL_n}}} \exp\left\{\frac{-L_kL_n}{2\nu^2}\left(\frac{\mathbf{1}^T\boldsymbol{\gamma}_{kn,t}}{L_kL_n} - (\alpha_k-\alpha_n)\right)^2\right\} \exp\left\{\frac{-(\alpha_n-\mu_{n,t-1})^2}{2\sigma^2_{n,t-1}}\right\} d\alpha_n \\
&\propto \exp\left\{\frac{-1}{2}\left[\frac{\nu^2}{2L_kL_n}+\sigma^2_{n,t-1}\right]^{-1}\left[\alpha_k-\mu_{n,t-1}+\frac{\mathbf{1}^T\boldsymbol{\gamma}_{kn,t}}{L_kL_n}\right]\right\}. \qquad (7)
\end{aligned}
$$

described in Section I. We also assess the voltage stability of a simulated power grid to compare the performance of the proposed BP-EKF and conventional scalar tracking [8].

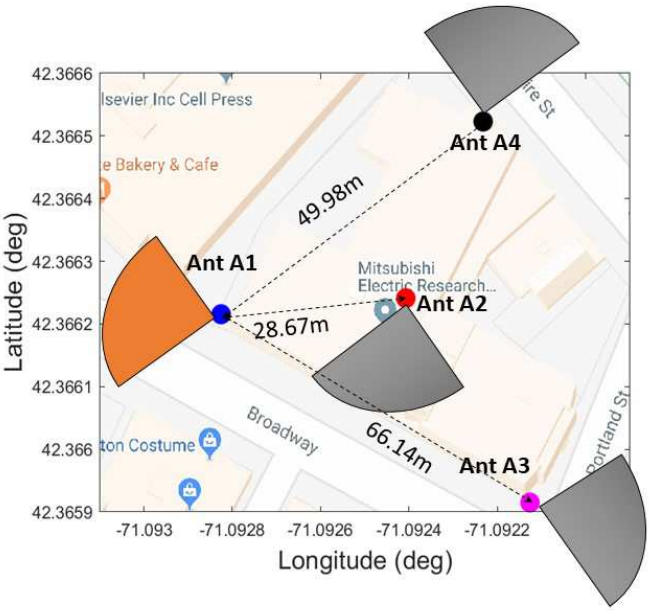

Fig. 4: Experiment setup consisting of four antenna-based DMDA with $A1$ antenna experiencing spoofing. The baseline information across antennas are pre-determined.

A. Implementation Details

The details of the implementation are divided into three main steps: simulating spoofed GPS signals, post-processing collected GPS signals and simulating power grid setup to assess the voltage stability.

1) Simulating spoofed GPS signals:

We simulated the received raw GPS signals using a C++ based software-defined GPS simulator known as GPS-SIM-SDR [17]. For a given stationary configuration of antenna and an ephemeris file, the GPS simulator generates baseband signal data streams. Based on the meaconing attack explained in Section I, we generated the corresponding spoofed GPS signals by adding high-powered simulated malicious samples to the generated authentic GPS samples. We collected simulated GPS signals at a sampling rate of 2.6 MHz, where each raw sample is a 16-bit complex. We mimicked the setup of a DMDA installed in a actual power substation by considering the pre-determined baseline information shown in Fig. 4. We designed a four-antenna based DMDA setup, in which each antenna is provided with selective visibility of the sky, such that the field of view of $A1, A2, A3, A4$ antennas are $135-225°$, $226-315°$, $316-45°$ and $46-135°$, respectively, in reference to geographic north. In the presence of simulated spoofing attacks, we consider the attacker to affects only A1 antenna, thereby, causing it to receive GPS signals from 9 satellites instead of the expected 3 satellites.

2) Post-processing GPS signals:

We post-processed the simulated GPS signals using a MATLAB-based software-defined radio known as SoftGNSS [18]. We utilized external ephemeris to extract authentic satellite positions, which are provided as input to the BP-EKF algorithm. We initialized the BP-EKF algorithm such that $\mu_{1,0}=0$ and $\sigma_{1,0}=\infty$ for the reference antenna and for the rest of the antennas, $\mu_{k,0}=0$ and $\sigma_{k,0}=0\,\forall\, k\in\{2,\ldots,M\}$.

3) Simulating power grid:

To assess the voltage stability at critical nodes in the microgrid, we utilized the MATLAB-based two-area Kundur Simulink model [19] to design a microgrid and main grid-based power setup, as seen in Fig. 5. We monitored the bus G1 at a critical node connecting the microgrid to the main grid by recording the phasor measurements using two PMUs, both of which are spoofed by a GPS attacker. However, the timing supplied to one of the PMUs is triggered using the proposed BP-EKF algorithm and the other is triggered via conventional scalar tracking. We analyzed the changes in a metric termed as voltage stability index (VSI) at the lth bus which represents G1 bus in the microgrid [2] shown in Fig. 5 and is given by

$$
I_{vs,l} = \frac{\sqrt{b_l^2 - 4a_lc_l}}{a_l}, \qquad (14)
$$

where $a_l \triangleq Q_{\mathrm{Z-load},l} + T_{lj}^2|Y_{lj}|\sin\left(\phi_{lj}\right)$, $b_l \triangleq Q_{\mathrm{I-load},l} + T_{lj}E_j|Y_{lj}|\sin\left(\theta_{lj}-\phi_{lj}\right)$, and $c \triangleq Q_{\mathrm{P-load},l} - Q_{\mathrm{max},l}$, such that, $Q_{\mathrm{Z-load,l}}, Q_{\mathrm{I-load,l}}$, $Q_{\mathrm{P-load,l}}$, and $Q_{\mathrm{max,l}}$ denote the nominal constant impedance, current, power, and maximum loads at the microgrid, respectively. At bus j, which represents a bus T1 in the main grid, E_j is voltage magnitude and δ_j is the voltage phase angle and $\theta_{lj} \triangleq \delta_l - \delta_j$ is phase angle difference between any bus l in microgrid and j in main grid. T_{lj} denote the transformer tap value, $|Y_{lj}|$ and ϕ_{lj} denotes the magnitude and angle of the admittance matrix.

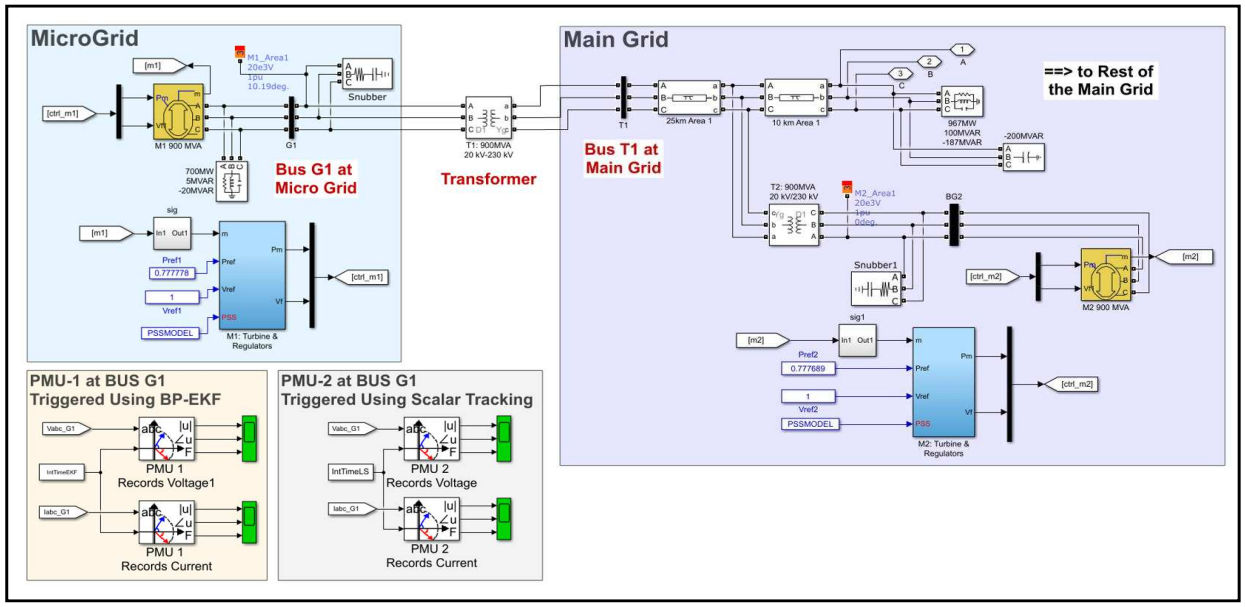

Fig. 5: The simulated grid setup consists of a microgrid which is connected to the main grid. The bus G1 monitors a critical node connecting the microgrid and the main grid. In the presence of meaconing, two PMUs are monitoring the bus G1, one of which is triggered using the BP-EKF algorithm and the other is triggered using the conventional scalar tracking scheme.

B. Meaconing

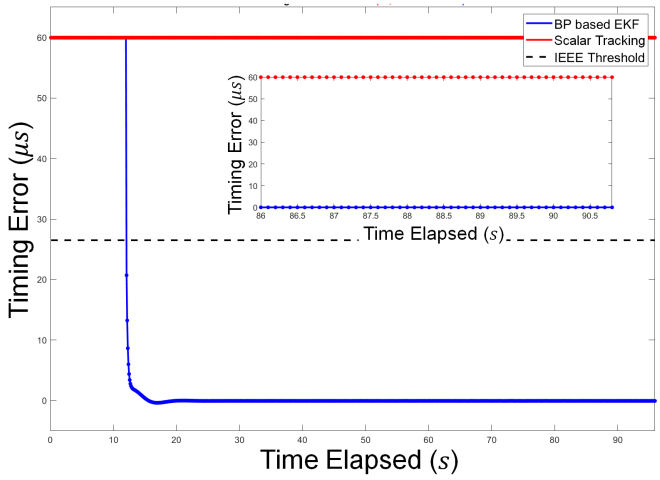

Fig. 6: Timing error estimated using the proposed BP-EKF algorithm, indicated in blue, is compared to that of the conventional scalar tracking scheme, indicated in red.

In this set of experiments, we added simulated meaconing to the simulated authentic GPS signal. The meaconing attack manipulates the target receiver to experience a timing delay of 60 μs and falsely estimate its position as the centroid of the antenna setup as compared to its true location. The attacker induces the pseudoranges corresponding to the subset of three expected satellites at this antenna to show a common error of 18000 m. The conventional scalar tracking with one omni-directional antenna, showed an RMS timing error of 59.95 μs as indicated by the red line in Fig. 6. However, the proposed BP-EKF algorithm, which is executed for $t \geq 12$s, demonstrated a significantly lower RMS timing error of -0.04 μs.

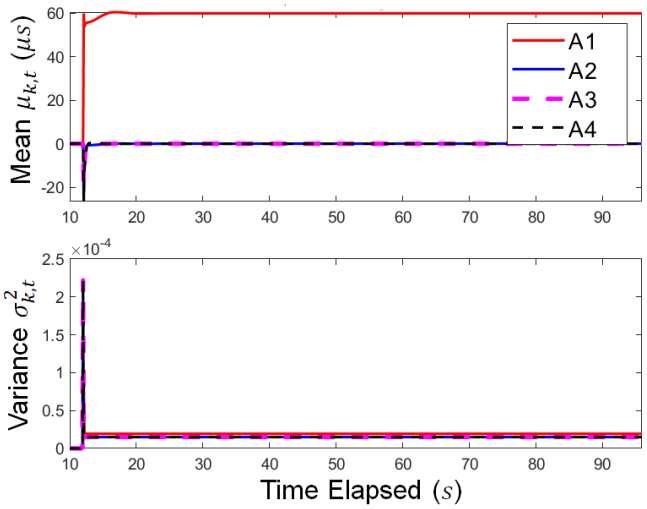

Fig. 7: Antenna-specific timing errors estimated during BP step, in particular its mean μ_1 and variance σ_1^2.

In particular, the proposed BP-EKF algorithm accurately not only detects and isolates the presence of spoofing attacks in A1 antenna but also accurately estimates the corresponding spoofing-induced timing error. This has been observed in Fig. 7, where the red line indicates that the timing error in A1 antenna calculated using the BP-EKF is $\alpha_k \approx 60$ μs, whereas the timing error in other antennas is close to zero.

Next, based on the VSI metric described in (14), we assessed the stability of the grid by comparing the perfor-

mance of two PMUs, one triggered via the proposed BP-EKF algorithm and the other via scalar tracking. As seen in Fig. 8, we observed an increase in the RMS VSI metric of 1.79, using the BP-EKF, indicating a significant improvement in voltage stability, whereas using scalar tracking, the RMS VSI metric is remained at a low value of 0.58.

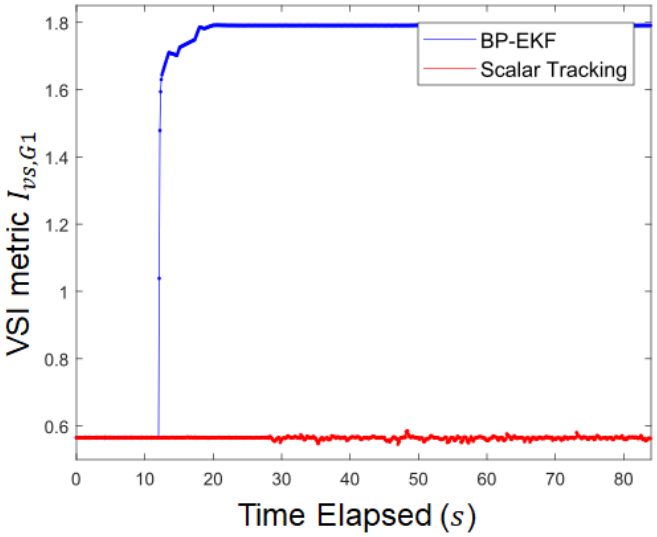

Fig. 8: Voltage Stability Index (VSI) of the G1 bus at the microgrid monitoring using two PMUs, one triggered via BP-EKF and the other via scalar tracking.

V. Conclusions and Future Works

To summarize, we have proposed an innovative geographically Distributed Multiple Directional Antennas (DMDA) setup, such that, each antenna points towards a different section of the sky. Thus, it receives GPS satellite signals from only a subset of total visible satellites. Based on this setup, we have developed a Belief Propagation-based Extended Kalman Filter (BP-EKF) algorithm that analyzes the single difference pseudorange residuals across each pair of antennas not only to detect the spoofing attacks but also to estimate the corresponding spoofing-induced timing error experienced by each antenna. Thereafter, we have corrected the pseudoranges that are later processed via an adaptive EKF to estimate the GPS timing.

We have validated the performance of the proposed BP-EKF using a four antenna-based DMDA setup, when subjected to a simulated meaconing attack that induces a delay of 60 μs. In this case, the scalar tracking that uses one omni-directional antenna has shown a high RMS timing error of 59.95 μs, thereby violating the IEEE-C37.118 standards, whereas the proposed BP-EKF algorithm demonstrates a low RMS timing error of -0.04 μs. In addition, to assess the stability of microgrid, we have evaluated the Voltage Stability Index (VSI) of the scalar tracking, which is at low RMS value of 0.58. In contrast, the BP-EKF can achieve a high RMS value of 1.79.

References

[1] M. Zima, M. Larsson, P. Korba, C. Rehtanz, and G. Andersson, "Design aspects for wide-area monitoring and control systems," *Proc. IEEE*, vol. 93, no. 5, pp. 980–996, 2005.

[2] Z. Wang, H. Sun, and D. Nikovski, "Static voltage stability detection using local measurement for microgrids in a power distribution network," in *Proc. IEEE Annual Conference on Decision and Control (CDC)*, (Osaka, Japan), pp. 3254–3259, Dec. 2015.

[3] V. V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. Begovic, and A. G. Phadke, "Wide-area monitoring, protection, and control of future electric power networks.," *Proc. IEEE*, vol. 99, no. 1, pp. 80–93, 2011.

[4] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 20–27, 2010.

[5] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[6] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, 2017.

[7] L. Heng, J. Makela, A. Dominguez-Garcia, R. Bobba, W. Sanders, and G. X. Gao, "Reliable GPS-based timing for power system applications: A multi-layered multi-receiver approach," in *Proc. IEEE Power and Energy Conference (PECI 2014)*, (Champaign, IL), Mar. 2014.

[8] P. Misra and P. Enge, "Global positioning system signals, measurements, and performance," *USA: Ganga Jamuna Press*, 2006.

[9] M. Lixia, C. Muscas, and S. Sulis, "On the accuracy specifications of phasor measurement units," in *Proc. IEEE Instrumentation and Measurement Technology Conference (I2MTC)*, (Austin, TX), pp. 1435–1440, May 2010.

[10] C. Fernández-Prades, J. Arribas, and P. Closas, "Robust GNSS receivers by array signal processing: Theory and implementation," *Proc. IEEE*, vol. 104, no. 6, pp. 1207–1220, 2016.

[11] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, no. 2, pp. 40–46, 2009.

[12] Z. Zhang and X. Zhan, "GNSS spoofing network monitoring based on differential pseudorange," *Sensors*, vol. 16, no. 10, p. 1771, 2016.

[13] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, 2001.

[14] M. Leng and Y.-C. Wu, "Distributed clock synchronization for wireless sensor networks using belief propagation," *IEEE Trans. Signal Process.*, vol. 59, pp. 5404–5414, 2011.

[15] M. K. Simon, *Probability distributions involving Gaussian random variables: A handbook for engineers and scientists*. Springer Science & Business Media, 2007.

[16] S. Akhlaghi, N. Zhou, and Z. Huang, "Adaptive adjustment of noise covariance in Kalman filter for dynamic state estimation," in *Proc. IEEE Power & Energy Society General Meeting*, (Chicago, IL), pp. 1–5, Jul. 2017.

[17] T. Ebinuma, "GPS-SDR-SIM," *[Online] Available: https://github.com/osqzss/gps-sdr-sim*.

[18] K. Paul, "Soft gnss," *[Online] Available: https://github.com/kristianpaul/SoftGNSS*.

[19] MathWorks, "PMU (PLL-based, Positive-Sequence) Kundur's Two-Area System," *[Online], Available: https://www.mathworks.com/help/physmod/sps/examples/pmu-pll-based-positive-sequence-kundur-s-two-area-system.html*.