Wide-Area GPS Time Monitoring Against Spoofing Using Belief Propagation

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

TR2019-044 June 28, 2019

Abstract
A wide-area time authentication algorithm is proposed to compute the Global Positioning System (GPS) timing that is resilient against spoofing attacks. The considered widearea network consists of multiple GPS receiving systems, each comprising of the innovative distributed multiple directional antennas (DMDA) setup triggered via a common clock. Based on the communication infrastructure of the grid, the single-difference pseudorange residuals across the antennas are processed using the wide-area belief propagation-based extended Kalman filter (BP-EKF) algorithm in a distributed manner. To detect spoofing, a KL-divergence-based threshold is used to estimate the dissimilarity in the antenna-specific timing errors. Thereafter, the pseudoranges are corrected using the BP estimates of timing error and processed via adaptive EKF to compute the GPS timing, which is given to the phasor measurement units (PMUs). We have demonstrated the successfully detection and mitigation of the external timing attack, by subjecting one receiving system to a simulated meaconing attack that induces a 60 micro second time delay. Thereafter, by analyzing the voltage stability index of a critical node in the simulated grid, we have also validated the compliance of the proposed wide-area BP-EKF estimated timing with the IEEE-C37.118 standards.

IEEE International Conference on Sensing, Communication and Networking

Wide-Area GPS Time Monitoring Against Spoofing Using Belief Propagation

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

***Abstract*—A wide-area time authentication algorithm is proposed to compute the Global Positioning System (GPS) timing that is resilient against spoofing attacks. The considered wide-area network consists of multiple GPS receiving systems, each comprising of the innovative distributed multiple directional antennas (DMDA) setup triggered via a common clock.**

Based on the communication infrastructure of the grid, the single-difference pseudorange residuals across the antennas are processed using the wide-area belief propagation-based extended Kalman filter (BP-EKF) algorithm in a distributed manner. To detect spoofing, a KL-divergence-based threshold is used to estimate the dissimilarity in the antenna-specific timing errors. Thereafter, the pseudoranges are corrected using the BP estimates of timing error and processed via adaptive EKF to compute the GPS timing, which is given to the phasor measurement units (PMUs). We have demonstrated the successfully detection and mitigation of the external timing attack, by subjecting one receiving system to a simulated meaconing attack that induces a 60 micro second time delay. Thereafter, by analyzing the voltage stability index of a critical node in the simulated grid, we have also validated the compliance of the proposed wide-area BP-EKF estimated timing with the IEEE-C37.118 standards.

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

I. Introduction

To monitor the grid stability, wide area monitoring system (WAMS) [1] measures the synchronized phasor measurements, i.e., voltage and current values, which are recorded using the advanced devices known as the phasor measurement units (PMUs) [2]. Utilizing the communication infrastructure proposed in the North American Synchro-Phasor Initiative [3], WAMS plays a crucial role in ensuring a high-resolution state estimation of the grid and early-detection of destabilizing conditions. PMUs rely on precise time-keeping sources, such as Global Navigation Satellite System (GNSS), to obtain microsecond level accuracy in timing [4]. However, GNSS civilian signals are unencrypted and their power is as low as -160 dBW, which makes them vulnerable to external spoofing attacks. The IEEE C37.118.1-2011 prescribes a criterion based on total vector error (TVE) [5], according to which we consider 1% TVE equivalent to a timing error of 26.5 μs, as a benchmark in our stability analysis.

While minimizing the detection probability of the attack, the spoofer broadcasts malicious look-alike GNSS signals to induce timing errors that disrupt the stability of the grid. A type of spoofing attack, namely, meaconing [6], which is also known as record-and-replay, involves recording the authentic GPS signals at a physical location and later broadcasting these recorded signals with higher power towards a target receiver. An attacker executing meaconing manipulates the target receiver's computed time, and may or may not affect the estimated position of the target receiver. Given the requirements for a relatively simple hardware and minimal knowledge of GNSS functioning [7], meaconing poses serious threats to the safety of the entire grid. Even though the current work focuses on meaconing, the generalized framework of this paper can be directly applicable for other attacks, namely, data-level and signal-level spoofing [8].

Prior research [9] utilized a multiple antenna-based quickest GPS spoofing detection algorithm, which applies a probabilistic metric of the carrier signal to noise ratio from two receiving antennas. The authors of [10] defined a method to exchange redundant time signals across power substations in a wide-area network by employing an IEEE 1588 standard [11], which provides a high-accuracy time over an Ethernet connection. Utilizing the sequential PMU data obtained from phasor data concentrators, a recent work [12] proposed a distributed real-time wide-area oscillation estimation approach that is robust to GPS spoofing. In [13], the authors authenticated the GPS timing using a network of widely dispersed static receivers and their known positions by cross-checking for the presence of encrypted military P(Y) codes. In contrast to existing work, we can summarize the contribution of this paper as follows:

1) This paper utilizes an innovative geographically distributed multiple directional antennas (DMDA) setup which was proposed by [14], in which each antenna points towards a different section of the sky, and therefore, receives GNSS satellite signals from only a subset of the total visible satellites.
2) With an aim to reduce the sensitivity of the prior distribution at each antenna in the BP-EKF algorithm and to improve the attack-resilience, this paper extends the belief-propagation (BP)-based extended Kalman filter (EKF) algorithm to develop a wide-area BP-EKF authentication algorithm.
3) By detecting and mitigating the effect of spoofing attacks, the proposed wide-area BP-EKF algorithm can authenticate a wide-area network of power substations in a distributed manner. A wide-area network is recognized as the grid that several power substations are located at different locations to prevent attacker to corrupt all

S. Bhamidipati is with the University of Illinois at Urbana-Champaign (UIUC), Urbana, IL, 61801, USA (email:sbhamid2@illinois.edu).

K. J. Kim, H. Sun, and P. V. Orlik are with Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, 02139 USA (e-mail: {kkim,hongbosun,porlik}@merl.com).

This work was done when S. Bhamidipati was working with MERL.

satellite signals received by different receiving systems.

II. DMDA Setup

Several advantages of the DMDA setup proposed by [14] are summarized as follows:

1) In authentic conditions, each directional antenna, as seen in Fig. 1, sees satellites that match the expected subset of satellites found in their section of the sky. However, during an attack, the spoofed antenna may see more satellites than expected.
2) Given that spoofing is a directed attack executed from a near-ground level ($<<< 20,200$ km), the attacker cannot simultaneously attack all the antennas of the DMDA configuration.
3) We utilize the geographical diversity between the antennas in the proposed DMDA setup to obtain the corresponding pre-computed baseline information, which is useful in distinguishing spoofing attacks affecting multiple antennas.
4) Since all the antennas in the proposed DMDA setup are triggered by a common clock, in authentic conditions, the pseudoranges measured 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.

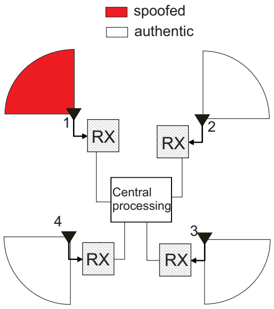


Fig. 1: Configuration of the employed DMDA setup. Sector of circle represents the field-of-view of each antenna.

III. The wide-area BP-EKF algorithm

In this section, we explain the wide-area BP-EKF architecture, which is used to perform GNSS spoofing detection and mitigation and thereafter, provides attack-resilient GNSS timing to the microgrids in the power distribution networks.

To perform a wide-area authentication of GPS timing against spoofing attacks, we consider a network of N power substations, as seen in Fig. 2. Each ath power substation, such that $\forall a \in \{1, \cdots, N\}$, is equipped with a GPS receiving system that includes a common clock and a DMDA setup with M_a antennas. For any ath receiving system, we define its *neighboring system* $\mathcal{S}_a$ based on the already-in place communication structure designed for PMU data monitoring. Any bth receiving system is included in its set of neighboring system $\mathcal{S}_a$, if there exists a communication link π_{ab} between ath and bth receiving systems, i.e., $b \in \mathcal{S}_a$, if $\pi_{ab} = 1, \forall b \in \{1, \cdots, N\},\ b \neq a$. We carry out the processing in a distributed manner, such that, each receiving system exchanges its *system data* with the neighboring systems based on the pre-existing wired or wireless communication framework [15]. The details regarding the system data are further explained in Section III-2. For any kth antenna in the ath receiving system, such that $k \in \{1, \cdots, M_a\}$, its *neighboring antennas* $\mathcal{B}_k^a$ represent the set of antennas in its receiving system excluding itself, as well as the antennas in the receiving systems that belong to its neighboring system $\mathcal{S}_a$, such that,

$$\mathcal{B}_k^a = \Big\{\{1, \cdots, M_a\} - k\Big\} \bigcup_{b \in \{1, \cdots, |\mathcal{S}_a|\}} \{1, \cdots, M_b\}.$$

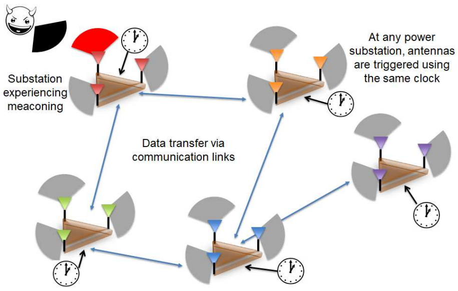

Substation experiencing meaconing
Data transfer via communication links
At any power substation, antennas are triggered using the same clock

Fig. 2: Wide-area network of GPS receiving systems, each equipped with a common clock and a DMDA setup.

Next, independently at each receiving system, we collectively process the information in a centralized processing (CP) unit. The overall framework of the proposed wide-area BP-EKF algorithm, seen in Fig. 3, is described as follows:

1) Across the wide-area, pseudoranges are measured at each directional antenna in each receiving system. Based on the communication structure, the *system data* is exchanged across the receiving systems.
2) At each receiving system, we form all the possible pairs of antennas, such that, first one represents an antenna within its receiving system and the second antenna belongs to the *neighboring antennas* of the first antenna. Across each antenna pair, we compute the *single difference residual vector* by considering, one satellite from the first antenna and the another satellite visible to the second antenna.
3) At each antenna, the marginal Gaussian distribution of the antenna-specific timing error is computed, which is termed as *belief*.
4) At each GPS receiving system, we correct the pseudoranges using the BP estimates of antenna-specific timing errors, which are later adaptively processed via EKF in the CP unit. The CP unit estimate the GPS timing, which is given to the PMUs for time-tagging the phasor measurements.
5) We utilize the BP estimates of the antenna-specific timing errors to compute a test statistic that is evaluated against a KL-divergence [16]-based threshold to authenticate the spoofing status of each GPS receiving system.

Highly computational extensive calculation of marginal distribution is simplified through the distributed algorithm, namely, BP. Thus, BP plays a pivotal role in maintaining accuracy while reducing latency involved in spoofing detection, which is critical for timing-related applications. Due to using a larger number of widely-distributed antennas, correlation between errors will be lower, which in-turn lead to a lower false alarm and missed detection probability. Unlike single area BP-EKF algorithm, the wide-area setup overcomes the case where spoofing affects all the antennas in one GPS receiving system.

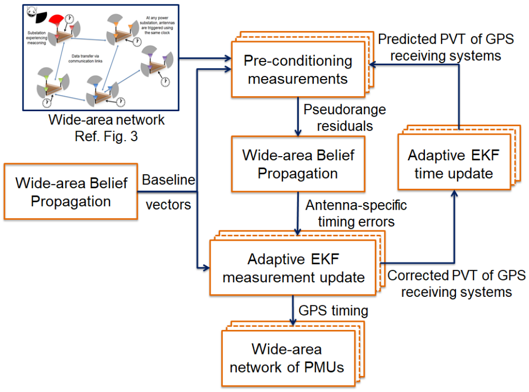

Substation experiencing meaconing
At any power substation, antennas are triggered using the same clock
Data transfer via communication links
Wide-area network
Ref. Fig. 3
Pre-conditioning measurements
Predicted PVT of GPS receiving systems
Pseudorange residuals
Wide-area Belief Propagation
Adaptive EKF time update
Wide-area Belief Propagation
Baseline vectors
Antenna-specific timing errors
Adaptive EKF measurement update
Corrected PVT of GPS receiving systems
GPS timing
Wide-area network of PMUs

Fig. 3: Flowchart of the wide-area BP-EKF algorithm.

By utilizing the GPS signals received at multiple power substations spread-out in a wide-area network, we describe the proposed wide-area BP-EKF algorithm as follows:

1) Pre-conditioning the GPS measurements:

At each ath receiving system, we obtain the pre-computed baseline vectors between the antennas, which are denoted by $\boldsymbol{b}_{kn}^a$, $k, n \in \{1, \dots, M_a\}$, $a \in \{1, \cdots, N\}$. We also define the three-dimensional (3D) position as $\boldsymbol{x}_{k,t}^a = [x, y, z]_k$ and 3D velocity as $\boldsymbol{v}_{k,t}^a = [\dot{x}, \dot{y}, \dot{z}]_k$ of the kth antenna at tth time.

At any ath receiving system, the pseudorange measured at the kth antenna corresponding to the ith satellite is given by

$$\begin{aligned}\rho_k^i &= ||\boldsymbol{x}_1^a - \boldsymbol{b}_{1k}^a - \boldsymbol{y}^i|| + (c\delta t_t^a + c\alpha_k^a - c\delta t^i) + I^i + \omega_k^i, \\ &= h_k^a\big(\boldsymbol{x}_1^a,\, T^a,\, \boldsymbol{y}_t^i\big) + c\alpha_k^a, \qquad (1)\end{aligned}$$

where i indexes the total visible satellites $L_{k,t}$ at the kth antenna in the ath receiving system. $\boldsymbol{y}_t^i$ and $c\delta t^i$ respectively denote the 3D position and clock corrections of the ith satellite. Given that the antennas are triggered using the same clock at each receiving system, the corresponding common clock bias $c\delta t_t^a$ is independent of the kth antenna considered. The antenna-specific timing errors in pseudorange are denoted by α_k^a and $h_k^a(.)$ denotes the measurement model of the kth antenna of the ath receiving system, which depends on the $k = 1$ antenna's 3D position $\boldsymbol{x}_{1,t}^a$, receiver clock bias $c\delta t_t^a$, pre-computed baseline vector $\boldsymbol{b}_{1k}^a$ and the satellite position $\boldsymbol{y}_t^i$. The atmospheric errors I_t^i related to ionosphere and troposphere are estimated using existing models [7]. ω_k^i represents the additive Gaussian white noise in the satellite measurements.

Given the predicted state vector $\hat{\boldsymbol{\beta}}_t^a = [\boldsymbol{x}_1,\, c\delta t,\, \boldsymbol{v}_1,\, c\delta\dot{t}]_t^T$ obtained from the EKF time update, the known baseline vectors $\boldsymbol{b}_{1k}^a$, the satellite 3D position $\boldsymbol{y}_t^i$, and clock corrections $c\delta t^i$, we compute the pseudorange residuals at tth time from (1) as follows:

$$\Delta\rho_{k,t}^i = \rho_{k,t}^i - ||\hat{\boldsymbol{x}}_{k,t} - \boldsymbol{y}^i|| - (c\delta\hat{t} - c\delta t^i) - I^i, \qquad (2)$$

where $\hat{\boldsymbol{x}}_{k,t} \triangleq \hat{\boldsymbol{\beta}}_t^a\{\boldsymbol{x}_1\} - \boldsymbol{b}_{1k}^a$, and $c\delta\hat{t} \triangleq \hat{\boldsymbol{\beta}}_t^a\{c\delta t\}$.

2) System data exchange and measurement likelihood:

Based on the communication structure of the wide-area network, the *system data* is exchanged across different GPS receiving systems. In particular, system data transmitted from the ath receiving system comprises of the following: number of antennas M_a as well as pseudorange residuals $\Delta\rho_{k,t}^i$ and beliefs $b_{t-1}(\alpha_k^a)$ at each kth antenna of the receiving system.

At the ath receiving system, we obtain the system data from all the receiving systems that belong to its neighboring system $\mathcal{S}_a$. Thereafter, we form all the possible pairs of antennas, by considering the first antenna from the same ath receiving system, i.e., $k \in \{1, \cdots, M_a\}$ and the second antenna from the set of its neighboring antennas, i.e., $n \in \mathcal{B}_k^a$. Later, 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

$$\gamma_{kn,t}^{ij} = \frac{1}{c}(\Delta\rho_{k,t}^i - \Delta\rho_{n,t}^j), \qquad (3)$$

such that,

$$\begin{aligned}\gamma_{kn,t}^{ij} &= \alpha_k^a - \alpha_n^b + \omega_{kn}^{ij} \\ &= \begin{cases} 0, & k, n \in \{1, \dots, M_a\},\ k \neq n \\ \eta_{ab}, & k \in \{1, \dots, M_a\},\ n \in \{1, \dots, M_b\}, a \neq b \end{cases} \qquad (4)\end{aligned}$$

where in authentic conditions, $\gamma_{kn}^{ij} \approx 0$ across any two antennas that belong to the same ath receiving system. However, across antennas that belong to two different ath and bth receiving systems, γ_{kn}^{ij} is a non-zero value η_{ab} due to the error in predicted clock bias estimates and the receiver noise. According to (4), we calculate the measurement metric $\boldsymbol{\gamma}_{kn,t} = \{\gamma_{kn,t}^{ij},\ i \in L_{k,t},\ j \in L_{n,t}\}$ across all the pairs of antennas and the corresponding satellites observed at the respective antennas. Across a pair of antennas, the corresponding measurement likelihood probability is calculated as

$$\begin{aligned}p(\boldsymbol{\gamma}_{kn,t}|\alpha_k^a, \alpha_n^b) &= \frac{1}{\sqrt{(2\pi\nu^2)^{L_{k,t}L_{n,t}}}} \\ &\exp\left\{\frac{-L_{k,t}L_{n,t}}{2\nu_{kn}^2}\Big(\frac{\boldsymbol{1}^T\boldsymbol{\gamma}_{kn,t}}{L_{k,t}L_{n,t}} + (\alpha_k^a - \alpha_n^b)\Big)^2\right\} \forall\ n \in \mathcal{B}_k^a, \quad (5)\end{aligned}$$

where $b \in S_a$ represents the GPS receiving system that corresponds to n, and ν_{kn}^2 denotes the measurement variance of the summation of single difference residual components which comprises of errors observed due to pseudoranges, errors in satellite ephemeris, predicted position and velocity of the antenna.

3) *Belief Propagation:*

To authenticate each receiving system against spoofing attacks as well as estimate the corresponding spoofing-induced timing errors at each antenna, we compute its *marginal distribution* using a factor graph-based BP framework.

At the ath receiving system, given the joint posterior distribution $p(\alpha_1, \dots, \alpha_{M_a}|\gamma_{kn})$, the marginal distributions $g(\cdot)$ is formulated as

$$\begin{aligned} &g(\alpha_k^a) = \\ &\int_{\alpha_1^a,\dots,\alpha_{k-1}^a} \int_{\alpha_{k+1}^a,\dots,\alpha_M^a} p(\alpha_1^a, \dots, \alpha_{M_a}^a|\{\gamma_{kn}\}_{k=1,\dots,M_a,n\in\mathcal{B}_k^a}) \\ &\quad d\alpha_1^a \dots d\alpha_{k-1}^a \, d\alpha_{k+1}^a \dots d\alpha_{M_a}^a. \end{aligned} \tag{6}$$

With an increased number of antennas in the wide-area network, (6) becomes computationally intractable. Thus, we formulate a factor graph-based BP to approximate the marginal distribution in a computationally-efficient manner, which is termed as belief $b_t(\alpha_k^a)$. We compute belief $b_t(\alpha_k^a)$ at the kth antenna as the product of its prior distribution and all the *incoming messages* from all the neighboring antennas. Given that the attacker transmits counterfeit GPS signals, the corresponding spoofing-induced timing errors follow a Gaussian distribution $\mathcal{N}(\cdot : \cdot, \cdot)$. Therefore, we model the belief as Gaussian [17] with the mean $\mu_{k,t}^a$ and variance $(\sigma_{k,t}^a)^2$, which is represented as follows:

$$\begin{aligned} b_t(\alpha_k^a) &= m_{f_k^a \to \alpha_k^a} \prod_{n\in\mathcal{B}_k^a} m_{f_{kn}^a \to \alpha_k^a}(\alpha_k^a), \\ &= \mathcal{N}\big(\alpha_k^a : \mu_{k,t}^a, (\sigma_{k,t}^a)^2\big), \end{aligned} \tag{7}$$

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

As seen in (7), at the kth antenna of the ath receiving system, we update the belief $b_t(\alpha_k^a)$ of the antenna-specific timing error by computing two kinds of messages, namely, measurement-related messages $m_{f_{kn}^a \to \alpha_k^a}$ and prior-related message $m_{f_k^a \to \alpha_k^a}$.

Firstly, the message $m_{f_{kn}^a \to \alpha_k^a}$ is based on the factor node f_{kn}^a and represents the belief of the nth neighboring antenna $n \in \mathcal{B}_k^a$ on the variable node α_k^a. We derive the message $m_{f_{kn}^a \to \alpha_k^a}$ from the Eqs. (5) and (7) to compute (8), which is provided at the top of the next page. We represent $m_{f_{kn}^a \to \alpha_k^a}$ as a Gaussian distribution given by

$$m_{f_{kn}^a \to \alpha_k^a}(\alpha_k^a) \approx \mathcal{N}\big(\alpha_k^a : \mu_{kn,t}^a, (\sigma_{kn,t}^a)^2\big), \tag{9}$$

where $\mu_{kn,t}^a = \mu_{n,t-1}^a - \dfrac{\mathbf{1}^T \gamma_{kn,t}}{L_{k,t}L_{n,t}}$ and $(\sigma_{kn,t}^a)^2 = \dfrac{\nu_{kn}^2}{2L_{k,t}L_{n,t}} + (\sigma_{kn,t-1}^a)^2$.

Secondly, we consider the message $m_{f_k^a \to \alpha_k^a}$, which represents the prior distribution formulated as a Gaussian, i.e., $p(\alpha_k^a) = \mathcal{N}\big(\alpha_k^a : \mu_{pk,t}^a, (\sigma_{pk,t}^a)^2\big)$, where the mean is denoted as $\mu_{pk,t}^a$ and variance as $(\sigma_{pk,t}^a)^2$. Based on this, the message from factor node f_k^a to the variable node α_k^a is computed as

$$\begin{aligned} m_{f_k^a \to \alpha_k^a} &= p(\alpha_k^a) \int b(\alpha_k^a) d\alpha_k^a \\ &= p(\alpha_k^a) = \mathcal{N}\big(\alpha_k^a : \mu_{pk,t}^a, (\sigma_{pk,t}^a)^2\big). \end{aligned} \tag{10}$$

Thus, we compute the updated belief for time instant t as

$$\begin{aligned} &b_t(\alpha_k^a) \\ &= \mathcal{N}\big(\alpha_k^a : \mu_{pk,t}^a, (\sigma_{pk,t}^a)^2\big) \prod_{n\in\mathcal{B}_k^a} \mathcal{N}\big(\alpha_k^a : \mu_{kn,t}^a, (\sigma_{kn,t}^a)^2\big), \\ &= \mathcal{N}\big(\alpha_k^a : \mu_{k,t}^a, (\sigma_{k,t}^a)^2\big), \end{aligned} \tag{11}$$

where

$$\begin{aligned} (\sigma_{k,t}^a)^2 &= \Big(\frac{1}{(\sigma_{pk,t}^a)^2} + \sum_{n\in\mathcal{B}_k^a} \frac{1}{(\sigma_{kn,t}^a)^2}\Big)^{-1}, \text{ and} \\ \mu_{k,t}^a &= (\sigma_{k,t}^a)^2 \Big(\frac{\mu_{pk,t}^a}{(\sigma_{pk,t}^a)^2} + \sum_{n\in\mathcal{B}_k^a} \frac{\mu_{kn,t}^a}{(\sigma_{kn,t}^a)^2}\Big). \end{aligned} \tag{12}$$

4) *Dependency of wide-area BP on prior distribution:*

As discussed in Section III-3, (10) indicates the prior distribution of the antenna-specific timing error. In the prior work [14], if the mismatch between the observed and the expected set of satellites, as explained in Section III-6, is ≥ 2, then we estimated the parameters, such that, $\mu_{pk,t}^a = 0$ and $(\sigma_{pk,t}^a)^2 = \infty$, thereby representing an approximated uniform distribution. However, by utilizing a wide-area network of antennas, we significantly reduce the dependency of the attack-resilience of the GPS timing on this prior distribution. To achieve this, among the N widely-dispersed power substations, we choose the GPS receiving system with the least spoofing risk, i.e., $a_m = \underset{a\in\{1,\cdots,N\}}{\arg\min}\ r_a$, where r_a, $\forall a \in \{1, \cdots, N\}$ is computed later in Section III-6. Except the a_mth receiving system, we assign the prior distribution of GPS receiving system, such that,

$$\mu_{pk,t}^a = 0,\ (\sigma_{pk,t}^a)^2 = \infty,\ \forall a \in \{1, \cdots, N\} - a_m.$$

However, for the a_mth receiving system, $\mu_{pk,t}^a$ and $(\sigma_{pk,t}^a)^2$ are computed from the empirical distribution calculated on-the fly by considering the most recent W timing errors $\alpha_{k,t-W:t}^{a_m} \forall k = \{1, \cdots, M\}$.

5) *Adaptive EKF:*

Independently at each ath GPS receiving system, we utilize the estimated $\alpha_{k,t}^a$ $\forall k \in \{1, \cdots, M_a\}$ using wide-area BP algorithm to correct the pseudoranges, such that,

$$\boldsymbol{\zeta}_t^a = [\rho_c^1, \dots, \rho_c^{L_a}],\ \forall a \in \{1, \cdots, N\},$$

where $\rho_c^i \triangleq \rho_k^i - c\alpha_k^a$ and $L_a \triangleq L_1 + \cdots + L_{M_a}$ indicates the total number of satellites. Thereafter, we execute a closed-loop adaptive-EKF algorithm, which has two main steps, namely, measurement update and time update.

By considering $\boldsymbol{\zeta}_t^a$, the adaptive measurement noise covariance matrix $\boldsymbol{R}_t^a$, the measurement model $\boldsymbol{H}_t^a$, the predicted

$$m_{f^a_{kn}\to\alpha^a_k}(\alpha^a_k) = \int_{n\in\mathcal{B}^a_k} p(\gamma_{kn}|\alpha^a_k,\alpha^b_n)\, b_{t-1}(\alpha^b_n) d\alpha^b_n,$$
$$= \int \frac{1}{\sqrt{(2\pi\nu^2)^{L_kL_n}}}\exp\bigg\{\frac{-L_kL_n}{2\nu^2}\Big(\frac{\mathbf{1}^T\boldsymbol{\gamma}_{kn,t}}{L_kL_n} - (\alpha^a_k - \alpha^b_n)\Big)^2\bigg\}\exp\bigg\{\frac{-(\alpha^b_n - \mu^b_{n,t-1})^2}{2(\sigma^b_{n,t-1})^2}\bigg\}d\alpha^b_n,$$
$$\propto \exp\bigg\{\frac{-1}{2}\bigg[\frac{\nu^2}{2L_kL_n} + (\sigma^b_{n,t-1})^2\bigg]^{-1}\bigg[\alpha^a_k - \mu^b_{n,t-1} + \frac{\mathbf{1}^T\boldsymbol{\gamma}_{kn,t}}{L_kL_n}\bigg]\bigg\}. \tag{8}$$

state vector $\hat{\boldsymbol{\beta}}^a$ and the predicted state covariance matrix $\hat{\boldsymbol{P}}^a_t$, we perform the measurement update as

$$\bar{\boldsymbol{\beta}}^a_t = \big(\boldsymbol{I}_8 - \boldsymbol{K}_t\boldsymbol{H}^a_t\big)\hat{\boldsymbol{\beta}}^a_t + \boldsymbol{K}_t\boldsymbol{\zeta}^a_t,$$
$$\bar{\boldsymbol{P}}^a_t = \big(\boldsymbol{I}_8 - \boldsymbol{K}_t\boldsymbol{H}^a_t\big)\hat{\boldsymbol{P}}^a_t,$$
$$\boldsymbol{K}_t = \hat{\boldsymbol{P}}^a_t(\boldsymbol{H}^a_t)^T\Big(\boldsymbol{H}^a_t\hat{\boldsymbol{P}}^a_t(\boldsymbol{H}^a_t)^T + \boldsymbol{R}^a_t\Big)^{-1},$$

$$\boldsymbol{h}^a_t(\boldsymbol{\beta}_t) = \begin{bmatrix} h_{1,t}\big(\boldsymbol{x}_{1,t},\, T_t,\, \boldsymbol{b}_{1k}\big) \\ \vdots \\ h_{L,t}\big(\boldsymbol{x}_{1,t},\, T_t,\, \boldsymbol{b}_{1L}\big)\end{bmatrix}, \tag{13}$$
$$\boldsymbol{H}_t = \frac{\partial \boldsymbol{h}^a_t(\boldsymbol{\beta}^a_t)}{\partial\boldsymbol{\beta}^a_t}\bigg|_{\hat{\boldsymbol{\beta}}^a_t},$$
$$\boldsymbol{\epsilon}_t = \boldsymbol{\zeta}_t - \boldsymbol{h}_t(\bar{\boldsymbol{\beta}}^a_t), \text{ and}$$
$$\boldsymbol{R}^a_{t+1} = d\boldsymbol{R}^a_t + (1-d)(\boldsymbol{\epsilon}_t^T\boldsymbol{\epsilon}_t + \boldsymbol{H}^a_t\hat{\boldsymbol{P}}^a_t(\boldsymbol{H}^a_t)^T),$$

where $\boldsymbol{K}_t$ represents the Kalman gain and $\boldsymbol{I}_8$ denotes the 8×8 identity matrix. At time instant t, we estimate the corrected receiver state $\bar{\boldsymbol{\beta}}^a_t$ and state covariance matrix $\bar{\boldsymbol{P}}^a_t$. We adaptively estimate the measurement noise covariance matrix $\boldsymbol{R}^a_t$ by assessing the post-residual vector $\boldsymbol{\epsilon}_t$ and considering the forgetting factor as $d = 0.3$ [18]. The EKF-estimated clock bias $c\delta t^a_t = \bar{\boldsymbol{\beta}}^a_t\{c\delta t\}$ is used to compute the GPS timing, which is provided to the PMUs.

During time update, we predict the next instant state vector using a state transition matrix $\boldsymbol{F}$ and a static process noise covariance $\boldsymbol{Q}^a_t$ given by

$$\hat{\boldsymbol{\beta}}^a_{t+1} = \boldsymbol{F}\bar{\boldsymbol{\beta}}^a_t, \text{ and } \hat{\boldsymbol{P}}^a_{t+1} = \boldsymbol{F}\bar{P}^a_t\boldsymbol{F}^T + \boldsymbol{Q}^a_t \tag{14}$$

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

$$\boldsymbol{F} = \begin{bmatrix}\boldsymbol{I}_4 & \delta t\boldsymbol{I}_4 \\ \mathbf{0}_4 & \boldsymbol{I}_4\end{bmatrix} \text{ and } \boldsymbol{Q}^a_t = \boldsymbol{F}\begin{bmatrix}\mathbf{0}_4 & \delta t\boldsymbol{I}_4 \\ \mathbf{0}_4 & \boldsymbol{\kappa}^a\end{bmatrix}\boldsymbol{F}^T,$$

where $\boldsymbol{\kappa}^a = \begin{bmatrix}\mathbf{0}_3 & 0 \\ 0 & c\tau^a\end{bmatrix}$, τ^a represents allan deviation of the front-end oscillator, and δt denotes the update interval of our adaptive EKF step.

6) Authentication of GPS receiving systems:

Based on the belief estimates of the timing error at each antenna, we compute the spoofing risk, denoted by r^a_t at each ath receiving system as follows:

$$r^a_t = \sum_{\nu=0}^{W}\sum_{i=1}^{M_a}\sum_{j=1,j\neq i}^{M_a}\left(\alpha^a_{i,t-\nu}\,\ln\left(\frac{\alpha^a_{i,t-\nu}}{\alpha^a_{j,t-\nu}}\right)\right). \tag{15}$$

To evaluate the spoofing risk at each ath receiving system, we need to monitor the values of the BP estimates of antenna-specific timing error as well as their similarity across the antennas within the GPS receiving system. Therefore, we evaluate the KL divergence [16]-based test statistic over the most recent W time instants, which is measured against a pre-determined threshold Π, such that, if $r^a_t <= \Pi$, then the ath receiving system is denoted as authentic, whereas if $r^a_t > \Pi$, then the ath receiving system has high spoofing risk and therefore, termed as unreliable.

IV. Experiments

In this section, we validate our wide-area BP-EKF algorithm to detect and mitigate the timing error caused due to simulated meaconing. We also assess the voltage stability of different microgrids triggered using different GPS receiving systems, to validate the attack-resilience of the proposed wide-area BP-EKF with respect to a single-area BP-EKF [14] and conventional scalar tracking [7].

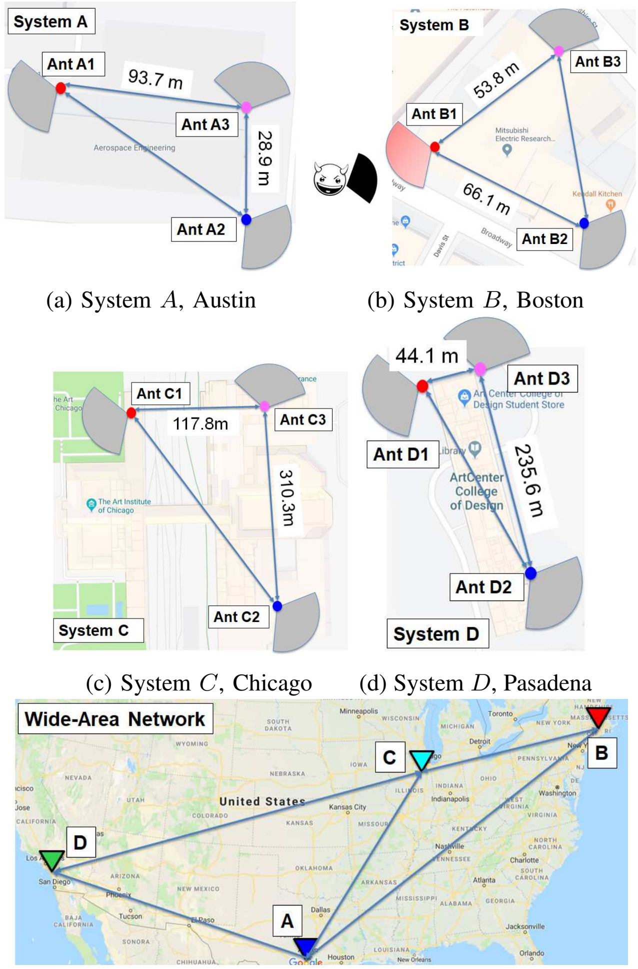
A. Wide-area Experimental Setup

As seen in Fig. 4, we consider four GPS receiving systems, in which the DMDA setup comprises of three antennas. In the wide-area network, we consider the GPS receiving systems to be located in Austin, Boston, Chicago and Pasadena, which are denoted by A, B, C, and D, respectively. We mimicked the setup of an actual power substation by considering the realistic pre-computed baseline vectors across the antennas in each DMDA setup.

We utilized the MATLAB-based two-area Kundur Simulink model [19] to design a wide-area power grid, which consists of four microgrids, denoted by A, B, C, and D, all of which are connected to one common main grid via different critical nodes, as seen in Fig. 5. We trigger each microgrid using the GPS timing estimated via one GPS receiving system each. We monitored the critical nodes at the microgrid and main grid by recording the corresponding phasor measurements using PMU. For example, we measured the PMU data at two buses, namely, AG and AT, which correspond to the Ath critical node connecting the microgrid-A and the main grid.

B. Implementation

The implementation details related to our wide-area network are divided into three stages: simulating the GPS signals, post-processing the collected GPS signals and assessing the voltage stability of the power grid.



(a) System A, Austin

(b) System B, Boston

(c) System C, Chicago

(d) System D, Pasadena

(e) Wide-area network and communication links

Fig. 4: Experiment setup consists of four GPS receiving systems in the wide-area network, with three antenna-based DMDA setup in each. The GPS receiving system in Boston is attacked by simulated meaconing, such that, the $B1$ antenna of the DMDA setup experiences spoofing.

1) *Simulating spoofed GPS signals:*

We simulated the raw GPS signals received at each receiving system using a C++ language-based software-defined GPS simulator known as GPS-SIM-SDR [20]. For a given stationary configuration of the antenna and an associated ephemeris file, the GPS simulator generates the corresponding base-band signal data streams. We collected the simulated GPS signals at a sampling rate of 2.6 MHz, where each raw sample is a 16-bit complex. At each DMDA setup, the corresponding antennas are provided with selective visibility of the sky, such that, the field of view are $150-270°$, $270-30°$, and $30-150°$, respectively, in reference to geographic north.

Utilizing this configuration, we simulated the authentic GPS signals received at each antenna in the three GPS receiving systems, located in Austin, Chicago and Pasadena, as seen in Fig. 4(a), 4(c) and 4(d). Based on the meaconing attack explained in Section I, we generated the spoofed GPS signals at the attacked GPS receiving system in Boston, as seen by red sector of Fig. 4(b), by adding high-powered and simulated malicious samples to the generated authentic GPS samples. Due to the proposed DMDA configuration, as explained in Section III-6, the attacker can only affect $B1$ antenna, thereby, causing it to receive malicious 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 [21]. We utilized the external ephemeris to extract authentic satellite positions, which are provided as input to the BP-EKF algorithm.

3) *Assessing the voltage stability:*

At the critical node connecting the microgrid-B and the main grid, we monitor the bus BG using three PMUs, such that, the timing supplied to one of the PMUs is triggered using the proposed wide-area BP-EKF, the second using single-area BP-EKF and the third via conventional scalar tracking. We monitor the buses AG,CG, and DG at all the other critical nodes using one PMU each, which is triggered using the GPS timing calculated via wide-area BP-EKF. At the lth bus in each of the four microgrids, namely, AG,BG,CG, or DG we analyzed the changes in a metric termed as voltage stability index (VSI) [22], which is given by

$$I_{vs,l} = \frac{\sqrt{b_l^2 - 4a_l c_l}}{a_l}, \tag{16}$$

where $a_l = Q_{\mathrm{Z-load},l} + T_{lj}^2|Y_{lj}|\sin\left(\phi_{lj}\right)$, $b_l = Q_{\mathrm{I-load},l} + T_{lj}E_j|Y_{lj}|\sin\left(\theta_{lj} - \phi_{lj}\right)$ and $c = Q_{\mathrm{P-load},l} - Q_{\mathrm{max},l}$, 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 the buses AT,BT,CT, or DT in the main grid, E_j is voltage magnitude and δ_j is the voltage phase angle and $\theta_{lj} = \delta_l - \delta_j$ 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.

C. *Under simulated meaconing attack*

Between the time duration $t = 0$ - 30 s, we induced a simulated meaconing attack causing a timing delay of 60 μs to the simulated authentic GPS signals received at the Bth GPS receiving system. At the B1 antenna, the attacker causes the pseudoranges corresponding to the 3 expected satellites to show a constant error of 18000 m till $t = 30$ s and later for $t \geq 30$ s these errors continue to grow due to the destabilization of the tracking loops.

As seen in Fig. 6, the conventional scalar tracking with one omni-directional antenna, showed an RMS timing error of 61.83 μs as indicated by the red-dotted line. We observed that the timing error induced by the scalar tracking causes the timing error to grow unbounded with time. However, the proposed BP-EKF algorithm, which is executed for $t >= 12$s, showed steady convergence and demonstrated significantly lower RMS timing errors of 0.16 μs, 0.15 μs 0.14 μs and 0.15 μs at A,B,C, and D GPS receiving systems, respectively,

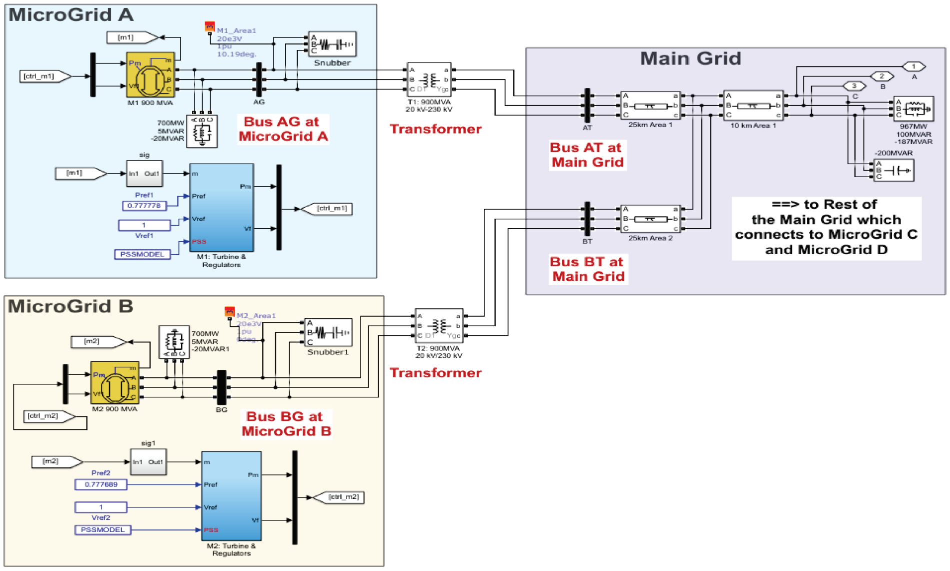


Fig. 5: The simulated grid setup consists of the buses AG,BG,CG, and DG monitor the critical nodes connecting the microgrid A,B,C, and and D to the main grid, respectively. Three PMUs monitor the bus BG, which are triggered using the wide-area BP-EKF, single-area BP-EKF and conventional least squares.

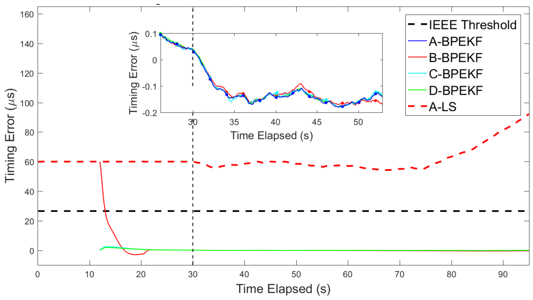


Fig. 6: Timing error estimated using the proposed BP-EKF algorithm, indicated in blue, as compared to conventional scalar tracking, indicated in red.

during the simulated meaconing attack. As seen in Fig. 7, the wide-area BP-EKF algorithm not only isolates the presence of spoofing attacks to B1 antenna but also accurately estimates the corresponding timing error as $\alpha_k^a \approx 60$ μs induced during the spoofing attack, i.e., $t = 0 - 30$ s. This can be observed by the red-solid line at the Bth GPS receiving system whereas the timing error in other antennas is close to zero. Next, based on the VSI metric described in (16), we assessed the stability of critical node connecting microgrid B to the main grid by comparing the performance of three PMUs, triggered via wide-area BP-EKF, as denoted by the magenta-solid line, single-area BP-EKF, as denoted by the black-dotted line and the least squares, as denoted by the red-dotted line. As compared to least squares, we observed an increase in the RMS VSI metric from 0.06 to 1.45 between $t = 12 - 30$ s, using the single-area and wide-area BP-EKF, as seen in Fig. 9. The proposed wide-area BP-EKF algorithm shows quicker convergence as compared to the single-area BP-EKF. Even after spoofing ends, the VSI metric is low < 0.4 for least squares indicating high timing errors, whereas the VSI metric computed via wide-area

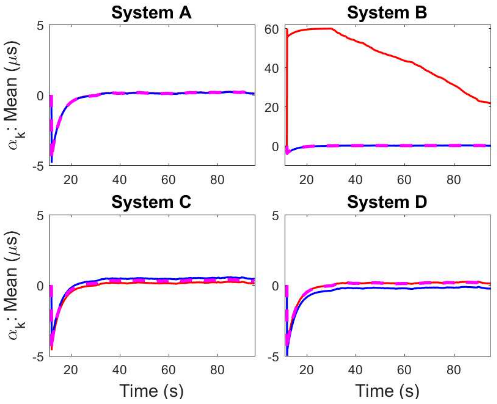


Fig. 7: Antenna-specific timing errors estimated during BP step, in particular its mean μ_1 and variance σ_1^2.

BP-EKF at all the microgrids is high, indicating high voltage stability.

In addition, we also analyzed the spoofing risk associated with each GPS receiving system, based on the KL test statistic described in (15). Considering a pre-determined threshold $\Pi = 10$ and $W = 20$, we observed that test statistics computed for the GPS receiving system A,C, and D fall below the threshold, indicating that they are authentic, whereas the KL test statistic for GPS receiving system B is above the threshold, indicating external attack.

V. Conclusions

We have proposed a wide-area time authentication algorithm using a wide-area network of GPS receiving systems, each comprising of geographically distributed multiple directional antennas. Based on the communication infrastructure of the grid, we have developed a wide-area BP-EKF algorithm to

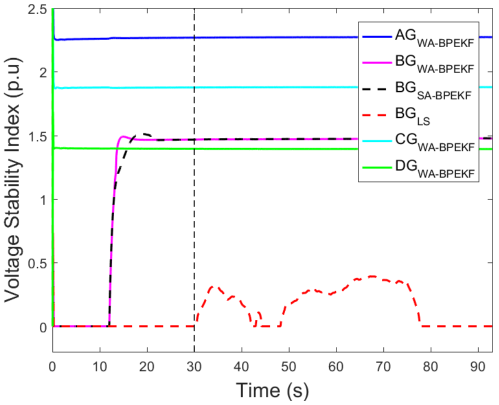


Fig. 8: VSI of the buses at the critical nodes of microgrid A, B, C, and D, of which bus BG being monitoring using three PMUs, triggered via wide-area BP-EKF, single-area BP-EKF and scalar tracking.

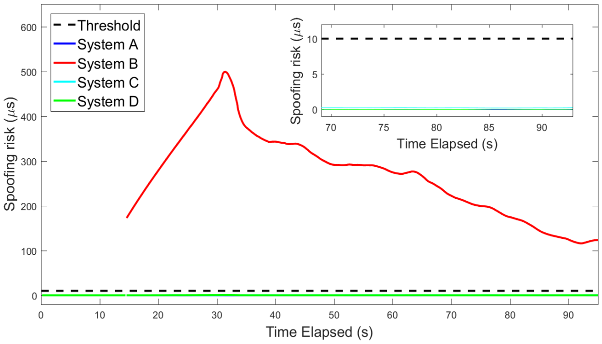


Fig. 9: Spoofing risk obtained via KL-divergence-based test statistic. The test statistics fall below the threshold for GPS receiving systems A, C, and, D indicating that they are authentic, whereas the test statistic for GPS receiving system B is above the threshold, indicating external spoofing attack.

estimate the marginal distribution of spoofing-induced timing errors at each antenna. After then, we have corrected for the pseudoranges which are processed via adaptive EKF to estimate the GPS timing. We have also formulated a KL-divergence-based test statistic to evaluate the reliability of each GPS receiving system.

We have validated the proposed wide-area BP-EKF using four GPS receiving systems, with three-antenna-based DMDA setup each and subjecting one GPS receiving system to a simulated meaconing attack that induces a delay of 60 μs. While one omni-directional antenna-based least squares has shown large RMS timing error of 61.8 μs, the proposed wide-area BP-EKF algorithm demonstrates low RMS timing error of 0.16 μs. We have assessed the voltage stability via the voltage stability index. The conventional least squares shows a low RMS value of 0.06, whereas the proposed BP-EKF is at a high RMS value of 1.45.

References

[1] 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.

[2] 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.

[3] R. Bobba, E. Heine, H. Khurana, and T. Yardley, "Exploring a tiered architecture for naspinet," in *Innovative Smart Grid Technologies (ISGT), 2010*, pp. 1–8, IEEE, 2010.

[4] 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.

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

[6] 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.

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

[8] 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.

[9] S. Gong, Z. Zhang, M. Trinkle, A. D. Dimitrovski, and H. Li, "GPS spoofing based time stamp attack on real time wide area monitoring in smart grid," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pp. 300–305, IEEE, 2012.

[10] K. Fodero, C. Huntley, and D. Whitehead, "Secure, wide-area time synchronization," in *proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA*, 2010.

[11] J. Eidson and K. Lee, "IEEE 1588 standard for a precision clock synchronization protocol for networked measurement and control systems," in *Sensors for Industry Conference, 2002. 2nd ISA/IEEE*, pp. 98–105, Ieee, 2002.

[12] Y. Wang and A. Chakrabortty, "Distributed monitoring of wide-area oscillations in the presence of GPS spoofing attacks," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pp. 1–5, July 2016.

[13] S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," *Position, Location and Navigation Symposium (PLANS), 2018 IEEE/ION*, pp. 1485–1491, 2018.

[14] S. Bhamidipati, K. J. Kim, H. Sun, and P. V. Orlik, "GPS spoofing detection and mitigation in PMUs using distributed multiple directional antennas," in *International Conference on Communications (ICC)*, pp. 1–7, 2019.

[15] P. T. Myrda, J. Taft, and P. Donner, "Recommended approach to a NASPInet architecture," in *System Science (HICSS), 2012 45th Hawaii International Conference on*, pp. 2072–2081, IEEE, 2012.

[16] M. A. Tschopp and E. Hernandez-Rivera, "Quantifying similarity and distance measures for vector-based datasets: Histograms, signals, and probability distribution functions," tech. rep., US Army Research Laboratory Aberdeen Proving Ground United States, 2017.

[17] 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.

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

[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.*

[20] T. Ebinuma, "Gps-sdr-sim," *[Online] Available: https://github.com/osqzss/gps-sdr-sim.*

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

[22] Z. Wang, H. Sun, and D. Nikovski, "Static voltage stability detection using local measurement for microgrids in a power distribution network," in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pp. 3254–3259, IEEE, 2015.