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

Joint BP and RNN for Resilient GPS Timing Against Spoofing Attacks

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

TR2019-036 June 28, 2019

Abstract

In this paper, we propose a new wide-area algorithm to secure the Global Positioning System (GPS) timing from spoofing attack. To achieve a trusted GPS timing, belief propagation (BP), recognized as one of the Artificial Intelligence (AI) approaches, and the recurrent neural network (RNN) are jointly integrated. BP is employed to authenticate each GPS receiving system in the wide-area network from malicious spoofing attacks and estimate the corresponding spoofing-induced timing error. To evaluate the spoofing status at each of the GPS receiving system, RNN is utilized to evaluate similarity in spoofing-induced errors across the antennas within the GPS receiving system. Having applied a proper training stage, simulation results show that the proposed joint BP-RNN algorithms can quickly detect the spoofed receiving system comparing with existing work.

EAI International Conference on Artificial Intelligence for Communications and Networks

Joint BP and RNN for Resilient GPS Timing Against Spoofing Attacks

Sriramya Bhamidipati[1], Kyeong Jin Kim[2], Hongbo Sun[2], Philip Orlik[2], and Jinyun Zhang[2]

[1] University of Illinois at Urbana-Champaign, Urbana, IL, 61801, USA
[2] Mitsubishi Electric Research Labs (MERL), Cambridge, MA, 02139, USA

Abstract. In this paper, we propose a new wide-area algorithm to secure the Global Positioning System (GPS) timing from spoofing attack. To achieve a trusted GPS timing, belief propagation (BP), recognized as one of the Artificial Intelligence (AI) approaches, and the recurrent neural network (RNN) are jointly integrated. BP is employed to authenticate each GPS receiving system in the wide-area network from malicious spoofing attacks and estimate the corresponding spoofing-induced timing error. To evaluate the spoofing status at each of the GPS receiving system, RNN is utilized to evaluate similarity in spoofing-induced errors across the antennas within the GPS receiving system. Having applied a proper training stage, simulation results show that the proposed joint BP-RNN algorithms can quickly detect the spoofed receiving system comparing with existing work.

Keywords— GPS spoofing, Artificial Intelligence, Belief Propagation, and Recurrent Neural Network.

1 Introduction

Now-a-days, Artificial Intelligence (AI) has been emerging as an important tool for revolutionizing different safety-critical infrastructures, such as, banking, electrical grids and communication networks. In electrical grids, AI offers unique solutions [1] to improve the overall grid resilience and localize the power disruptions caused by the increasing complexity of interconnected grids, high power demand and distributed generation with the usage of renewable sources.

AI techniques are already being incorporated in the power plants to increase the production and also by grid operators to optimize the energy consumption [2]. Recently, GE developed an AI related technology [3] for wind turbines in Japan that is expected to lower the overall maintenance costs by 20% and increase the power output by 5%. Similarly, Google's DeepMind is in discussion with the UK's National Grid to develop AI solutions [4] that balance the requirements of supply and demand in Britain. Also, IBM showed an improvement of 30% in solar forecasting while working with the U.S. Department of Energy SunShot Initiative [5].

In addition to efficient energy production and consumption, another critical research area is related to improving the grid resilience against power disruptions that can potentially destabilize the grid [6]. A few notable incidents that occurred in the recent past are the Northeastern blackout in 2003 [7], which is caused due to the shutdown of a

high-voltage power line and power outrage of Ukraine [8] in 2015, which caused by the malicious cyber attacks. Recently, there has been a world-wide effort to modernize the grid, coined as *Smart Grid*, which refers to a fully automated power network that monitors and controls every node as well as ensures a steady flow of electricity and exchange of information [9].

Smart grids utilize the concept of microgrids [10] in power distribution networks, which possess the capability to function both when connected to a traditional grid as well as an independent electrical island. However, unlimited power consumption causes the microgrid to be vulnerable to voltage collapse, which needs to accurately monitored. Therefore, smart grids rely on advanced devices, namely, Phasor Measurement Units (PMUs), which provide better insights into the state of the smart grid and in turn help optimize the grid efficiency. PMUs require precise time-keeping sources, such as GPS, to obtain global timing for synchronization [11]. However, GPS civilian signals are unencrypted and their power is as low as -160 dBW, which makes them vulnerable to external spoofing attacks [12]. Based on the IEEE C37.118.1-2011 standard for synchrophasors [13], in this work, we consider 1% TVE equivalent to a timing error of 26.5 μs, as a benchmark in our power grid stability analysis.

In this paper we mainly focus on a sophisticated type of spoofing attack, known as signal-level spoofing [14]. However, our proposed algorithm is also directly applicable for the detection and mitigation of other spoofing attacks [15]-[16]. One scenario of a sophisticated signal-level spoofing is a three-stage attack during which, a spoofer simulates and broadcasts malicious look-alike GPS signals identical to the authentic signals received at the target receiver and thereafter, increases the power of these malicious signals. Once the target receiver locks onto the malicious signals, the spoofed manipulates the receiver time to deviate slowly from its authentic value. Given there are no abrupt changes in GPS timing, this attack is harder to detect and more dangerous as compared to other attacks.

AI has immense potential to serve as a *automated brain* that can analyzes the GNSS measurements to tackle these malicious spoofing attacks [17]-[18]. In [19], spoofing detection has been performed by computing the wavelet transformation coefficients of both spoofing and authentic signal, which are later fed into support vector machines, the probabilistic neural networks and the decision tree. In our prior work [20], to isolate spoofing attacks, we proposed a geographically Distributed Multiple Directional Antennas (DMDA) setup, with each antenna facing a different part of the sky, thereby, each receiving signals from only a subset of the total visible GPS satellites. In particular, we designed a Belief Propagation (BP)-based Extended Kalman Filter (EKF) algorithm for single power substation that utilizes the proposed DMDA setup to detect timing anomalies caused due to spoofing. Next, in [21], we extended our work to develop a wide-area-based BP-EKF algorithm that reduces the overall sensitivity of the prior distribution of timing error at each antenna.

To improve the resilience of the grid during sophisticated spoofing attacks, we further extend our work to develop an innovative wide-area joint BP and Recurrent Neural Network (RNN) algorithm, which is based on two powerful tools used in the AI community, namely, BP [22] that isolates the timing errors observed at each antenna and RNN [23] that adaptively analyzes the timing errors to authenticate the spoofing status

of each power substation in the wide-area network. Using our joint BP-RNN algorithm, we can not only detect and isolate these malicious attacks but also mitigate the corresponding spoofing-induced timing errors.

2 Joint BP and RNN algorithm

In this section, we first briefly outline the details of our DMDA setup [20] and later explain the proposed wide-area communication structure. Next, we describe the algorithm details of our wide-area joint BP-RNN algorithm.

2.1 DMDA Setup

Several advantages of the employed DMDA setup in [20] are summarized as follows:

- During a spoofing attack, an attacked antenna may see more satellites in its section of the sky than expected, whereas each of the directional antennas in authentic conditions sees the expected number of satellites in its section of the sky.
- Due to a limited height of physical location of a directed attack, all the directional antennas are not in the line of sight from the attacker. Thus, a geographical diversity can be achievable from malicious spoofing attacks.
- All the antennas are triggered by the same clock, so that a metric, which distinguish an authentic condition from a non-authentic spoofing condition, can be developed.

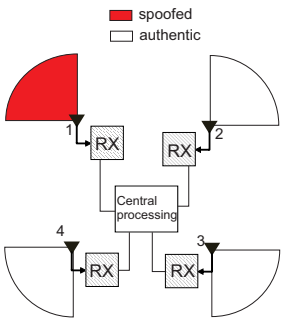


Fig. 1: Configuration of the DMDA setup [20]. Each directional antenna is provided with selective visibility by pointing it towards a different section of the sky, such that, not all the directional antennas can be spoofed simultaneously. Sector of circle represents the field-of-view of each antenna.

2.2 Proposed wide-area communication structure

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. We assume the system configuration as follows:

- Any ath infrastructure, with $\forall a \in \{1, \cdots, N\}$, is equipped with a single DMDA based GPS receiving system that includes a common clock and a DMDA setup composed of M_a antennas. For the ath infrastructure, we define $\mathcal{S}_a$ as the set of *neighboring infrastructures*. Note that bth infrastructure is included in $\mathcal{S}_a$ only when a communication link, π_{ab}, between ath and bth infrastructure exists, that is, $b \in \mathcal{S}_a,$ if $\pi_{ab} = 1, \forall b \in \{1, \cdots, N\},\ b \neq a$.
- For any kth antenna in the ath receiving system, with $k \in \{1, \cdots, M_a\}$, its *neighboring antennas* $\mathcal{B}_k^a$ represents the set of antennas in its infrastructure excluding itself, as well as the antennas belong to its neighboring infrastructures $\mathcal{S}_a$,

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

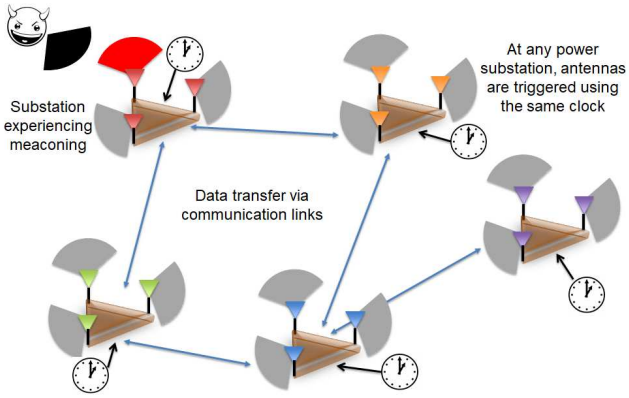


Fig. 2: Wide-area network of GPS receiving systems, each equipped with a common clock and a DMDA setup.

The overall framework of the proposed wide-area joint BP-RNN algorithm, illustrated Fig. 3, is described as follows:

- Across the infrastructures, pseudoranges are measured at each directional antenna, in each of the receiving systems. Based on the communication structure, the *system data* is exchanged across the receiving systems.
- At each of the receiving systems, we form $\mathcal{B}_k^a$. Then, we compute the *single difference pseudorange residual vector* by considering one satellite visible to the first antenna and the another satellite visible to the second antenna in $\mathcal{B}_k^a$.
- At each antenna, *belief* is computed according to the marginal Gaussian distribution of the antenna-specific timing error.
- Using the BP estimates of antenna-specific timing errors, at each GPS receiving system, the pseudoranges are corrected, which are utilized by EKF in the CP unit. The CP unit provides the trustworthy GPS timing, which is given to the infrastructures for a time synchronization.

– A Bidirectional LSTM-based RNN [24] utilizes the BP estimates of the antenna-specific timing errors to compute a test statistic, which authenticates the spoofing status of each GPS receiving system.

Across the wide-area network, by implementing a distributed architecture, it is possible to efficiently utilize the already in-place communication platform. Highly computational extensive calculation of marginal distribution is simplified through the distributed AI algorithm, namely, BP. BP plays a pivotal role in maintaining accuracy while reducing the latency involved in spoofing detection, which is critical for timing-related applications. Our wide-area algorithm can be easily scaled to any number of GPS receiving systems and any number of directional antennas within the GPS receiving system. 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. Similarly, by utilizing a BP-RNN framework, it is possible to adaptively analyze the antenna-specific timing errors to quickly detect different kinds of spoofing attacks, ranging from easy-to-execute meaconing to sophisticated signal-level spoofing attack.

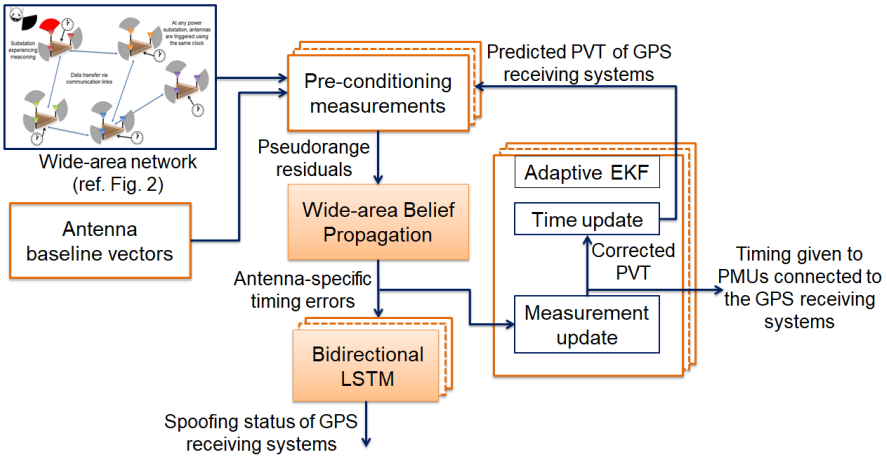


Fig. 3: Flowchart of the wide-area joint BP-RNN algorithm.

2.3 Detailed Descriptions of the Proposed Algorithm

By utilizing the GPS signals received at multiple infrastructures geographically distributed, we describe the proposed wide-area joint BP-RNN algorithm as follows:

Pre-conditioning the GPS measurements

Considering a wide-area network of N GPS receiving systems, the baseline vectors between the antennas installed at the ath receiving system are computed as $\boldsymbol{b}^a_{kn}$, $k, n \in$

$\{1, \ldots, M_a\}$. The three-dimensional (3D) position and 3D velocity of the kth antenna at tth time are respectively defined as $\boldsymbol{x}_{k,t}^a \triangleq [x, y, z]_k$ and $\boldsymbol{v}_{k,t}^a \triangleq [\dot{x}, \dot{y}, \dot{z}]_k$. At the ath receiving system, the pseudorange observed at the kth antenna corresponding to the ith satellite is given by

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

where $i \in L_{k,t}$ denotes the ith satellite among the $L_{k,t}$ visible satellites at the kth antenna in the ath receiving system. In addition, $\boldsymbol{y}_t^i$ and $c\delta t^i$ respectively denote the 3D position and clock corrections of the ith visible satellite. Note that since all the antennas installed at the ath receiving system is triggered by the same clock, the clock bias, $c\delta t_t^a$, is independent of k. The antenna-specific timing errors in pseudorange are denoted by α_k^a. For a proper processing, the antenna, specified by $k = 1$, is recognized as the reference antenna. Furthermore, $h_k^a(\cdot, \cdot, \cdot)$ denotes the measurement model of the kth antenna of the ath receiving system, which depends on the reference antenna's 3D position, $\boldsymbol{x}_{1,t}^a$, receiver clock bias, $c\delta t_t^a$, 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 [25]. The additive Gaussian white noise in the satellite measurements is represented by ω_k^i.

Having utilized the predicted state vector $\hat{\boldsymbol{\beta}}_t^a \triangleq [\hat{\boldsymbol{x}}_1, c\delta\hat{t}, \hat{\boldsymbol{v}}_1, c\delta\dot{\hat{t}}]_t^T$ obtained from the EKF time update at time t, the known baseline vector, $\boldsymbol{b}_{1k}^a$, with respect to the reference antenna, the satellite 3D position, $\boldsymbol{y}_t^i$, and clock corrections, $c\delta t^i$, the pseudorange residuals at tth time can be computed as follows:

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

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

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, pseudorange residuals, $\Delta\rho_{k,t}^i$, and beliefs at the kth antenna of the receiving system, $b_{t-1}(\alpha_k^a)$. At the ath receiving system, we collect 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, $k \in \{1, \cdots, M_a\}$, and the second antenna, $n \in \mathcal{B}_k^a$. After then, the single difference pseudorange residuals between the ith satellite visible to the kth antenna and that of the jth satellite visible to the nth antenna as follows:

$$\begin{aligned} \gamma_{kn,t}^{ij} &\triangleq \Delta\rho_{k,t}^i - \Delta\rho_{n,t}^j \\ &= \alpha_k^a - \alpha_n^b + \omega_{kn}^{ij} \\ &= \begin{cases} 0 & k, n \in \{1, \ldots, M_a\},\ k \neq n \\ \eta_{ab} & k \in \{1, \ldots, M_a\},\ n \in \{1, \ldots, M_b\}, a \neq b, \end{cases} \end{aligned} \tag{3}$$

where in authentic conditions, $\gamma_{kn}^{ij} \approx 0$ across any two antennas that belong to the same receiving system. However, across antennas that belong to two different receiving systems, that is, $a \neq b$, γ_{kn}^{ij} is a non-zero value η_{ab} due to the error in predicted clock bias estimates and the receiver noise. Thereafter, we calculate the measurement metric vector, denoted by $\boldsymbol{\gamma}_{kn,t} \stackrel{\triangle}{=} \{\gamma_{kn,t}^{ij}, i \in L_{k,t}, j \in L_{n,t}\}$ 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

$$p(\boldsymbol{\gamma}_{kn,t}|\alpha_k^a, \alpha_n^b) = \frac{1}{\sqrt{(2\pi\nu^2)^{L_{k,t}L_{n,t}}}} \exp\left\{\frac{-L_{k,t}L_{n,t}}{2\nu_{kn}^2}\left(\frac{\mathbf{1}^T\boldsymbol{\gamma}_{kn,t}}{L_{k,t}L_{n,t}} + (\alpha_k^a - \alpha_n^b)\right)^2\right\} \forall\, n \in \mathcal{B}_k^a, \quad (4)$$

where ν_{kn}^2 denotes the measurement variance of the summation of single difference residual components which comprises errors observed from pseudoranges, and errors in satellite ephemeris, predicted position and velocity of the antenna.

Belief Propagation (BP)

To authenticate each receiving system against spoofing attacks and estimate the corresponding spoofing-induced timing errors at each antenna, the marginal distribution using a factor graph-based BP framework is used as an AI approach. BP [22] is a sum-product message passing algorithm to make inferences on graphical models, such as the factor graphs. Factor graph is a probabilistic graphical model [26], 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. At the ath receiving system, given the joint posterior distribution, $p(\alpha_1, \ldots, \alpha_{M_a}|\boldsymbol{\gamma}_{kn})$, the marginal distribution, $g(\cdot)$, is formulated as follows:

$$g(\alpha_k^a) = \int_{\alpha_1^a,\ldots,\alpha_{k-1}^a} \int_{\alpha_{k+1}^a,\ldots,\alpha_M^a} p(\alpha_1^a, \ldots, \alpha_{M_a}^a|\{\boldsymbol{\gamma}_{kn}\}_{k=1,\ldots,M_a, n\in\mathcal{B}_k^a}) \, d\alpha_1^a \ldots d\alpha_{k-1}^a \, d\alpha_{k+1}^a \ldots d\alpha_{M_a}^a, \quad (5)$$

where $\mathcal{B}_k^a$ denotes the neighboring antennas of the kth antenna in the ath receiving system. With an increased total number of antennas, that is, $\sum_{a=1}^{N} M_a$ in the wide-area network, (5) becomes computationally intractable. Thus, a factor graph-based BP is formulated to approximate the marginal distribution in a computationally-efficient manner, which is termed as belief, $b_t(\alpha_k^a)$. Belief at the kth antenna, $b_t(\alpha_k^a)$, is computed as the product of its prior distribution and all the incoming messages from all the neighboring antennas $\mathcal{B}_k^a$. Given that the attacker transmits counterfeit GPS signals, the corresponding spoofing-induced timing errors follow a Gaussian distribution $\mathcal{N}(:,\cdot,\cdot)$. Therefore, belief can be represented by Gaussian process [27] with mean, $\mu_{k,t}^a$, and variance, $(\sigma_{k,t}^a)^2$, as follows:

$$\begin{aligned} b_t(\alpha_k^a) &= m_{f_k^a \to \alpha_k^a} \prod_{n\in\mathcal{B}_k^a} m_{f_{kn}^a \to \alpha_k^a}(\alpha_k^a), \\ &= \mathcal{N}\Big(\alpha_k^a : \mu_{k,t}^a, (\sigma_{k,t}^a)^2\Big), \end{aligned} \quad (6)$$

where the factor node, f^a_{kn}, connects two variable nodes, α^a_k and α^b_n, based on the likelihood probability, $p(\boldsymbol{\gamma}_{kn}|\alpha^a_k, \alpha^b_n)$, and the other factor node, f^a_k, connects to its corresponding variable node, α^a_k, and indicates the prior distribution of α^a_k.

As seen from (6), at the kth antenna of the ath receiving system, belief, $b_t(\alpha^a_k)$, is updated by computing two kinds of messages, namely, measurement-related messages, $m_{f^a_{kn}\to\alpha^a_k}$, and prior-related message, $m_{f^a_k\to\alpha^a_k}$, as follows:

– The message, $m_{f^a_{kn}\to\alpha^a_k}$, is based on the factor node, f^a_{kn}, and represents the belief of the nth neighboring antenna, $n \in \mathcal{B}^a_k$, on the variable node, α^a_k. From (4) and (6), we derive the message, $m_{f^a_{kn}\to\alpha^a_k}$, as follows:

$$\begin{aligned} m_{f^a_{kn}\to\alpha^a_k}(\alpha^a_k) &= \int_{n\in\mathcal{B}^a_k} p(\boldsymbol{\gamma}_{kn}|\alpha^a_k, \alpha^b_n)\, b_{t-1}(\alpha^b_n) d\alpha^b_n, \\ &= \int \frac{1}{\sqrt{(2\pi\nu^2)^{L_k L_n}}} \exp\left\{ \frac{-L_k L_n}{2\nu^2} \left(\frac{\mathbf{1}^T \boldsymbol{\gamma}_{kn,t}}{L_k L_n} - (\alpha^a_k - \alpha^b_n) \right)^2 \right\} \\ &\quad \exp\left\{ \frac{-(\alpha^b_n - \mu^b_{n,t-1})^2}{2(\sigma^b_{n,t-1})^2} \right\} d\alpha^b_n, \\ &= \mathcal{N}\Big(\alpha^a_k : \mu^a_{kn,t},\, (\sigma^a_{kn,t})^2\Big), \end{aligned} \tag{7}$$

where $\mu^a_{kn,t} = \mu^b_{n,t-1} - \dfrac{\mathbf{1}^T \boldsymbol{\gamma}_{kn,t}}{L_{k,t} L_{n,t}}$ and $(\sigma^a_{kn,t})^2 = \dfrac{\nu^2_{kn}}{2L_{k,t}L_{n,t}} + (\sigma^a_{n,t-1})^2$.

– The message, $m_{f^a_k\to\alpha^a_k}$, represents the prior distribution formulated as a Gaussian; that is,

$$m_{f^a_k\to\alpha^a_k} = p(\alpha^a_k) \int b(\alpha^a_k) d\alpha^a_k = p(\alpha^a_k) = \mathcal{N}\Big(\alpha^a_k : \mu^a_{pk,t}, (\sigma^a_{pk,t})^2\Big). \tag{8}$$

Based on (7) and (8), the updated belief at time instant t is computed as follows:

$$\begin{aligned} b_t(\alpha^a_k) &= \mathcal{N}\Big(\alpha^a_k : \mu^a_{pk,t}, (\sigma^a_{pk,t})^2\Big) \prod_{n\in\mathcal{B}^a_k} \mathcal{N}\Big(\alpha^a_k : \mu^a_{kn,t}, (\sigma^a_{kn,t})^2\Big), \\ &= \mathcal{N}\Big(\alpha^a_k : \mu^a_{k,t}, (\sigma^a_{k,t})^2\Big), \end{aligned} \tag{9}$$

where

$$\begin{aligned} (\sigma^a_{k,t})^2 &= \left(\frac{1}{(\sigma^a_{pk,t})^2} + \sum_{n\in\mathcal{B}^a_k} \frac{1}{(\sigma^a_{kn,t})^2} \right)^{-1}, \text{ and} \\ \mu^a_{k,t} &= (\sigma^a_{k,t})^2 \left(\frac{\mu^a_{pk,t}}{(\sigma^a_{pk,t})^2} + \sum_{n\in\mathcal{B}^a_k} \frac{\mu^a_{kn,t}}{(\sigma^a_{kn,t})^2} \right). \end{aligned} \tag{10}$$

Dependency of wide-area BP on prior distribution

Note that (8) specifies the prior distribution of the antenna-specific timing error. In

our prior work [20], if the mismatch between the observed and the expected set of satellites is ≥ 2, then we assumed that $\mu^a_{pk,t} = 0$ and $(\sigma^a_{pk,t})^2 = \infty$, 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 infrastructures, we choose the GPS receiving system with the least spoofing risk, that is,

$$a_m = \underset{a\in\{1,\cdots,N\}}{\arg\min}\ r^a_t,$$

where $r^a_t, \forall a \in \{1, \cdots, N\}$, is computed later in Section 2.3. Except the a_mth receiving system, we assign the prior distribution of GPS receiving system, such that, $\mu^a_{pk,t} = 0$ and $(\sigma^a_{pk,t})^2 = \infty, \forall a \in \{1, \cdots, N\} - a_m$. However, for the a_mth receiving system, $\mu_{pk,t}$ and $\sigma^2_{pk,t}$ are computed from the empirical distribution calculated on-the fly by considering the most recent W timing errors; that is, $\alpha^{a_m}_{k,t-W:t}, \forall k = \{1, \cdots, M\}$.

RNN-based authentication of GPS receiving systems

Based on the belief estimates of the timing error at each antenna, we design an AI-based RNN framework to authenticate each GPS receiving system in the wide-area network. To evaluate the spoofing status 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. By utilizing the vast amounts of available GPS data, we initially train a coarse RNN-based framework offline that we later finely train during the initialization stage, to adaptively estimate the spoofing status of each ath receiving system, which is denoted by $r^a_t \in \{0, 1\}$, such that, 0 indicates authentic and 1 indicates spoofed.

The architecture of our RNN framework is such that, at any time instant, the shape of the input features $\theta^a_t \triangleq [\alpha^a_1, \cdots, \alpha^a_{M_a}]^T_t$ is a $M_a \times 1$ vector that stacks the estimated antenna-specific timing errors across all antennas in each ath receiving system. This captures the spatial similarity in the antenna-specific timing errors. We also consider multiple time instants of input features as input to our RNN, so as to capture the temporal variations in the absolute values of these input features. In particular, we utilize Long Short Term Memory (LSTM) [24], a special kind of RNN, for training our data, given its capability to retain the information learned from long time sequences. This is especially useful during signal-level spoofing attacks, described in Section 1, where the rate of change in timing errors are not abrupt but increases gradually over time. The overall architecture of our multivariate time-series-based Bidirectional-LSTM [28], as seen in Fig. 4, consists of an input layer, forward layer, backward layer, activation layer and finally an output layer. In the input layer, we consider W^a time instants of *input nodes* denoted by $\theta_{t-W^a:t}$. In the output layer, we consider one *output node* at each instant, which either takes the value 0 or 1, thereby indicating the spoofing status r^a_t of the ath receiving system. The input to the final output layer is obtained by combining the outputs from the forward and backward layers in a activation layer, which is governed by a softmax function [29].

The forward and backward layers are comprised of *LSTM units*, which consists of a *cell* that analyzes the dependencies between elements in our multivariate time sequence.

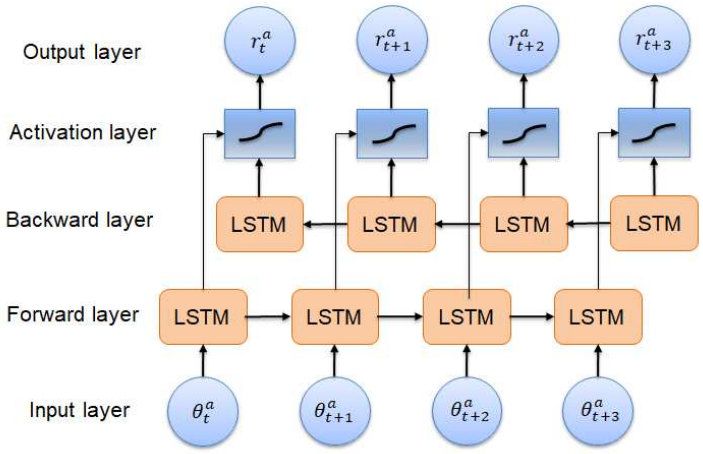


Fig. 4: Overall architecture of our Bidirectional-LSTM, which takes the antenna-specific timing errors of all antennas within the ath GPS receiving system, denoted by θ_t^a and estimates the spoofing status, denoted by r_t^a.

Within each cell, we consider regulators called *gates*, which control the information that is passed through the LSTM unit. The equations related to the processing within each LSTM unit are provided in (11). Our LSTM network utilizes three kinds of gates: an input gate, an output gate, and a forget gate. The input gate controls the extent to which a new value flows into the cell, the forget gate controls the extent to which a value remains in the cell and the output gate controls the extent to which the value in the cell is used to compute the output activation of the LSTM unit. We implement a logistic activation function [30], denoted by σ_g at each gate. The associated unknown weights and biases at these connections are estimated during the training stage.

$$\begin{aligned} f_t &= \sigma_g\left(W_f\theta_t^a + U_f h_{t-1} + b_f\right), \\ i_t &= \sigma_g\left(W_i\theta_t^a + U_i h_{t-1} + b_i\right), \\ o_t &= \sigma_g\left(W_o\theta_t^a + U_o h_{t-1} + b_o\right), \\ c_t &= f_t \circ c_{t-1} + i_t \circ \sigma_c\left(W_c\theta_t^a + U_c h_{t-1} + b_c\right), \text{ and} \\ h_t &= o_t \circ \sigma_h\left(c_t\right), \end{aligned} \tag{11}$$

where θ_t^a denotes the input feature at tth time instant given as an input to the LSTM network, h_t denotes the hidden state vector, and c_t denotes the cell state vector. Similarly, f_t, i_t, o_t denotes the activation vector associated with the forget gate, input gate and output gate, respectively. As mentioned above, W_f, W_i, W_o, U_f, U_i, U_o, b_f, b_i, b_o represents the weights and biases in different layers indicated by their subscripts, and are estimated during the training stage.

During our training stage, considering same number of antennas in each GPS receiving system, we utilize the antenna-specific timing errors obtained from different GPS receiving systems to train our coarse Bidirectional-LSTM network. Using a GPS

simulator, we generate various cases of authentic and simulated spoofing attacks. Thereafter, during an initialization, by processing several minutes of received data, we further finely train our Bidirectional-LSTM network to account for the individual GPS receiving system-based noise distribution related to timing.

Adaptive EKF

According to [20], we summarize the adaptive EKF as follows:

- Define corrected psedoranges: $\boldsymbol{\zeta}_t^a \triangleq [\rho_c^1, \ldots, \rho_c^{L_a}],\ \forall a$, with $\rho_c^i \triangleq \rho_k^i - \alpha_k^a$ and $L^a \triangleq L_1 + \cdots + L_{M_a}$.
- Define required quantities: the measurement noise covariance matrix, $\boldsymbol{R}_t^a$, measurement model, $\boldsymbol{H}_t^a$, predicted state vector, $\hat{\boldsymbol{\beta}}^a$, predicted state covariance matrix, $\hat{\boldsymbol{P}}_t^a$, state transition matrix, $\boldsymbol{F}$, and static process noise covariance, $\boldsymbol{Q}_t^a$.
- Perform measurement update:

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

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

  where $\boldsymbol{K}_t$ represents the Kalman gain and $\boldsymbol{I}_8$ denotes the 8×8 identity matrix. According to [31], a forgetting factor fixed by $d = 0.3$.
- Perform time update:

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

  where

$$\boldsymbol{F} = \begin{bmatrix} \boldsymbol{I}_4 & \delta t \boldsymbol{I}_4 \\ \boldsymbol{0}_{4\times 4} & \boldsymbol{I}_4 \end{bmatrix}, \boldsymbol{Q}_t^a = \boldsymbol{F} \begin{bmatrix} \boldsymbol{0}_{4\times 4} & \delta t \boldsymbol{I}_4 \\ \boldsymbol{0}_{4\times 4} & \boldsymbol{\kappa}^a \end{bmatrix} \boldsymbol{F}^T,\ \text{and}\ \boldsymbol{\kappa}^a = \begin{bmatrix} \boldsymbol{0}_{3\times 3} & 0 \\ 0 & c\tau^a \end{bmatrix}$$

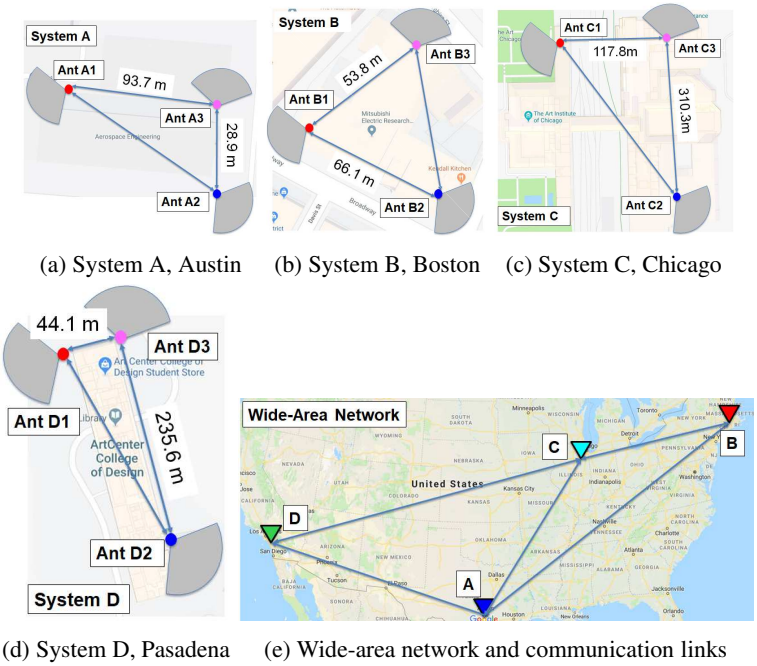
  with τ^a representing allan deviation of the front-end oscillator, δt representing the update interval of our adaptive EKF step, $\boldsymbol{I}_4$ denotes the identity matrix of size 4×4 and $\boldsymbol{0}_{4\times 4}$ denotes the zero matrix of size 4×4.

3 Experiments

In this section, we validate our wide-area joint BP-RNN algorithm via two experimental scenarios, to detect and mitigate the timing error caused by simulated signal-level spoofing attacks. We demonstrate the capability of our BP algorithm to accurately estimate the associated timing errors and our RNN-framework to adaptively authenticate the spoofing status of the GPS receiving systems in the wide-area network.

3.1 Experimental setup and implementation details

As seen in Fig. 5, we consider four GPS receiving systems, such that, the DMDA setup in each GPS receiving system comprises of three antennas. In our wide-area network, we consider the GPS receiving systems to be located in Austin, Boston, Chicago, and Pasadena, denoted by A,B,C, and D, respectively. We considered realistic pre-computed baseline vectors across the antennas in each DMDA setup, marked in the Fig. 5, to mimic the setup of actual power substations.



(a) System A, Austin (b) System B, Boston (c) System C, Chicago

(d) System D, Pasadena (e) Wide-area network and communication links

Fig. 5: The simulated experimental setup consists of four GPS receiving systems in the wide-area network, with three antenna-based DMDA setup in each. In the first experiment case, the GPS receiving system in Boston is attacked by simulated signal-level spoofing, such that, the B1 antenna of the DMDA setup experiences spoofing. In the second experiment case, the GPS receiving station in Pasadena is attacked by a different simulated signal-level spoofing, during which the D3 antenna is affected.

For a given stationary configuration of the antenna and an associated ephemeris file, we simulated the GPS signals received at each antenna and at each receiving system, using a C++-based software-defined GPS simulator known as GPS-SIM-SDR [32]. We collected the simulated GPS signals at a sampling rate of 2.5MHz, 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 $150-270^{\circ}$, $270-30^{\circ}$, and $30-150^{\circ}$, respectively, in reference to geographic north.

Utilizing this setup, we simulated the authentic GPS signals received at each antenna in the three GPS receiving systems, i.e., Austin, Chicago, and Pasadena for the first experiment and Austin, Boston, and Chicago for the second experiment. Based on the signal-level spoofing attack explained in Section 1, we generated the spoofed GPS signals at the attacked GPS receiving system, i.e., Boston for the first experiment and Pasadena for the second experiment, by adding high-powered and simulated malicious samples to the generated authentic simulated GPS samples. We post-processed the simulated GPS signals using a MATLAB-based software-defined radio known as SoftGNSS [33]. We utilized the external ephemeris to extract authentic satellite positions, which are provided as input to the algorithm.

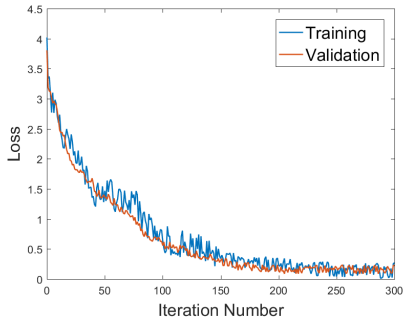


Fig. 6: Loss function obtained for training and validation of Bidirectional-LSTM, which consists of 50 hidden nodes and a batch size of 1028.

Hyper-parameters			**Accuracy (%)**	
Hidden nodes	**Batch size**	**Iterations**	**Training**	**Validation**
50	**1028**	**300**	**83.4**	**84.1**
100	1028	300	76.9	71.3
50	512	300	72.6	73.7

Table 1: Training and validation accuracy for different hyper-parameter settings

For training and validating our Bidirectional-LSTM, we considered 1000000 data samples of input features, that is, antenna specific timing error-based vector $\theta_t^a, \forall a$, obtained from different GPS receiving systems. Out of the 1000000 data samples of input features considered, 99% of the data is used for training our Bidirectional-LSTM, while rest is used for validating the neural network at the end of each epoch. The total considered data samples consists of 65% authentic data, which is obtained from real-world GPS signals collected using a GPS receiver as well as simulated GPS signals obtained from a GPS simulator. In addition, rest of the 40% of the training data comprises of simulated GPS signals affected by different configurations and types of simulated spoofing

attacks. We executed back propagation by considering the cost function to be mean squared error and utilized an Adam optimizer [34]. We considered $W^a = 60, \forall a$ time instants of the past antenna-specific timing errors at each ath GPS receiving system to estimate the spoofing status r_t^a at each time instant. Based on the training and validation accuracy for different hyper-parameter settings, as seen in Table 1, during testing, we utilize our trained RNN that is initialized with 50 hidden nodes and a batch size of 1028. The training and validating loss for the chosen hyper-parameters is seen in Fig. 6.

3.2 Under simulated signal-level spoofing attack

In the simulated authentic GPS signals received at the Bth GPS receiving system, during the time duration $t = 25$ - 60s we induced simulated signal-level spoofing that causes an increasing timing error from 0 - 28μs in a span of 35s. Due to the DMDA configuration at the GPS receiving system, the attacker can only affect B1 antenna, thereby, causing it to receive malicious GPS signals from 9 satellites instead of the expected 3 satellites. At the B1 antenna, the attacker causes the pseudoranges to show an increasing time error during $t = 25$ - 60s. For $t \geq 60$s these errors further continue to grow due to the destabilization of receiver tracking loops.

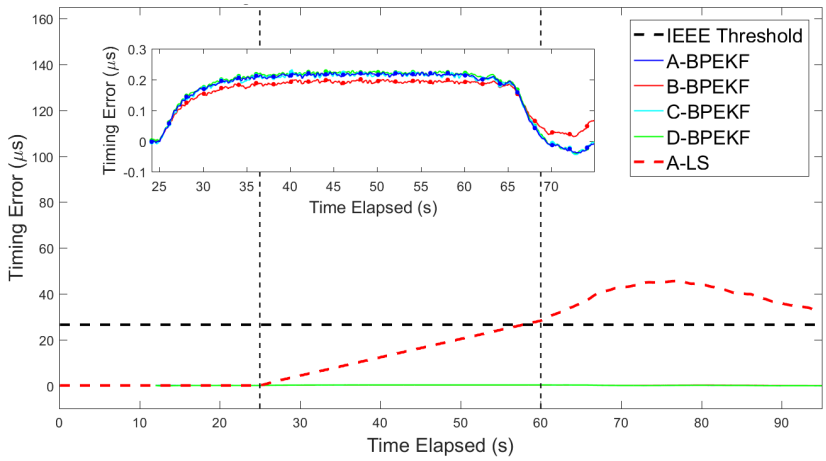


Fig. 7: Timing error estimated using our wide-area joint BP-RNN algorithm, indicated by dotted-solid line, as compared to least-squares, indicated by the dashed line.

As seen in Fig. 7, the conventional least-squares approach with one omni-directional antenna, showed an RMS timing error of 29.8μs as indicated by the red-dashed line. After the spoofing starts at $t = 25$s, we observed that the timing error computed via least-squares increases with time, even after spoofing ends, thereby, exceeding beyond 26.5μs and violating the IEEE C37.118-1 standards. However, our proposed joint BP and RNN algorithm, which is executed for $t \geq 12$s, showed steady convergence and demonstrated

significantly lower RMS timing errors of 0.13μs, 0.14μs, 0.13μs and 0.13μs at A,B,C, and D GPS receiving systems, respectively, during the simulated signal-level spoofing.

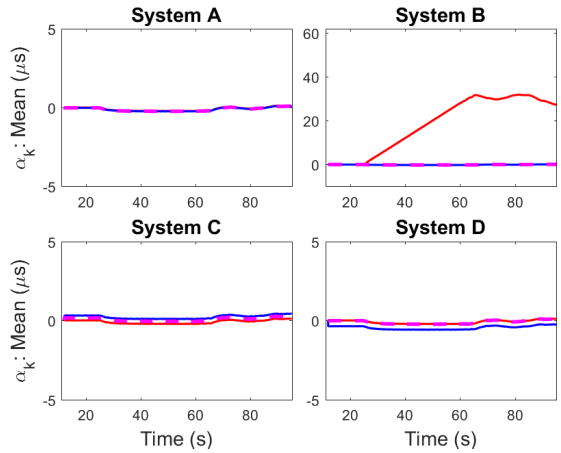


Fig. 8: Antenna-specific timing errors μ_k^a estimated during BP step at all the GPS receiving systems. The different antennas in the DMDA setup of each receiving system are indicated by red, blue and magenta lines.

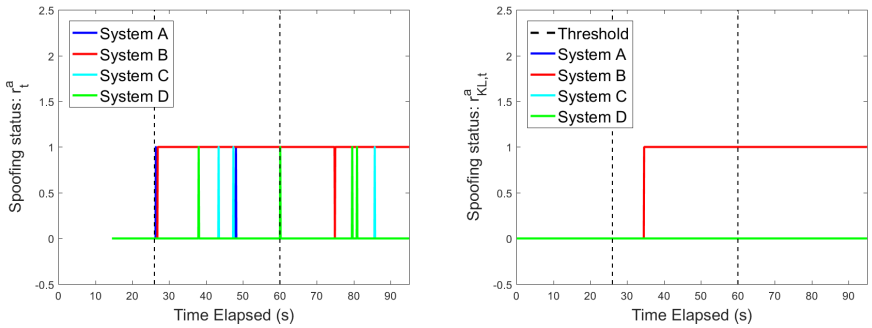
As seen in Fig. 8, the wide-area BP-RNN algorithm not only isolates the presence of spoofing attacks to B1 antenna but also accurately estimates the increasing timing error as $\alpha_{k,t}^a$ - $\alpha_{k,t-1}^a \approx 0.4\mu$s/s induced during the spoofing attack, that is, $t = 25 - 60$s. This can be observed by the red solid line at the Bth GPS receiving system whereas the timing error in other antennas is close to zero.

In addition, we also analyzed the spoofing status associated with each GPS receiving system, based on the Bidirectional-LSTM. We compared the performance of our RNN approach, seen in Fig. 9(a) with that of a KL-divergence approach [35], seen in Fig. 9(b) with pre-determined threshold manually set as $\mathit{\Pi} = 25$. When the KL-test statistic $m_{KL,t}^a > \mathit{\Pi}$, the KL-based metric $r_{KL,t}^a = 1$ indicating spoofed GPS receiving system and $r_{KL,t}^a = 0$ otherwise, indicating authentic conditions. The KL-test statistics, $m_{KL,t}^a$, are calculated as follows:

$$m_{KL,t}^a = \sum_{\nu=0}^{W} \sum_{i=1}^{M_a} \sum_{j=1, j\neq i}^{M_a} \left(\alpha_{i,t-\nu}^a \ln \left(\frac{\alpha_{i,t-\nu}^a}{\alpha_{j,t-\nu}^a} \right) \right). \tag{14}$$

In Fig. 9, we observed that while demonstrating similar consistency in performance as that of the KL-divergence-based metric, our RNN-based metric quickly detects that the Bth receiving system is being spoofed at $t = 25.7$s, that is, 0.7s after the spoofing starts, as compared to the KL-based metric that first detects spoofing at a later time $t = 34.6$s. Therefore, even though the simulated signal-level spoofing does not cause abrupt changes in the timing errors, by analyzing the multivariate time-series of

antenna-specific timing errors, our trained RNN-based metric quickly as well as accurately detects spoofing attacks at the Bth GPS receiving system.



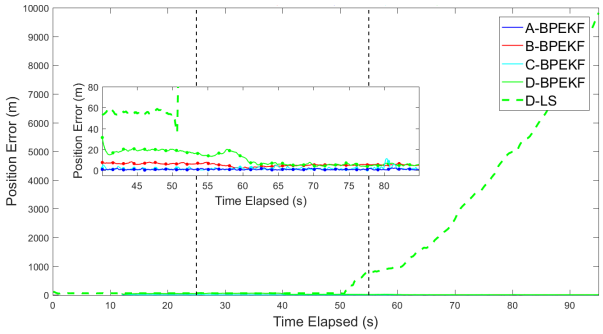
(a) RNN-based metric (b) KL-based metric

Fig. 9: Spoofing status estimated using (a) RNN-based metric; (b) KL-based metric. RNN-based metric detects the presence of spoofing at the Bth receiving system 0.7 s after the spoofing starts at $t = 25$ s, whereas KL-divergence first detects spoofing 9.6 s after the spoofing starts.

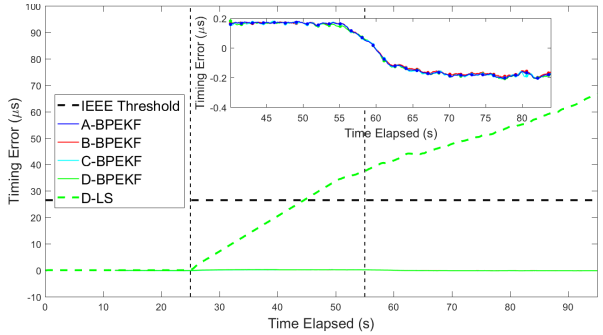
3.3 Under simulated coordinated spoofing attack

In the next set of experiments, we generated a simulated signal-level spoofing attack that induces both a constant change in position of 55m and an increasing timing error of 33μs in a span of 25s. During a time duration of $t = 25$ - 50s, these simulated spoofing signals are added to the simulated authentic GPS signals received at the Dth GPS receiving system are induced with spoofing signals. Due to our DMDA setup, the attacker only successfully spoofs the satellite signals received at the D3 antenna. Similar to Section 3.2, due to the destabilization of receiver tracking loops caused during the attack, the pseudorange errors continue to grow unbounded.

Due to unbounded increase in pseudorange errors, the error in both position and timing obtained via conventional least-squares approach diverged, which is indicated by the green dashed line in the Fig. 10(a) and Fig. 10(b), respectively. In particular, we observed that the IEEE C37.118-1 standards related to the timing error obtained via least-squares approach is violated within 10 s after the start of spoofing attack. However, as seen in Fig. 10(b), our proposed joint BP and RNN algorithm, which is initialized at $t = 12$s, similar to the Section 3.2, showed a convergence trend with RMS timing errors of 0.14μs, 0.16μs, 0.15μs and 0.15μs at A, B, C, and Dth GPS receiving systems respectively. Similarly, as seen in Fig. 10(a), the RMS position errors computed using BP-RNN algorithm are 5.11m, 19.28m, 1.38m, 0.77m at A, B, C, and Dth GPS receiving systems, respectively, whereas least-squares approach showed an RMS position error of 2410.71m.



(a) Position error



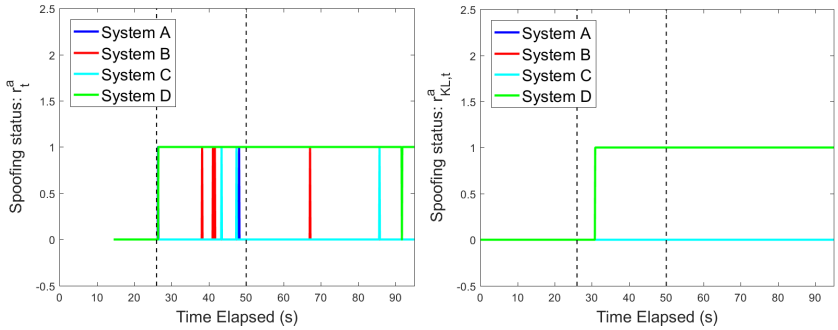
(b) Timing error

Fig. 10: Position and timing errors estimated using the proposed wide-area joint BP-RNN algorithm, indicated by the dotted-solid lines, as compared to the conventional least squares approach, indicated by the dashed line. In particular, green represents the Dth GPS receiving system. Due to spoofing, the least squares solution in both position and timing diverged, whereas our wide-area BP-RNN showed steady convergence.

Based on the Bidirectional LSTM, explained in Section 3.1, we analyzed the spoofing status computed using our BP-RNN algorithm, as seen in Fig. 11(a) and compared its performance with that of the KL-divergence approach, as seen in Fig. 11(b) and described in (14). The KL-divergence approach detected the spoofing attack for the first time at $t = 31.2$s, whereas our BP-RNN approach quickly detected the spoofing attack at $t = 25.4$s, while simultaneously demonstrating low false alarms and misdetections. Therefore, we validated the improved performance of the proposed wide-area joint BP and RNN algorithm even during more sophisticated attacks that involve both position and timing being spoofed.

4 Conclusions

To summarize, we have proposed a wide-area joint Belief Propagation and Recurrent Neural Network (BP-RNN) algorithm to detect and mitigate the spoofing attacks as well



(a) RNN-based metric (b) KL-based metric

Fig. 11: Spoofing status estimated using (a) RNN-based metric; (b) KL-based metric. RNN-based metric detects the presence of spoofing at the Bth receiving system 0.7 s after the spoofing starts at $t = 25$ s, whereas KL-divergence first detects spoofing 9.6 s after the spoofing starts.

as estimate the attack-resilient GPS timing that is given to the geographically distributed infrastructures, which are monitored by PMUs. By considering a wide-area network of GPS receiving systems, we have estimated the marginal distribution of the spoofing-induced timing errors at each antenna using distributed BP algorithm. In addition, based on the BP-estimated timing errors, we have adaptively evaluated the spoofing status of each GPS receiving system using an RNN framework. We have validated the pro-

Spoofing attack	**RMS timing error of attacked GPS receiving system**	
	BP-RNN	**Least-Squares**
Timing error of 28μs in a span of 35s	0.14μs	29.8μs
Position error of 55m and timing error of 33μs in a span of 25s	0.16μs	37.94μs

Table 2: Summarizing the RMS timing errors of the attacked GPS receiving system estimated via the proposed wide-area BP-RNN and conventional least-squares approach

posed wide-area BP-RNN using four GPS receiving systems, with three-antenna-based DMDA setup each and subjecting one GPS receiving system to a simulated signal-level spoofing attack. For two cases of simulated spoofing attacks, the RMS timing errors obtained via the proposed wide-area BP-RNN algorithm and conventional least squares approach are listed in Table 2. While one omni-directional antenna-based least squares has shown large RMS timing errors that violated the IEEE-C37.118 standards, the wide-area BP-RNN algorithm has demonstrated low RMS timing errors of less than 0.16μs. Also, as compared to the existing works, we have assessed the improved performance

of our RNN-based metric, which has shown a quick detection of spoofing, that is, 0.7s after the spoofing attack starts in the first experiment and 0.4 after spoofing attack starts in the second experiment.

References

1. M. Q. Raza and A. Khosravi, "A review on artificial intelligence based load demand forecasting techniques for smart grid and buildings," *Renewable and Sustainable Energy Reviews*, vol. 50, pp. 1352–1372, 2015.
2. G. K. Venayagamoorthy, "Potentials and promises of computational intelligence for smart grids," in *Power & Energy Society General Meeting, 2009. PES'09. IEEE*, pp. 1–6, IEEE, 2009.
3. B.-h. Li, B.-c. Hou, W.-t. Yu, X.-b. Lu, and C.-w. Yang, "Applications of artificial intelligence in intelligent manufacturing: a review," *Frontiers of Information Technology & Electronic Engineering*, vol. 18, no. 1, pp. 86–96, 2017.
4. R. Edwin, "Community energy consumption management," Jan. 9 2003. US Patent App. 10/159,294.
5. A. Tuohy, J. Zack, S. E. Haupt, J. Sharp, M. Ahlstrom, S. Dise, E. Grimit, C. Mohrlen, M. Lange, M. G. Casado, *et al.*, "Solar forecasting: methods, challenges, and performance," *IEEE Power and Energy Magazine*, vol. 13, no. 6, pp. 50–59, 2015.
6. S. J. Fernandez, M. Shankar, J. J. Nutaro, Y. Liu, A. D. Dimitrovski, O. A. Omitaomu, C. S. Groer, K. L. Spafford, and R. R. Vatsavai, "Real-time simulation of power grid disruption," July 25 2013. US Patent App. 13/747,779.
7. S. Lin, B. A. Fletcher, M. Luo, R. Chinery, and S.-A. Hwang, "Health impact in New York city during the Northeastern blackout of 2003," *Public Health Reports*, vol. 126, no. 3, pp. 384–393, 2011.
8. G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.
9. P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, no. 3, pp. 75–77, 2009.
10. 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.
11. 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.
12. 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.
13. K. Martin, D. Hamai, M. Adamiak, S. Anderson, M. Begovic, G. Benmouyal, G. Brunello, J. Burger, J. Cai, B. Dickerson, *et al.*, "Exploring the ieee standard c37. 118–2005 synchrophasors for power systems," *IEEE Trans. Power Del.*, vol. 23, no. 4, pp. 1805–1811, 2008.
14. 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.
15. S. Bhamidipati and G. X. Gao, "Gps multi-receiver joint direct time estimation and spoofer localization," *IEEE Transactions on Aerospace and Electronic Systems*, 2018, DOI: 10.1109/TAES.2018.2879532.

16. 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.
17. E. Shafiee, M. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers," *The Journal of Navigation*, vol. 71, no. 1, pp. 169–188, 2018.
18. D. LaST, "GNSS: The present imperfect," *Inside GNSS*, vol. 5, no. 3, pp. 60–64, 2010.
19. M.R.Mosavi, R.Zebarjad, and M.Moazedi, "Novel anti-spoofing methods based on discrete Wavelet transform in the acquisition and tracking stages of civil GPS receiver," *International Journal of Wireless Information Networks*, vol. 25, pp. 449–460, 2018.
20. 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)*, 2018. Under publication.
21. S. Bhamidipati, K. J. Kim, H. Sun, and P. V. Orlik, "Wide-area GPS time monitoring against spoofing using belief propagation," in *International Conference on Sensing, Communication, and Networking (SECON)*, 2019. Under reviewing.
22. J. S. Yedidia, W. T. Freeman, and Y. Weiss, "Understanding belief propagation and its generalizations," *Exploring artificial intelligence in the new millennium*, vol. 8, pp. 236–239, 2003.
23. T. Mikolov, M. Karafiát, L. Burget, J. Černockỳ, and S. Khudanpur, "Recurrent neural network based language model," in *Eleventh Annual Conference of the International Speech Communication Association*, 2010.
24. S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
25. P. Misra and P. Enge, "Global positioning system signals, measurements, and performance," *USA: Ganga Jamuna Press*, 2006.
26. 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.
27. 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.
28. A. Graves and J. Schmidhuber, "Framewise phoneme classification with bidirectional LSTM and other neural network architectures," *Neural Networks*, vol. 18, no. 5-6, pp. 602–610, 2005.
29. K. Gimpel and N. A. Smith, "Softmax-margin CRFs: Training log-linear models with cost functions," in *Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics*, pp. 733–736, Association for Computational Linguistics, 2010.
30. F. E. Harrell, "Ordinal logistic regression," in *Regression modeling strategies*, pp. 311–325, Springer, 2015.
31. 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.
32. T. Ebinuma, "Gps-sdr-sim," *[Online] Available: https://github.com/osqzss/gps-sdr-sim*.
33. K. Paul, "Soft GNSS," *[Online] Available: https://github.com/kristianpaul/SoftGNSS*.
34. I. Bello, B. Zoph, V. Vasudevan, and Q. V. Le, "Neural optimizer search with reinforcement learning," in *Proceedings of the 34th International Conference on Machine Learning-Volume 70*, pp. 459–468, JMLR. org, 2017.
35. S. Eguchi and J. Copas, "Interpreting kullback–leibler divergence with the neyman–pearson lemma," *Journal of Multivariate Analysis*, vol. 97, no. 9, pp. 2034–2040, 2006.