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

Artificial Intelligence-Based Distributed Belief Propagation and Recurrent Neural Network Algorithm for Wide-Area Monitoring Systems

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

TR2020-058 May 14, 2020

Abstract

To monitor the power grid over a wide-area, the wide-area monitoring system (WAMS) has been developed. At each substation, the Global Positioning System (GPS) receiving system resides to provide a trusted timing. Thus, it is critical for the WAMS to maintain an authentic GPS timing over a widearea. However, the GPS timing is susceptible to spoofing due to the unencrypted signal structure and its low signal power. Thus, to obtain the trusted GPS timing from spoofing, a new wide-area monitoring algorithm, which is comprised of distributed belief propagation (BP) and a bi-directional recurrent neural network (RNN), is developed under the frame of Artificial Intelligence (AI). This joint BP-RNN algorithm authenticates each power substation by evaluating the estimated GPS timing error by its distributed processing capability. Especially, the bi-directional RNN provides a fast timing error estimation under the frame of AI. Simulation results validate the fast detection time over the Kullback–Leibler divergencebased approach, and timing error estimation accuracy over the limit provided by the IEEE C37.118.1-2011 standard.

IEEE Network

Artificial Intelligence-Based Distributed Belief Propagation and Recurrent Neural Network Algorithm for Wide-Area Monitoring Systems

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

Abstract

To monitor the power grid over a wide-area, the wide-area monitoring system (WAMS) has been developed. At each substation, the Global Positioning System (GPS) receiving system resides to provide a trusted timing. Thus, it is critical for the WAMS to maintain an authentic GPS timing over a wide-area. However, the GPS timing is susceptible to spoofing due to the unencrypted signal structure and its low signal power. Thus, to obtain the trusted GPS timing from spoofing, a new wide-area monitoring algorithm, which is comprised of distributed belief propagation (BP) and a bi-directional recurrent neural network (RNN), is developed under the frame of Artificial Intelligence (AI). This joint BP-RNN algorithm authenticates each power substation by evaluating the estimated GPS timing error by its distributed processing capability. Especially, the bi-directional RNN provides a fast timing error estimation under the frame of AI. Simulation results validate the fast detection time over the Kullback–Leibler divergence-based approach, and timing error estimation accuracy over the limit provided by the IEEE C37.118.1-2011 standard.

I. Introduction

In the recent past, Artificial Intelligence (AI) has been playing a pivotal role in modernizing different safety-critical applications, such as, banking, autonomous driving and electrical power grids. In power substations, AI techniques are already being utilized to provide robust solutions for increasing the production, optimizing the energy consumption, detecting the anomalies and localizing the disruptions. Google's DeepMind is collaborating with the UK's National Grid to develop AI solutions [1] that balance the supply and demand of electricity.

Sriramya Bhamidipati is with the University of Illinois at Urbana-Champaign. Kyeong Jin Kim (corresponding author), Hongbo Sun, and Philip V. Orlik are with Mitsubishi Electric Research Laboratories (MERL). This work was done when S. Bhamidipati was working with MERL.

To perform high-resolution grid monitoring and early-stage detection of grid destabilizing conditions, Wide-Area Monitoring Systems (WAMS) are developed that analyze the information obtained from a wide-area network of power substations. In this context, WAMS relies on advanced devices, known as Phasor Measurement Units (PMUs) to monitor the voltage and current phasor measurements, which are indicative of the grid stability conditions. PMUs utilize precise time sources, such as, Global Positioning System (GPS), to time-tag the phasor measurements and to obtain global time synchronization. However, due to the unencrypted signal structure and a very low signal power, the civilian GPS signals are susceptible to external spoofing attacks. In 2017, a mass GPS spoofing incident that was reported near the Russian port of Novorossiysk has demonstrated the real-world threats to critical infrastructure due to GPS spoofing [2]. In [3], the authors validated the vulnerability of GPS timing provided to PMUs during the presence of spoofing. Based on the IEEE C37.118.1-2011 standard for synchrophasors [4], we consider 1% total vector error equivalent to a timing error of 26.5 μs, as a benchmark in our power grid stability analysis.

A. Technical Literature Review

In [5], the authors computed the Wavelet transformation coefficients of both spoofing and authentic signals that are later given to the support vector machines and probabilistic neural networks for the detection of spoofing attacks. In [6], a particle filter based anti-spoofing algorithm was developed utilizing variations in decoded pseudorange measurements. In [7], a geographically distributed multiple directional antennas (DMDA) setup was proposed to isolate the spoofing attacks, with each antenna receiving satellite signals from only a subsection of the sky. A belief propagation (BP)-based Extended Kalman filter (EKF) algorithm that utilizes the proposed DMDA setup for a single power substation was designed by [7] and for a wide-area network of power substations was designed by [8]. In [9], a wide-area AI-based BP-EKF algorithm that authenticates all the power substations in the wide-area network and reduces the sensitivity due to the prior distribution of timing error was proposed. However, the authors of [9] investigated only one power substation attacked by a simple spoofing attack.

B. Motivation

In this article, we propose an AI-based approach that not only detects but also isolates and mitigates different types of spoofing attacks [2], ranging from simple record-and-replay-based meaconing to sophisticated signal-level spoofing. Signal-level spoofing is caused by generating and later broadcasting counterfeit GPS satellite signals that causes the receiver to lock onto these high-powered malicious signals instead of the authentic ones. Once locked, the attacker is capable of smoothly manipulating the target

receiver to an incorrect physical location or timing or both. Given no abrupt changes in the navigation solution, this sophisticated signal-level attack is harder to detect, more dangerous comparing other attacks and is therefore, the focus of this article. However, our proposed algorithm is also directly applicable for the detection and mitigation of other spoofing attacks.

C. Our Contributions

In contrast to the existing work, in this work, we utilize two powerful AI tools, namely, BP and recurrent neural networks (RNNs) to develop a wide-area joint BP and RNN algorithm that validates the enhanced attack-resilience of the grid during coordinated spoofing attacks, which affect multiple power substations. In addition, we perform extensive experiments to validate the improved spoofing detection times of the proposed AI-based joint BP-RNN as compared to the prior work [8]. We utilize the AI-based BP framework [10] to estimate the timing errors induced at each antenna in the wide-area network. We also utilize the AI-based RNN architecture [11] to authenticate the GPS signals received at different power substations by learning the spatial and temporal variations in the BP estimated timing errors.

The rest of the paper is organized as follows: Section II describes the system overview and high-level architecture; Section III describe the algorithm details of our joint BP and RNN algorithm; Section IV validates the improvement in performance, namely timing accuracy and detection times, of the proposed algorithm under coordinated spoofing attack; and Section V concludes the paper.

II. System Overview

In this section, we explain the wide-area system configuration of the joint BP-RNN algorithm and later describe its high-level system architecture. Since the GPS receiving system is installed at each substation in WAMS, the GPS receiving system can be recognized as the power substation.

A. System configuration

The important aspects related to the system configuration includes the wide-area network of power substations and the antenna configuration at each power substation in the network.

1) Wide-area network:

By receiving information from different locations, it is possible to conduct self-healing, fault-tolerance and dynamic optimization [12], [13]. However, these works did not investigate the GPS timing attack over a wide-area network.

Given the limitations related to the physical area covered by a spoofing transmitter, we consider a wide-area network of N geographically distributed GPS receiving systems. This spatial separation significantly minimizes the possibility of multiple GPS receiving systems being simultaneously affected by the same spoofer. Therefore, the wide-area network of receiving systems can communicate with each other to cross-validate the authenticity of all the GPS receiving systems. To exchange data across power substations, we leverage the already in-place communication network of the power systems.

All the GPS receiving systems with a valid communication link to the ath receiving system are categorized as its neighbor set and represented by N_a. At the ath GPS receiving system, we consider a setup of multiple antennas with the number of antennas represented as M_a. All the antennas within the system are independently triggered using a common clock. Similarly, for any kth antenna in the ath receiving system, the set of neighboring antennas, represented by $\mathcal{B}_k^a = \Big\{\{1, \cdots, M_a\} - k\Big\} \bigcup_{b \in \{1, \cdots, |N_a|\}} \{1, \cdots, M_b\}$, include the antennas within the ath receiving system excluding itself as well as the antennas that belong to its neighbor set N_a with its number denoted by $|N_a|$. The wide-area communication structure is designed, such that, each GPS receiving system has a central processing (CP) unit, which receives/sends system data from its neighboring set of GPS receiving systems.

2) Distributed multiple directional antennas:

We can see that the distance between target receiver and the attacker is quite small as compared to its distance from the authentic GPS satellites. This causes spoofing to behave as a directed attack. Therefore, we isolate the spoofing attacks by considering multiple directional antennas at each GPS receiving system. Each directional antenna is pointed towards a different section of the sky, so that during spoofing, not all the antennas can be in the line-of-sight from the attacker, and hence cannot be simultaneously affected.

When multiple directional antennas are attacked, all the spoofed antennas pinpoint to the same incorrect physical location. To utilize this characteristic to our advantage, we incorporate geographical separation among the multiple directional antennas located within the power substation. As mentioned above, all the antennas within the GPS receiving system are triggered by the same clock, based on which we design a metric for distinguishing authentic condition from that of a spoofed condition. The block diagram of the DMDA is provided in Fig. 1.

B. System architecture and key advantages

By utilizing the system configuration described in Section II-A, the architecture of the proposed wide-area joint BP-RNN algorithm, shown in Fig. 2 is outlined as follows:

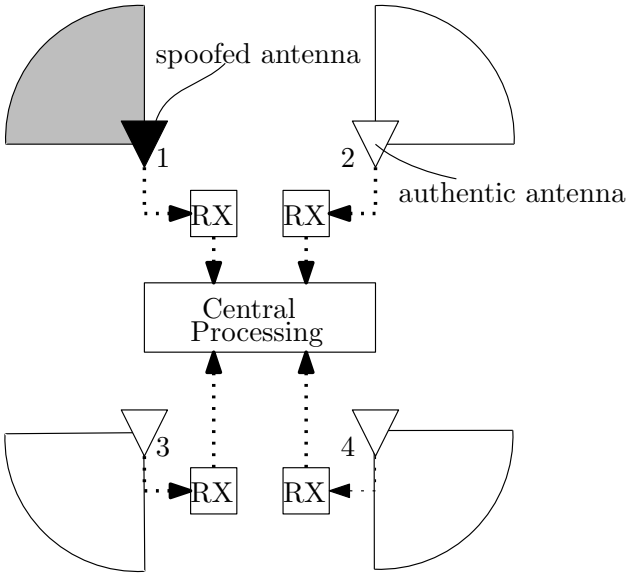


Fig. 1: Block diagram of the DMDA setup [7]. Sector of circle represents the field-of-view of each antenna.

1) Across different power substations, we leverage the pseudoranges measured at each stationary antenna, predicted navigation state vector of the EKF module and the pre-determined antenna baseline distances within the GPS receiving system to compute the pseudorange residuals, which are exchanged across the GPS receiving systems via communication links.
2) At the CP unit of each GPS receiving system, we compute the single difference pseudorange residual vector for each antenna, by considering one pseudorange residual corresponding to the satellite observed by itself and the other pseudorange residual corresponding to the antenna in its neighboring set.
3) Next, we compute the approximate marginal distribution of the antenna-specific timing error via an AI-based BP framework [10], where we estimate the timing errors based on the single difference pseudorange residuals.
4) Next, we correct the pseudoranges based on the BP estimates of the antenna-specific timing errors, which are later processed via the measurement update step of the adaptive EKF module [14] in the CP unit. The CP unit provides the estimated GPS timing to the power substation, where it is utilized by the PMUs for time-tagging the phasor measurements.
5) In parallel, we provide the BP estimates of the antenna-specific timing errors to our trained bi-directional Long Short-Term Memory (LSTM)-based RNN [11] framework, so as to compute the authenticity of the estimated GPS timing at each GPS receiving system.

The AI-based BP framework of the proposed joint BP-RNN algorithm provides a computationally-efficient platform to approximate the marginal distribution of the wide-area network of antenna-specific timing errors. Instead of a centralized communication framework, which has a single critical point of failure, we opt for a distributed communication platform that is not only robust against failure, but also exhibits lower processing latencies and quicker spoofing detection times. The joint BP-RNN algorithm is easily scalable to any number of GPS receiving systems and any number of directional antennas within the GPS receiving system. With an increase in the number of widely-distributed antennas, the correlation between the measurement errors will be lower, which would lead to lower false alarm and misdetection rates.

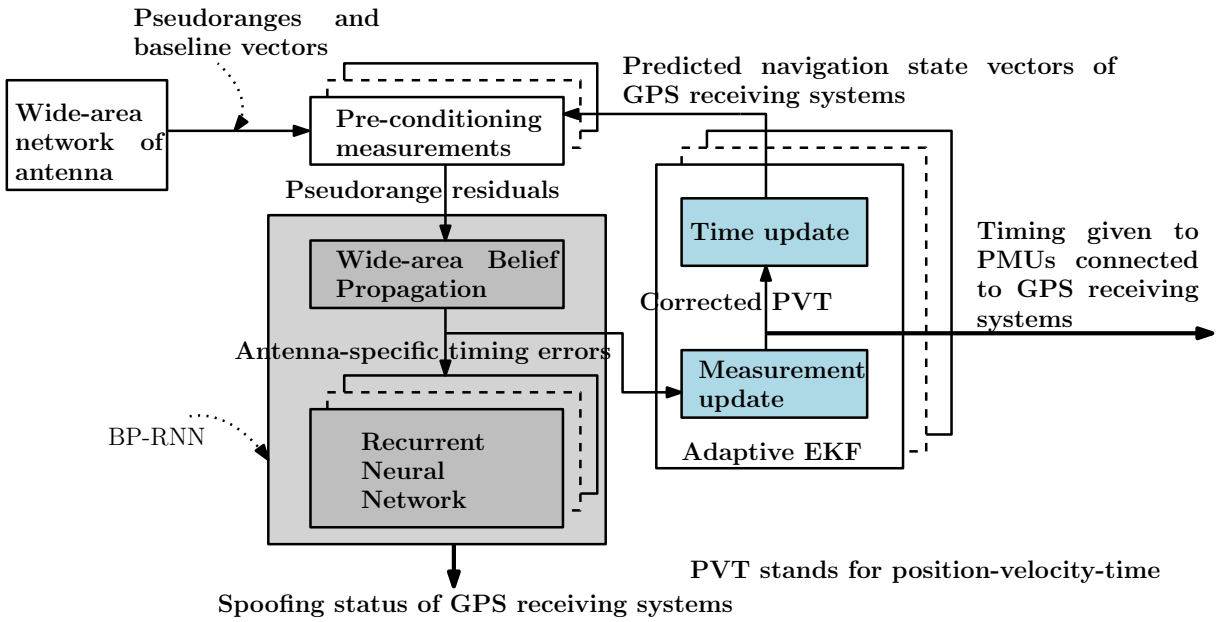


Fig. 2: Block diagram of the wide-area joint BP-RNN.

Utilizing a wide-area network of GPS receiving systems as compared to single system, addresses the spoofing scenario when all the antennas are affected within the same power substation and also reduces the overall sensitivity on the prior distribution of the antenna-specific timing error. Similarly, by utilizing the 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.

III. Joint BP and RNN algorithm

In this section, we describe the proposed AI-based joint BP and RNN algorithm, which utilizes a wide-area network of the DMDA setup, to compute the spoofing-resilient GPS timing. The steps of the

BP-RNN algorithm, which is used to compute the attack-resilient GPS timing, is outlined as follows:

A. GPS measurement likelihood

At the ath receiving system, among the M_a directional antennas, the kth antenna obtains measurements from the L_k set of satellites visible to it. We assign one antenna of the DMDA setup at each GPS receiving system as the master antenna, whose navigation state vector $\boldsymbol{\beta}_t^a$ is propagated using the EKF module. The navigation state vector $\boldsymbol{\beta}_t^a \triangleq [\boldsymbol{x}_1, c\delta t, \boldsymbol{v}_1, c\delta \dot{t}]_t^T$ consists of the 3D position, common clock bias, 3D velocity and common clock drift of the master antenna.

Based on the predicted navigation state vector $\hat{\boldsymbol{\beta}}_t^a$ of the master antenna obtained from the EKF module and the pre-determined antenna baseline distances at the ath receiving system, we compute the measurement residuals of the ith satellite tracked by the kth antenna. During a spoofing attack targeted to manipulate the GPS timing, the measurements have an additional unknown bias, which is termed as antenna-specific timing error, denoted by α_k^a, and is common across the satellites observed at the same antenna.

In this work, we consider the pseudoranges to compute the measurement residuals, denoted by $\Delta\rho_k^i$ for $k \in \{1, \cdots, M_a\}$ and $i \in L_{k,t}$, that serves as a metric to indicate the corresponding antenna-specific timing error. We also formulate a common measurement model at each ath GPS receiving system that takes in the navigation state vector of the master antenna and the pre-determined baseline distances between the master and other antennas to compute the expected pseudoranges from all the visible satellites L^a, such that $L^a = L_1 + \cdots + L_{M_a}$. Alternatively, one can use the other available measurements, such as, pseudorange rates, Doppler, carrier phase and so on.

Next, at each ath GPS receiving system and at time instant t, we perform pre-conditioning on the measurement residuals by calculating the single difference residuals $\boldsymbol{\gamma}_{kn,t}^{ij}$ across all possible pairs of satellites, where the first measurement residual corresponds to the ith satellite observed by one antenna, say kth $\forall k \in \{1, \cdots, M_a\}$, and the second residual corresponds to the jth satellite at another antenna, say nth $\forall n \in \{1, \cdots, \mathcal{B}_k^a\}$, that belongs to the neighboring set of the first antenna.

During authentic conditions, the single difference measurement residuals across any two antennas, say kth and nth, that belong to the same GPS receiving system, should be close to zero, i.e., $\gamma_{kn}^{ij} \approx 0$ for $\forall i \in L_k$ and $\forall j \in L_n$ as the timing errors are negligible when triggered using a common clock. However, across two antennas that belong to different GPS receiving systems, the single difference measurement residuals are a non-zero value, due to the difference in the clock bias.

Across a pair of antennas, say kth and nth, stacking the single different measurement residuals, we have $\boldsymbol{\gamma}_{kn,t} \triangleq \{\gamma_{kn,t}^{ij}, i \in L_{k,t}, j \in L_{n,t}\}$. Then, the corresponding measurement likelihood probability is

calculated as

$$p(\boldsymbol{\gamma}_{kn,t}|\alpha_k^a,\alpha_n^b) = C_1 \text{exp}\Big\{ C_2 \Big(\frac{\mathbf{1}^T \boldsymbol{\gamma}_{kn,t}}{L_{k,t} L_{n,t}} + (\alpha_k^a - \alpha_n^b) \Big)^2 \Big\} \;\forall\; n \in \mathcal{B}_k^a, \tag{1}$$

where $C1 \triangleq 1/\sqrt{(2\pi\nu_{kn}^2)^{L_{k,t}L_{n,t}}}$, $C_2 \triangleq -L_{k,t}L_{n,t}/2\nu_{kn}^2$, 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, and predicted position and velocity of the antenna.

B. Timing errors via AI-based BP framework

We design a wide-area BP algorithm to compute the marginal distribution of the antenna-specific timing errors $\alpha_{k,t}^a$ over a wide area. BP [10] is a sum-product message passing algorithm for distributed systems to make inferences on the unobserved variables in the graphical models. With an increase in the number of GPS receiving systems in the wide-area network and the number of antennas in each GPS receiving system, computing the exact marginal distribution of the spoofing-induced timing errors becomes quite computationally expensive. In this regard, AI-based BP approximates the marginal distribution, termed as belief $b_t(\alpha_k^a)$, in a computationally-efficient manner. Given that an attacker broadcasts counterfeit look-alike GPS signals, it is justified to consider that the associated timing errors induced by the spoofer follow a Gaussian distribution. Therefore, we model the belief of antenna-specific timing errors as Gaussian distribution with mean $\mu_{k,t}^a$ and variance $(\sigma_{k,t}^a)^2$

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

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

We update the belief $b_t(\alpha_k^a)$ at the kth antenna of the ath receiving system, by computing the product of its prior distribution, which is indicated by the prior-related message and all the incoming messages from all the neighboring antennas $\mathcal{B}_k^a$, which is indicated by the measurement-related messages. We evaluate the two kinds of messages, namely, measurement-related messages, $m_{f_{kn}^a \to \alpha_k^a}$, and prior-related message, $m_{f_k^a \to \alpha_k^a}$, as follows:

$$\begin{aligned} m_{f_{kn}^a \to \alpha_k^a}(\alpha_k^a) &= \int_{n \in \mathcal{B}_k^a} p(\boldsymbol{\gamma}_{kn}|\alpha_k^a,\alpha_n^b)\, b_{t-1}(\alpha_n^b)\; d\alpha_n^b, \\ &= \mathcal{N}\Big(\alpha_k^a : \mu_{kn,t}^a,\, (\sigma_{kn,t}^a)^2\Big) \text{ and} \end{aligned}$$

$$m_{f_k^a \to \alpha_k^a} = \mathcal{N}\Big(\alpha_k^a : \mu_{pk,t}^a, (\sigma_{pk,t}^a)^2\Big), \tag{3}$$

where $m_{f_{kn}^a \to \alpha_k^a}$ takes into account the belief of the nth neighboring antenna, $n \in \mathcal{B}_k^a$ with $\mu_{kn,t}^a = \mu_{n,t-1}^b - \dfrac{\mathbf{1}^T \boldsymbol{\gamma}_{kn,t}}{L_{k,t} L_{n,t}}$ and $(\sigma_{kn,t}^a)^2 = \dfrac{\nu_{kn}^2}{2L_{k,t}L_{n,t}} + (\sigma_{n,t-1}^a)^2$. In addition, $m_{f_k^a \to \alpha_k^a}$, represents the prior distribution formulated as a Gaussian, with mean $\mu_{pk,t}^a$ and variance $(\sigma_{pk,t}^a)^2$. Note that interested authors can find detailed derivations of (2) and (3) in [7]. Details regarding the calculation of prior distribution for different antennas is given in the Section IV-B.

For the kth antenna, we update the belief, as described in (2), by computing the product of measurement-related messages from its neighboring set of antennas and the prior-related message from itself. The belief $b_t(\alpha_k^a)$ represents the estimated antenna-specific timing error at time instant t.

C. Spoofing status via bi-directional RNNs

During signal-level spoofing, as explained in Section I, the rate of change of the timing errors may be constant, might have sudden jumps or may even gradually change with time. Given these requirements, the designed neural network needs to be able to retain information learnt from long multivariate time sequences, which are obtained from different antennas. Therefore, we authenticate each GPS receiving system by utilizing all the estimated spoofing-induced timing errors at its antennas, via another AI-based approach known as RNN that meets these requirements. Note that, existing literature showed evidences of an increased performance by considering a combination of RNN and Convolutional Neural Network. However, this involves a longer reaction time to the GPS timing attack. Considering both the reaction time and detection performance, we employ bi-directional LSTMs for estimating the spoofing status.

We train our neural network to estimate the authenticity of the GPS receiving system based on the temporal variation of the timing errors at each antenna and the spatial variation indicated by the similarity in the estimated timing errors across the antennas. Therefore, in the joint BP-RNN, we compute the BP-estimated timing errors at each time instant, but we estimate the RNN-based spoofing status at periodic time intervals. In particular, we analyze a time series of the past and future BP-estimated timing errors to compute the corresponding spoofing status. Therefore, we opt for bi-directional LSTM as compared to a uni-directional LSTM. This is justified because bi-directional LSTMs preserve the information from both the past and future, thereby efficiently capturing the big picture trend of the slow-varying timing errors associated with the sophisticated signal-level spoofing.

As seen in Fig. 3, the employed bi-directional-LSTM architecture consists of an input layer, forward layer, backward layer, activation layer, and an output layer. In the input layer, we consider W^a time instants of input nodes, denoted by $\theta_{t-W^a:t}^a$, such that, $\theta_t^a \triangleq [\alpha_1^a, \cdots, \alpha_{M_a}^a]_t^T$. The outputs from the forward and

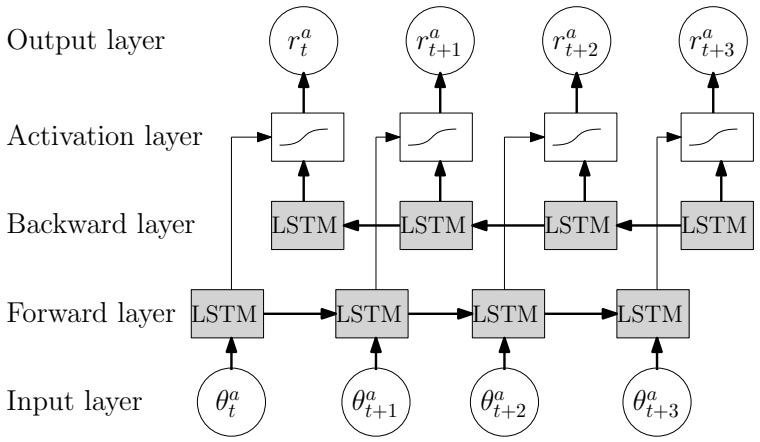


Fig. 3: Overall architecture of our bi-directional-LSTM, which takes the antenna-specific timing errors of all antennas within the ath GPS receiving system, denoted by θ_t^a and estimates the spoofing status, denoted by r_t^a.

backward layers are combined in a Softmax function-based activation layer. This is later provided as input to the final output layer. The output layer consists of one output node, that is, either 0-authentic or 1-spoofed, thereby indicating the spoofing status r_t^a of the ath receiving system.

The forward and backward layers consist of components called LSTM units, each of which is composed of a cell, an input gate, an output gate and a forget gate. The cell keeps track of the dependencies among the input sequence via regulators called gates, which in-turn control the information passed through the LSTM unit. The input gate decides the extent to which new information flows into the cell, forget gate controls the extent to which the information is retained, and finally, the output gate controls the extent to which the information is used to compute the output activation of the LSTM unit. Each gate is paired with a logistic activation function and also associated with unknown weights and biases, which are estimated during the training stage. Detailed explanation regarding the working of LSTM is explained in [11].

D. GPS timing via Adaptive EKF

By utilizing the BP estimates of the antenna-specific timing errors, the adaptive EKF module is executed independently at each GPS receiving system. As explained in [7], we summarize the adaptive EKF in three stages, namely, adaptive covariance estimation, measurement update and time update. To compute the adaptive covariance estimation, we first calculate the corrected pseudoranges, which are obtained by computing the difference between the measured pseudorange and the BP-estimated timing error. By utilizing the previous estimate of covariance and the Kalman measurement residual, we calculate the covariance at the current time instant based on an associated value of the forgetting factor [14]. Next, we

perform measurement update using Kalman filter equations that estimate the navigation state vector of the master antenna and its associated covariance, by computing the optimal Kalman gain that minimizes the residual error. The clock bias obtained as output from the adaptive EKF module is used to calculate the attack-resilient GPS timing that is later given to the PMUs. Next, we propagate the adaptive EKF module to estimate the predicted navigation state vector for the next time instant using a constant velocity linear transition matrix.

IV. Experiments

In this section, we demonstrate the performance of the proposed wide-area BP-RNN algorithm to not only detect but also successfully isolate and mitigate the coordinated spoofing attack affecting multiple power substations.

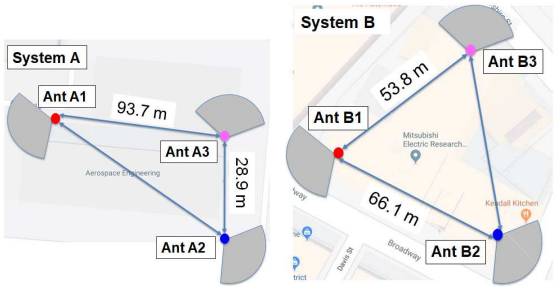
A. Experimental setup

As seen in Fig. 4, we consider a simulated network of four GPS receiving systems located at Austin, Boston, Chicago and Kansas City, which are denoted by A, B, C, and D, respectively. At each GPS receiving system, the installed DMDA setup comprises of three stationary antennas, whose fixed baseline distances are pre-computed and later used for the calculation of pseudorange residuals, as explained in Section III-A. The geographical separation between the antennas within the GPS receiving system are considered such that, they mimic the infrastructure of an actual power substation. Using a publicly available ephemeris file, we simulated the GPS signals received at each antenna and at each GPS receiving system via a C++ simulator known as GPS-SIM-SDR [15]. We collected the simulated GPS signals at a sampling rate of 2.5 MHz. The antennas at each DMDA setup are provided with the 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.

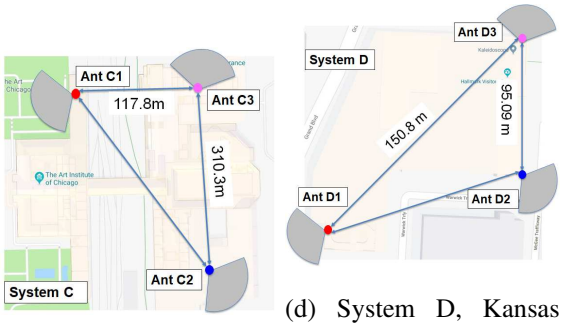
Based on the signal-level spoofing attack explained in Section I, we introduced a malicious coordinated spoofing attack that affects two GPS receiving systems, i.e., Austin and Chicago. We simulated two spoofers, which independently target one GPS receiving system each, by adding high-powered and simulated malicious samples to the generated authentic simulated GPS samples. Authentic satellite positions extracted from external ephemeris file are given to the proposed wide-area joint BP-RNN.

B. Implementation details

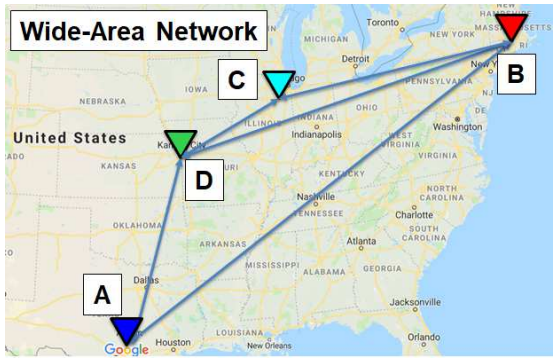
In this subsection, we describe the various implementation choices related to the prior distribution of antenna-specific timing errors, communication data protocol, and training of the bi-directional-LSTM.



(a) System A, Austin (b) System B, Boston



(c) System C, Chicago (d) System D, Kansas City



(e) Wide-area network and communication links

Fig. 4: The simulated WAMS experimental setup consists of four GPS receiving systems, each of which assumes a three antenna-based DMDA setup.

1) Prior distribution:

Utilizing a wide-area network of antennas reduces the sensitivity of the antenna-specific timing errors on the prior distribution. Therefore, among the N widely-dispersed infrastructures, we choose the GPS receiving system with the least spoofing risk, i.e., $a_m = \underset{a\in\{1,\cdots,N\}}{\arg\min}\ r_t^a$, where r_t^a was computed by RNN. 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, $\alpha_{k,t-W:t}^{a_m} \forall k = \{1, \cdots, M_{a_m}\}$. The rest of the GPS receiving systems are assigned by uniform prior distribution, which is approximated as Gaussian with $\mu_{pk,t}^{a} = 0$ and $(\sigma_{pk,t}^{a})^2 = \infty, \forall a \in \{1, \cdots, N\} - a_m$.

2) Communication data protocol:

By utilizing the wide-area communication structure of the power systems, we exchange *system data* across different GPS receiving systems in a distributed manner. The system data transmitted/received from the ath receiving system comprises of the following information: number of antennas M_a as well as the pseudorange residuals $\Delta\rho_{k,t}^{i}$ and beliefs $b_{t-1}(\alpha_k^a)$ for its kth antenna $k \in \{1, \cdots, M_a\}$.

3) Training of bi-directional-LSTM network:

We performed training and validation of the bi-directional-LSTM by considering 1 million samples of input features, namely, BP-estimates of timing errors, which are obtained from different GPS receiving systems. Out of the 1 million samples, 99% of the data was allocated for training the bi-directional-LSTM, whereas the rest of 1% was used for validation at the end of 10 training iterations. In addition, out of the 1 million input samples considered, 65% data was generated under authentic conditions, which was obtained from both real-world GPS signals collected using a GPS receiver and simulated GPS data obtained from the C++-based GPS simulator. The rest of 35% input samples are generated under different attacker configurations and different magnitudes of spoofing attacks, We setup the neural network to execute back propagation so that the corresponding network weights are fine tuned. We consider our cost function to be mean-squared error and also utilized an Adam optimizer.

TABLE I: Training and validation accuracy for different hyper-parameter settings

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

To train the bi-directional LSTM, we consider a multivariate time sequence as input, with three antennas at each GPS receiving system and $W^a = 60$, time instants of the past antenna-specific timing errors. The

training and validation accuracy for different hyper-parameter settings are described in Table I. Based on this, the final chosen network architecture consists of 50 hidden nodes and a batch size of 1028.

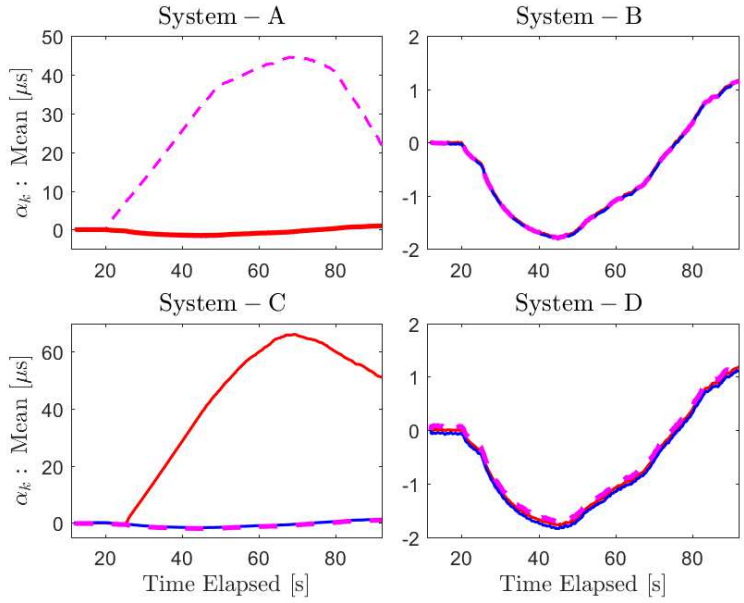
C. Under simulated spoofing attack

The entire time duration of the simulated experiment was 100 s, during which a simulated coordinated spoofing attack was introduced for a partial duration. Between $t = 25$-45 s, a signal-level spoofing attack, corresponding to the first spoofer, was induced at the Cth receiving system located at Chicago. In particular, we generated simulated spoofed GPS signals that induces a constant change in position of 74 m and a gradually increasing timing error from $0-45$ μs in a span of 20 s. In addition, during $t = 20$-45 s, another independent spoofing attack associated to a second spoofer was induced at the Ath receiving system located at Austin. Without a position change, this spoofing attack induced a gradually increasing timing error from $0-40$ μs in a span of 25 s. Because of the DMDA-based antenna configuration and the direction of attack, the first attacker can only successfully spoof C1 antenna at the Cth receiving system and the second attacker can only spoof A3 antenna at the Ath receiving system.

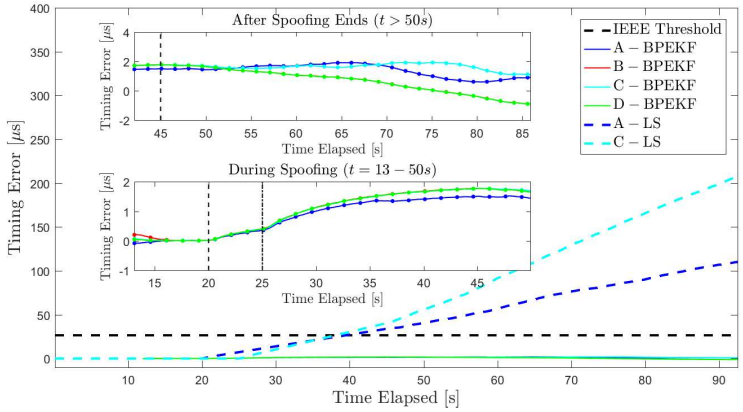
Fig. 5(a) shows the wide-area BP estimates of the antenna-specific timing errors at all the GPS receiving systems. We validated that the proposed wide-area BP-RNN algorithm not only detects C1 and A3 antennas to be affected by spoofing but also accurately estimates the timing error introduced in the system. In addition, the mean of the antenna-specific timing errors at Bth and Dth GPS receiving systems are low, thereby, validating its authenticity.

We observe in Fig. 5(b) that the conventional least squares-based timing estimates of omni-directional antennas placed at both C1 and A3 antenna locations diverged with time and shows an RMS timing error of 97.35 μs and 58.90 μs, respectively. In particular, after the spoofing attacks starts, the IEEE-C37.118-1 threshold is violated within 13 s at C1 antenna and within 19.5 s at A3 antenna. However, the proposed wide-area joint BP and RNN algorithm, which starts at t=12 s, shows a steady convergence with the RMS timing errors as 1.23 μs, 0.56 μs, 1.28 μs and 0.55 μs at A, B, C and Dth GPS receiving systems, respectively.

Next, in Fig. 6, we validate the robustness of the bi-directional-LSTM network in computing the spoofing status of the GPS receiving systems. We compare the performance of the trained bi-directional LSTM network, explained in Section III-C, with that of Kullback-Leibler (KL)-divergence approach, whose threshold was manually set to 10. In [8], we designed the KL-based metric, such that when the KL-test statistic is greater than this threshold, the KL-based metric $r^a_{KL,t} = 1$ indicating a spoofed GPS receiving system and $r^a_{KL,t} = 0$ otherwise, indicating an authentic condition.



(a) Mean of antenna-specific timing errors

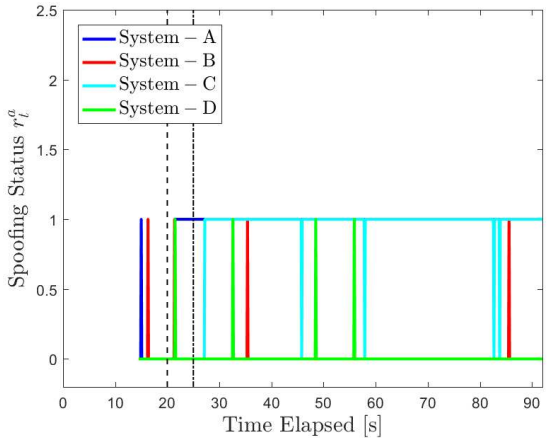


(b) GPS timing error

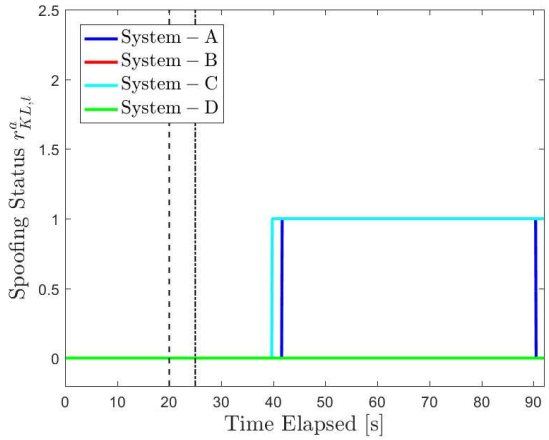
Fig. 5: (a) Mean of the BP estimated belief indicating the antenna-specific timing errors at all the receiving systems. The red, blue and magenta represent the three antennas at four receiving systems (substations); (b) Timing errors estimated via the proposed wide-area joint BP-RNN algorithm.

At the Cth and Ath receiving systems, the KL-divergence approach detects the spoofing attack for the first time after 9.8 s and 7.3 s respectively, whereas the BP-RNN approach quickly detects the spoofing attack after 2.1 s, 1.6 s, respectively. We observe that the bi-directional-LSTM shows a comparable performance as KL-divergence in terms of low false alarms and misdetections. Therefore, during coordinated spoofing attack in which both position and timing of multiple power substations

are manipulated, we demonstrate improved detection times of the proposed wide-area joint BP-RNN algorithm as compared to the prior work [8].



(a) RNN-based metric



(b) KL-based metric [8]

Fig. 6: Spoofing status estimated using (a) RNN-based metric; (b) KL-based metric.

V. Conclusion

In this article, we have introduced a wide-area spoofing-resilient time authentication algorithm using a network of GPS receiving systems, each consisting of a DMDA setup. By utilizing the communication network of power systems, we have designed a distributed architecture of AI-based BP framework that analyzes the pseudorange residuals computed across the power substations of WAMS to estimate the marginal distribution of the antenna-specific timing errors. After then, we have authenticated each substation by analyzing the spatial and temporal variations in the BP estimates of timing errors via a trained bi-directional-LSTM framework.

We have validated the improved performance of the proposed wide-area joint BP-RNN algorithm using four GPS receiving systems, each comprising of three antennas-based DMDA setup and subjecting one GPS receiving system to a simulated signal-level spoofing attack. While a single omni-directional antenna-based least squares has shown large RMS timing errors of 97.35 μs that violated the IEEE-C37.118 standards within 13 s after the spoofing attack starts, the wide-area BP-RNN algorithm has demonstrated low RMS timing errors of less than 1.23 μs. While exhibiting low false alarm and misdetection rates, we have demonstrated that the proposed AI-based RNN metric has quickly detected the spoofing attack 2.1 s after it starts.

Given the availability of large amounts of open-source GPS data, for our future work, we aim to explore advanced AI approaches, such as ResNets and autoencoders, to further improve the detection times while reducing the associated false alarm and mis-detection rates.

REFERENCES

[1] R. Edwin, "Community energy consumption management," Jan. 9 2003. US Patent App. 10/159,294.

[2] S. Bhamidipati and G. X. Gao, "GPS multi-receiver joint direct time estimation and spoofer localization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 4, pp. 1907–1919, 2019.

[3] 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.

[4] K. Martin *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.

[5] 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," *Int. J. of Wireless Information Networks*, vol. 25, pp. 449–460, 2018.

[6] S. Han, D. Luo, W. Meng, and C. Li, "A novel anti-spoofing method based on particle filter for GNSS," in *Proc. IEEE Int. Conf. Commun.*, (Sydney, Australia), pp. 5413–5418, Jun. 2014.

[7] S. Bhamidipati, K. J. Kim, H. Sun, and P. V. Orlik, "GPS spoofing detection and mitigation in PMUs using distributed multiple directional antennas," in *Proc. IEEE Int. Conf. Commun.*, (Shanghai, China), pp. 1–7, 2019.

[8] S. Bhamidipati, K. J. Kim, H. Sun, and P. V. Orlik, "Wide-area GPS time monitoring against spoofing using belief propagation," in *Proc. IEEE Int. Conf. Sensing, Communication, and Networking*, (Boston, MA), pp. 1–8, 2019.

[9] S. Bhamidipati, K. J. Kim, H. Sun, P. V. Orlik, and J. Zhang, "Joint BP and RNN for resilient GPS timing against spoofing attacks," in *Proc. Int. Conf. Artificial Intelligence for Communications and Networks*, (Harbin, China), 2019.

[10] 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.

[11] T. Mikolov *et al.*, "Recurrent neural network based language model," in *Proc. Annual Conf. Inter. Speech Communication Association*, (Chiba, Japan), Sep. 2010.

[12] S. Ray and G. K. Venayagamoorthy, "Real-time implementation of a measurement-based adaptive wide-area control system considering communication delays," *IET Generation, Transmission Distribution*, vol. 2, pp. 62–70, Jan. 2008.

[13] P. Wall *et al.*, "Deployment and demonstration of wide area monitoring system in power system of Great Britain," *J. of Modern Power Systems and Clean Energy*, vol. 4, no. 3, pp. 506–518, 2016.

[14] K. H. Kim, J. G. Lee, C. G. Park, and G. I. Jee, "The stability analysis of the adaptive fading extended Kalman filter," in *Proc. IEEE Int. Conf. Control Applications*, (Singapore), pp. 982–987, Oct. 2007.

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

BIOGRAPHIES

Sriramya Bhamidipati (sbhamid2@illinois.edu) is a visiting student under Prof. Gao in the Department of Aeronautics and Astronautics at Stanford. She is a Ph.D. candidate in the Department of Aerospace Engineering at the University of Illinois at Urbana-Champaign, where she also received her masters degree in 2017. She obtained her B.Tech. in Aerospace from the Indian Institute of Technology Bombay in 2015. Her research is related to developing robust and attack-resilient PNT solutions with applications to power systems, ground vehicles and UAVs.

Kyeong Jin Kim [SM'11] (kkim@merl.com) received the M.S. and Ph.D. degrees from the University of California, Santa Barbara, CA, USA, in 2000. Since 2012, he has been a Senior Principal Research Staff with the Mitsubishi Electric Research Laboratories, Cambridge, MA, USA. His research include transceiver design, resource management, scheduling in the cooperative wireless communications system, cooperative spectrum sharing system, physical layer secrecy system, and AI-based smart grid. Dr. Kim currently serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and a leading guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS: SPECIAL ISSUE ON SPATIAL MODULATION IN EMERGING WIRELESS SYSTEMS.

Hongbo Sun [SM'00] (hongbosun@merl.com) received a Ph.D. degree in Electrical Engineering from Chongqing University in Chongqing, China in 1991. Dr. Sun is currently a Senior Principal Research Scientist at Mitsubishi Electric Research Laboratories in Cambridge, Massachusetts, USA. His research interests include power system operation and control, power system planning and analysis, and smart grid applications.

Philip V. Orlik [SM'12] (porlik@merl.com) received the B.E. degree in 1994 and the M.S. degree in 1997 both from the State University of New York at Stony Brook. In 1999 he earned his Ph. D. in electrical engineering also from SUNY Stony Brook. In 2000 he joined Mitsubishi Electric Research Laboratories Inc. located in Cambridge, MA where he is currently the Manager of the Electronics and Communications Group. His primary research focus is on advanced wireless and wired communications, sensor/IoT networks. Other research interests include vehicular/car-to-car communications, mobility modeling, performance analysis, and queuing theory.