GPS Time Authentication against Spoofing via a Network of Receivers for Power Systems

Sriramya Bhamidipati Student Member, IEEE, Tara Yasmin Mina, Student Member, IEEE and Grace Xingxin Gao Senior Member, IEEE

Abstract—Due to the unencrypted structure of civil GPS signals, the timing information supplied to the PMUs in the power grid is vulnerable to spoofing attacks. We propose our GPS time authentication algorithm using a network of widely dispersed static receivers and their known positions. Without requiring the knowledge of the exact P(Y) code sequences, we cross-check for the presence of these encrypted codes across the receivers to detect spoofing attacks.

First, we perform pair-wise cross-correlation of the conditioned quadrature-phase, carrier wiped-off incoming signal across the receivers. Later, we utilize position-information aiding to estimate the expected time offset between the received P(Y) codes at different receivers. Thereafter, we authenticate each receiver by analyzing the weighted summation of the pairwise cross-correlation peak offset and magnitude across the receivers and their common satellites.

To validate our networked spoofing detection algorithm, we utilize four GPS receivers located in Idaho, Illinois, Colorado and Ohio. Under the presence of simulated spoofing attacks, namely signal-level spoofing and a record-and-replay attack, we demonstrate that our networked approach successfully detects these spoofing events with high probability.

I. INTRODUCTION

The push to modernize the U.S. power grid by recent legislation [1] has led to an increased investment in the installation of Phasor Measurement Units (PMUs). PMUs monitor the power grid by recording time-tagged voltage and current phasors at critical substations. In particular, the American Recovery and Reinvestment Act of 2009 [2] prompted the installation of over 1000 additional PMUs from a mere 166 before the legislation was passed. Fig. 1 shows the widely dispersed and geographically distributed network of PMUs [3] across the U.S.

To synchronize this network, each PMU timestamps the measured voltage and current phasors with the precise time estimated by a GPS receiver [4]. GPS has advantages of providing microsecond-level accuracy in estimating Universal Time Coordinated (UTC) time, has global coverage and is freely available to all users. However, because the civilian GPS signal structure and relevant code sequences are publicly available [5], the timing information supplied to PMUs is vulnerable to external spoofing attacks [6].

Some of the GPS spoofing attacks which threaten the stability of the power systems include:

1) Meaconing: A spooper executing a meaconing attack (also known as a record-and-replay) as seen in Fig. 2(a), records the GPS signals and replays them at a later time to overpower the authentic signals and manipulate the receiver [7]. To execute this attack, the spooper does not require knowledge of the encrypted codes and is capable of spoofing even military receivers.

2) Signal-level spoofing: This is a sophisticated three-stage attack as shown in Fig. 2(b). At first, a spooper generates and broadcasts counterfeit GPS signals identical to the authentic signals received at the target receiver [8]. In the second stage, the power of these malicious signals is slowly increased to mislead the target receiver to lock onto these counterfeit signals. Once locked, the spooper manipulates the time by moving the counterfeit signal away from the true time. Since there is no sudden change in the GPS timing output, this method cannot easily be detected by traditional methods.

Fig. 1: Geographically distributed PMUs deployed across the U.S to monitor the power grid stability [9].

Previous research [10]-[12] performed GPS signal authentication of a user receiver via cross-correlation of sampled military signals against a reference receiver. While the authors provided a strong validation of the concept, the cross-check relies on one reference receiver to be secure at all times. In case the reference receiver or the communication link is compromised, the spoofing detection is also compromised. Our prior work [13] has demonstrated an increased probability of signal-level spoofing detection for a general framework by utilizing a small number of distributed, low-cost receivers as opposed to one reference station.
In our current work, we cross-check the encrypted signature across a network of geographically distributed receivers to analyze the spoofing status of each receiver in the power systems. In addition, we utilize the known position of static GPS receivers to develop a two-stage authentication procedure which not only detects signal-level spoofing, that cannot generate P(Y) codes but also a record-and-replay attack, which transmits a delayed P(Y) code. We leverage the existing power grid resources, namely the secure communication channels and a centralized power grid monitoring system, to collectively cross-check the GPS snippets across receivers.

The rest of the paper is organized as follows: Section II describes our architecture and its key characteristics; Section III explains our networked spoofing detection algorithm in detail; Section IV experimentally validates the successful detection of simulated spoofing attacks, namely record-and-replay and signal-level spoofing, using four geographically distributed receivers; Section V concludes the paper.

II. OUR ARCHITECTURE

In this section, we describe the various aspects considered in our networked spoofing detection algorithm, as outlined in Fig. 3. Our proposed algorithm adds an additional protection layer to our prior proposed receiver algorithms [14]-[15] in providing robust GPS timing for PMUs. The key characteristics of our algorithm are as follows:

1. Widely dispersed network of receivers:
   By leveraging the geographically distributed architecture of the U.S power grid as described in Section I, we consider a handful (4-8) of GPS receivers situated at widely dispersed locations. This is because the probability of these widely dispersed receivers being spoofed by the same attacker and at the same time is minimal. In addition, this also eliminates the need for a secure receiver to be present as a reference for cross-checking.

2. Utilizing encrypted P(Y) codes:
   The presence of P(Y) codes in the quadrature-phase of L1 C/A GPS signals serves as a unique authentication signature that cannot be forged by a spoofer because of its encrypted nature. Without requiring the knowledge of these exact sequences, we utilize the conditioned GPS snippet to authenticate the receivers via pair-wise cross-correlations performed among a network of receivers.

Fig. 3: System architecture of our proposed approach. Our approach utilizes the component of the GPS signal consisting of encrypted military P(Y) codes as a unique authentication signature, without requiring knowledge of the exact P(Y) code sequences. We further take advantage of the existing communication network between PMU stations to leverage the geographical redundancy of multiple PMU sites.

3. Position Information Aiding:
   Given that each power substation is static, we pre-compute the position $X_k = [x, y, z]^{\text{known}}, k = 1, \ldots, M$ of our $M$ widely distributed network of receivers. The existing power grid network provides PMUs with satellite ephemeris data from external sources, thus we can utilize this available information to obtain the accurate satellite position $S_i = [x_s, y_s, z_s], i = 1, \ldots, N$ of the $N$ satellites in view. This position information aiding is especially useful in detecting a meaconed signal, which contains the P(Y) codes but at a delayed received time. By using the known receiver positions, we compute the expected offset between the received P(Y) codes at different PMU sites. The consistency between the expected offsets using position-information aiding and the computed offset for the pairwise cross-correlation peak is useful to detect a meaconing attack.

Fig. 4: In our centralized spoofing detection algorithm, a network of receivers send the P(Y) snippet at a requested time to the central unit, such as Phasor Data Concentrator (PDC). Later, the central unit collectively authenticates the spoofing status of all the receivers.

4. Centralized Platform for implementation:
   We implemented a centralized framework as shown in Fig. 4 for our networked spoofing detection based on several key advantages. A centralized architecture allows for less
computational complexity at each PMU as well as fewer communication links in the network overall. In addition, given that currently the phasor data is authenticated at a centralized platform known as PDC, we will be able to easily incorporate our algorithm in the existing power grid communication network.

III. NETWORKED SPOOFING DETECTION

In this section, we explain our networked spoofing detection algorithm in detail as shown in Fig. 5. Among the network of receivers being evaluated, we assume to have at least one common satellite in view for each receiver pair.

A. Conditioning of GPS signals

At the \( k^{th} \) receiver, the baseband GPS signal [16] received from the \( i^{th} \) satellite at time \( t \) is represented as

\[
s_i^j(t) = \Lambda_c^i(t) e^{j(2\pi f_d^i t + \phi_{L1}^i)} + j\Lambda_p^i(t) p^i(t - \tau_{d,k}^i) D^i(t - \tau_{d,k}^i) \sin(2\pi f_d^i t + \phi_{L1}^i)
\]

(1)

where \( \Lambda_c^i \) and \( \Lambda_p^i \) are the received signal power of the civilian \( C/A \) and military \( P(Y) \) components of the GPS L1 signal; \( D^i \) represents the navigation message with a bit rate of 50 bps for the \( i^{th} \) satellite; \( p^i \) is the \( C/A \) code sequence with a chip rate of \( f_{C/A} = 1.023 \text{ MHz} \) and \( P(Y) \) code sequence with a chip rate of \( f_{P(Y)} = 10.23 \text{ MHz} \); \( \phi_{L1}^i \) represents the carrier phase offset.

Fig. 5: Our networked GPS spoofing detection algorithm analyzes the pair-wise cross-correlation of the conditioned GPS snippets obtained from a network of receivers.

Even though the encryption is unknown, different geographically distributed receivers receive the same encrypted \( P(Y) \) codes and therefore a correlation peak across receivers is expected for the common satellites in view. By continuously tracking the GPS satellite signal, we compute an accurate estimate of the GPS signal parameters, namely the \( C/A \) code delay \( \tau_{d,k}^i \) and the carrier Doppler frequency \( f_d^i \). After the tracking loops converge, at the receiver level, we perform carrier wipe-off of the incoming GPS signal and later isolate the corresponding quadrature component to obtain the conditioned GPS snippet given by

\[
s_{P,k}^j[t] = I(s_{k}^j[t] \exp(-j2\pi f_{d,k} t - \phi_{L1}^i))
\]

\[
= \Lambda_{P,k}^i |p_k^i| D_k^i[t] + n_k[t]
\]

(2)

where \( t \in \{1, \ldots, T_{snip} \} \) represents the indices of samples considered with \( T_{snip} = L_{snip}/f_{C/A} \) and \( n_k[t] \) is the noise associated.

The length of the snippet \( L_{snip} \) required for cross-correlation is determined by the narrow front-end sampling frequency which attenuates the wide-band \( P(Y) \) signal. At a near-future receiver time requested by the central unit, the conditioned snippet mentioned in Eq. (2) is generated for all satellites in view at each receiver. These snippets are sent to the central unit for further processing.

B. Utilizing networked approach

Before performing pairwise cross-correlation we execute time alignment by utilizing various resources such as counting the GPS \( C/A \) code chips, synchronization infrastructure of power grid using precise time protocol services [17] and position-information aiding. Thereafter, we perform our networked spoofing detection analysis in the central unit as follows:

1. Cross-correlating the receivers pairwise:

The first step is to carry out pair-wise cross-correlations among each pair of receivers for each common satellite in view. For each receiver pair \((j, k)\), where \( j, k \in 1, \ldots, M \) and \( j \neq k \), and for the \( i^{th} \) commonly viewed, the pair-wise cross-correlation is computed as:

\[
c c_{j,k}^i[t] = \sum_{n=0}^{T_{snip}} s_{P,j}^i[n + t] \cdot \text{conj}(s_{P,k}^i[n])
\]

(3)

where given \( M \) receivers, \( \left( \begin{array}{c} M \\ 2 \end{array} \right) \) pair-wise cross-correlations are possible.

2. Evaluating the pair-wise spoofing decision:

Next, we analyze the characteristics of the pair-wise cross-correlation based on multiple hypothesis testing to detect the spoofing attacks. We define three hypothesis based on the characteristics of two test statistics i.e., pair-wise cross-correlation peak offset and magnitude:

- \( H_0 \) denotes the hypothesis that one or both the receivers do not contain the \( P(Y) \) code sequence which is observed through the absence of peak in the pair-wise cross-correlation.
- \( H_1 \) denotes the hypothesis that both the receivers contain the exact same \( P(Y) \) code which is observed through a strong centered peak present in the pair-wise cross-correlation.
- \( H_2 \) denotes the hypothesis that both the receivers contain \( P(Y) \) code but are shifted with respect to each other. This is observed through the presence of a strong off-centered peak in the pair-wise cross-correlation.

The foremost condition to be checked is the presence or absence of a correlation peak above a certain pre-defined
primary pair-wise threshold \((\max (cc^i_{1,k_2}[t]) > \zeta_p)\). If satisfied, the primary pair-wise statistic \(B^i_{k_1,k_2}\) is voted one. If the condition is not satisfied, \(B^i_{k_1,k_2}\) is voted zero in accordance with \(H_0\) hypothesis. This indicates the absence of the authentic P(Y) code in one or both of the receivers which may be due to the spoofing attacks, namely signal-level spoofing.

3. Aggregating across satellites and receivers:

In the third step, for each \(k^{th}\) receiver, we aggregate the primary pair-wise statistic obtained from the network of receivers and the corresponding common satellites in view \(N_n\) for each pair as

\[
B_k = \sum_{n=0,n \neq k}^{M} \sum_{i=0}^{N_n} w^i_n C^i_{k,n} \tag{4}
\]

where \(w^i_n = f(SNR^i_n, SNR^i_{n,n}, cc^i_{n,n}) \ast g(X_k, X_n, S^i)\).

Moreover, we perform weighted summation across satellites and receivers \(w^i_k\) to obtain a more accurate primary cumulative statistic \(B_k\). While summing across satellites, higher weight \(f(.)\) is given to the satellites with the highest pair-wise cross-correlation magnitude, elevation and Signal-to-Noise Ratio (SNR) as they experience lower signal blockage and atmospheric effects. Whereas in case of summation across receivers, higher weight \(g(.)\) is given to the receiver pair with large enough separation distance so as to minimize the cross-talk between channels [18].

TABLE I: Evaluating the cumulative pair-wise cross-correlation to obtain primary and secondary spoofing decisions for each receiver.

<table>
<thead>
<tr>
<th>Cumulative Statistic</th>
<th>Spooing status of (k^{th}) receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Secondary</td>
</tr>
<tr>
<td>(B_k &lt; \eta_p)</td>
<td>-</td>
</tr>
<tr>
<td>(B_k \geq \eta_p)</td>
<td>Spooed: absence of P(Y) code</td>
</tr>
<tr>
<td>(B_k \geq \eta_s)</td>
<td>Meaconed: shifted P(Y) code</td>
</tr>
<tr>
<td>(B_k \geq \eta_s)</td>
<td>Not spoofed: centered P(Y) code</td>
</tr>
</tbody>
</table>

4. Evaluating the cumulative spoofing decision:

If our primary cumulative statistic for a particular \(k^{th}\) receiver is less than a pre-defined primary cumulative threshold \(\eta_p\), i.e., \(B_k < \eta_p\), then a spoofing decision of boolean true is transmitted back to that receiver as seen in Table I.

However, if our statistic \(B_k \geq \eta_p\), then further analysis is carried out to ascertain its spoofing status and verify that the receiver is not experiencing a meaconing attack. To do this, we evaluate the expected offset between two receivers based on position-information aiding using

\[
\Delta t^i_{j,k} = |\Delta t^i_{j} - \Delta t^i_{k}| \tag{5}
\]

where \(j \in \{1, \ldots, M\} \forall j \neq k\).

We evaluate another important metric from the pair-wise correlation which is the peak offset i.e., \(\arg\max (cc^i_{j,k}[t])\). We evaluate if this following condition is satisfied i.e., \(\left( \arg\max (cc^i_{j,k}[t]) - \Delta t^i_{j,k} \right) < \zeta\), where \(\zeta\) is the secondary pair-wise threshold. The violation of the above condition indicates the presence of a meaconing attack, since the relative time delay between the signals received from the \(j^{th}\) satellite at the \(j^{th}\) and \(k^{th}\) receivers, is significantly greater than what is expected. Therefore, if the condition is true, the secondary pair-wise statistic \(C^i_{j,k}\) is voted one, thereby satisfying the \(H_1\) hypothesis. If found to be false, \(C^i_{j,k} = 0\), satisfying \(H_2\) hypothesis.

Lastly, a cumulative summation is performed for each of the receivers as

\[
C_k = \sum_{n=0,n \neq k}^{M} \sum_{i=0}^{N_n} \left( w^i_n C^i_{k,n} \right) \tag{6}
\]

where \(C_k\) is the secondary cumulative statistic evaluated at each receiver in the network i.e., \(k \in \{1, \ldots, M\}\). Also, \(\eta_s\) is the pre-defined secondary cumulative threshold. Finally, if \(C_k \geq \eta_s\), then a boolean decision of the \(k^{th}\) receiver being authentic is sent back to the receiver. However, if \(C_k < \eta_s\), then a boolean decision of the \(k^{th}\) receiver is being meaconed is sent back.

IV. EXPERIMENTS AND RESULTS

In this section, we demonstrate the successful detection of several simulated spoofing attacks using our spoofing detection algorithm, by performing collective time authentication across a geographically distributed network of receivers.

A. Experimental setup

Our experimental setup consists of four GPS stations located in Idaho, Illinois, Colorado and Ohio respectively as shown in Fig. 6. Each station is equipped with a Trimble Z plus antenna as seen in Fig. 7, external chip scale atomic clock Microsemi Quantum SA.45s CSAC and Universal Software Radio Peripheral (USRP-N210) to collect the data.

![Fig. 6: Four geographically distributed receivers are considered at Mountain Home, Idaho; Boulder, Colorado; Champaign Illinois and Cleveland, Ohio.](image)

We collected data at a sampling rate of 2.5 \(MHz\) with 32-bit samples for Idaho and Illinois and 8-bit samples for Colorado and Ohio respectively. We simulated the spoofing attacks and post-processed the collected raw GPS signals using our pyGNSS [19] platform, a Python based object-oriented framework.
We pre-compute the locations of the static receivers using multi-receiver vector tracking [20] and use them for position-information aiding. We generate the conditioned GPS snippets by performing scalar tracking and we evaluate the robustness of our algorithm in detecting spoofing attacks for this conventional GPS scalar tracking approach.

### B. Intermediate results

In authentic conditions, the pair-wise cross-correlation of the time aligned conditioned GPS snippets between Illinois and Colorado, \(512 \text{ ms} \) long is shown in Fig. 8. We observe a strong single centered peak which indicates the presence of the same P(Y) code sequence at both the receivers.

![Fig. 8: Pair-wise cross-correlation peak of satellite PRN 31 across Illinois and Colorado receivers. Centered cross-correlation peak indicates the presence of authentic P(Y) code sequence.](image)

We also conducted additional analysis to evaluate the trend of the Peak-to-Noise Ratio (PNR) by varying the snippet length considered as seen in Fig. 9. Here, we can observe that by cross-correlating \(128 \text{ ms} \) snippet, the PNR is \(1.2 \text{ dB} \) which increases to \(2 \text{ dB} \) for a snippet length of \(512 \text{ ms} \).

### C. Under signal-level spoofing

We simulated signal-level spoofing by generating counterfeit signals that deviated from the authentic C/A code at 0.01 \(\text{ms/s} \). It is separately verified that under this simulated spoofing attack, the traditional scalar tracking locked onto the malicious signals and estimated inaccurate time thereby violating the IEEE C37.118.1 standards for PMU timing accuracy [21].

These simulated spoofing attacks were added to the data collected at Idaho receiver. We authenticated the Illinois receiver which is authentic and Idaho receiver which is being spoofed by using a network of four cross-check receivers and six pair-wise cross-correlations.

In Fig. 10, we observed that the value of primary cumulative statistic \(B_k\) of our Illinois receiver denoted by the blue line, with average of 0.0156, is greater than the threshold \(\eta_p = 0.003\). However, for Idaho receiver denoted by the red line in the presence of spoofing, the value of \(B_k < \eta_p\) and showed an average of 0.001. This is because when the scalar tracking locked onto the malicious signals, which does not include the authentic P(Y) component and hence no cross-correlation peak as seen in Fig. 11. Therefore, we demonstrated successfully detection signal-level spoofing attacks using our networked spoofing detection algorithm.

![Fig. 10: Variation in the primary cumulative statistic \(B_k\). The dotted black line denotes the primary cumulative threshold \(\eta_p = 0.003\). The blue line represents the authentic Illinois receiver \(B_k > \eta_p\) while the red line represents the spoofed Idaho receiver \(B_k < \eta_p\). Our algorithm successfully detected the occurrence of signal-level spoofing attack in Idaho.](image)

**D. Under meaconing**

At the Idaho GPS receiver, we added simulated meaconing signals of 3 \(\text{dB} \) higher power than the authentic signals that induced an error 0.5 \(\text{ms} \) in time. In this scenario, we compared both the cumulative statistics i.e., primary \(B_k\) and secondary \(C_k\) of meaconed Idaho receiver data and authentic Illinois data.
we demonstrated an increased resilience in the GPS timing supplied to the PMU devices.

**ACKNOWLEDGMENT**

This material is based upon work supported by the Department of Homeland Security under contract number HSHQDC-17-C-B0025 and the applicable copyright notice of 17 U.S.C. 401. In addition, the authors would like to thank their lab members at the University of Illinois: Arthur Chu and Cara Yang for helping with the experimental setup and data collection.

**REFERENCES**


**Biographies**

**Sriramya Bhamidipati** is a doctoral student in the Aerospace Engineering Department at the University of Illinois at Urbana-Champaign. She received her M.S degree in Aerospace Engineering from University of Illinois at Urbana-Champaign in 2017. She received her B.Tech. with honors in Aerospace Engineering and minor in Systems and Controls Engineering from Indian Institute of Technology Bombay, India in 2015.

**Tara Yasmin Mina** is a graduate student in the department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. She received her B.S. degree in Electrical Engineering from Iowa State University in 2017.

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