Detecting GPS Spoofing via a Multi-Receiver Hybrid Communication Network for Power Grids

Tara Mina, Sriramya Bhamidipati, and Grace Xingxin Gao
Goals for Power Grid Modernization

- **Automatic control** of power grid
- **Reduce failures** or large-scale blackouts (Ex: NE Blackout 2003)
- Improve visualization of power flow
- **Continuously monitor state** of U.S. power grid network
- Install robust **network of monitoring devices** across the grid
Synchronizing Data in Power Grid Network

Real-time monitoring of power grid through a widely dispersed network of Phasor Measurement Units (PMUs)
- PMUs measure voltage and current phasors
- Provides measurement with precise time-stamp, via GPS
- Significant timing inaccuracies can induce a generator to trip [1]

Global Positioning System (GPS)

- Number of satellites: 31 operational
- Orbit: $\approx 20,200 \text{ km}$ in altitude ($\approx 12 \text{ hr}$ period orbit)
- Each satellite:
  - Carries several **atomic clocks** (Cesium and/or Rubidium)
  - Continuously sends precisely timed signals to Earth
How GPS Enables Navigation

- Precise **satellite position** \((X_S, Y_S, Z_S)\) provided to user
- After receiver obtains the satellite signal:
  - Deciphers exact **time of transmission** \(t_{TX}\) of received signal
  - Notes **user’s received time** \(t_{RX}\), and compares to compute distance from the satellite

\[
d = c (t_{RX} - t_{TX})
\]

\((X_S, Y_S, Z_S)\)

\((X_R, Y_R, Z_R)\)
How GPS Enables Navigation

- Precise satellite position \((X_S, Y_S, Z_S)\) provided to user
- After receiver obtains the satellite signal:
  - Deciphers exact time of transmission \(t_{TX}\) of received signal
  - Notes user’s received time \(t_{RX}\), and compares to compute distance from the satellite

\[
d = c (t_{RX} - t_{TX})
\]
How GPS Enables Navigation

- Precise **satellite position** \((X_S, Y_S, Z_S)\) provided to user
- After receiver obtains the satellite signal:
  - Deciphers exact **time of transmission** \(t_{TX}\) of received signal
  - Notes **user’s received time** \(t_{RX}\), and compares to compute distance from the satellite

\[
d = c (t_{RX} - t_{TX})
\]

But, user’s clock is not accurate…

\[\rightarrow t_{RX} \text{ is inaccurate}\]
How GPS Enables Navigation

- Precise **satellite position** \((X_S, Y_S, Z_S)\) provided to user
- After receiver obtains the satellite signal:
  - Deciphers exact **time of transmission** \(t_{TX}\) of received signal
  - Notes user’s received time \(t_{RX}\), and compares to **roughly approximate** distance from the satellite

\[
d \approx c (t_{RX} - t_{TX})
\]
How GPS Enables Navigation

- Precise satellite position \((X_S, Y_S, Z_S)\) provided to user
- After receiver obtains the satellite signal:
  - Deciphers exact time of transmission \(t_{TX}\) of received signal
  - Notes user’s received time \(t_{RX}\), and compares to roughly approximate distance from the satellite

"Pseudo" because:
Receiver clock is inaccurate
\(\rightarrow t_{RX} \) is inaccurate
\(\rightarrow c(t_{RX} - t_{TX}) \neq d\) (true range)
How GPS Enables Navigation

• Precise satellite position \((X_S, Y_S, Z_S)\) provided to user
• After receiver obtains the satellite signal:
  - Deciphers exact time of transmission \(t_{TX}\) of received signal
  - Notes user’s received time \(t_{RX}\), and compares to roughly approximate distance from the satellite

\[d = c \left( t_{RX} - t_{TX} + \Delta t \right)\]

receiver clock bias correction
How GPS Enables Navigation

- User has **4 unknowns**:  
  - 3D Position \((X_R, Y_R, Z_R)\)  
  - Clock bias \((\Delta t)\)

- Require **at least 4 equations**, or satellites in view  
  (usually \(\geq 6\) in open environments)

- For **each satellite signal**, we have **1 equation**:

\[
\rho = c(t_{RX} - t_{TX}) = d - c \Delta t \\
= \sqrt{(X_S - X_R)^2 + (Y_S - Y_R)^2 + (Z_S - Z_R)^2} - c \Delta t
\]
Civilian GPS and its Vulnerability

• Commercial (non-military) users utilize civilian GPS signal

• Civilian GPS signal (C/A) in L1 band:
  - Center frequency: 1575.42 MHz
  - Bandwidth: 2.046 MHz
  - Available to all users

<table>
<thead>
<tr>
<th>GPS Advantages for Power Grid</th>
<th>GPS Disadvantages for Power Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provides global coverage</td>
<td>• Freely available</td>
</tr>
<tr>
<td>• Sub-μs level timing accuracy</td>
<td>• Vulnerable to spoofing: attacker forges GPS signal to falsify receiver’s position and/or time</td>
</tr>
<tr>
<td>• Freely available</td>
<td></td>
</tr>
</tbody>
</table>
Military Signals for Authentication

Encrypted Military P(Y) GPS signal
- Orthogonal to civilian GPS signals, with same center frequency
- Because of encryption, cannot be generated by spoofer
- Presence of P(Y) signal in quadrature phase component indicates authentic GPS signal [2-3]

Prior Work and Main Challenges

- Shown handful of receivers (2-8) can be authenticated \[4\]
- Utilized centralized framework approach \[5\]
- Must extend to entire widespread network of PMUs

---

[5] Bhamidipati, Mina & Gao, ION PLANS, 2018
Key Objectives

- Develop spoofing detection architecture for coordinated authentication of all PMUs, with existing resources
- Provide defense against coordinated spoofing attacks
- Demonstrate successful operation of algorithm during government-sponsored, real-world spoofing scenario
Outline

• GPS: How it Works
• Hybrid Network Architecture Framework
• Spoofing Detection Approach
  − Pairwise Check and Preliminary Statistic Computation
  − Regionally Representative Snippet
• Implementational Considerations
  − Communication Protocol
  − Spoofing Risk Assessment
  − Subset Selection Algorithm
• Experimental Setup and Results
• Summary
NASPInet Communication Structure

- North American Synchrophasor Initiative network (NASPInet) [9]
- Regional utility networks connected via Data Bus
- Resources prioritized in regional sub-networks

Hierarchical Architecture Network

- Utilize communication to compare received GPS signals
- Proposed hybrid architecture network will overlay NASPInet
High-level Process Diagram

1. Snippets and Signal Params. from PMUs
2. Snippet conditioning and Pairwise Cross-correlation
3. Compute Preliminary Spoofing Decisions
4. Create a Regionally Representative Snippet
5. Pairwise Cross-correlation with Distant Snippets
6. Compute Final Spoofing Decisions

Regional PMU Network

Data Bus to Wide-Area Distributed Network of PDCs

Snippets from PMUs in Regional Network

Representative Snippets from distant PDCs

Phasor Data Concentrator

University of Illinois at Urbana-Champaign
Outline

• GPS: How it Works
• Hybrid Network Architecture Framework
• Spoofing Detection Approach
  - Pairwise Check and Preliminary Statistic Computation
  - Regionally Representative Snippet
• Implementational Considerations
  - Communication Protocol
  - Spoofing Risk Assessment
  - Subset Selection Algorithm
• Experimental Setup and Results
• Summary
Typical Correlation Observed (Authentic)

Typical correlation (authentic): **single peak** above noise floor
Typical Correlation Observed (Spoofed)

Quadrature-Phase Correlation between Western U.S. Receiver (30.2 deg) and Ohio (57.1 deg) (PRN 14)

Typical correlation (spoofed): no peak above noise floor
Pairwise Statistic for Cross-Checking

- Correlation result $P_{ri,rj,k}$ between receivers $r_i$ and $r_j$ for PRN $k$:
  - Authentic: $P_{ri,rj,k} \sim p_0 = \mathcal{N}(\mu, \sigma^2)$ where $\mu > 0$
  - Spoofed: $P_{ri,rj,k} \sim p_1 = \mathcal{N}(0, \sigma^2)$

- Pairwise statistic $\gamma_{ri,rj,k}$:
  - Indicates amount of signal match for PRN $k$ between receivers $r_i$ and $r_j$
  - Consists of 2 terms:
    - Thresholded correlation result: $P^T_{ri,rj,k} = P_{ri,rj,k} \mathbb{1} \{P_{ri,rj,k} \geq \tau_{pair}\}$
    - Pairwise weight $w_{ri,rj,k}$, accounts for signal quality, receiver reliability, etc.
      
      $$\gamma_{ri,rj,k} = w_{ri,rj,k} \left(P^T_{ri,rj,k}\right)$$
Authentication within Regional Network

\[ \mathcal{V}_{r_i r_j, k} \quad \text{Pairwise Statistic between receivers } r_i \text{ and } r_j \text{ for PRN } k \]

\[ A_{r_i, k} \quad \text{Statistical Contribution of PRN } k \text{ for receiver } r_i \]

\[ A_{r_i} \quad \text{Preliminary Spoofing Statistic for receiver } r_i \]

\[ A_{r_i, k} = \sum_{j \neq i} \mathcal{V}_{r_i r_j, k} \]

\[ A_{r_i} = \sum_{k} A_{r_i, k} \]

Above Preliminary Threshold? [Yes/No]

Preliminary Conclusion: Authentic [Yes]

Preliminary Conclusion: Spoofed [No]

Create Regionally Representative Snippets (for each PRN)

To distant networks
Incorporate Representative Snippets

- **$A_{r_i}$**
  - **Preliminary Conclusion:** Authentic
    - **Yes**
      - Create Regionally Representative Snippets (for each PRN)
      - Pairwise Cross-Correlate
      - Compute PNR
      - Aggregate Results
      - Moving Average Filter
      - **Yes**
        - Above Secondary Threshold?
        - **Yes**
          - **Confirmed Authenticity**
        - **No**
          - **Confirmed Lack of Authenticity**
    - **No**
      - **Coordinated Spoofing**

- **$A_{r_i,k}$**
  - Statistical Contribution of PRN $k$ for receiver $r_i$
  - **$A_{r_i}$**
    - Preliminary Spoofing Statistic for receiver $r_i$

- **Representative Snippets**
  - Send to Distant Networks
  - Representative Snippets from distant networks
Outline

• GPS: How it Works
• Hybrid Network Architecture Framework
• Spoofing Detection Approach
  - Pairwise Check and Preliminary Statistic Computation
  - Regionally Representative Snippet
• Implementational Considerations
  - Communication Protocol
  - Spoofing Risk Assessment
  - Subset Selection Algorithm
• Experimental Setup and Results
• Summary
Data Required for Communication Protocol

Data items to be sent by each PMU:

- Raw GPS signal fragment
- Signal tracking parameters for each visible satellite PRN
  - Time of transmission start index
  - Doppler Frequency
  - Carrier phase

Starting index
(transmission time for PRN \( k \))

\[ N = \frac{T_{\text{snip}}}{\tau_{\text{track}}} \]

\[
\begin{bmatrix}
  \phi^k[0] & \phi^k[1] & \phi^k[2] & \ldots & \ldots & \phi^k[N-1] & \phi^k[N]
\end{bmatrix}
\]

Carrier frequency and carrier phase estimates (from scalar tracking)
Communication Protocol Structure

- **Data block**: data for each *authentication time*
- **Data Packet**: ~1 KB of specific data with header information
- **Data Frame**: organizes data into segments, includes check sum

Segmented data structure allows for:
- Isolation of corrupted/missing data
- Optimized rate of data transfer and storage
Bandwidth Requirements

• Reducing communication bandwidth requirements:
  − Raw GPS signal fragment sent from PMU devices to PDC
  − Appropriate signal tracking parameters sent for processing

• Main factors affecting overall bandwidth:
  − Signal fragment length (500 milliseconds)
  − Sampling rate (2.5 MHz)
  − Data sample resolution (8-bit samples)
  − Tracking parameter resolution (32-bit samples)
  − Number of visible satellite PRNs (about 6)
  − Desired rate of authentication (assuming 1 per minute)

• Bandwidth computed: ~23 KB per second

• Fiber optic cable: ~10 GB per second ( < 0.001% bandwidth)
Evaluation of Spoofing Risk

- Known position
  - Pseudorange residuals
    - Chi-squared distribution
    - $p(r_t | \Delta \rho_{1:N})$

- Local oscillator
  - Clock residuals
    - Bernoulli distribution
    - $p(r_t | \Delta T)$

- SNR values
  - Empirical distribution
    - $p(r_t | SNR_{1:N})$

- Historical data
  - Weighted average
    - $p(r_t | r_{t-1:t-w})$

Spoofing risk

- $p(r_t)$
Optimization: Subset Selection

- For cross-checking:
  - Utilizing all PMUs, quite computationally expensive
  - Optimal subset of PMUs
- Cost function:
  \[ f(\Omega) = \sum_{i,j \in \Omega; i \neq j} g(i)g(j)h(i,j) \]
- \( g(i) = (1 - \text{spoofing risk}) \ast \text{comm. link} \ast \text{security} \)
- \( h(i,j) = \text{dist}(i,j) \): Larger the separation, lesser likelihood of both spoofed
Outline

• GPS: How it Works
• Hybrid Network Architecture Framework
• Spoofing Detection Approach
  − Pairwise Check and Preliminary Statistic Computation
  − Regionally Representative Snippet
• Implementational Considerations
  − Communication Protocol
  − Spoofing Risk Assessment
  − Subset Selection Algorithm
• Experimental Setup and Results
• Summary
Experimental Setup

Recorded GPS signal during live-sky spoofing event

Sample rate: 2.5 \( MHz \)
Snippet length: 500 ms
Post-process: \textit{PyGNSS} \cite{10}

\cite{10} Wycoff & Gao, GPS World, 2015
Preliminary Threshold Determination

Generalized Gamma pdf:

\[
f(x, \alpha, c, \beta, l) = \frac{|c| \gamma^c \alpha^{-1} \exp(-\gamma^c)}{\gamma(\alpha)}
\]

\[y = \beta(x - l)\]

Authentic:
\[
\begin{align*}
\alpha &= 27.2 \\
c &= 0.517 \\
\beta &= 1.82 \\
l &= 486
\end{align*}
\]

Spoofed:
\[
\begin{align*}
\alpha &= 11.3 \\
c &= 0.370 \\
\beta &= 0.346 \\
l &= 0
\end{align*}
\]

Threshold chosen to maximize authentic / spoofed conditional probabilities
Preliminary Statistics – Regional Networks

Preliminary Statistic Computed During Spoofing Event for U.S. Regional Network

Preliminary Statistic Computed During Spoofing Event for South American Regional Network
**Secondary Threshold Determination**

Generalized Gamma pdf:

\[
f(x, \alpha, c, \beta, l) = \frac{|c|y^{c\alpha-1}\exp(-y^c)}{\gamma(\alpha)} \\
y = \beta(x - l)
\]

Authentic:
- \( \alpha = 1.53 \)
- \( c = 1.74 \)
- \( \beta = 33.7 \)
- \( l = 20.0 \)

Spoofed:
- \( \alpha = 1.18 \)
- \( c = 2.69 \)
- \( \beta = 5.80 \)
- \( l = 13.7 \)

*Threshold chosen to maximize authentic / spoofed conditional probabilities*
Final Statistic – Representative Snippets

- U.S. representative snippet matches that of South America
- Snippet at Western U.S. receiver (spoofed) has poor match
Summary

- Proposed hybrid architecture to detect spoofing at each PMU
  - Provides a defense against coordinated attacks on regional networks
  - Uses regionally representative snippets to reduce bandwidth/processing

- Demonstrated algorithm successfully operates on wide-spread network during government-sponsored, real-world spoofing attack
  - Detects signal manipulation on victim receiver
  - Simultaneously authenticates other receivers in hybrid network
Acknowledgements

Special thanks to:

Prof. Jade Morton and Mr. Steve Taylor
for collecting data at the Peru, Chile, Colorado, and Ohio sites.

Additionally, thanks to our lab members:

Craig Babiarz, Arthur Chu, Matthew Peretic, and Cara Yang
for assisting with the experimental setup and data collection at the Illinois site and the Western U.S. spoofing location.
Thank You!

Tara Yasmin Mina
Electrical and Computer Engineering
Email: tymina2@illinois.edu

Sriramya Bhamidipati
Aerospace Engineering
Email: sbhamid2@illinois.edu