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

Tara Mina, Sriramya Bhamidipati, and Grace Xingxin Gao
Use of Synchronized Data in Power Grid

- Power grid state monitored by Phasor Measurement Units (PMUs)
  - Use civilian GPS for synchronization – vulnerable to spoofing
- Significant timing inaccuracies can induce generator trip [1]
- Potential cascading failure, similar to Northeastern Blackout 2003 [2]

Prior Work and Main Challenges

- Presence of encrypted military P(Y) code for authentication [4-5]
- Shown handful of receivers (2-8) can be authenticated [6]
- Utilized centralized framework approach [7]
- Must extend to entire widespread network of PMUs

Heng, Work & Gao, IEEE ITS, 2015
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

• Hybrid Network Architecture Framework

• Spoofing Detection Algorithm
  - Computing Preliminary Spoofing Statistic
  - Generating Regionally Representative Snippets
  - Determining Final Spoofing Decision

• 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

Snippets and Signal Params. from PMUs

Snippet conditioning and Pairwise Cross-correlation

Compute **Preliminary** Spoofing Decisions

Create a **Regionally Representative** Snippet

Pairwise Cross-correlation with Distant Snippets

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
Outline

• Hybrid Network Architecture Framework
• Spoofing Detection Algorithm
  – Computing Preliminary Spoofing Statistic
  – Generating Regionally Representative Snippets
  – Determining Final Spoofing Decision
• Experimental Setup and Results
• Summary
Authentication within Regional Network

\[ \gamma_{r_ir_j,k} \] – Pairwise Statistic between receivers \( r_i \) and \( r_j \) for PRN \( k \)

\[ A_{r_i,k} \] – Statistical Contribution of PRN \( k \) for receiver \( r_i \)

\[ A_{r_i} \] – Preliminary Spoofing Statistic for receiver \( r_i \)

\[ A_{r_i,k} = \sum_{j \neq i} \gamma_{r_ir_j,k} \]

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

Preliminary Conclusion: Authentic

Preliminary Conclusion: Spoofed

Create Regionally Representative Snippets (for each PRN)

To distant networks
Incorporate Representative Snippets

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

- Preliminary Conclusion: Spoofed
  - Pairwise Cross-Correlate
    - Compute PNR
    - Aggregate Results
    - Moving Average Filter
  - Above Secondary Threshold?
    - Yes: Confirmed 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 $r_i$
Outline

• Hybrid Network Architecture Framework
• Spoofing Detection Algorithm
  − Computing Preliminary Spoofing Statistic
  − Generating Regionally Representative Snippets
  − Determining Final Spoofing Decision
• 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: PyGNSS


Spoofing Data Collection Setup

Rooftop Antenna Setup
Typical Correlation Plots Observed

Quadrature-Phase Correlation between Colorado (71.1 deg) and Ohio (51.1 deg) (PRN 22)

Typical correlation: single peak above noise floor
Authentication despite Noisy Correlation

Quadrature-Phase Correlation between Pachon, Chile (79.3 deg) and Tololo, Chile (79.2 deg) (PRN 10)

Can utilize knowledge of tracking accuracy to pick peak through noise
Verifying Spoofing despite Noisy Correlation

Quadrature-Phase Correlation between Western U.S. Receiver (79.3 deg) and Colorado (71.1 deg) (PRN 22)

Using tracking accuracy avoids choosing noisy result during spoofing
Preliminary Threshold Determination

Threshold chosen to maximize authentic / spoofed conditional probabilities

Generalized Gamma Distribution pdf:

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

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

Authentic:
\[ \alpha = 27.2 \quad \beta = 1.82 \quad l = 486 \]
\[ c = 0.517 \]

Spoofed:
\[ \alpha = 11.3 \quad \beta = 0.346 \]
\[ c = 0.370 \quad l = 0 \]
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

Spoofed

Authentic

Threshold

University of Illinois at Urbana-Champaign
Secondary Threshold Determination

Generalized Gamma Distribution pdf:

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

Authentic:
\[
\begin{align*}
\alpha &= 1.53 \\
c &= 1.74 \\
\beta &= 33.7 \\
l &= 20.0
\end{align*}
\]

Spoofed:
\[
\begin{align*}
\alpha &= 1.18 \\
c &= 2.69 \\
\beta &= 5.80 \\
l &= 13.7
\end{align*}
\]

Threshold chosen to maximize authentic / spoofed conditional probabilities
• **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
  - Use 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
University of Illinois at Urbana-Champaign
Email: tymina2@illinois.edu
Typical Spoofed Cross-correlation
Modeling Communication Delays

- Inherent delay due to overhead, may be different for each PMU
- Given: probability distribution of communication delay between PMU and PDCs
- Assumption: Each additional delay is an iid random variable for each PMU in the network
- Can determine CDF of time to receive all snippets from regional network

\[
P\{T \leq t\} = P\{ (X_1 \leq t - t_1) \cap (X_2 \leq t - t_2) \cap \cdots \cap (X_M \leq t - t_M) \}\]

\[
P\{T \leq t\} = \prod_{i=1}^{M} P\{X_i \leq t - t_i\} \]
Processing Time Required

- Inherent delay due to overhead, may be different for each PMU
- Given: $M$ devices in regional network, $k_i$ satellites observed at $i^{th}$ PMU, $L$ servers at central unit each with mean service rate of $\mu$
- Assumption: Poisson process for snippet arrivals, at rate $\lambda$
- Utilization factor (fraction of time each server is busy processing):
  \[ \rho = \frac{\lambda}{L \mu} \]
- Expected time to condition all snippets:
  \[ \left( \sum_{i=1}^{M} \sum_{j=1}^{k_i} \frac{1}{\mu} \right) \cdot \left( \frac{\rho}{L} \right) = \sum_{i=1}^{M} \sum_{j=1}^{k_i} \frac{\lambda}{L^2 \mu^2} \]
Preliminary Statistics – Regional Networks

Generate U.S. Representative Snippet

Generate S.A. Representative Snippet

Spoofed