nano-tera.ch

swiss scientific initiative in health / security / environment systems

SmartGrid RTD 2013

# Undetectable PMU Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation


S. Barreto, M. Pignati, G. Dan, M. Paolone, J.-Y. Le Boudec

LCA2, DESL - EPFL

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE


## Context

- **Synchrophasor measurements are vulnerable to timing attacks**:
  - GPS → Spoofing a GPS signal
  - PTP/White Rabbit →Inserting an asymmetric delay unknown to the protocol.

⚠ **Can we change the state of the network by just attacking the reference time of a subset of PMUs, undetectable by residual analysis?**

## System Model

- 1-ph direct-sequence model of a transmission network with ***N*** buses.
- Only PMU measurements (voltage or current).
- ***M*** measurements, measurement vector ***z*** in $C^N$.

## Attack Model

- Attacker knows ***Y*** and ***H*** matrices.
- He manipulates ***p*** different time references with $\boldsymbol{\alpha_i}$ different attack-angles *(i=1:p)*.
- The attacker applies each $\boldsymbol{\alpha_i}$ attack-angle to a subset of PMUs *(**$A_i$**)*.

✔ We use linear algebra with complex numbers to derive a close-form expression, and compute the attacking angles when *p=2*.

$$\alpha_1 = 2\arg(W_{1,1}+W_{1,2}) (\bmod 2\pi)$$
$$\alpha_2 = -2\arg(W_{1,2}) + 2\arg(W_{1,1}+W_{1,2}) (\bmod 2\pi)$$

$$\begin{cases} W_{i,j} = \sum_{l,m,n\in\mathcal{M}} \Psi_{l,i}\Psi_{m,j}\bar{F}_{n,l}F_{n,m}\bar{z}_l z_m \\ \Psi_{m,i} = 1 \text{ if } m \in \mathcal{A}_i \text{ and } \Psi_{m,i} = 0 \text{ otherwise} \\ F \triangleq H(H^\dagger H)^{-1}H^\dagger - I \end{cases}$$

✔ The expression for $\alpha$ **requires** the ***W* matrix** to be low rank (**rank-1**).

✔ We use the index of separation (***IoS***) of the W matrix to **derive an easy-to-do test** to **find vulnerable spots** to attack, **regardless of the state of the grid**

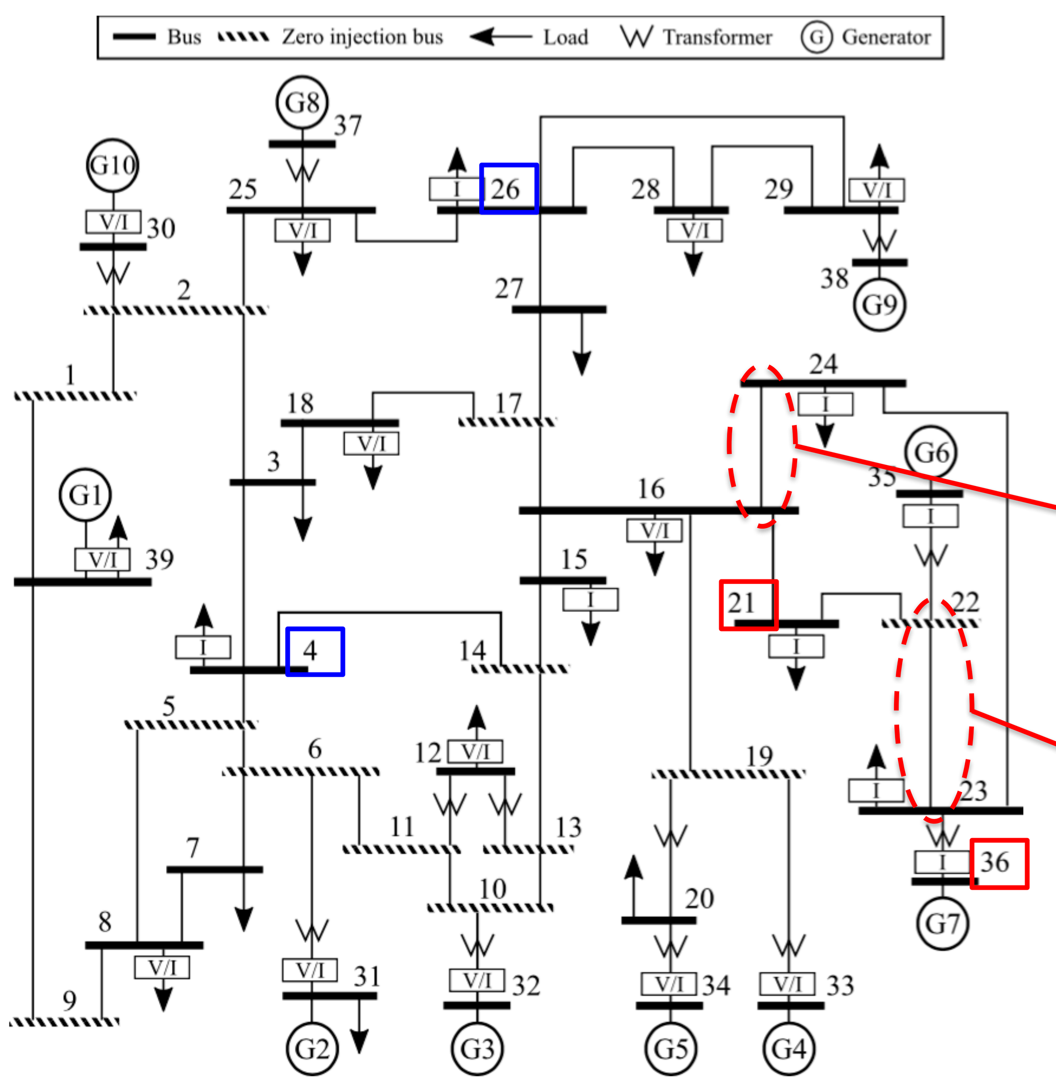
$$\text{IoS} = \frac{\lambda_{\max}}{\sum_i \lambda_i} = \frac{\Lambda_{1,1}}{\Lambda_{1,1}+\Lambda_{2,2}} \Rightarrow IoS^* = \frac{1}{2} + \frac{|f_{12}|}{2\,(f_{11}f_{22})^{\frac{1}{2}}} \Rightarrow f_{i,j} = \sum_{l,m}\sum_{n} \Psi_{l,i}\Psi_{m,j}\bar{F}_{n,l}F_{n,m}$$

## Results

We applied *IoS** equation to all possible combination of attack locations to discover undetectable spots

Attack-location combinations

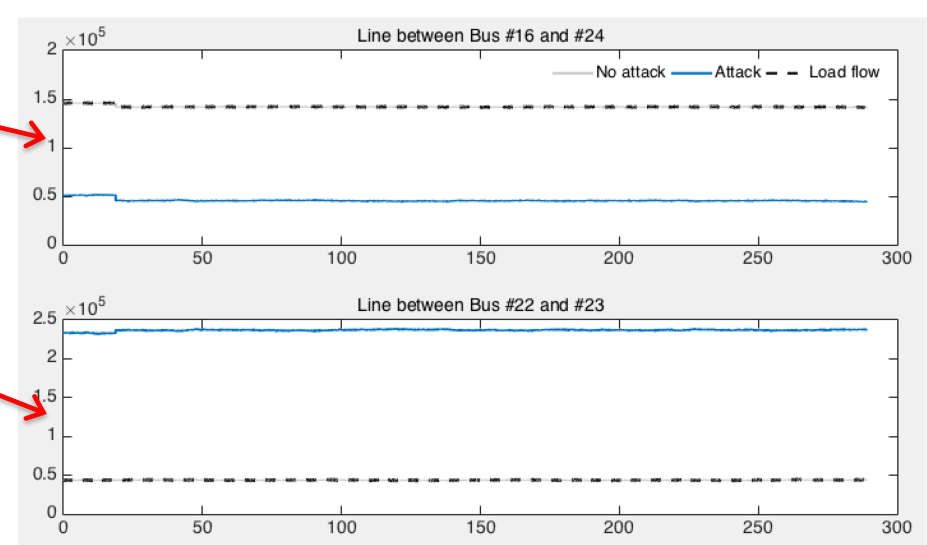
| Bus PMU1 | Bus PMU2 | IoS* | Bus PMU1 | Bus PMU2 | IoS* |
|---|---|---|---|---|---|
| 4 | 15 | 0.8437 | 21 | 24 | 1.0000 |
| 4 | 21 | 0.6613 | 21 | 26 | 0.8395 |
| 4 | 23 | 0.6613 | 21 | 35 | 1.0000 |
| 4 | 24 | 0.6613 | 21 | 36 | 1.0000 |
| 4 | 26 | 0.5282 | 23 | 24 | 1.0000 |
| 4 | 35 | 0.6613 | 23 | 26 | 0.8395 |
| 4 | 36 | 0.6613 | 23 | 35 | 1.0000 |
| 15 | 21 | 0.9516 | 23 | 36 | 1.0000 |
| 15 | 23 | 0.9516 | 24 | 26 | 0.8395 |
| 15 | 24 | 0.9516 | 24 | 35 | 1.0000 |
| 15 | 26 | 0.7669 | 24 | 36 | 1.0000 |
| 15 | 35 | 0.9516 | 26 | 35 | 0.8395 |
| 15 | 36 | 0.9516 | 26 | 36 | 0.8395 |
| 21 | 23 | 1.0000 | 35 | 36 | 1.0000 |




### Impact

⚡ We **deceive** the network operator **into believing** that **power flows** have **under- or over-utilization**

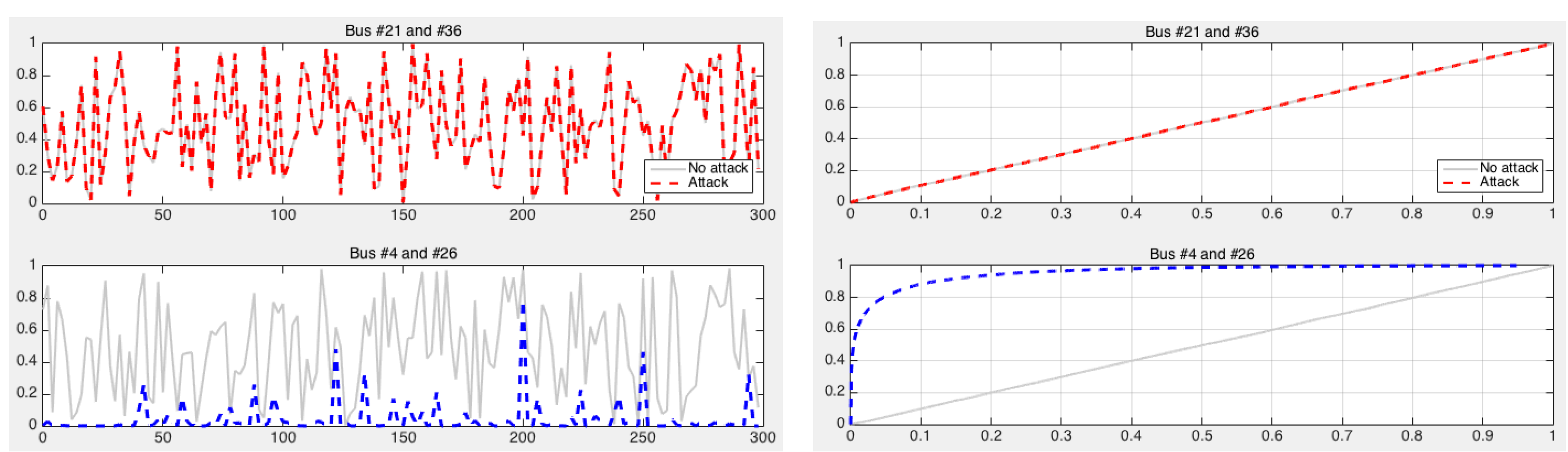
⚡ Up to 500% error in power-flow estimation




Comparison of the true apparent power flow in two lines and the estimated apparent power flow for the no-attack and attack scenarios

### Undetectability

- We use state-of-the-art bad-data detection mechanisms (i.e., $\chi^2$ test, Largest Normalized Residual Test) to prove undetectability.
- **The residuals are statistically the same before and after the attack.**




Comparison of *p*-values and CDFs of the *p*-values for the $\chi^2$ test applied to two attack locations: ideal location (in red), and lowest *IoS**-performer location (in blue). Non-attacked case is illustrated in grey.


*References*

S. Barreto, M. Pignati, G. Dan, M. Paolone, J.-Y. Le Boudec, "*Undetectable PMU Timing-Attack on Linear State-Estimation Using Rank-1 Approximation*," submitted to IEEE Transactions on Smart Grids.

S. Barreto, A. Suresh, J.-Y. Le Boudec, "*Cyber-attack on Packet-Based Time Synchronization Protocols: the Undetectable Delay Box*", to be presented in I2MTC 2016, May 22-26, Taipei, Taiwan.