Undetectable Attacks on PMU Time Synchronization

György Dán (gyuri@kth.se)
Department of Network and Systems Engineering
School of Electrical Engineering
Joint work with E. Shereen, S. Barreto, M. Pignati, M. Paolone, J.Y. Le Boudec
Phasor measurement units (PMUs)

Source: NASPI
WAMPAC for Efficiency and Stability

• Improved efficiency
  • Real-time congestion management
  • Network model parameter measurement and estimation

• Improved situational awareness and stability
  • Early stability warning
  • Real-time congestion management
  • Inter-area oscillation damping
  • Real-time angular, voltage, and frequency stability
  • Anti-islanding protection
  • Real-time state estimation

Source: WECC

Synchrophasor Measurements with PMUs

- Voltage phasor

- Accuracy requirement (C37.118)
  - Total Vector Error (TVE) of 1%
  - Time accuracy 1%@50Hz≈31.8μs
Time Synchronization for PMUs

Space-based
- GPS, Glonass, Galileo
- Trilateration
- Accuracy \( \sim 40\text{ns} \)

Network-based
- IEEE 1588-2008 (PTPv2)
- Request-response
- Accuracy \( \sim 100\text{ns} \)
  - Hardware timestamping
  - Calibration/symmetry assumption

N.M. Freris, S.R. Graham, P.R.Kumar, “Fundamental Limits on Synchronizing Clocks over Networks,” TAC 56(6)
Are PMU measurements vulnerable?

Mis-estimation of the System State (Voltage Phasors) by altering Voltage/Current Measurements

- Compromise PMU
- Alter Time Reference of PMU
- Tamper with PMU’s transducers
- MITM Attack to forge PMU data
Are PMU measurements vulnerable to Time Synchronization Attacks?

- Could an attacker compromise PMU time references?
- Could an attack remain undetected?
- Is an attack easy to compute?
- Could an attack have significant impact?
GPS Security

Spoofing

- Theoretical and experimental results
- “A small group located off the south coast of Italy successfully took control of an $80 million super-yacht’s navigation system using a homemade device, and sent the luxury vessel on a potentially disastrous wayward path.” 2013

Reliability

- “GPS timing issues have been reported from some user communities to the U.S. Coast Guard Navigation Center (NAVCEN) over the last 12 hours” Jan 26, 2016 – 13 μs offset from UTC

Ng, Y., Gao, G.X, “Advanced Multi-Receiver Position-Information-Aided Vector Tracking for Robust GPS Time Transfer to PMUs”, GNSS 2015
PTPv2 Security
PTPv2 Security
PTPv2 Security
PTPv2 Security

- Annex K (experimental)
  - HMAC for integrity
  - Crypto takes time...
- MACsec (IEEE 802.1AE)
  - Link layer integrity
- SecurityTLV

- Easily compromised
  - Access to network
  - Compromised switch
  - Delay box

Are PMU measurements vulnerable to Time Synchronization Attacks?

- Could an attacker compromise PMU time references? **YES**
- Could an attack remain undetected?
- Is an attack easy to compute?
- Could an attack have significant impact?
System Model

- System of $N$ buses
  - System state $x \in \mathbb{C}^N$
- $M$ PMUs
  - Voltage phasors
  - Nodal current injection phasors
- $M \times N$ measurement matrix $H$

$$
H_{m,m} = 1, \ m \in \mathcal{M}^V \\
H_{m,n} = 0, \ m \in \mathcal{M}^V, m \neq n \\
H_{m,n} = Y_{m,n}, \ m \in \mathcal{M}^I, n \in \mathcal{N}.
$$

- Measurement model

$$
z = Hx + e,$$
State Estimation and Bad Data Detection

- System state estimate
  \[ \hat{x} = (H^\dagger H)^{-1} H^\dagger z \]

- Measurement estimate
  \[ \hat{z} = H \hat{x} \]

- Measurement residual: Bad Data Detection (BDD)
  \[ r = \hat{z} - z \]

- Statistical tests for detecting outliers (e.g., LNR)
- Verification matrix
  \[ F \triangleq H(H^\dagger H)^{-1} H^\dagger - I \]

- N.b.: \( z = Hx \leftrightarrow Fz = 0 \)
Attack Model

• Attacker knows
  • System model $H$
  • Measurements $z$
• Attacker manipulates
  • $p$ time references
  • Phase angle attack $\alpha=(\alpha_1, \ldots, \alpha_p)$
  • Set of PMUs using time reference $i$ is $A_i$

• Impact of attack on measurements
  \[
  u_i = \cos \alpha_i + j \sin \alpha_i = e^{j\alpha_i} \\
  \Delta z_m = z_m(u_i - 1), \quad \text{if } m \in A_i \\
  \Delta z_m = 0, \quad \text{if } m \in M \setminus \bigcup_i A_i
  \]
Undetectable Time-Synchronization Attack

Undetectable attack $\alpha=(\alpha_1, \ldots, \alpha_p)$

$$Fz = F(z + \Delta z) \Rightarrow F\Delta z = 0$$
Undetectable Time-Synchronization Attack

Undetectable attack $\alpha = (\alpha_1, \ldots, \alpha_p)$

$$Fz = F(z + \Delta z) \Rightarrow F\Delta z = 0$$

Attack-measurement indicator

$$\Psi_{m,i} = 1 \text{ if } m \in A_i$$

$$\Psi_{m,i} = 0 \text{ otherwise.}$$

Change of measurement vector

$$\Delta z = (u_1 - 1) \text{ diag}(z) \Psi_{:,1} + \ldots + (u_p - 1) \text{ diag}(z) \Psi_{:,p}$$

Attack $\alpha$ is undetectable iff

$$\sum_{i=1}^{p} (u_i - 1)F \text{ diag}(z) \Psi_{:,i} = 0$$
Undetectable Time-Synchronization Attack

Undetectable attack \( \alpha = (\alpha_1, \ldots, \alpha_p) \)
\[
Fz = F(z + \Delta z) \Rightarrow F\Delta z = 0
\]

Attack-measurement indicator
\[
\Psi_{m,i} = 1 \text{ if } m \in A_i \\
\Psi_{m,i} = 0 \text{ otherwise.}
\]

Change of measurement vector
\[
\Delta z = (u_1 - 1) \text{ diag}(z)\Psi_{:,1} + \ldots + (u_p - 1) \text{ diag}(z)\Psi_{:,p}
\]

Attack \( \alpha \) is undetectable iff
\[
\sum_{i=1}^{p} (u_i - 1) F \text{ diag}(z)\Psi_{:,i} = 0
\]

Attack-angle matrix \((pxp, \text{ Hermitian})\)
\[
W \triangleq \Psi^T \text{ diag}(z)^\dagger F^\dagger F \text{ diag}(z)\Psi
\]
Undetectable Time-Synchronization Attack

Undetectable attack \( \alpha=(\alpha_1, \ldots, \alpha_p) \)
\[
Fz = F(z + \Delta z) \Rightarrow F\Delta z = 0
\]

Attack-measurement indicator
\[
\Psi_{m,i} = 1 \text{ if } m \in A_i \\
\Psi_{m,i} = 0 \text{ otherwise.}
\]

Change of measurement vector
\[
\Delta z = (u_1 - 1) \text{ diag}(z)\Psi_{:, 1} + \ldots + (u_p - 1) \text{ diag}(z)\Psi_{:, p}
\]

Attack \( \alpha \) is undetectable iff
\[
\sum_{i=1}^{p} (u_i - 1)F \text{ diag}(z)\Psi_{:, i} = 0
\]

Attack-angle matrix \((p \times p, \text{ Hermitian})\)
\[
W \triangleq \Psi^T \text{ diag}(z)^\dagger F^\dagger F \text{ diag}(z)\Psi
\]

**Condition for Undetectability:**
Attack \( \alpha=(\alpha_1, \ldots, \alpha_p) \) is absolutely undetectable iff
\[
W(\vec{u} - \vec{1}) = 0
\]
Time-synchronization attack with 1 delay

Attacker attacks 1 time reference
- $p=1$, $\alpha=(\alpha_1)$

Attack-angle matrix
- $W=(W_{1,1})$

Undetectability requires
$$W_{1,1}(u_1 - 1) = 0$$

$$W_{1,1} = \sum_{l,m \in A_1, n \in M} F_n,l F_{n,m} \bar{z}_l z_m = 0 \quad u_1 = 1$$
Time-synchronization attack with 1 delay

Attacker attacks 1 time reference
- $p=1$, $\alpha=(\alpha_1)$

Attack-angle matrix
- $W=(W_{1,1})$

Undetectability requires
$$W_{1,1}(u_1 - 1) = 0$$

$$W_{1,1} = \sum_{l,m \in A_{1}, n \in M} F_{n,l} F_{n,m} \tilde{z}_l \tilde{z}_m = 0 \quad u_1 = 1$$

Attack against single PMU can be detected.
Time-synchronization attack with 2 delays

Attacker attacks 2 time references

- \( p=2, \quad \alpha=(\alpha_1, \alpha_2) \)

Attack-angle matrix \( W \)

\[
W_{1,1}(u_1 - 1) + W_{1,2}(u_2 - 1) = 0
\]

\[
W_{2,1}(u_1 - 1) + W_{2,2}(u_2 - 1) = 0
\]

Assume \( r(W)=1 \)

\[
W_{1,1}(u_1 - 1) = -W_{1,2}(u_2 - 1)
\]

\[
|u_1| = |u_2| = 1
\]
Time-synchronization attack with 2 delays

Attacker attacks 2 time references

- $p=2$, $\alpha=(\alpha_1, \alpha_2)$

Attack-angle matrix $W$

$$W_{1,1}(u_1 - 1) + W_{1,2}(u_2 - 1) = 0$$
$$W_{2,1}(u_1 - 1) + W_{2,2}(u_2 - 1) = 0.$$ 

Assume $r(W)=1$

$$W_{1,1}(u_1 - 1) = -W_{1,2}(u_2 - 1)$$

$$|u_1| = |u_2| = 1$$
Time-synchronization attack with 2 delays

Attacker attacks 2 time references
- $p=2$, $\alpha=(\alpha_1, \alpha_2)$

Attack-angle matrix $W$

\[
\begin{align*}
W_{1,1}(u_1 - 1) + W_{1,2}(u_2 - 1) &= 0 \\
W_{2,1}(u_1 - 1) + W_{2,2}(u_2 - 1) &= 0.
\end{align*}
\]

**Result:** If $r(W)=1$ then there is 1 non-trivial undetectable attack $\alpha=(\alpha_1, \alpha_2)$ with

\[
\begin{align*}
\alpha_1 &= 2 \arg(W_{1,1} + W_{1,2})(\text{mod } 2\pi) \\
\alpha_2 &= -2 \arg(W_{1,2}) + 2 \arg(W_{1,1} + W_{1,2})(\text{mod } 2\pi)
\end{align*}
\]

Note: for $r(W)=2$ there is **no** non-trivial undetectable attack
- But we can approximate $W$ with a rank-1 matrix…
Rank-1 Approximation Attack

Decomposition of $W$
- $W = U \Lambda U^\dagger$
- $\Lambda$ diagonal matrix of eigenvalues

Replace smallest eigenvalue by 0
- $\tilde{\Lambda} = \text{diag}(\Lambda_{1,1}, 0)$

Construct approximate attack-angle matrix
- $\tilde{W} = U \tilde{\Lambda} U^\dagger$

Construct undetectable attack $\tilde{\alpha}$ for
- $\tilde{W}(\tilde{u} - \tilde{1}) = 0$
Time synchronization attacks with >2 delays

Disjoint pairs $\left(z_{m_1}, z_{m_2}\right)$, $\left(z_{m_3}, z_{m_4}\right)$ of PMUs

- Undetectable attacks can be computed simultaneously or sequentially
Time synchronization attacks with >2 delays

Disjoint pairs \((z_{m_1}, z_{m_2})(z_{m_3}, z_{m_4})\) of PMUs
- Undetectable attacks can be computed simultaneously or sequentially

Overlapping pairs \([z_{m_1}, z_{m_2}][z_{m_2}, z_{m_3}]\) of PMUs
- Undetectable attacks can be computed sequentially
- Countably infinite attacks possible
- Greedy algorithm for maximizing impact
Are PMU measurements vulnerable to Time Synchronization Attacks?

- Could an attacker compromise PMU time references? YES
- Could an attack remain undetected? YES
- Is an attack easy to compute?
- Could an attack have significant impact?
Finding Vulnerable Attack Locations

- Index of separation for $p=2$
  \[ \text{IoS} = \frac{\lambda_{\text{max}}}{\sum_i \lambda_i} = \frac{\Lambda_{1,1}}{\Lambda_{1,1} + \Lambda_{2,2}}. \]

- Sufficient condition for $r(W)=1$
  \[ \text{IoS} = \frac{1}{2} + \frac{1}{2} \sqrt{1 - 4 \frac{\det(W)}{\text{trace}(W)^2}}. \]
  \[ \text{IoS}(W) = 1 \implies \text{rank}(W) = 1. \]
Finding Vulnerable Attack Locations

- Index of separation for $p=2$
  \[ \text{IoS} = \frac{\lambda_{\text{max}}}{\sum \lambda_i} = \frac{\Lambda_{1,1}}{\Lambda_{1,1} + \Lambda_{2,2}}. \]

- Sufficient condition for $r(W)=1$
  \[ \text{IoS} = \frac{1}{2} + \frac{1}{2} \sqrt{1 - \frac{\det(W)}{\text{trace}(W)^2}}. \]
  \[ \text{IoS}(W) = 1 \implies \text{rank}(W) = 1. \]

- **Result**: For $p=2$ and one measurement point per delay $\text{IoS}(W) \geq \text{IoS}^*$, where
  \[ \text{IoS}^* = \frac{1}{2} + \frac{|f_{12}|}{2 (f_{11} f_{22})^{\frac{1}{2}}}, \]
  \[ f_{i,j} = \sum_l \sum_m \Psi_{l,i} \Psi_{m,j} F_{n,l} F_{n,m}. \]

- Observation 1: $\text{IoS}^* = 1 \implies \text{IoS}(W) = 1$
- Observation 2: $\text{IoS}^*$ depends only on $H$ and attack location
Are PMU measurements vulnerable to Time Synchronization Attacks?

- Could an attacker compromise PMU time references? **YES**
- Could an attack remain undetected? **YES**
- Is an attack easy to compute? **YES**
- Could an attack have significant impact?
Numerical results: Methodology

IEEE 39-bus network fed with real load profiles@50Hz

- 12 zero-injection buses
- 21 PMUs, (13 V+I, 8 I)

Load profile at Bus#4
Undetectable Attack

- P-values from $\chi^2$ test
- Attack undetectable despite load fluctuation when IoS* = 1

IoS* = 1

IoS = 0.5282
Impact on Estimated Power Flow (p=2)

- Attack can cause over or underestimation of power flow
- Error above 500%...
Impact on Estimated Power Flow ($p>2$)

- Single pair (#21,#36), simultaneous and sequential attack
- Attacking multiple PMUs increases attack impact
Summary and Open Questions

- Time synchronization attacks
  - can be undetectable
  - easy to compute
  - can have significant impact

S. Barreto, M. Pignati, G. Dán, J-Y Le Boudec, M Paolone, ``Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation,''
IEEE Trans. on Smart Grid, to appear
Summary and Open Questions

- Time synchronization attacks
  - can be undetectable
  - easy to compute
  - can have significant impact

- General results for $p>2$
- Detection algorithms
- Mitigation algorithms

S. Barreto, M. Pignati, G. Dán, J-Y Le Boudec, M Paolone, ``Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation,''

IEEE Trans. on Smart Grid, to appear
Bibliography

- Ng, Y., Gao, G.X , “Advanced Multi-Receiver Position-Information-Aided Vector Tracking for Robust GPS Time Transfer to PMUs”, GNSS 2015
Undetectable Attacks on PMU Time Synchronization

György Dán (gyuri@kth.se)
Department of Network and Systems Engineering
School of Electrical Engineering
Joint work with E. Shereen, S. Barreto, M. Pignati, M. Paolone, J.Y. Le Boudec