KTH ROYAL INSTITUTE
OF TECHNOLOGY

Resilient Time Synchronization for the Smart Grid

Vulnerabilities and Mitigation Schemes

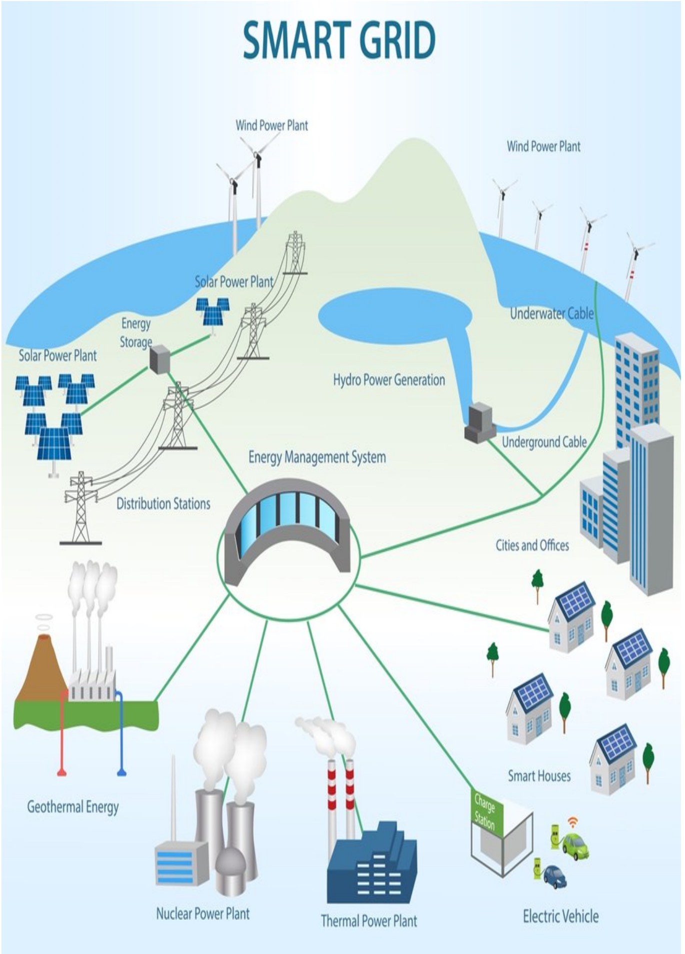
György Dán
KTH/EECS/NSE

Keynote, IEEE SmartGridComm 2019

Reliable, Flexible, Efficient, Sustainable

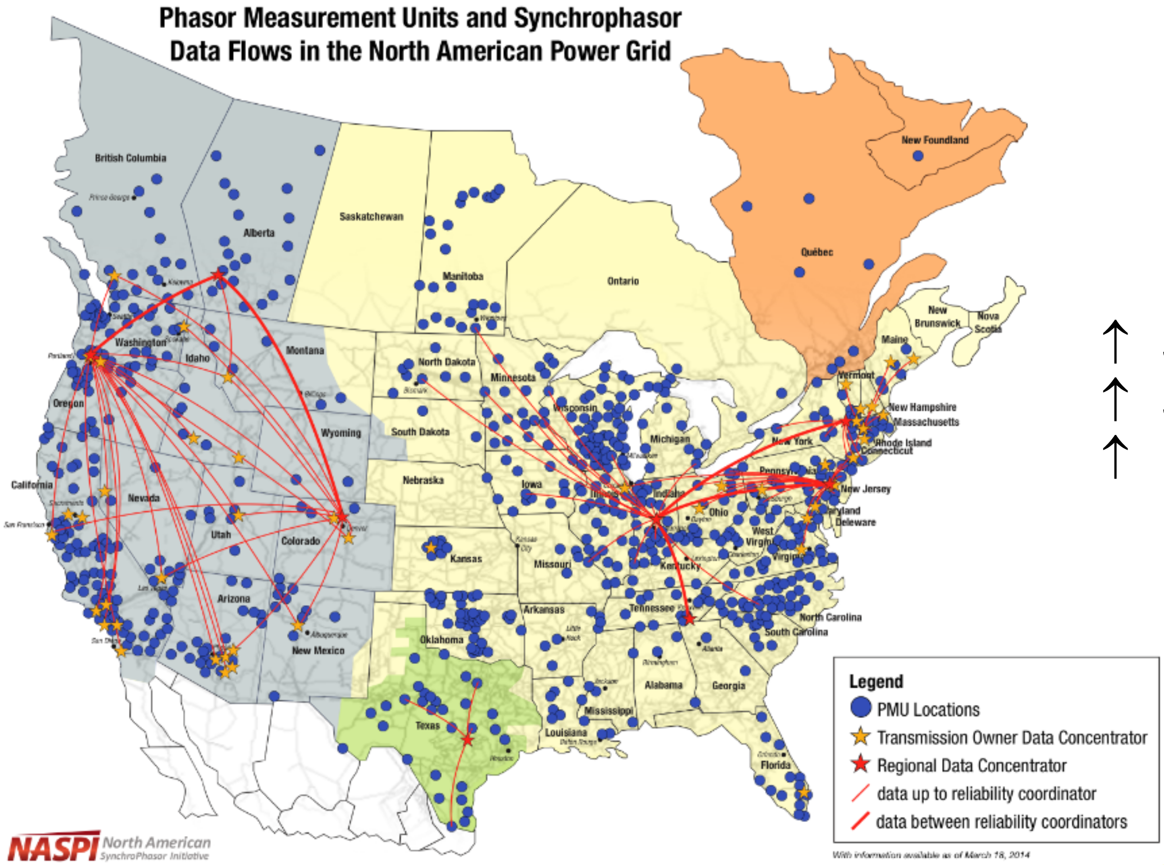
Reliable
- Improved protection
- Real-time voltage stability monitoring
- Wide-area damping control
- Fault location
- Islanding detection

Efficient and Sustainable
- Model validation
- Load disaggregation
- Real-time state estimation
- Predictive maintenance



Shutterstock/monicaodo

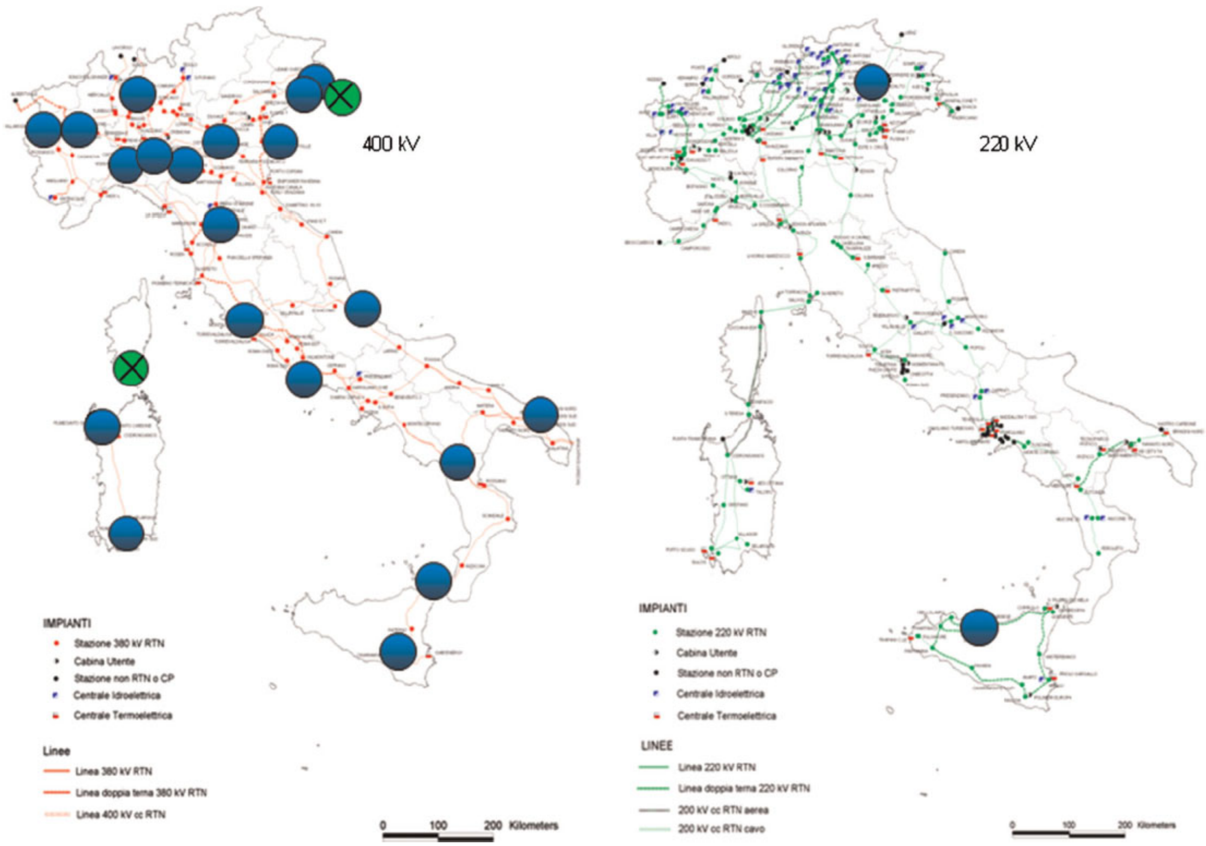
Phasor measurement units (PMUs)



Source: NASPI

- ↑ Situational awareness
- ↑ Stability
- ↑ Efficiency

Phasor measurement units (PMUs)

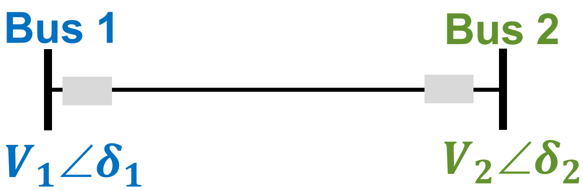


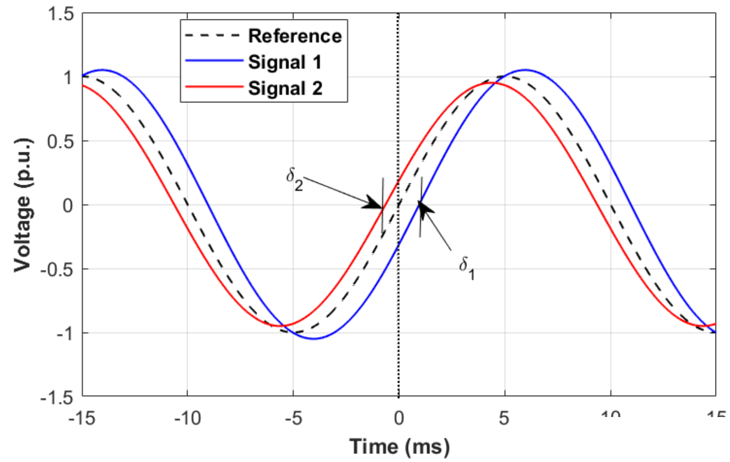
- ↑ Situational awareness
- ↑ Stability
- ↑ Efficiency

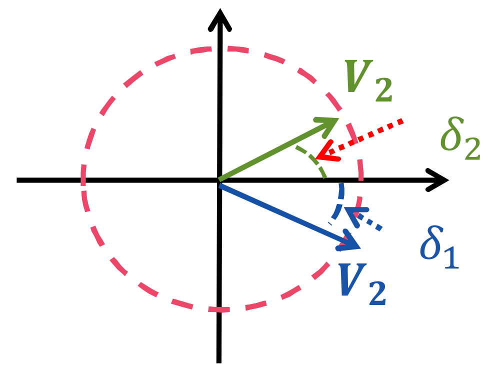
Source: Cirio et al "Wide area monitoring in the Italian power system: Architecture, functions and experiences", European Transactions on Electrical Power 21(4):1541 – 1556, 2011

Synchrophasor Measurements

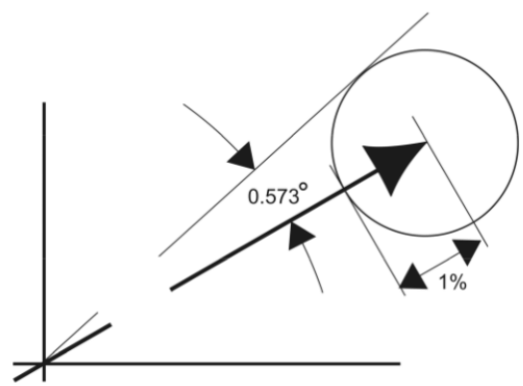
- Voltage phasor





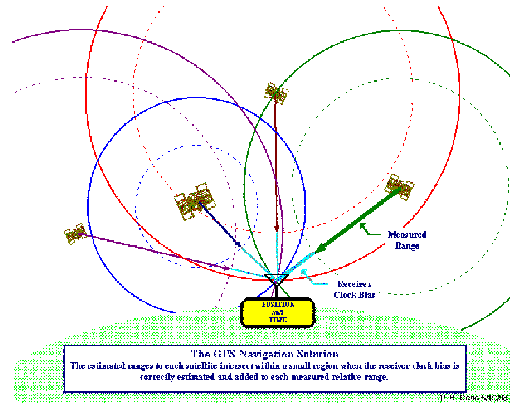


- Accuracy requirement (IEEE C37.118)
  - Total Vector Error (TVE) of 1%
  - Time accuracy 1%@50Hz≈31.8μs



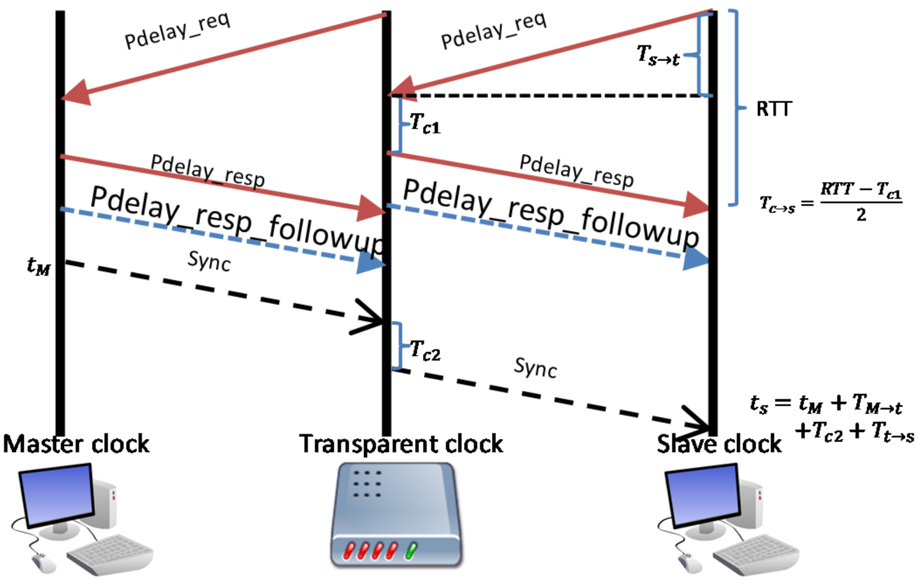
Source: IEEE C37.118-2011

Time Synchronization for PMUs



Space-based (SBTS)

- GPS, Glonass, Galileo, BeiDou-2
- Trilateration
- Accuracy ~10-40ns

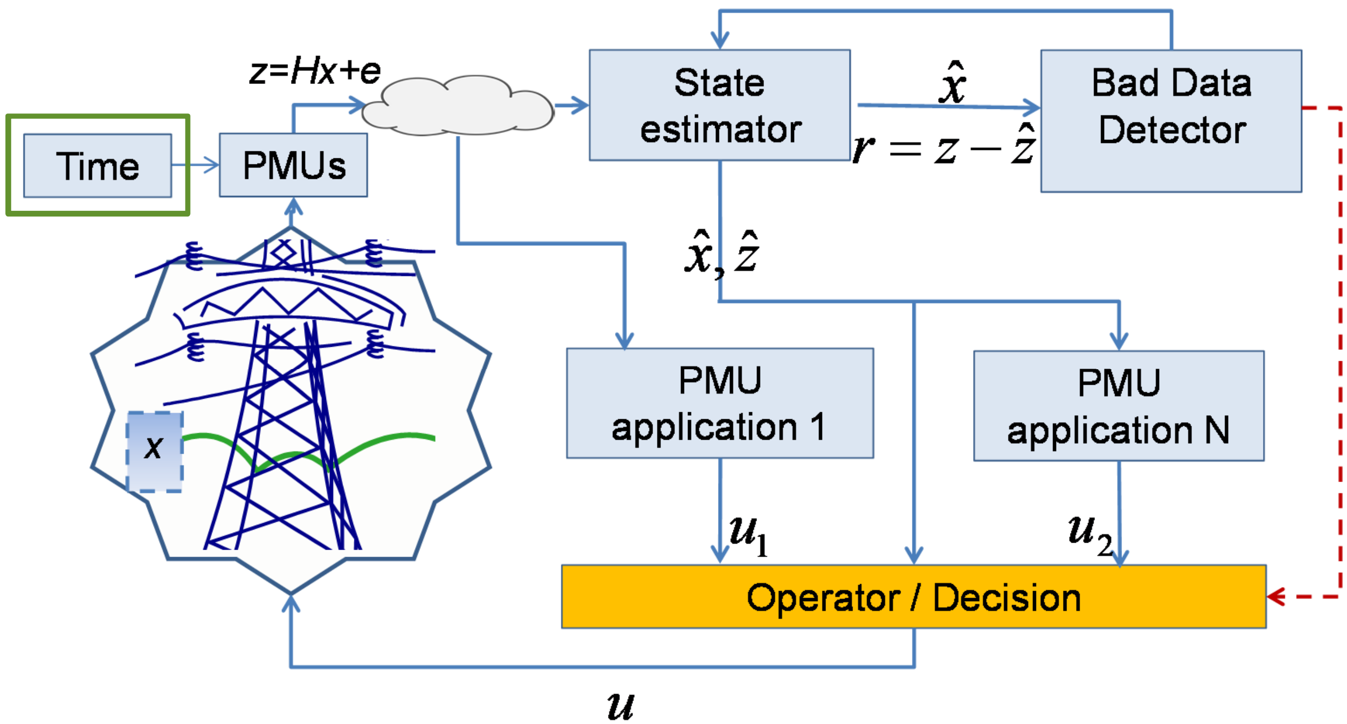


Network-based (NBTS)

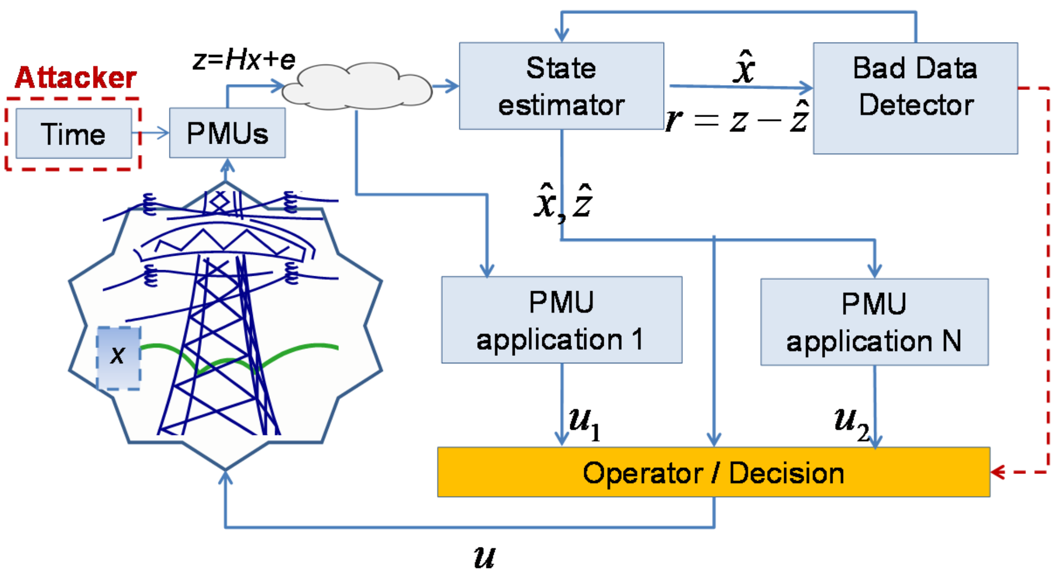
- IEEE 1588-2008 (PTPv2)
- Request-response
- Accuracy ~100ns
  - Hardware timestamping
  - Calibration/symmetry assumption

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

OODA Loop for Synchrophasors

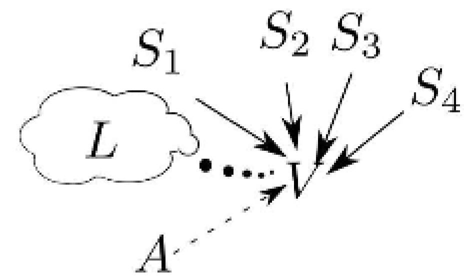


Are Synchrophasors Vulnerable to Time Synchronization Attacks?



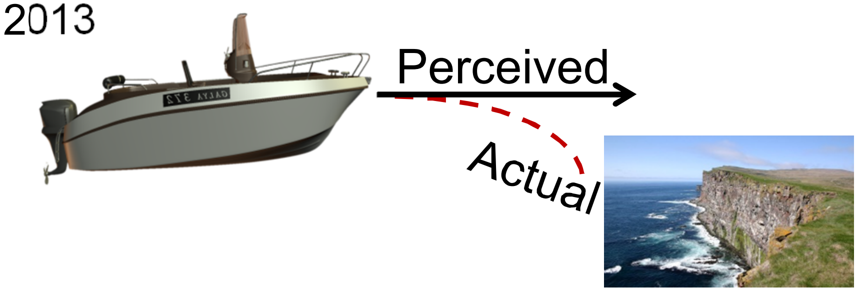
- Could an attacker compromise PMU time references?
- Could an attack remain undetected?
- Is an attack easy to compute?
- Could an attack have significant impact?

SBTS Security (GPS)



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

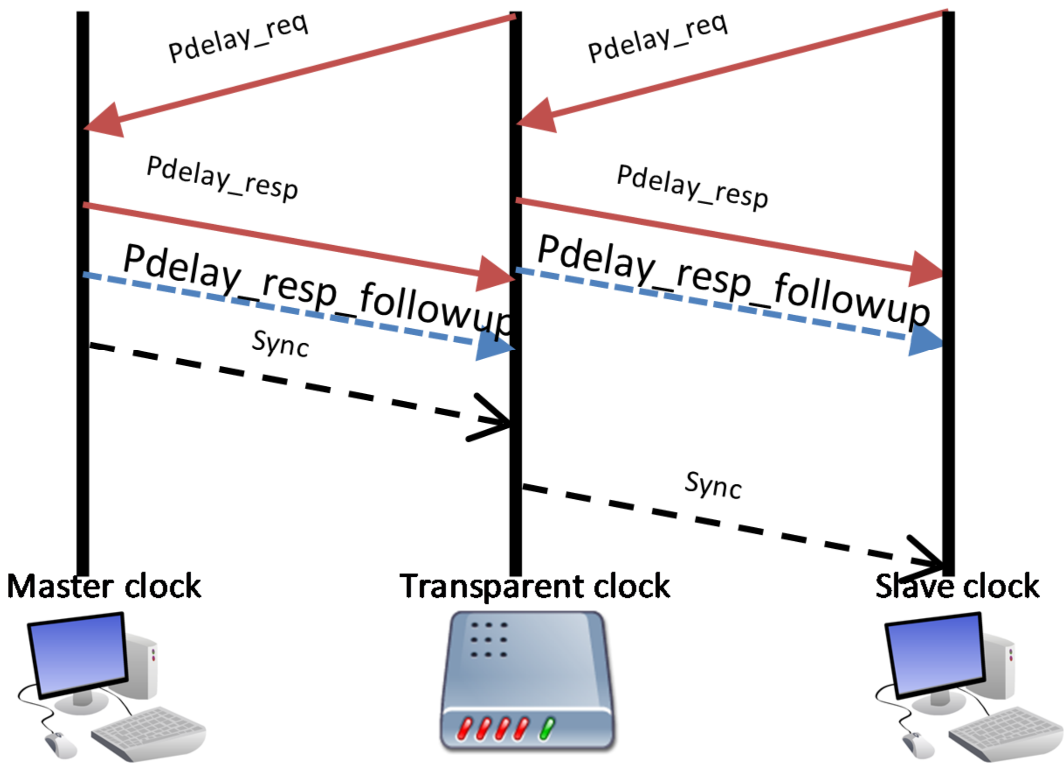


Reliability

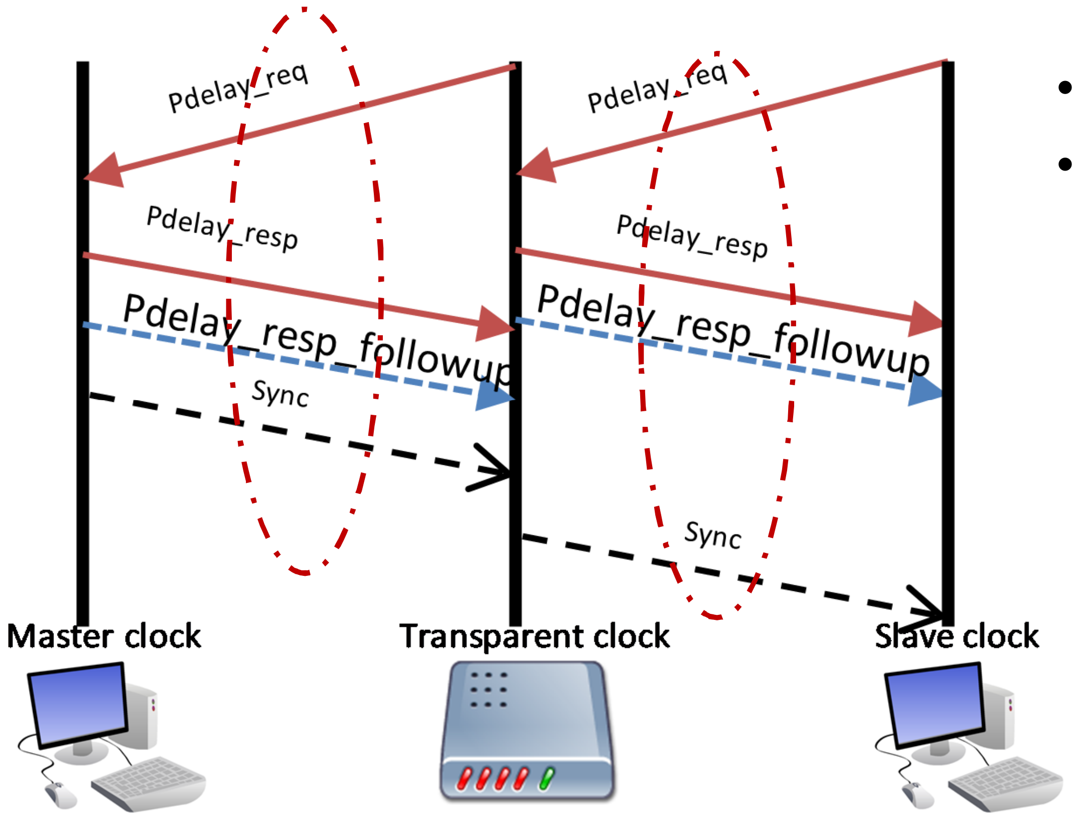
- “GPS timing issues have been reported from some user communities to the U.S. Coast Guard Navigation Center (NAVCEN) over the last 12 hours” Jan 26, 2016 – **13 μs offset from UTC**

Tippenhauer et al, “On the requirements for successful GPS spoofing attacks”, in Proc. ACM CCS, 2011
Ng, Y., Gao, G.X , “Advanced Multi-Receiver Position-Information-Aided Vector Tracking for Robust GPS Time Transfer to PMUs”, GNSS 2015

PTPv2 Security

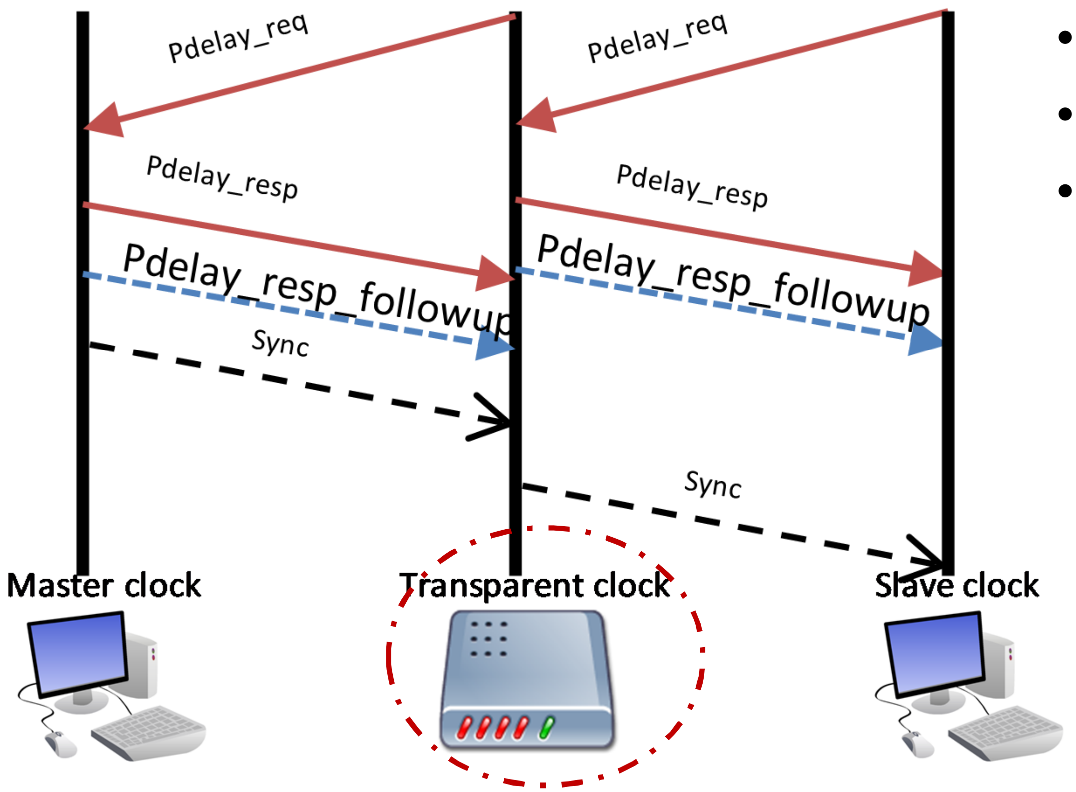


PTPv2 Security



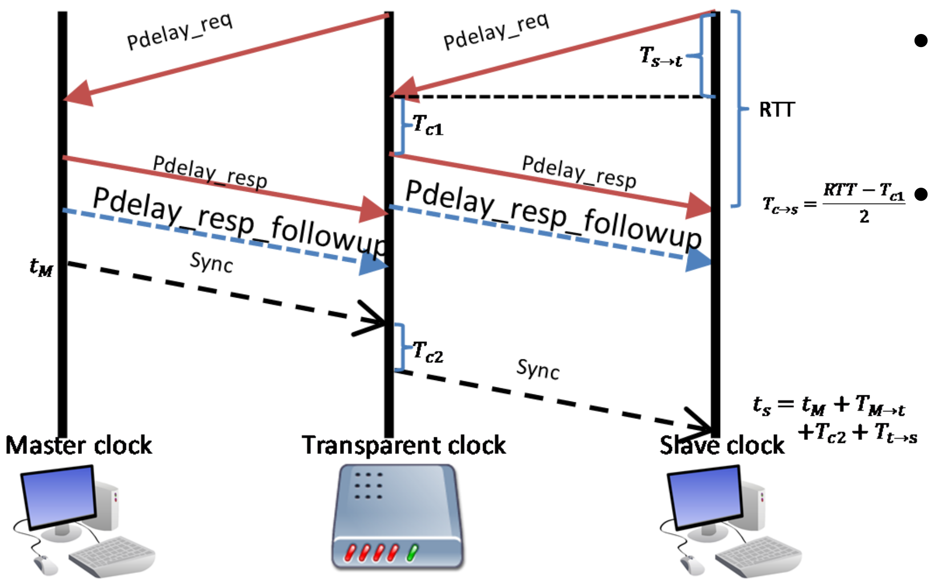
- Spoofing
- Delay attack

PTPv2 Security



- Spoofing
- Delay attack
- Software compromise

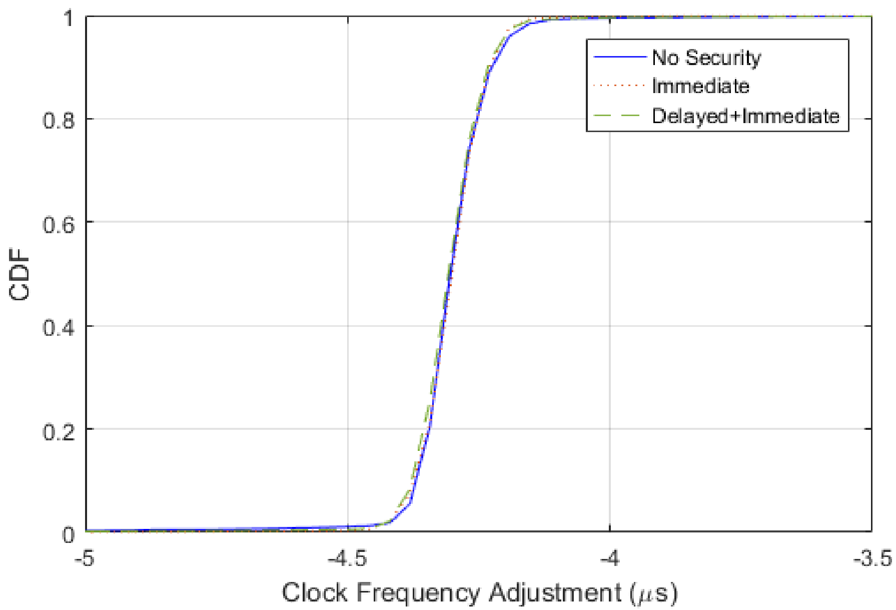
Securing PTP: PTPv2.1 AuthenticationTLV



- Integrity protection (Immediate)
  - Based on group key (HMAC)
- Authentication (Delayed)
  - Secure multicast (TESLA)
  - Unmutable fields only

E. Shereen, F. Bitard, G. Dán, S. Fries, T. Sel,"Next Steps in Security for Time Synchronization: Experiences from implementing IEEE 1588 v2.1," *in Proc. of IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), Sep. 2019*

Securing PTP: PTPv2.1 AuthenticationTLV

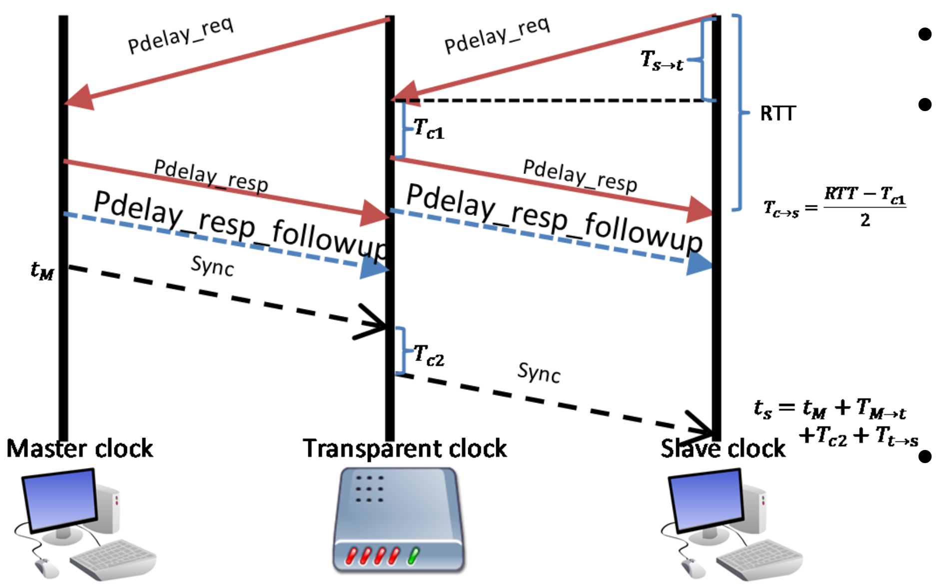


- Integrity protection (Immediate)
  - Based on group key (HMAC)
- Authentication (Delayed)
  - Secure multicast (TESLA)
  - Unmutable fields only
- Implementation in LinuxPTP
  - Accuracy
  - Overhead

	No Security	Immediate	Delayed + Immediate
Processing time / min	8 ms	24 ms	27 ms

E. Shereen, F. Bitard, G. Dán, S. Fries, T. Sel,"Next Steps in Security for Time Synchronization: Experiences from implementing IEEE 1588 v2.1," *in Proc. of IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), Sep. 2019*

How Secure is PTPv2.1?

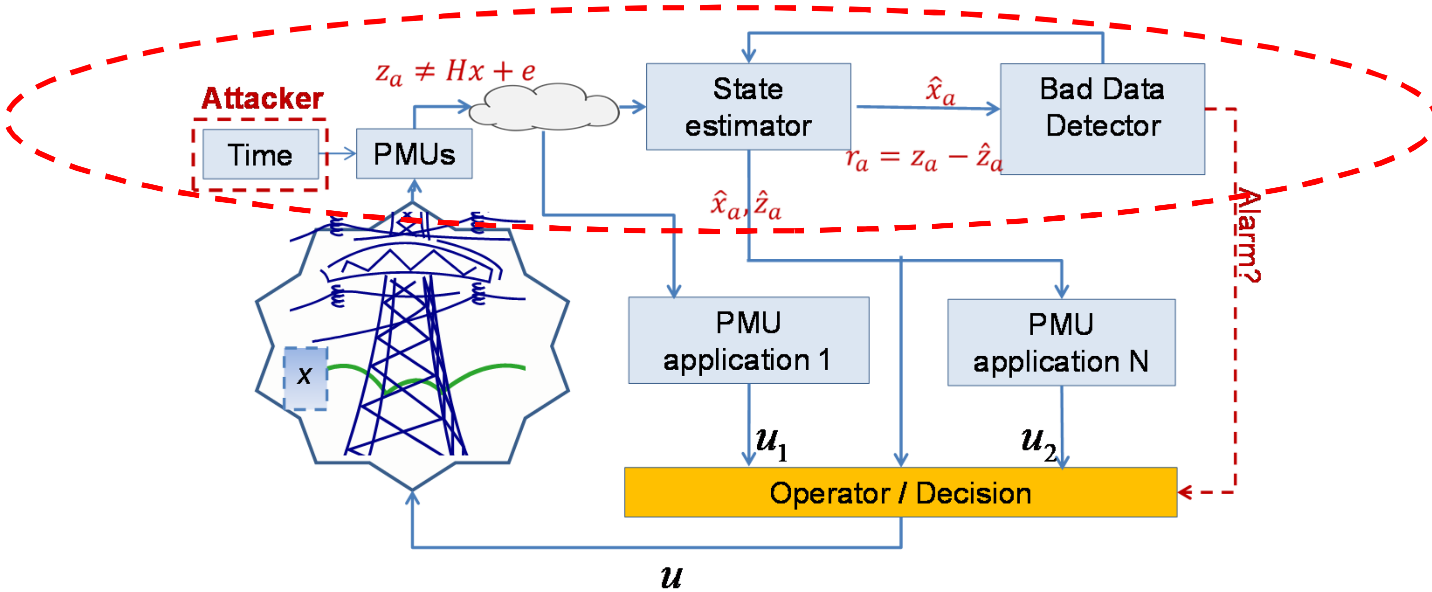


- Protects only data in transit
- Vulnerable to
  - Software compromise
  - Group key disclosure
  - Delay attacks
- Could benefit from
  - Constant time crypto

Are precise time synchronization and end-to-end security compatible?

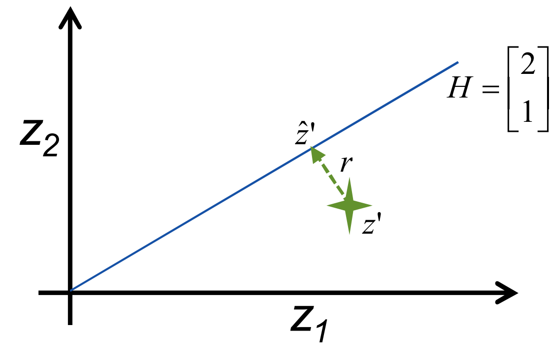
E. Shereen, F. Bitard, G. Dán, S. Fries, T. Sel,"Next Steps in Security for Time Synchronization: Experiences from implementing IEEE 1588 v2.1," *in Proc. of IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), Sep. 2019*

Are Synchrophasors 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?

Physics-based approach: Linear state estimation



System model

- Linear measurement model (*V,I=YV*)

$$\hat{z}' = H'\hat{x}' + e,$$

- Linear state estimation

$$\hat{x}' = (H'^T D H')^{-1} H'^T D z' = G^{-1} H'^T D z'$$

- Residual for Bad data detection (BDD)

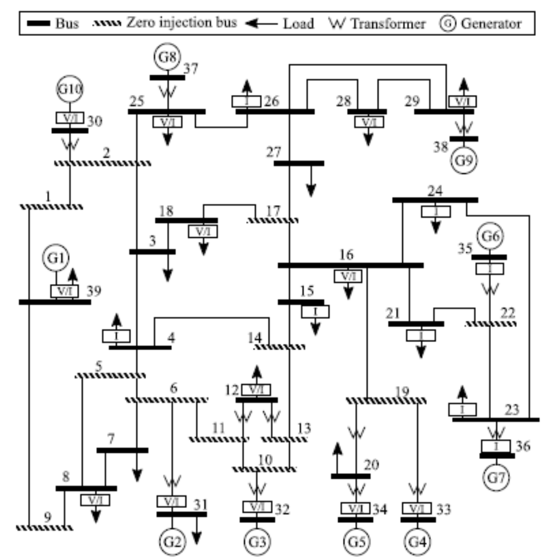
$$r = \hat{z}' - z'.$$

Attacker model

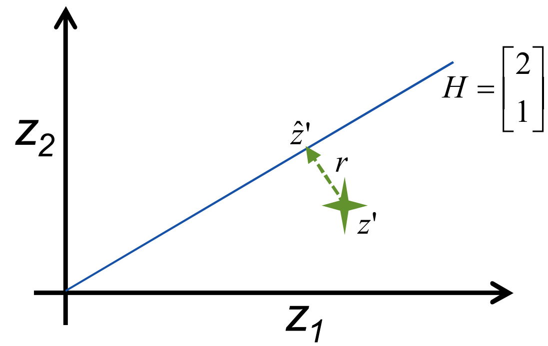
- Knows the instantaneous measurements (z')
- Knows the system model (*H)*
- Can manipulate *p* time references
  - Manipulated measurement $z_i^a = z_i' u_i = z_i' e_i^{\alpha j}$

Question

- Can attacker manipulate time references without changing the residual?



Physics-based approach: Linear state estimation



System model

- Linear measurement model (*V*,*I*=*YV*)

$$\hat{z}' = H'\hat{x}' + e,$$

- Linear state estimation

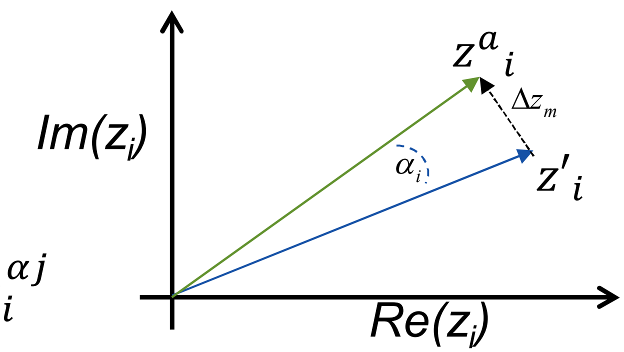
$$\hat{x}' = (H'^T DH')^{-1} H'^T Dz' = G^{-1} H'^T Dz'$$

- Residual for Bad data detection (BDD)

$$r = \hat{z}' - z'.$$

Attacker model

- Knows the instantaneous measurements (z')
- Knows the system model (*H*)
- Can manipulate *p* time references
  - Manipulated measurement $z_i^a = z_i' u_i = z_i' e_i^{\alpha j}$



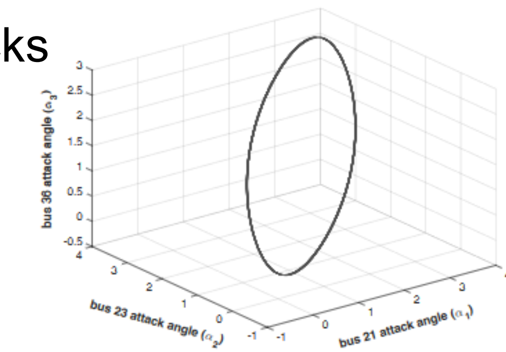
Question

- Can attacker manipulate time references without changing the residual?

Undetectable Time Synchronization Attacks

Feasibility

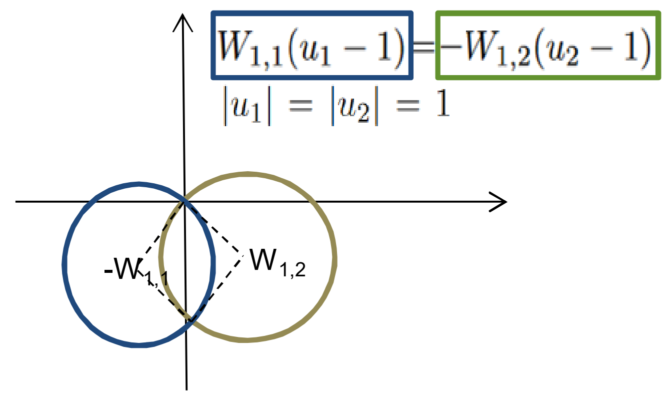
- Necessary and sufficient condition for undetectable attacks
  - Based on system topology
- *p*=1 : No attack possible
- *p*=2 : 1 non-trivial attack may be possible
- *p*>2: Continuum of attacks



Computability

- O(1) algorithm for computing attack angles α_i

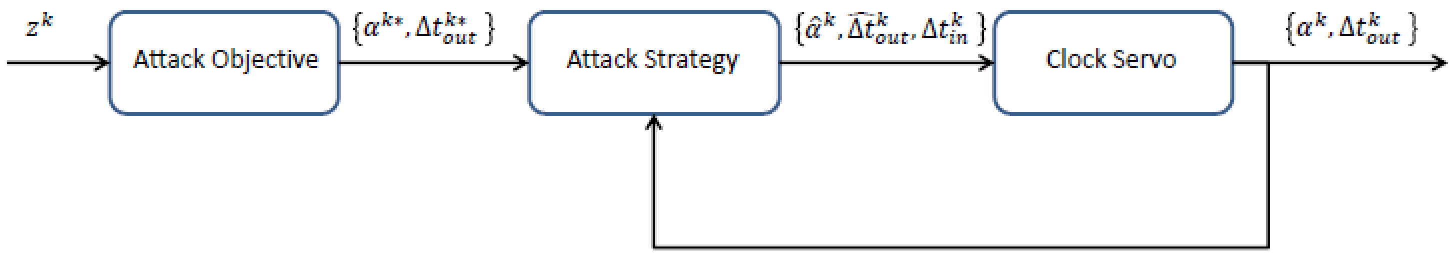
- Efficient algorithm for finding attackable sets of PMUs based on equivalence classes



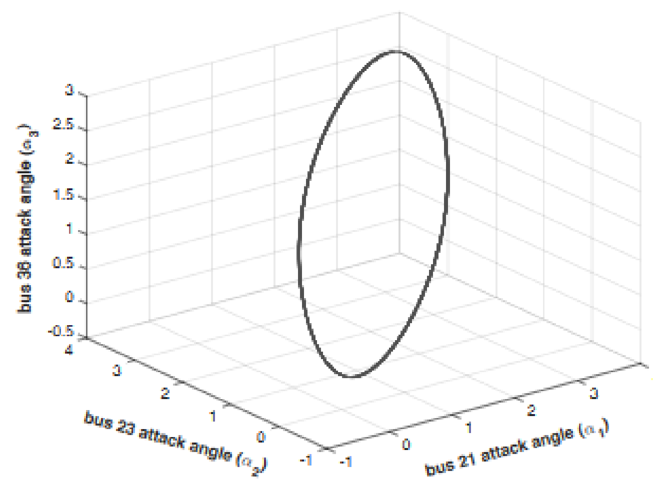
S. Barreto, M. Pignati, G. Dán, J-Y Le Boudec, M. Paolone, ``Undetectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation,'' IEEE Trans. on Smart Grid, 9(4), 2018
E. Shereen, M Delcourt, S. Barreto, G. Dán, J-Y. Le Boudec, M. Paolone, ``Feasibility of Time Synchronization Attacks against PMU-based State-Estimation," IEEE Trans. on Instrumentation and Measurement, to appear

Implementing Time Synchronization Attacks

- Consider practical constraints – clock servo



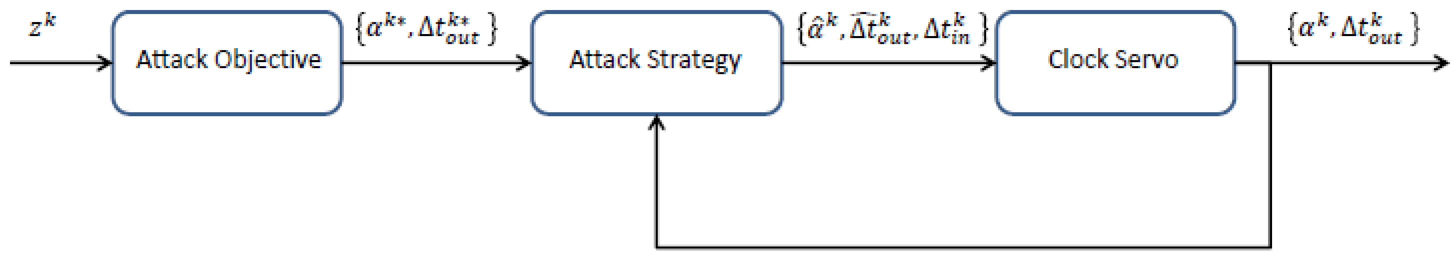
- Idea:
  - Small changes at a time
  - Track clock servo output
- Algorithms
  - Brute force (BF)
  - Clock-servo aware (OCPI)



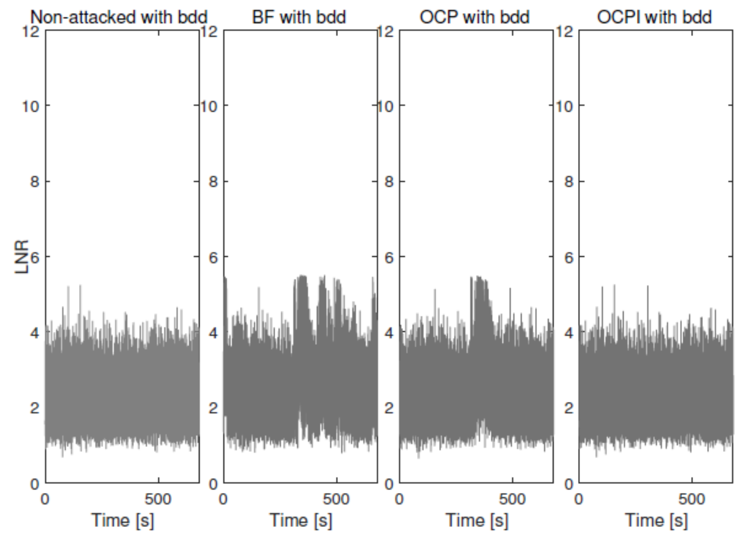
S. Barreto, E. Shereen, M. Pignati, G. Dán, J-Y. Le Boudec, M Paolone,``A Continuum of Undetectable Timing-Attacks on PMU-based Linear State-Estimation,'' *in Proc. of IEEE SmartGridComm, Oct. 2017*
E. Shereen, M. Delcourt, S. Barreto, G. Dán, M. Paolone, J-Y. Le Boudec, "Feasibility of Time Synchronization Attacks against PMU-based State-Estimation" IEEE Trans. on Instr. and Measurment, to appear

Implementing Time Synchronization Attacks

- Consider practical constraints – clock servo

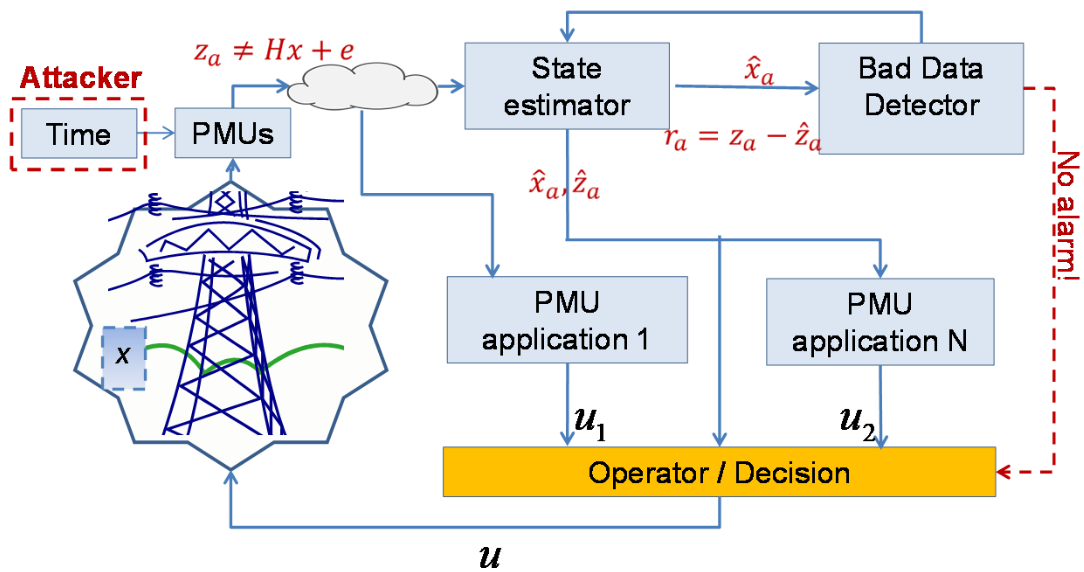


- Idea:
  - Small changes at a time
  - Track clock servo output
- Algorithms
  - Brute force (BF)
  - Clock-servo aware (OCPI)



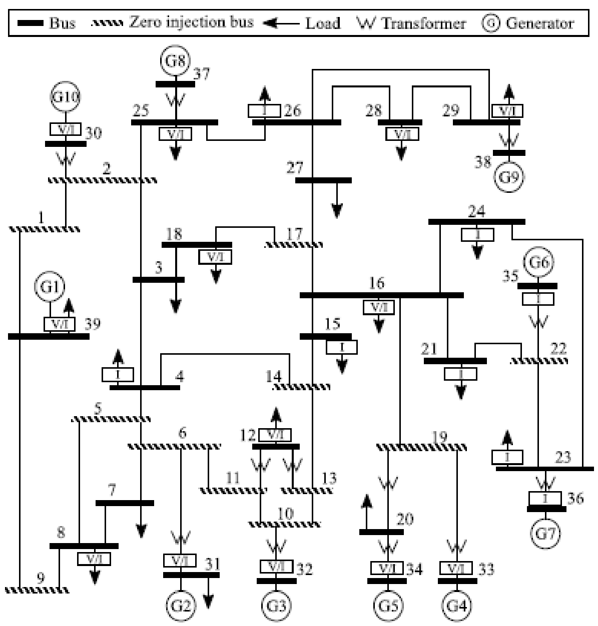
S. Barreto, E. Shereen, M. Pignati, G. Dán, J-Y. Le Boudec, M Paolone,``A Continuum of Undetectable Timing-Attacks on PMU-based Linear State-Estimation,'' *in Proc. of IEEE SmartGridComm, Oct. 2017*
E. Shereen, M. Delcourt, S. Barreto, G. Dán, M. Paolone, J-Y. Le Boudec, "Feasibility of Time Synchronization Attacks against PMU-based State-Estimation" IEEE Trans. on Instr. and Measurment, to appear

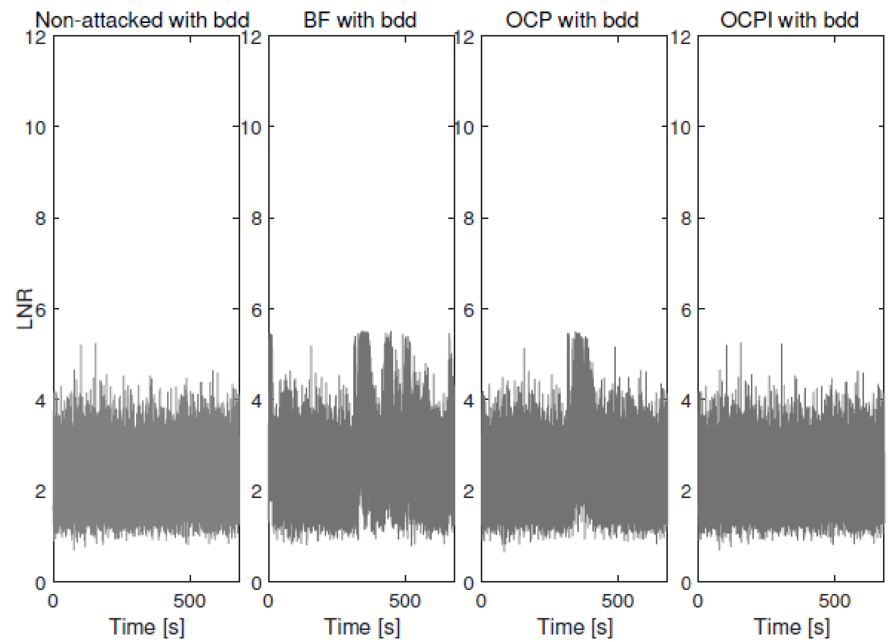
Are Synchrophasors Vulnerable to Time Synchronization Attacks?



- 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?

Impact on Estimated Power Flow (p=5)





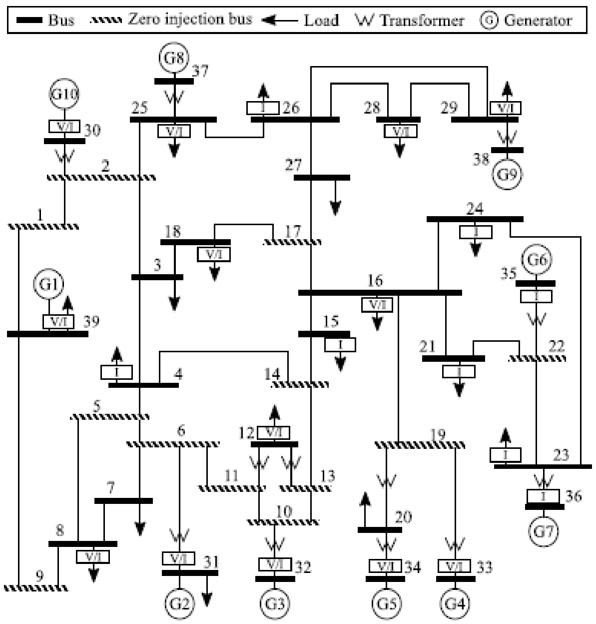
IEEE 39-bus network

- Real load profiles@50Hz
- 34 V,I measurements

- BF: Brute force greedy attack
- OCPI: PI clock servo-aware attack

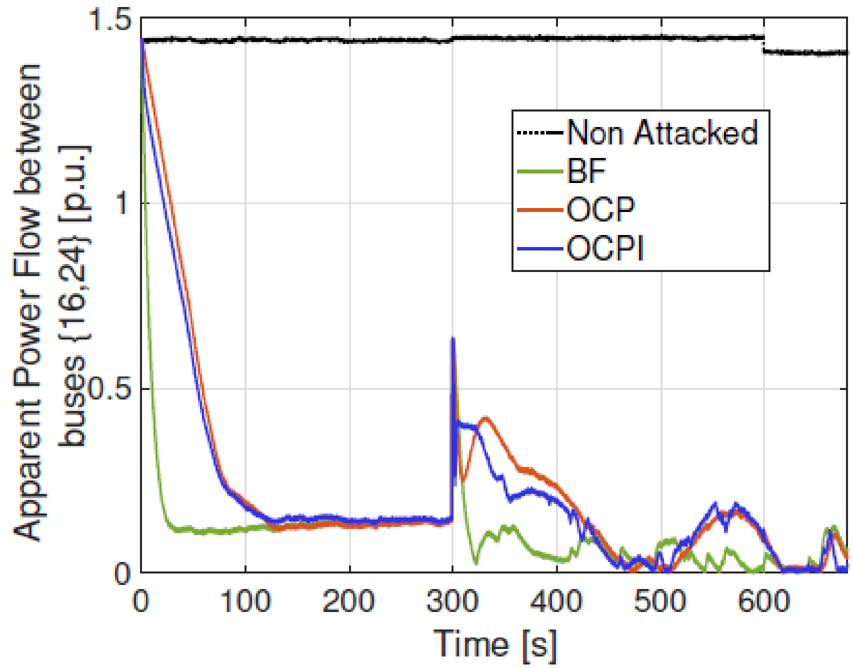
E. Shereen, M Delcourt, S. Barreto, G. Dán, J-Y. Le Boudec, M. Paolone, ``Feasibility of Time Synchronization Attacks against PMU-based State-Estimation,'' IEEE Trans. on Instrumentation and Measurement, to appear

Impact on Estimated Power Flow (p=5)



IEEE 39-bus network

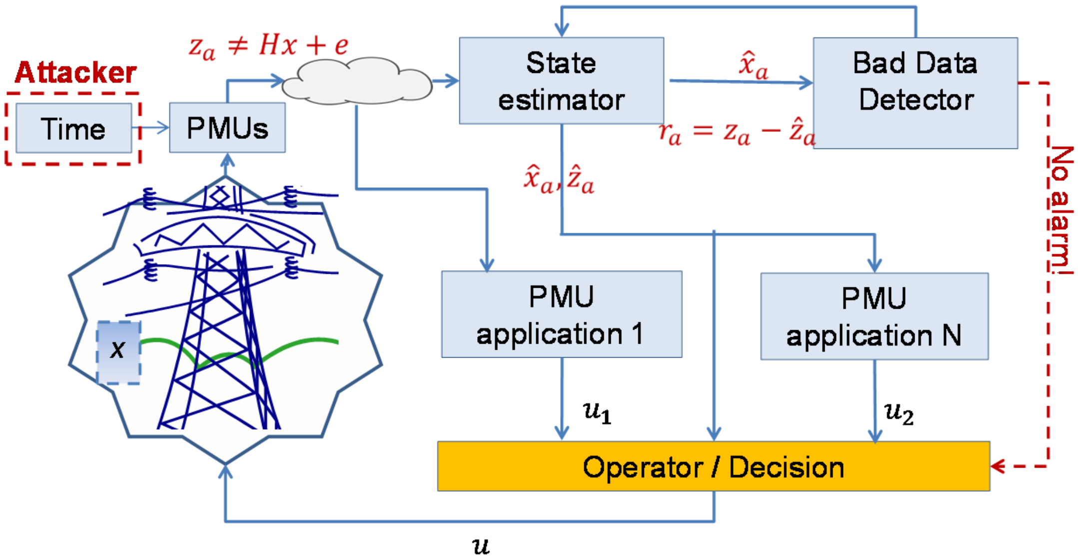
- Real load profiles@50Hz
- 34 V,I measurements



- BF: Brute force greedy attack
- OCPI: PI clock servo-aware attack

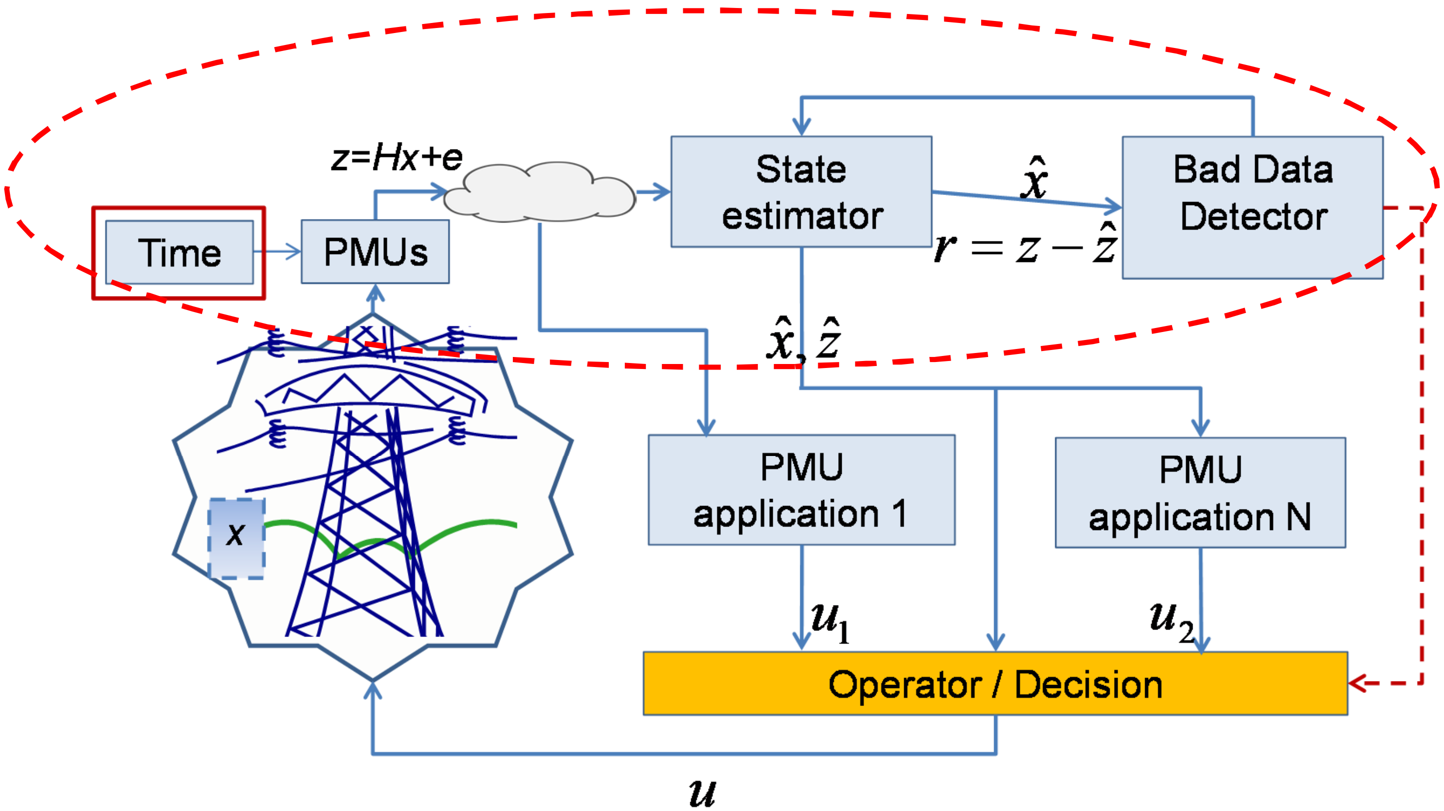
E. Shereen, M Delcourt, S. Barreto, G. Dán, J-Y. Le Boudec, M. Paolone, ``Feasibility of Time Synchronization Attacks against PMU-based State-Estimation,'' IEEE Trans. on Instrumentation and Measurement, to appear

Are Synchrophasors Vulnerable to Time Synchronization Attacks?



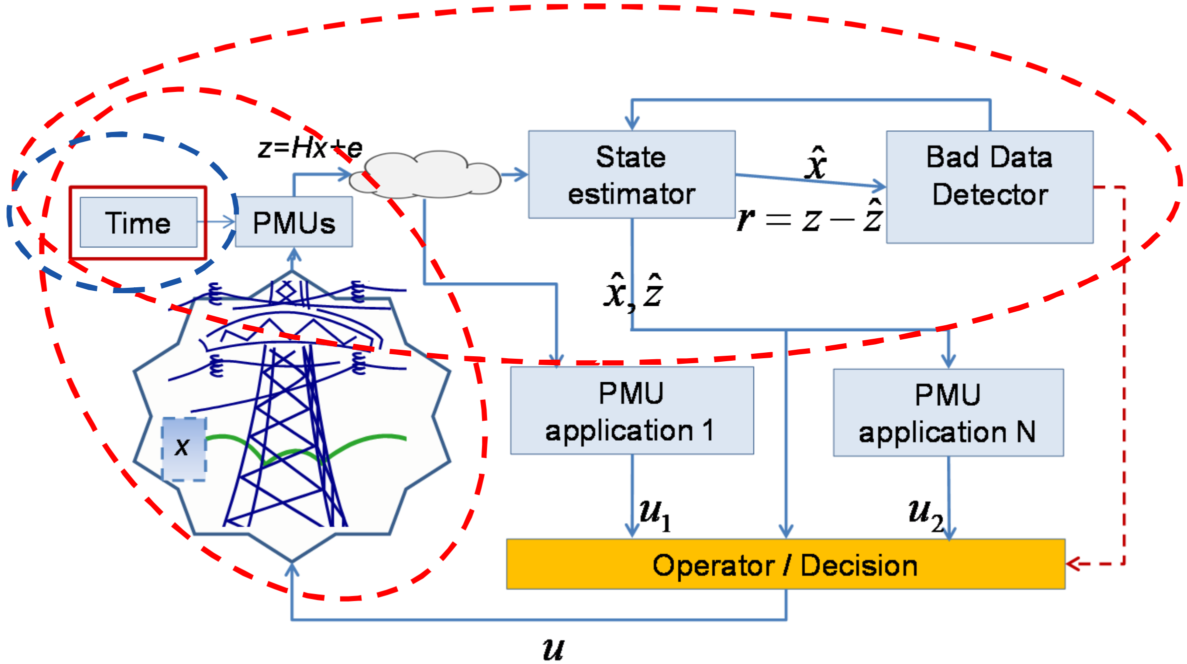
- Could an attacker compromise PMU time references? **YES**
- Could an attack remain undetected? **YES**
- Is an attack easy to compute? **YES**
- Could an attack have significant impact? **YES**

OODA Loop Revisited



Cyber-physical Detection and Mitigation

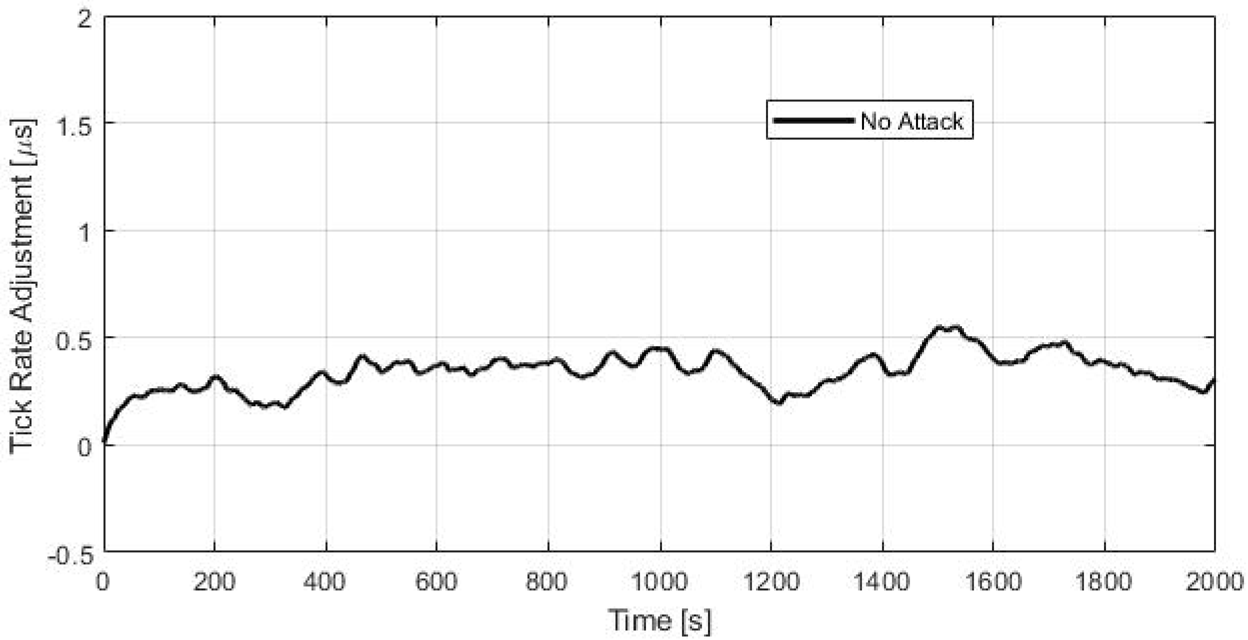
- Impact-based detection
  - Passive
  - Active
    - Perturbation/MTD
  - Measurement level
    - Temporal/spatial
  - Application level



Time Synchronization Attack Detection

Existing approach

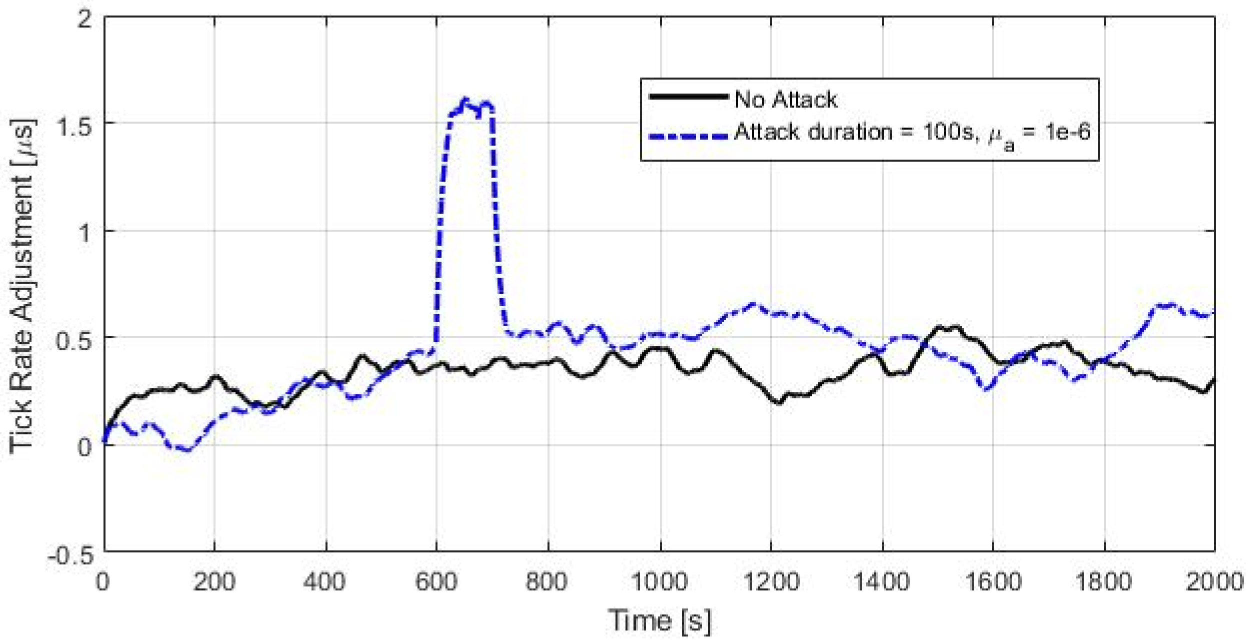
- Tick rate adjustment change detection (e.g., CUSUM)



Time Synchronization Attack Detection

Existing approach

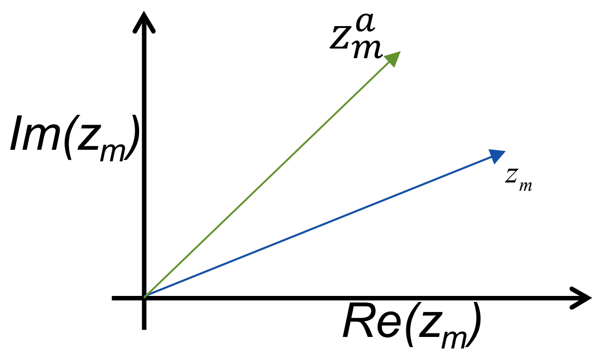
- Tick rate adjustment change detection (e.g., CUSUM)



Correlation-based Time Synchronization Attack Detection

Cyber-physical systems view

- Combine information from physical system and the clock

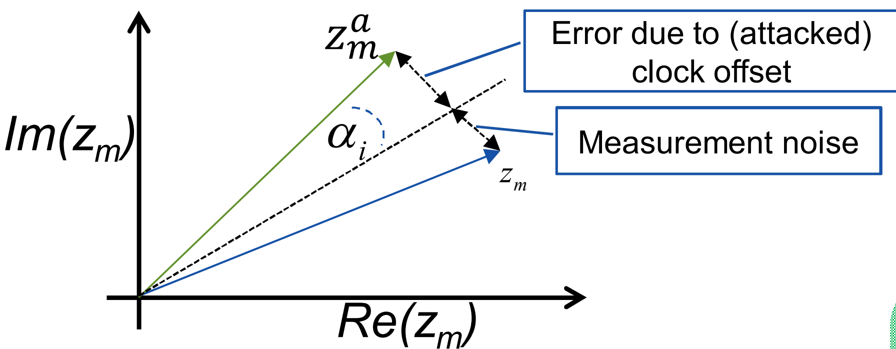


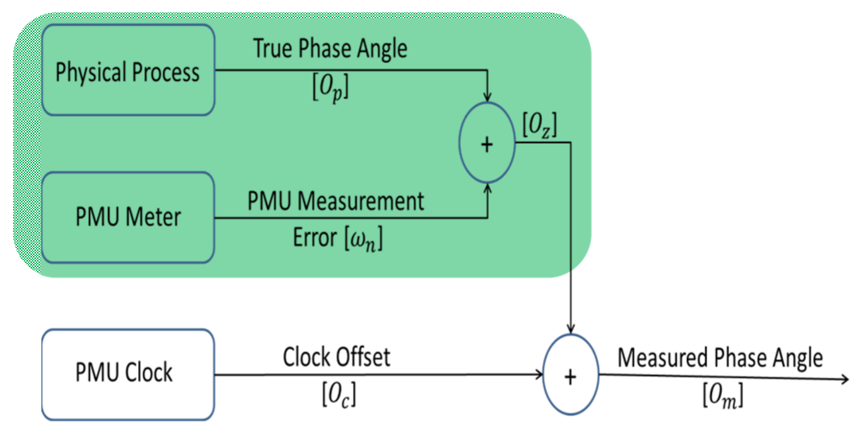
E. Shereen, G. Dán, "Correlation-based Detection of PMU Time Synchronization Attacks," *in Proc. of IEEE SmartGridComm, Oct. 2018*

Correlation-based Time Synchronization Attack Detection

Cyber-physical systems view

- Combine information from physical system and the clock



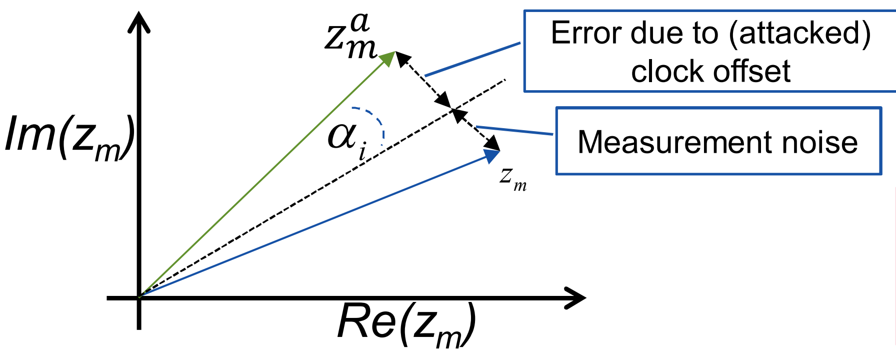


E. Shereen, G. Dán, "Correlation-based Detection of PMU Time Synchronization Attacks," *in Proc. of IEEE SmartGridComm, Oct. 2018*

Correlation-based Time Synchronization Attack Detection

Cyber-physical systems view

- Combine information from physical system and the clock

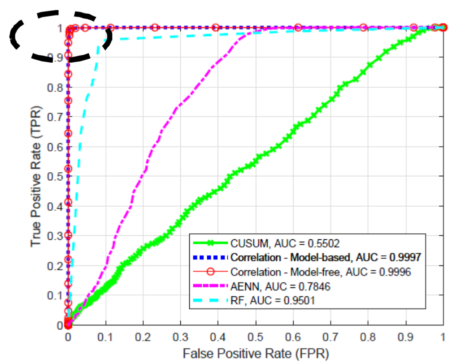


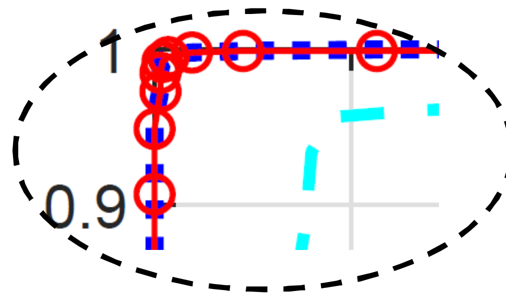
Hypothesis: Attack affects correlation between phase angle sequence and adjustments

Result: Mathematical model of correlation

Proposed detectors:

- Model-based: needs parameter estimation
- Model-free: needs estimated correlation



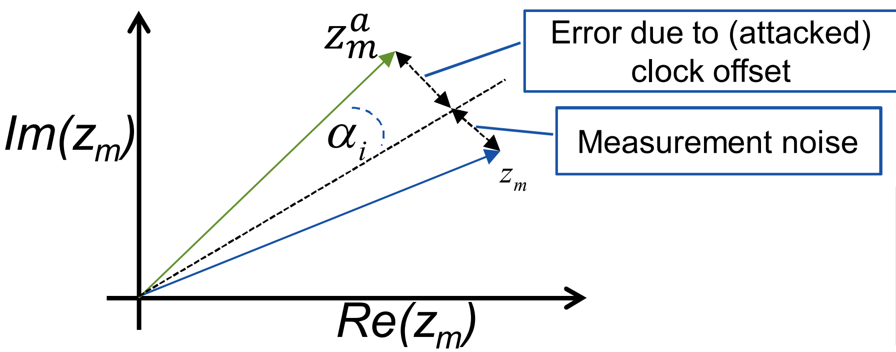


E. Shereen, G. Dán, ‘’ Model-based and Data-driven Detectors for Time Synchronization Attacks against PMUs,” IEEE Journal on Selected Areas in Communications (JSAC), to appear

Correlation-based Time Synchronization Attack Detection

Cyber-physical systems view

- Combine information from physical system and the clock

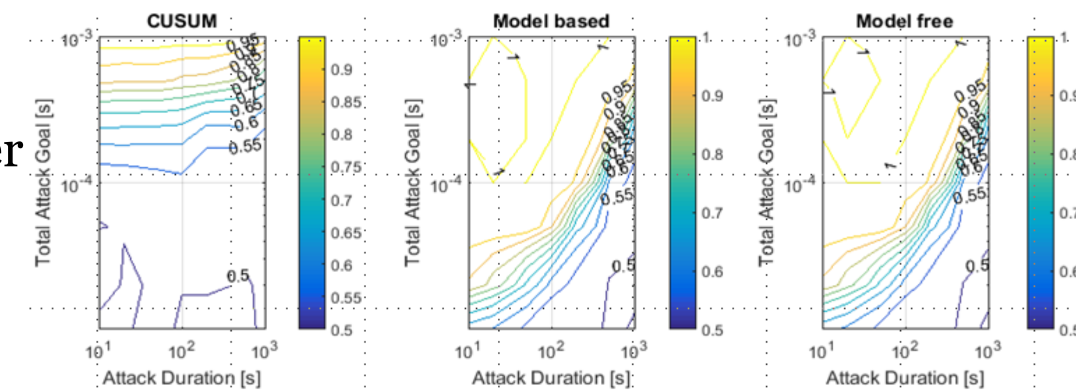


Hypothesis: Attack affects correlation between phase angle sequence and adjustments

Result: Mathematical model of correlation

Proposed detectors:

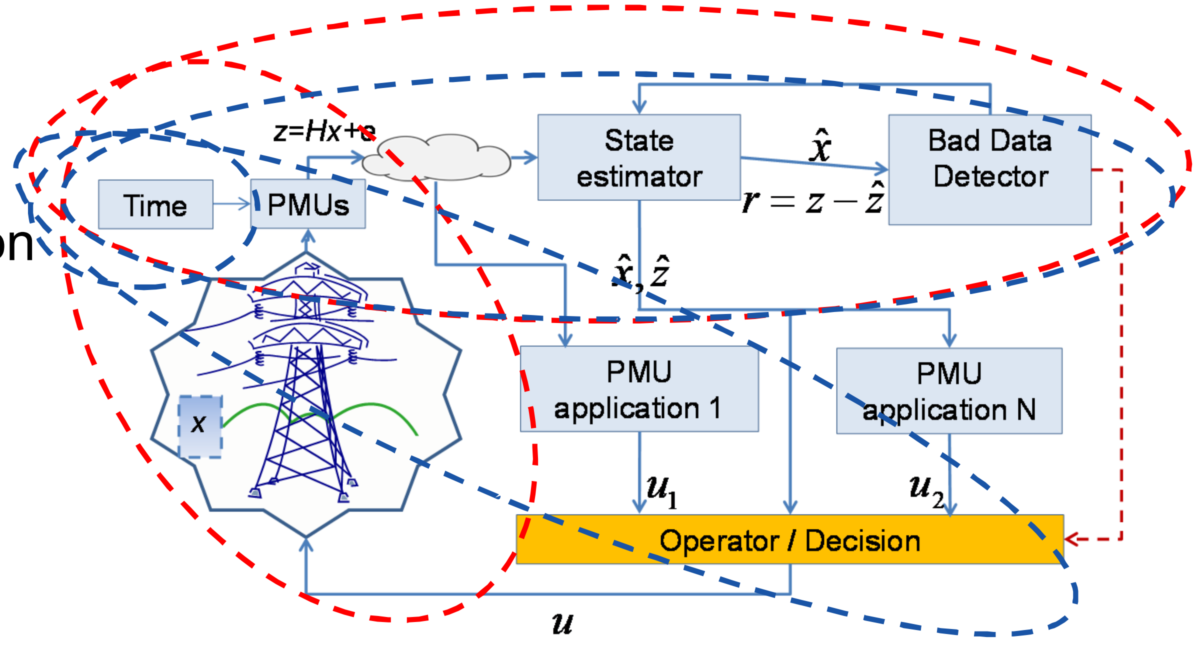
- Model-based: needs parameter estimation
- Model-free: needs estimated correlation



E. Shereen, G. Dán, '' Model-based and Data-driven Detectors for Time Synchronization Attacks against PMUs," IEEE Journal on Selected Areas in Communications (JSAC), to appear

Time for a Resilient Smart Grid

- Detection
  - Passive/Active
  - Measurement/Application
  - Attack characterization



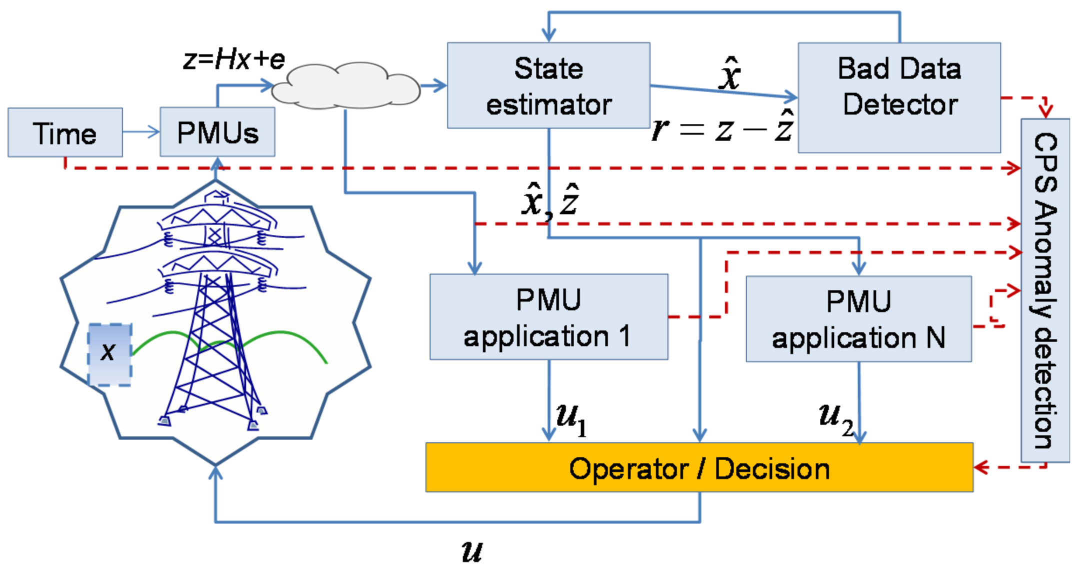
- Mitigation
  - Cyber
  - Cyber-physical

- Design of resilient applications
  - Graceful performance degradation

- Game theoretical models
  - Strategic attacker behavior

Time for a Resilient Smart Grid

- Detection
  - Passive/Active
  - Measurement/Application
  - Attack characterization



- Mitigation
  - Cyber
  - Cyber-physical

- Design of resilient applications
  - Graceful performance degradation

- Game theoretical models
  - Strategic attacker behavior

Acknowledgements

Thanks to

- Ezzeldin Shereen
- Florian Bitard
- Sergio Barreto
- Marguerite Delcourt
- Marco Pignati
- Jean-Yves Le Boudec
- Mario Paolone
- Steffen Fries
- Tolga Sel

References

- E. Shereen, G. Dán, ‘’ Model-based and Data-driven Detectors for Time Synchronization Attacks against PMUs,” IEEE Journal on Selected Areas in Communications (JSAC), to appear
- E. Shereen, F. Bitard, G. Dán, S. Fries, T. Sel,"Next Steps in Security for Time Synchronization: Experiences from implementing IEEE 1588 v2.1," *in Proc. of IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), Sep. 2019*
- E. Shereen, M Delcourt, S. Barreto, G. Dán, J-Y. Le Boudec, M. Paolone, ``Feasibility of Time Synchronization Attacks against PMU-based State-Estimation," IEEE Trans. on Instrumentation and Measurement, to appear
- E. Shereen, G. Dán, "Correlation-based Detection of PMU Time Synchronization Attacks," *in Proc. of IEEE SmartGridComm, Oct. 2018*
- S. Barreto, E. Shereen, M. Pignati, G. Dán, J-Y Le Boudec, M Paolone, “A Continuum of Undetectable Timing-Attacks on PMU-based Linear State-Estimation," in Proc. of IEEE SmartGridComm, Oct. 2017
- 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,* vol. 9, no. 4, Jul. 2018,
- S. Barreto, A. Suresh, J-Y Le Boudec, “Cyber-attack on Packet-Based Time Synchronization Protocols: the Undetectable Delay Box”, in Proc. of IEEE Intl. Instrumentation and Measurement Techn. Conf., 2016
- Cirio et al “Wide area monitoring in the Italian power system: Architecture, functions and experiences”, European Transactions on Electrical Power 21(4):1541 – 1556, 2011
- Tippennhauer et al, “On the requirements for successful GPS spoofing attacks”, in Proc. ACM CCS, 2011
- Ng, Y., Gao, G.X , “Advanced Multi-Receiver Position-Information-Aided Vector Tracking for Robust GPS Time Transfer to PMUs”, GNSS 2015
- N.M. Freris, S.R. Graham, P.R.Kumar, “Fundamental Limits on Synchronizing Clocks over Networks,” TAC 56(6)

KTH ROYAL INSTITUTE
OF TECHNOLOGY

Resilient Time Synchronization for the Smart Grid

Vulnerabilities and Mitigation Schemes

György Dán
KTH/EECS/NSE

IEEE SmartGridComm 2019