Improved IEEE 1588 (PTP) Synchronization using Estimation Theory and Related work

Prof. Rick S. Blum
Robert W. Wieseman Endowled Professorship, IEEE Fellow
Electrical and Computer Engineering Department
Lehigh University
rblum@lehigh.edu
Thanks to Army Research Office, DoE SEEDs cybersecurity center, PITA, LSI
http://www.ece.lehigh.edu/SPCRL/spcrl.htm

Synchronization in LTE 4G Networks

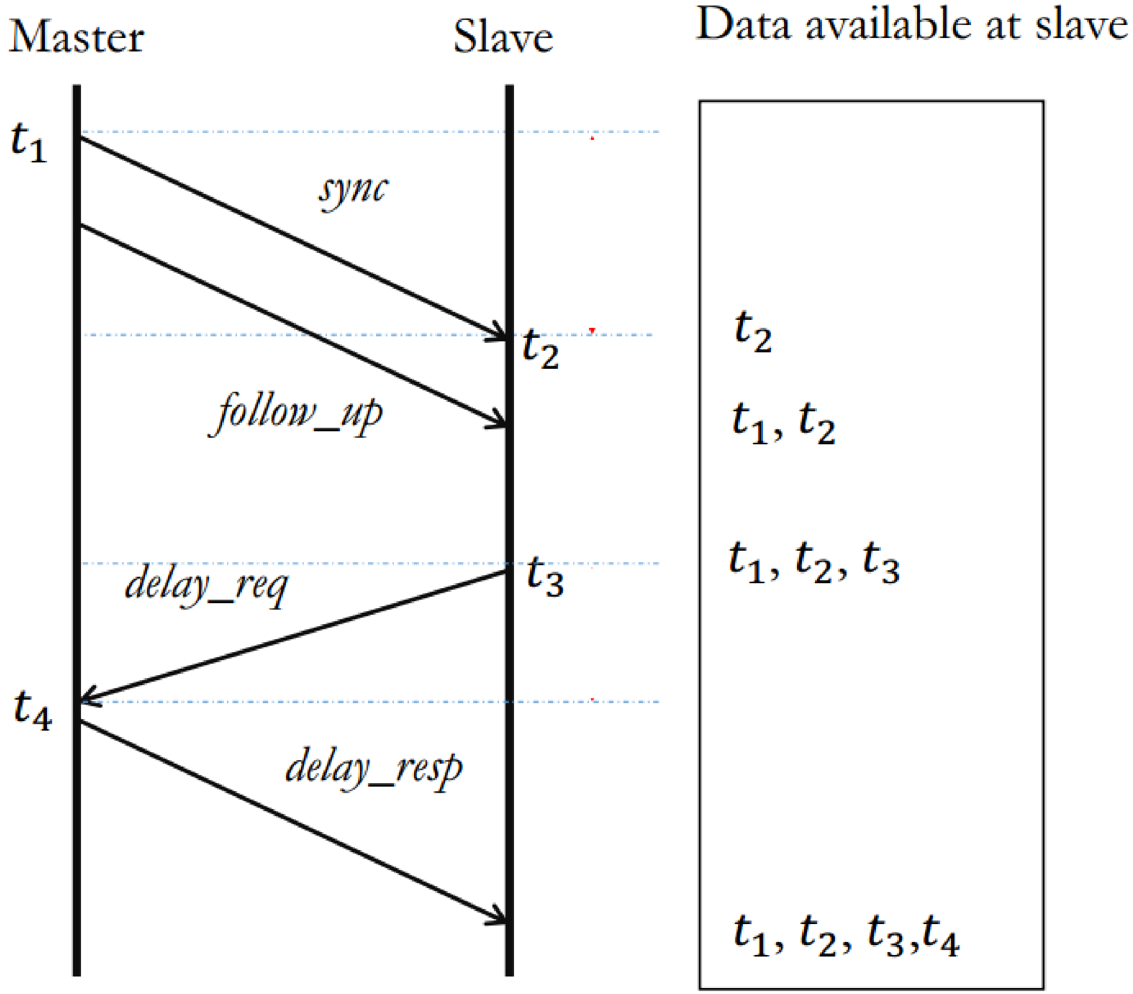
- Synchronization between base station clocks is critical in LTE networks as it allows for
  - ✓Improved capacity
  - ✓Seamless handovers.
- Synchronization based on GPS may be infeasible or expensive.
- IEEE 1588 precision time protocol (PTP) is a cost effective alternative as it can utilize the existing mobile backhaul networks to provide synchronization.
- Typical PTP deployment in 4G networks:
  - Frequency synchronization: achieved via physical layer signals present in synchronous Ethernet (SyncE).
  - Phase synchronization: achieved by exchanging packets over backhaul networks.

Challenges for synchronization in Backhaul Networks

- End-to-end delays in packet switched networks are stochastic – due to random queuing delays at switches/routers.
- Especially true for mobile backhaul networks as they are typically leased from commercial ISPs and shared with other users.
- The random queuing delays hamper the PTP phase synchronization.
- Need to improve PTP phase synchronization performance in these mobile backhaul networks due to stringent accuracy requirements.
- Accuracy requirement in 4G LTE TDD: $|\text{clock phase error}| \leq 1.25\ \mu s$.

Two-way Message Exchange

- Is a fundamental mechanism in many synchronization protocols including PTP.
- The slave node exchanges a series of synchronization packets with the master node and uses the timestamps of the packets to estimate the phase offset.
- Master clock: $c_M(t) = t$.
- Slave clock: $c_s(t) = t + \delta$, where δ denotes the phase offset.
- Data available at slave
  1) t_1
  2) $t_2 = t_1 + d_{ms} + \delta$
  3) t_3
  4) $t_4 = t_3 + d_{sm} - \delta$.
- d_{ms}, d_{sm}: end-to-end delays.
- Aim: Given the time stamps $\{t_1, t_2, t_3, t_4\}$, estimate δ.



- The end-to-end delays can be modeled as:

$$d_{ms} = d + w_1,$$
$$d_{sm} = d + w_2.$$

  - d: constant network delays due to link propagation times.
  - w_1, w_2: variable network delays due to queuing at switches/routers.

- It suffices to retain only the difference of the time stamps

$$y_1 = t_2 - t_1 = d + \delta + w_1,$$
$$y_2 = t_4 - t_3 = d - \delta + w_2.$$

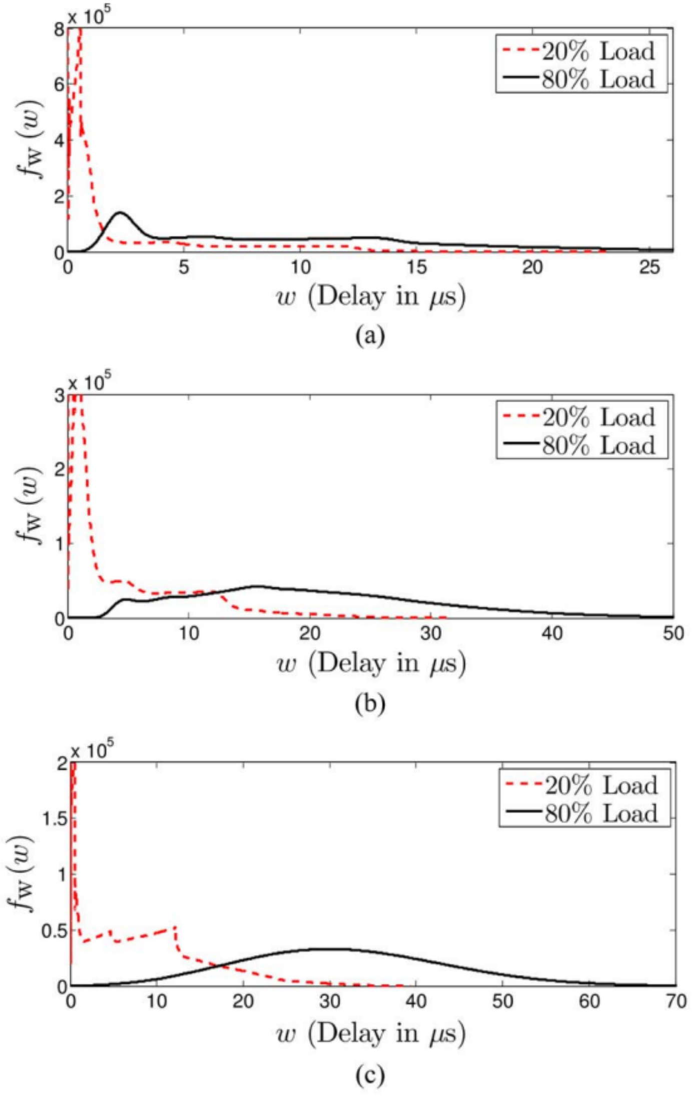
- Suppose P two-way exchanges are performed. We then have

$$\boldsymbol{y} = \boldsymbol{A\theta} + \boldsymbol{w}$$

- where we have $\boldsymbol{y} = [y_{11}, y_{12}, \cdots, y_{1N}, y_{21}, \cdots, y_{2N}]^T$, $\mathbf{w} = [w_{11}, \cdots, w_{1N}, w_{21}, \cdots, w_{2N}]^T$ and $\boldsymbol{\theta} = [d, \delta]^T$.
- **Goal:** Given the observations $\boldsymbol{y}$**,** design a phase offset estimation (POE) scheme to get an estimate of the phase offset δ.

Distribution of the queuing delays

- In the context of backhaul networks, the ITU-T G.8261 specification provides models (Traffic Model 1 - TM1 and Traffic Model 2 - TM2) for modeling the queuing delays.
- Some of these empirical PDF ($f_w(w)$) of the queuing delays under various loads and for varying number of switches are shown:
    a) 10 switches, TM1
    b) 10 switches, TM2
    c) 20 switches, TM1
- The load in a network refers to the percentage of the total link capacity consumed by the background traffic.



Conventional POE schemes

- The commonly used POE schemes have the form

$$\hat{\delta}(\boldsymbol{y}) = \frac{1}{2}[g(y_{11}, \cdots, y_{1P}) - g(y_{21}, \cdots, y_{2P})]$$

where $g(.)$ can be the sample minimum/mean/maximum/median functions.

- The queuing delays in backhaul networks have finite support; as a result, typical bounds such as the Cramer-Rao lower bound are not available to evaluate the performance of a POE scheme since their regularity conditions are violated.

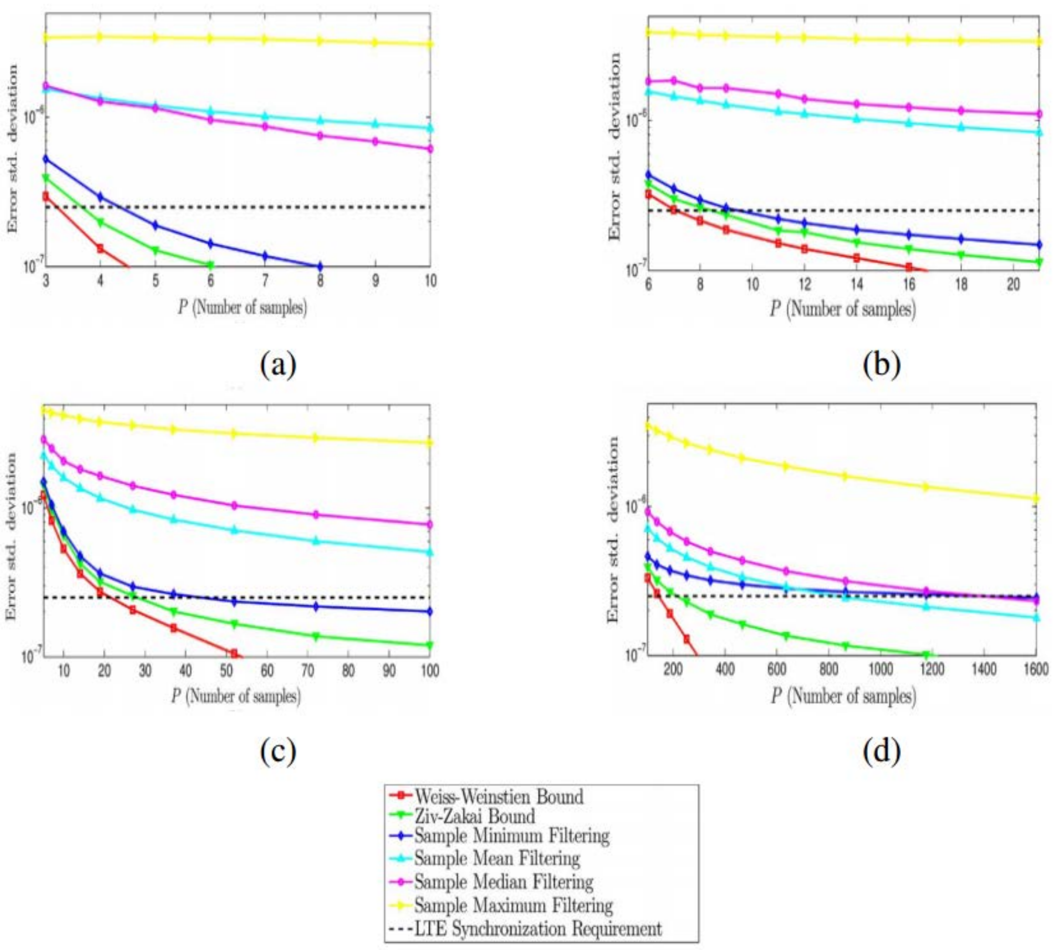
- Little was known on how well the POE schemes perform relative to the theoretical best achievable performance.

Performance lower bounds for POE schemes

- We derived performance lower bounds using the Weiss-Weinstien bound and Ziv-Zakai bound for the POE problem [1].

- These lower bounds are presented along with the performance of some of the available schemes in the literature for the backhaul network scenarios.
  a) TM1 – 20% load
  b) TM2 – 20% load
  c) TM1 – 80% load
  d) TM2 – 80% load

- We can see that the available schemes in the literature are not close to the performance lower bounds in some cases, including those under high load.



[1]. A. Guruswamy, R. S. Blum, S. Kishore, and M. Bordogna, ``Performance Lower Bounds for Phase Offset Estimation in IEEE 1588 Synchronization", IEEE Transactions on Communications, Vol. 63 , No. 1, pp. 243-253, January 2015.

Optimum POE scheme

- We have derived the optimum estimator for the POE problem [2].
- This estimator minimizes the maximum mean squared error (MSE) over all values of the unknown parameters.
- The optimum estimator is an extension of the well-studied Pitman estimator, which is known to be optimum for scalar location parameter problems.
- The optimum estimator provides us with fundamental lower limit on MSE for any POE scheme.

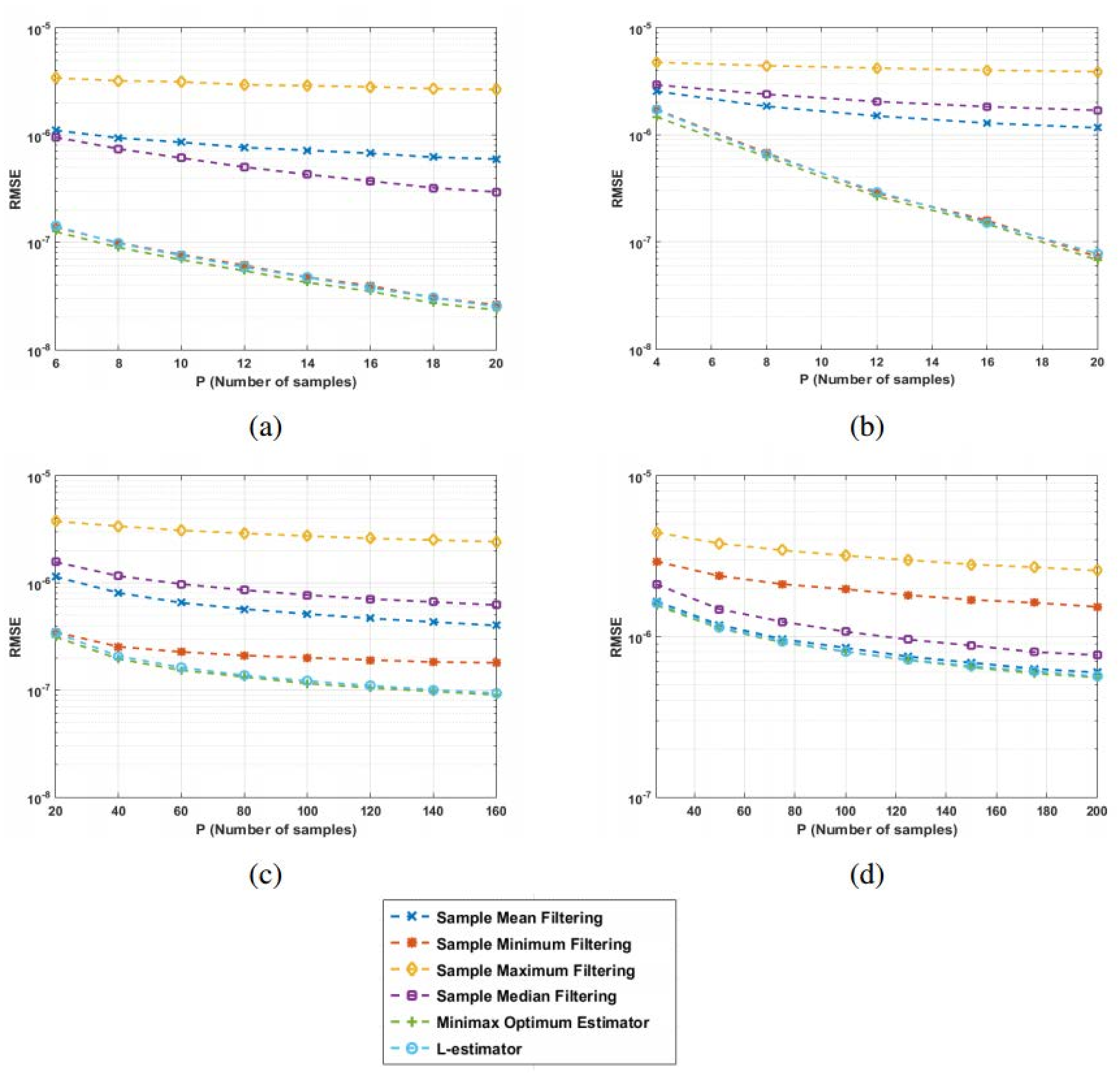
[2]. A. Guruswamy, R. S. Blum, S. Kishore, and M. Bordogna, ``Minimax Optimum Estimators for Phase Synchronization in IEEE 1588", IEEE Transactions on Communications, Vol. 63 , No. 9, pp. 3350-3362, Dec. 2015.

L-estimators

- The optimum estimator offers the best performance in terms of minimizing the MSE.
- However, it is computationally intensive, and requires complete knowledge of the queuing delay distributions.
- As a result, they might not be feasible for real-time scenarios when compared to the conventional POE schemes available in the literature.
- We proposed estimators for the POE problem which are linear combination of order statistics, and require only the mean and the variance of the queuing delay sequence (2 scalars) [3].
- These estimators, referred to as L-estimators, while being computationally efficient are robust to network model uncertainties, and offer near optimal performance in a wide variety of network scenarios.

[3]. A. Guruswamy, R. S. Blum, S. Kishore, and M. Bordogna, ``On the Optimum Design of L-Estimators for Phase Offset Estimation in IEEE 1588", IEEE Transactions on Communications, Vol. 63 , No. 9, pp. 5101-5115, Dec. 2015.

Simulation results



- Standard deviation of estimator error with 10 switches and cross traffic flows under varying load factors.
    a) TM1 – 20% load
    b) TM2 – 20% load
    c) TM1 – 80% load
    d) TM2 – 80% load.

Overview of Related Research in our Lab at Lehigh

- We are presently working on combating delay attacks in PTP (ARO). Journal paper just submitted:

Anantha K. Karthik and Rick S. Blum, Estimation Theory Based Robust Phase Offset Estimation in the Presence of Delay Attacks, IEEE Trans Communications (on arXiv).

- We have research on GPS spoofing attack detection on PMU data (DoE).
- We have research on mitigation of general spoofing and man-in-the middle attacks of sensor systems (ARO), including GPS spoofing as special case (4 journal papers).
- We have research on showing DoA checking will not protect you from GPS spoofing (see last slide).

Other Applications: The Grid: Our DoE Cybersecurity Center (SEEDs)

https://seedscenter.uark.edu/

P. Pradhan, K. Nagananda, P. Venkitasubramanium, S.Kishore and R.S. Blum, ”GPS Spoofing Attack Characterization and Detection in Smart Grids,” IEEE Conference on Communications and Network Security, 2016.

Publication List For General Attacks on Sensor and IoT Systems

1. J. Zhang, R. S. Blum, X. Lu, and D. Conus, “Asymptotically optimum distributed estimation in the presence of attacks,” *Signal Processing, IEEE Transactions on*, vol. 63, no. 5, pp. 1086–1101, March 2015.
2. B. Alnajjab, J. Zhang, and R. S. Blum, “Attacks on sensor network estimation systems with quantization: Performance and optimum processing,” vol. 63, no. 24, pp. 6659-6672, IEEE Transactions on Signal Processing, Dec.15, 2015
3. J. Zhang, R. S. Blum, L Kaplan, and X. Lu, “Functional Forms of Optimum Spoofing Attacks for Vector Parameter Estimation in Quantized Sensor Networks,” accepted to IEEE Transactions on Signal Processing.
4. J. Zhang and R. S. Blum, “Distributed estimation in the presence of attacks for large scale sensor networks,” in Information Sciences and Systems (CISS), 2014 48th Annual Conference on. IEEE, 2014, pp. 1–6.
5. B. Alnajjab and R. S. Blum, “After-attack performance of parameter estimation systems,” in Information Sciences and Systems (CISS), 2014 48th Annual Conference on. IEEE, 2014, pp. 1–6.
6. J. Zhang and R. S. Blum, “Distributed joint spoofing attack identification and estimation in sensor networks,” in Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit International Conference on. IEEE, 2015.
7. J. Zhang, R. S. Blum, L. Kaplan, and X. Lu, “A fundamental limitation on maximum parameter dimension for accurate estimation using quantized data,” submitted to IEEE Transactions on Information Theory.

DoA Checking Protection for GPS (more)

1. There are some who think that GPS spoofing can be completely solved by checking direction of arrival.

2. This is not really true as our research shows.

3. Seeking funding for further studies.