Cyber Attacks on Internet of Things Sensor Systems for Inference

Rick S. Blum and Collaborators
IEEE Fellow, IEEE SPS Distinguished Lecturer
SEEDS Lehigh lead PI
Department of Electrical and Computer Engineering, Lehigh University

Center for Advanced Signal and Image Sciences workshop at the Lawrence Livermore National Laboratory Keynote

LEHIGH UNIVERSITY

Greeting from Lehigh University. Collaborations Welcome. Visit our beautiful campus between NYC & Phila. www.ece.lehigh.edu

Strong Theoretical Researchers on cybersecurity and machine learning
rblum@Lehigh.edu

The Internet of Things (IoT) makes possible Smart-X where

$$X \in \left\{ \begin{array}{c} city, factory, grid, \\ building, home, transportation, \\ healthcare, agriculure, metering \end{array} \right\}$$

Borrowed from
Vince Poor, Princeton

Importance of IoT:

- IoT a market opportunity for equipment manufacturers, internet service providers and application developers.
- Over 1 trillion IoT sensors, machines, objects, devices by 2022
- IoT smart objects to reach 45% of all Internet traffic by 2022
- Top Three Applications and Market Share: Healthcare (41%), Manufacturing (37%), Electricity (7%)

Security of IoT:

- Desired real time control/reaction & low complexity sensor nodes makes standard security too slow and complex

- Interest in layers of security and new approaches

Solutions:

- 1. Use the best processing with multiple sensors to combat attacks on sensor data and communications (focus here)

- 2. Employ lower complexity encryption and authentication

- 3. Employ Physical Layer Security

LEHIGH UNIVERSITY

Goal/Focus:

J. Zhang, R. S. Blum and H. V. Poor, "Approaches to Secure Inference in the Internet of Things", IEEE Signal Processing Magazine, Vol 35, Issue 5, pp. 50-63, 2018.

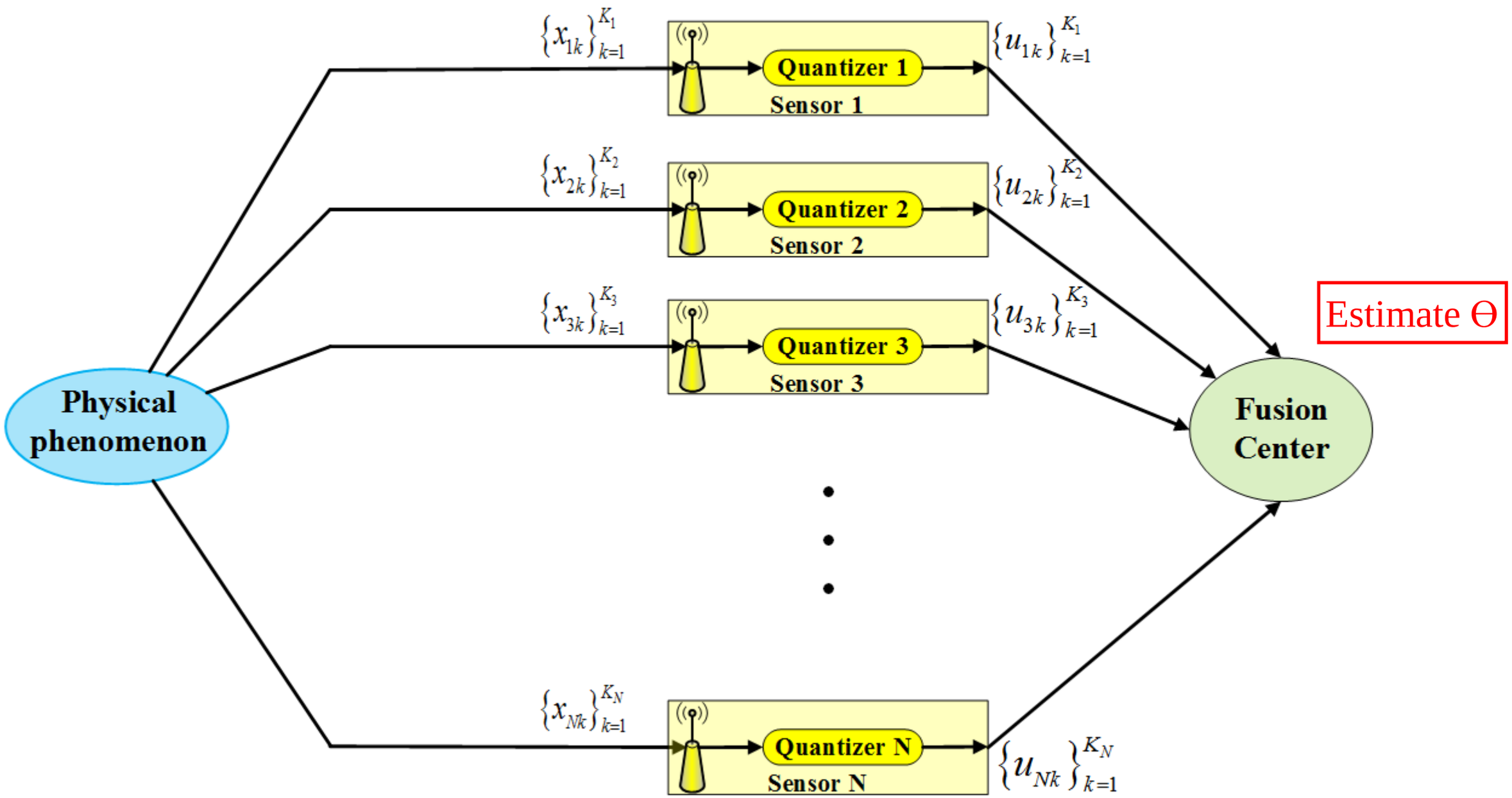
- Attackers modify data entering/communicated from sensors.

- Provide tight bounds (w sufficient data) on performance of best algorithms trying to estimate a parameter after attack.
- Results hold for any estimation algorithm, deep learning, machine learning, ….
- Example algorithms that achieve performance close to bounds illustrated. Use attacked data? How?
- Attacks that make attacked data useless for reducing bounds described. Attacks provide guaranteed degradation to bounds regardless of the algorithms the estimation system employs.

- References are supplied for various extensions to all results.
- Beyond sensing - Brief discussion of applications to IEEE 1588 for clock synchronization is provided.

1. Multiple Sensor Network Estimation System

Phenomenon → Sensors → Fusion Center:



Simple Estimation Problem

Temperature Estimation Example:

In the ABSENCE any attacks:

- At each sensor: Measured Temperature = Actual temperature + Noise

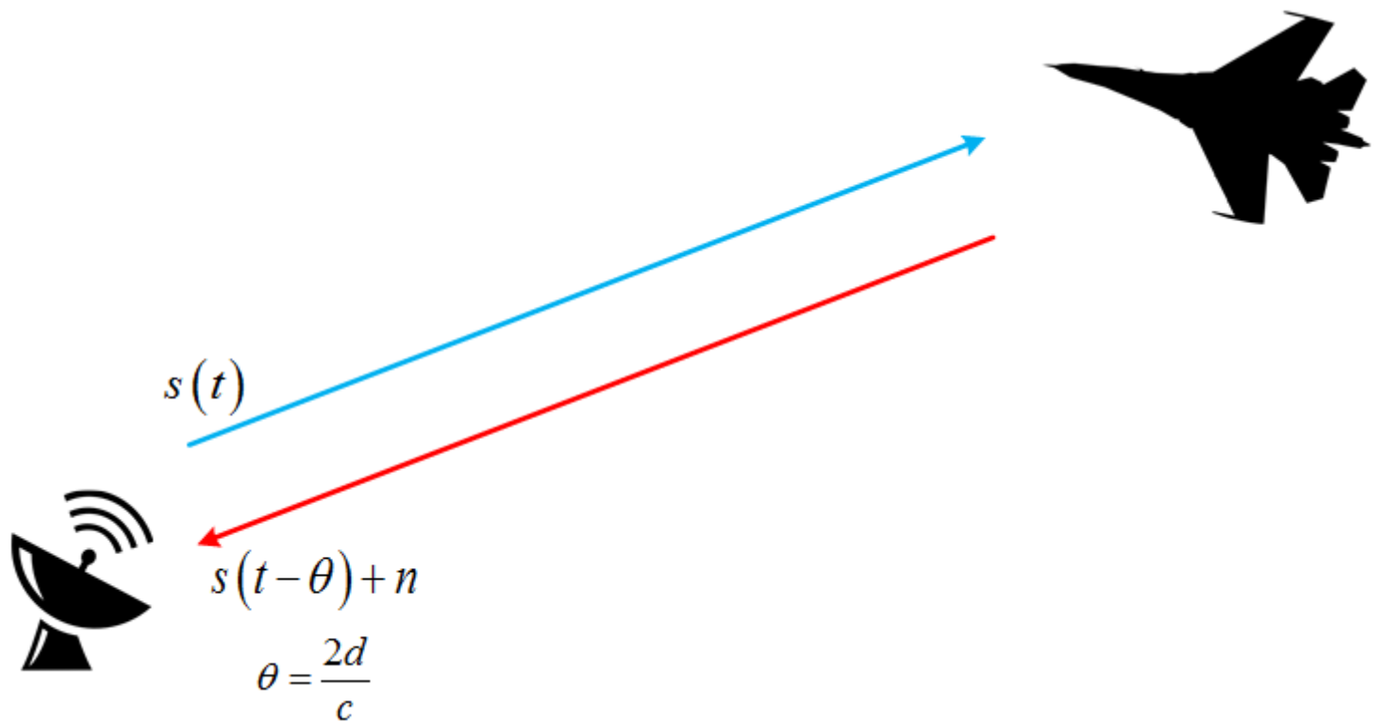
- The noise at each sensor is independent (unrelated) to others

- $X_{jk} = \theta + W_{jk}$ *so* $X_{jk} \sim N(\theta, \sigma^2)$

More Complicated Estimation Problem

Estimation Example in Radar System (Localization):

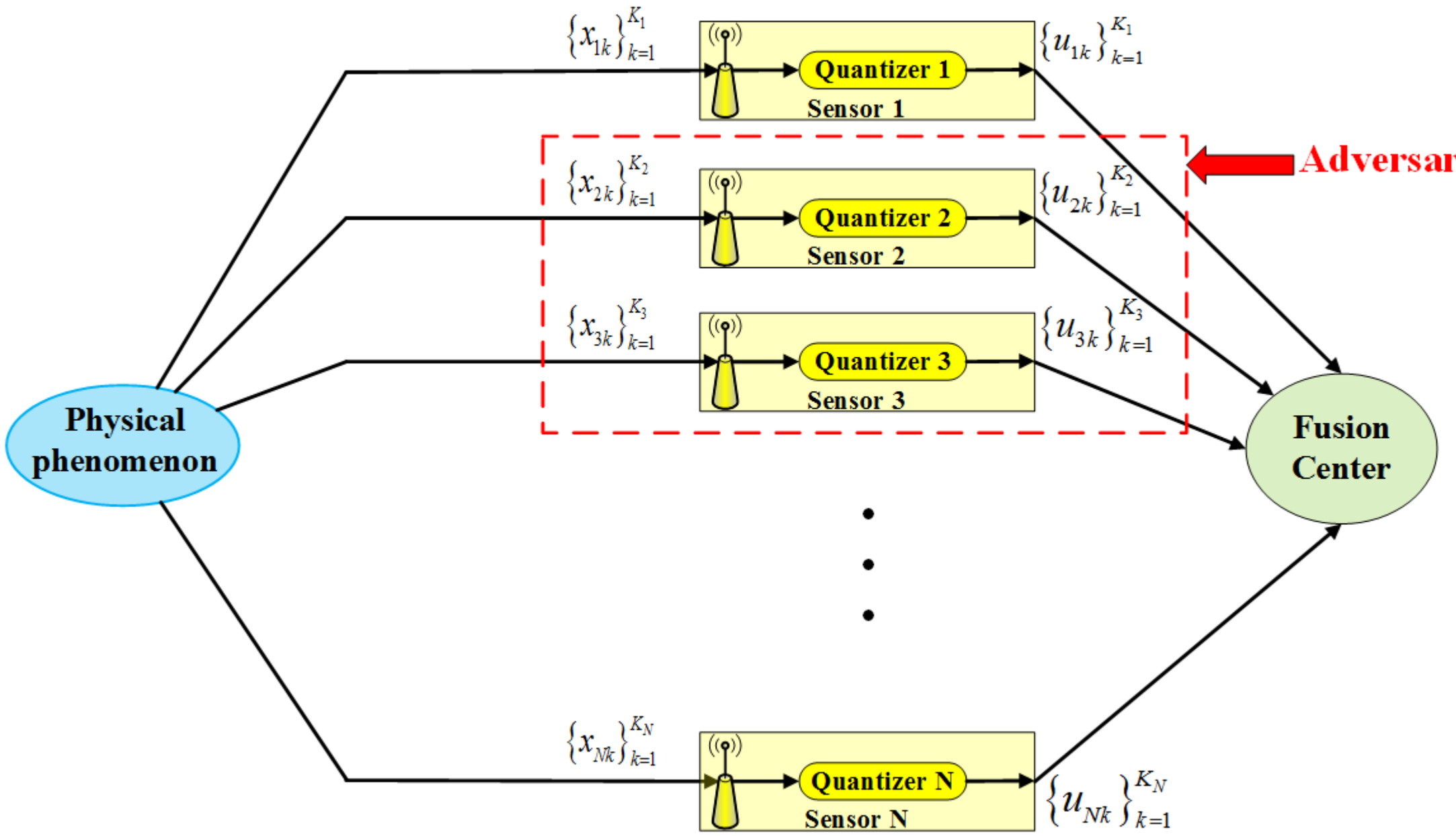
In the ABSENCE any attacks:



Self driving cars

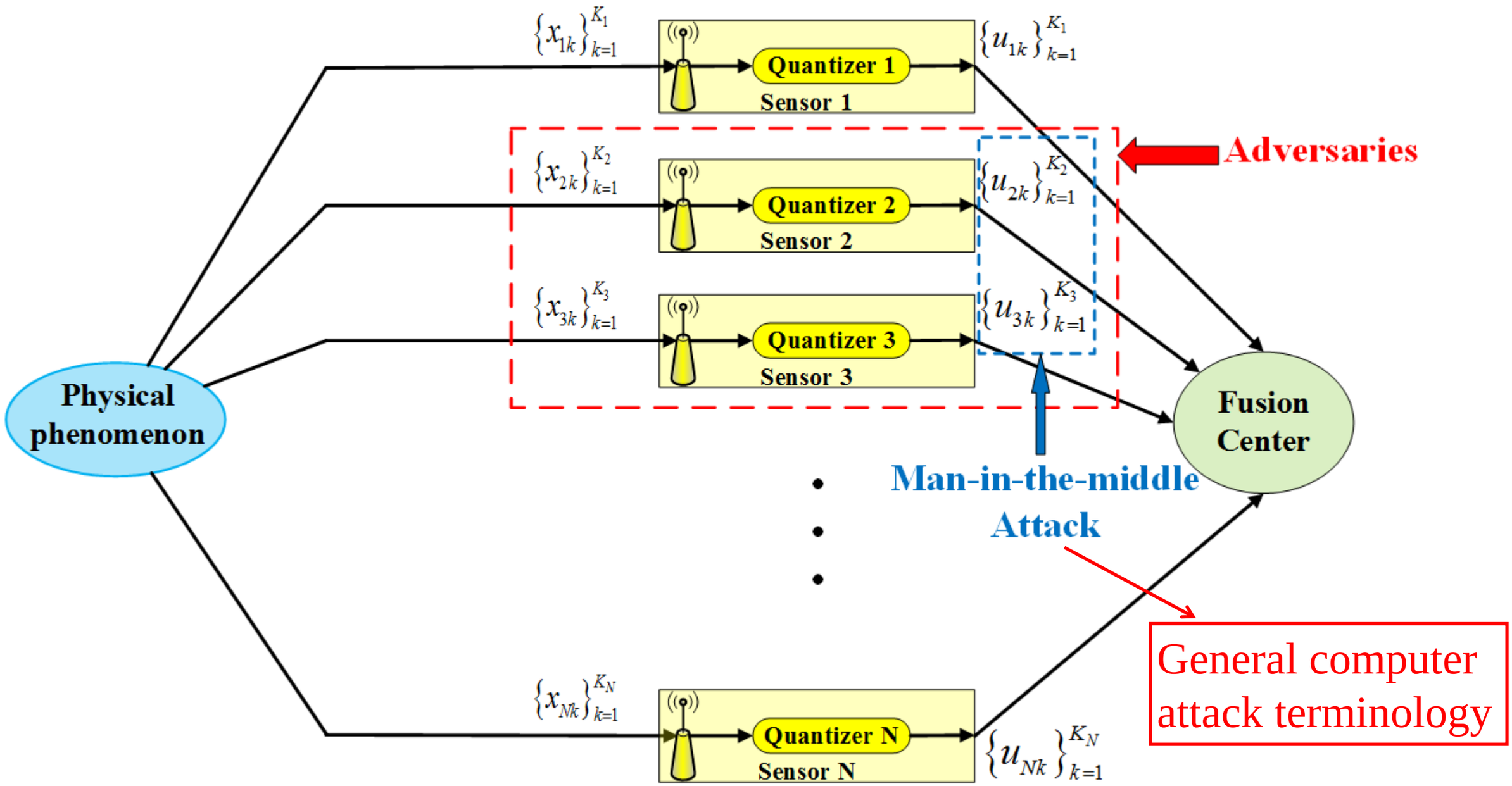
Attacks on Distributed Sensor Network Estimation System

Phenomenon → Sensors → Fusion Center:



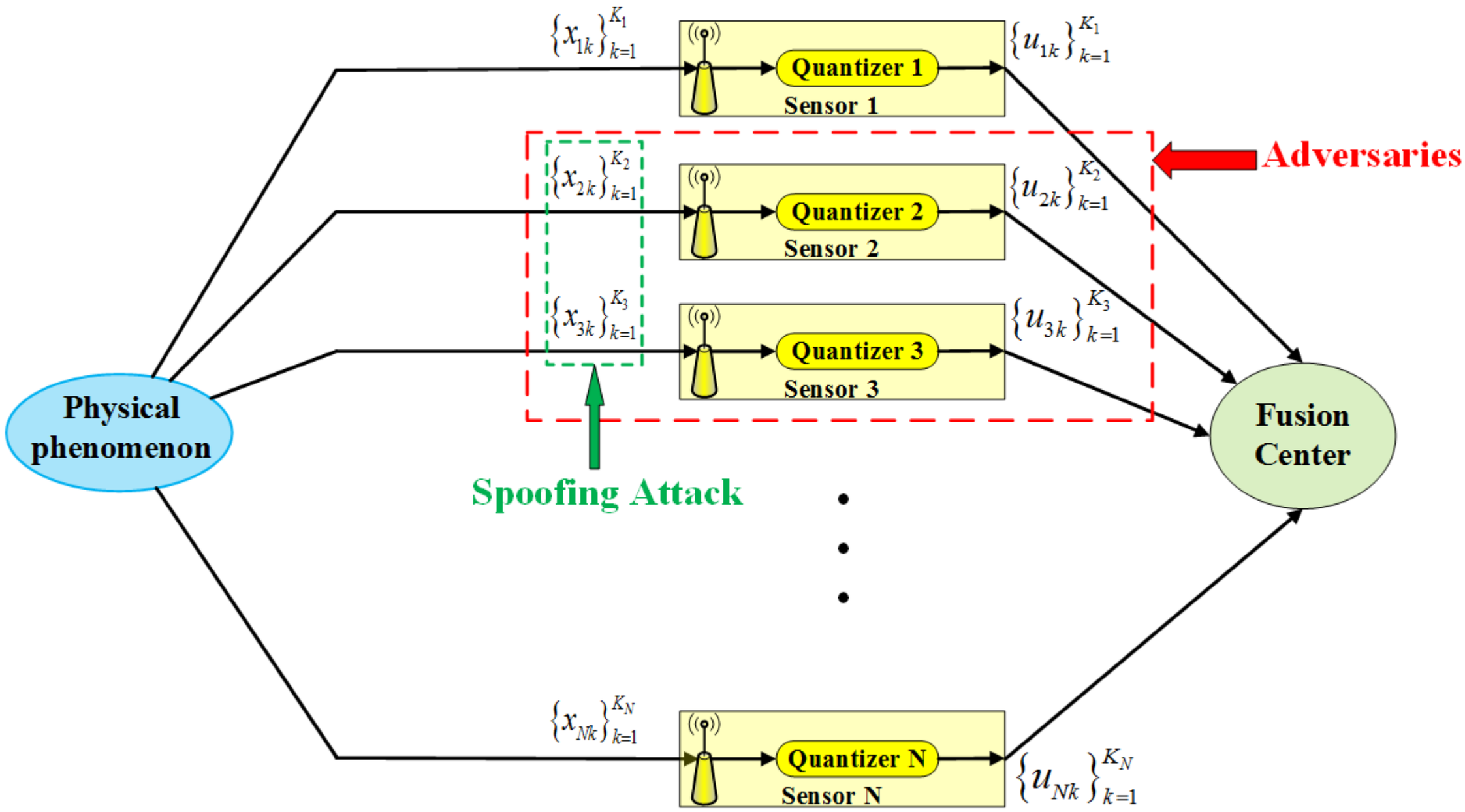
Attacks on Distributed Sensor Network Estimation System

Spoofing Attacks and Man-in-the-middle Attacks :



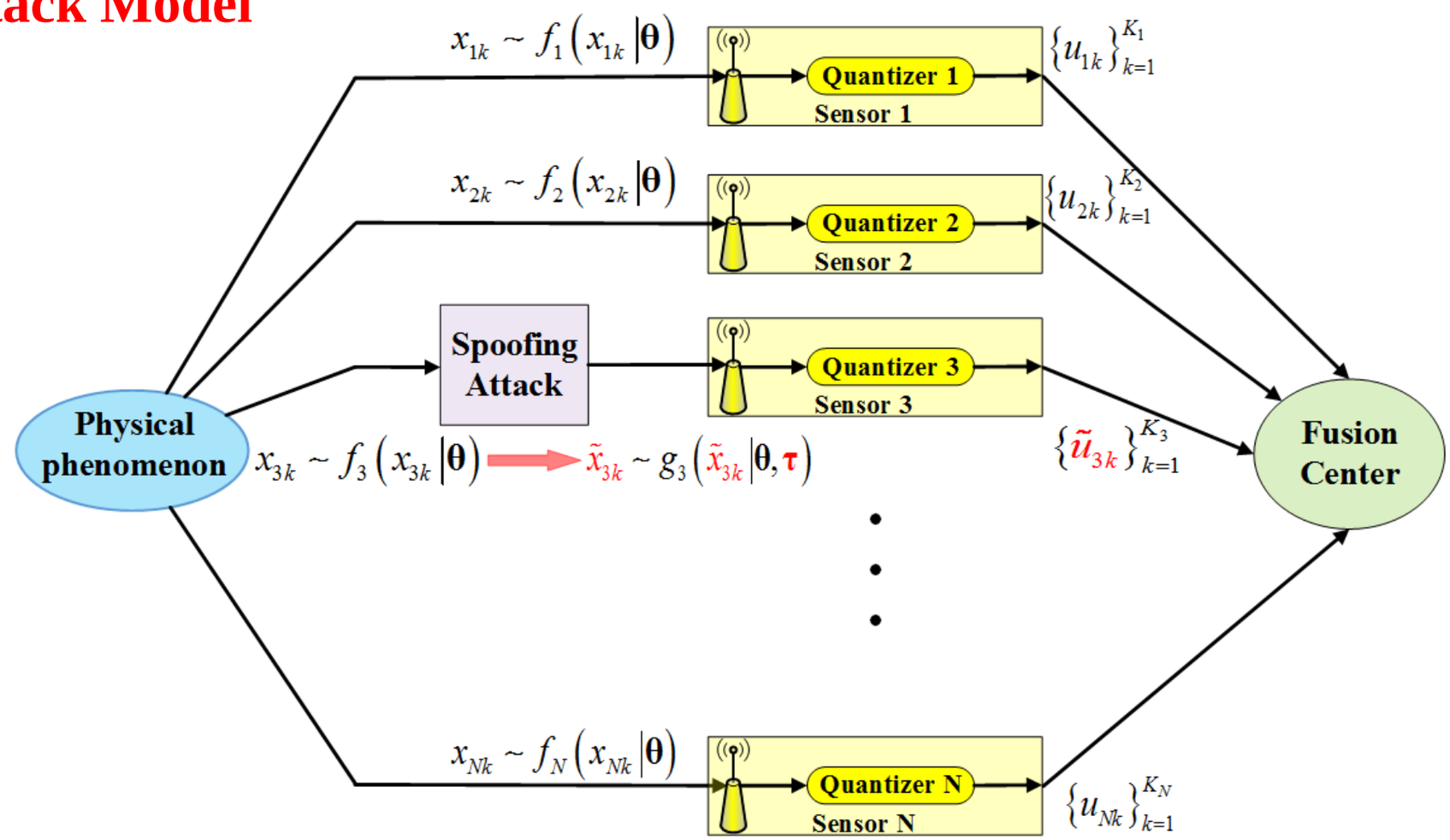
Attacks on Distributed Sensor Network Estimation System

Spoofing Attacks and Man-in-the-middle Attacks:



Distributed Estimation System and Attack Model

With Attack Model



If j-th sensor is under the p-th spoofing attack, then

$$x_{jk} \rightarrow \tilde{x}_{jk}$$

$$\boxed{f_j(x_{jk}|\boldsymbol{\theta}) \rightarrow g_j(\tilde{x}_{jk}|\boldsymbol{\theta},\boldsymbol{\tau})}$$

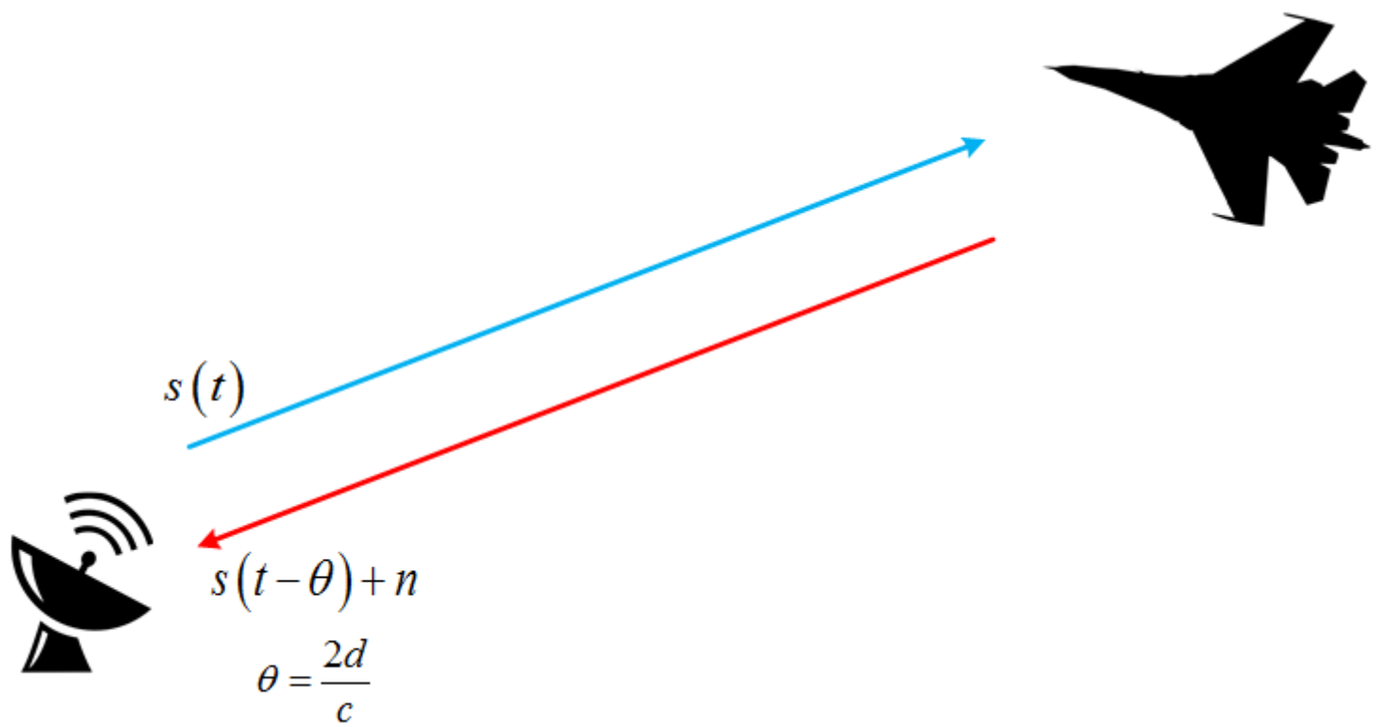
Spoofing attack changes the pdf of obs, and new pdf can depend on $\boldsymbol{\tau}$

Attack Vector Parameter

Motivation of Spoofing Attack Model

Simple Example in Radar System:

In the ABSENCE of spoofing attacks:



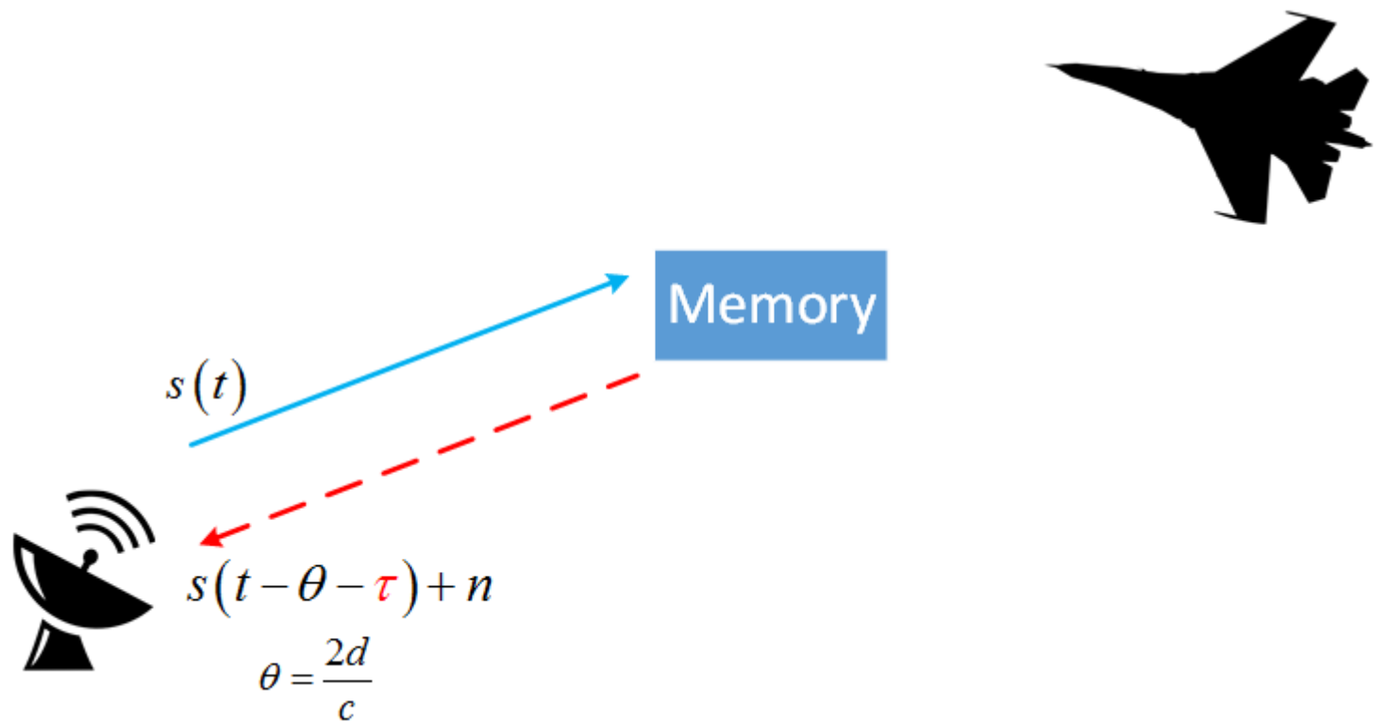
Spoofing Attacks in Radar Systems [6, 7]: Radars will appear in all cars (esp self-driving) to fuse with video to avoid hitting people.

Radar chips costing less than $1 under development -> All IoT

Motivation of Spoofing Attack Model

Simple Example in Radar System:

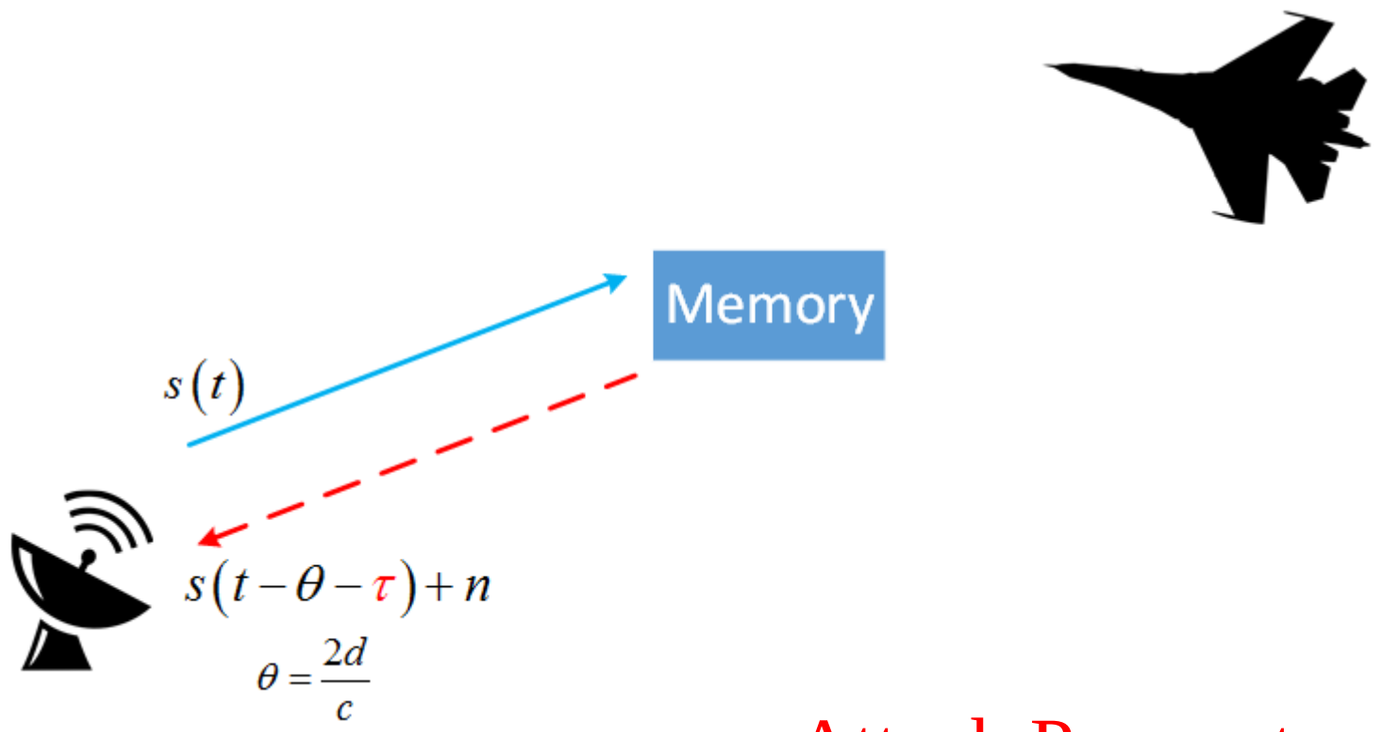
In the PRESENCE of spoofing attacks:



Motivation of Spoofing Attack Model

Simple Example in Radar System:

In the PRESENCE of spoofing attacks:



Attack Parameter

The essential effect of the spoofing attack:

$$f(x|\theta) \xrightarrow{\text{Under Spoofing Attack}} g(x|\theta,\tau) = f(x|\theta+\tau)$$

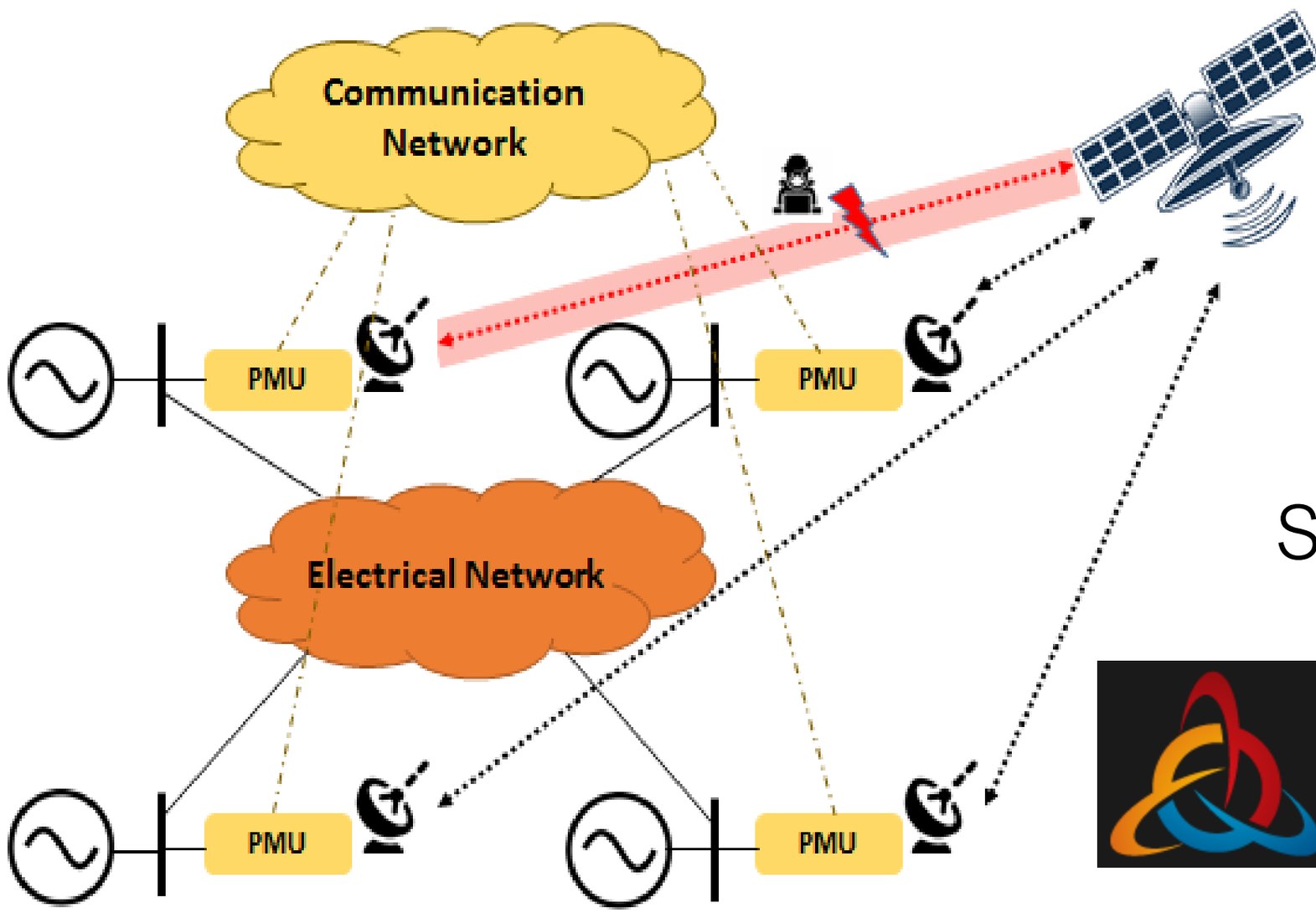
Similar spoofing attack examples can be found in **Smart grids**.

In one special case where one modified delay term returns

Great Interest in Spoofing Attacks

Spoofing Attacks in Smart Grids [3-5]: Falsify the measurements at the attacked Phasor Measurement Units, e.g. data-injection attack. or GPS spoofing

[3] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, “Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions,” Signal Processing Magazine, IEEE, vol. 29, no. 5, pp. 106–115, 2012.
[4] T. T. Kim and H. V. Poor, “Strategic protection against data injection attacks on power grids,” Smart Grid, IEEE Transactions on, vol. 2, no. 2, pp. 326–333, 2011.
[5] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” Smart Grid, IEEE Transactions on, vol. 2, no. 4, pp. 645–658, 2011.



GPS Spoofing

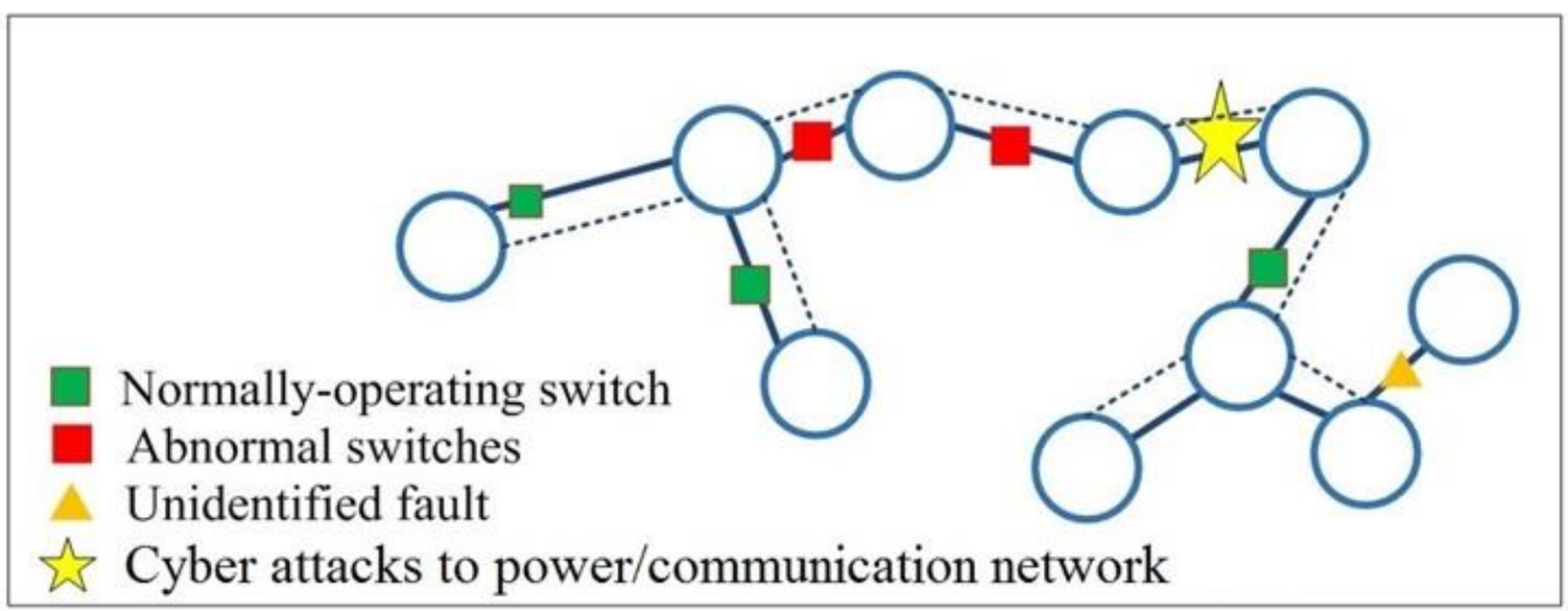
Topology Attacks (with CMU)

Topology attacks in Smart Grid [6-8]: Affect the network operator's knowledge of the topology of the grid either by physically affecting the lines in the grid (***Physical Topology Attacks***) or by manipulating the topological information communicated to the operator (***Cyber Topology Attacks***).

[6] J. Weimer, S. Kar, and K. H. Johansson, "Distributed detection and isolation of topology attacks in power networks," in Proceedings of the1st international conference on High Confidence Networked Systems. ACM, 2012, pp. 65–72.

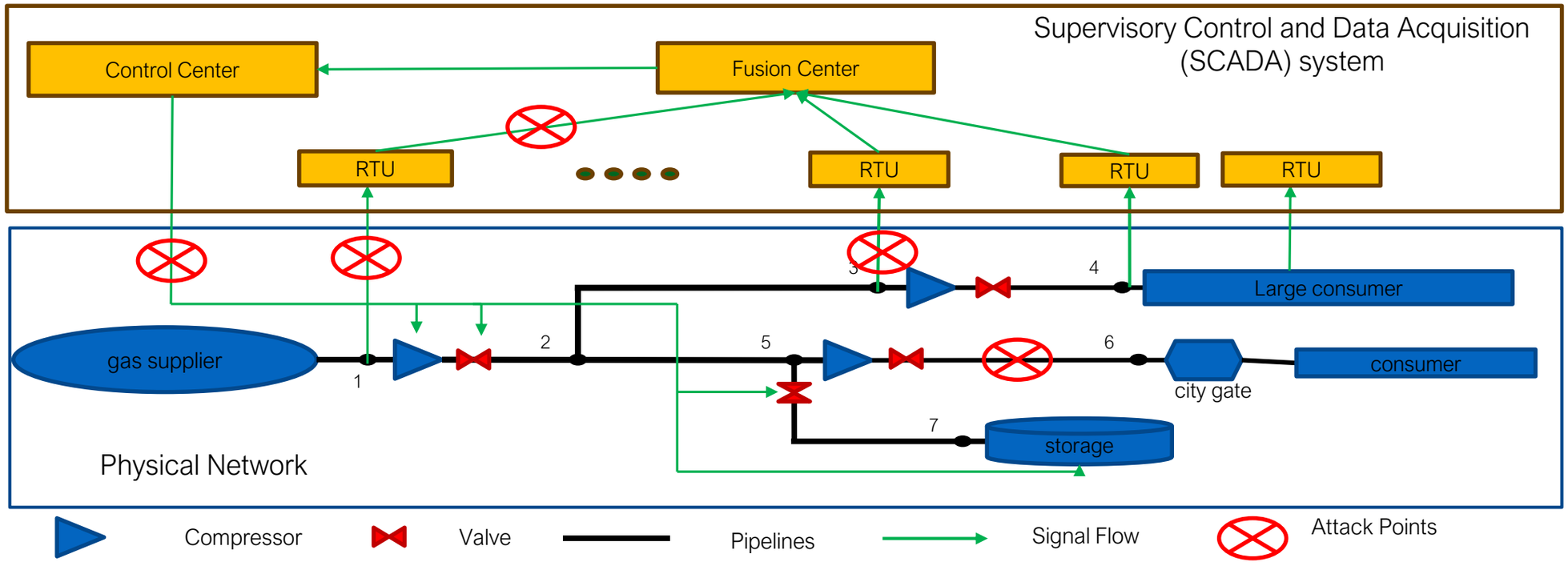
[7] Ananth Narayan Samudrala, M. Hadi Amini, Soummya Kar, and Rick S. Blum, "Optimal Sensor Placement for Topology Identification in Smart Power Grids", 2019 53rd Annual Conference on Information Sciences and Systems (CISS), March 2019.

[8] Ananth Narayan Samudrala, M. H. Amini, S. Kar, and R. S. Blum, "Sensor Placement for Outage Identifiability in Power Distribution Networks", submitted to IEEE Transactions on Smart Grid, 2019.



Attacks on Natural Gas Networks

- **Natural gas networks** threatened by cyber-attacks [9].
- Topology also important for natural gas networks. Incorrect topology information can cause the operator to apply inappropriate control causing **damage** and **disturption**.
- Operator can use our **topology verification algorithm [10]** to determine from sensor measurements if the topology matches what the operator believes.
- Gas networks threated by other types of cyber attacks: false data injection, spoofing attack and man-in-the-middle attack [11].



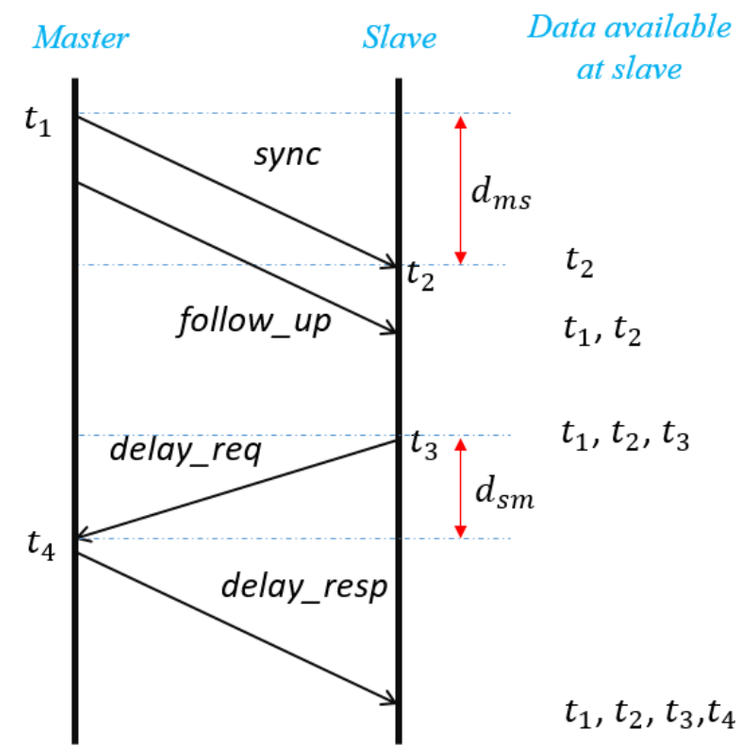
[9] Ponemon Institute, “The state of cybersecurity in the oil & gas industry: United States”, U.S. , 2017, pp 1-6.

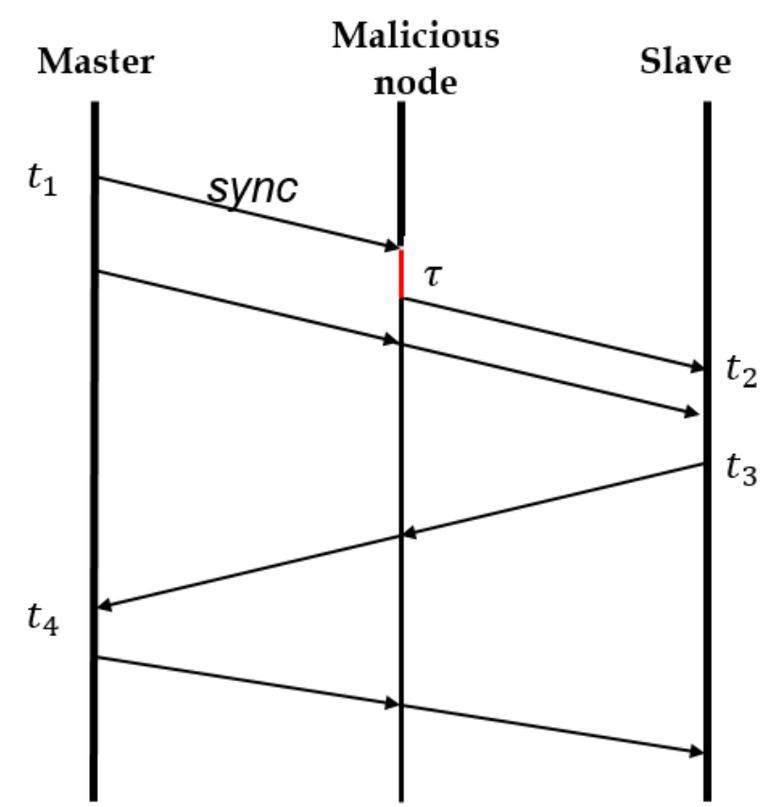
[10] Z. Wang and R. Blum, “Topology attack detection in natural gas delivery networks”, in Information Sciences and Systems (CISS), 2019 53rd Annual Conference on. IEEE, 2019, pp. 1–6.

[11] V. Do, L. Fillatre, I. Nikiforov, and P. Willett, “Security of SCADA systems against cyber-physical attacks”, IEEE Aerospace and Electronic Magenize, Vol. 32, pp 28-45, 2017.

Delay Attacks in IEEE 1588

- IEEE 1588 is a popular time synchronization protocol offering timing accuracy close to GPS-based timing.
- Standard prescribed by Time-Sensitive Networking task group of the IEEE 802.1 working group and used in LTE networks, smart grids and Industrial automation applications.
- Generally assumed that propagation delays in the forward and reverse path are equal. (Necessary for obtaining a unique solution for the clock skew and offset.)
- Malicious nodes can delay timing packets, degrading the performance of the clock synchronization algorithms [12]. Delay attacks CANNOT be countered using cryptographic protocols, as the attacker is not modifying the content of the timing packet [13-14].





[12]. M. Ullmann and M. Vögeler, "Delay attacks — Implication on NTP and PTP time synchronization," *2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, Brescia, 2009, pp. 1-6.

[13] A. K. Karthik and R. S. Blum, "Estimation theory-based robust phase offset determination in presence of possible path asymmetries", in IEEE Transactions on Communications, vol. 66, no. 4, pp. 1624–1635, April 2018.

[14] A. K. Karthik and R. S. Blum, "Robust phase offset estimation for IEEE 1588 PTP in electrical grid networks", in 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, August 2018, pp. 1–5.

LEHIGH UNIVERSITY

Part I: Optimum Processing in the Presence of Man-in-the-Middle Attacks - Asymptotic

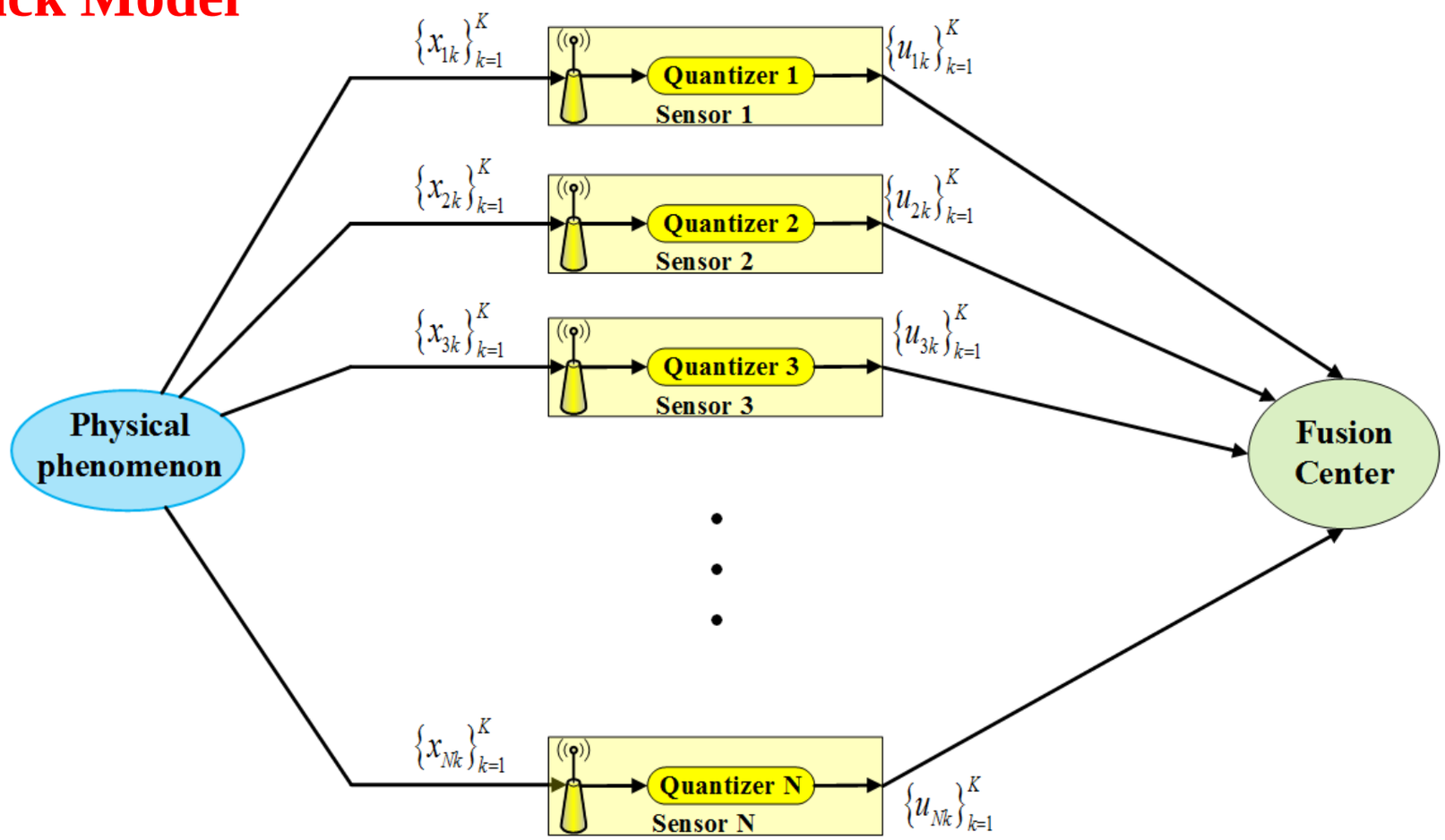
J. Zhang, R. S. Blum, X. Lu, and D. Conus, “Asymptotically optimum distributed estimation in the presence of attacks,” Signal Processing, IEEE Transactions on, vol. 63, no. 5, pp. 1086–1101, March 2015.

B. Alnajjab, J. Zhang, and R. S. Blum, “Attacks on sensor network estimation systems with quantization: Performance and optimum processing,” IEEE Transactions on Signal Processing, vol. 63, no. 24, pp. 6659-6672, Dec.15, 2015

Jiangfan Zhang, Xiaodong Wang, Rick S. Blum and Lance M. Kaplan, "Attack D etection in Sensor Network Target Localization Systems with Quantized Data", I EEE Transactions on Signal Processing, Vol. 66, No. 8, 2070 – 2085, April15, 20 18. – also general to spoofing.

System Model

Without Attack Model



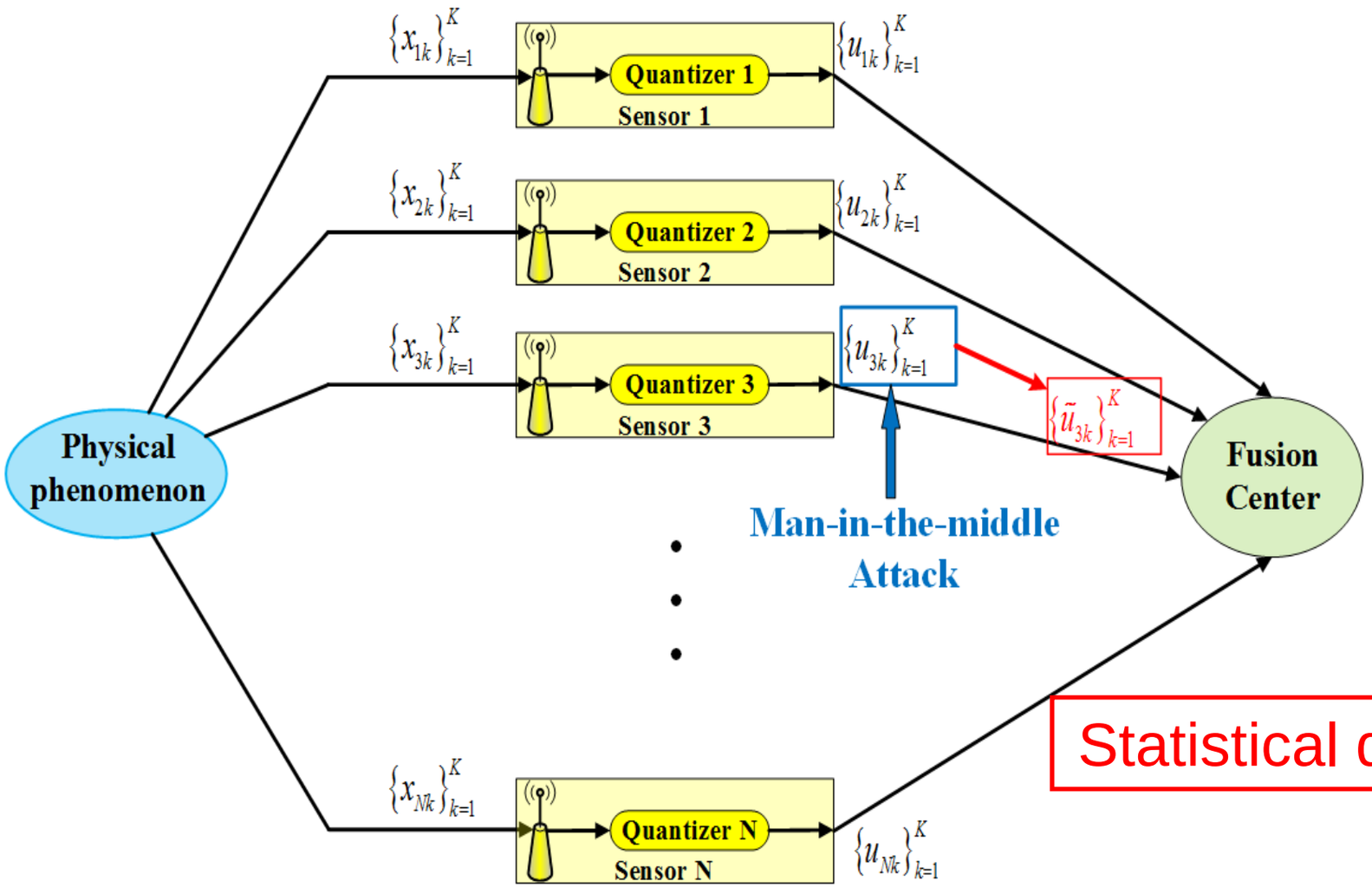
Estimate Θ

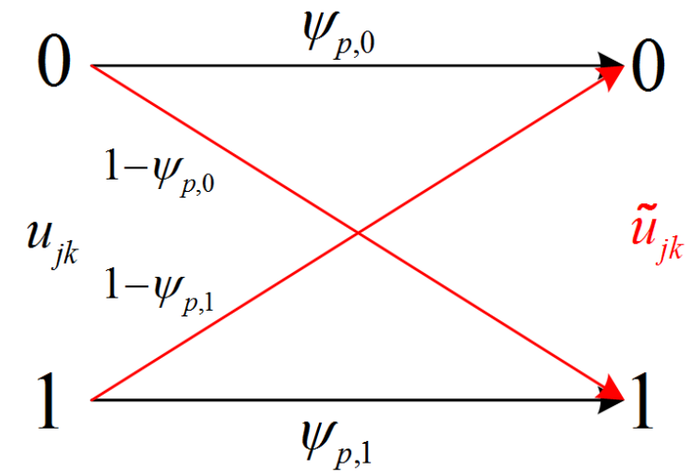
For simplicity of analysis, assume:

- $x_{jk} = \theta + n_{jk}$, $\forall j = 1,2,\ldots,N$, $\forall k = 1,2,\ldots,K$.
- θ : deterministic scalar parameter to be estimated;
- n_{jk}: additive zero-mean, known pdf $f(n_{jk})$, i.i.d.
- Binary quantizer: $u_{jk} = 1\{x_{jk} \in (\tau, \infty)\}$

B. Alnajjab, J. Zhang, and R. S. Blum, "Attacks on sensor network estimation systems with quantization: Performance and optimum processing," IEEE Transactions on Signal Processing, vol. 63, no. 24, pp. 6659-6672, Dec.15, 2015

Man-in-the-middle Attack Model





Statistical description of the p-th attack:

- $\mathcal{A}_p$: the set of sensors subjected to the p-th attack for all $p = 1,2,\ldots,P$.
- $\mathcal{A}_0$: the set of unattacked sensors.

LEHIGH UNIVERSITY

Identification and Categorization of Attacked Sensors

Theorem: Under some assumptions (set of unattacked > any attacked set),

1) For any N, as $K \to \infty$, the FC is able to determine P and identify $\{\mathcal{A}_p\}_{p=0}^{P}$ w.p.1.
2) If each sensor observes a finite number $K > \gamma$ of time samples then as $N \to \infty$, the FC is able to determine P. Moreover, for each p-th attack, the FC can identify an approximate group $\widetilde{\mathcal{A}}_p$ of $\mathcal{A}_p$ such that

The percentage of different sensors between $\mathcal{A}_p$ and $\widetilde{\mathcal{A}}_p$ can be made small as $K \uparrow$

Assumptions:

- $\mathcal{P}_0 > \mathcal{P}_p + \Delta_0, \forall p \geq 1; \mathcal{P}_p \geq \Delta, \forall p \geq 1.$

$$\gamma = -\frac{8 \ln 2}{\gamma^* \min\{\Delta\Delta_0, \Delta^2\}} + 1$$

J. Zhang, R. S. Blum, X. Lu, and D. Conus, "Asymptotically optimum distributed estimation in the presence of attacks," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1086–1101, March 2015.

LEHIGH UNIVERSITY

Can Categorize: Is Attacked Data Useful?

Based on CRB, achievable asymptotic lower bound on MSE for unbiased estimators, CRB from FIM

For most attacks → can estimate the attack parameters $\{(\psi_{p,0}, \psi_{p,1})\}_{p=1}^{P}$.

They make attacked data useful for better estimation of θ,

once we use a sufficient quantization approach (change τ).

Quantization limits dimension of θ → discuss later

J. Zhang, R. S. Blum, X. Lu, and D. Conus, "Asymptotically optimum distributed estimation in the presence of attacks," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1086–1101, March 2015.

LEHIGH UNIVERSITY

Can Categorize: Is Attacked Data Useful?

For some special Attacks: Attacked data can never be useful.

We provide a mathematical calculation that decides.

Attack can make data pmf independent on θ

Gives Gain

Relative CRB Gain:

Ignore attacked data

$$CRB_{\text{relative gain}}(\theta) \triangleq \frac{CRB_{\text{SEA}}(\theta)}{CRB_{\text{TQA}}(\theta)} = 1 + \frac{1}{[\mathbf{\Gamma}_0]_{1,1}} \sum_{p=1}^{P} \frac{\det\left(\mathbf{\Gamma}_p\left(\{1, 2p, 2p+1\}, \{1, 2p, 2p+1\}\right)\right)}{\det\left(\mathbf{\Gamma}_p\left(\{2p, 2p+1\}, \{2p, 2p+1\}\right)\right)}$$

Uses attacked data

Rank tells if data useful for reducing CRB

J. Zhang, R. S. Blum, X. Lu, and D. Conus, "Asymptotically optimum distributed estimation in the presence of attacks," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1086–1101, March 2015.

OPTIMUM ESTIMATION UNDER ATTACK

Taken together (Categorization, use attacked data) → This describes Optimum Processing under any man-in-the-middle attack

→ Use standard approach (ML) for possible joint estimation of desired and attack parameters.

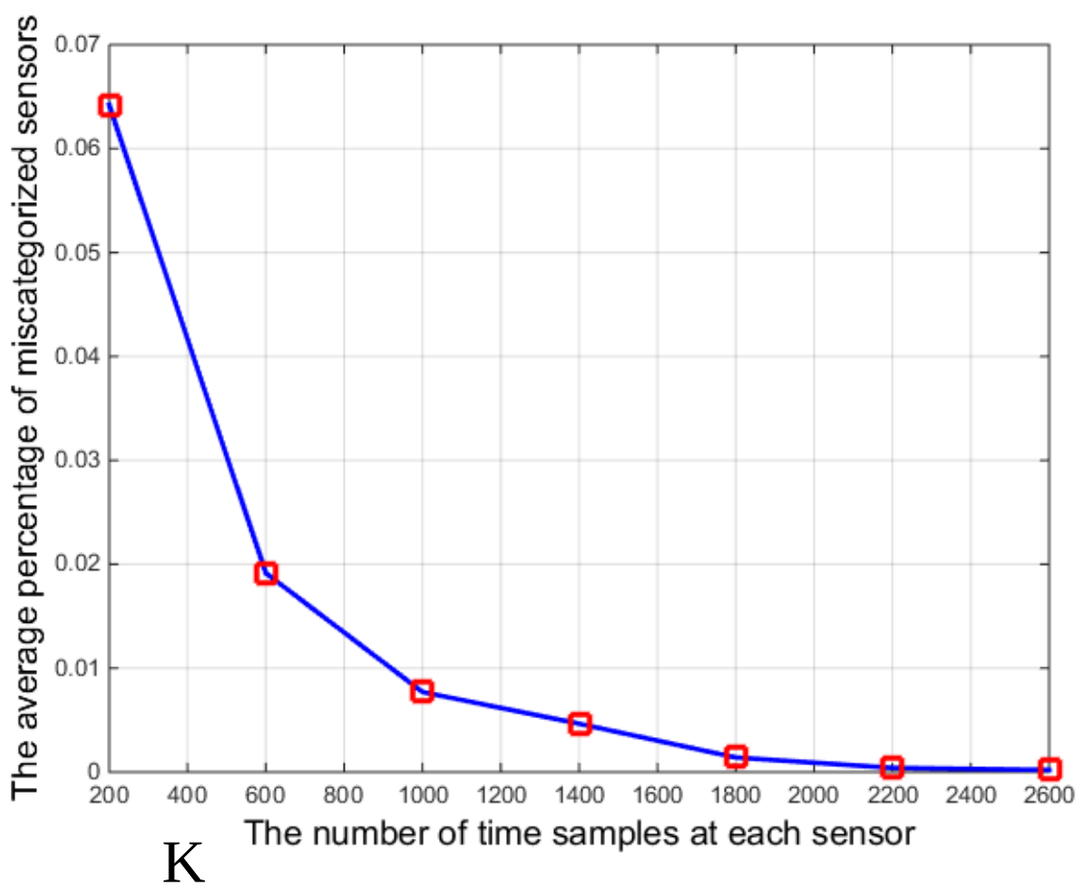
Later: EM example where we don't need much data

Numerical Results

Identification and Categorization of Attacked Sensors:

Setup:

- $N = 10,\ \theta = 1, \tau = 1.$
- Additive noise: standard normal distributed.
- 1st Attack: $\mathcal{P}_1 = 30\%$, $(\psi_{1,0}, \psi_{1,1}) = (0.2, 0.8)$.
- 2nd Attack: $\mathcal{P}_2 = 20\%$, $(\psi_{1,0}, \psi_{1,1}) = (0.7, 0.1)$.
- Monte Carlo approximation (200 times) of the ensemble average of the percentage of miscategorized sensors.



K ↑, misclassification ↓

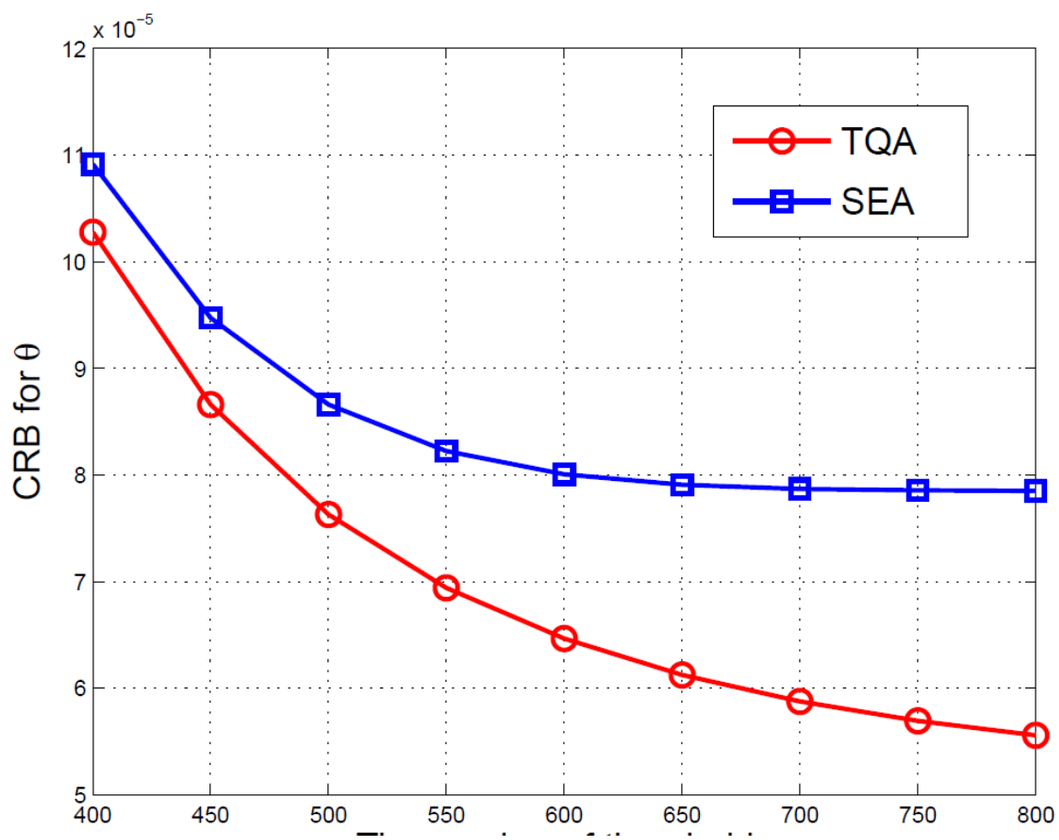
Verify the Theorem on the identification and categorization of attacked sensors.

Numerical Results

Asymptotic MSE ignoring (SEA) and using (TQA) attacked data):

Setup:

- $N = 100,\ \theta = 2$
- Additive noise: standard normal distributed.
- Length of each time slot: $K_t = 10$.
- The set of 801 thresholds: $Q = \{0, -0.125, 0.125, -0.250, 0.250, \ldots, -5, 5\}$.
- 1st Attack: $\mathcal{P}_1 = 25\%$, $(\psi_{1,0}, \psi_{1,1}) = (0.9, 0.95)$.
- 2nd Attack: $\mathcal{P}_2 = 20\%$, $(\psi_{1,0}, \psi_{1,1}) = (0.15, 0.2)$.



K, the number of time samples

❖Significant CRB improvement.

Verify the superiority of the TQA.

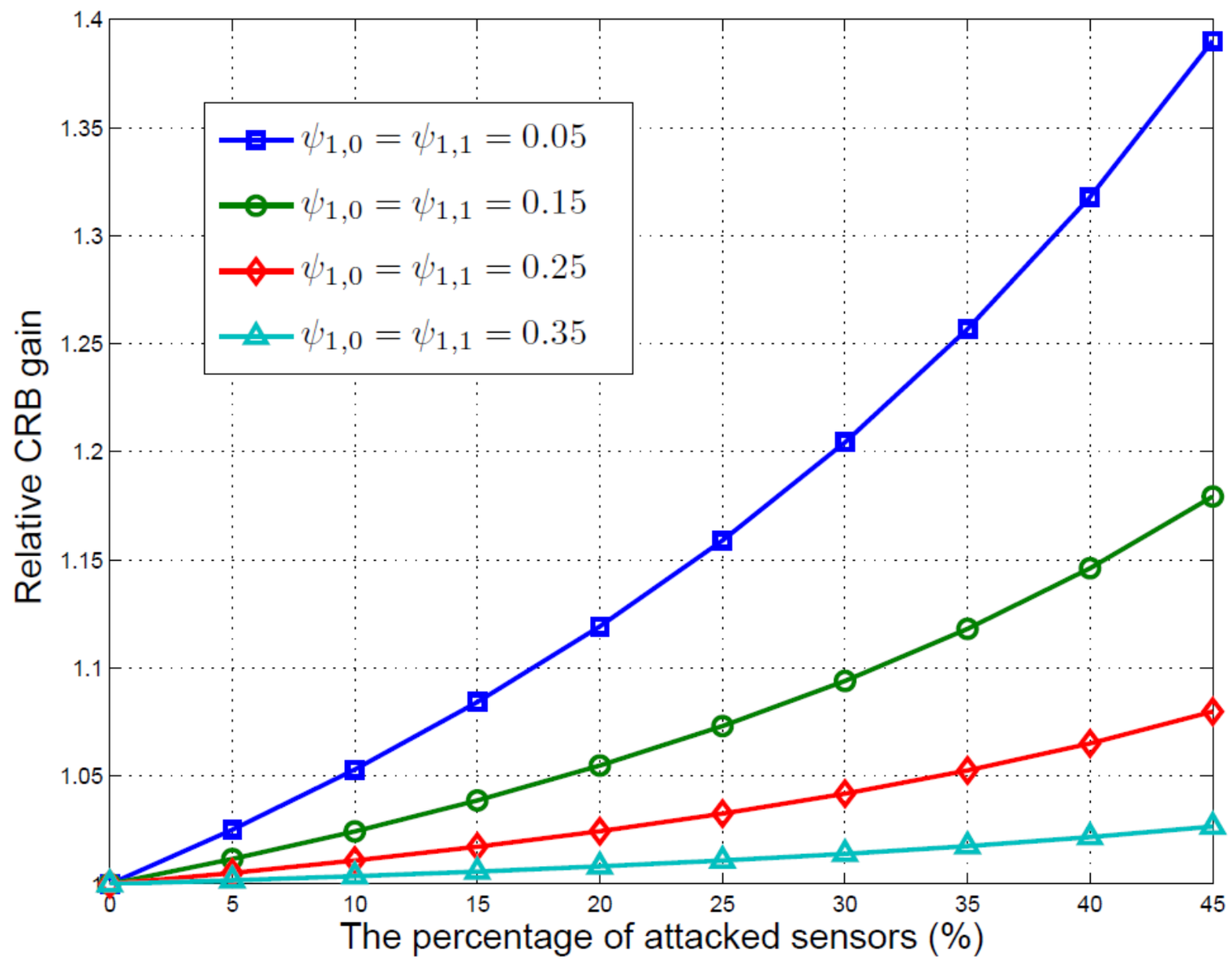
SEA: use only unattacked

Numerical Results

Relative Asymptotic MSE Gain vs the Percentage of Attacked Sensors :

- One attack
- Same as last
- All of Q

Verify some attacks make data useless.



Part II:
Optimal Spoofing Attacks

Describes the most effective attacks → make data useless

J. Zhang, R. S. Blum, L Kaplan, and X. Lu, "Functional Forms of Optimum Spoofing Attacks for Vector Parameter Estimation in Quantized Sensor Networks," IEEE Transactions on Signal Processing, Volume 65, Issue 3, Feb. 2017, pp. 705-720.

Guaranteed Degradation Spoofing Attack **(no math)**

Optimal Guaranteed Degradation Spoofing Attack (OGDSA): Maximizes the Asymptotic MSE for $\boldsymbol{\theta}$ under the assumption that $\{\mathcal{A}_{\mathrm{p}}\}_{\mathrm{p}=0}^{\mathrm{P}}$ is known to the FC.

There are TWO types of OPT ATTACKS (OGDSAs)

1. Can't estimate attack parameters (FIM not invertible) Inestimable Spoofing Attack (ISA)

→ can occur JUST BECAUSE YOU QUANTIZE

2. Attacked data from $\mathcal{A}_p$ useless for reducing Asymptotic MSE, but can estimate attack parameters (FIM is invertible).

Optimal Estimable Spoofing Attack (OESA)

→ have necessary and sufficient conditions for OESA

Any OGDSA implies attacked data is not helpful!

Inestimable Spoofing Attack (ISA) just from Quantization

Theorem:

For the p-th spoofing attack, if

Dim of $\boldsymbol{\tau}^{(\mathbf{p})}$

$$D_p > \sum_{j \in \mathcal{A}_p} K_j \left(R_j - 1\right)$$

quant symbols

Only determined by the numbers of quantization levels employed in a given $\mathcal{A}_p$

FIM of attack parameter vector is singular, and hence, the p-th attack is ISA.

Quantization Induced Limitations!

One functional form of ISA:

Employs $D_p > \sum_{j \in \mathcal{A}_p} K_j \left(R_j - 1\right)$ **and**

$$\tilde{x}_{jk} = \tau_1^{(p)} + \tau_2^{(p)} (x_{jk}) + \tau_3^{(p)} (x_{jk})^2 + \cdots + \tau_{D_p}^{(p)} (x_{jk})^{D_p - 1}$$

Attack parameters

$$\boldsymbol{\tau}^{(p)} = \left[\tau_1^{(p)}, \tau_2^{(p)}, \ldots, \tau_{D_p}^{(p)}\right]^T$$

Optimal Estimable Spoofing Attack

OESA: the *p*-th spoofing attack is OESA,

If FIM for estimating attack parameters is nonsingular, but attacked data not useful for estimating $\boldsymbol{\theta}$.

Theorem:

The necessary and sufficient conditions for OESA is roughly (see paper)

Range space of FIM for estimating θ from pth attacked data is a subset of the range space of FIM for estimating the pth attack parameters

Functional Form of OESA

Range space ideas → Gives general nec and suff conditions for how to manipulate the data for opt attacks

Corollary (A Class of Spoofing Attacks that Satisfies OESA):

Sufficient condition that the p-th spoofing attack is OESA for any values of $\boldsymbol{\theta}$, $\boldsymbol{\tau}^{(p)}$ and $\{I_j^{(r)}\}$ is

$$g_j\left(x \,\middle|\, \boldsymbol{\theta}, \boldsymbol{\tau}^{(p)}\right) = \tilde{g}_j\left(x \,\middle|\, \lambda_p \boldsymbol{\theta} + \boldsymbol{\tau}^{(p)}\right)$$

→ To get the above equation, the pdf must be a function of a linear combination of $\boldsymbol{\theta}$ and $\boldsymbol{\tau}^{(p)}$, nor $\boldsymbol{\theta}$ and $\boldsymbol{\tau}^{(p)}$ alone!

for some $\tilde{g}_j$.

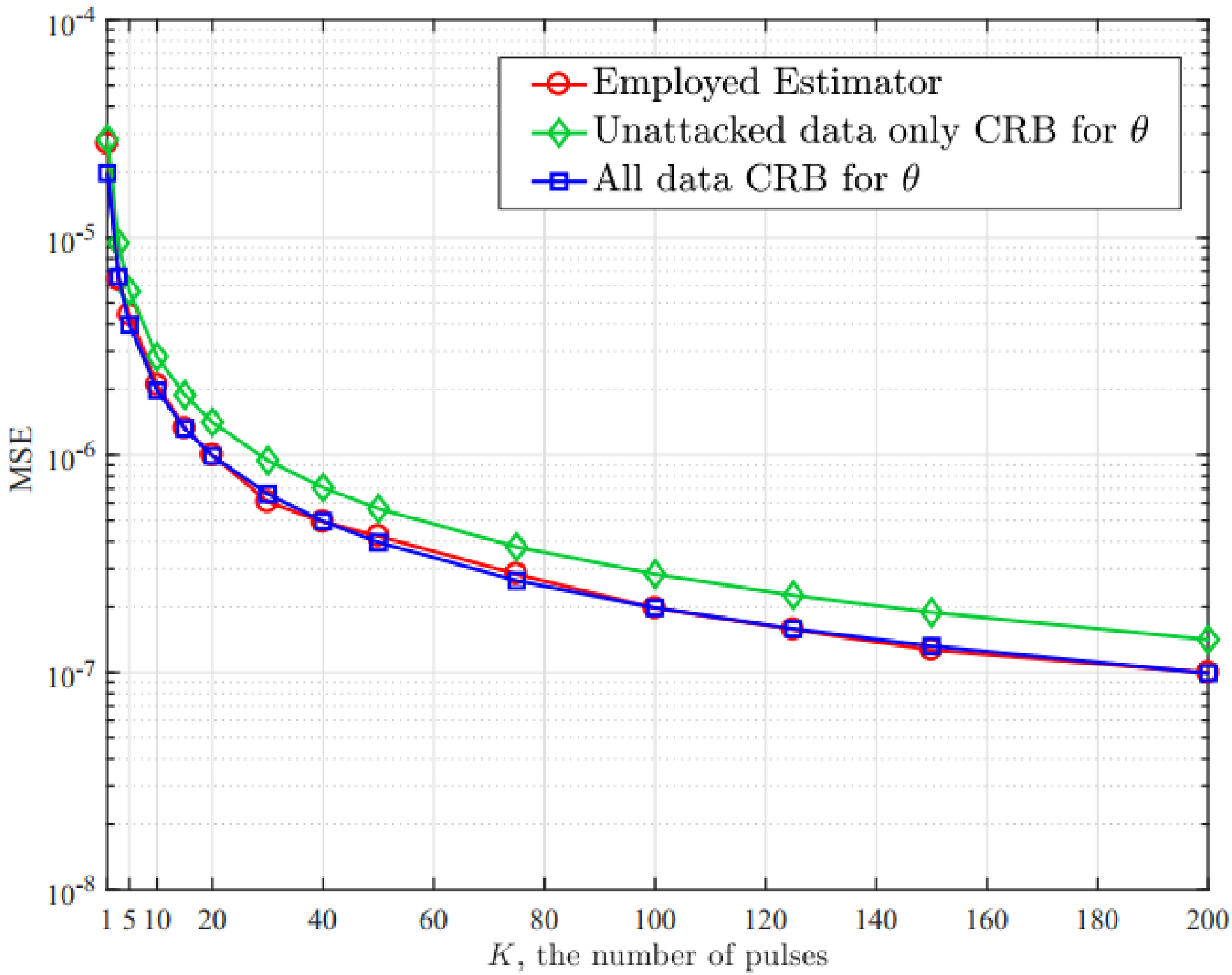
Example: Non-OGDSA

- MIMO radar with 1 Tx and N = 10 Rx, first three Rx under attack.
- Each Rx has identical 4 bit quantizer with thresholds {-∞, -5, -4, -3, ..., 8, 9, ∞}.
- After attack m-th measurement, k-th pulse at j-th Rx

$$\tilde{x}_{jm}^{(k)} = \sqrt{E_j} a_j s(t_{jm}^{(k)} - \theta_j) + \xi_j + n_{jm}^{(k)}, \quad m=1,2,\ldots, M, \; k=1,2,\ldots,K \qquad (1)$$

- θ_j is the desired parameter
- $\{n_{jm}^{(k)}\}$ is iid N(0,5). sequence with variance $\sigma^2 = 5$.
- $s(t) = (2/T^2)^{1/4} \exp(-\pi t^2/T^2)$
- sampling times are $t_{jm}^{(k)} = (m - 1)\Delta t$, $\forall m = 1, 2, ..., M$.
- assume distance between target and any Rx >> distance between Rxs so $\theta_j = \theta \; \forall$ j.
- T = 0.1, Δt = 0.001, θ = 0.02, and $E_j = 1$, $a_j = 1$ for all j.
- Attack parameters are $\xi_1 = 1$, $\xi_2 = -2$ and $\xi_3 = -1$.
- Employ an EM-based joint attack identification and parameter estimation approach

Non-OGDSA: Data Injection



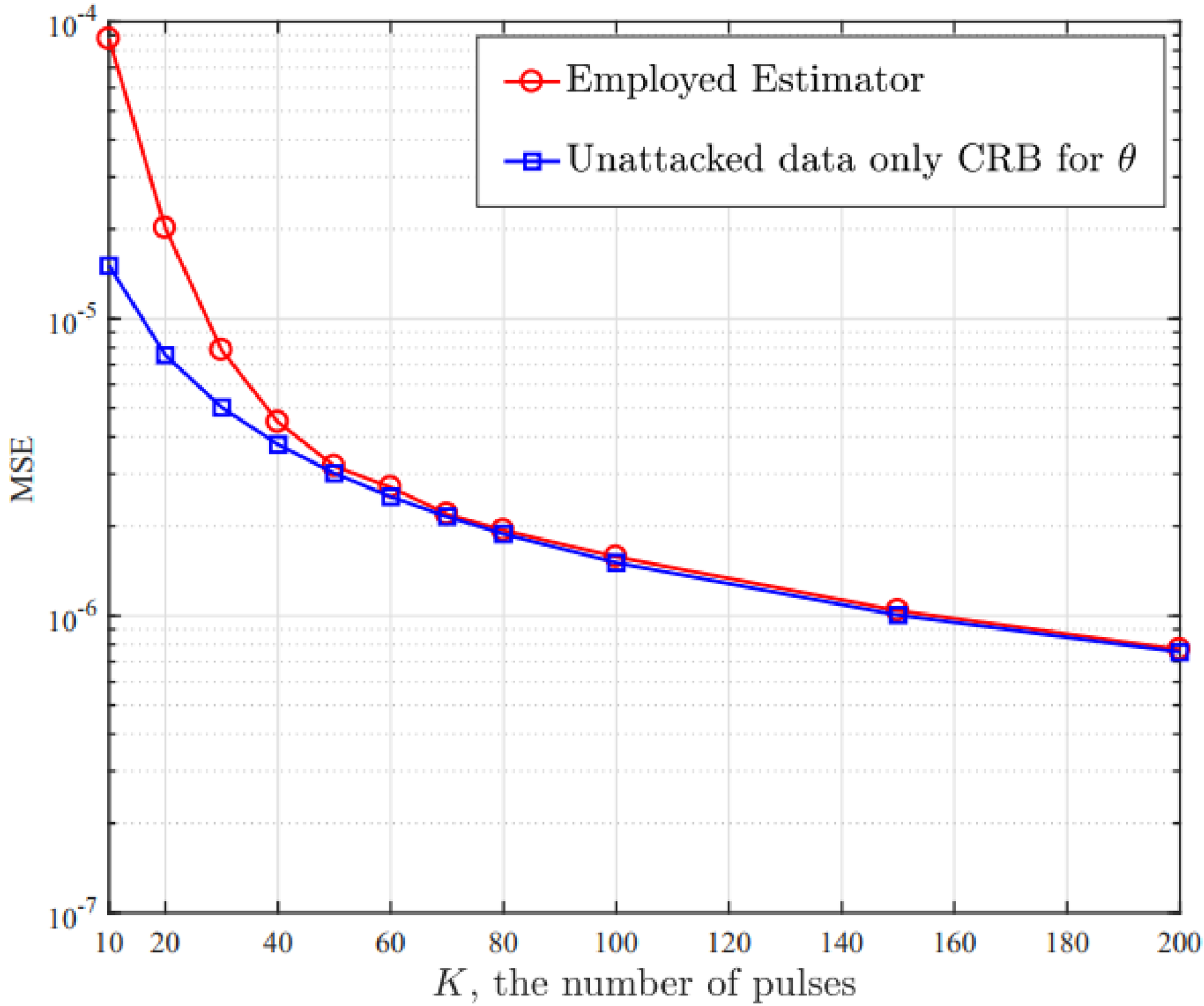
Example: OGDSA Attack

- Attack alters the delay in the received signal
- j-th Rx under attack for j = 1, 2, 3 (ξ_1 = 0.04, ξ_2= 0.05 and ξ_3 = 0.06) as per

$$\tilde{x}_{jm}^{(k)} = \sqrt{E_j} a_j s(t_{jm}^{(k)} - \theta_j - \xi_j) + n_{jm}^{(k)}, \quad (2)$$

- ξ_j is the delay introduced by the OGDSA attack.

ODGSA: Delay


Employed Estimator
Unattacked data only CRB for θ
MSE
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10
20
40
60
80
100
120
140
160
180
200
K, the number of pulses

Implications for Unattacked Systems

- Limitations of Estimation with Quantized Data (big data implications?)

Consider independent observations quantized using P distinct quantizer designs with R_j, $j = 1,2,\ldots,P$ symbols. Assume observations into jth quantizer design come from M_j different pdfs. The FIM is singular if

$$D_{\boldsymbol{\theta}} > \lambda\left(\{M_j\},\{R_j\}\right) \triangleq \sum_{j=1}^{P} M_j\left(R_j - 1\right)$$

Dim of $\boldsymbol{\theta}$

Estimation Capacity

Sufficient but not necessary

Have shown this also leads to nonidentifiablity & have nonindependent results

$$P = M_1 = R_1 - 1 = 1 \; then \;\; D_\theta = 1$$

J. Zhang, R. S. Blum, L. Kaplan, and X. Lu, "A fundamental limitation on maximum parameter dimension for accurate estimation using quantized data," IEEE Transactions on Information Theory, Vol. 64, Issue 9, pp. 6180-6195, Sept. 2018 (also on ArXiv).

Publication List

1. J. Zhang, R. S. Blum and H. V. Poor, “Approaches to Secure Inference in the Internet of Things”, IEEE Signal Processing Magazine, Vol 35, Issue 5, pp. 50-63, 2018.

2. 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.

3. B. Alnajjab, J. Zhang, and R. S. Blum, “Attacks on sensor network estimation systems with quantization: Performance and optimum processing,” IEEE Transactions on Signal Processing, vol. 63, no. 24, pp. 6659-6672, Dec.15, 2015

4. J. Zhang, R. S. Blum, L Kaplan, and X. Lu, “Functional Forms of Optimum Spoofing Attacks for Vector Parameter Estimation in Quantized Sensor Networks,” IEEE Transactions on Signal Processing, Volume 65, Issue 3, pp. 705-720, Feb. 2017.

5. 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.

6. 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.

7. J. Zhang, R. S. Blum, L. Kaplan, and X. Lu, “A fundamental limitation on maximum parameter dimension for accurate estimation using quantized data,” IEEE Transactions on Information Theory, Vol. 64, Issue 9, pp. 6180-6195, Sept. 2018 (also on ArXiv).

8. Jiangfan Zhang, Xiaodong Wang, Rick S. Blum and Lance M. Kaplan, "Attack Detection in Sensor Network Target Localization Systems with Quantized Data", IEEE Transactions on Signal Processing, Vol. 66, No. 8, 2070 – 2085, April15, 2018.

Publication List

9. A. K. Karthik and R. S. Blum, “Estimation theory-based robust phase offset determination in presence of possible path asymmetries”, in IEEE Transactions on Communications, vol. 66, no. 4, pp. 1624–1635, April 2018.
10. A. K. Karthik and R. S. Blum, “Optimum full information, unlimited complexity, invariant and minimax clock skew and offset estimators for IEEE 1588”, in IEEE Transactions on Communications (Early Access).
11. A. K. Karthik and R. S. Blum, “Robust phase offset estimation for IEEE 1588 PTP in electrical grid networks”, in 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, August 2018, pp. 1–5.
12. Z. Wang and R. Blum, “Topology attack detection in natural gas delivery networks”, in Information Sciences and Systems (CISS), 2019 53rd Annual Conference on. IEEE, 2019, pp. 1–6.
13. A. N. Samudrala, M. H. Amini, S. Kar, and R. S. Blum, "Optimal Sensor Placement for Topology Identification in Smart Power Grids", 2019 53rd Annual Conference on Information Sciences and Systems (CISS), March 2019.
14. A. N. Samudrala, M. H. Amini, S. Kar, and R. S. Blum, "Sensor Placement for Outage Identifiability in Power Distribution Networks", submitted to *IEEE Transactions on Smart Grid*, 2019.

Thank You!

rblum@Lehigh.edu

Related and Future Work

Applying these ideas to general IoT systems in a few projects (IEEE 1588), but specific interest in smart electrical Grid and other power networks (gas) as part of our DoE cybersecurity center.

Working on other approaches: physical layer security, low complexity encryption and authentication, with some emphasis on sensor systems performing estimation, hypothesis testing. Focus on inference problems.