REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
14-02-2018	Final Report	1-Jul-2014 - 28-Aug-2017

4. TITLE AND SUBTITLE
Final Report: Impacts and Mitigation of Attacks on Sensor Networks

5a. CONTRACT NUMBER
W911NF-14-1-0245

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Lehigh University
Research & Sponsored Programs
526 Brodhead Avenue
Bethlehem, PA 18015 -3008

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
64875-NS.15

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Rick Blum
UU	UU	UU	UU		19b. TELEPHONE NUMBER 610-758-3459

RPPR Final Report
as of 23-Mar-2018

Agency Code:

Proposal Number: 64875NS **Agreement Number: W911NF-14-1-0245**
INVESTIGATOR(S):

Name: Rick Blum
Email: rblum@ece.lehigh.edu
Phone Number: 6107583459
Principal: Y

Organization: **Lehigh University**
Address: Research & Sponsored Programs, Bethlehem, PA 180153008
Country: USA

DUNS Number: 808264444 EIN: 240795445
Report Date: 28-Nov-2017 Date Received: 14-Feb-2018
Final Report for Period Beginning 01-Jul-2014 and Ending 28-Aug-2017
Title: Impacts and Mitigation of Attacks on Sensor Networks
Begin Performance Period: 01-Jul-2014 **End Performance Period:** 28-Aug-2017
Report Term: 0-Other

Submitted By: Rick Blum Email: rblum@ece.lehigh.edu
Phone: (610) 758-3459

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 4 **STEM Participants:** 0

Major Goals: The objective of this effort is to make significant progress towards developing the fundamental theory of cyberattacks on sensor networks employing digital communications, while advancing the state of the art design and analysis approaches for estimation algorithms under attack. The goal was to find advanced signal processing techniques to make the impacts small. If we can develop such technology this would be important for the Army and for all US defense agencies. In the complicated world we live in, we feel this would be an important contribution to guard the safety of our country and we would be very proud of such an accomplishment. This effort is focused on theory, but we must put the theory in place before practical development can take place. In the process we will train the next generation of undergraduate and graduate students to take the next needed steps to implement the theory we are developing. Since there has been so little investigation in the area of attacks on sensor networks deployed for estimation, the possible kinds of attacks, their impacts, the role of the information the attacker has and the impacts of evasive measures taken by the estimation system appear unknown. Thus, our initial work attempted to investigate these issues and to provide some understanding that would guide our future investigations. With a better understanding of these issues, we were able to define much narrower problems where we could pursue optimum processing and its performance, along with bounding the impact of attacks while understanding what kinds of attacks were of the greatest concern. Here we focused on attacks that appear important for some specific scenarios that appear practical but which involve models with reasonable complexity such that analysis is tractable. To obtain the results described here, we developed some interesting ways to use large deviation theory and estimation theory, along with some novel bounding approaches and, in a few cases, comparisons to unachievable bounds.

Accomplishments: Man-in-the-Middle Attacks - In our first investigations of distributed sensor network estimation problems in the presence of man-in-the-middle attacks, our team considered the most investigated sensor network observation model. Under a man-in-the-middle attack, the quantized outputs of some vulnerable subsets of sensors are hijacked by adversaries. We grant the adversaries, assumed to employ a finite number P of distinct attacks in total at any given time, the largest power to manipulate the quantized data at their compromised sensors under the constraint that they do not have information about what computations the
fusion system is using. We assume that each adversary can modify the quantized data to bring about an arbitrary probability mass function (pmf) at the output of each sensor the adversary controls. Under these assumptions, our team studied, for the first time, the ability of the fusion center (FC) to identify the attacked sensors and categorize them into different groups corresponding to distinctly different types of attacks. We assume that the set of unattacked sensors is a larger percentage of all sensors than any set of identically attacked sensors to avoid ambiguity between a set of attacked and a set of unattacked sensors. It
is shown that increasing the number K of time samples at each sensor and enlarging the size N of the sensor

network can both ameliorate the identification and categorization, but to different extents. As K goes to infinity, the attacked sensors can be perfectly identified and categorized, while with finite but sufficiently large K, as N goes to infinity, it can be shown that the fusion center can also ascertain the number of attacks and obtain an approximate categorization with a sufficiently small percentage of sensors that are misclassified. Next, in order to improve the estimation performance by utilizing the attacked observations, we considered joint estimation of the statistical description of the attacks and the parameter to be estimated after the sensors have been well categorized. We provide necessary and sufficient conditions under which utilizing the compromised sensors in the proposed fashion will lead to better estimation performance when compared to approaches where the compromised sensors are ignored. We also provide closed form expressions for the best performance that can be achieved in each case.

Bad Data Detectors, Spoofing Attacks and General Attacks/Models - In another study, our team considered a different but practical scenario where the sensors employ bad data detectors which check if the observed sensor data fits the unattacked observation model assumed by the estimation algorithm. Only sensor data which passes the checks made by the bad data detectors will be employed in the subsequent estimation procedure. Here spoofing attacks, which modify the physical phenomenon observed by the sensors, become
of considerable interest since, unlike in man-in-the-middle attacks, the attacker can launch spoofing attacks which are guaranteed to pass the bad data detectors even if the attacker has no knowledge about the quantization approach employed by the sensor system or the true value of the parameter to be estimated. In such cases, asymptotically optimum processing is investigated. It is then shown that it is possible to identify the attacked sensors, under stated assumptions, with perfect accuracy as the number of observations K from each sensor tends to infinity. If the number of sensors tends to infinity for finite K, it is shown that the attacked sensors can be identified with a given accuracy that can be set by K, allowing considerable design flexibility. While optimum processing is of considerable interest, the impact of attacks on both optimum and suboptimum processing is also of great interest. In another study, we provide a general approach to characterize the after-attack estimation performance of any estimation approach, optimum or suboptimum, under any general type of attack, without any assumptions on the estimation problem, the observation models, the number of sensors, the number of observations or the independence of any observations to any others. A classification of these general attacks, which are much more general than those assumed in any previous work, that categorizes them into classes, according to the information available to the attacking entity, is introduced and some
notable properties of these attack classes are studied and highlighted using examples. Such investigations are of significant practical importance as some legacy or even modern systems have not been designed to detect and react to attacks.

General Spoofing Attack with Guaranteed Attack Degradation - Our more recent work focuses on the performance of spoofing attacks on systems solving vector estimation problems where the attacks employ general functions to manipulate the data which involve unknown attack parameters which must be estimated. To fit with the existing work in the community, the forms of the functions used to manipulate the data are assumed known down to the unknown parameters. For the first time, necessary and sufficient conditions are provided under which the attacks provide a guaranteed attack performance in terms of an accepted metric, Cramer-Rao Bound (CRB), regardless of the processing the estimation system employs. Interestingly, these conditions imply that, for any such highly desirable attacks, when the attacked sensors can be perfectly identified by the estimation system, it is essentially impossible to employ the attacked data in order to improve performance as measured by the adopted metric. These highly desirable attacks make the attacked data useless. It is shown that it is always possible to construct one of these highly desirable attacks by properly employing a sufficiently large dimension attack vector parameter relative to the number of quantization levels employed. This appears to be a very basic and important result. For a class of spoofing attacks and a sufficient number of observations in
numerical tests, a computationally efficient heuristic for the joint identification of the attacked sensors and estimation of the desired vector parameter achieves the same performance as an unrealizable approach which employs optimum processing after being told which sensors are attacked.

Fundamental Limits on Parameter Estimation with Quantized Data - Our studies on systems under attack uncovered some new, very basic, and important theory that applies even to systems which are not under attack. For an estimation system based on quantized data, a critical quantity called the estimation capacity describes a quantization induced fundamental limit on the estimation capabilities of the system. To be specific, if the dimension of the desired vector parameter is larger than the estimation capacity of the quantized estimation system, then it will be impossible to accurately estimate the desired parameter with an unbiased estimator (commonly employed). Interestingly, the estimation capacity doesn't depend on the exact distributions of the observations or the exact quantization regions. Instead, it depends on the number of different types of quantizers employed at different sensors and times, the number of quantization levels (or regions) employed by these different quantizers, and on

the number of different statistical models which are viewed by different sensors. Thus, our analysis reveals that for any given observation model there is a link between complexity of the quantization approach employed and the largest dimension of the vector parameter which can be accurately estimated by the unbiased estimator. While the just described estimation capacity result tells us that the quantization approach we employ can limit the dimension of a vector parameters that can be accurately estimated, it does not explain why this happens. We also provide a very rigorous analysis for this.

Training Opportunities: PhD students and postdocs have been trained in how to do research by our accomplished team. This includes how to write papers and proposals; how to present results; how to choose topics; and how to do important work. The students and postdocs had chances to present their work at conferences and in meetings with our ARL collaborators. One of the students was able to work at ARL over two summers. One PhD student is now on a postdoc at Columbia University and is interviewing for faculty positions. He has had several interviews at good U.S. universities and will likely become a faculty member.

Results Dissemination: Our research results were published in journal papers in the best journals and we have presented our results at the best conferences. The PI has given talks on the research at the best schools. All papers are first put on the archive ArXiv before publication and then the reference for the accepted paper is put on our lab website. The work has been presented at several IEEE distinguished lectures since the PI is an IEEE Signal Processing Society distinguished lecturer. The work has also been presented at plenary talks at a few conferences.

Honors and Awards: The PI was named an IEEE Signal Processing Society Distinguished Lecturer.
He was invited to talk at an future IEEE Signal Processing Society Summer School and to give a future ICASSP tutorial.

Protocol Activity Status:

Technology Transfer: The PI and his graduate student meet each week (during the grant and after) with ARL researchers Brian M Sadler and Paul Yu (both experts on security). They are helping the PI supervise his student Jake.Perazzone on security research related to the grant. Jake spent two summers at ARL, the second one was using funds from this grant. Brian and Paul have really helped make the research practical and have guided us in excellent directions. We feel very lucky to work with them. Jake's tuition and stipend have been supported by a Dept. of Education grant.

There was many discussions with ARDEC about technology transfer but nothing has come of this.

PARTICIPANTS:

Participant Type: PD/PI
Participant: Rick S Blum
Person Months Worked: 5.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Jiangfan Zhang
Person Months Worked: 3.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

RPPR Final Report
as of 23-Mar-2018

Participant Type: Postdoctoral (scholar, fellow or other postdoctoral position)
Participant: Jiangfan Zhang
Person Months Worked: 8.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Basel Alnajjab
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Anand Guraswamy
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: David Saska
Person Months Worked: 2.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Jake Perazzone
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

CONFERENCE PAPERS:

RPPR Final Report
as of 23-Mar-2018

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE China Summit and International Conference on Signal and Information Processing
Date Received: 16-Jul-2016 Conference Date: 13-Jul-2015 Date Published:
Conference Location: Chengdu, China
Paper Title: DISTRIBUTED JOINT SPOOFING ATTACK IDENTIFICATION AND ESTIMATION INSENSOR NETWORKS
Authors: Jiangfan Zhang and Rick S. Blum
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP)
Date Received: 16-Jul-2016 Conference Date: 12-Jul-2015 Date Published:
Conference Location: Chengdu, China
Paper Title: Wireless information and power transfer design with scheduling for cooperative networks
Authors: Zheng Zhou, Mugen Peng, Zhongyuan Zhao, and Rick S. Blum
Acknowledged Federal Support: **Y**

Optimum Functional Forms of Spoofing Attacks, Optimum Processing for Man-in-the-Middle Attacks and Interesting Implications to Unattacked Quantized Sensor Estimation and IoT Systems

Rick S. Blum and Collaborators
IEEE SPS Distinguished Lecturer
Department of Electrical and Computer Engineering
Lehigh University

Thanks to IEEE SPS and ARO

This work was supported by the U. S. Army Research Laboratory and the U.S. Army Research Office and was accomplished under Agreement Number W911NF-14-1-0245.

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:

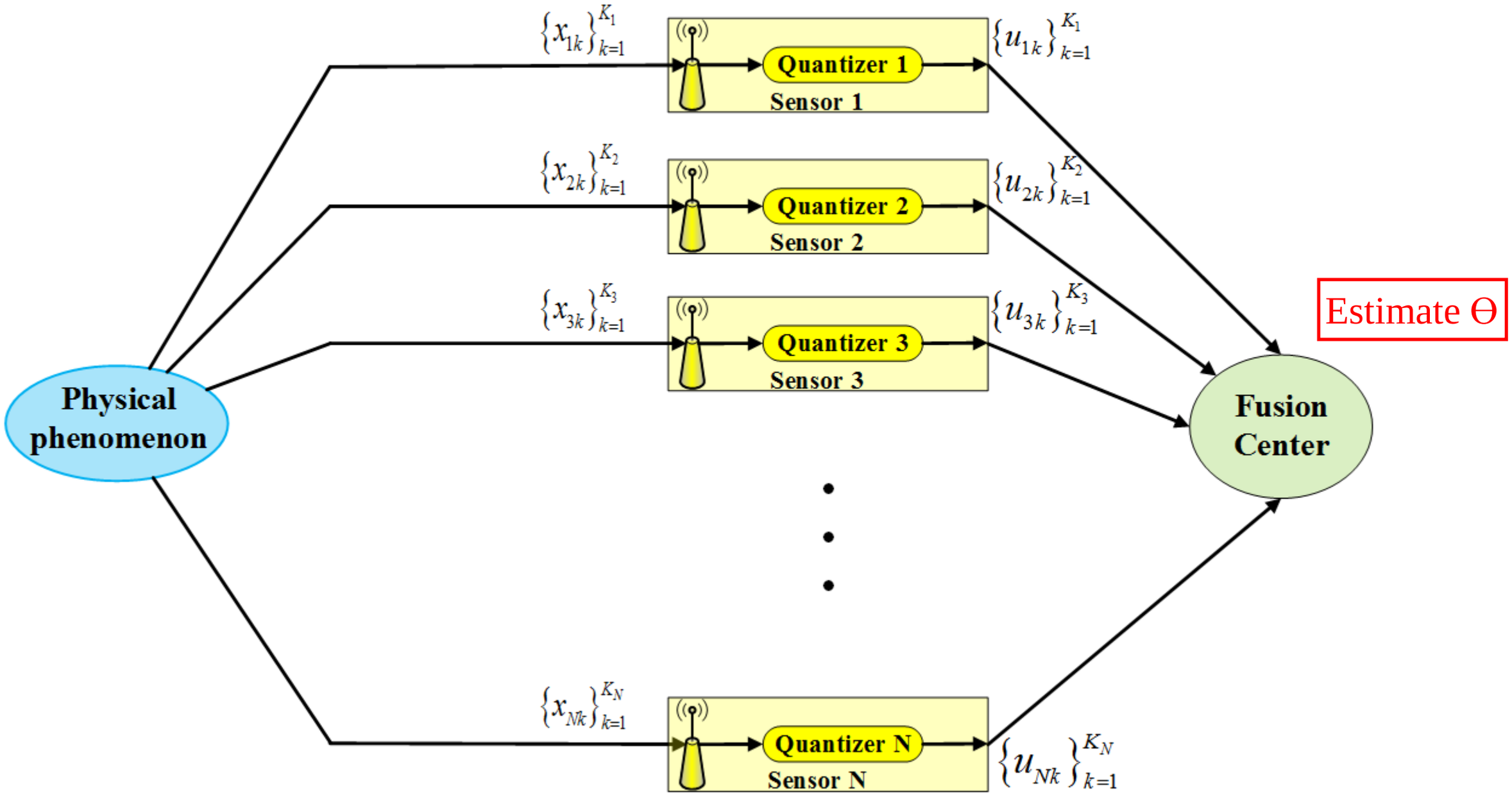
- Desired real time control/reaction & low complexity sensor nodes makes standard security too slow and complex

Solutions:

- 1. Require Consistency from multiple sensors (focus here)
- 2. Employ lower complexity encryption and authentication
- 3. Employ Physical Layer Security

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

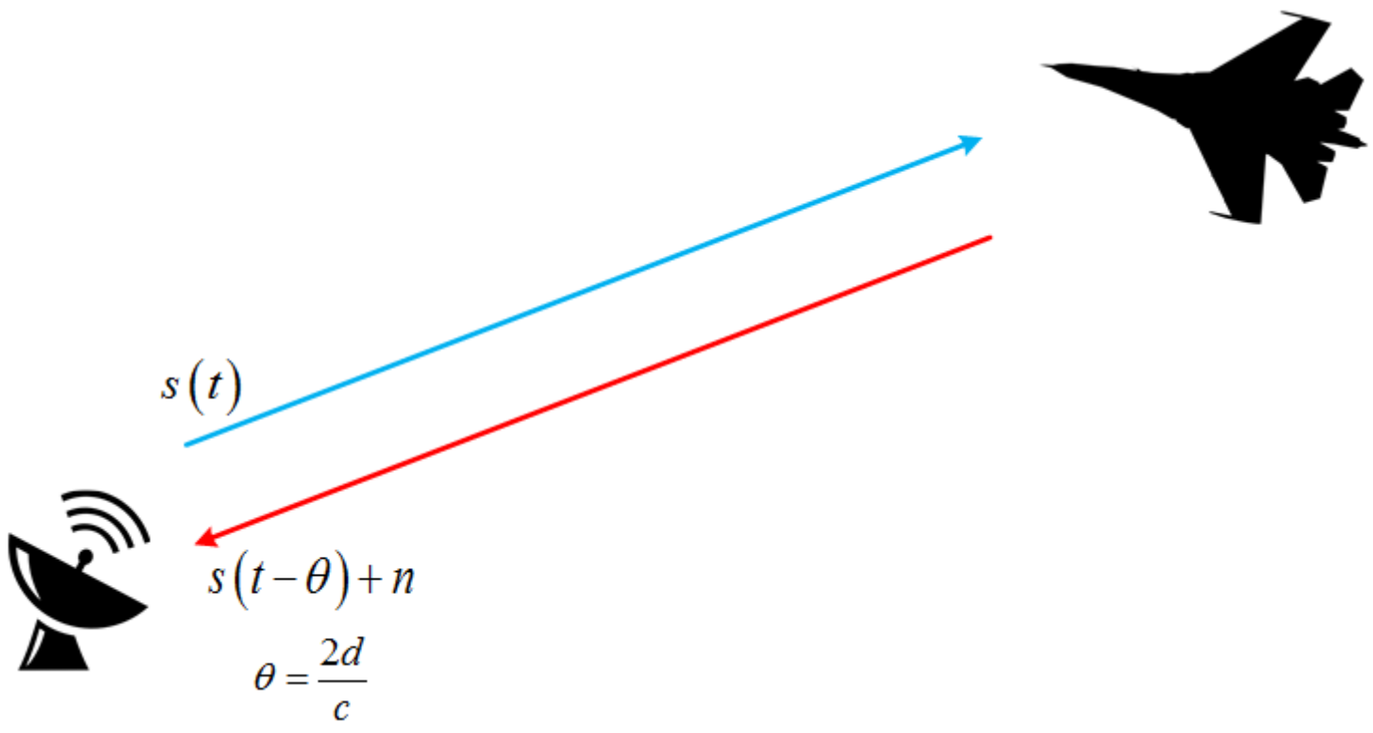
- The noise at each sensor is independent (unrelated) to others

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

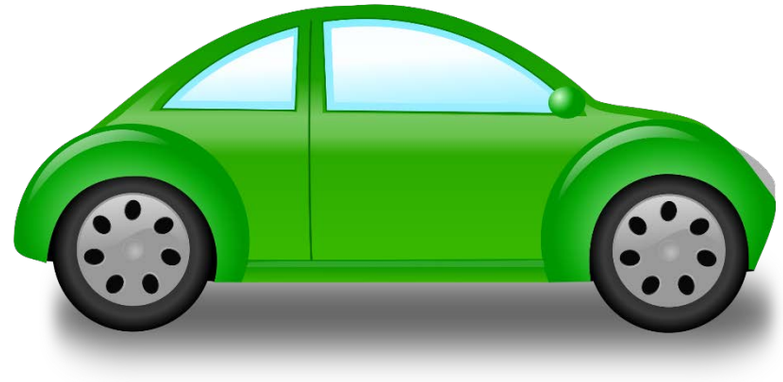
More Complicated Estimation Problem

Estimation Example in Radar System (Localization):

In the ABSENCE any attacks:

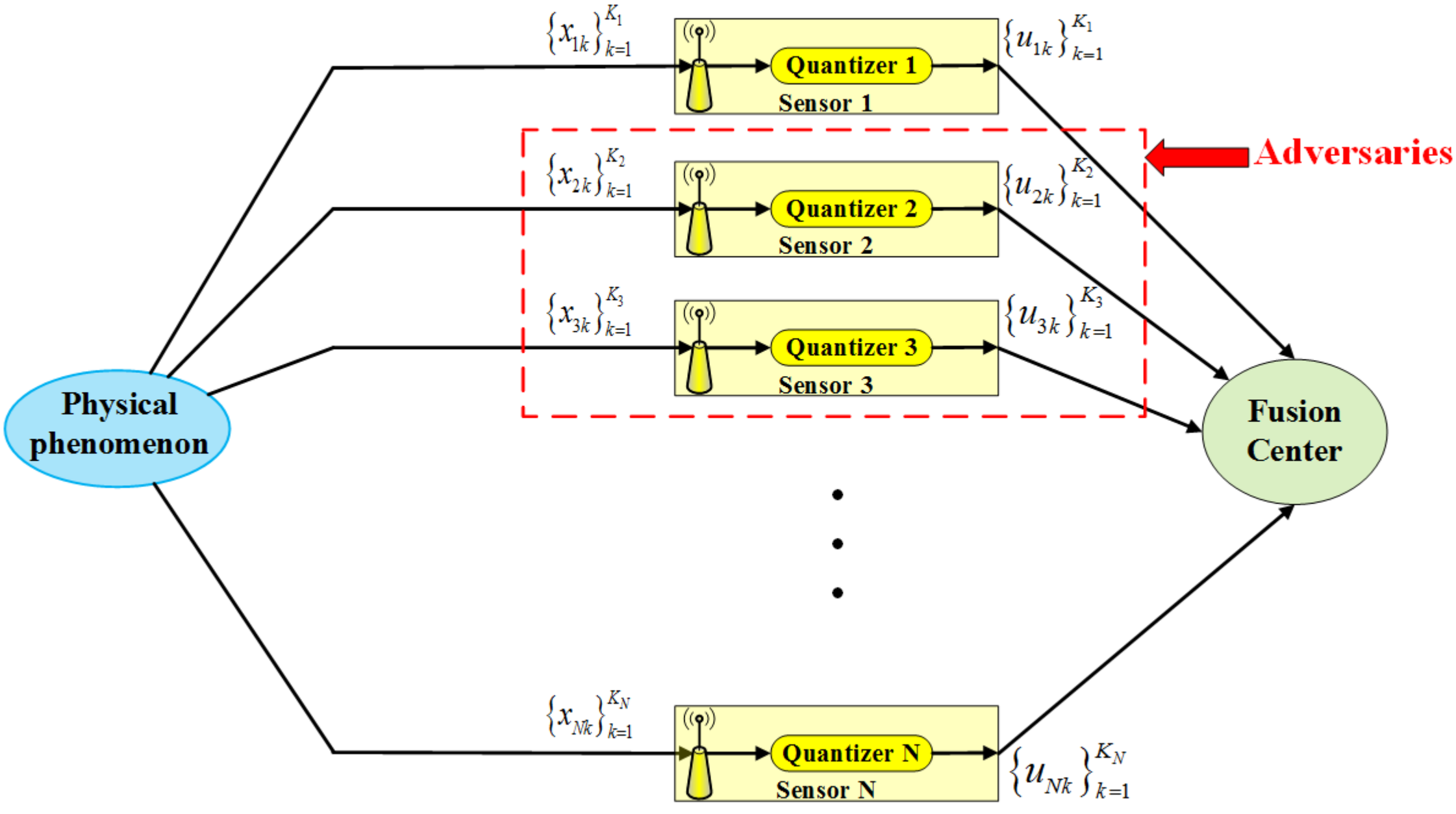


Self driving cars



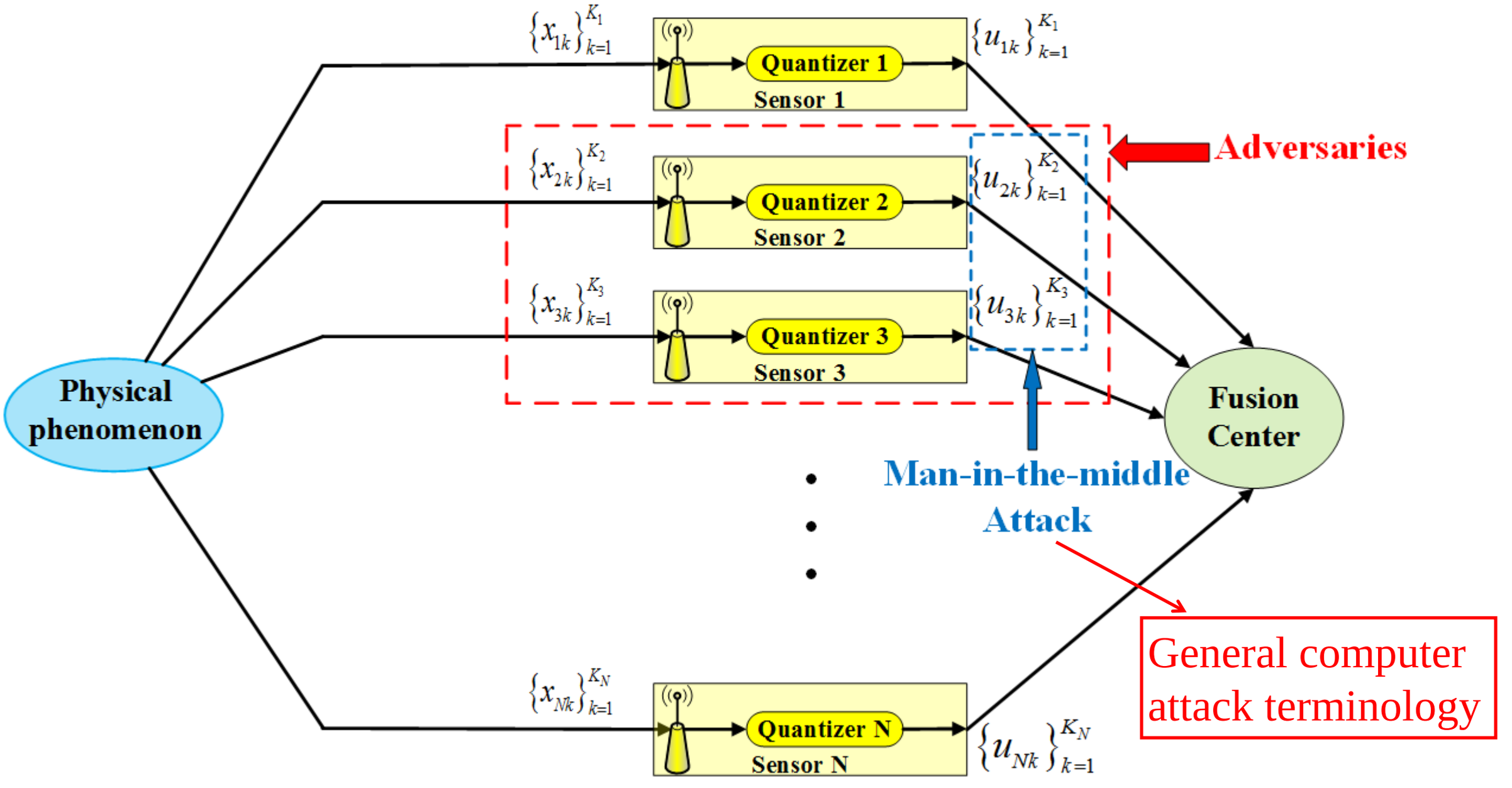
Attacks on Distributed Sensor Network Estimation System

Phenomenon → Sensors → Fusion Center:



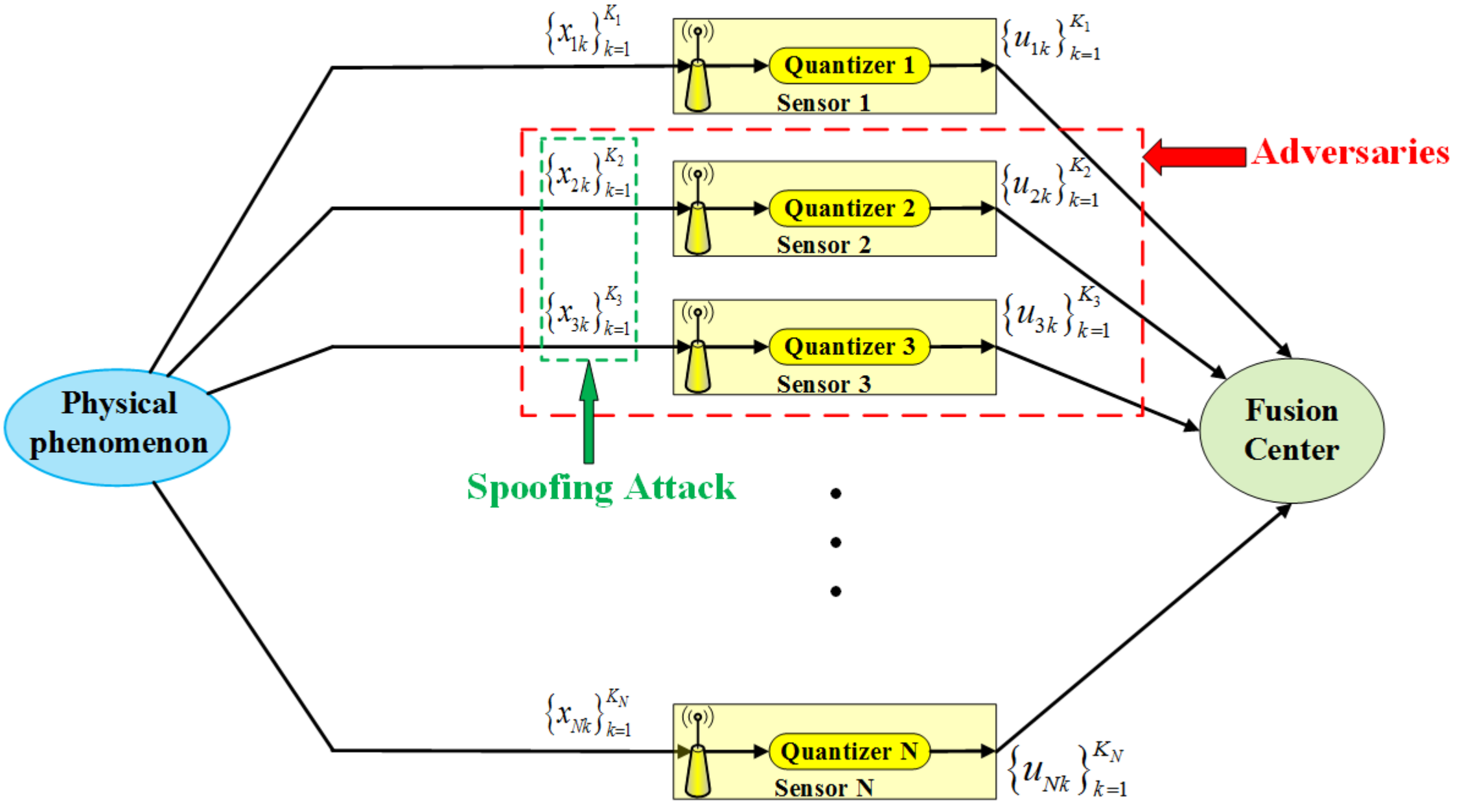
Attacks on Distributed Sensor Network Estimation System

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



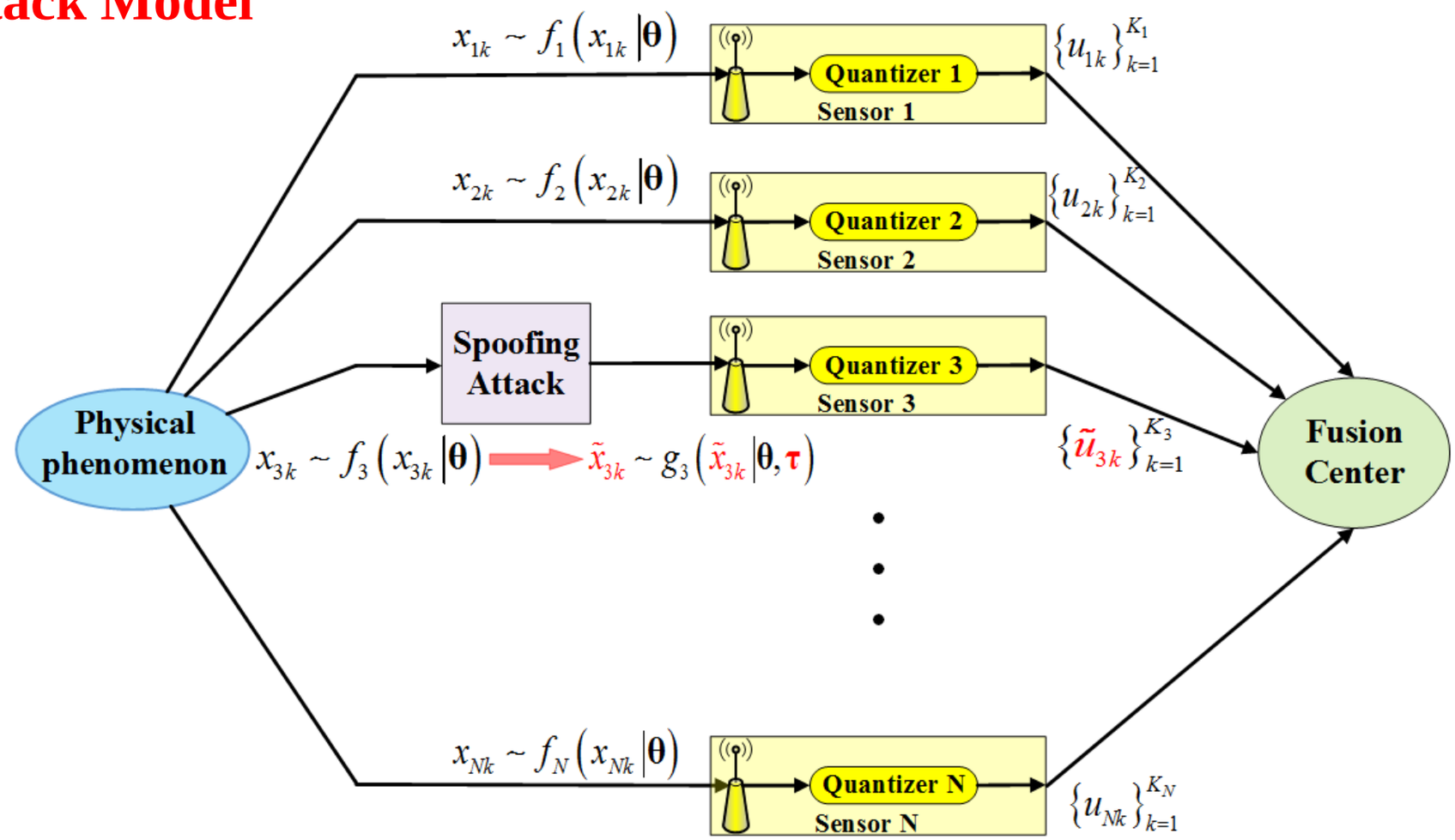
Attacks on Distributed Sensor Network Estimation System

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

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

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

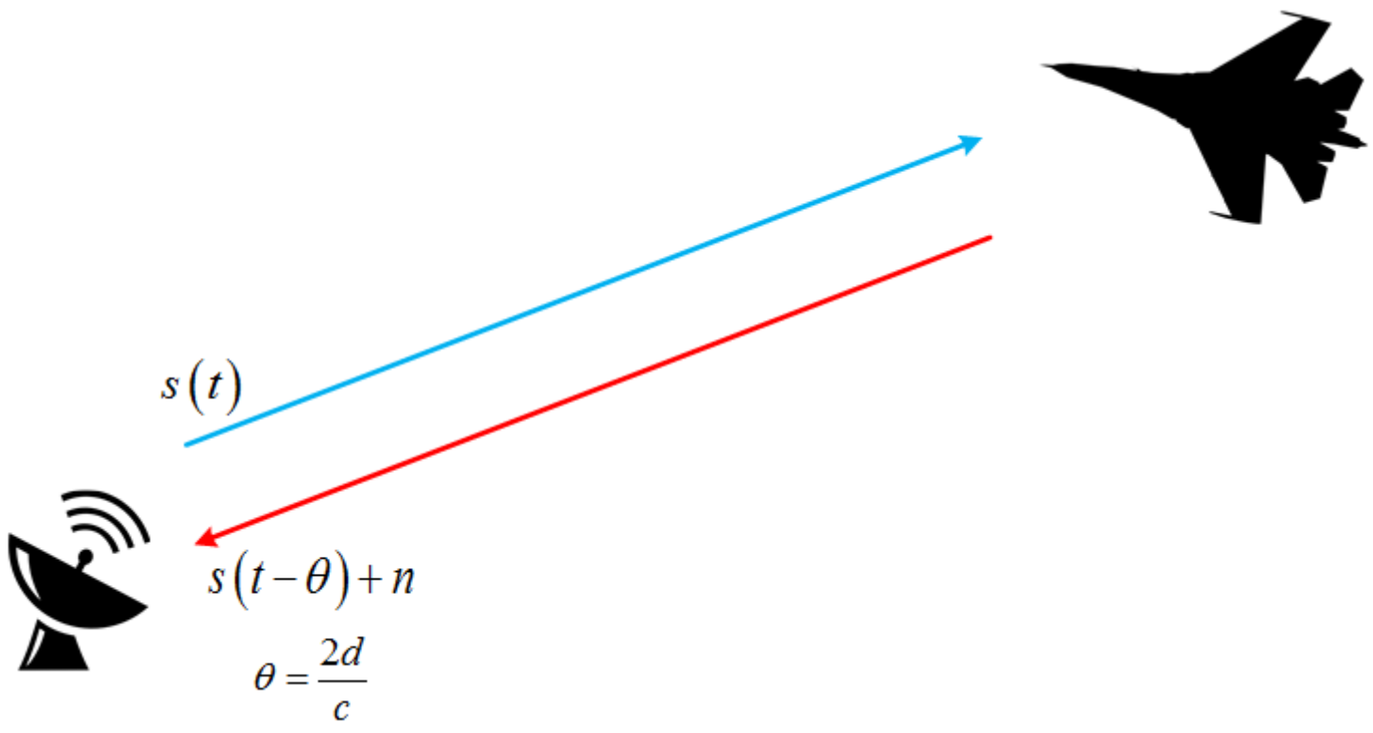
Spoofing attack changes the pdf of obs, and new pdf can depend on $\boldsymbol{\tau}$

Attack Vector Parameter

Motivation of Spoofing Attack Model

Simple Example in Radar System:

In the ABSENCE of spoofing attacks:



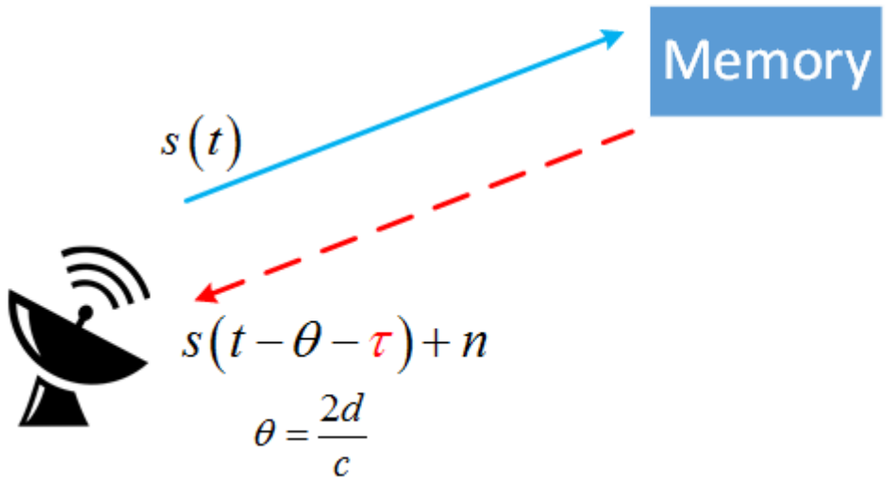
Spoofing Attacks in Radar Systems [6, 7]: Radars will appear in all cars (esp self-driving) to fuse with video to avoid hitting people.

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

Motivation of Spoofing Attack Model

Simple Example in Radar System:

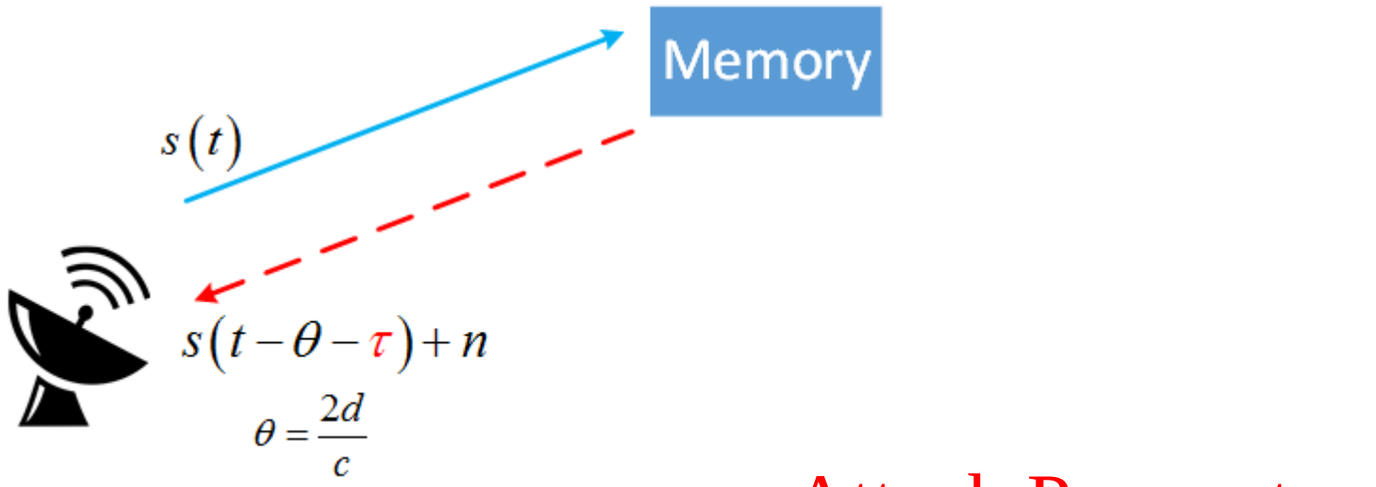
In the PRESENCE of spoofing attacks:



Motivation of Spoofing Attack Model

Simple Example in Radar System:

In the PRESENCE of spoofing attacks:



The essential effect of the spoofing attack:

Attack Parameter

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

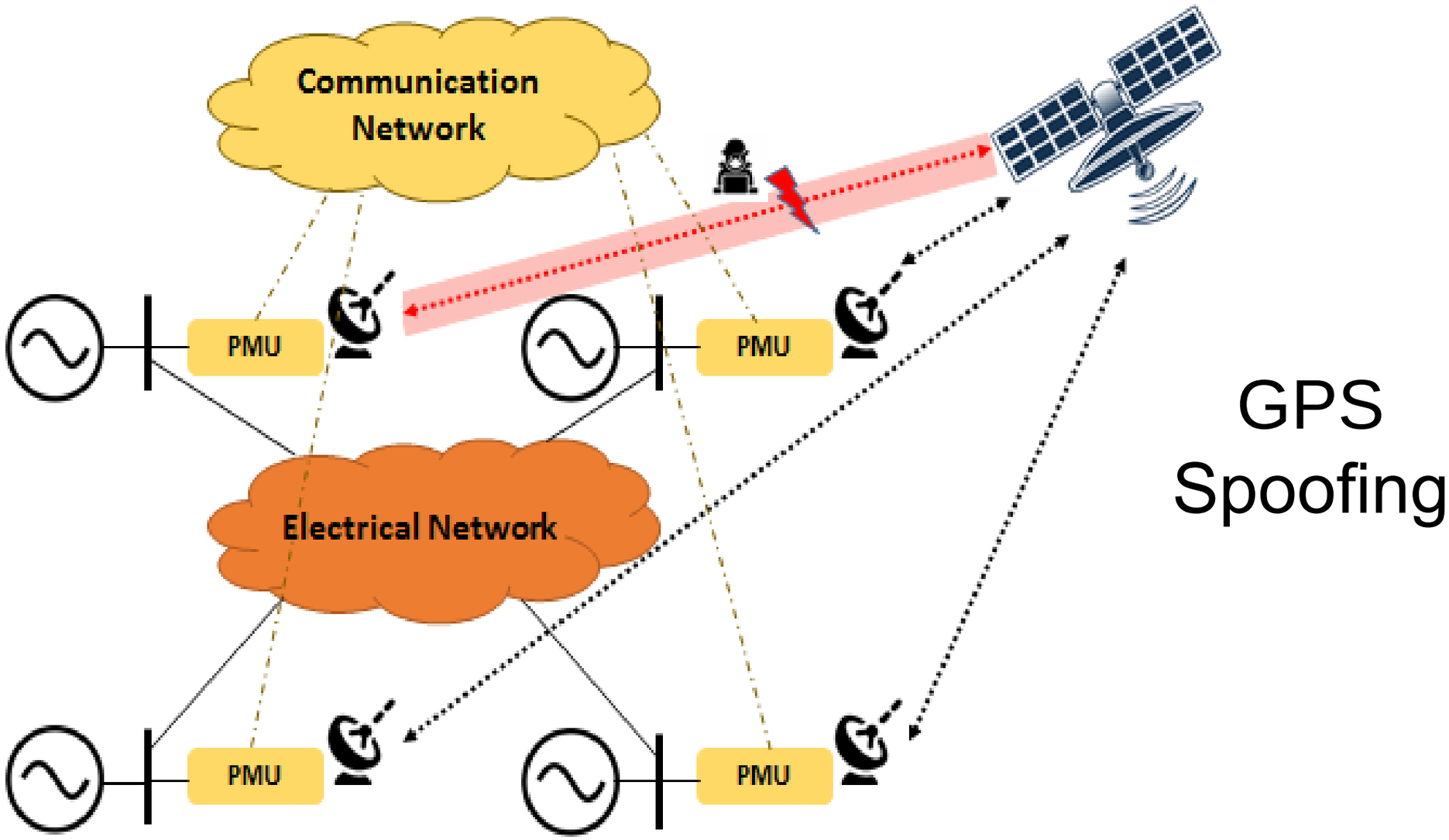
In one special case where one modified delay term returns

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

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.



Part I: Optimum Processing in the Presence of Man-in-the-Middle Attacks (and Spoofing) - Asymptotic

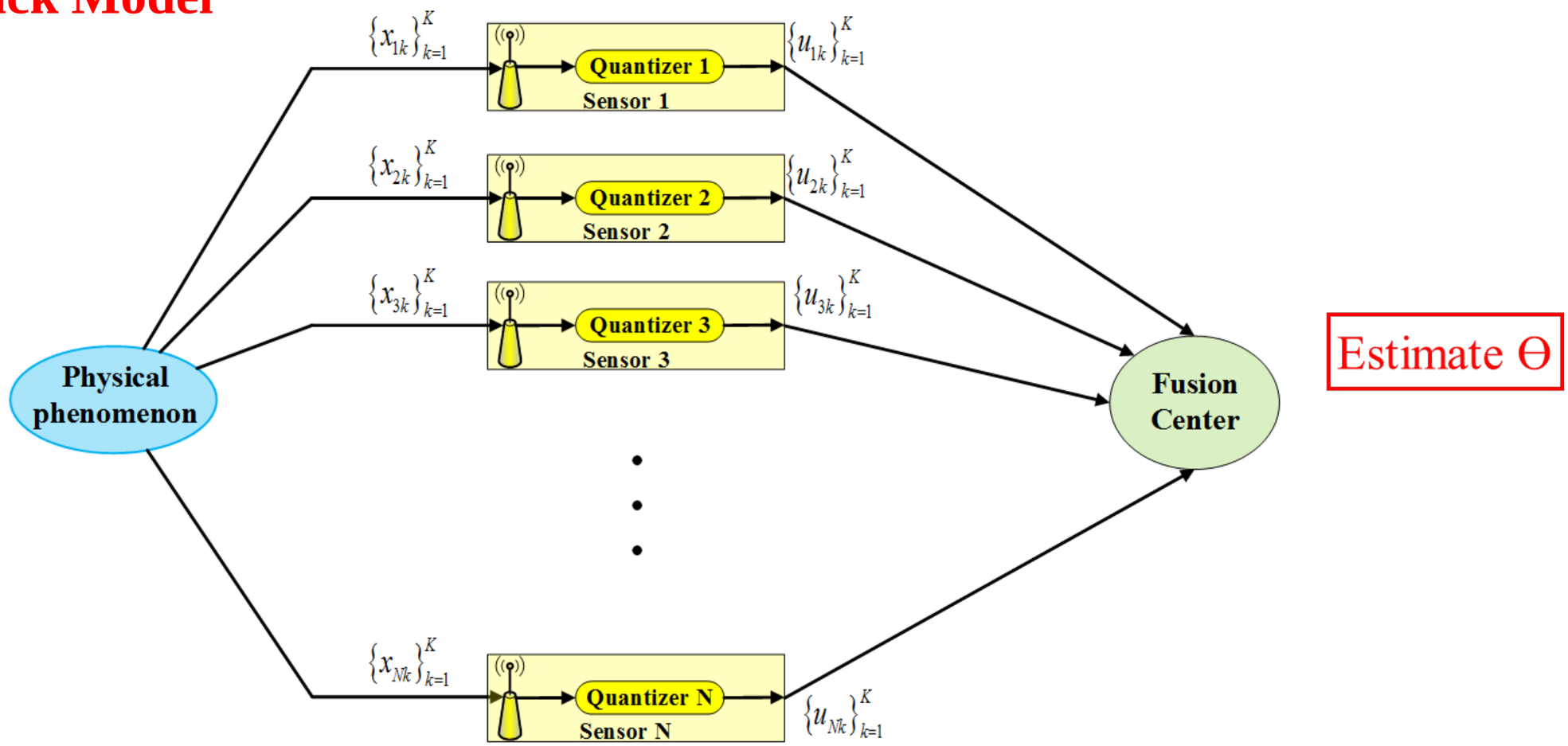
J. Zhang, R. S. Blum, X. Lu, and D. Conus, “Asymptotically optimum distributed estimation in the presence of attacks,” Signal Processing, IEEE Transactions on, vol. 63, no. 5, pp. 1086–1101, March 2015.

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 Detection in Sensor Network Target Localization Systems with Quantized Data", to appear in IEEE Transactions on Signal Processing. – also general to spoofing.

System Model

Without Attack Model

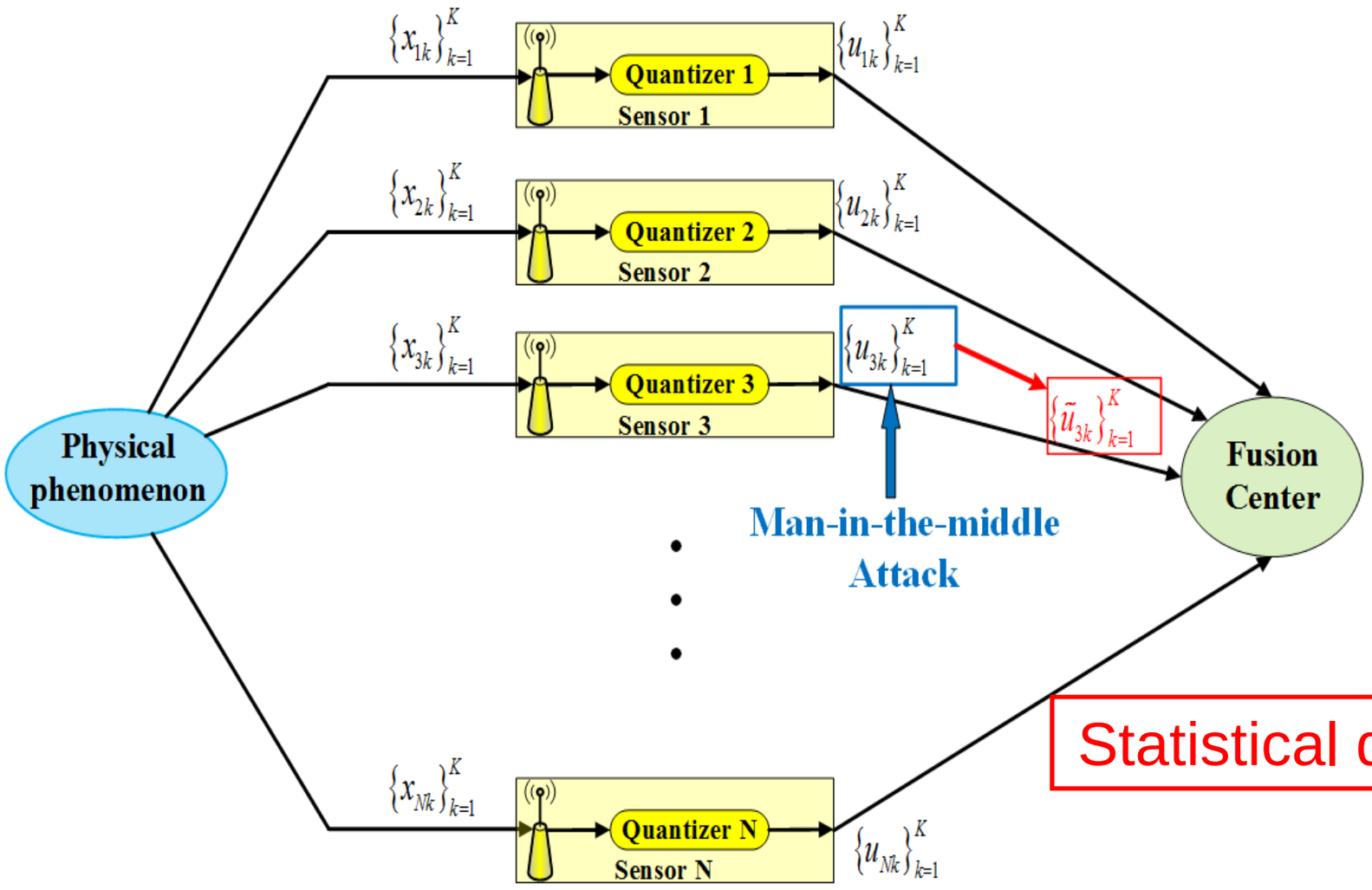


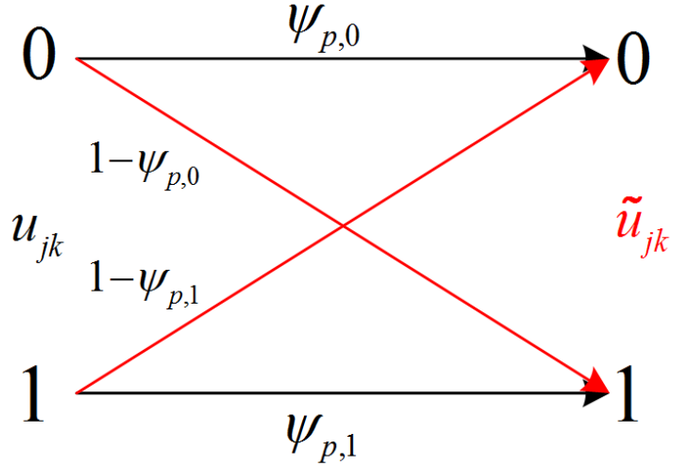
For simplicity of analysis, assume:

- $x_{jk} = \theta + n_{jk},\ \forall j = 1,2,\ldots,N,\ \forall k = 1,2,\ldots,K.$
- 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 $p = 1,2, \dots, P$.
- $\mathcal{A}_0$: 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 $K\rightarrow\infty$, 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 $N\rightarrow\infty$, 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.

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 (change τ).

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

We provide a mathematical calculation that decides. ***Gives Gain***

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.

Attack can make data not dependent on θ

OPTIMUM ESTIMATION UNDER ATTACK

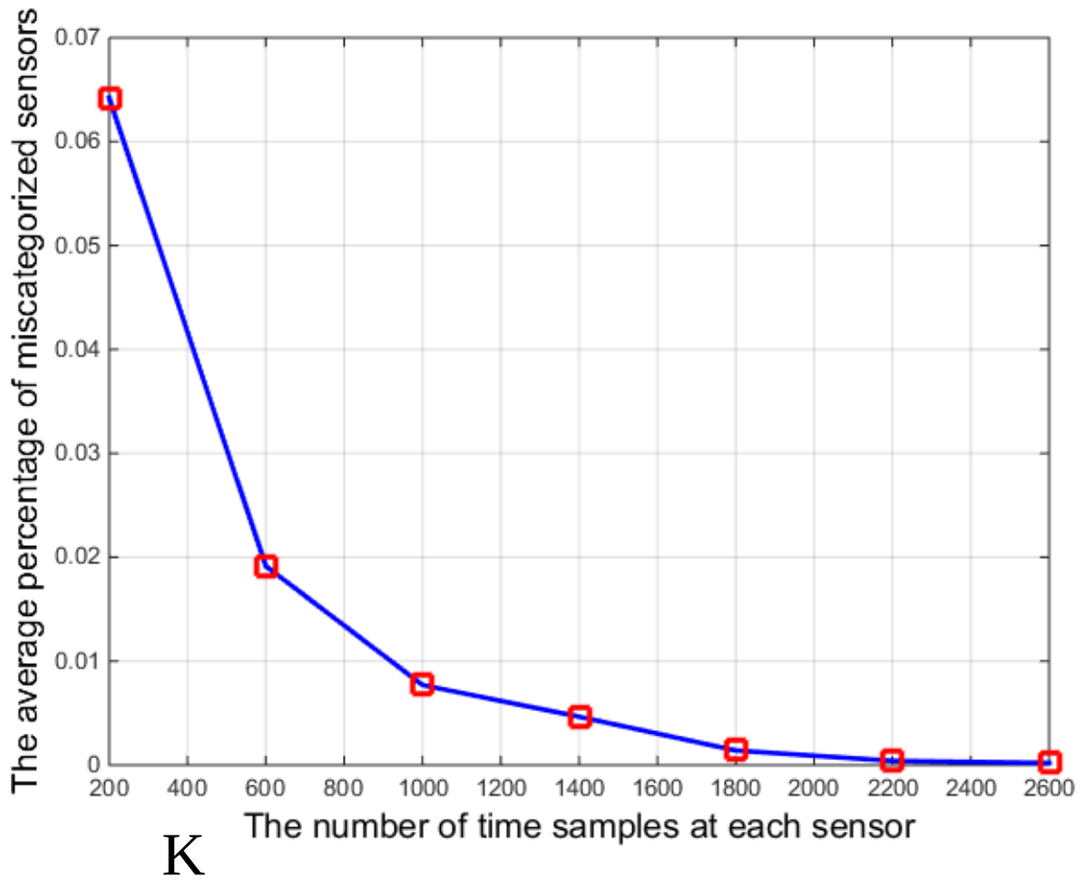
Taken together → This describes Optimum Processing under any man-in-the-middle attack – have generalized to cases with spoofing attacks.

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 ↓

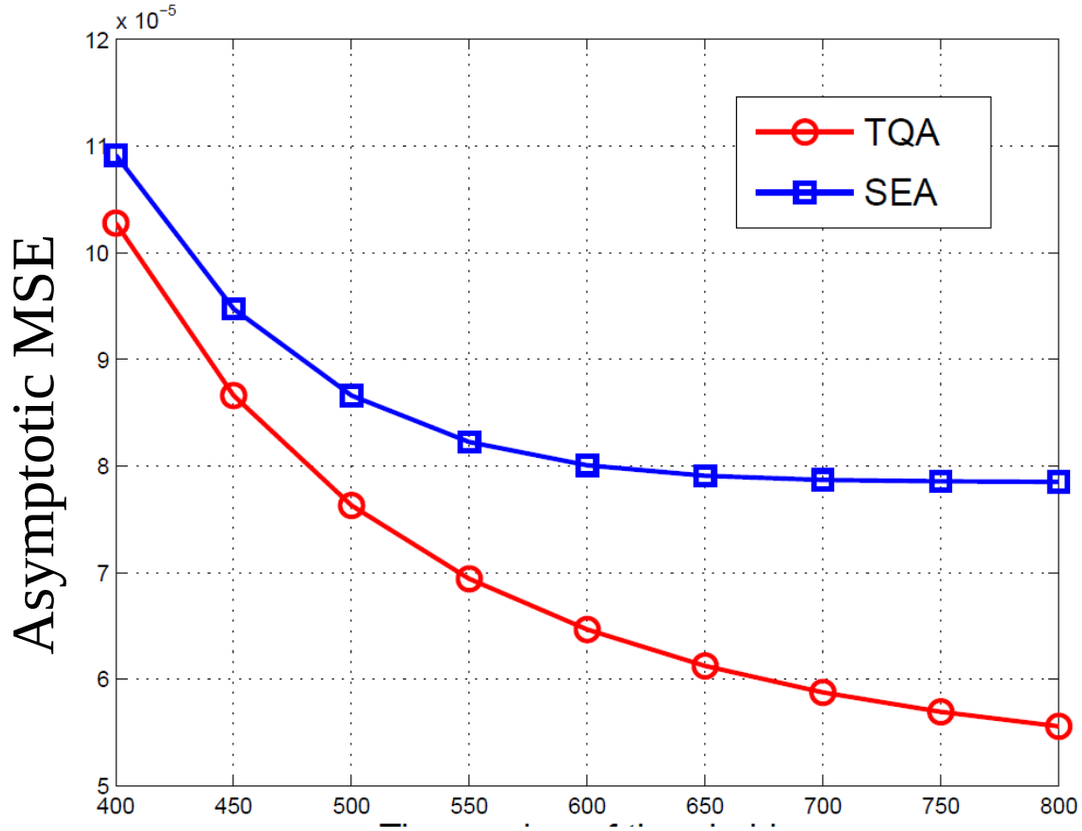
Verify the Theorem on the identification and categorization of attacked sensors.

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: $\mathcal{P}_2 = 20\%$, $(\psi_{1,0}, \psi_{1,1}) = (0.15, 0.2)$.



❖Significant CRB improvement.

Verify the superiority of the TQA.

SEA: use only unattacked

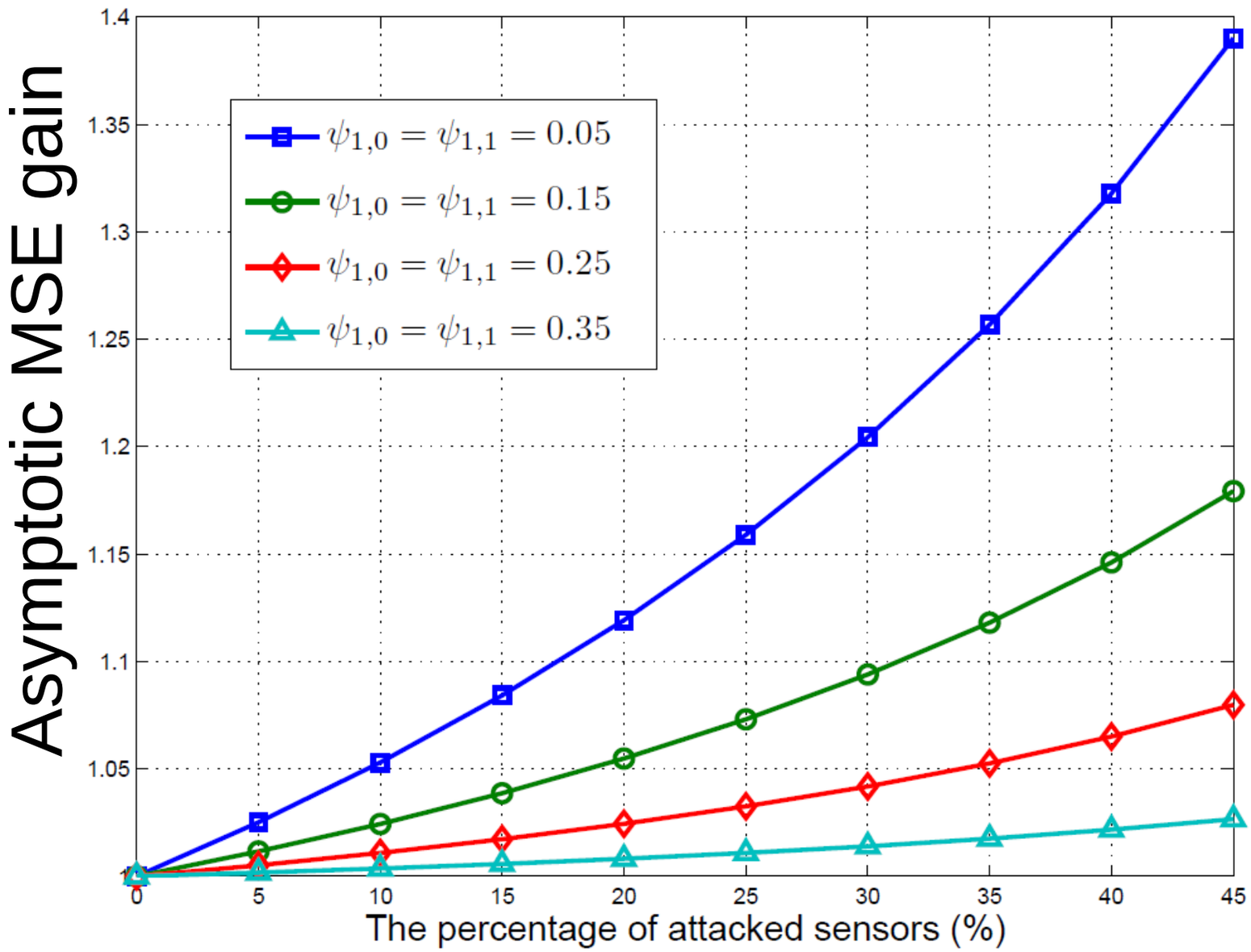
Numerical Results

Relative Asymptotic MSE Gain vs the Percentage of Attacked Sensors :

- One attack
- Same as last
- All of Q

Verify some attacks make data useless.

$$\frac{MSE_{SEA}}{MSE_{TVQ}} =$$



Part II:
Functional Forms of Optimal Spoofing Attacks (Man-in-Middle)

Describes the most effective attacks → make data useless – have generalized to cases with spoofing attacks.

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 $\{\mathcal{A}_p\}_{p=0}^{P}$ 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 $\boldsymbol{\tau}^{(\mathbf{p})}$ → $D_p > \sum_{j \in \mathcal{A}_p} K_j \left(R_j - 1\right)$ → Only determined by the numbers of quantization levels employed in a given $\mathcal{A}_p$

quant symbols

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 $\tilde{g}_j$.

Implications for Unattacked Systems

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

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

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

Sufficient but not necessary

Dim of $\boldsymbol{\theta}$

Estimation Capacity

Have shown this also
leads to nonidentifiablity
& have nonindependent results

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

Publication List

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,” IEEE Transactions on Signal Processing, Volume 65, Issue 3, Feb. 2017, pp. 705-720.

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, R. S. Blum, L. Kaplan, and X. Lu, “A fundamental limitation on maximum parameter dimension for accurate estimation using quantized data,” in review or IEEE Transactions on Information Theory (on ArXiv).

Thank You!

rblum@Lehigh.edu