Jiangfan Zhang, Rick S. Blum, and H. Vincent Poor

Approaches to Secure Inference in the Internet of Things

Performance bounds, algorithms, and effective attacks on IoT sensor networks

INTERNET OF THINGS—ISTOCKPHOTO.COM/IAREMENKO
CIRCUITS—IMAGE LICENSED BY INGRAM PUBLISHING

Digital Object Identifier 10.1109/MSP.2018.2842261
Date of publication: 28 August 2018

The Internet of Things (IoT) improves pervasive sensing and control capabilities via the aid of modern digital communication, signal processing, and massive deployment of sensors but presents severe security challenges. Attackers can modify the data entering or communicated from the IoT sensors, which can have a serious impact on any algorithm using these data for inference. This article describes how to provide tight bounds (with sufficient data) on the performance of the best unbiased algorithms estimating a parameter from the attacked data and communications under any assumed statistical model describing how the sensor data depends on the parameter before attack. The results hold regardless of the unbiased estimation algorithm adopted, which could employ deep learning, machine learning, statistical signal processing, or any other approach. Example algorithms that achieve performance close to these bounds are illustrated. Attacks that make the attacked data useless for reducing these bounds are also described. These attacks provide a guaranteed attack performance in terms of the bounds regardless of the algorithms the unbiased estimation system employs. References are supplied that provide various extensions to all of the specific results presented in this article and a brief discussion of low-complexity encryption and physical layer security is provided.

Introduction

The IoT will introduce an unprecedented increase in sensor resources and data-producing sensor-like objects for many applications. Over 1 trillion IoT sensors, machines, objects, and devices are expected to be connected to the Internet by 2022. The top three IoT applications by market share are anticipated to be health care (41%), manufacturing, (37%), and electricity grids (7%). Even more impressive, IoT smart objects are expected to generate 45% of all Internet traffic by 2022. While the Internet has been available for many years, the integration of sensing technology into the Internet is still very immature and brings new problems that have not yet been addressed. Serious security concerns for IoT systems have already been demonstrated, and the future brings even more concerns. For

 1053-5888/18©2018IEEE

example, self-driving cars could become dangerous weapons unless adequate security solutions are developed. For these reasons, many researchers are focused on finding new cybersecurity technologies for the IoT to augment current technology [1], [2]. Each new technology, including the inferential sensor processing technology that is the focus of this article, can form one layer of a multilayer security paradigm, with the other layers employing different approaches drawn from both new and existing alternatives. The hope is that if one layer is defeated, the other layers could still provide protection.

Typically, large IoT systems are composed of low-cost and spatially distributed sensor nodes with limited battery power and low computing capacity, which makes them particularly vulnerable to cyberattacks by adversaries. This has led to great interest in studying the vulnerability of the IoT in various applications and from different perspectives; see [3]–[24] and the references therein. Moreover, due to the dominance of digital technology, quantization has been widely employed at the sensors in IoT systems. The more recent topic of cybersecurity for IoT has received less attention than the topic of cybersecurity for other systems, but the increasing adoption of sensors and IoT networks makes this a very important issue. This article focuses on machine-learning (we do not study attacks on the training here) and signal processing approaches to the development of security in inferential sensor processing for the IoT using quantized data. The discussion will mainly focus on estimation in the presence of active cyberattacks that manipulate the data in IoT systems, although the ideas can also be generalized in many interesting ways beyond estimation applications. To provide a clear picture in a limited space, we focus on techniques to allow the estimation system to identify such attacks and perform robust processing in their presence. In fact, we provide tight bounds (for sufficient sample sizes) on the best possible performance the unbiased estimation system can achieve. We also describe optimized attacks from the attacker's point of view. At the end of the article, we provide a brief discussion of some specific aspects of some related topics of interest, including eavesdropping, secrecy, encryption, and authentication.

The topic of impact and mitigation of cyberattacks on systems solving hypothesis testing problems was studied in [3], [4], [7]–[9], and references therein. Investigations on cyberattacks on estimation systems have been studied in [6], [7], [10]–[15], [17], [23], and references therein. The early work in [3], [4], [6], [7]–[9], [13]–[15], and [23] set the tone for many later investigations and influenced most of the discussions in this article. In particular, the impact and mitigation of cyberattacks on systems solving hypothesis testing problems was studied in [3], [4], [7], [9], and references therein. Distributed detection in tree topologies in the presence of cyberattacks was considered in [8]. Investigations of cyberattacks on estimation systems have been studied in [6], [7], [10]–[15], [17], [23], and references therein. The problem of distributed spectrum sensing in a cognitive radio network under cyberattacks was studied in [4], [5], and [25]. Several cyberattack detection techniques were proposed for IoT localization systems in [6], [12], [18], and [19]. More recently, the data-injection attacks in smart grids were considered in [13]–[15], [26], and the references therein.

According to where they occur, cyberattacks in IoT systems can be categorized into two classes, as illustrated in Figure 1. We call any attack modifying a signal in the IoT system prior to quantization a *spoofing attack*. It has been shown [12] that the same changes in the signals in the IoT system produced by any spoofing attack can also be produced by changing the data going into the sensors to be different from that coming from the physical phenomenon being monitored. We call any attack modifying a signal in the IoT system after quantization a *man-in-the-middle attack* (*MiMA*). The same changes in the signals in the IoT system produced by any MiMA [12] can also be produced by changing the quantized data transmitted

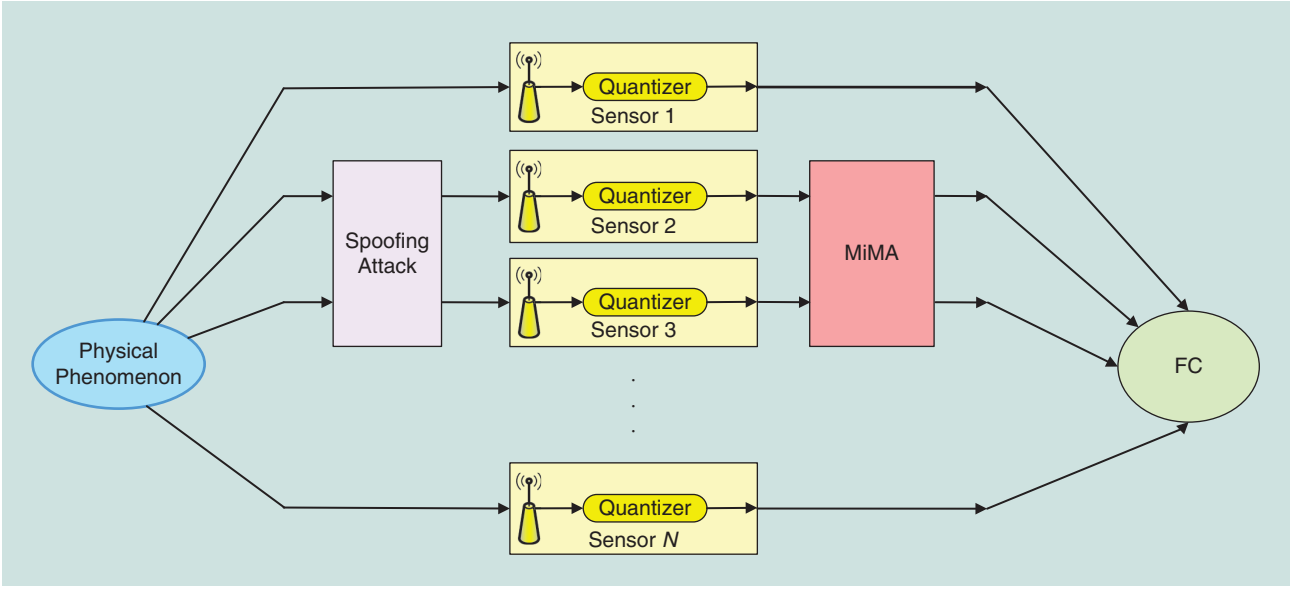

FIGURE 1. Cyberattacks in IoT systems.

by the sensors. Further, combinations of these two possible classes of attacks can represent any type of possible attack even if the actual attack modifies the sensor hardware or software as opposed to changing the data entering or leaving the sensor node.

MiMAs caused by an attacker intercepting a communication packet and changing its contents or by an attacker forcing a sensor node to transmit false data have received previous research attention. For instance, MiMAs were studied for distributed spectrum sensing in a cognitive radio network in [4], [5], and [25]. The distributed detection problem in the presence of MiMAs was investigated in [3]. Mitigation techniques for MiMAs were studied in localization problems in [6] and [12]. Spoofing attacks have also been studied for localization problems; see [18], [19], and the references therein. In [18, Table I], a summary of different types of spoofing attacks for localization problems is provided. The dangers of spoofing attacks on global positioning system (GPS) receivers that provide important information to everything from car navigation to national power grids have drawn serious public concern [27], [28]. Radar and sonar systems also suffer from spoofing attacks in practice. As an example of a spoofing attack technique, the application of an electronic countermeasure (ECM), which is designed to deceive a radar or sonar system, can critically degrade the detection and estimation performance of the system [29]. One popular technique for the implementation of ECMs employs digital radio-frequency memory (DRFM) to store a received radar signal and transmit it back to the radar receiver to confuse the victim radar system. DRFM can mislead the estimation of the range of the target by altering the delay of the pulses received by the radar system and fool the system into incorrectly estimating the velocity of the target by introducing a fake Doppler shift in the retransmitted signal [30]. Since radar systems are being installed by most car manufacturers, with the ultimate application being self-driving cars, spoofing attacks are potentially very dangerous. The data-injection attack in smart grids is another typical example of a spoofing attack; see [13]–[15], [26], and the references therein.

Regarding MiMAs, we focus on the fundamental problems in identifying and mitigating the impact of malicious cyberattacks. In particular, it is shown that, under some assumptions, it is possible to correctly identify the attacked sensors and categorize them into differently attacked groups. One such assumption is that the largest group of similarly attacked sensors are unattacked. Furthermore, once the differently attacked sensors have been categorized, necessary and sufficient conditions are provided that describe when the attacked sensor data can and cannot improve the estimation performance in terms of the Cramér–Rao bound (CRB).

All existing research on attacks on IoT systems performing inference considers cases in which the attacker replaces the unattacked sensor or communication data by a function of the unattacked data where the form of the function is known down to some unknown scalar quantities which are called *attack parameters*. For example, a specific type of spoofing attack, called a *data-injection attack*, adds an unknown attack parameter to the sensor data. Thus, the function here is a linear function with unit slope, and the attack parameter is the value added to the sensor data. We consider much more general types of attacks and describe the functions that guarantee the IoT estimation system can achieve, at best, a given level of performance no matter what approach the estimator takes. This shows the existence of very powerful attacks, from the attacker's point of view, such that the attacker is guaranteed to force the estimation system to have performance below some unacceptable value. To be precise, for a generalized spoofing attack using known functions with unknown attack parameters, necessary and sufficient conditions are provided under which the attack provides a guaranteed attack performance in terms of CRB degradation regardless of the processing the IoT system employs, thus defining a highly desirable attack. Further analysis of these attacks reveals that the quantization imposes a limit on the capability of the system to defend against attacks, which can be exploited to construct an optimal attack by properly employing a sufficiently large dimensional attack vector parameter relative to the number of quantization symbols employed.

The most general attacks, which include combinations of MiMAs and spoofing attacks, are illustrated in the section "General Attacks in Vector Parameter Estimation Systems," when estimating the location of an object. With the help of two secure sensors, a class of detectors is proposed to detect the attacked sensors by scrutinizing the existence of a geometric inconsistency. Moreover, it is shown that the error probability of the proposed attack detector decays exponentially by employing large deviations techniques.

Originally motivated by our research on cybersecurity, we reveal a fundamental limitation on quantized estimation systems not under attack. A critical quantity called *inestimable dimension for quantized data* (*IDQD*) is introduced, which does not depend on the estimation problem, the quantization regions, or the exact statistical models of the observations but instead depends only on the number of sensors and on the precision of the quantizers employed by the system. It is shown that, if the dimension of the desired vector parameter is larger than the IDQD of the quantized estimation system, then the Fisher information matrix (FIM) for estimating the desired vector parameter is singular, and, moreover, there exist infinitely many nonidentifiable vector parameter points in the vector parameter space.

MiMAs

To introduce a simple problem, we consider a set of N distributed IoT sensors, each making K time observations of a deterministic scalar parameter θ corrupted by additive noise. At the jth sensor, the observation at the kth time instant is described by

$$x_{jk} = \theta + n_{jk}, \forall j = 1,2,...,N, \forall k = 1,2,...,K, \qquad (1)$$

where n_{jk} denotes an additive noise sample with zero-mean probability density function (pdf) $f(n_{jk})$ and $\{n_{jk}\}$ is an

independent and identically distributed sequence. (Extensions to general estimation problems and nonbinary quatization are considered in [11].) Each observation x_{jk} is individually quantized, and the result is denoted by u_{jk}. All of the quantized observations are sent to the fusion center (FC) for use in estimating θ. While we allow these communications to be attacked, we ignore any other errors in the communications to keep things simple, including those due to noise or fading.

Lately, there has been great interest in the extreme case where each sensor is restricted to transmitting a single bit per observation to the FC. A basic approach is to decide $u_{jk} = 1$ if $x_{jk} > \nu$, where ν is a fixed threshold, and $u_{jk} = 0$ otherwise. Thus, without attacks $\Pr(u_{jk} = 0 \,|\, \theta) = F(\nu - \theta)$ and $\Pr(u_{jk} = 1 \,|\, \theta) = 1 - F(\nu - \theta)$, where $F(x) \triangleq \int_{-\infty}^{x} f(t)dt$ denotes the cumulative distribution function (cdf) corresponding to the pdf $f(x)$. By employing the invariance of the maximum likelihood estimate (MLE), the naive MLE (NMLE), the MLE formulated under the assumption of no attack, of the parameter θ can be expressed as

$$\hat{\theta}_{\mathrm{NML}} = \nu - F^{-1}\left(1 - \frac{1}{KN}\sum_{j=1}^{N}\sum_{k=1}^{K} u_{jk}\right), \tag{2}$$

which, without the presence of an adversary, can be expected to provide asymptotically unbiased and efficient estimation.

Let, at most, P distinct malicious attacks (P arbitrary) be launched at a given time, where each attack follows a fairly general adversary model to be described next. Let $\mathcal{A}_p$ denote the set of sensors subjected to the pth attack, and let $\tilde{u}_{jk}$ represent the after-attack quantized observation, which is a modified version of u_{jk}. The statistical description of the pth attack can be represented by a probability transition matrix $\mathbf{\Psi}_p$,

$$\mathbf{\Psi}_p \triangleq \begin{bmatrix} \psi_{p,0} & 1-\psi_{p,1} \\ 1-\psi_{p,0} & \psi_{p,1} \end{bmatrix}, \tag{3}$$

where $\psi_{p,0} \triangleq \Pr(\tilde{u}_{jk} = 0 | u_{jk} = 0)$ and $\psi_{p,1} \triangleq \Pr(\tilde{u}_{jk} = 1 | u_{jk} = 1)$ are attack parameters that determine the modification probabilities (flipping probabilities). Here, we assume the attacker does not know θ, and so the attack parameters do not depend on θ. Extended discussion of various cases in which the attacker has more or less information about the estimation system and the estimation problem are considered in [11]. Due to the pth attack, the after-attack probability mass function (pmf) of the observations can be related to the before-attack pmf using

$$\begin{bmatrix} 1-\tilde{p}(\mathbf{\Psi}_p,\theta) \\ \tilde{p}(\mathbf{\Psi}_p,\theta) \end{bmatrix} \triangleq \begin{bmatrix} \Pr(\tilde{u}_{jk}=0|\theta) \\ \Pr(\tilde{u}_{jk}=1|\theta) \end{bmatrix} = \mathbf{\Psi}_p \begin{bmatrix} \Pr(u_{jk}=0|\theta) \\ \Pr(u_{jk}=1|\theta) \end{bmatrix}. \tag{4}$$

For the sake of expressing the after-attack pmfs of observations in a uniform form for both attacked and unattacked sensors, define the set $\mathcal{A}_0$ of unattacked sensors, that is, if $j \in \mathcal{A}_0$, then $\tilde{u}_{jk}$ and u_{jk} have the same distribution.

Assumption 1

The following assumption on attacks is made throughout this article.

1) Over the K sample estimation time interval described in (1) and for all p, the pth attack is statistically described as in (4) for all the sensors in the set $\mathcal{A}_p$. The set $\mathcal{A}_p$ and the attack parameters are unknown to the FC. Let $\mathcal{P}_p \triangleq |\mathcal{A}_p|/N$. Moreover, we assume that the group of unattacked sensors is the largest group $\mathcal{P}_0 > \mathcal{P}_p + \Delta_0$ for all $p \geq 1$ where Δ_0 is a positive constant. Further, the sets $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_P$ are disjoint $\mathcal{A}_p \cap \mathcal{A}_{p'} = \emptyset \quad if \quad p \neq p'$.
2) Significant attacks. Since attacks that cause very small changes to $\tilde{p}(\mathbf{\Psi}_0, \theta)$ cause very little impact on performance (similar to small noise), we only consider attacks that produce at least a minimum distortion d_{impact} on $\tilde{p}(\mathbf{\Psi}_0, \theta)$ and tamper with at least Δ percent of sensors so that

$$|\tilde{p}(\mathbf{\Psi}_p,\theta) - \tilde{p}(\mathbf{\Psi}_0,\theta)| \geq d_{\mathrm{impact}}, \quad \forall p = 1,2,...,P, \tag{5}$$

$$\mathcal{P}_p \triangleq |\mathcal{A}_p|/N \geq \Delta > 0, \quad \forall p = 1,2,...,P. \tag{6}$$

3) Various attacks. The changes caused by two distinct types of attacks are considerably different; otherwise, these two types of attacks can be treated as identical. To this end, we assume that

$$|\tilde{p}(\mathbf{\Psi}_l,\theta) - \tilde{p}(\mathbf{\Psi}_m,\theta)| \geq d_{\mathrm{diff}}, \quad \forall l \neq m. \tag{7}$$

It is worth mentioning that the adversary model assumed in (4) can change the after-attack pmf to have any desired valid values satisfying (5) and (7) through proper choice of the two attack parameters $\psi_{p,0}$ and $\psi_{p,1}$. In this sense, it is a fairly general adversary model.

Identification and categorization of attacked sensors

The following theorem describes the identification and categorization of the attacked sensors.

Theorem 1

Under Assumption 1, for any N as $K \to \infty$, the FC can always identify from the observations, without further knowledge, a $\mathcal{P}_0$ percentage group of sensors that contains 0% attacked sensors. Similarly, as $K \to \infty$, the FC is also able to identify P other groups of sensors that, respectively, make up $\{\mathcal{P}_p\}_{p=1}^{P}$ percent of all sensors, such that for $p = 1,2,...,P$, group p contains 0% sensors not experiencing attack p.

On the other hand, assume each sensor observes a finite number K of time samples such that

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

where γ^* is a constant defined in [10]. Under Assumption 1, as $N \to \infty$, the FC can determine P and a group of sensors $\tilde{\mathcal{A}}_p$ corresponding to $\mathcal{A}_p$, for $p = 1,\ldots,P$, with $\tilde{\mathcal{P}}_p \triangleq |\tilde{\mathcal{A}}_p|/N, \mathcal{P}_p^* \triangleq |(\tilde{\mathcal{A}}_p \backslash \mathcal{A}_p) \cup (\mathcal{A}_p \backslash \tilde{\mathcal{A}}_p)|/N$, and $\delta \triangleq -(4\ln 2/\Delta(K-1)\gamma^*)$, which satisfy

$$0 \leq |\tilde{\mathcal{P}}_p - \mathcal{P}_p| \leq \mathcal{P}_p^* < \delta. \tag{9}$$

One should notice the stark differences in Theorem 1 when we increase N to large values instead of K. Given that we define a sensor as attacked or unattacked, this does make sense. When we are given more data at a given sensor for which we already had some data, then the new data will certainly help us better categorize the statistical model for the data at this sensor. If we increase K at a group of fixed sensors, this will help us determine which sensors are attacked, which are not, and which sensors are similarly attacked. If we are given data from a new sensor, from which we had not previously been given data, then we are also given a new problem: "Is this sensor attacked?" Thus, given our problem formulation, increasing K to large values is more helpful than increasing N to large values.

The essential idea toward accomplishing the identification and categorization of the attacked sensors is to recognize that the statistical description of the data at the differently attacked sensors will be significantly different based on Assumption 1. Thus, one could estimate the pmfs of the quantized data at each sensor using histograms and then classify the sensors into different groups representing the different attacks or the group of unattacked sensors. As the number of observations at each sensor K becomes large, it seems reasonable that the estimates become more accurate for larger K. Many other methods can also be used for identification and categorization. We can use the estimate in (2) to also see the statistical differences from sensor to sensor for sufficiently large K given the good properties of this estimate for the described problem. Note that Assumption 1 defines significant differences in the pmfs of unattacked and attacked data [numerical values for d_{impact} in (5) can be chosen based on which differences cause significant performance degradation to the estimation performance when the data are assumed to be unattacked]. Note that Assumption 1 also defines significant differences in the pmfs of differently attacked data [numerical values for d_{diff} in (7) can be chosen based on which differences cause significant degradation if ignored]. We also need a way to distinguish which group is unattacked. If we know the largest group is unattacked, as assumed in Assumption 1, or if we have some protected sensors, these are some methods to distinguish which group is unattacked from among the groups of sensors deemed to be statistically different.

Estimation performance improvement via using attacked sensor data

As demonstrated by Theorem 1, when each sensor accumulates sufficiently many time samples, then the FC is able to determine the number of attacks in the network and very accurately categorize the sensors into different groups according to distinct types of attacks. In the rest of this section, we assume that the sensors have been well categorized into the groups $\{\mathcal{A}_p\}_{p=0}^{P}$, and we attempt to estimate the desired parameter θ. For simplicity, we assume the categorizations are exactly correct $(K \to \infty)$, but the following results would only be approximately true if errors are made $(K \not\to \infty)$. There are two approaches:

1) Ignore the data at the attacked sensors and just employ the data at the unattacked sensors to estimate the desired parameter. We refer to this approach as the *simple estimation approach* (*SEA*).
2) Use the data at the attacked sensors and jointly estimate the desired parameter and the unknown attack parameters.

It requires less complexity to take approach 1), which avoids estimating any parameters describing the attacks. However, to attempt to take approach 2), and potentially do better than approach 1), we will investigate the performance of the joint estimation of the desired parameter and the unknown attack parameters. Let $\boldsymbol{\theta} \stackrel{\Delta}{=} [\theta, \psi_{1,0}, \psi_{1,1}, ..., \psi_{P,0}, \psi_{P,1}]^T$ denote a vector containing the desired scalar parameter θ along with all of the unknown parameters of the attacks. The estimation performance is evaluated by the mean-squared error (MSE), which is lower bounded in a positive definite sense using

$$\mathbb{E}\{[\hat{\boldsymbol{\theta}}(\mathbf{u}) - \boldsymbol{\theta}][\hat{\boldsymbol{\theta}}(\mathbf{u}) - \boldsymbol{\theta}]^T\} \succeq \mathbf{J}^{-1}(\boldsymbol{\theta}), \tag{10}$$

where $\hat{\boldsymbol{\theta}}$ is any unbiased estimator of $\boldsymbol{\theta}$, $\mathbf{u}$ denotes the vector that contains all employed quantized observations $\{u_{jk}\}$, $\mathbf{J}(\boldsymbol{\theta})$is the FIM, and the (1, 1) component of $\mathbf{J}^{-1}(\boldsymbol{\theta})$ is the CRB for estimating the desired scalar parameter θ. Note that the CRB is an asymptotically achievable bound on MSE. In typical applications, a good estimator with the required number of observations to achieve the desired performance usually performs close to the CRB. We will make use of the CRB and FIM to benchmark the estimation performance of unbiased parameter estimators. In our studies of inference for the IoT in this article, we restrict attention to unbiased estimators. Extensions to biased estimators is a topic of current research. If the FIM is singular for the data from a specific sensor, then those data are no longer useful to reduce the MSE when the data are fused with data from other sensors [17]. An attacker can create this situation with a proper attack [17]. Thus, the FIM can provide a rigorous way to identify good attacks that make the attacked data useless. Knowing that attacked data are useless for reducing the MSE when those data are fused with data from other sensors is also useful in the estimation procedure [10]. Thus, the CRB and FIM are very powerful while being relatively easy to compute. General calculations of MSE are generally intractable. This explains why the CRB is the most widely used lower bound and why analysis based on the FIM is so common. One can certainly expand the work discussed here to go beyond these metrics, but there will be a cost in terms of computational complexity and the simplicity of explanation obtained by simple closed-form expressions.

It is shown in [10] that using the fixed threshold approach described before (2) will not allow joint estimation of the desired and attack parameters, since the FIM for that estimation is singular. This phenomenon is explained by the theory we provide in the section "Implications for Unattacked Systems." There we show that the quantized observations from a given quantization approach are really only capable of accurately estimating a parameter with dimension smaller than a given value. The quantization approach with a common threshold for all sensors and for all samples at each sensor can only estimate a scalar parameter for the given problem. This approach cannot jointly estimate both the desired scalar parameter and the attack parameters. To overcome this, we can employ a

quantization scheme that allows us to estimate a larger dimensional parameter, with a dimension $2P + 1$ for the $2P$ attack parameters and the desired scalar parameter θ. In particular, we define a set of Q distinct thresholds $\mathfrak{T} = \{\nu_1, \nu_2, ..., \nu_Q\}$ and employ different thresholds over Q distinct time slots $\{\mathcal{T}_t\}_{t=1}^{Q}$, while using the same threshold at each sensor. We refer to this approach as the *time-variant quantization approach* (*TQA*). Let $\tilde{p}_p^{(t)} \triangleq \Pr(\tilde{u}_{jk} = 1 | \boldsymbol{\theta})$ for $j \in \mathcal{A}_p, k \in \mathcal{T}_t$, and let $\boldsymbol{\Xi}_p \triangleq \frac{d}{d\theta}[\tilde{p}_p^{(1)}, \tilde{p}_p^{(2)}, \ldots, \tilde{p}_p^{(Q)}]$.

In Theorem 2, we provide necessary and sufficient conditions under which the CRB performance of estimating the desired scalar parameter θ can be improved by employing observations from an attacked sensor.

Theorem 2

The FIM for estimating $\boldsymbol{\theta}$ is nonsingular provided that $Q \geq 2$. Moreover, the CRB for the desired scalar parameter θ can be improved by utilizing the observations from the set of attacked sensors in our proposed fashion (TQA) if and only if for some $p \in \{1, 2, \ldots, P\}$, $\text{rank}(\boldsymbol{\Xi}_p) = 3$. Otherwise, there is no CRB improvement, but also no loss in CRB, from utilizing the attacked observations.

In particular, by employing the TQA, the relative CRB gain from utilizing the observations at the attacked sensors is

$$\frac{\text{CRB using SEA}}{\text{CRB using TQA}} = 1 + \frac{1}{[\boldsymbol{\Gamma}_0]_{1,1}} \sum_{p=1}^{P} \frac{\det(\boldsymbol{\Gamma}_p(\{1, 2p, 2p+1\}, \{1, 2p, 2p+1\}))}{\det(\boldsymbol{\Gamma}_p(\{2p, 2p+1\}, \{2p, 2p+1\}))}, \tag{11}$$

where $\boldsymbol{\Gamma}_p(\{i_1, i_2, \ldots, i_L\}, \{j_1, j_2, \ldots, j_M\})$ denotes the submatrix of $\boldsymbol{\Gamma}_p \triangleq \boldsymbol{\Xi}_p \boldsymbol{\Lambda}_p \boldsymbol{\Xi}_p^T$ ($\text{p} = 0, 1, \ldots, \text{P}$), which consists of the elements located in the $\{i_l\}_{l=1}^{L}$th rows and $\{j_m\}_{m=1}^{M}$th columns. $[\boldsymbol{\Gamma}_0]_{1,1}$ is the (1,1) component of $\boldsymbol{\Gamma}_0$. The matrix $\boldsymbol{\Lambda}_p$ is a Q-by-Q diagonal matrix, and the tth diagonal element of $\boldsymbol{\Lambda}_p$ is $K_t \mathcal{P}_p / \tilde{p}_p^{(t)}(1 - \tilde{p}_p^{(t)})$, where K_t is the number of time samples in $\mathcal{T}_t$.

Interpretation of Theorem 2 and (11) is now given. Recall that the CRB is a lower bound on the MSE of any unbiased estimator. The CRB is achieveable with a reasonable number of observations. The ratio of the CRB of the approach that ignores the attacked data to the CRB of the approach using the attacked data is shown in (11). Here, we see the power of the CRB in allowing us to obtain fairly simple closed-form expressions that we could not obtain using general expressions of MSE. One of the most interesting aspects of (11) is when the ratio is larger than unity. If the ratio is larger than unity, then it is advantageous to use the attacked data in terms of CRB. If the ratio is unity, then the estimator can ignore the attacked data. From (11), and noting the provable nonnegativity of the second term due to the positive semidefiniteness of $\boldsymbol{\Gamma}_p$, the ratio must be unity or larger. Thus, (11) describes the utility of the attacked data in a very simple manner. Note that (11) also describes the exact value of the improvement. Since the determinant of any rank deficient matrix is zero, (11) also verifies Theorem 2, since the denominator matrix in the second term is always full rank and the numerator needs the matrix $\boldsymbol{\Xi}_p$ referred to in Theorem 2 to have rank three for some p to ensure that the ratio of CRBs will be greater than unity. Note that each entry of one of the columns of $\boldsymbol{\Xi}_p$ is obtained by taking a derivative with respect to one of the components of the vector $\boldsymbol{\theta}$. Since the pmf of the data under the pth attack can depend only on θ and the two pth attack parameters and not on the other attack parameters, then $\boldsymbol{\Xi}_p$ can have at most three nonzero rows. Due to this, $\boldsymbol{\Gamma}_p$ can have only nine nonzero entries, which explains the form of (11).

Generalizations and motivating IoT estimation problems

In [11], we provide extensions to the previously discussed results for nonbinary quantization and general estimation problems. For these cases, we provide a theorem similar to Theorem 1 on the ability to categorize and classify the differently attacked and unattacked sensors. After classification, one can similarly judge if the data at a group of similarly attacked sensors can be useful to improve estimation performance in terms of CRB. Once again, some attacks will make the attacked data useless for this purpose. This generalization allows us to consider many important IoT estimation applications.

One application that has drawn significant attention lately is that of self-driving cars. Attacks in this application are especially concerning since loss of life could result. This application clearly convinces us of the importance of further developing the kind of theory initiated in this article. It turns out that most car manufacturers are convinced that the best way to stop self-driving cars from injuring people is to fuse radar and video data. In fact, some may want to fuse other sensors as well. Car manufacturers are all developing inexpensive integrated circuit chips to fully incorporate the radar processing. Interestingly, when these inexpensive integrated circuit chips become available, this will encourage extensive use of radar in all kinds of applications and products, beyond autonomous vehicles. Surveillance applications will certainly benefit. In fact, the same process will likely be followed for other complicated sensors. Thus, when inexpensive integrated circuits become available for these other sensors, this will encourage extensive use of these sensors in all kinds of applications and products. Since these sensors can be attacked, methods for protecting these sensors, like the ones presented here, become extremely important. Attacks on the sensors (the GPS is also a sensor) or communications in self-driving cars are one application motivating this work.

In [12], we focus on location estimation under possible simultaneous MiMAs and spoofing attacks, but similar approaches can be applied for other vector parameter estimation problems. These vector parameter estimation problems can be important in medical, manufacturing, and smart grid applications, among others. We discuss [12] in more detail in the section "General Attacks in Vector Parameter Estimation Systems."

Illustrative example: Identification and categorization of attacked sensors

Consider a network with $N = 10$ sensors, which is subject to two attacks that control 30% and 20% of the sensors,

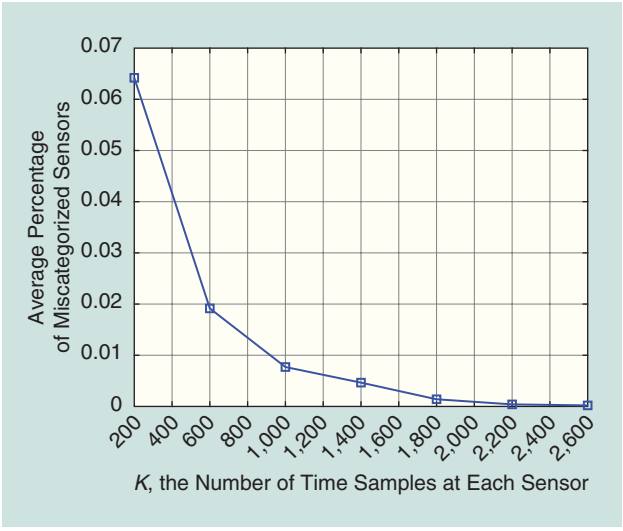

FIGURE 2. Identification and categorization of attacked sensors.

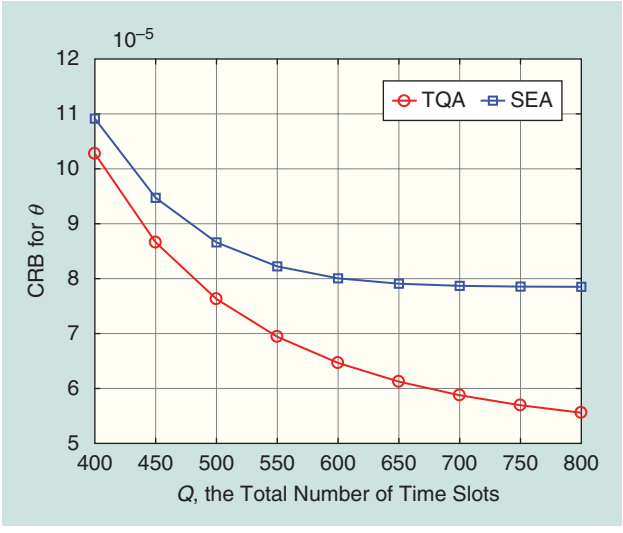

FIGURE 3. The CRB comparison between the TQA and the SEA.

respectively, and modify their observations with attack parameters $(\psi_{1,0}, \psi_{1,1}) = (0.2, 0.8)$ and $(\psi_{2,0}, \psi_{2,1}) = (0.7, 0.1)$. The parameter to be estimated is $\theta = 1$, the threshold of the quantizer in (2) is $\upsilon = 1$, $\Delta_0 = \Delta = 20\%$, and the additive noise obeys a standard normal distribution. In agreement with Theorem 1, Figure 2 depicts a 200-run Monte Carlo approximation of the average percentage of miscategorized sensors that appears to decrease toward zero as the number of time samples at each sensor increases.

Illustrative example: CRB comparison between the TQA and the SEA

Consider a network with $N = 100$ sensors, $\theta = 2$, and two different attacks. The first attack tampers with 25% of the sensors using attack parameters $\psi_{1,0} = 0.9$ and $\psi_{1,1} = 0.95$. The other attack controls 20% of the sensors while using the attack parameters $\psi_{2,0} = 0.15$ and $\psi_{2,1} = 0.2$. The length of each time slot is fixed at $K_t = 10$, and the set of 801 thresholds is $\mathfrak{T} = \{0, -0.125, 0.125, -0.250, 0.250, \ldots, -5, 5\}$. All other settings are similar to those of Figure 2. Figure 3 depicts the CRB when estimating θ for the two approaches with varying Q, the total number of time slots. For a given Q, each sensor observes QK_t time samples and picks the first Q thresholds from the set of thresholds $\mathfrak{T}$ to quantize the time samples in different time slots. It is seen that the CRBs for both approaches decrease as Q grows, which is reasonable since the number of time samples at each sensor increases. Moreover, Figure 3 illustrates that the TQA provides significant CRB performance gain when compared to the SEA, which implies that the set of thresholds leads to $\text{rank}(\Xi_p) = 3$ for at least one p based on Theorem 2, and the number of p for which this occurs increases with the increase in Q over the region shown.

Highly desirable spoofing attacks

In the previous section, we essentially described optimum processing of MiMA data for cases with a sufficiently large number of observations. We described how to find which sensors were attacked and how to develop groups of similarly attacked sensors. We also described how and when to use the data at the attacked sensors and when to not use these data. The method we proposed to use the attacked data involved estimating the attack parameters of a model describing the attack. With this model, we can follow accepted estimation theory to develop an estimation procedure using both the unattacked data and the attacked data. We could use, for example, an MLE procedure since we assume a large number of observations. Grouping together the similarly attacked data would help this procedure. We note that one could develop algorithms to automatically do the sensor grouping of similarly attacked sensors, determination of which sensors are unattacked, and MLE using an approach similar to that in [17]. Further, one can extend many of the ideas considered in this section to spoofing attacks; see [12].

In this section, besides considering spoofing attacks, we shift our considerations to find highly desirable attacks from the attacker's point of view. In particular, we are interested in attacks that will guarantee that the after-attack estimation performance must produce a CRB larger than some specified value, regardless of how the estimation system processes the data. To provide insight into spoofing attacks, vector-desired parameter estimation cases, arbitrary nonbinary quantization, and nonidentically distributed samples, we consider all of these in this section.

Let the after-attack unquantized observation $\tilde{x}_{jk}$ be a component of an independent sequence over $(j,k) \in \{1,\ldots,N\} \times \{1,\ldots,K\}$, and assume each $\tilde{x}_{jk}$ may be exposed to a spoofing attack to yield a pdf that can be expressed as

$$\tilde{x}_{jk} \sim \begin{cases} f_{jk}(\tilde{x}_{jk}|\boldsymbol{\theta}), & \text{if } j \in \mathcal{A}_0, \\ g_{jk}(\tilde{x}_{jk}|\boldsymbol{\theta}, \boldsymbol{\tau}^{(p)}), & \text{if } j \in \mathcal{A}_p. \end{cases} \tag{12}$$

The notations $\tilde{x}_{jk}$ and $\tilde{u}_{jk}$ denote the after-attack unquantized and quantized measurements regardless of whether the jth sensor is attacked or not, respectively. From (12), if $j \in \mathcal{A}_p$ for $p = 1,2,\ldots,P$, then the after-attack pdf $g_{jk}\left(x_{jk}|\boldsymbol{\theta}, \boldsymbol{\tau}^{(p)}\right)$ is parametrized by the desired vector parameter $\boldsymbol{\theta}$ with dimension $D_{\boldsymbol{\theta}}$ and the attack vector parameter $\boldsymbol{\tau}^{(p)}$ with dimension D_p.

To conform to previous work on spoofing attacks, the functional forms of the attacks, and equivalently $\{g_{jk}\}$, are assumed known to the attacked system, but the desired and attack vector parameters are not. All existing research considers cases in which the attacker replaces the unattacked sensor data by a function of the unattacked data, where the form of the function is known down to some unknown scalar quantities, which we call *attack parameters*. For example, a specific type of spoofing attack, called a *data-injection attack*, adds an unknown attack parameter to the sensor data. Thus, the function here is a linear function with unit slope, and the attack parameter is the value added to the sensor data.

Along with considering a vector desired parameter, this section generalizes the quantization model to allow nonbinary quantization. At the jth sensor, each after-attack measurement $\tilde{x}_{jk}$ is quantized to $\tilde{u}_{jk}$ by using an R_j-symbol quantizer with quantization regions $\{I_j^{(r)}\}_{r=1}^{R_j}$, that is,

$$\tilde{u}_{jk} = \sum_{r=1}^{R_j} \{\tilde{x}_{jk} \in I_j^{(r)}\} r, \tag{13}$$

where $\{\cdot\}$ is the indicator function. Let

$$\boldsymbol{\Theta} \triangleq [\boldsymbol{\theta}^T, (\boldsymbol{\tau}^{(1)})^T, \ldots, (\boldsymbol{\tau}^{(P)})^T]^T \tag{14}$$

denote a vector containing the unknown vector parameter $\boldsymbol{\theta}$ along with all of the unknown attack vector parameters that parametrize the spoofing attacks.

Optimal guaranteed degradation spoofing attack

Now we define a highly desirable attack.

Definition 1

Consider attacks imposing $\{f_{jk}(x_{jk}|\boldsymbol{\theta})\}$ and $\left\{g_{jk}\left(\tilde{x}_{jk}|\boldsymbol{\theta}, \boldsymbol{\tau}^{(p)}\right)\right\}$. The optimal guaranteed degradation spoofing attack (OGDSA) maximizes the degradation of the CRB for the vector parameter of interest at the FC when the attacked sensors are well identified and categorized according to distinct types of spoofing attacks by the FC. The CRB for the case where the attacked sensors are well identified and categorized provides a lower bound on the CRB for any case, including cases with unidentified and uncategorized attacked sensors, thus providing guaranteed sufficiently undesirable estimation performance for the estimation system and justifying the name. One class of attacks that are OGDSA are called *inestimable spoofing attacks* (*ISAs*), defined next and further illuminated by Theorem 3.

Definition 2 (Inestimable spoofing attack)

The pth spoofing attack is referred to as an *ISA* if the corresponding FIM for estimating $\boldsymbol{\tau}^{(p)}$ is singular. Such an attack can result from a sufficiently powerful attack relative to the number of quantization symbols employed by the quantizers as quantified by Theorem 3.

Theorem 3

For the pth spoofing attack, if the dimension D_p of the attack parameter $\boldsymbol{\tau}^{(p)}$ satisfies

$$D_p > \sum_{j \in \mathcal{A}_p} K(R_j - 1), \tag{15}$$

then the FIM for estimating $\boldsymbol{\tau}^{(p)}$ is singular, and, furthermore, the FIM for estimating $\boldsymbol{\Theta}$ is also singular.

Recall from the discussion just prior to Theorem 2 that the fixed threshold quantization approach fails for MIMAs due to a singular FIM. Theorem 3 shows that similar failures (certain FIMs become singular) can occur for spoofing attacks. The failures occur because the quantization approach produces data that cannot be used to estimate more parameters than the right-hand side of (15). Thus, if we form an attack that involves more attack parameters than the right-hand side of (15), then the FIM for estimating $\boldsymbol{\tau}^{(p)}$ is singular. To attack the estimation system and cause such a failure, one only needs to map the unattacked data through a function depending on all of the components of the attack parameter vector whose dimension is larger than the right-hand side of (15). A polynomial with coefficients that are the components of the attack parameter vector is one such function. Now, after quantization, an unbiased estimation approach is not capable of estimating the attack parameters to statistically model the attacked data (by modeling the function), so it cannot recover the desired parameter. The other possible class of OGDSAs, called *optimal estimable spoofing attacks* (*OESAs*), are a subset of estimable spoofing attacks (ESAs), defined next.

Definition 3 (ESA)

The pth OGDSA spoofing attack is said to be estimable if the corresponding FIM for estimating $\boldsymbol{\tau}^{(p)}$ is nonsingular. Reference [17] demonstrates that the attacked observations are useless for estimating the desired vector parameter under an OESA. Theorem 4 is useful for catagorizing ESAs.

Theorem 4

In the presence of ESAs, the CRB must satisfy

$$\mathrm{CRB}_{\mathrm{ESA}}(\boldsymbol{\theta}) \triangleq [\mathbf{J}_{\boldsymbol{\Theta}}^{-1}]_{1:D_{\boldsymbol{\theta}}} \preceq \mathbf{J}_{\mathcal{A}_0}^{-1}, \tag{16}$$

where $\mathbf{J}_{\boldsymbol{\Theta}}$ denotes the FIM for estimating $\boldsymbol{\Theta}$, and $[\mathbf{J}_{\boldsymbol{\Theta}}^{-1}]_{1:D_{\boldsymbol{\theta}}}$ is the $D_{\boldsymbol{\theta}}$-by-$D_{\boldsymbol{\theta}}$ leading principal minor of $\mathbf{J}_{\boldsymbol{\Theta}}$. The matrix $\mathbf{J}_{\mathcal{A}_0}$ is the FIM for estimating the desired vector parameter $\boldsymbol{\theta}$ by using only the data from $\mathcal{A}_0$.

In [17], necessary and sufficient conditions are provided for the equality in (16) that ultimately defines the class of OESAs for a given estimation problem. The necessary and sufficient conditions are provided in terms of a relationship between the subspaces spanned by the columns of certain matrices related to the FIMs for estimating $\boldsymbol{\theta}$ and $\boldsymbol{\tau}^{(p)}$ using data under the pth attack. One trivial example of an OESA, which may be relatively easy to detect, is to replace the original measurements at the attacked sensors by some regenerated data obeying a distribution not parametrized by $\boldsymbol{\theta}$. Nontrivial OESAs can also be given. For example, it is also shown in [17] that a generalization of an additive shift in $\boldsymbol{\theta}$, the attack thus replacing $\boldsymbol{\theta}$ by $\boldsymbol{\theta} + \boldsymbol{\tau}^{(p)}$, is always an OESA for any estimation problem. It is clear that such an attack is very hard for the estimation system to deal with since the unattacked estimation algorithm will be capable of estimating $\boldsymbol{\theta} + \boldsymbol{\tau}^{(p)}$, but it cannot resolve $\boldsymbol{\theta}$ and $\boldsymbol{\tau}^{(p)}$ since an uncountable number of choices for $\boldsymbol{\theta}$ and $\boldsymbol{\tau}^{(p)}$ will all lead to

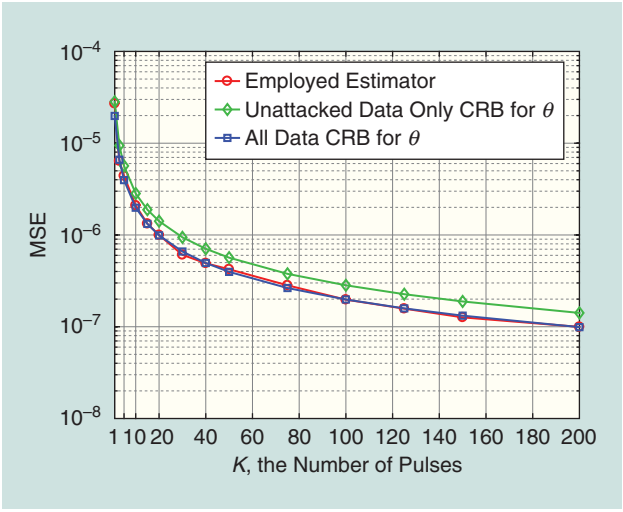

FIGURE 4. The attack performance of the data-injection attacks (non-OGDSA).

the same value of $\boldsymbol{\theta} + \boldsymbol{\tau}^{(p)}$. The estimation system has no way to choose the right one in this settling. On the other hand, other attacks, with different functional forms, can be OESAs for one estimation problem but not for another problem.

It is worth mentioning that, if sensors are correctly categorized, the CRB cannot be worse than the one that ignores the attacked sensors, so the attacked sensors can generally help in terms of reducing CRB. This explains (16) in an intuitive way. However, from the definitions of the ISA and OESA, the OGDSAs essentially make the data from the attacked sensors useless in terms of reducing CRB. Thus they give the equality in (16).

Illustrative example: Comparison between OGDSA and non-OGDSA for multiple-input, multiple-output (MIMO) radar

Previously, we explained how radars are being used in self-driving cars to avoid accidents in which humans and animals might be seriously hurt. Here, we give an example where a radar is spoofed. Consider a multiple-transmitter, multiple-receiver radar (often called a *MIMO radar)* with one transmit station and $N = 10$ receive stations. The first three receive stations are under spoofing attacks. Each station makes M measurements of each pulse in the pulse train and employs an identical 4-bit quantizer with a set of thresholds $\{-\infty, -5, -4, -3, ..., 8, 9, \infty\}$ to convert analog measurements to quantized data before transmitting them to the FC. Without any attack, the mth measurement of the kth pulse in the pulse train at the jth station can be expressed as

$$x_{jm}^{(k)} = \sqrt{E_j}\, a_j s(t_{jm}^{(k)} - \theta_j) + n_{jm}^{(k)}, \tag{17}$$

where θ_j is the desired parameter (delay of the transmitted signal after reflection from the radar target), $m = 1, 2, ..., M$, $k = 1, 2, ..., K$, and K is the total number of pulses in the pulse train. Assume $\{n_{jm}^{(k)}\}$ is an independent and identically distributed zero-mean Gaussian noise sequence with variance $\sigma^2 = 5$. The signal $s(t)$ is a Gaussian pulse signal [31], that is, $s(t) = (2/T^2)^{1/4} \exp(-\pi t^2/T^2)$, and the sampling times are $t_{jm}^{(k)} = (m-1)\,\Delta t, \forall m = 1, 2, ..., M$. To simplify the model, we assume that the distance between the target and any receiving station is much larger than the distances between every pair of receive stations, and, hence, we can assume that $\theta_j = \theta$ for all j. We set the quantities $T = 0.1$, $\Delta t = 0.001, \theta = 0.02$, and $E_j = 1, a_j = 1$ for all j.

First, we consider the attack performance of a non-OGDSA for this estimation problem, called a *data-injection attack*. If the jth station is under a data-injection attack for $j = 1, 2, 3$, the mth after-attack measurement of the kth pulse in the pulse train is given by

$$\tilde{x}_{jm}^{(k)} = \sqrt{E_j}\, a_j s(t_{jm}^{(k)} - \theta_j) + \xi_j + n_{jm}^{(k)}, \tag{18}$$

where the attack parameters are $\xi_1 = 1$, $\xi_2 = -2$, and $\xi_3 = -1$. We employ an expectation-maximum-based joint attack identification and parameter estimation approach proposed in [17] to estimate the desired parameter θ. Figure 4 depicts the MSE performance of the employed estimator plotted on a log scale, where $M = 40$. The clairvoyant CRB for estimating θ, which knows which sensors are attacked and uses data from all sensors, is also plotted in Figure 4 along with the CRB for estimating θ, which uses data only from unattacked sensors. Figure 4 shows that the CRB that uses only the unattacked sensor data is strictly larger than the CRB that uses all the data, which implies that the attacked data are useful for reducing the CRB. As expected, the data-injection attack does not make the attacked data useless for reducing the CRB as opposed to an OGDSA. Moreover, the employed estimation approach can outperform the CRB that uses only the unattacked data and asymptotically achieves the clairvoyant CRB that uses all sensor data.

Next, we consider another spoofing attack, called a *delay attack,* which is a shift-in-parameter OESA (previously discussed and mentioned after Theorem 4). This attack alters the delay in the received signal, possibly by employing DRFM along with a receiver/transmitter [17] to transmit the signal back toward the receive antennas with an arbitrary delay chosen by the attacker. For the jth station, which is under a delay attack for $j = 1, 2, 3$, the mth after-attack measurement of the kth pulse in the pulse train is given by

$$\tilde{x}_{jm}^{(k)} = \sqrt{E_j}\, a_j s(t_{jm}^{(k)} - \theta_j - \xi_j) + n_{jm}^{(k)}, \tag{19}$$

where ξ_j is the delay introduced by the delay attack. It can be shown that the delay attack in (19) is an OGDSA [17], which is also an OESA. In Figure 5, the simulation setting is the same as that in Figure 4, except $M = 3$ and the attack parameters are $\xi_1 = 0.04$, $\xi_2 = 0.05$, and $\xi_3 = 0.06$. We employ the same estimation approach as that employed in Figure 4. Figure 5 illustrates the MSE performance of the employed estimator along with the CRB for θ, which knows which sensors are attacked and uses data only from unattacked sensors. It is worth mentioning that the employed approach can perfectly identify the attacked sensors with large K [17], and it is seen that the MSE performance of the employed estimator converges to the CRB using only unattacked data. Most importantly, the large K results in Figure 5 agree with the previously stated theoretical

results saying the attacked data are not useful in reducing the CRB under an OGDSA.

General attacks in vector parameter estimation systems

In the sections "MiMAs" and "Highly Desirable Spoofing Attacks," we considered MiMAs and spoofing attacks separately. In this section, we consider the most general attacks, which include combinations of MiMAs and spoofing attacks, when estimating the location of an acoustic emitter [6] at $\boldsymbol{\zeta}_{\mathrm{T}} = [y_{\mathrm{T}}, z_{\mathrm{T}}]$, where y_{T} and z_{T} denote the coordinates of the emitter location in the two-dimensional plane. We assume that the emitter is in some region of interest (ROI) $\mathcal{S}$. For the jth sensor, we use $\boldsymbol{\zeta}_j = [y_j, z_j]$ to denote its location. In addition to N insecure sensors, the estimation system has access to two secure sensors, considered the $(N+1)$th and $(N+2)$th sensors, respectively. These two secure sensors are well protected and thereby are guaranteed to be unattacked, while the other N sensors are open to attacks. We assume that the signal radiated from the emitter obeys an isotropic power attenuation model [6] and each sensor observes K data samples. The kth data sample at the jth sensor is described as $x_{jk} = P_0(D_0/D_j)^{\gamma} + n_{jk}$, $j = 1,2,\ldots,N+2$, where the distance D_j between the jth sensor and the emitter is defined by $D_j \triangleq \|\boldsymbol{\zeta}_j - \boldsymbol{\zeta}_{\mathrm{T}}\| = \sqrt{(y_j - y_{\mathrm{T}})^2 + (z_j - z_{\mathrm{T}})^2}, \forall j$, the quantity P_0 is the power measured at a reference distance D_0, γ is the path-loss exponent that is a positive constant, and n_{jk} denotes the additive noise sample with pdf $f_j(n_{jk})$. We assume that P_0, D_0, γ, $\{f_j(\cdot)\}_{j=1}^{N+2}$, and $\{\boldsymbol{\zeta}_j\}_{j=1}^{N+2}$ are known to the FC. Moreover, we assume $\{n_{jk}\}$ are independent and, for each j, $\{n_{jk}\}_{k=1}^{K}$ is an identically distributed sequence.

Each sensor j quantizes its sample x_{jk} to one-bit data u_{jk} by using the threshold ν_j, and then transmits u_{jk} to the FC, that is, $u_{jk} \triangleq \{x_{jk} \in (\nu_j, \infty)\}, \forall j$ and $\forall k$, where $\{\cdot\}$ is the indicator function. We assume that the thresholds $\{\nu_j\}_{j=1}^{N+2}$ are known to the FC.

If $j \in \mathcal{A}_p$ for some $p \geq 1$, the after-attack quantized data can be generally expressed as $\tilde{u}_{jk} = \tilde{h}_{jk}(\{h_{jk}(x_{jk}) \in (\nu_j, \infty)\})$, where the maps $h_{jk}(\cdot)$ and $\tilde{h}_{jk}(\cdot)$ represent the effects of the spoofing attack and the MiMA at time k, respectively. Similar to (2), the NMLE of the distance D_j can be expressed as

$$\hat{D}_j^{(K)} = D_0 P_0^{\frac{1}{\gamma}} \left[\nu_j - F_j^{-1}\left(\frac{1}{K} \sum_{k=1}^{K} (1 - \tilde{u}_{jk}) \right) \right]^{-\frac{1}{\gamma}}, \tag{20}$$

which yields that, for the two secure sensors, that is, the $(N+1)$th and $(N+2)$th sensors, we have

$$\hat{D}_{N+1}^{(K)} \to D_{N+1} \text{ and } \hat{D}_{N+2}^{(K)} \to D_{N+2} \text{ almost surely, as } K \to \infty, \tag{21}$$

since $\tilde{u}_{jk} = u_{jk}$ for $j = N+1$ and $N+2$. Based on this fact, we can generate two circles that are centered at the $(N+1)$th and $(N+2)$th sensors with radii equal to $\hat{D}_{N+1}^{(K)}$ and $\hat{D}_{N+2}^{(K)}$, respectively. In the asymptotic regime, where $K \to \infty$, the intersection point of these two circles pinpoints the location of the emitter

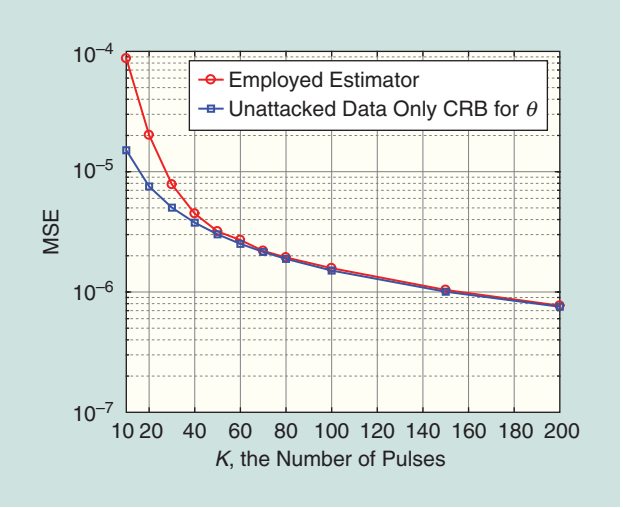

FIGURE 5. The attack performance of the DRFM attacks (OGDSA).

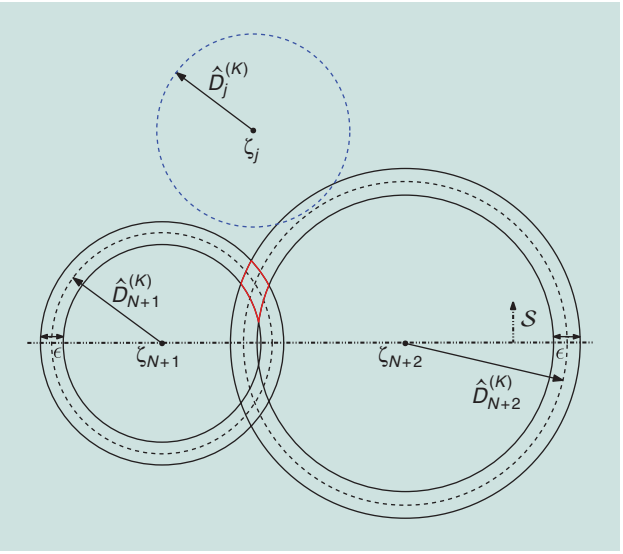

FIGURE 6. A geometric illustration of the proposed detectors.

under the assumption that the ROI $\mathcal{S}$ is contained in one of the two half spaces produced by dividing the whole space by the line passing through the two secure sensors. Similarly, if the jth sensor is unattacked (attacked), the circle centered at the jth sensor with radius equal to $\hat{D}_j^{(K)}$ should (should not) pass through this intersection point in the asymptotic regime where $K \to \infty$. Thus, we can determine whether the jth sensor is attacked or not by checking this geometric consistency among the circles associated with the two secure sensors and the jth sensor in the asymptotic regime where $K \to \infty$.

In the regime where K is finite, the attack-detection procedure is similar except that, for each of the two secure sensors, the associated circle is replaced by a ring with some constant width ε; see Figure 6. We declare that the jth sensor is unattacked (attacked) if the circle (the blue dashed circle in Figure 6) associated with the jth sensor passes (does not pass) through the overlap area (the area enclosed by the red curves in Figure 6) of the rings associated with the two secure sensors. In the exact situation in

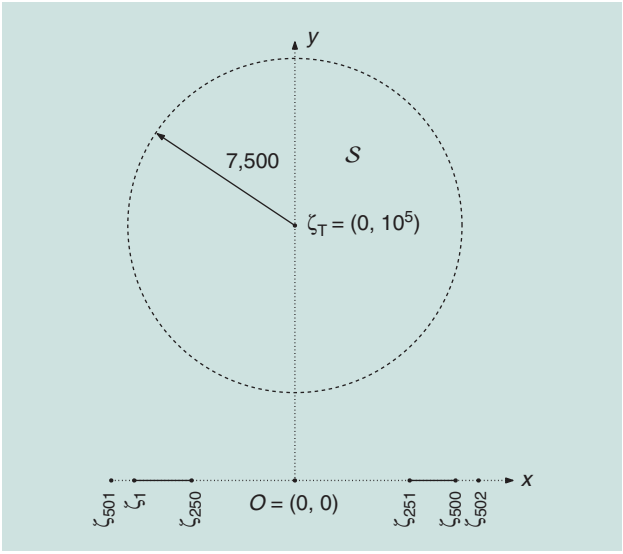

FIGURE 7. The simulation configuration.

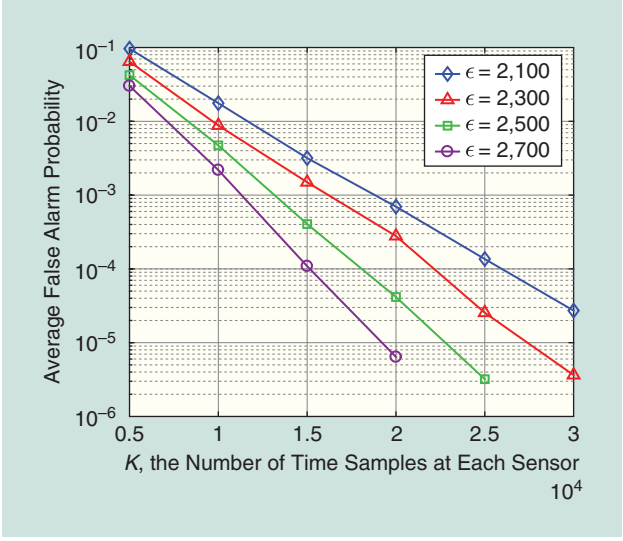

FIGURE 8. The false alarm probability for different ϵ.

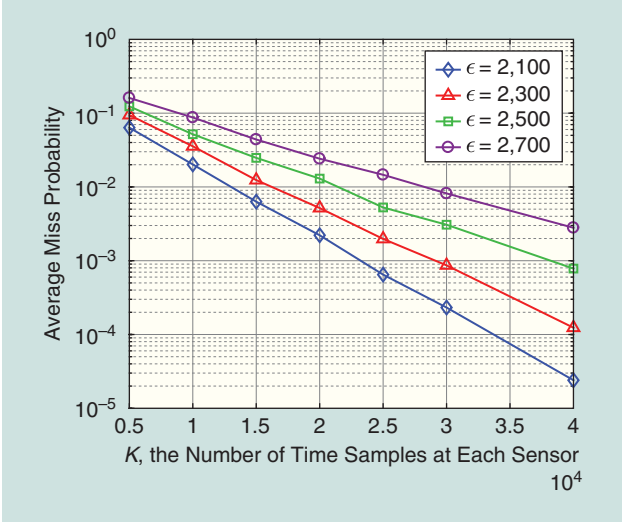

FIGURE 9. The miss probability for different ϵ.

Figure 6, we would declare an attack. The mathematical formulation of this attack-detection idea can be found in [12].

By employing large deviations principles, we derive the following theorem regarding the performance of the proposed detectors.

Theorem 5

If widths of the rings associated with the two secure sensors are smaller than C_0, where C_0 is a constant defined in [12], then the false alarm and miss probabilities are upper bounded by two exponentially decaying functions of K, respectively. The rates of decay can also be found in [12].

The idea of detecting attacks in this emitter localization problem can be generalized to the general IoT sensor network estimation problem equipped with secure sensors. In particular, we can employ the data from the secure sensors to generate some constraints that are satisfied by the desired parameters with high probability (that the desired parameters must lie in the overlap of two rings for the just-described localization example was one such constraint). Then we can detect whether or not each insecure sensor is attacked by checking whether or not the NMLE based on the data from the sensor satisfies the constraints.

Illustrative example: Proposed detector for general attacks

To illustrate Theorem 5, we test the performance of the proposed detector for an example case. The system configuration is illustrated in Figure 7. Consider a network consisting of two groups of sensors with $N = 500$. The two secure sensors are located at $\boldsymbol{\zeta}_{501} = (-10^3, 0)$ and $\boldsymbol{\zeta}_{502} = (10^3, 0)$, respectively. The rest of the sensors are all located along the x-axis and are partitioned into two groups. In the first group, the sensors $\{1, 2, ..., 250, 501\}$ are evenly spaced between $(-10^3, 0)$ and $(-0.9 \times 10^3, 0)$, while sensors in second group $\{251, 252, ..., 500, 502\}$ are evenly spaced between $(0.9 \times 10^3, 0)$ and $(10^3, 0)$. The ROI $\mathcal{S}$ is a disc centered at $(0, 10^5)$ and with radius equal to 7,500. The emitter is located at $\boldsymbol{\zeta}_T = (0, 10^5)$. We assume that $P_0 = 1$, $D_0 = 10^5$, and $\gamma = 2$. The thresholds $\nu_j = 1$ for all j and n_{jk} follow a Gaussian distribution with zero mean and unit variance. We assume that 250 sensors $\{1, 2, ..., 250\}$ are under a MiMA as described in (3) with $\psi_{j,0} = 0$ and $\psi_{j,1} = 0.94$ for $j = 1, 2, ..., 250$. The rest of the sensors are unattacked.

The average false alarm and miss probabilities versus K are depicted on a log scale in Figures 8 and 9 for four detectors with $\epsilon = 2,100; 2,300; 2,500;$ and $2,700$, respectively. Figures 8 and 9 show that, for each detector, the average false alarm and miss probabilities decrease exponentially as K grows, which agrees with the theoretical results in Theorem 5. Moreover, as illustrated in Figure 8, the larger the value of ϵ, the smaller the average false alarm probability. On the other hand, Figure 9 shows that the larger the value of ϵ, the larger the average miss probability. Thus, the proper tradeoff between the false alarm and miss probabilities can be chosen by adjusting the value of ϵ.

Implications for unattacked systems

Motivated by Theorem 3, a fundamental limitation on quantized estimation systems not under attack is uncovered. Before

proceeding, we first provide two definitions on the identifiability of a vector parameter point and a vector parameter space. Let $\boldsymbol{\Omega} \subseteq \mathbb{R}^{D_{\boldsymbol{\theta}}}$ denote the parameter space of interest with a nonempty interior.

Definition 4 (Identifiable vector parameter point)

The vector parameter point $\boldsymbol{\theta} \in \boldsymbol{\Omega}$ is called identifiable if the conditional distribution of the data conditioned on $\boldsymbol{\theta}$ is not identical to that for any other vector parameter point in $\boldsymbol{\Omega}$.

Definition 5 (Identifiable vector parameter space)

The vector parameter space $\boldsymbol{\Omega}$ is considered identifiable if every vector parameter point in $\boldsymbol{\Omega}$ is identifiable.

Under some mild assumptions [32], we can derive Theorem 6 on the fundamental limitation of quantized estimation systems.

Theorem 6

Let $D_{\boldsymbol{\theta}}$ be the dimension of a vector parameter in $\boldsymbol{\Omega}$ we want to estimate from L independent observations quantized using Q distinct quantizer designs with R_j, $j = 1, 2, \ldots, Q$ symbols. Assume the jth group of observations, all quantized by an identical quantizer, are generated from M_j different pdfs. If

$$D_{\boldsymbol{\theta}} > \sum_{j=1}^{Q} M_j(R_j - 1), \tag{22}$$

then the FIM is singular, and, moreover, the vector parameter space $\boldsymbol{\Omega}$ is not identifiable.

In addition, for any open subset $O \subseteq \boldsymbol{\Omega}$ in $\mathbb{R}^{D_{\boldsymbol{\theta}}}$, there are infinitely many vector parameter points in O that are not identifiable.

For identical $(Q = 1)$ binary $(R_j = 1)$ quantization at each sensor and identically distributed observations $(M_1 = 1)$ at each sensor, $\Sigma_{j=1}^{Q} M_j(R_j - 1) = 1$, so a scalar parameter $(D_\theta = 1)$ alone will not satisfy the sufficient condition in (22) for FIM singularity in this case. Note that we have already given just such an example in the section "MiMAs" $(\Sigma_{j=1}^{Q} M_j(R_j - 1) = 1)$ in the discussion just prior to Theorem 2, where the fixed threshold quantization approach worked well (no singular FIM) when there was no attack, since we were estimating a scalar parameter θ. However, the approach failed (singular FIM) with the attack since the parameter to estimate had dimension three and, yet, the right-hand side of (22) is exactly one.

Note that the quantity $\Sigma_{j=1}^{Q} M_j(R_j - 1)$ does not depend on the quantization regions, the number L of observations, the pdfs that generate the observations, or the particular estimation problem but instead depends only on the number of different pdfs involved, the number of quantizers employed, and the number of quantization symbols. This critical quantity is referred to as the *IDQD*.

Theorem 6 reveals a fundamental limitation when utilizing quantized data for estimating a vector parameter and sheds light on the preliminary design of a quantized estimation system. To be specific, the quantization and sensing approach employed should guarantee that the IDQD of the quantized estimation system is larger than or equal to the dimension of the vector parameter of interest. For some specific estimation problems, the singularity of the FIM and the nonidentifiability of the parameter space can exist even if the condition in (22) does not hold.

In some cases, where $D_{\boldsymbol{\theta}}$ is larger than the IDQD, all vector parameter points in $\boldsymbol{\Omega}$ are nonidentifiable, while in some other cases, there exist some parameter points in $\boldsymbol{\Omega}$ that are identifiable. Thus, a singular FIM does not necessarily determine the nonidentifiability of the parameter point though it does determine the nonidentifiability of the parameter space. Moreover, it can be shown that, if $D_{\boldsymbol{\theta}}$ is larger than the IDQD, the cardinality of a set of parameter points such that the conditional distribution of the data conditioned on the parameter is identical to that for some other parameter point can be as small as one and can also be uncountably infinite. Generalized results that do not require some assumptions in Theorem 6, e.g., independence, can be found in [32].

Some recent work on related protection layers employing signal processing

Many IoT applications, for example, smart grid and manufacturing, require sensor data to be sent from one location to a different location so the data can be used to change a control or reconfigure the grid or manufacturing process. To provide the low latency required to avoid unstable control loops, low-complexity encryption approaches have received attention for estimation using sensor data in the IoT. An interesting low-complexity approach to encrypt binary quantized data was suggested in [33], which is called *stochastic encryption*. The basic idea is to flip the binary data using an approach similar to our attack model in (4). Then the desired user, who knows the flipping probabilities, will use a maximum likelihood decoding approach to estimate the desired parameter, θ, in (1). The estimation performance loss due to not knowing how each bit was flipped but knowing only the flipping probabilities is shown to be small in [33] with proper design.

It is also shown in [33] that any eavesdroppers will have very poor estimation performance for properly chosen flipping probabilities. The flipping probabilities act as an encryption key for a very low-complexity encryption process that is suitable for a low-complexity sensor node. Using Theorem 6, we have shown [34] that the approach in [33] can only estimate a scalar parameter, so in [34] and [35], we generalized the approach by using different quantizers and flipping probabilities at each sensor, which can also employ nonbinary quantization. Based on Theorem 6, such approaches can be designed to potentially estimate vector parameters of any size while retaining the advantages of the approach suggested in [33]. Now, one might think that, after observing a sufficiently large window of data, an eavesdropper might be able to estimate the flipping probabilities and break the code to estimate the parameter of interest. In [34], we show this is not possible if the eavesdropper employed an unbiased estimator based on Theorem 6. The quantization approach is not of sufficient complexity to allow the eavesdropper to estimate all the quantities needed for him or her to develop an accurate estimate of the parameter of interest.

Stochastic encryption was also considered for defending against eavesdroppers in the context of sequential hypothesis

testing in [36]. Since the flipping probabilities are known only to the desired user but not to the eavesdropper, the desired user employs the optimal sequential probability ratio test (SPRT) for sequential detection, whereas the eavesdropper employs a mismatched SPRT. However, every stochastic encryption degrades the performance of the SPRT at the desired user by increasing the expected sample size. In [36], an optimal stochastic encryption is obtained analytically in the sense of maximizing the difference between the expected sample sizes required at the eavesdropper and the desired user, provided that the acceptable tolerance of the increase in the expected sample size at the desired user induced by the stochastic encryption is small enough.

We next describe a technology based on information theory that can provide additional layers of protection that has received recent attention. All communications networks are designed using layers that are different than the security layers we mentioned previously. The lowest layer of a communication network is the physical layer. Most currently employed security procedures are implemented in the network or higher layers, which are a few layers above the physical layer. Since one can do things at the physical layer that cannot be done at the higher layers, the idea of physical layer security seems very attractive. Using physical layer security for the right situations, one can design signals that ensure a required information rate is received by the desired user, but the rates received by the eavesdropper are guaranteed to be less than some small value. Such results exploit information-theoretic ideas and have been called *information-theoretic secrecy*.

The seminal work of Shannon [37] and Wyner [38] laid the foundation for physical layer security, by providing basic formalisms for security in cipher systems and wiretap channels, respectively. Csiszár and Körner generalized Wyner's work to the broadcast channel with confidential messages in [39], which provides a model that aids in the understanding of security in wireless systems. Excellent surveys on physical layer security can be found in [40]–[42]. Authentication, a counterpart of secrecy, has also been given a physical layer security treatment. The study of authentication in an information-theoretic context began with [43] and was extended to the physical layer by Lai et al. in [44]. Besides the information-theoretic investigations, much work has also been done with authentication at the physical layer with practical schemes that utilize the characteristics of the channel and the communication devices to uniquely identify sources. A survey on this topic can be found in [45], and practical methods for wireless authentication utilizing fingerprint embedding at the physical layer can be found in [46] and [47].

Conclusions

In this article, the estimation of an unknown deterministic scalar parameter in the presence of MiMAs has been introduced first. The capability of the IoT systems, in terms of identifying and categorizing the attacked sensors into different groups according to distinct types of attacks, has been outlined in the face of MiMAs. Necessary and sufficient conditions have been provided under which utilizing the attacked sensor data will lead to a more favorable CRB when compared to approaches where the attacked sensors are ignored. Next, necessary and sufficient conditions have been provided under which spoofing attacks provide a guaranteed attack performance in terms of the CRB for estimating a deterministic parameter vector regardless of the processing the estimation system employs. It has been shown that it is always possible to construct such a highly desirable attack by properly employing an attack vector parameter having a sufficiently large dimension relative to the number of quantization symbols employed, which had not been observed previously. In addition, the most general attacks, which include combinations of MiMAs and spoofing attacks, have been considered in an emitter localization system. Attack detectors have been proposed whose false alarm and miss probabilities decrease exponentially as the number of measurement samples increases. For unattacked quantized estimation systems, a general limitation on the dimension of a vector parameter that can be accurately estimated has been uncovered. References that provide various extensions to all of the specific results presented in this article have been supplied, and a brief discussion of low-complexity encryption and physical layer security has been provided.

Acknowledgments

We would like to thank Jake Perazzone for his helpful discussions on physical layer security. This material is based upon work partially supported by the U.S. Army Research Laboratory and the U.S. Army Research Office under grant number W911NF-17-1-0331 and by the National Science Foundation under grants ECCS-1647198, ECCS-1744129, CNS-1702555, and CNS-1702808.

Authors

Jiangfan Zhang (jz2833@columbia.edu) received the B.Eng. degree in communication engineering from Huazhong University of Science and Technology, Wuhan, China, in 2008, the M.Eng. degree in information and communication engineering from Zhejiang University, Hangzhou, China, 2011, and the Ph.D. degree in electrical engineering from Lehigh University, Bethlehem, Pennsylvania, in 2016. He is currently a postdoctoral research scientist in the Department of Electrical Engineering at Columbia University, New York. He is a recipient of the Dean's Doctoral Student Assistantship, Gotshall Fellowship, and a P.C. Rossin Doctoral Fellow at Lehigh University.

Rick S. Blum (rblum@lehigh.edu) is the Robert W. Wieseman Professor of Electrical Engineering at Lehigh University, Bethlehem, Pennsylvania. His research interests include signal processing/machine learning for cybersecurity, smart grid, communications, sensor networking, radar, and sensor processing. He is a Fellow of the IEEE, an IEEE Signal Processing Society Distinguished Lecturer, an IEEE Third Millennium Medal winner, and a member of Eta Kappa Nu and Sigma Xi, and he holds several patents. He was awarded an Office of Naval Research Young Investigator Award and a National Science Foundation Research Initiation Award. He was an associate editor of several IEEE transactions and special issues.

H. Vincent Poor (poor@princeton.edu) is the Michael Henry Strater University Professor of Electrical Engineering

at Princeton University, New Jersey. His interests include information theory and signal processing, with applications in wireless networks, energy systems, and related fields. He is an IEEE Fellow, a member of the U.S. National Academy of Engineering and the U.S. National Academy of Sciences, and a foreign member of the Chinese Academy of Sciences and the Royal Society. He received the Technical Achievement and Society Awards of the IEEE Signal Processing Society in 2007 and 2011, respectively. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal and a D.Sc. *honoris causa* from Syracuse University, also in 2017.

References

[1] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[2] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci.*, vol. 114, no. 1, pp. 19–26, 2017.

[3] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of Byzantine attacks," *IEEE Trans. Signal Process.*, vol. 57, no. 1, pp. 16–29, 2009.

[4] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, 2011.

[5] X. He, H. Dai, and P. Ning, "A Byzantine attack defender in cognitive radio networks: The conditional frequency check," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2512–2523, 2013.

[6] A. Vempaty, O. Ozdemir, K. Agrawal, H. Chen, and P. Varshney, "Localization in wireless sensor networks: Byzantines and mitigation techniques," *IEEE Trans. Signal Processing*, vol. 61, no. 6, pp. 1495–1508, Mar. 2013.

[7] A. Vempaty, L. Tong, and P. Varshney, "Distributed inference with Byzantine data: State-of-the-art review on data falsification attacks," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 65–75, 2013.

[8] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, "Distributed detection in tree topologies with Byzantines," *IEEE Trans. Signal Process.*, vol. 62, no. 12, pp. 3208–3219, 2014.

[9] B. Kailkhura, V. S. S. Nadendla, and P. K. Varshney, "Distributed inference in the presence of eavesdroppers: A survey," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 40–46, 2015.

[10] J. Zhang, R. S. Blum, X. Lu, and D. Conus, "Asymptotically optimum distributed estimation in the presence of attacks," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1086–1101, Mar. 2015.

[11] B. Alnajjab, J. Zhang, and R. S. Blum, "Attacks on sensor network parameter estimation with quantization: Performance and asymptotically optimum processing," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6659–6672, Dec. 2015.

[12] J. Zhang, X. Wang, R. S. Blum, and L. M. Kaplan, "Attack detection in sensor network target localization systems with quantized data," *IEEE Trans. Signal Process.*, vol. 66, no. 8, pp. 2070–2085, Apr. 2018.

[13] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[15] 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," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, 2012.

[16] D. He, S. Chan, and M. Guizani, "Cyber security analysis and protection of wireless sensor networks for smart grid monitoring," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 98–103, Dec. 2017.

[17] J. Zhang, R. S. Blum, L. M. Kaplan, and X. Lu, "Functional forms of optimum spoofing attacks for vector parameter estimation in quantized sensor networks," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 705–720, 2017.

[18] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proc. 4th Int. Symp. Information Processing Sensor Networks,* Apr. 2005, pp. 91–98.

[19] J. H. Lee and R. Buehrer, "Characterization and detection of location spoofing attacks," *J. Commun. Netw.*, vol. 14, no. 4, pp. 396–409, Aug. 2012.

[20] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," in *Proc. IEEE Conf. Communications and Network Security,* 2016, pp. 391–395.

[21] C. Wilson and V. Veeravalli, "MMSE estimation in a sensor network in the presence of an adversary," in *Proc. IEEE Int. Symp. Information Theory,* 2016, pp. 2479–2483.

[22] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things," *IEEE Power Electron. Mag.*, vol. 4, no. 4, pp. 37–43, Dec. 2017.

[23] V. Nadendla, Y. S. Han, and P. K. Varshney, "Distributed inference with M-ary quantized data in the presence of Byzantine attacks," *IEEE Trans. Signal Process.*, vol. 62, no. 10, pp. 2681–2695, 2014.

[24] Y. Zhao, A. Goldsmith, and H. V. Poor, "Minimum sparsity of unobservable power network attacks," *IEEE Trans. Autom. Control*, vol. 62, no. 7, pp. 3354–3368, 2017.

[25] A. Vempaty, K. Agrawal, H. Chen, and P. Varshney, "Adaptive learning of Byzantines' behavior in cooperative spectrum sensing," in *Proc. IEEE Wireless Communications and Networking Conf.,* 2011, pp. 1310–1315.

[26] D. Liu, P. Ning, A. Liu, C. Wang, and W. K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Trans. Inf. Syst. Security*, vol. 11, no. 4, p. 22, 2008.

[27] E. Bland. (2008). GPS 'spoofing' could threaten national security. [Online]. Available: http://www.nbcnews.com/id/26992456

[28] A. Couts. (2013). Want to see this $80 million super yacht sink? With GPS spoofing, now you can! [Online]. Available: http://www.digitaltrends.com/mobile/gps-spoofing/

[29] M. I. Skolnik, *Introduction to Radar Systems*, 2nd ed. New York: McGraw Hill Book Co., 1980.

[30] S. Roome, "Digital radio frequency memory," *Electron. Commun. Eng. J.*, vol. 2, no. 4, pp. 147–153, Aug. 1990.

[31] Q. He, R. S. Blum, and A. M. Haimovich, "Noncoherent MIMO radar for location and velocity estimation: More antennas means better performance," *IEEE Trans. Signal Process.*, vol. 58, no. 7, pp. 3661–3680, 2010.

[32] J. Zhang, R. S. Blum, L. Kaplan, and X. Lu, "A fundamental limitation on maximum parameter dimension for accurate estimation with quantized data," arXiv Preprint, arXiv:1605.07679, 2016.

[33] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 273–289, 2008.

[34] A. N. Samudrala and R. S. Blum, "On the estimation and secrecy capabilities of stochastic encryption for parameter estimation in IOT," in *Proc. IEEE Annu. Conf. Information Science and Systems*, 2018, pp. 1–6.

[35] A. N. Samudrala and R. S. Blum, "Asymptotic analysis of a new low complexity encryption approach for the Internet of Things, smart cities and smart grid," in *Proc. IEEE Int. Conf. Smart Grid and Smart Cities*, 2017, pp. 200–204.

[36] J. Zhang and X. Wang, "Asymptotically optimal stochastic encryption for quantized sequential detection in the presence of eavesdroppers," arXiv Preprint, arXiv:1703.02141, 2017.

[37] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[38] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[39] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[40] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci.*, vol. 114, no. 1, pp. 19–26, 2017.

[41] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[42] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering.* Cambridge, U.K.: Cambridge Univ. Press, 2011.

[43] G. J. Simmons, "Authentication theory/coding theory," in *Proc. Workshop Theory and Application Cryptographic Techniques*, 1984, pp. 411–431.

[44] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 906–916, 2009.

[45] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, pp. 56–62, Oct. 2010.

[46] J. B. Perazzone, P. L. Yu, B. M. Sadler and R. S. Blum, "Cryptographic side-channel signaling and authentication via fingerprint embedding," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2216–2225, Sept. 2018.

[47] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen and H. V. Poor, "Authenticating users using fine-grained channel information," *IEEE Trans. Mobile Comput.*, vol. 17, no. 2, pp. 251–264, 2018.

SP