Attack Detection in Sensor Network Target Localization Systems With Quantized Data

Jiangfan Zhang, *Member, IEEE*, Xiaodong Wang, *Fellow, IEEE*, Rick S. Blum, *Fellow, IEEE*, and Lance M. Kaplan, *Fellow, IEEE*

***Abstract*—We consider a sensor network focused on target localization, where sensors measure the signal strength emitted from the target. Each measurement is quantized to one bit and sent to the fusion center. A general attack is considered at some sensors that attempts to cause the fusion center to produce an inaccurate estimation of the target location. The attack is a combination of man-in-the-middle, hacking, and spoofing attacks that can effectively change both signals going into and coming out of the sensor nodes in a realistic manner. We show that the essential effect of attacks is to alter the naive estimate of the distance between the target and each attacked sensor, which ignores the existence of attacks, to a different extent, giving rise to a geometric inconsistency among the attacked and unattacked sensors. With the help of two secure sensors, a class of detectors are proposed to detect the attacked sensors by scrutinizing the existence of the geometric inconsistency. We show that the false alarm and miss probabilities of the proposed detectors decrease exponentially as the number of measurement samples increases, which implies that with sufficient measurement samples, the proposed detectors can identify the attacked and unattacked sensors with any required accuracy. Numerical results show that compared to the cases where all sensors are employed without detecting attacks or only the secure sensors are employed, the localization performance can be significantly improved if we employ the secure sensors and the sensors which are declared as unattacked by the proposed detector.**

***Index Terms*—Target localization, attack detection, spoofing attack, man-in-the-middle attack, malfunction, sensor network, large deviations theory.**

I. Introduction

Sensor networks find wide applications ranging from inexpensive commercial systems to complex military and homeland defense surveillance systems and have seen ever growing interest in recent years [1]. One important application of sensor networks is to estimate the location of a target in a region of interest (ROI) [2]–[4]. Recent technological advances in digital wireless communications and digital electronics have led to the dominance of digital transmission and processing using quantized data in such systems. Hence, a great deal of attention has focused on target localization in sensor networks using quantized data, see [5]–[7] for instance.

Typically, large-scale sensor networks are comprised of low-cost and spatially distributed sensor nodes with limited battery capacity and low computing power, which makes the system vulnerable to cyberattacks by adversaries. This has led to a vast interest in studying the vulnerability of sensor networks in various applications and from different perspectives, see [8]–[15] and the references therein. Depending on the place where the attack is launched, there are generally three categories of attacks in sensor networks, namely spoofing attacks, hacking attacks, and man-in-the-middle attacks (MiMA). To be specific, the spoofing attack changes the phenomenon observed by the attacked sensors and tampers with the observations coming into the sensors. For example, data-injection attack is one type of spoofing attack [10]. The hacking attack aims at hacking into the sensors, modifying the hardware, and/or reprogramming the devices, with the goal of disrupting the data processing in the attacked sensors. Note that malfunctions of sensors can also be considered as hacking attacks. The MiMA takes place between the sensors and a fusion center (FC), which maliciously falsifies the data transmitted from the attacked sensors to the FC, see [7], [11], [12] for instance. The main goal of the adversaries is to undermine the sensor network and render the FC to reach an inaccurate estimate of the target location in terms of large mean-square estimation error. A simple and intuitive method to combat the attacks is to identify the attacked sensors so that the FC can either discard data from these sensors, or make use of attacked data to improve its estimate of the target location via jointly estimating the target location and the attacks [11], [12], [15].

A. *Summary of Results and Main Contributions*

In this paper, we consider a sensor network containing two widely separated secure sensors which have a very high level of security and thereby are guaranteed to be tamper-proof. The rest of sensors are insecure, which are subject to arbitrary forms of attacks. In practice, the two secure sensors can be well protected,

Manuscript received May 15, 2017; revised October 2, 2017 and December 20, 2017; accepted January 15, 2018. Date of publication February 5, 2018; date of current version March 8, 2018. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Wee Peng Tay. This work was supported in part by the U.S. National Science Foundation (NSF) under Grant CIF1064575, in part by the U.S. Office of Naval Research under Grant N000141410667, in part by the U.S. Army Research Laboratory and the U.S. Army Research Office under Grant W911NF-17-1-0331, and in part by the NSF under Grants ECCS-1744129 and CNS-1702555. *(Corresponding author: Xiaodong Wang.)*

J. Zhang and X. Wang are with the Department of Electrical Engineering, Columbia University in the City of New York, New York, NY 10027 USA (e-mail: jz2833@columbia.edu; wangx@ee.columbia.edu).

R. S. Blum is with the Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA 18015 USA (e-mail: rblum@eecs.lehigh.edu).

L. M. Kaplan is with the Networked Sensing and Fusion Branch, U.S. Army Research Laboratory, Adelphi MD 20783 USA (e-mail: lance.m.kaplan@us.army.mil).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2018.2802459

built with powerful chips, and supplied with sufficient power, thereby highly sophisticated encryption algorithms and security procedures can be implemented.

This paper aims at developing a general detection approach which does not rely on the form of the attacks or attack parameters, to identify the attacked sensors in the sensor network with provable detection performance guarantee. It is worth mentioning that the problem of attack detection in target localization systems is difficult, since the statistical model of sensor data depend on the target location and the attack strategy which are both unknown to the FC. By exploring the impact of the attacks on the statistical model of the sensor data, we reveal that the essential effect of attacks is to alter the naive estimate of the distance between the target and each attacked sensor, which ignores the existence of attacks, to a different extent, giving rise to a geometric inconsistency among the attacked and unattacked sensors. Motivated by this fact, a class of detectors are proposed to detect the attacked sensors via scrutinizing the existence of the geometric inconsistency. To be specific, a naive maximum likelihood estimator (NMLE), the MLE formulated under the assumption of no attack, is first employed to estimate the distance between the target and each sensor. For each insecure sensor, a circle is generated which is centered at the sensor with radius equal to the NMLE of its distance to the target. For each of the two secure sensors, a ring with some constant width is generated. This ring is centered at the sensor and is bisected by a circle with radius equal to the NMLE of the distance from the sensor to the target. If the circle of an insecure sensor passes through the common area of the two rings, the sensor is declared unattacked; otherwise, we declare that it is under attack. A thorough performance analysis is carried out for the proposed detectors, showing that the false alarm and miss probabilities decrease exponentially as the number of data samples at each sensor grows, which implies that for a sufficiently large number of samples, the proposed detectors can identify the attacked sensors with an arbitrary level of accuracy. Moreover, the numerical results demonstrate that compared to the cases where all sensors are employed without detecting attacks or only the secure sensors are employed, the performance of estimating the target location can be significantly improved if we employ the secure sensors and the sensors which are declared as unattacked by the proposed detector.

B. Related Works

With the proliferation of sensor network applications, there is an increasing concern about the security of sensor networks, see [8], [9], [16]–[19] for instance. Most existing works on the security in sensor network target localization systems only consider analog measurements. However, for a typical sensor network with limited resources, it is desirable that only quantized data is transmitted from sensors to the FC [5]–[7]. Moreover, there is a lack of theoretical performance analysis of attack detection strategies.

Attack detection in the context of target localization with quantized data has not been well investigated in the literature. In [7], a specific attack model is considered and a practical approach is proposed to detect attacks in target localization systems. In particular, several secure sensors are employed to provide a coarse estimate of the target location, and then the expected behaviors of attacked and unattacked sensors are calculated based on the coarse estimate and the attack model. This method is based on heuristic and there is no detection performance guarantee. In our proposed approach, the estimate of the target location is not required, and moreover, the attack detection performance is rigorously investigated, which demonstrates that any identification accuracy can be achieved if the number of data samples is sufficiently large. In addition, the approach in [7] requires the knowledge of the statistical model of the attack, which is not required by our proposed approach.

The remainder of the paper is organized as follows. Section II describes the system and adversary model. In Section III, a class of detectors are proposed to identify the attacked sensors in the sensor network. Section IV investigates the performance of the proposed detectors. In Section V, several numerical results are provided to corroborate our theoretical analysis. Finally, Section VI provides our conclusions.

II. System and Adversary Models

In this section, the system and general attack models are introduced. We also demonstrate how the general attack model relates to some popular forms of attacks in practice.

A. System Model

Consider a sensor network consisting of N sensors and a FC to estimate the location of a target at $\boldsymbol{\theta}_{\mathrm{T}} = [x_{\mathrm{T}}, y_{\mathrm{T}}]$, where x_{T} and y_{T} denote the coordinates of the target location on the two-dimensional plane. For the j-th sensor, we use $\boldsymbol{\theta}_j = [x_j, y_j]$ to denote its location. Besides the N sensors, there also exist two secure sensors in the sensor network which are labeled as the $(N+1)$-th and $(N+2)$-th sensors, respectively. These two secure sensors are well protected and thereby are guaranteed to be tamper proof, while the other N sensors are insecure, which are subject to threat from adversaries. We assume that the signal radiated from the target obeys an isotropic power attenuation model, and each sensor observes K data samples. The k-th data sample at the j-th sensor is described as

$$s_{jk} = P_0 \left(\frac{D_0}{D_j} \right)^{\gamma} + n_{jk}, \; j = 1, 2, ..., N+2, \qquad (1)$$

where the distance D_j between the j-th sensor and the target is defined by

$$D_j \triangleq \| \boldsymbol{\theta}_j - \boldsymbol{\theta}_{\mathrm{T}} \| = \sqrt{(x_j - x_{\mathrm{T}})^2 + (y_j - y_{\mathrm{T}})^2}, \; \forall j, \qquad (2)$$

the quantity P_0 is the power measured at a reference distance D_0, γ is the path-loss exponent which is a positive constant, and n_{jk} denotes the additive noise sample with probability density function (pdf) $f_j(n_{jk})$.

We assume that P_0, D_0, γ, $\{f_j(\cdot)\}_{j=1}^{N+2}$, and $\{\boldsymbol{\theta}_j\}_{j=1}^{N+2}$ 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. In addition, we assume that the target stays in a specified ROI $\mathcal{A}$ where no sensor exists. By defining

$$D_{\mathrm{L}} \triangleq \min_{j=1,2,...,N+2} \inf_{\boldsymbol{\theta} \in \mathcal{A}} \| \boldsymbol{\theta}_j - \boldsymbol{\theta} \| > 0, \qquad (3)$$

$$\text{and} \quad D_{\mathrm{U}} \triangleq \max_{j=1,2,...,N+2} \sup_{\boldsymbol{\theta} \in \mathcal{A}} \| \boldsymbol{\theta}_j - \boldsymbol{\theta} \| < \infty, \qquad (4)$$

we know that for any $j \in \{1, 2, ..., N+2\}$,

$$D_j \in [D_{\mathrm{L}}, D_{\mathrm{U}}]. \qquad (5)$$

Regarding the secure sensors and the ROI $\mathcal{A}$, we make the following assumption.

Assumption 1: The secure sensors are widely separated so that

$$D_{\mathrm{S}} \triangleq \|\boldsymbol{\theta}_{N+1} - \boldsymbol{\theta}_{N+2}\| > D_{\mathrm{U}} - D_{\mathrm{L}} + 2\Upsilon_1 \tag{6}$$

for some positive constant Υ_1. In addition, the ROI $\mathcal{A}$ is contained in one of the two half spaces produced by dividing the whole space by the line passing through the two secure sensors. By the triangle inequality of sides, we assume

$$\inf_{\boldsymbol{\theta}_{\mathrm{T}} \in \mathcal{A}} \{D_{N+1} + D_{N+2}\} > D_{\mathrm{S}} + 2\Upsilon_2 \tag{7}$$

for some positive constant Υ_2.

Due to the low-rate communication constraint between the sensors and the FC, each sensor j quantizes its sample s_{jk} to one bit and then transmits the bit to the FC. For simplicity, we assume that the sensors employ the following threshold quantizers $\{\mathcal{Q}_j\}_{j=1}^{N+2}$

$$u_{jk} = \mathcal{Q}_j(s_{jk}) \triangleq \mathbb{1}\{s_{jk} \in (\tau_j, \infty)\}, \ \forall j \text{ and } \forall k, \tag{8}$$

where $\mathbb{1}\{\cdot\}$ is the indicator function, τ_j is the threshold employed at the j-th sensor and we assume that the thresholds $\{\tau_j\}_{j=1}^{N+2}$ are known to the FC.

Using (1) and (8), define

$$p_j(\boldsymbol{\theta}_{\mathrm{T}}) \triangleq \Pr(u_{jk} = 0 | \boldsymbol{\theta}_{\mathrm{T}}) = F_j\left(\tau_j - P_0\left(\frac{D_0}{D_j}\right)^{\gamma}\right), \tag{9}$$

where $F_j(x) \triangleq \int_{-\infty}^{x} f_j(t)\,dt$. By employing (5) and (9), we can define

$$\rho_j^{(\mathrm{L})} \triangleq \inf_{\boldsymbol{\theta} \in \mathcal{A}} p_j(\boldsymbol{\theta}) = F_j\left(\tau_j - P_0\left(\frac{D_0}{D_{\mathrm{L}}}\right)^{\gamma}\right), \tag{10}$$

$$\rho_j^{(\mathrm{U})} \triangleq \sup_{\boldsymbol{\theta} \in \mathcal{A}} p_j(\boldsymbol{\theta}) = F_j\left(\tau_j - P_0\left(\frac{D_0}{D_{\mathrm{U}}}\right)^{\gamma}\right), \tag{11}$$

and hence,

$$p_j(\boldsymbol{\theta}_{\mathrm{T}}) \in \left[\rho_j^{(\mathrm{L})}, \rho_j^{(\mathrm{U})}\right], \ j = 1, 2, ..., N+2. \tag{12}$$

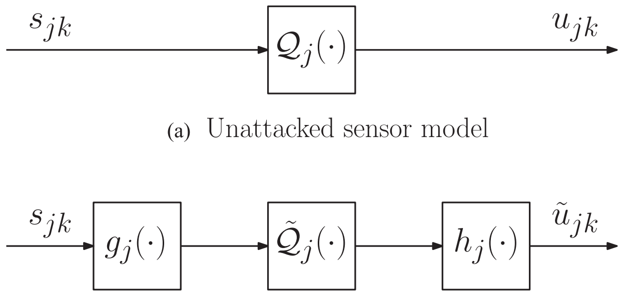
We assume that $f_j(x)$ is continuous, and $F_j^{-1}(x)$ exists and is differentiable over the open interval $(0, 1)$ for each j. Noticing that $\frac{\partial F_j^{-1}(x)}{\partial x} = [f_j(F_j^{-1}(x))]^{-1}$, the differentiability of $F_j^{-1}(x)$ implies $0 < f_j(x) < \infty$ over $\{x | F_j(x) \in (0, 1)\}$, and therefore, $F_j(x)$ is strictly increasing over $\{x | F_j(x) \in (0, 1)\}$.

It is clear that if there exists some $\boldsymbol{\theta} \in \mathcal{A}$ such that

$$\tau_j - P_0\left(\frac{D_0}{\|\boldsymbol{\theta}_j - \boldsymbol{\theta}\|}\right)^{\gamma} \notin \operatorname{supp}(f_j) \triangleq \{x | f_j(x) \neq 0\}, \tag{13}$$

then $F_j(\tau_j - P_0(\frac{D_0}{\|\boldsymbol{\theta}_j - \boldsymbol{\theta}\|})^{\gamma}) = 0$ or 1, and hence, the quantized data from the j-th sensor is useless in the sense of improving the performance of estimating $\boldsymbol{\theta}$. To this end, we assume that the quantizers are well designed, and thereby τ_j, D_{L} and D_{U} satisfy

$$\begin{aligned} \inf\{\operatorname{supp}(f_j)\} &< \tau_j - P_0\left(\frac{D_0}{D_{\mathrm{L}}}\right)^{\gamma} \\ &< \tau_j - P_0\left(\frac{D_0}{D_{\mathrm{U}}}\right)^{\gamma} < \sup\{\operatorname{supp}(f_j)\}, \end{aligned} \tag{14}$$



(a) Unattacked sensor model

(b) Attacked sensor model

Fig. 1. Unattacked and attacked sensor models.

which yields $\forall j$,

$$\begin{aligned} 0 &< F_j\left(\tau_j - P_0\left(\frac{D_0}{D_{\mathrm{L}}}\right)^{\gamma}\right) \\ &< F_j\left(\tau_j - P_0\left(\frac{D_0}{D_{\mathrm{U}}}\right)^{\gamma}\right) < F_j(\tau_j) \leq 1, \end{aligned} \tag{15}$$

since $F_j(\cdot)$ is strictly increasing, from (10) and (11), we know

$$0 < \rho_j^{(\mathrm{L})} < \rho_j^{(\mathrm{U})} < F_j(\tau_j) \leq 1. \tag{16}$$

B. Adversary Model

We consider a general attack model which brings about a change in the statistical model of u_{jk}. Let $\mathcal{U}$ and $\mathcal{V}$ denote the set of unattacked and attacked sensors, respectively.

In general, if $j \in \mathcal{V}$, three types of possible attacks can affect the j-th sensor, which are illustrated in Fig. 1 (b). First, the adversaries can tamper with the observations $\{s_{jk}\}_{k=1}^{K}$. Such attacks are called spoofing attacks, which can be represented by a mapping $g_j(\cdot)$. The second type of attack which we call hacking, aims at modifying the sensor hardware and/or software, and thereby modifying the quantizer $\mathcal{Q}_j(\cdot)$ to $\tilde{\mathcal{Q}}_j(\cdot)$ in the attacked sensors as shown in Fig. 1 (b). The last type of possible attack occurs between the sensors and the FC, which is referred to as man-in-the-middle attacks (MiMA). The MiMA can be described by a mapping $h_j(\cdot)$ that modifies the quantized data before it arrives at the FC. Therefore, the post attack quantized data can be generally expressed as[1]

$$\tilde{u}_{jk} = h_j\left(\tilde{\mathcal{Q}}_j(g_j(s_{jk}))\right). \tag{17}$$

With regard to the alphabet set of $\tilde{u}_{jk}$, we make the following assumption.

Assumption 2: We assume that if $j \in \mathcal{V}$, then the alphabet set of $\tilde{u}_{jk}$ is still $\{0, 1\}$. Otherwise, the detection of attacks is trivial.

Define

$$\tilde{p}_j(\boldsymbol{\theta}_{\mathrm{T}}) \triangleq \Pr(\tilde{u}_{jk} = 0 | \boldsymbol{\theta}_{\mathrm{T}}) = p_j(\boldsymbol{\theta}_{\mathrm{T}}) + \Psi_j, j = 1, 2, ..., N, \tag{18}$$

where the quantity Ψ_j represents the impact of the attacks on the statistical model of the data. Clearly, if $\Psi_j = 0$, then we can ignore the corresponding attack, since it is ineffective from

[1] We use the notation $\tilde{u}_{jk}$ to denote the quantized data received at the FC when attacks are considered, no matter whether the j-th sensor is attacked or not. If $j \in \mathcal{U}$, then $\tilde{u}_{jk} = u_{jk}$.

the perspective of the FC. Hence, without loss of generality, if $j \in \mathcal{V}$, then we assume $\Psi_j \neq 0$, while if $j \in \mathcal{U}$, then $\tilde{u}_{jk} = u_{jk}$ and $\Psi_j = 0$.

To illustrate (18) in a concrete way, we take the MiMA as an example. Under a class of MiMAs [7], [11], [12], the quantized data u_{jk} is flipped with probability $\psi_{j,i}$ if $u_{jk} = i$ for $i \in \{0, 1\}$, i.e., if the j-th sensor is attacked,

$$\begin{cases} \Pr\left(\tilde{u}_{jk} = 1 \,|u_{jk} = 0\right) = \psi_{j,0}, \\ \Pr\left(\tilde{u}_{jk} = 0 \,|u_{jk} = 1\right) = \psi_{j,1}, \end{cases} \tag{19}$$

where $\psi_{j,i} \in [0, 1]$. Using (19), we have

$$\tilde{p}_j(\boldsymbol{\theta}_{\mathrm{T}}) = (1 - \psi_{j,0} - \psi_{j,1})\, p_j(\boldsymbol{\theta}_{\mathrm{T}}) + \psi_{j,1}, \tag{20}$$

$$\text{and} \qquad \Psi_j = \psi_{j,1} - (\psi_{j,0} + \psi_{j,1})\, p_j(\boldsymbol{\theta}_{\mathrm{T}}). \tag{21}$$

Besides the man-in-the-middle attacks, the spoofing attacks can also be shown to agree with (18) [8], [9], [15].

From a practical point of view, the following assumptions on the attacks are made throughout this paper.

Assumption 3:

1) For each j, Ψ_j is constant over time.
2) *Subtle Attacks:* By the strong law of large numbers, we know that as $K \to \infty$, $\frac{1}{K}\sum_{k=1}^{K}(1 - \tilde{u}_{jk}) \to \tilde{p}_j(\boldsymbol{\theta}_{\mathrm{T}})$ almost surely. Thus, if $\tilde{p}_j(\boldsymbol{\theta}_{\mathrm{T}}) \notin [\rho_j^{(\mathrm{L})}, \rho_j^{(\mathrm{U})}]$, then with sufficient observations, the attack against the j-th sensor can be detected at the FC by checking whether $\frac{1}{K}\sum_{k=1}^{K}(1 - \tilde{u}_{jk})$ is in the range $[\rho_j^{(\mathrm{L})}, \rho_j^{(\mathrm{U})}]$. For this reason, in order to reduce the possibility of being detected, the adversaries should ensure

$$\tilde{p}_j(\boldsymbol{\theta}_{\mathrm{T}}) \in \left[\rho_j^{(\mathrm{L})}, \rho_j^{(\mathrm{U})}\right],\ j \in \mathcal{V}. \tag{22}$$

3) *Significant Attacks:* In order to bring about sufficient impact on the statistical characterization of the bits from the attacked sensors, every adversary is required to guarantee a minimum distortion, i.e.,

$$|\Psi_j| > \kappa,\ j \in \mathcal{V}, \tag{23}$$

for some positive constant κ. Otherwise, the attacks can be ignored.

It is worth mentioning that Assumption 3 1) does not require that the attacks illustrated in (17) are time-invariant, and it only implies that the impact of the attacks on the statistical model of the data is stationary, which is widely assumed in the literature on attacks in sensor networks, see [7], [10], [11] and reference therein for instance. If Assumption 3 1) is not satisfied, then the statistical model of the data from the attacked sensor is time-variant. Thus, with sufficient observations, the attacked sensors can be easily detected by just checking whether the empirical probability mass function of the data in different sufficiently long time periods is constant or not. To this end, the adversaries should ensure Assumption 3 1) to reduce the possibility of being detected.

Our problem is to design an efficient strategy for the FC to identify the attacked sensors, based on the binary observations it receives from all sensors, and to provide a performance analysis on the proposed attack detection strategy.

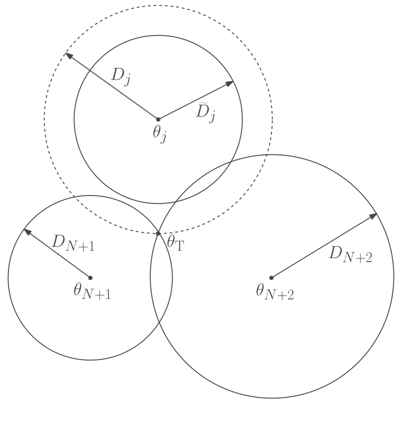


Fig. 2. Geometric inconsistency among the j-th, $(N+1)$-th and $(N+2)$-th sensors when $j \in \mathcal{V}$.

III. Attack Detectors Based on Naive Maximum Likelihood Estimator

In this section, we first show that by employing a naive maximum likelihood estimator (NMLE), a geometric inconsistency among each attacked sensor and other unattacked sensors can be utilized to distinguish between the attacked and unattacked ones. Then, a class of detectors which are based on the NMLE are proposed to detect the attacks in the sensor network.

A. Naive Maximum Likelihood Estimator and Geometric Inconsistency

For any j, from (9) and by employing the existence of $F_j^{-1}(x)$, we can obtain

$$D_j = D_0 P_0^{\frac{1}{\gamma}} \left[\tau_j - F_j^{-1}\left(p_j(\boldsymbol{\theta}_{\mathrm{T}})\right)\right]^{-\frac{1}{\gamma}}. \tag{24}$$

Then the NMLE, which is the MLE ignoring the existence of attacks, of D_j is given by

$$\widehat{D}_j^{(K)} = D_0 P_0^{\frac{1}{\gamma}} \left[\tau_j - F_j^{-1}\left(\xi_j^{(K)}\right)\right]^{-\frac{1}{\gamma}}, \tag{25}$$

$$\text{where} \qquad \xi_j^{(K)} \triangleq \frac{1}{K}\sum_{k=1}^{K}\left(1 - \tilde{u}_{jk}\right). \tag{26}$$

Furthermore, define

$$\widetilde{D}_j \triangleq D_0 P_0^{\frac{1}{\gamma}} \left[\tau_j - F_j^{-1}\left(\tilde{p}_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)\right]^{-\frac{1}{\gamma}}. \tag{27}$$

It is seen from (27) that $\widetilde{D}_j$ is a monotonic function of $\tilde{p}_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)$, and since from (23), we know $\tilde{p}_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right) \neq p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)$, we have $\widetilde{D}_j \neq D_j$. What's more, by the strong law of large numbers, we know

$$\widehat{D}_j^{(K)} \to \begin{cases} D_j, \text{ if } j \in \mathcal{U} \\ \widetilde{D}_j, \text{ if } j \in \mathcal{V} \end{cases} \text{almost surely, as } K \to \infty. \tag{28}$$

This implies that, from the perspective of the NMLE, if $j \in \mathcal{V}$, the essential effect of the attack is a falsification of the distance D_j between the target and the j-th sensor to some different $\widetilde{D}_j$. This gives rise to a geometric inconsistency between the j-th sensor and the two secure sensors, which is illustrated in Fig. 2. Specifically, if $j \in \mathcal{U}$, as illustrated in Fig. 2, the three circles centered at the j-th, $(N+1)$-th and $(N+2)$-th sensors

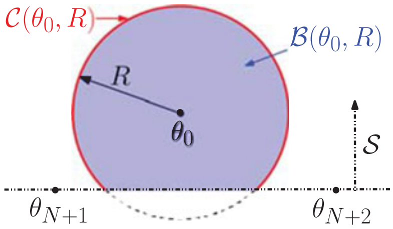


Fig. 3. Geometric illustration of $\mathcal{C}(\boldsymbol{\theta}_0, R)$ and $\mathcal{B}(\boldsymbol{\theta}_0, R)$.

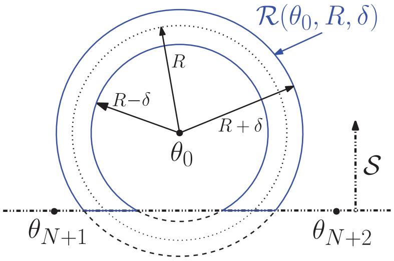


Fig. 4. Geometric illustration of $\mathcal{R}(\boldsymbol{\theta}_0, R, \delta)$.

and with radii D_j, D_{N+1} and D_{N+2}, respectively, intersect at the point $\boldsymbol{\theta}_\mathrm{T}$; while if $j \in \mathcal{V}$, then the three circles centered at the j-th, $(N+1)$-th and $(N+2)$-th sensors and with radii $\widetilde{D}_j$, D_{N+1} and D_{N+2} do not intersect at $\boldsymbol{\theta}_\mathrm{T}$ as illustrated in Fig. 2.

Motivated by this fact, consider three circles centered at the j-th, $(N+1)$-th and $(N+2)$-th sensors and with radii $\widehat{D}_j^{(K)}$, $\widehat{D}_{N+1}^{(K)}$ and $\widehat{D}_{N+2}^{(K)}$, respectively. If $j \in \mathcal{V}$, then from (28), we know that with sufficiently large K and Assumption 3, it is impossible for these three circles to intersect at a common point. This observation forms the basis of the proposed attack detection strategy.

B. Attack Detection Strategy

In order to mathematically formulate the attack detector, we first define three geometric shapes. According to Assumption 1, the ROI $\mathcal{A}$ is contained in one of the two half spaces produced by dividing the whole space by the line passing through the two secure sensors. We use $\mathcal{S}$ to represent this half space. Let $\mathcal{C}(\boldsymbol{\theta}_0, R)$ denote the intersection of $\mathcal{S}$ and the circle centered at $\boldsymbol{\theta}_0$ and with radius R, i.e.,

$$\mathcal{C}(\boldsymbol{\theta}_0, R) \triangleq \{\boldsymbol{\theta} \in \mathcal{S} \,|\, \|\boldsymbol{\theta} - \boldsymbol{\theta}_0\| = R\}, \tag{29}$$

which is illustrated by the red curve in Fig. 3. Let $\mathcal{R}(\boldsymbol{\theta}_0, R, \delta)$ denote the intersection of $\mathcal{S}$ and the ring centered at $\boldsymbol{\theta}_0$, with radius R and width δ, i.e.,

$$\mathcal{R}(\boldsymbol{\theta}_0, R, \delta) \triangleq \{\boldsymbol{\theta} \in \mathcal{S} \,|\, R - \delta \leq \|\boldsymbol{\theta} - \boldsymbol{\theta}_0\| \leq R + \delta\}. \tag{30}$$

The region enclosed by the blue boundary in Fig. 4 depicts an example of $\mathcal{R}(\boldsymbol{\theta}_0, R, \delta)$. Let $\mathcal{B}(\boldsymbol{\theta}_0, R)$ denote the intersection of $\mathcal{S}$ and the ball centered at $\boldsymbol{\theta}_0$ and with radius R, i.e.,

$$\mathcal{B}(\boldsymbol{\theta}_0, R) \triangleq \{\boldsymbol{\theta} \in \mathcal{S} \,|\, \|\boldsymbol{\theta} - \boldsymbol{\theta}_0\| \leq R\}. \tag{31}$$

which is the blue region in Fig. 3.

It is worth mentioning that even though $j \in \mathcal{U}$, due to the estimation error with finite K, the three circles centered at the j-th, $(N+1)$-th and $(N+2)$-th sensors and with radii $\widehat{D}_j^{(K)}$, $\widehat{D}_{N+1}^{(K)}$ and $\widehat{D}_{N+2}^{(K)}$, respectively, typically will not intersect at a common point. Thus, for finite K, checking the geometric inconsistency among $\mathcal{C}(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)})$, $\mathcal{C}(\boldsymbol{\theta}_{N+1}, \widehat{D}_{N+1}^{(K)})$ and $\mathcal{C}(\boldsymbol{\theta}_{N+2}, \widehat{D}_{N+2}^{(K)})$ cannot reliably tell whether the j-th sensor is unattacked or not. To overcome this, we replace $\mathcal{C}(\boldsymbol{\theta}_{N+1}, \widehat{D}_{N+1}^{(K)})$ and $\mathcal{C}(\boldsymbol{\theta}_{N+2}, \widehat{D}_{N+2}^{(K)})$ with $\mathcal{R}(\boldsymbol{\theta}_{N+1}, \widehat{D}_{N+1}^{(K)}, \delta)$ and $\mathcal{R}(\boldsymbol{\theta}_{N+2}, \widehat{D}_{N+2}^{(K)}, \delta)$ for some δ, respectively, and scrutinize whether $\mathcal{C}(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)})$ pass through the common area of $\mathcal{R}(\boldsymbol{\theta}_{N+1}, \widehat{D}_{N+1}^{(K)}, \delta)$ and $\mathcal{R}(\boldsymbol{\theta}_{N+2}, \widehat{D}_{N+2}^{(K)}, \delta)$ instead.

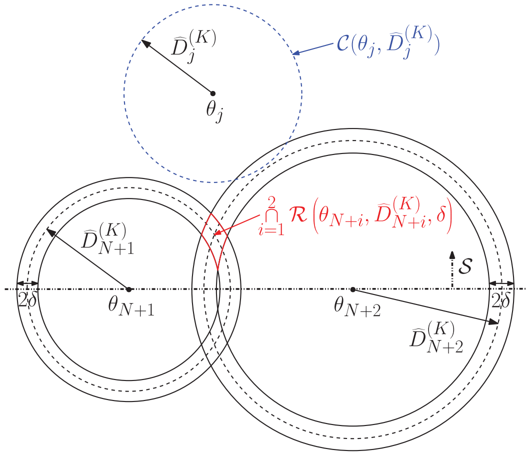

$\widehat{D}_j^{(K)}$
$\mathcal{C}(\theta_j, \widehat{D}_j^{(K)})$
θ_j
$\bigcap_{i=1}^{2} \mathcal{R}\left(\theta_{N+i}, \widehat{D}_{N+i}^{(K)}, \delta\right)$
$\widehat{D}_{N+1}^{(K)}$
$\mathcal{S}$
2δ
θ_{N+1}
θ_{N+2}
2δ
$\widehat{D}_{N+2}^{(K)}$

Fig. 5. Geometric illustration of the proposed detectors.

To be specific, for the j-th sensor, $j = 1, 2, \ldots, N$, we consider the following hypothesis testing problem

$$\begin{cases} \mathcal{H}_0 : j \in \mathcal{U} \\ \mathcal{H}_1 : j \in \mathcal{V} \end{cases} \tag{32}$$

and a class of detectors

$$\varpi_j(\delta) = \begin{cases} 0, & \text{if } \mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\cap_{i=1}^{2} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, \widehat{D}_{N+i}^{(K)}, \delta\right)\right] \neq \emptyset, \\ 1, & \text{if } \mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\cap_{i=1}^{2} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, \widehat{D}_{N+i}^{(K)}, \delta\right)\right] = \emptyset, \end{cases} \tag{33}$$

for some constant δ, where $\widehat{D}_j^{(K)}$ is defined in (25).

The geometric illustration of the proposed detector in (33) is depicted in Fig. 5, where the region enclosed by the red curves is the common area of $\mathcal{R}(\boldsymbol{\theta}_{N+1}, \widehat{D}_{N+1}^{(K)}, \delta)$ and $\mathcal{R}(\boldsymbol{\theta}_{N+2}, \widehat{D}_{N+2}^{(K)}, \delta)$ which plays an important role in the attack detection process. It is worth noticing that the center of this common area is determined by two random variables $\widehat{D}_{N+1}^{(K)}$ and $\widehat{D}_{N+2}^{(K)}$, and thereby is randomly located. To this end, this common area may not cover the true target location $\boldsymbol{\theta}_\mathrm{T}$. In addition, the size of the common area of $\mathcal{R}(\boldsymbol{\theta}_{N+1}, \widehat{D}_{N+1}^{(K)}, \delta)$ and $\mathcal{R}(\boldsymbol{\theta}_{N+2}, \widehat{D}_{N+2}^{(K)}, \delta)$ depends on the parameter δ which impacts the false alarm and miss probabilities of the proposed detector.

IV. Performance Analysis of the Proposed Detector

In this section, the detection performance of the proposed detector in (33) is investigated. We will show that the false alarm and miss probabilities of the proposed detector decay exponentially fast as the number of data samples at each sensor increases.

To start with, we provide the following lemma regarding the lower and upper bounds on the common area of $\mathcal{R}(\boldsymbol{\theta}_{N+1}, D_{N+1}, \delta)$ and $\mathcal{R}(\boldsymbol{\theta}_{N+2}, D_{N+2}, \delta)$.

Lemma 1: If

$$\delta < \Upsilon \triangleq \min\{\Upsilon_1, \Upsilon_2\}, \tag{34}$$

then

$$\sup_{\boldsymbol{\theta} \in \overset{2}{\underset{i=1}{\cap}} \mathcal{R}(\boldsymbol{\theta}_{N+i}, D_{N+i}, \delta)} \|\boldsymbol{\theta} - \boldsymbol{\theta}_{\mathrm{T}}\| < \Phi(\delta) \tag{35}$$

with $\Phi(\delta) \triangleq (2D_U + \Upsilon)^{\frac{1}{2}} \left[\frac{2D_U + \Upsilon}{D_S}\left(\frac{\Upsilon}{D_S} + 1\right) + 2\right]^{\frac{1}{2}} \sqrt{\delta}.$ (36)

This implies

$$\mathcal{B}(\boldsymbol{\theta}_{\mathrm{T}}, \delta) \subseteq \overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, D_{N+i}, \delta\right) \subseteq \mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}}, \Phi(\delta)\right). \tag{37}$$

Proof: Refer to Appendix A. ■

As demonstrated by Lemma 1, the common area of $\mathcal{R}(\boldsymbol{\theta}_{N+1}, D_{N+1}, \delta)$ and $\mathcal{R}(\boldsymbol{\theta}_{N+2}, D_{N+2}, \delta)$ can be bounded by two balls from below and above. Moreover, the radii of these two balls are both increasing functions of the given δ. It will be shown later that by employing the two balls to approximate the irregular area $\cap_{i=1}^{2}\mathcal{R}(\boldsymbol{\theta}_{N+i}, D_{N+i}, \delta)$ from below and above, the detection performance analysis of the proposed detector in (33) can be considerably facilitated.

A. Upper Bound on False Alarm Probability

From (33), the false alarm and miss probabilities of the proposed detector are given by $\mathbb{P}_0\left(\varpi_j\left(\delta\right)=1\right)$ and $\mathbb{P}_1(\varpi_j\left(\delta\right)=0)$, respectively, where $\mathbb{P}_i$ denotes the probability measure under hypothesis $\mathcal{H}_i$.

Let $\mathcal{E}_i$ denote the event

$$\mathcal{E}_i \triangleq \left\{\left|\widehat{D}_{N+i}^{(K)} - D_{N+i}\right| < \frac{1}{2}\delta\right\},\ i = 1, 2, \tag{38}$$

and $\mathcal{E}_i^{\mathrm{C}}$ denotes the complement of the event $\mathcal{E}_i$, where δ satisfies (34). The false alarm probability of the detector in (33) can be expressed as

$$\begin{aligned}
&\mathbb{P}_0\left(\varpi_j\left(\delta\right)=1\right)\\
&= \mathbb{P}_0\left(\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, \widehat{D}_{N+i}^{(K)}, \delta\right)\right] = \emptyset\right)\\
&= \mathbb{P}_0\left(\left\{\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, \widehat{D}_{N+i}^{(K)}, \delta\right)\right] = \emptyset\right\}\right.\\
&\qquad\qquad \left.\cap \left(\mathcal{E}_1 \cap \mathcal{E}_2\right)\right)\\
&+ \mathbb{P}_0\left(\left\{\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, \widehat{D}_{N+i}^{(K)}, \delta\right)\right] = \emptyset\right\}\right.\\
&\qquad\qquad \left.\cap \left(\mathcal{E}_1^{\mathrm{C}} \cup \mathcal{E}_2^{\mathrm{C}}\right)\right).
\end{aligned} \tag{39}$$

Note that $\mathcal{E}_i$ implies that

$$\mathcal{R}\left(\boldsymbol{\theta}_{N+i}, D_{N+i}, \frac{1}{2}\delta\right) \subseteq \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, \widehat{D}_{N+i}^{(K)}, \delta\right), \tag{40}$$

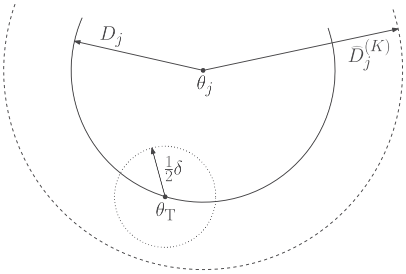


Fig. 6. Geometric illustration of (45).

and hence, from (39), we can obtain

$$\begin{aligned}
&\mathbb{P}_0\left(\varpi_j\left(\delta\right)=1\right)\\
&\le \mathbb{P}_0\left(\left\{\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, D_{N+i}, \frac{1}{2}\delta\right)\right] = \emptyset\right\}\right.\\
&\qquad\qquad \left.\cap \left(\mathcal{E}_1 \cap \mathcal{E}_2\right)\right)\\
&+ \mathbb{P}_0\left(\left\{\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, \widehat{D}_{N+i}^{(K)}, \delta\right)\right] = \emptyset\right\}\right.\\
&\qquad\qquad \left.\cap \left(\mathcal{E}_1^{\mathrm{C}} \cup \mathcal{E}_2^{\mathrm{C}}\right)\right)\\
&\le \mathbb{P}_0\left(\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, D_{N+i}, \frac{1}{2}\delta\right)\right] = \emptyset\right)\\
&\quad + \mathbb{P}_0\left(\mathcal{E}_1^{\mathrm{C}} \cup \mathcal{E}_2^{\mathrm{C}}\right) \qquad (41)\\
&\le \mathbb{P}_0\left(\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \left[\overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, D_{N+i}, \frac{1}{2}\delta\right)\right] = \emptyset\right)\\
&\quad + \mathbb{P}_0\left(\mathcal{E}_1^{\mathrm{C}}\right) + \mathbb{P}_0\left(\mathcal{E}_2^{\mathrm{C}}\right), \qquad (42)
\end{aligned}$$

where (41) is due to the fact that $\mathbb{P}_0(\mathcal{E} \cap \mathcal{F}) \le \mathbb{P}_0(\mathcal{E})$ for any two events $\mathcal{E}$ and $\mathcal{F}$. Moreover, from Lemma 1, we know

$$\mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}}, \frac{1}{2}\delta\right) \subseteq \overset{2}{\underset{i=1}{\cap}} \mathcal{R}\left(\boldsymbol{\theta}_{N+i}, D_{N+i}, \frac{1}{2}\delta\right), \tag{43}$$

which yields

$$\begin{aligned}
\mathbb{P}_0\left(\varpi_j\left(\delta\right)=1\right) &\le \mathbb{P}_0\left(\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}}, \frac{1}{2}\delta\right) = \emptyset\right)\\
&\quad + \mathbb{P}_0\left(\mathcal{E}_1^{\mathrm{C}}\right) + \mathbb{P}_0\left(\mathcal{E}_2^{\mathrm{C}}\right).
\end{aligned} \tag{44}$$

In addition, as illustrated in Fig. 6, if $j \in \mathcal{U}$, we know $\boldsymbol{\theta}_{\mathrm{T}} \in \mathcal{C}(\boldsymbol{\theta}_j, D_j)$ which yields that under hypothesis $\mathcal{H}_0$,

$$\begin{aligned}
&\left\{\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}}, \frac{1}{2}\delta\right) = \emptyset\right\}\\
&\Leftrightarrow \left\{\left|\widehat{D}_j^{(K)} - D_j\right| \ge \frac{1}{2}\delta\right\},
\end{aligned} \tag{45}$$

and therefore, by employing (38), (44) and (45), we reach the following theorem.

Theorem 1: If δ satisfies (34), the false alarm probability of the proposed detector in (33) can be bounded from above as per

$$\begin{aligned}
&\mathbb{P}_0\left(\varpi_j\left(\delta\right)=1\right)\\
&\leq \mathbb{P}_0\left(\left|\widehat{D}_j^{(K)}-D_j\right|\geq\frac{1}{2}\delta\right)+\mathbb{P}_0\left(\mathcal{E}_1^{\mathrm{C}}\right)+\mathbb{P}_0\left(\mathcal{E}_2^{\mathrm{C}}\right)\\
&=\mathbb{P}_0\left(\left|\widehat{D}_j^{(K)}-D_j\right|\geq\frac{1}{2}\delta\right)\\
&\quad+\sum_{i=1}^{2}\mathbb{P}_0\left(\left|\widehat{D}_{N+i}^{(K)}-D_{N+i}\right|\geq\frac{1}{2}\delta\right). \qquad (46)
\end{aligned}$$

B. Upper Bound on Miss Probability

On the other hand, considering that δ satisfies (34), the miss probability of the detector in (33) can be bounded from above as per

$$\begin{aligned}
&\mathbb{P}_1\left(\varpi_j\left(\delta\right)=0\right)\\
&=\mathbb{P}_1\left(\mathcal{C}\left(\boldsymbol{\theta}_j,\widehat{D}_j^{(K)}\right)\cap\left[\bigcap_{i=1}^{2}\mathcal{R}\left(\boldsymbol{\theta}_{N+i},\widehat{D}_{N+i}^{(K)},\delta\right)\right]\neq\emptyset\right)\\
&=\mathbb{P}_1\left(\left\{\mathcal{C}\left(\boldsymbol{\theta}_j,\widehat{D}_j^{(K)}\right)\cap\left[\bigcap_{i=1}^{2}\mathcal{R}\left(\boldsymbol{\theta}_{N+i},\widehat{D}_{N+i}^{(K)},\delta\right)\right]\neq\emptyset\right\}\right.\\
&\qquad\left.\cap\left(\mathcal{E}_1\cap\mathcal{E}_2\right)\right)\\
&\quad+\mathbb{P}_1\left(\left\{\mathcal{C}\left(\boldsymbol{\theta}_j,\widehat{D}_j^{(K)}\right)\cap\left[\bigcap_{i=1}^{2}\mathcal{R}\left(\boldsymbol{\theta}_{N+i},\widehat{D}_{N+i}^{(K)},\delta\right)\right]\neq\emptyset\right\}\right.\\
&\qquad\left.\cap\left(\mathcal{E}_1^{\mathrm{C}}\cup\mathcal{E}_2^{\mathrm{C}}\right)\right)\\
&\leq\mathbb{P}_1\left(\left\{\mathcal{C}\left(\boldsymbol{\theta}_j,\widehat{D}_j^{(K)}\right)\cap\left[\bigcap_{i=1}^{2}\mathcal{R}\left(\boldsymbol{\theta}_{N+i},D_{N+i},\frac{3}{2}\delta\right)\right]\neq\emptyset\right\}\right.\\
&\qquad\left.\cap\left(\mathcal{E}_1\cap\mathcal{E}_2\right)\right)+\mathbb{P}_1\left(\mathcal{E}_1^{\mathrm{C}}\cup\mathcal{E}_2^{\mathrm{C}}\right) \qquad (47)\\
&\leq\mathbb{P}_1\left(\mathcal{C}\left(\boldsymbol{\theta}_j,\widehat{D}_j^{(K)}\right)\cap\left[\bigcap_{i=1}^{2}\mathcal{R}\left(\boldsymbol{\theta}_{N+i},D_{N+i},\frac{3}{2}\delta\right)\right]\neq\emptyset\right)\\
&\quad+\mathbb{P}_1\left(\mathcal{E}_1^{\mathrm{C}}\right)+\mathbb{P}_1\left(\mathcal{E}_2^{\mathrm{C}}\right)\\
&\quad\leq\mathbb{P}_1\left(\mathcal{C}\left(\boldsymbol{\theta}_j,\widehat{D}_j^{(K)}\right)\cap\mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}},\Phi\left(\frac{3}{2}\delta\right)\right)\neq\emptyset\right)\\
&\qquad+\mathbb{P}_1\left(\mathcal{E}_1^{\mathrm{C}}\right)+\mathbb{P}_1\left(\mathcal{E}_2^{\mathrm{C}}\right), \qquad (48)
\end{aligned}$$

where (47) is due to the fact that if $\mathcal{E}_1$ and $\mathcal{E}_2$ occur, then

$$\mathcal{R}\left(\boldsymbol{\theta}_{N+i},\widehat{D}_{N+i}^{(K)},\delta\right)\subseteq\mathcal{R}\left(\boldsymbol{\theta}_{N+i},D_{N+i},\frac{3}{2}\delta\right),\ i=1,2, \qquad (49)$$

and (48) is because $\cap_{i=1}^{2}\mathcal{R}\left(\boldsymbol{\theta}_{N+i},D_{N+i},\frac{3}{2}\delta\right)\subseteq\mathcal{B}(\boldsymbol{\theta}_{\mathrm{T}},\Phi(\frac{3}{2}\delta))$ according to Lemma 1.

Since the first term in (48) is hard to deal with, we employ an upper bound on it which is provided in the following lemma.

Lemma 2: Define

$$\lambda_j\triangleq\frac{\kappa D_0P_0^{\frac{1}{\gamma}}\left[\tau_j-F_j^{-1}\left(\rho_j^{(\mathrm{L})}\right)\right]^{-\frac{\gamma+1}{\gamma}}}{\gamma\sup\limits_{x\in\left[F_j^{-1}(\rho_j^{(\mathrm{L})}),F_j^{-1}(\rho_j^{(\mathrm{U})})\right]}f_j\left(x\right)}, \qquad (50)$$

and denote

$$\lambda=\min_{j=1,2,\ldots,N}\left\{\lambda_j\right\}. \qquad (51)$$

If

$$\begin{aligned}
0<\delta<\min&\left\{\left\{(2D_U+\Upsilon)^{\frac{1}{2}}\left[\frac{6D_U+3\Upsilon}{2D_S}\left(\frac{\Upsilon}{D_S}+1\right)+3\right]^{\frac{1}{2}}\right.\right.\\
&\left.\left.+\frac{1}{2}\Upsilon^{\frac{1}{2}}\right\}^{-2}\lambda^2,\Upsilon\right\}, \qquad (52)
\end{aligned}$$

then

$$\begin{aligned}
&\mathbb{P}_1\left(\mathcal{C}\left(\boldsymbol{\theta}_j,\widehat{D}_j^{(K)}\right)\cap\mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}},\Phi\left(\frac{3}{2}\delta\right)\right)\neq\emptyset\right)\\
&\leq\mathbb{P}_1\left(\left|\widehat{D}_j^{(K)}-\widetilde{D}_j\right|\geq\frac{1}{2}\delta\right), \qquad (53)
\end{aligned}$$

where $\widetilde{D}_j$ is defined in (27).

Proof: Refer to Appendix B. ■

It is worth mentioning that since $f_j(x)$ is continuous and positive over $\{x|F_j(x)\in(0,1)\}$, the denominator $\sup_{x\in[F_j^{-1}(\rho_j^{(\mathrm{L})}),F_j^{-1}(\rho_j^{(\mathrm{U})})]}f_j(x)$ in (50) is positive and bounded. Moreover, according to (10), we know that $\tau_j>F_j^{-1}(\rho_j^{(\mathrm{L})})$, since F_j^{-1} is strictly increasing. Therefore, $0<\lambda_j<\infty$, and hence, $0<\lambda<\infty$.

By employing (38), (48) and Lemma 2, we reach the following theorem.

Theorem 2: if δ satisfies (52), then an upper bound on the miss probability of the detector in (33) can be expressed as

$$\begin{aligned}
&\mathbb{P}_1\left(\varpi_j\left(\delta\right)=0\right)\\
&\leq\mathbb{P}_1\left(\left|\widehat{D}_j^{(K)}-\widetilde{D}_j\right|\geq\frac{1}{2}\delta\right)+\mathbb{P}_1\left(\mathcal{E}_1^{\mathrm{C}}\right)+\mathbb{P}_1\left(\mathcal{E}_2^{\mathrm{C}}\right)\\
&=\mathbb{P}_1\left(\left|\widehat{D}_j^{(K)}-\widetilde{D}_j\right|\geq\frac{1}{2}\delta\right)\\
&\quad+\sum_{i=1}^{2}\mathbb{P}_1\left(\left|\widehat{D}_{N+i}^{(K)}-D_{N+i}\right|\geq\frac{1}{2}\delta\right). \qquad (54)
\end{aligned}$$

C. Exponential Decay of False Alarm and Miss Probabilities

It is seen from (46) and (54) that the upper bounds on the false alarm and miss probabilities have some similarities. To be specific, since the $(N+1)$-th and $(N+2)$-th sensors are secure, $\mathbb{P}_0(|\widehat{D}_{N+i}^{(K)}-D_{N+i}|\geq\frac{1}{2}\delta)=\mathbb{P}_1(|\widehat{D}_{N+i}^{(K)}-D_{N+i}|\geq\frac{1}{2}\delta)$ for $i=1,2$. Thus, the second term in (46) is the same as the second term in (54). Moreover, as $K\to\infty$, $\widehat{D}_j^{(K)}\to D_j$ almost surely under hypothesis $\mathcal{H}_0$, while $\widehat{D}_j^{(K)}\to\widetilde{D}_j$ almost surely under hypothesis $\mathcal{H}_1$, one can expect that the first term in (46) and the first term in (54) behave in a very similar way as K

increases, except for the change in $\widehat{D}_j^{(K)}$ due to the attack. In the following theorem, by employing (46) and (54), we show that the false alarm and miss probabilities of the detector in (33) decay at least exponentially with respect to K.

Theorem 3: If (52) holds, then the false alarm and miss probabilities are upper bounded by

$$\mathbb{P}_0\left(\varpi_j\left(\delta\right)=1\right)\le 12e^{-\eta_j^{(0)}(\delta)K}, \tag{55}$$

$$\mathbb{P}_1\left(\varpi_j\left(\delta\right)=0\right)\le 12e^{-\eta_j^{(1)}(\delta)K}, \tag{56}$$

for some positive constants $\eta_j^{(0)}\left(\delta\right)$ and $\eta_j^{(1)}\left(\delta\right)$.

Proof: Before proceeding, we define a sequence of events $\mathcal{F}_{j,K}$ as

$$\mathcal{F}_{j,K}\triangleq\left\{\xi_j^{(K)}\in\left[\varepsilon_j^{(\mathrm{L})},\varepsilon_j^{(\mathrm{U})}\right]\right\}, \tag{57}$$

where $\xi_j^{(K)}$ is defined in (26). The constants $\varepsilon_j^{(\mathrm{L})}$ and $\varepsilon_j^{(\mathrm{U})}$ in (57) are defined as

$$\varepsilon_j^{(\mathrm{L})}\triangleq\sigma_j^{(\mathrm{L})}\rho_j^{(\mathrm{L})},\varepsilon_j^{(\mathrm{U})}\triangleq\sigma_j^{(\mathrm{U})}\rho_j^{(\mathrm{U})}+\left(1-\sigma_j^{(\mathrm{U})}\right)F_j\left(\tau_j\right) \tag{58}$$

for some numbers $\sigma_j^{(\mathrm{L})},\sigma_j^{(\mathrm{U})}\in(0,1)$, where $F_j\left(\tau_j\right)\triangleq\int_{-\infty}^{\tau_j}f_j\left(t\right)dt$, and $\rho_j^{(\mathrm{L})}$ and $\rho_j^{(\mathrm{U})}$ are defined in (10) and (11), respectively. From (16) and (58), we know that

$$0<\varepsilon_j^{(\mathrm{L})}<\rho_j^{(\mathrm{L})}<\rho_j^{(\mathrm{U})}<\varepsilon_j^{(\mathrm{U})}<F_j\left(\tau_j\right)\le 1. \tag{59}$$

Let's first consider the upper bound on the false alarm probability as illustrated in (46). For any $j\in\{1,2,...,N+2\}$,

$$\begin{aligned}&\mathbb{P}_0\left(\left|\widehat{D}_j^{(K)}-D_j\right|\ge\frac{1}{2}\delta\right)\\&=\mathbb{P}_0\left(\left\{\left|\widehat{D}_j^{(K)}-D_j\right|\ge\frac{1}{2}\delta\right\}\cap\mathcal{F}_{j,K}\right)\\&\quad+\mathbb{P}_0\left(\left\{\left|\widehat{D}_j^{(K)}-D_j\right|\ge\frac{1}{2}\delta\right\}\cap\mathcal{F}_{j,K}^{\mathrm{C}}\right)\\&\le\mathbb{P}_0\left(\left\{\left|\widehat{D}_j^{(K)}-D_j\right|\ge\frac{1}{2}\delta\right\}\cap\mathcal{F}_{j,K}\right)+\mathbb{P}_0\left(\mathcal{F}_{j,K}^{\mathrm{C}}\right).\end{aligned} \tag{60}$$

Note that under hypothesis $\mathcal{H}_0$, if $\xi_j^{(K)}\in[\varepsilon_j^{(\mathrm{L})},\varepsilon_j^{(\mathrm{U})}]$, then by employing (24), (25) and (59), we can obtain

$$\begin{aligned}&\left|\widehat{D}_j^{(K)}-D_j\right|\\&=D_0P_0^{\frac{1}{\gamma}}\left|\left[\tau_j-F_j^{-1}\left(\xi_j^{(K)}\right)\right]^{-\frac{1}{\gamma}}-\left[\tau_j-F_j^{-1}\left(p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)\right]^{-\frac{1}{\gamma}}\right|\\&\le D_0P_0^{\frac{1}{\gamma}}\sup_{x\in\left[\varepsilon_j^{(\mathrm{L})},\varepsilon_j^{(\mathrm{U})}\right]}\left|\frac{\partial\left[\tau_j-F_j^{-1}\left(x\right)\right]^{-\frac{1}{\gamma}}}{\partial x}\right|\left|\xi_j^{(K)}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right|\end{aligned} \tag{61}$$

$$\begin{aligned}&=\frac{D_0P_0^{\frac{1}{\gamma}}}{\gamma}\sup_{x\in\left[\varepsilon_j^{(\mathrm{L})},\varepsilon_j^{(\mathrm{U})}\right]}\left|\frac{\left[\tau_j-F_j^{-1}\left(x\right)\right]^{-\frac{\gamma+1}{\gamma}}}{f_j\left(F_j^{-1}\left(x\right)\right)}\right|\left|\xi_j^{(K)}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right|\\&\le\underbrace{\frac{D_0P_0^{\frac{1}{\gamma}}\left[\tau_j-F_j^{-1}\left(\varepsilon_j^{(\mathrm{U})}\right)\right]^{-\frac{\gamma+1}{\gamma}}}{\gamma\inf_{x\in\left[F_j^{-1}\left(\varepsilon_j^{(\mathrm{L})}\right),F_j^{-1}\left(\varepsilon_j^{(\mathrm{U})}\right)\right]}f_j\left(x\right)}}_{\Xi_j}\left|\xi_j^{(K)}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right|,\end{aligned} \tag{62}$$

where (61) is due to the fact that $p_j(\boldsymbol{\theta}_{\mathrm{T}})\in[\varepsilon_j^{(\mathrm{L})},\varepsilon_j^{(\mathrm{U})}]$ and $\xi_j^{(K)}\in[\varepsilon_j^{(\mathrm{L})},\varepsilon_j^{(\mathrm{U})}]$. Since $f_j(x)$ is continuous and $0<f_j(x)<\infty$ over $\{x|F_j(x)\in(0,1)\}$, we know

$$\begin{aligned}&\inf_{x\in\left[F_j^{-1}\left(\varepsilon_j^{(\mathrm{L})}\right),F_j^{-1}\left(\varepsilon_j^{(\mathrm{U})}\right)\right]}f_j\left(x\right)\\&=\min_{x\in\left[F_j^{-1}\left(\varepsilon_j^{(\mathrm{L})}\right),F_j^{-1}\left(\varepsilon_j^{(\mathrm{U})}\right)\right]}f_j\left(x\right)\in(0,\infty),\end{aligned} \tag{63}$$

and moreover, from (59), we know

$$\tau_j-F_j^{-1}\left(\varepsilon_j^{(\mathrm{U})}\right)>0, \tag{64}$$

since $\varepsilon_j^{(\mathrm{U})}<F_j\left(\tau_j\right)$. Therefore, it is clear that $\Xi_j\in(0,\infty)$.

By employing (62), we can obtain

$$\begin{aligned}&\mathbb{P}_0\left(\left\{\left|D_j^{(K)}-D_j\right|\ge\frac{1}{2}\delta\right\}\cap\mathcal{F}_{j,K}\right)\\&\le\mathbb{P}_0\left(\left\{\Xi_j\left|\xi_j^{(K)}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right|\ge\frac{1}{2}\delta\right\}\cap\mathcal{F}_{j,K}\right)\\&\le\mathbb{P}_0\left(\xi_j^{(K)}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\ge\frac{\delta}{2\Xi_j}\right)\\&\qquad+\mathbb{P}_0\left(\xi_j^{(K)}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\le-\frac{\delta}{2\Xi_j}\right)\\&=\mathbb{P}_0\left(\sum_{k=1}^{K}\underbrace{\left(1-\tilde{u}_{jk}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)}_{X_{jk}}\ge\frac{\delta}{2\Xi_j}K\right)\\&\quad+\mathbb{P}_0\left(\sum_{k=1}^{K}\underbrace{\left(\tilde{u}_{jk}+p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)-1\right)}_{Y_{jk}}\ge\frac{\delta}{2\Xi_j}K\right).\end{aligned} \tag{65}$$

It is easy to see that under hypothesis $\mathcal{H}_0$, $\{X_{jk}\}_{k=1}^{K}$ is a sequence of independent and identically distributed random variables with distribution

$$q_{X_j}\triangleq\mathbb{P}_0\left(X_{jk}=1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)=p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right) \tag{66}$$

$$\bar{q}_{X_j}\triangleq\mathbb{P}_0\left(X_{jk}=-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)=1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right). \tag{67}$$

Since

$$\frac{\delta}{2\Xi_j}K>\mathbb{E}_0\left\{X_{jk}\right\}=\left[1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right]q_{X_j}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\bar{q}_{X_j}=0, \tag{68}$$

by employing the large deviations theory [20], we can obtain

$$\mathbb{P}_0\left(\sum_{k=1}^{K}\left(1-\tilde{u}_{jk}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)\geq\frac{\delta}{2\Xi_j}K\right)\leq e^{-\eta_{j,1}(\delta)K},\tag{69}$$

where the rate function $\eta_{j,1}(\delta)$ is defined as

$$\begin{aligned}\eta_{j,1}(\delta)&\triangleq-\lim_{K\to\infty}\frac{1}{K}\ln\mathbb{P}_0\left(\sum_{k=1}^{K}X_{jk}\geq\frac{\delta}{2\Xi_j}K\right)\\&=\frac{\delta}{2\Xi_j}\mu^*-\ln\phi_{X_j}\left(\mu^*\right),\end{aligned}\tag{70}$$

and $\phi_{X_j}(\mu)\triangleq\mathbb{E}_0\left\{e^{\mu X_{jk}}\right\}$

$$=p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)e^{\mu(1-p_j(\boldsymbol{\theta}_{\mathrm{T}}))}+\left(1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)e^{-\mu p_j(\boldsymbol{\theta}_{\mathrm{T}})}.\tag{71}$$

Moreover, the quantity μ^* in (70) is the solution of the equation

$$\frac{d}{d\mu}\phi_{X_j}(\mu)=\frac{\delta}{2\Xi_j}\phi_{X_j}(\mu).\tag{72}$$

By employing (70)–(72), the rate function $\eta_{j,1}(\delta)$ can be obtained as

$$\begin{aligned}\eta_{j,1}(\delta)&=\eta_{j,1}^*(\delta)\\&\triangleq\left(\frac{\delta}{2\Xi_j}+p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)\ln\frac{\left(\frac{\delta}{2\Xi_j}+p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)\left(1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)}{p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\left(1-\frac{\delta}{2\Xi_j}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)}\\&\quad-\ln\frac{1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)}{1-\frac{\delta}{2\Xi_j}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)},\end{aligned}\tag{73}$$

provided that

$$\frac{\delta}{2\Xi_j}\leq1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right).\tag{74}$$

It is seen from (66) and (67) that

$$\sum_{k=1}^{K}\left(1-\tilde{u}_{jk}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)\leq\left(1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)K,\tag{75}$$

which implies that for the case where $\frac{\delta}{2\Xi_j}>1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)$,

$$\mathbb{P}_0\left(\sum_{k=1}^{K}\left(1-\tilde{u}_{jk}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)\geq\frac{\delta}{2\Xi_j}K\right)=0.\tag{76}$$

Therefore, the rate function $\eta_{j,1}(\delta)$ can be written as[2]

$$\begin{aligned}\eta_{j,1}(\delta)&=\eta_{j,1}^*(\delta)\,\mathbb{1}\left\{\frac{\delta}{2\Xi_j}\leq1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right\}\\&\quad+\infty\mathbb{1}\left\{\frac{\delta}{2\Xi_j}>1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right\},\end{aligned}\tag{77}$$

where $\eta_{j,1}^*(\delta)$ is defined in (73).

Similarly, noting that under hypothesis $\mathcal{H}_0$, $\{Y_{jk}\}_{k=1}^{K}$ is a sequence of independent and identically distributed random variables with distribution

$$q_{X_j}\triangleq\mathbb{P}_0\left(Y_{jk}=p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)-1\right)=p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\tag{78}$$

$$\bar{q}_{X_j}\triangleq\mathbb{P}_0\left(Y_{jk}=p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)=1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right),\tag{79}$$

we can obtain

$$\mathbb{P}_0\left(\sum_{k=1}^{K}\left(\tilde{u}_{jk}+p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)-1\right)\geq\frac{\delta}{2\Xi_j}K\right)\leq e^{-\eta_{j,2}(\delta)K},\tag{80}$$

where the rate function $\eta_{j,2}(\delta)$ is given by

$$\begin{aligned}\eta_{j,2}(\delta)&=\eta_{j,2}^*(\delta)\,\mathbb{1}\left\{\frac{\delta}{2\Xi_j}\leq p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right\}\\&\quad+\infty\mathbb{1}\left\{\frac{\delta}{2\Xi_j}>p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right\}\end{aligned}\tag{81}$$

where $\eta_{j,2}^*(\delta)$ is defined as

$$\begin{aligned}&\eta_{j,2}^*(\delta)\\&\triangleq-\left(p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)-\frac{\delta}{2\Xi_j}\right)\ln\frac{p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\left(1+\frac{\delta}{2\Xi_j}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)}{\left(p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)-\frac{\delta}{2\Xi_j}\right)\left(1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)}\\&\quad+\ln\frac{1+\frac{\delta}{2\Xi_j}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)}{1-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)}.\end{aligned}\tag{82}$$

As a result, from (65), (69) and (80), we can obtain

$$\begin{aligned}&\mathbb{P}_0\left(\left\{\left|D_j^{(K)}-D_j\right|\geq\frac{1}{2}\delta\right\}\cap\mathcal{F}_{j,K}\right)\\&\leq e^{-\eta_{j,1}(\delta)K}+e^{-\eta_{j,2}(\delta)K},\end{aligned}\tag{83}$$

where $\eta_{j,1}(\delta)$ and $\eta_{j,2}(\delta)$ are defined in (77) and (81), respectively.

Now, we consider the second term in (60). From (12) and (59), we know

$$0<\varepsilon_j^{(\mathrm{L})}<p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)<\varepsilon_j^{(\mathrm{U})}<1,\tag{84}$$

and hence, by employing similar arguments, we can obtain

$$\begin{aligned}&\mathbb{P}_0\left(\mathcal{F}_{j,K}^{\mathrm{C}}\right)\\&=\mathbb{P}_0\left(\xi_j^{(K)}\notin\left[\varepsilon_j^{(\mathrm{L})},\varepsilon_j^{(\mathrm{U})}\right]\right)\\&=\mathbb{P}_0\left(\xi_j^{(K)}>\varepsilon_j^{(\mathrm{U})}\right)+\mathbb{P}_0\left(\xi_j^{(K)}<\varepsilon_j^{(\mathrm{L})}\right)\\&\leq\mathbb{P}_0\left(\xi_j^{(K)}\geq\varepsilon_j^{(\mathrm{U})}\right)+\mathbb{P}_0\left(\xi_j^{(K)}\leq\varepsilon_j^{(\mathrm{L})}\right)\\&=\mathbb{P}_0\left(\sum_{k=1}^{K}1-\tilde{u}_{jk}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\geq\left(\varepsilon_j^{(\mathrm{U})}-p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right)K\right)\\&\quad+\mathbb{P}_0\left(\sum_{k=1}^{K}\tilde{u}_{jk}+p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)-1\geq\left(p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)-\varepsilon_j^{(\mathrm{L})}\right)K\right)\\&\leq e^{-\eta_{\varepsilon_j^{(\mathrm{U})}}K}+e^{-\eta_{\varepsilon_j^{(\mathrm{L})}}K},\end{aligned}\tag{85}$$

[2] Regarding the second term of the right-hand side of (77), we define $\infty\cdot0=0$.

where the rate functions can be expressed as

$$\eta_{\varepsilon_j^{(\mathrm{U})}} = \varepsilon_j^{(\mathrm{U})} \ln \frac{\varepsilon_j^{(\mathrm{U})}\left(1-p_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)}{p_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\left(1-\varepsilon_j^{(\mathrm{U})}\right)} - \ln \frac{1-p_j\left(\boldsymbol{\theta}_\mathrm{T}\right)}{1-\varepsilon_j^{(\mathrm{U})}}, \quad (86)$$

$$\eta_{\varepsilon_j^{(\mathrm{L})}} = \ln \frac{1-\varepsilon_j^{(\mathrm{L})}}{1-p_j\left(\boldsymbol{\theta}_\mathrm{T}\right)} - \varepsilon_j^{(\mathrm{L})} \ln \frac{p_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\left(1-\varepsilon_j^{(\mathrm{L})}\right)}{\varepsilon_j^{(\mathrm{L})}\left(1-p_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)}. \quad (87)$$

It is worth noticing that $\eta_{\varepsilon_j^{(\mathrm{L})}}$ and $\eta_{\varepsilon_j^{(\mathrm{U})}}$ do not depend on δ.

As a result, from (60), (83) and (85), we know that for any $j \in \{1, 2, ..., N+2\}$, $\mathbb{P}_0(|\widehat{D}_j^{(K)} - D_j| \geq \frac{1}{2}\delta)$ can be bounded from above as per

$$\begin{aligned}&\mathbb{P}_0\left(\left|\widehat{D}_j^{(K)} - D_j\right| \geq \frac{1}{2}\delta\right)\\ &\quad \leq e^{-\eta_{j,1}(\delta)K} + e^{-\eta_{j,2}(\delta)K} + e^{-\eta_{\varepsilon_j^{(\mathrm{L})}}K} + e^{-\eta_{\varepsilon_j^{(\mathrm{U})}}K}, \quad (88)\end{aligned}$$

which yields an upper bound on the false alarm probability of the detector in (33)

$$\begin{aligned}&\mathbb{P}_0\left(\varpi_j\left(\delta\right)=1\right)\\ &\leq \sum_{i=j,N+1,N+2} e^{-\eta_{i,1}(\delta)K} + e^{-\eta_{i,2}(\delta)K} + e^{-\eta_{\varepsilon_i^{(\mathrm{U})}}K} + e^{-\eta_{\varepsilon_i^{(\mathrm{L})}}K}\\ &\leq 12 e^{-\eta_j^{(0)}(\delta)K}, \quad (89)\end{aligned}$$

where $\eta_j^{(0)}\left(\delta\right)$ is defined as

$$\eta_j^{(0)}(\delta) \triangleq \min_{i=j,N+1,N+2}\left\{\eta_{i,1}\left(\delta\right), \eta_{i,2}\left(\delta\right), \eta_{\varepsilon_i^{(\mathrm{L})}}, \eta_{\varepsilon_i^{(\mathrm{U})}}\right\}. \quad (90)$$

Next, we consider the upper bound on the miss detection probability as given in (54).

By employing (18) and following the steps for obtaining (77), (81), (86), (87) and (88), we can obtain

$$\begin{aligned}&\mathbb{P}_1\left(\left|D_j^{(K)} - \widetilde{D}_j\right| \geq \frac{1}{2}\delta\right)\\ &\quad \leq e^{-\tilde{\eta}_{j,1}(\delta)K} + e^{-\tilde{\eta}_{j,2}(\delta)K} + e^{-\tilde{\eta}_{\varepsilon_j^{(\mathrm{L})}}K} + e^{-\tilde{\eta}_{\varepsilon_j^{(\mathrm{U})}}K} \quad (91)\end{aligned}$$

where $\tilde{\eta}_{j,1}(\delta)$, $\tilde{\eta}_{j,2}(\delta)$, $\tilde{\eta}_{\varepsilon_j^{(\mathrm{L})}}$ and $\tilde{\eta}_{\varepsilon_j^{(\mathrm{U})}}$ can be expressed as

$$\begin{aligned}\tilde{\eta}_{j,1}\left(\delta\right) &= \tilde{\eta}_{j,1}^*\left(\delta\right)\mathbb{1}\left\{\frac{\delta}{2\Xi_j} \leq 1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right\}\\ &\quad + \infty\mathbb{1}\left\{\frac{\delta}{2\Xi_j} > 1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right\}, \quad (92)\end{aligned}$$

$$\begin{aligned}\tilde{\eta}_{j,2}\left(\delta\right) &= \tilde{\eta}_{j,2}^*\left(\delta\right)\mathbb{1}\left\{\frac{\delta}{2\Xi_j} \leq \tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right\}\\ &\quad + \infty\mathbb{1}\left\{\frac{\delta}{2\Xi_j} > \tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right\}, \quad (93)\end{aligned}$$

$$\tilde{\eta}_{\varepsilon_j^{(\mathrm{L})}} = \ln \frac{1-\varepsilon_j^{(\mathrm{L})}}{1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)} - \varepsilon_j^{(\mathrm{L})} \ln \frac{\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\left(1-\varepsilon_j^{(\mathrm{L})}\right)}{\varepsilon_j^{(\mathrm{L})}\left(1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)}. \quad (94)$$

$$\tilde{\eta}_{\varepsilon_j^{(\mathrm{U})}} = \varepsilon_j^{(\mathrm{U})} \ln \frac{\varepsilon_j^{(\mathrm{U})}\left(1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)}{\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\left(1-\varepsilon_j^{(\mathrm{U})}\right)} - \ln \frac{1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)}{1-\varepsilon_j^{(\mathrm{U})}}, \quad (95)$$

and $\tilde{\eta}_{j,1}^*\left(\delta\right)$ and $\tilde{\eta}_{j,2}^*\left(\delta\right)$ are defined as

$$\begin{aligned}\tilde{\eta}_{j,1}^*(\delta) &\triangleq \left(\frac{\delta}{2\Xi_j} + \tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right) \ln \frac{\left(\frac{\delta}{2\Xi_j} + \tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)\left(1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)}{\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\left(1-\frac{\delta}{2\Xi_j}-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)}\\ &\quad - \ln \frac{1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)}{1-\frac{\delta}{2\Xi_j}-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)}, \quad (96)\end{aligned}$$

$$\begin{aligned}\tilde{\eta}_{j,2}^*(\delta) &\triangleq -\left(\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right) - \frac{\delta}{2\Xi_j}\right) \ln \frac{\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\left(1+\frac{\delta}{2\Xi_j}-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)}{\left(\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)-\frac{\delta}{2\Xi_j}\right)\left(1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)\right)}\\ &\quad + \ln \frac{1+\frac{\delta}{2\Xi_j}-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)}{1-\tilde{p}_j\left(\boldsymbol{\theta}_\mathrm{T}\right)}. \quad (97)\end{aligned}$$

Moreover, noticing that

$$\begin{aligned}&\mathbb{P}_1\left(\left|\widehat{D}_{N+i}^{(K)} - D_{N+i}\right| \geq \frac{1}{2}\delta\right)\\ &\quad = \mathbb{P}_0\left(\left|\widehat{D}_{N+i}^{(K)} - D_{N+i}\right| \geq \frac{1}{2}\delta\right),\ i=1,2, \quad (98)\end{aligned}$$

by employing (54), (88) and (91), we can obtain

$$\begin{aligned}&\mathbb{P}_1\left(\varpi_j\left(\delta\right)=0\right)\\ &\leq e^{-\tilde{\eta}_{j,1}(\delta)K} + e^{-\tilde{\eta}_{j,2}(\delta)K} + e^{-\tilde{\eta}_{\varepsilon_j^{(\mathrm{L})}}K} + e^{-\tilde{\eta}_{\varepsilon_j^{(\mathrm{U})}}K}\\ &\quad + \sum_{i=N+1}^{N+2} e^{-\eta_{i,1}(\delta)K} + e^{-\eta_{i,2}(\delta)K} + e^{-\eta_{\varepsilon_i^{(\mathrm{U})}}K} + e^{-\eta_{\varepsilon_i^{(\mathrm{L})}}K}\\ &\leq 12 e^{-\eta_j^{(1)}(\delta)K}, \quad (99)\end{aligned}$$

where the quantity $\eta_j^{(1)}\left(\delta\right)$ is defined as

$$\begin{aligned}\eta_j^{(1)}\left(\delta\right) \triangleq \min_{i=N+1,N+2}\Big\{&\tilde{\eta}_{j,1}\left(\delta\right), \tilde{\eta}_{j,2}\left(\delta\right), \tilde{\eta}_{\varepsilon_j^{(\mathrm{L})}}, \tilde{\eta}_{\varepsilon_j^{(\mathrm{U})}},\\ &\eta_{i,1}\left(\delta\right), \eta_{i,2}\left(\delta\right), \eta_{\varepsilon_i^{(\mathrm{L})}}, \eta_{\varepsilon_i^{(\mathrm{U})}}\Big\}. \quad (100)\end{aligned}$$

■

As demonstrated by Theorem 3, the false alarm and miss probabilities of the proposed detector in (33) are guaranteed to decay exponentially as K increases. The decay rates are illustrated in (90) and (100) which depend on the choice of δ. In general, a smaller δ leads to a larger false alarm probability and a smaller miss probability. Hence, the trade-off between the false alarm and miss probabilities can be sought via altering the value of δ.

Using Theorem 3, the average detector error probability P_e can be bounded from above as per

$$\begin{aligned}P_\mathrm{e} &= \frac{1}{N}\sum_{j\in\mathcal{U}}\mathbb{P}_0\left(\varpi_j=1\right) + \frac{1}{N}\sum_{j\in\mathcal{V}}\mathbb{P}_1\left(\varpi_j=0\right)\\ &\leq \frac{12}{N}\sum_{j\in\mathcal{U}} e^{-\eta_j^{(0)}(\delta)K} + \frac{12}{N}\sum_{j\in\mathcal{V}} e^{-\eta_j^{(1)}(\delta)K}\\ &\leq C_\mathrm{e} e^{-\eta_\mathrm{e}(\delta)K}, \quad (101)\end{aligned}$$

where the positive constants C_{e} and $\eta_{\mathrm{e}}(\delta)$ are defined as

$$C_{\mathrm{e}} = 12 \text{ and } \eta_{\mathrm{e}}(\delta) \triangleq \min_{j=1,2,\ldots,N} \left\{\eta_j^{(0)}(\delta), \eta_j^{(1)}(\delta)\right\}. \quad (102)$$

This observation is summarized in the following corollary.

Corollary 1: If (52) holds, then the average detector error probability decreases at least exponentially as K increases.

It is worth pointing out that the sufficient condition on δ in Theorem 3 and Corollary 1 are generally not necessary, which is observed in all the numerical experiments that we carried out. In addition, the proposed detector in (33) can be generalized to the cases where arbitrary quantizers are employed at the sensors. The generalization only requires respective replacements of $\widehat{D}_j^{(K)}$, $\widehat{D}_{N+1}^{(K)}$ and $\widehat{D}_{N+2}^{(K)}$ in (33) by the corresponding NMLEs of D_j, D_{N+1} and D_{N+2} based on the quantizers employed, respectively.

It is also worth mentioning that the detection performance of the proposed approach may be able to be further improved by incorporating the other insecure sensors' data into the decision rule. However, since the states (attacked or unattacked) of the sensors are unknown, if the other insecure sensors' data is incorporated into the decision rule, then the computation of the test statistic may require an exhaustive search through all possible combinations of the states of the incorporated sensors, which is on the order of 2^N. In contrast, for checking the states of all the insecure sensors, the complexity of the proposed detection approach in (33) is on the order of N which is more amenable to implementation. In light of this, the proposed approach can be considered scalable with respect to the sensor network size.

V. Simulation Results

In this section, we first introduce how to implement the proposed attack detector in practice, and then we test the performance of the proposed attack detector to corroborate the theoretical results in previous sections.

A. Implementation of the Attack Detector

By employing (25), $\widehat{D}_j^{(K)}$, $\widehat{D}_{N+1}^{(K)}$ and $\widehat{D}_{N+2}^{(K)}$ can be computed, and thereby the analytical expression of $\mathcal{C}(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)})$ can be obtained. Note that every point $\boldsymbol{\theta}$ in the common area of $\mathcal{R}(\boldsymbol{\theta}_{N+1}, \widehat{D}_{N+1}^{(K)}, \delta)$ and $\mathcal{R}(\boldsymbol{\theta}_{N+2}, \widehat{D}_{N+2}^{(K)}, \delta)$ satisfies the condition

$$\begin{cases} -\delta \leq \|\boldsymbol{\theta} - \boldsymbol{\theta}_{N+1}\| - \widehat{D}_{N+1}^{(K)} \leq \delta, \\ -\delta \leq \|\boldsymbol{\theta} - \boldsymbol{\theta}_{N+2}\| - \widehat{D}_{N+2}^{(K)} \leq \delta. \end{cases} \quad (103)$$

Therefore, to implement the attack detector in (33), we only need to check whether any point on the circle $\mathcal{C}(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)})$ satisfies the condition in (103) or not.

One brute force way to do this is to discretize $\mathcal{C}(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)})$ to finitely many points which are evenly spaced along the circle, and then we check the condition in (103) for these points. In particular, we can discretize $\mathcal{C}(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)})$ to M points $\{\boldsymbol{\theta}_{\mathcal{C}}^{(m)}\}_{m=1}^{M}$ in the way that

$$\boldsymbol{\theta}_{\mathcal{C}}^{(m)} = \left[x_j + \widehat{D}_j^{(K)} \cos\left(\frac{2\pi}{M}(m-1)\right), \right. \\ \left. y_j + \widehat{D}_j^{(K)} \sin\left(\frac{2\pi}{M}(m-1)\right)\right], \quad (104)$$

where x_j and y_j are the coordinates of the j-th sensor. We summarize this implementation in Algorithm 1. Intuitively, we expect that this approach may not work well for small M.

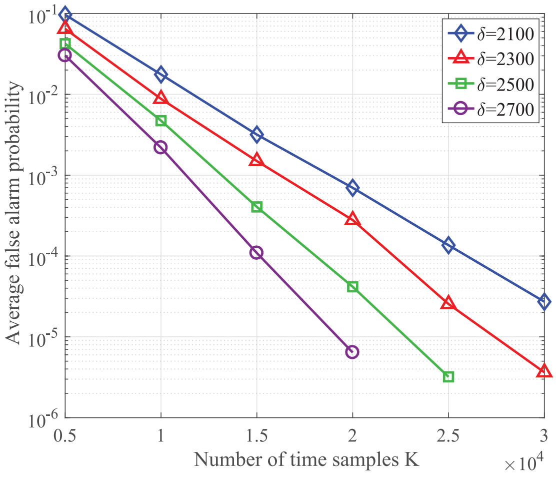


Fig. 7. Average false alarm probabilities for different δ.

Algorithm 1: Implementation of attack detector.

```
Input: $\{u_{ik}\}_{k=1}^{K}$ for $i = N+1, N+2$, $\{\tilde{u}_{jk}\}_{k=1}^{K}$, and $\delta$;
Output: $\varpi_j(\delta)$;
Compute $\widehat{D}_j^{(K)}$, $\widehat{D}_{N+1}^{(K)}$ and $\widehat{D}_{N+2}^{(K)}$ by employing (25);
Discretize $\mathcal{C}(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)})$ to $\{\boldsymbol{\theta}_{\mathcal{C}}^{(m)}\}_{m=1}^{M}$ by employing (104);
$m \leftarrow 1$ and $\varpi_j(\delta) \leftarrow 1$;
while $m \leq M$ and $\varpi_j(\delta) = 1$ do
    if $\boldsymbol{\theta}_{\mathcal{C}}^{(m)} \in \mathcal{S}$ and (103) holds then
        $\varpi_j(\delta) \leftarrow 0$;
    end if
    $m \leftarrow m + 1$;
end while
```

B. Simulation Setup

Consider a sensor network consisting of two groups of sensors with $N = 500$. The two secure sensors are located at $\boldsymbol{\theta}_{501} = [-10^3, 0]$ and $\boldsymbol{\theta}_{502} = [10^3, 0]$, respectively. The rest of sensors are all located along the x-axis, and are partitioned into two groups. The first group of sensors $\{1, 2, \ldots, 250, 501\}$ are evenly spaced along x-axis between $[-10^3, 0]$ and $[-0.9 \times 10^3, 0]$, while the second group of sensors $\{251, 252, \ldots, 500, 502\}$ are evenly spaced along x-axis between $[0.9 \times 10^3, 0]$ and $[10^3, 0]$. The ROI $\mathcal{A}$ is a disc centered at $[0, 10^5]$ and with radius equal to 7500. The target is located at $\boldsymbol{\theta}_{\mathrm{T}} = [0, 10^5]$. In the simulation, $P_0 = 1$, $D_0 = 10^5$, and $\gamma = 2$. When employing Algorithm 1 to implement the attack detector, M is chosen to be 5×10^5. In addition, the threshold $\tau_j = 1$ for all j, and n_{jk} follows a Gaussian distribution with zero mean and unit variance.

C. Attack Detection Performance

We assume that 250 sensors $\{1, 2, \ldots, 250\}$ are under the MiMA as described in (19) with $\psi_{j,0} = 0$ and $\psi_{j,1} = 0.06$ for $j = 1, 2, \ldots, 250$. The average false alarm probability and the average miss probability over 2500 Monte Carlo runs versus the number K of data samples are depicted on a log scale in Fig. 7 and Fig. 8 for four detectors with $\delta = 2100, 2300, 2500, 2700$,

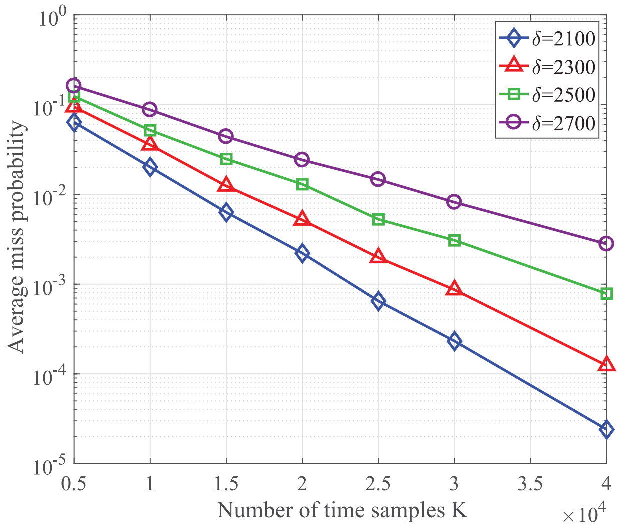


Fig. 8. Average miss probabilities for different δ.

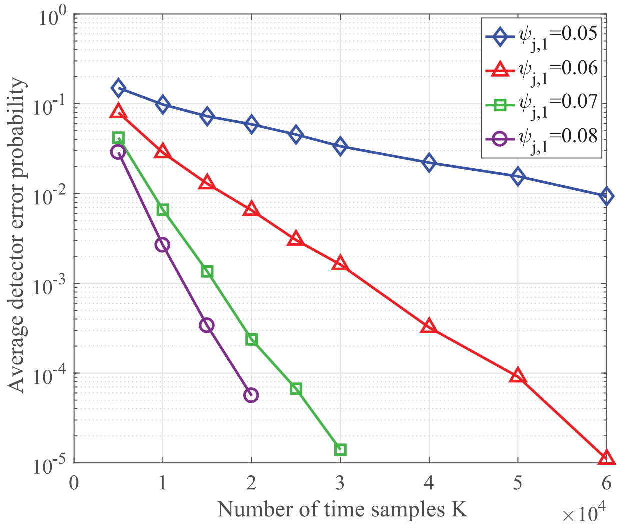


Fig. 9. Attack detection performance of the proposed detector under different attacks.

respectively. It is seen from Fig. 7 and Fig. 8 that for each detector, the average false alarm probability and the average miss probability decrease exponentially as K grows which agrees with the theoretical results in the previous section. Moreover, as illustrated in Fig. 7, the larger the value of δ, the smaller the average false alarm probability. On the other hand, it is seen from Fig. 8 that the larger the value of δ, the larger the average miss probability. Thus, the trade-off between the false alarm and miss probabilities can be sought via adjusting the value of δ.

Now, we consider the attack detection performance of the proposed detector under different attacks. In Fig. 9, $\delta = 2500$, the number of Monte Carlo runs is 2000, and the different attacks are all MiMA and for $j = 1, 2, ..., 250$, $[\psi_{j,0}, \psi_{j,1}] = [0, 0.05]$, $[0, 0.06]$, $[0, 0.07]$ and $[0, 0.08]$, respectively. As expected from the intuition that the attack which brings about a larger impact on the statistical model of the data should be easier to be detected, Fig. 9 demonstrates that the larger the value of $\psi_{j,1}$, the smaller the average detector error probability. It is worth mentioning that under different attacks, the false alarm probabilities achieved by the detector should be the same. Therefore, for different attacks, the difference in the average detector error probabilities is mainly determined by the difference in the average miss probabilities.

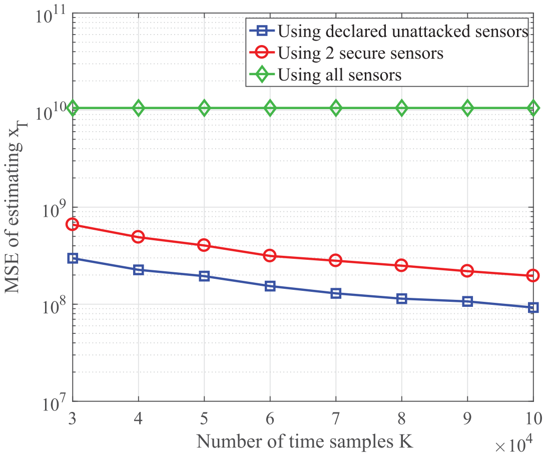


Fig. 10. MSE performance of estimating x_{T}.

D. Localization Performance Improvement after Detecting Attacks

In this subsection, we consider the performance improvement in estimating the location of the target with the help of the proposed attack detectors in (33). In particular, we consider the maximum likelihood estimator (MLE) of $\boldsymbol{\theta}_{\mathrm{T}}$ which can be expressed as

$$(\hat{x}_{\mathrm{T}}, \hat{y}_{\mathrm{T}}) = \hat{\boldsymbol{\theta}}_{\mathrm{T}} \triangleq \arg \max_{\boldsymbol{\theta}_{\mathrm{T}}} \sum_{j \in \mathcal{W}} \left\{ \sum_{k=1}^{K} (1 - \tilde{u}_{jk}) \ln p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right) + \sum_{k=1}^{K} \tilde{u}_{jk} \ln\left[1 - p_j\left(\boldsymbol{\theta}_{\mathrm{T}}\right)\right] \right\}, \quad (105)$$

where $p_j(\boldsymbol{\theta}_{\mathrm{T}})$ is defined in (9) and $\mathcal{W}$ denotes the set of sensors whose data are employed for estimating $\boldsymbol{\theta}_{\mathrm{T}}$.

We assume that 250 sensors $\{1, 2, ..., 250\}$ are under the MiMA as described in (19) with $\psi_{j,0} = 0$ and $\psi_{j,1} = 0.08$ for $j = 1, 2, ..., 250$. Given the page limits, we just present the numerical results on the performance of estimating x_{T}. The performance of estimating y_{T} is similar. Fig. 10 illustrates the mean square error (MSE) performance of the estimator in (105) on a log scale for three cases where all sensors are employed, i.e., $\mathcal{W} = \{1, 2, ..., 502\}$, only two secure sensors are employed, i.e., $\mathcal{W} = \{501, 502\}$, and $\mathcal{W}$ consists of the two secure sensors and the sensors which are declared as unattacked by the proposed detector in (33) with $\delta = 2500$, respectively. In addition, the biases of the estimators in estimating x_{T} are depicted in Fig. 11. It is seen from Fig. 11 that the bias for the case where all sensors are employed is very large, since the attacked data are employed by the estimator which mismatch the model specified in (105). In contrast, the biases for the other two cases are very close to 0 which agree with the asymptotic property of the MLE. Fig. 10 shows that the MSE performance for the case where all sensors are employed is very large due to the large bias. Furthermore, the MSE performance for the case where the two secure sensors and the sensors which are declared as unattacked are employed is smaller than that for the case where only the two secure sensors are employed, which are depicted by the blue and red curves, respectively. This is because, as illustrated by Fig. 9, the error

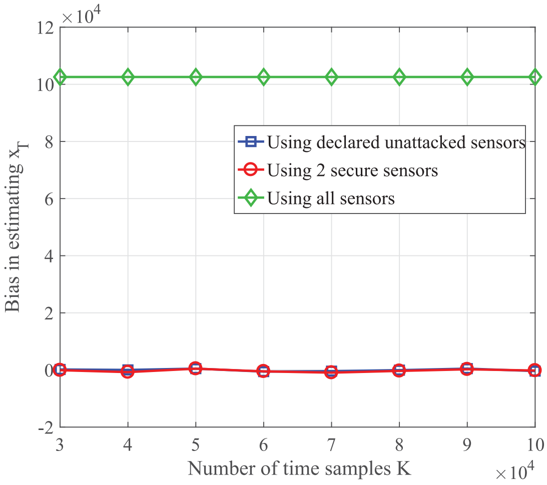


Fig. 11. Bias in estimating x_{T}.

probability of the proposed detector is almost zero for the range of K considered in Fig. 10, and therefore, more unattacked sensors are employed in the blue curve. Thus, it is no wonder that the blue curve outperforms the red one in Fig. 10.

VI. Conclusions

This work has investigated the attack detection in sensor network target localization systems with quantized data. By exploring the impact of the attacks on the statistical model of the sensor data, we have revealed that from the perspective of the NMLE, the essential effect of attacks is a falsification of the estimated distance between the target and each attacked sensor, and hence, gives rise to a geometric inconsistency among the attacked and unattacked sensors. Motivated by this fact, a class of detectors are proposed to detect the attacks in the sensor network via scrutinizing the existence of the geometric inconsistency. A rigorous detection performance analysis for the proposed detectors has been carried out, showing that the false alarm and miss probabilities decay exponentially as the number of data samples at each sensor grows, which implies that for a sufficiently large number of samples, the proposed detectors can identify the attacked sensors with any required level of accuracy. It is worth mentioning that the detection performance of the proposed approach may be able to be further improved by incorporating other sensors's data into the decision rule, which will be considered in future work.

Appendix A
Proof of Lemma 1

Consider R_{N+1} and R_{N+2} which satisfy

$$|R_i - D_i| \le \delta < \Upsilon, \quad \text{for } i = N+1, N+2, \tag{106}$$

and denote

$$\boldsymbol{\theta}'_{\mathrm{T}} \triangleq \mathcal{C}(\boldsymbol{\theta}_{N+1}, R_{N+1}) \cap \mathcal{C}(\boldsymbol{\theta}_{N+2}, R_{N+2}). \tag{107}$$

From (7) and (106), we know that

$$\begin{aligned} R_{N+1} + R_{N+2} &\ge D_{N+1} + D_{N+2} - 2\delta \\ &> \inf_{\boldsymbol{\theta}_{\mathrm{T}} \in \mathcal{A}} \{D_{N+1} + D_{N+2}\} - 2\Upsilon_2 = D_{\mathrm{S}}, \end{aligned} \tag{108}$$

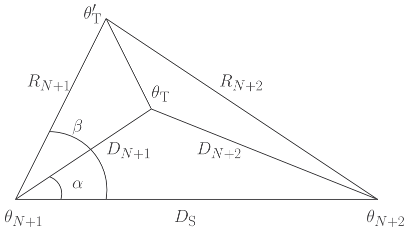


Fig. 12. Geometric illustration.

and moreover, by employing (6) and (106), we can obtain

$$\begin{aligned} |R_{N+1} - R_{N+2}| &< |D_{N+1} - D_{N+2}| + 2\delta < D_{\mathrm{U}} - D_{\mathrm{L}} + 2\Upsilon \\ &\le D_{\mathrm{U}} - D_{\mathrm{L}} + 2\Upsilon_1 < D_{\mathrm{S}}. \end{aligned} \tag{109}$$

Thus, R_{N+1}, R_{N+2} and D_{S} can be the sides of a triangle, and hence, $\boldsymbol{\theta}'_{\mathrm{T}}$ exists and cannot be on the line passing through $\boldsymbol{\theta}_{N+1}$ and $\boldsymbol{\theta}_{N+2}$, which implies that the angle $\beta \triangleq \angle \boldsymbol{\theta}'_{\mathrm{T}} \boldsymbol{\theta}_{N+1} \boldsymbol{\theta}_{N+2}$ in Fig. 12 satisfies $\beta \in (0, \pi)$.

Let α denote the angle $\angle \boldsymbol{\theta}_{\mathrm{T}} \boldsymbol{\theta}_{N+1} \boldsymbol{\theta}_{N+2}$ as illustrated in Fig. 12. By the law of cosines, we can obtain

$$\begin{aligned} d(R_{N+1}, R_{N+2}) &\triangleq \|\boldsymbol{\theta}'_{\mathrm{T}} - \boldsymbol{\theta}_{\mathrm{T}}\| \\ &= \sqrt{R_{N+1}^2 + D_{N+1}^2 - 2R_{N+1}D_{N+1}\cos(\beta - \alpha)}. \end{aligned} \tag{110}$$

According to Assumption 1, we know

$$D_{\mathrm{S}} > |D_{N+1} - D_{N+2}| \text{ and } D_{N+1} + D_{N+2} > D_{\mathrm{S}}, \tag{111}$$

which yields $\alpha \in (0, \pi)$, and hence,

$$\beta - \alpha \in (-\pi, \pi). \tag{112}$$

From (110), we know that for any given R_{N+1}, $d(R_{N+1}, R_{N+2})$ is maximized when $\cos(\beta - \alpha)$ is minimized. Since α is fixed and $\beta - \alpha \in (-\pi, \pi)$, $\cos(\beta - \alpha)$ is minimized when β is either maximized or minimized, which implies that $d(R_{N+1}, R_{N+2})$ is maximized when β is either maximized or minimized.

Furthermore, by the law of cosines, we can obtain

$$\cos(\beta) = \frac{R_{N+1}^2 + D_{\mathrm{S}}^2 - R_{N+2}^2}{2R_{N+1}D_{\mathrm{S}}}. \tag{113}$$

Since $\beta \in (0, \pi)$ and $\cos(\beta)$ is decreasing over $\beta \in (0, \pi)$, for any given R_{N+1}, β is maximized if R_{N+2} is maximized, while β is minimized if R_{N+2} is minimized. Therefore, for any given R_{N+1}, $d(R_{N+1}, R_{N+2})$ is maximized only when $R_{N+2} = D_{N+2} + \delta$ or $R_{N+2} = D_{N+2} - \delta$, since $|R_{N+2} - D_{N+2}| \le \delta$.

Similarly, for any given R_{N+2}, $d(R_{N+1}, R_{N+2})$ is maximized only when $R_{N+1} = D_{N+1} + \delta$ or $R_{N+1} = D_{N+1} - \delta$.

Thus, for any given R_{N+1} and R_{N+2} satisfying (106), the maximal $d(R_{N+1}, R_{N+2})$ can only be achieved when $R_{N+1} \in \{D_{N+1} - \delta, D_{N+1} + \delta\}$ and $R_{N+2} \in \{D_{N+2} - \delta, D_{N+2} + \delta\}$. To this end, in order to prove $\cap_{i=1}^{2} \mathcal{R}(\boldsymbol{\theta}_{N+i}, D_{N+i}, \delta) \subseteq \mathcal{B}(\boldsymbol{\theta}_{\mathrm{T}}, \Phi(\delta))$, we only need to consider

$$R_{N+1} \in \{D_{N+1} - \delta, D_{N+1} + \delta\}, \tag{114}$$

$$R_{N+2} \in \{D_{N+2} - \delta, D_{N+2} + \delta\}, \tag{115}$$

and show $\boldsymbol{\theta}'_{\mathrm{T}} \in \mathcal{B}(\boldsymbol{\theta}_{\mathrm{T}}, \Phi(\delta))$.

Without loss of generality, we assume that $\boldsymbol{\theta}_{N+1} = \mathbf{0}$, $\boldsymbol{\theta}_{N+2} = (D_{\rm S}, 0)$, and $\boldsymbol{\theta}_{\rm T}$ is in the half space above the line passing through $\boldsymbol{\theta}_{N+1}$ and $\boldsymbol{\theta}_{N+2}$. Since $\boldsymbol{\theta}_{\rm T} \triangleq \mathcal{C}(\boldsymbol{\theta}_{N+1}, D_{N+1}) \cap \mathcal{C}(\boldsymbol{\theta}_{N+2}, D_{N+2})$, we can obtain

$$\begin{cases} x_{\rm T}^2 + y_{\rm T}^2 = D_{N+1}^2, \\ (x_{\rm T} - D_{\rm S})^2 + y_{\rm T}^2 = D_{N+2}^2, \end{cases} \tag{116}$$

which yields

$$\begin{cases} x_{\rm T} = \frac{D_{N+1}^2 - D_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}, \\ y_{\rm T} = \sqrt{D_{N+1}^2 - \left(\frac{D_{N+1}^2 - D_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}\right)^2}. \end{cases} \tag{117}$$

Similarly, with regard to $\boldsymbol{\theta}'_{\rm T} = (x'_{\rm T}, y'_{\rm T}) = \mathcal{C}(\boldsymbol{\theta}_{N+1}, R_{N+1}) \cap \mathcal{C}(\boldsymbol{\theta}_{N+2}, R_{N+2})$, we also can obtain

$$\begin{cases} x'_{\rm T} = \frac{R_{N+1}^2 - R_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}, \\ y'_{\rm T} = \sqrt{R_{N+1}^2 - \left(\frac{R_{N+1}^2 - R_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}\right)^2}. \end{cases} \tag{118}$$

By employing (117) and (118), $d(R_{N+1}, R_{N+2})^2$ can be expressed as

$$\begin{aligned} &d(R_{N+1}, R_{N+2})^2 \\ &= \underbrace{\left(\frac{R_{N+1}^2 - R_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}} - \frac{D_{N+1}^2 - D_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}\right)^2}_{d_x} + d_y, \end{aligned} \tag{119}$$

where d_y is defined as

$$\begin{aligned} d_y \triangleq \Bigg[&\sqrt{R_{N+1}^2 - \left(\frac{R_{N+1}^2 - R_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}\right)^2} \\ &- \sqrt{D_{N+1}^2 - \left(\frac{D_{N+1}^2 - D_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}\right)^2}\Bigg]^2. \end{aligned} \tag{120}$$

From (114) and (115), d_x can be bounded from above as per

$$\begin{aligned} d_x &= \left(\frac{R_{N+1}^2 - D_{N+1}^2 + D_{N+2}^2 - R_{N+2}^2}{2D_{\rm S}}\right)^2 \\ &= \Bigg[\frac{(R_{N+1} - D_{N+1})(R_{N+1} + D_{N+1})}{2D_{\rm S}} \\ &\qquad + \frac{(D_{N+2} - R_{N+2})(D_{N+2} + R_{N+2})}{2D_{\rm S}}\Bigg]^2 \\ &\le \frac{1}{D_{\rm S}^2}\delta^2 (D_{N+1} + D_{N+2} + \delta)^2 \\ &\le \frac{1}{D_{\rm S}^2}(2D_{\rm U} + \delta)^2 \delta^2. \end{aligned} \tag{121}$$

Moreover, by using the fact that $\sqrt{|x|} - \sqrt{|y|} \le \sqrt{|x - y|}$ for any x and y, d_y can be bounded from above as per

$$\begin{aligned} d_y &\le \Bigg|R_{N+1}^2 - \left(\frac{R_{N+1}^2 - R_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}\right)^2 \\ &\qquad - D_{N+1}^2 + \left(\frac{D_{N+1}^2 - D_{N+2}^2 + D_{\rm S}^2}{2D_{\rm S}}\right)^2\Bigg| \\ &\le |(R_{N+1} - D_{N+1})(R_{N+1} + D_{N+1})| \\ &\quad + \Bigg|\frac{R_{N+1}^2 - R_{N+2}^2 - D_{N+1}^2 + D_{N+2}^2}{2D_{\rm S}} \\ &\qquad \times \frac{R_{N+1}^2 - R_{N+2}^2 + D_{N+1}^2 - D_{N+2}^2 + 2D_{\rm S}^2}{2D_{\rm S}}\Bigg|. \end{aligned} \tag{122}$$

By employing (114), (115) and (122), we can obtain

$$\begin{aligned} d_y &\le \delta(2D_{N+1} + \delta) + \frac{|R_{N+1}^2 - D_{N+1}^2| + |R_{N+2}^2 - D_{N+2}^2|}{4D_{\rm S}^2} \\ &\qquad \times \left(|R_{N+1}^2 - D_{N+2}^2| + |R_{N+2}^2 - D_{N+1}^2| + 2D_{\rm S}^2\right) \\ &\le \delta(2D_{N+1} + \delta) + \frac{\delta(2D_{N+1} + \delta) + \delta(2D_{N+2} + \delta)}{4D_{\rm S}^2} \\ &\qquad \times \Big[|(R_{N+1} - D_{N+2})(R_{N+1} + D_{N+2})| \\ &\qquad\quad + |(R_{N+2} - D_{N+1})(R_{N+2} + D_{N+1})| + 2D_{\rm S}^2\Big] \\ &\le \delta(2D_{N+1} + \delta) + \frac{\delta(D_{N+1} + D_{N+2} + \delta)}{D_{\rm S}^2} \\ &\qquad \times \left[(|D_{N+1} - D_{N+2}| + \delta)(D_{N+1} + D_{N+2} + \delta) + D_{\rm S}^2\right] \end{aligned} \tag{123}$$

$$\begin{aligned} &\le \delta(2D_{N+1} + \delta) + \delta(2D_{\rm U} + \delta) \\ &\qquad \times \left[\frac{(D_{\rm U} - D_{\rm L} + \delta)(D_{N+1} + D_{N+2} + \delta)}{D_{\rm S}^2} + 1\right] \\ &\le \delta(2D_{\rm U} + \delta) + \delta(2D_{\rm U} + \delta)\left(\frac{2D_{\rm U} + \delta}{D_{\rm S}} + 1\right) \end{aligned} \tag{124}$$

$$\le (2D_{\rm U} + \delta)\left(\frac{2D_{\rm U} + \delta}{D_{\rm S}} + 2\right)\delta, \tag{125}$$

where (123) is from (106), and (124) is due to $D_{N+1} \le D_{\rm U}$ and Assumption 1 that $D_{\rm S} > D_{\rm U} - D_{\rm L} + 2\Upsilon > D_{\rm U} - D_{\rm L} + \delta$, since $\delta < \Upsilon$.

From (119), (121) and (125), we can obtain

$$\begin{aligned} &d(R_{N+1}, R_{N+2})^2 \\ &\le \frac{1}{D_S^2}(2D_U + \delta)^2\delta^2 + (2D_U + \delta)\left(\frac{2D_U + \delta}{D_S} + 2\right)\delta \end{aligned}$$

$$\begin{aligned}&\leq (2D_U + \delta)\left[\frac{2D_U+\delta}{D_S}\left(\frac{\delta}{D_S}+1\right)+2\right]\delta\\&< (2D_U + \Upsilon)\left[\frac{2D_U+\Upsilon}{D_S}\left(\frac{\Upsilon}{D_S}+1\right)+2\right]\delta, \qquad (126)\end{aligned}$$

which implies

$$\begin{aligned}&d(R_{N+1}, R_{N+2})\\&< (2D_U+\Upsilon)^{\frac{1}{2}}\left[\frac{2D_U+\Upsilon}{D_S}\left(\frac{\Upsilon}{D_S}+1\right)+2\right]^{\frac{1}{2}}\sqrt{\delta}, \quad (127)\end{aligned}$$

and therefore,

$$\boldsymbol{\theta}'_{\mathrm{T}} \in \mathcal{B}(\boldsymbol{\theta}_{\mathrm{T}}, \Phi(\delta)). \qquad (128)$$

Moreover, note that $\mathcal{B}(\boldsymbol{\theta}_{\mathrm{T}}, \delta) \subset \mathcal{R}(\boldsymbol{\theta}_{N+1}, D_{N+1}, \delta)$ and $\mathcal{B}$ $(\boldsymbol{\theta}_{\mathrm{T}}, \delta) \subset \mathcal{R}(\boldsymbol{\theta}_{N+2}, D_{N+2}, \delta)$, and hence $\mathcal{B}(\boldsymbol{\theta}_{\mathrm{T}}, \delta) \subseteq \cap_{i=1}^{2}\mathcal{R}$ $(\boldsymbol{\theta}_{N+i}, D_{N+i}, \delta)$. This completes the proof.

Appendix B
Proof of Lemma 2

By employing (36) and (52), we can obtain

$$\begin{aligned}&\Phi\left(\frac{3}{2}\delta\right)+\frac{1}{2}\delta\\&=(2D_U+\Upsilon)^{\frac{1}{2}}\left[\frac{2D_U+\Upsilon}{D_S}\left(\frac{\Upsilon}{D_S}+1\right)+2\right]^{\frac{1}{2}}\sqrt{\frac{3}{2}\delta}+\frac{1}{2}\delta\\&<\left\{(2D_U+\Upsilon)^{\frac{1}{2}}\left[\frac{6D_U+3\Upsilon}{2D_S}\left(\frac{\Upsilon}{D_S}+1\right)+3\right]^{\frac{1}{2}}+\frac{1}{2}\Upsilon^{\frac{1}{2}}\right\}\sqrt{\delta}\\&<\lambda, \qquad (129)\end{aligned}$$

and hence, $\Phi(\frac{3}{2}\delta) < \lambda$.

Furthermore, from (27), (50) and (51), we can obtain that

$$\begin{aligned}&\left|\widetilde{D}_j - D_j\right|\\&= D_0 P_0^{\frac{1}{\gamma}}\left|\left[\tau_j - F_j^{-1}(\tilde{p}_j(\boldsymbol{\theta}_{\mathrm{T}}))\right]^{-\frac{1}{\gamma}} - \left[\tau_j - F_j^{-1}(p_j(\boldsymbol{\theta}_{\mathrm{T}}))\right]^{-\frac{1}{\gamma}}\right|\\&\geq D_0 P_0^{\frac{1}{\gamma}} \inf_{x\in\left[\rho_j^{(\mathrm{L})}, \rho_j^{(\mathrm{U})}\right]}\left|\frac{\partial\left[\tau_j - F_j^{-1}(x)\right]^{-\frac{1}{\gamma}}}{\partial x}\right|\\&\quad\times\left|\tilde{p}_j(\boldsymbol{\theta}_{\mathrm{T}}) - p_j(\boldsymbol{\theta}_{\mathrm{T}})\right| \qquad (130)\\&= \frac{D_0 P_0^{\frac{1}{\gamma}}}{\gamma}\inf_{x\in\left[\rho_j^{(\mathrm{L})}, \rho_j^{(\mathrm{U})}\right]}\left|\frac{\left[\tau_j - F_j^{-1}(x)\right]^{-\frac{\gamma+1}{\gamma}}}{f_j\left(F_j^{-1}(x)\right)}\right|\\&\quad\times\left|\tilde{p}_j(\boldsymbol{\theta}_{\mathrm{T}}) - p_j(\boldsymbol{\theta}_{\mathrm{T}})\right|\\&\geq \frac{\kappa D_0 P_0^{\frac{1}{\gamma}}\left[\tau_j - F_j^{-1}\left(\rho_j^{(\mathrm{L})}\right)\right]^{-\frac{\gamma+1}{\gamma}}}{\gamma \sup_{x\in\left[F_j^{-1}(\rho_j^{(\mathrm{L})}), F_j^{-1}(\rho_j^{(\mathrm{U})})\right]} f_j(x)} \qquad (131)\\&> \lambda, \qquad (132)\end{aligned}$$

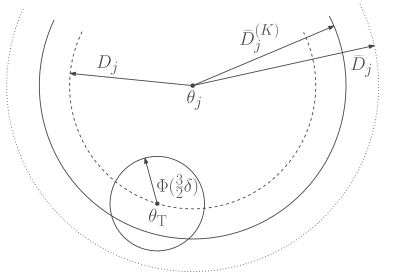


Fig. 13. Geometric illustration of (135).

where (130) is due to (12) and (22), and (131) is from (23). Thus, we know

$$\mathcal{C}\left(\boldsymbol{\theta}_j, \widetilde{D}_j\right) \cap \mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}}, \Phi\left(\frac{3}{2}\delta\right)\right) = \emptyset, \qquad (133)$$

since $\boldsymbol{\theta}_{\mathrm{T}} \in \mathcal{C}(\boldsymbol{\theta}_j, D_j)$ and $\Phi(\frac{3}{2}\delta) < \lambda$.

As illustrated in Fig. 13, if

$$\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}}, \Phi\left(\frac{3}{2}\delta\right)\right) \neq \emptyset, \qquad (134)$$

then

$$\left|\widehat{D}_j^{(K)} - \widetilde{D}_j\right| \geq \left|\widetilde{D}_j - D_j\right| - \Phi\left(\frac{3}{2}\delta\right), \qquad (135)$$

which implies

$$\left|\widehat{D}_j^{(K)} - \widetilde{D}_j\right| \geq \lambda - \Phi\left(\frac{3}{2}\delta\right) > \frac{1}{2}\delta, \qquad (136)$$

by employing (129) and (132). Therefore,

$$\begin{aligned}&\mathbb{P}_1\left(\mathcal{C}\left(\boldsymbol{\theta}_j, \widehat{D}_j^{(K)}\right) \cap \mathcal{B}\left(\boldsymbol{\theta}_{\mathrm{T}}, \Phi\left(\frac{3}{2}\delta\right)\right) \neq \emptyset\right)\\&\leq \mathbb{P}_1\left(\left|\widehat{D}_j^{(K)} - \widetilde{D}_j\right| \geq \frac{1}{2}\delta\right), \qquad (137)\end{aligned}$$

which completes the proof.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] L. M. Kaplan, Q. Le, and N. Molnar, “Maximum likelihood methods for bearings-only target localization,” in *Proc. Int. Conf. Acoust., Speech, Signal Process.*, Salt Lake City, UT, USA, May 2001, vol. 5, pp. 3001–3004.

[3] Y. Shen and M. Z. Win, “Fundamental limits of wideband localization—Part I: A general framework,” *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 4956–4980, Oct. 2010.

[4] A. Vempaty, Y. S. Han, and P. K. Varshney, “Target localization in wireless sensor networks using error correcting codes,” *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 697–712, Jan. 2014.

[5] R. Niu and P. K. Varshney, “Target location estimation in sensor networks with quantized data,” *IEEE Trans. Signal Process.*, vol. 54, no. 12, pp. 4519–4528, Dec. 2006.

[6] O. Ozdemir, R. Niu, and P. K. Varshney, “Channel aware target localization with quantized data in wireless sensor networks,” *IEEE Trans. Signal Process.*, vol. 57, no. 3, pp. 1190–1202, Mar. 2009.

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

[8] Z. Li, W. Trappe, Y. Zhang, and B. Nath, “Robust statistical methods for securing wireless localization in sensor networks,” in *Proc. Int. Workshop Inf. Process. Sens. Netw.*, Apr. 2005, pp. 91–98.

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

[10] 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, Sep. 2012.

[11] 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, Sep. 2013.

[12] 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.

[13] 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.

[14] J. Zhang and R. S. Blum, "Distributed joint spoofing attack identification and estimation in sensor networks," in *Proc. IEEE China Summit Int. Conf. Signal Inf. Process.*, 2015, pp. 701–705.

[15] 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, Feb. 2017.

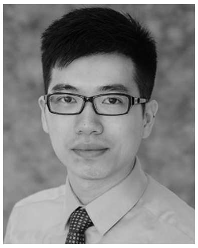
[16] A. Boukerche, H. Oliveira, E. F. Nakamura, and A. A. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 96–101, Apr. 2008.

[17] L. M. Huie and M. L. Fowler, "Strategies for information injection for networks estimating emitter location," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 51, no. 3, pp. 1597–1608, Jul. 2015.

[18] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 221–232, Feb. 2006.

[19] W. T. Zhu, Y. Xiang, J. Zhou, R. H. Deng, and F. Bao, "Secure localization with attack detection in wireless sensor networks," *Int. J. Inf. Security*, vol. 10, no. 3, pp. 155–171, 2011.

[20] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*, 2nd ed. New York, NY, USA: Springer-Verlag, 2009.



Jiangfan Zhang (S'10–M'17) received the B.Eng. degree in communication engineering from the 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, PA, USA, in 2016.

He is currently a Postdoctoral Research Scientist with the Department of Electrical Engineering, Columbia University in the City of New York, New York, NY, USA. His research interests include signal processing for cyber-physical systems, Internet of Things/sensor networks, cybersecurity, smart grid, radar, and sonar processing.

Dr. Zhang is a recipient of the Dean's Doctoral Student Assistantship, Gotshall Fellowship, and a P. C. Rossin Doctoral Fellow at Lehigh University.

Xiaodong Wang (S'98–M'98–SM'04–F'08) received the Ph.D degree in electrical engineering from Princeton University, Princeton, NJ, USA. He is currently a Professor of electrical engineering with Columbia University, New York. His research interests include the general areas of computing, signal processing, and communications, and has authored/coauthored extensively in these areas. Among his publications, he authored the book entitled *Wireless Communication Systems: Advanced Techniques for Signal Reception* (Prentice-Hall, 2003). His current research interests include wireless communications, statistical signal processing, and genomic signal processing. He received the 1999 NSF CAREER Award, the 2001 IEEE Communications Society and Information Theory Society Joint Paper Award, and the 2011 IEEE Communication Society Award for Outstanding Paper on New Communication Topics. He has served as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON SIGNAL PROCESSING, and the IEEE TRANSACTIONS ON INFORMATION THEORY. He is listed as an ISI highly cited author.

Rick S. Blum (S'83–M'84–SM'94–F'05) received the B.S. degree in electrical engineering from Pennsylvania State University, State College, PA, USA, in 1984, and the M.S. and Ph.D. degrees in electrical engineering from the University of Pennsylvania, Philadelphia, PA, USA, in 1987 and 1991, respectively. He also received the Graduate degree from GE's Advanced Course in Engineering.

From 1984 to 1991, he was a member of technical staff with General Electric Aerospace, Valley Forge, Pennsylvania. Since 1991, he has been with the Electrical and Computer Engineering Department, Lehigh University, Bethlehem, PA, USA, where he is currently a Professor and holds the Robert W. Wieseman Chaired Research Professorship in electrical engineering. He is on the editorial board for the *Journal of Advances in Information Fusion* of the International Society of Information Fusion. He was an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING and for the IEEE COMMUNICATIONS LETTERS. He has edited special issues for the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, and the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is a member of the SAM Technical Committee (TC) of the IEEE Signal Processing Society. He was a member of the Signal Processing for Communications TC of the IEEE Signal Processing Society and is a member of the Communications Theory TC of the IEEE Communication Society. He was on the Awards Committee of the IEEE Communication Society. His research interests include signal processing for smart grid, communications, sensor networking, radar and sensor processing.

Dr. Blum is a former IEEE Signal Processing Society Distinguished Lecturer, an IEEE Third Millennium Medal Winner, a member of Eta Kappa Nu and Sigma Xi, and holds several patents. He was a recipient of an ONR Young Investigator Award and an NSF Research Initiation Award. His IEEE Fellow Citation "for scientific contributions to detection, data fusion, and signal processing with multiple sensors" acknowledges contributions to the field of sensor networking.

Lance M. Kaplan (S'88–M'89–SM'00–F'16) received the B.S. degree with distinction from Duke University, Durham, NC, USA, in 1989, and the M.S. and Ph.D. degrees from the University of Southern California, Los Angeles, CA, USA, in 1991 and 1994, respectively, all in electrical engineering. From 1987 to 1990, he was a Technical Assistant with the Georgia Tech Research Institute. He held a National Science Foundation Graduate Fellowship and a USC Dean's Merit Fellowship from 1990 to 1993, and was a Research Assistant with the Signal and Image Processing Institute, University of Southern California, from 1993 to 1994. Then, he worked on staff with the Reconnaissance Systems Department, Hughes Aircraft Company, from 1994 to 1996. From 1996 to 2004, he was a member of the Faculty with the Department of Engineering and a Senior Investigator with the Center of Theoretical Studies of Physical Systems, Clark Atlanta University (CAU), Atlanta, GA, USA. He is currently a Researcher with the Networked Sensing and Fusion Branch, U.S. Army Research Laboratory. His current research interests include information/data fusion, reasoning under uncertainty, network science, resource management and signal and image processing. He serves on the Board of Governors for the IEEE Aerospace and Electronic Systems Society (2008–2013, 2018–Present) and as VP of Conferences for the International Society of Information Fusion (ISIF) (2014–Present). Previous, he served as the Editor-in-Chief for the IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS (2012–2017) and on the Board of Directors of ISIF (2012–2014). He is a three time recipient of the CAU Electrical Engineering Instructional Excellence Award from 1999 to 2001. He is a Fellow of ARL.