# Distributed Target Localization with M-ary Quantized Data in Wireless Sensor Networks under Byzantine Data Attacks

Huifang Chen, *Member, IEEE,* Congqi Shen, Lei Xie, *Member, IEEE,*

***Abstract*—In this paper, we investigate the problem of distributed target localization with M-ary quantized data in wireless sensor networks (WSNs) under Byzantine data attacks. Through compromising a number of sensor nodes, an attacker can launch Byzantine data attacks by modifying the compromised sensors' quantized local measurement to one of other quantized levels independently and probabilistically and sending the falsified quantized measurement to the fusion center (FC). We analyze the negative effect of the Byzantine data attacks on the performance of distributed target location estimation. From the perspective of the attacker, we derive the condition to nullify the estimation capability of the FC. We also find an optimal strategy of resource-constrained Byzantine data attacks, which maximally deteriorates the estimation performance of the network. To mitigate the effect of Byzantine data attacks on the distributed target localization, we propose a novel malicious node identification method and a reliable target location estimation approach from the perspective of the defender. In the proposed malicious node identification method, the FC distinguishes the type of sensor nodes by using the report history and the location of each sensor node, the knowledge of the quantization scheme and the estimate of the target location. Using the proposed malicious node identification method, the FC identifies the malicious sensor(s) in the network and excludes them from the distributed estimation process, and estimates the location of the target using quantized data from the residual sensor nodes. Evaluation results show that the proposed malicious node identification method can remove malicious sensor(s) successfully, and the proposed location estimation approach is robust against Byzantine data attacks.**

***Index Terms*—Wireless sensor networks, distributed target localization, malicious node identification method, Byzantine data attacks**

## I. Introduction

DISTRIBUTED estimation and/or tracking the location of a target is a typical application in wireless sensor networks (WSNs). The framework of distributed target localization consists of a group of spatially deployed sensor nodes and a fusion center (FC). In this framework, sensor nodes obtain the local measurements about a target, and send processed data to the FC. The FC estimates the target location in a region of interest (ROI) [1].

Distributed target localization in WSNs has been widely studied in the past two decades (See [2] and references therein). Several target localization techniques, such as direction of arrival (DOA), time of arrival (TOA), and time-difference of arrival (TDOA), were proposed in [3] and [4]. However, these techniques require precise time synchronization and extensive local processing at each sensor node. Some research has focused on developing target localization techniques without suffering from imperfect time synchronization [5].

Distributed target localization techniques are suitable for the low battery supply and limited resource features of WSNs. The received signal strength (RSS) based methods, which employ the least-square (LS) or maximum-likelihood (ML) based source localization techniques, were proposed in [6] and [7]. Due to the limited energy and bandwidth in realistic WSNs, the RSS of each sensor node should be quantized into binary or multi-bit measurement. Sensor nodes send quantized local measurements to save the communication overhead. RSS-based target localization methods with quantized data were proposed in [8] and [9]. At the FC, the quantized local measurements are collected to estimate the location of the target using the ML estimator [10] or the LS estimator [11]. However, the attack issue was not considered in these methods.

For an application to estimate the location of a target in the ROI, secure localization is extremely important in situations where malicious sensor nodes attempt to disrupt the network and unable its capability. Many mechanisms have been proposed for secure distributed localization in WSNs [12-13]. Although many types of security threats exist, we focus on addressing Byzantine data attack problem in the framework of distributed target localization.

Byzantine data attack is a typical malicious behavior of Byzantine attacks proposed by Lamport et al. [14]. For Byzantine data attacks in distributed target localization, an attacker compromises some sensor nodes in the WSN and forces them to send falsified quantized measurements to the FC [15]. The goal of the attacker is to undermine the network so that the FC cannot correctly estimate the target location.

In recent years, Byzantine data attack problem in the framework of distributed target localization has been studied from the perspectives of the attacker [16]-[21] and the defender [23]-[25].

Byzantine independent data attack with binary quantized data is studied in [16]. It is concluded that if half of sensor nodes in the network are malicious, the FC becomes incapable of estimating the target location correctly by utilizing the data collected from sensor nodes (i.e., the FC is blind). Byzantine deterministic independent data attack with M-ary quantized data is studied in [17]. It is concluded that the attack cost

Huifang Chen, Congqi Shen and Lei Xie are with College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, P. R. China (e-mail: chenhf@zju.edu.cn, shencq@zju.edu.cn, xiel@zju.edu.cn).

Manuscript received May 2, 2017.

increases as the number of quantization levels increases. Our previous work also has the similar conclusion [18]. However, probabilistic data attack is not considered in [17] and the optimal attack strategy is not addressed in the case that the FC is not made blind by the attacker in [18]. In [19], Byzantine data attack with binary quantized data is modeled as a binary symmetric channel, and the fraction of malicious nodes for blinding the FC under the deterministic attack is derived. Moreover, the optimal Byzantine data attack strategy has been studied when the FC is blind. It is concluded that the optimal Byzantine data attack strategy with binary quantized data is to flip the quantized data before transmitting to the FC [19]. In [20], it is concluded that the optimal deterministic Byzantine data attack strategy is to falsify the true data with the same probability when the reported data is quantized into M-ary. However, the optimal strategy for probabilistic data attack with M-ary quantized data when the FC is blind is not found in [19] and [20]. Therefore, we will study the optimal strategy under probabilistic data attack with M-ary quantized data when the FC is blind in this work.

In addition, some researchers studied Byzantine data attack problem in the distributed inference. In [21], Byzantine nodes are assumed to have the knowledge of the statistics of local quantization outputs, and the optimal Byzantine attack strategy is derived. However, this assumption is too strong for a real scenario. In [22], all the data attacks are classified according to the information available for attackers. The attackers with *a priori* knowledge always cause a more serious damage to the network than those without any information. However, the optimal strategy for probabilistic data attack as the FC is not made blind completely is still not found.

From the perspective of the defender, some methods have been proposed to mitigate the effect of Byzantines by tolerating the falsified data [23-24]. A distributed target localization method using error correcting codes in the presence of Byzantine nodes is proposed in [23], where the FC iteratively decides the ROI by performing an M-ary hypothesis test. Moreover, non-ideal channel is considered in distributed target localization method under Byzantine data attacks in [24]. The distributed estimation under Byzantine data attack in a two-node network is investigated in [25]. However, the performance of tolerant-based attack mitigation methods degrades obviously when the number of Byzantine nodes increases.

A more effective way is to identify Byzantine nodes and exclude the data reported from malicious nodes. However, few researchers have studied the identification-based attack mitigation techniques in distributed estimation. Similar technique has been widely studied in the framework of the distributed detection [26]-[33]. A learning-based framework is proposed to identify Byzantine nodes in [26]. The FC declares a sensor to be malicious if it behaves different from trusted nodes, where the behavior statistics of anchors are needed. An improved algorithm is proposed in [27], where less number of anchors is needed. In [28], jointly spectrum sensing and spectrum sharing is addressed in order to improve the spectrum sensing performance and the capability of identifying malicious nodes. In these methods, anchors are needed. In [29], authors developed an identification method. The principle of this identification method is to observe a sensor's behavior during some periods and decide on whether it behaves closer to an honest node or a Byzantine node. The expectation behavior of an honest node or a Byzantine node is obtained by anchors. How to guarantee the security of anchors in an unsafe network is not resolved in these techniques.

Some identification-based attack mitigation methods without anchors have been proposed in [20], [30]-[32]. It is concluded in [30] that the FC can perfectly identify malicious nodes without any anchor if the observation period is infinite. A deviation-based malicious node identification algorithm is presented in [20]. In this algorithm, the FC calculates the deviation of each sensor between the real amplitude and the inverse of the quantizer. If the deviation is larger than the threshold, the sensor is declared to be malicious. However, it is assumed that the FC knows the true location of the target, which is too strong for a realistic scenario. In [31], an abnormality identification algorithm based on proximity is proposed to detect malicious nodes, where it is assumed that a small part of sensor nodes is malicious. Authors in [32] adopt a similar technique to resolve secure target identification problem. With the best of our knowledge, the malicious node identification problem in the distributed target localization without anchors is only addressed in [20]. However, the proposed algorithm is under the assumption that the true location of the target is known such that the *a posteriori* probabilities of malicious nodes can be computed. It is necessary to resolve the malicious node identification problem without anchors and *a priori* knowledge about the true target location. This is another motivation of our work.

In this paper, we study the problem of distributed target localization with M-ary quantized data under Byzantine data attacks from the perspectives of attacker and defender. The main contributions of this paper are summarized as follows.

First, we introduce a probabilistic and independent Byzantine data attack model for the distributed target localization with M-ary quantized data, where malicious sensors independently modified the quantized levels according to the attack probability and the real M-ary quantized level. In the defined attack model, the attacker is assumed to have no knowledge about the true location of the target and the set of quantization thresholds.

Second, we characterize the negative effect of Byzantine data attack on the performance of distributed target localization with M-ary quantized data. By making the determinant of posterior Fisher information matrix (FIM) be the prior's contribution to posterior FIM, we derive the optimal Byzantine data attack strategy which makes the FC blind completely. Furthermore, we find an optimal highly-symmetric strategy of resource-constrained Byzantine data attacks, which maximally deteriorates the estimation performance of the network.

Third, we propose a malicious node identification method, in which the FC identifies the type of senor nodes by using the report history and the location of each sensor node, the knowledge of the quantization threshold set and the estimate of the target location. The performance of malicious node identification method, such as the identification probability and the detectability, is analytically evaluated.

Fourth, using the proposed malicious node identification method, we present a reliable target location estimation approach performed at the FC. By identifying and excluding identified malicious sensor(s) from the target location estimation process at the FC, the proposed estimation approach is robust against Byzantine data attacks.

The remainder of this paper is organized as follows. The problem of distributed target localization with M-ary quantized data under Byzantine data attacks are introduced in Section II. In Section III, the impact of probabilistic Byzantine data attack on the performance of distributed target localization with M-ary quantized data is analyzed, and the optimal attack strategies are addressed. To defend against Byzantine data attacks, a malicious node identification method and a reliable target location estimation approach are presented in Section IV. Numerical results are given in Section V. Section VI concludes the paper.

For clarity, we explain the denotation of some notations used in this paper. $TY_i$ denotes the type of sensor $i$, and $TY_i \in \{\mathrm{H}, \mathrm{B}\}$, where H and B correspond to "honest" and "malicious", respectively. $\mathcal{TY}_i$ denotes the type of sensor $i$ to be declared using the malicious node identification method, and $\mathcal{TY}_i \in \{\mathrm{H}, \mathrm{B}\}$. $\mathcal{N}(\cdot, \cdot)$ denotes the normal distribution. $\mathcal{A} \backslash \mathcal{B}$ denotes the operation of excluding $\mathcal{B}$ from $\mathcal{A}$, where $\mathcal{A}$ and $\mathcal{B}$ are two sets.

## II. Preliminaries

In this section, we introduce the distributed target localization problem with M-ary quantized data in a WSN under Byzantine data attacks.

### A. System Model

We consider a scenario where $N$ sensor nodes are randomly deployed in a field to estimate the location of a target at $\theta = (x_\mathrm{t}, y_\mathrm{t})$, where $x_\mathrm{t}$ and $y_\mathrm{t}$ denote the coordinates of the target in the ROI within the 2-D Cartesian plane, as shown in Fig. 1. Among the sensor nodes in the network, $\alpha$ fraction is assumed to be malicious. Theses malicious sensor nodes maybe send falsified data to the FC to deteriorate the estimation process.

It is assumed that the target location has a prior distribution, $p_0(\theta)$. For simplicity, we assume that $p_0(\theta)$ is a Gaussian distribution, i.e., $\theta \sim \mathcal{N}(\varpi_\theta, \sigma_\theta^2 \mathbf{I})$, where the mean $\varpi_\theta$ is the center of the ROI, and the variance $\sigma_\theta^2 \mathbf{I}$ is large enough such that the ROI includes the target's 99% confidence region.

The signal radiated from the target is assumed to follow an isotropic power attenuation model [16]. That is, the signal power received at sensor $i$, $a_i$, is given as $(a_i)^2 = P_0 (d_0/d_i)^\kappa$, where $P_0$ is the power measured at a reference distance $d_0$, $\kappa$ is the path-loss exponent, $d_i$ is the distance between the target and sensor $i$ located at $(x_i, y_i)$, and $d_i = [(x_\mathrm{t} - x_i)^2 + (y_\mathrm{t} - y_i)^2]^{1/2}$. It is assumed that $d_i \neq 0$, which means that the target is not on a sensor. Without loss of generality, $d_0 = 1$ and $\kappa = 2$ in this paper.

### B. Local Observation and Quantization

At each sensor node, the signal amplitude is corrupted by additive white Gaussian noise (AWGN). Hence, the corrupted signal amplitude at sensor $i$, $s_i$, is $s_i = a_i + n_i$, where the noise $n_i$ follows $\mathcal{N}(0, \sigma_n^2)$. Due to energy and bandwidth limitations in a real WSN, each sensor node uses an M-ary quantizer and sends its quantized measurement to the FC. That is, $s_i$ is quantized into M-ary measurement, $u_i$, using the quantization rule as

$$u_i = \psi(s_i) = m, \text{if } \eta_m < s_i \leq \eta_{m+1}, m = 1, 2, \ldots, M, \quad i = 1, 2, \ldots, N, \quad (1)$$

where $\psi(\cdot)$ denotes the quantization process, $M$ is the number of quantization levels, $u_i$ denotes the quantized level of $s_i$, $\eta_m$ and $\eta_{m+1}$ denote the $m$th and $(m+1)$th quantization boundaries, respectively. There are several quantization methods that can be considered at sensor nodes, such as the uniform quantization, the maximum output entropy (MOE) quantization and the minimum average error (MAE) quantization [33]. It is shown in [33] that, if a signal follows the normal distribution, the quantizers with MOE and MAE are approximately the same within a multiplicative constant. Hence, the MOE quantization method is adopted in this paper.

For the distributed target localization scheme with M-ary quantized data, designing the quantization thresholds is an important issue. It is reasonable that the same type of sensor nodes uses the same quantization threshold set. That is, the honest nodes use $\boldsymbol{\eta}^\mathrm{H}$, while the Byzantine nodes use $\boldsymbol{\eta}^\mathrm{B}$. It is shown in [16] that for the Byzantine and honest nodes, the optimal strategy is to use $\boldsymbol{\eta} = \boldsymbol{\eta}^\mathrm{H} = \boldsymbol{\eta}^\mathrm{B}$ since the attacker has no knowledge about the set of the quantization thresholds.

Due to the Gaussian noise assumption, the probability that $u_i$ takes a specific value $m$ is

$$P(u_i = m|\theta) = Q\left(\frac{\eta_{im} - a_i}{\sigma_n}\right) - Q\left(\frac{\eta_{i(m+1)} - a_i}{\sigma_n}\right), \quad m = 1, 2, \ldots, M, \quad (2)$$

where $Q(\cdot)$ is the complementary distribution function of the standard Gaussian distribution, and $Q(x) \triangleq \int_x^{+\infty} \exp\left(-t^2/2\right) dt/\sqrt{2\pi}$.

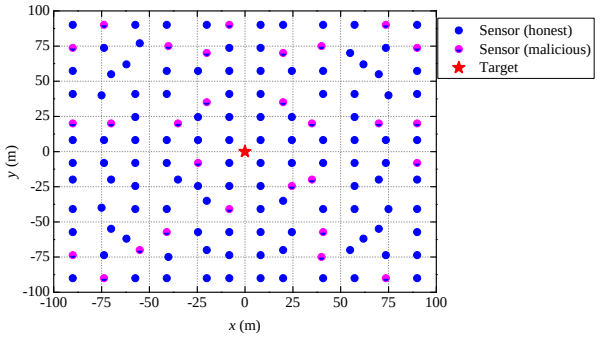



Fig. 1. The target in a deployed sensor field.

### C. Attack Model

In a comprised WSN, Byzantine nodes may not transmit their true quantized measurements to the FC. Let $v_i$ be the quantized measurement transmitted by sensor $i$. If sensor $i$ is honest, $v_i = u_i$; otherwise, sensor $i$ may modify $u_i$ to

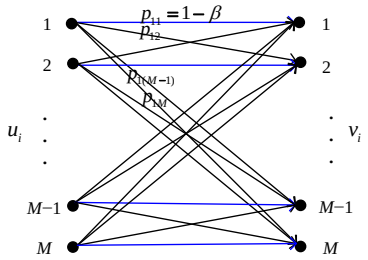



Fig. 2. Probabilistic Byzantine data attack model.

$v_i$ according to the Byzantine data attack model described following, and $v_i \neq u_i$.

Here, we introduce a probabilistic Byzantine data attack model. Let $\beta$ denote the attack probability of a malicious node. That is, Byzantine node $i$ behaves maliciously with probability $\beta$, and behaves normally with probability $1-\beta$. Let $TY_i$ be the type of sensor $i$ and $TY_i \in \{\mathrm{H}, \mathrm{B}\}$. If $TY_i = \mathrm{H}$, sensor $i$ is an honest node, while $TY_i = \mathrm{B}$ means that sensor $i$ is a Byzantine node.

It is assumed that the Byzantine node has no knowledge of the true location of the target and the set of quantization thresholds used. Based on the local quantized measurement, Byzantine node $i$ falsifies its quantized measurement according to the model as illustrated in Fig. 2. Specifically, at each measurement, Byzantine node $i$ with $u_i = l$ behaves normally with probability $1-\beta$, $p_{ll} \triangleq \Pr(v_i = l \mid u_i = l, TY_i = \mathrm{B}) = 1-\beta$; Byzantine node $i$ modifies its quantized measurement $u_i = l$ into $v_i = k$ with probability $p_{lk}$, $p_{lk} \triangleq \Pr(v_i = k \mid u_i = l, TY_i = \mathrm{B})$ and $k \neq l$. Obviously, $\sum_{\substack{k=1 \\ k\neq l}}^{M} p_{lk} = \beta, l = 1, 2, \ldots, M$.

The transition probabilities illustrated in Fig. 2 can be denoted using a row-stochastic matrix, $\mathbf{P}$.

Based on the probabilistic Byzantine data attack model introduced above, for Byzantine node $i$, the probability of $v_i$ is represented as

$$\begin{aligned} P(v_i = k \mid \theta, TY_i = \mathrm{B}) &= (1-\beta) P(u_i = k \mid \theta, TY_i = \mathrm{B}) \\ &+ \sum_{\substack{l=1 \\ l\neq k}}^{M} p_{lk} P(u_i = l \mid \theta, TY_i = \mathrm{B}), k = 1, 2, \ldots, M. \end{aligned} \quad (3)$$

Obviously, if sensor $i$ is honest, the probability of $v_i$ is the same as that of $u_i$. That is,

$$P(v_i = k \mid \theta, TY_i = \mathrm{H}) = P(u_i = k \mid \theta, TY_i = \mathrm{H}), \quad k = 1, 2, \ldots, M. \quad (4)$$

### D. Target Location Estimation at the FC

It is assumed that the wireless communication channel between the sensor nodes and the FC is perfect. Although the quantized measurements may be corrupted by the noise and interference in the wireless channel, the influence can be avoided using an efficient channel coding mechanism. Thus, the effect of the wireless channel errors between the sensor nodes and the FC is neglected in this paper. In other words, the quantized data received by the FC are the transmitted quantized measurements from sensor nodes, $\mathbf{v} = [v_1 \ v_2 \ \ldots \ v_N]$. The FC estimates the location of the target using $\mathbf{v}$.

If no malicious node identification process is implemented, the FC is not aware of the type of the node. It is reasonable to assume that sensor $i$ is compromised with a probability $\alpha$. Therefore, the conditional distribution of $v_i$ at the FC is

$$\begin{aligned} P(v_i = k \mid \theta) &= \alpha P(v_i = k \mid \theta, TY_i = \mathrm{B}) \\ &+ (1-\alpha) P(v_i = k \mid \theta, TY_i = \mathrm{H}) \\ &= (1-\alpha\beta) + \sum_{\substack{l=1 \\ l\neq k}}^{M} [\alpha p_{lk} - (1-\alpha\beta)] P(u_i = l \mid \theta). \end{aligned} \quad (5)$$

The likelihood function of $\mathbf{v}$ at the FC is represented as

$$P(\mathbf{v} \mid \theta) = \prod_{i=1}^{N} \prod_{k=1}^{M} P(v_i = k \mid \theta)^{\delta(v_i - k)}, \quad (6)$$

where $\delta(\cdot)$ is the Kronecker delta function, and $\delta(x) = \begin{cases} 0 & ; \quad x \neq 0 \\ 1 & ; \quad x = 0 \end{cases}$.

The log-likelihood function of $\mathbf{v}$ can be written as

$$\ln P(\mathbf{v} \mid \theta) = \sum_{i=1}^{N} \sum_{k=1}^{M} \delta(v_i - k) \ln P(v_i = k \mid \theta). \quad (7)$$

After collecting $\mathbf{v}$, the FC estimates the target location using the maximum likelihood (ML) estimator as in [9]. That is,

$$\hat{\theta} = \arg\max_{\theta} \sum_{i=1}^{N} \sum_{k=1}^{M} \delta(v_i - k) \ln P(v_i = k \mid \theta). \quad (8)$$

### E. Performance Metrics

The posterior Cramer-Rao lower bound (PCRLB) and posterior Fisher information matrix (FIM) are two performance metrics to analyze the estimation performance. Let $\hat{\theta}(\mathbf{v})$ be an estimator of $\theta$. The covariance matrix of the estimation error is bounded below by the PCRLB. The PCRLB can be given as the inverse of FIM, $E\left\{\left[\hat{\theta}(\mathbf{v}) - \theta\right]\left[\hat{\theta}(\mathbf{v}) - \theta\right]^T\right\} \geq \mathbf{F}^{-1}$, where $\mathbf{F}$ is the FIM.

The FIM and its elements are given as

$$\begin{aligned} \mathbf{F} &= -E[\nabla_\theta \nabla_\theta^T \ln P(\mathbf{v} \mid \theta)] - E[\nabla_\theta \nabla_\theta^T \ln p_0(\theta)] \\ &= \mathbf{F}_{\mathrm{D}} + \mathbf{F}_\theta = \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix} + \begin{pmatrix} 1/\sigma_\theta^2 & 0 \\ 0 & 1/\sigma_\theta^2 \end{pmatrix}, \end{aligned} \quad (9)$$

$$F_{11} = \int p_0(\theta) \left( \sum_{i=1}^{N} \sum_{k=1}^{M} \frac{-1}{P(v_i = k \mid \theta)} \left[ \frac{\partial P(v_i = k \mid \theta)}{\partial x_{\mathrm{t}}} \right]^2 \right) d\theta, \quad (9.a)$$

$$F_{22} = \int p_0(\theta) \left( \sum_{i=1}^{N} \sum_{k=1}^{M} \frac{-1}{P(v_i = k \mid \theta)} \left[ \frac{\partial P(v_i = k \mid \theta)}{\partial y_{\mathrm{t}}} \right]^2 \right) d\theta, \quad (9.b)$$

$$F_{12} = F_{21} = \int p_0(\theta) \left( \sum_{i=1}^{N} \sum_{k=1}^{M} \frac{-1}{P(v_i = k \mid \theta)} \frac{\partial P(v_i = k \mid \theta)}{\partial x_{\mathrm{t}}} \frac{\partial P(v_i = k \mid \theta)}{\partial y_{\mathrm{t}}} \right) d\theta, \tag{9.c}$$

$$\frac{\partial P(v_i = k \mid \theta)}{\partial x_{\mathrm{t}}} = \sum_{\substack{l=1 \\ l \neq k}}^{M} \frac{[\alpha p_{lk} - (1 - \alpha\beta)] a_i}{\sigma_n \sqrt{2\pi} d_i^2} (x_i - x_{\mathrm{t}}) \left[ \exp\left( -\frac{(\eta_l - a_i)^2}{2\sigma_n^2} \right) - \exp\left( -\frac{(\eta_{l+1} - a_i)^2}{2\sigma_n^2} \right) \right], \tag{9.d}$$

$$\frac{\partial P(v_i = k \mid \theta)}{\partial y_{\mathrm{t}}} = \sum_{\substack{l=1 \\ l \neq k}}^{M} \frac{[\alpha p_{lk} - (1 - \alpha\beta)] a_i}{\sigma_n \sqrt{2\pi} d_i^2} (y_i - y_{\mathrm{t}}) \left[ \exp\left( -\frac{(\eta_l - a_i)^2}{2\sigma_n^2} \right) - \exp\left( -\frac{(\eta_{l+1} - a_i)^2}{2\sigma_n^2} \right) \right]. \tag{9.e}$$

From the perspective of the attacker, the aim is to destroy the network so that the estimation performance of the FC is degraded. The most serious case is to make the FC blind (completely dysfunctional), in which the location of the target estimated by the FC is no better than merely estimating the target location using the prior distribution of $\theta$. Although being incapable of making the FC blind, the attacker will try to degrade the estimation performance of the FC as far as possible. In this paper, we will analyze the impact of probabilistic Byzantine data attack on the estimation performance of distributed target localization, and derive the optimal attack strategy.

On the other hand, in the view of the defender, the objective is to make the FC reliably estimate the location of the target although Byzantine nodes exist in the network. In this paper, we present a secure distributed target localization scheme with M-ary quantized data in the WSN, where the malicious node identification method performed at the FC is mainly studied.

## III. Optimal Byzantine Attack Strategy

The goal of the attacker is to cause much damage to the functionality of the FC as possible. That is, Byzantine nodes would want the PCRLB to be large to have the maximum damage. In this section, we address the Byzantine data attack strategy on the estimation performance of distributed target localization with M-ary quantized data.

### A. Blind Condition of Byzantine Data Attack

First, we focus on the Byzantine data attack making the FC blind completely.

If Byzantine nodes can make the PCRLB approach infinity, the FC will be made incapable of estimating the location of the target using the data from sensor nodes. In other words, when the contribution of data received from sensor nodes to posterior FIM approaches zero, the FC is completely blind. In this scenario, it is better for the FC to estimate the location of the target using the prior distribution of $\theta$.

Let $\alpha_{\text{blind}}$ denote the minimum fraction of malicious nodes which makes the FC incapable of estimating the target location using data from sensor nodes.

*Theorem 1:* If the attacker with attack probability $\beta$ has no knowledge of the quantization thresholds used at each sensor node, the optimal Byzantine data attack strategy for the distributed target localization with M-ary quantized data to 'blind' the FC completely is given as

$$\alpha_{\text{blind}} = \min(1, (M-1)/M\beta), \quad p_k = \begin{cases} \beta/(M-1) & ; \text{ if } l \neq k. \\ 1 - \beta & ; \text{ if } l = k. \end{cases} \tag{10}$$

*Proof:* Since FIM is multi-dimensional, malicious sensor nodes will try to make the determinant of FIM approach to the prior's contribution to posterior FIM. In other words, $\alpha_{\text{blind}}$ can be found by making $|\mathbf{F}_{\mathrm{D}}| = 0$.

Substituting (9) into $F_{11}F_{22} - F_{12}F_{21} = 0$, we can find $\alpha_{\text{blind}} = (M-1)/M\beta$.

To completely blind the FC is equivalent to making $P(v_i = k \mid \theta) = 1/M$ for all $k \in \{1, 2, \ldots, M\}$. Substituting $\alpha_{\text{blind}} = (M-1)/M\beta$ into (5), we have $p_{ll} = 1 - \beta$, and $p_{lk} = \beta/(M-1)$ for all $k \in \{1, 2, \ldots, M\}$ and $l \neq k$. ■

Therefore, when the fraction of malicious nodes in the WSN, $\alpha$, is greater than or equal to $\alpha_{\text{blind}}$, the attacker can 'blind' the FC completely.

### B. Optimal Byzantine Attack Strategy

If the attacker does not have enough resources to compromise $\alpha_{\text{blind}}$ fraction of sensor nodes in the network, the optimal attack strategy for the attacker is to deteriorate the estimation performance of the network to the maximal extent.

According to Theorem 1, we restrict our attention to the set of highly-symmetric $\mathbf{P}$ for the sake of tractability. In other words, we assume that

$$p_{lk} = \begin{cases} p & ; \text{ if } l \neq k. \\ 1 - (M-1)p & ; \text{ if } l = k. \end{cases} \tag{11}$$

Hence, the conditional distribution of $v_i$ at the FC can be rewritten as

$$\begin{aligned} P(v_i = k \mid \theta) &= (1-\alpha) P(u_i = k \mid \theta) + \\ &\alpha[(1 - (M-1)p) P(u_i = k \mid \theta) + \sum_{\substack{l=1 \\ l \neq k}}^{M} p P(u_i = l \mid \theta)] \\ &= (1 - \alpha M p) P(u_i = k | \theta) + \alpha p. \end{aligned} \tag{12}$$

The optimal Byzantine data attack strategy is presented in Theorem 2.

*Theorem 2:* Given the value of the fraction of malicious nodes and $\alpha < \alpha_{\text{blind}}$, the FC cannot be made blind completely. The problem of finding the optimal $\mathbf{P}$ as given in (11) can be formulated as

$$\min_{\mathbf{P}} \ \mathbf{F} \ , \text{ s.t. } \ 0 \leq p \leq \frac{\beta}{M-1}. \tag{P.1}$$

Solving the problem formulated in (P.1), when $\alpha < \min(1, M - 1/M\beta)$, and the attacker with a given $\beta$ has no knowledge of the quantization thresholds used at each sensor node, the optimal Byzantine data attack strategy for the distributed target localization with M-ary quantized data is given as

$$p_{lk} = \begin{cases} \frac{\beta}{M-1} & ; \quad \text{if } l \neq k. \\ 1-\beta & ; \quad \text{if } l = k. \end{cases} \tag{13}$$

*Proof:* See Appendix A. ∎

## IV. Mitigation of Byzantine Data Attacks in Distributed Target Localization

If the attacker cannot compromise enough sensor nodes, the FC will not be made blind completely. For the distributed target localization in a WSN under Byzantine data attacks, it is important to identify the type of sensor nodes and exclude malicious nodes from the target location estimation process at the FC. Hence, we mainly focus on the malicious node identification method in this section.

### A. Malicious Node Identification Method

In order to detect malicious nodes, the FC observes the received quantized data from each sensor node over a time window $T$, where $T$ is the number of local observations that have been completed. The history of received quantized data of sensor $i$ is denoted by $\boldsymbol{v}_i = (v_i(1), v_i(2), \ldots, v_i(T))$, where $v_i(t)$ is the received quantized data of sensor $i$ at time interval $t$.

At each time interval, the FC estimates the location of the target using the received quantized data from the sensor nodes with (8).

Let $\hat{\theta}(t)$ be the estimated location of the target at time interval $t$. According to the estimated location of the target, $\hat{\theta}(t) = (\hat{x}_{\rm t}(t), \hat{y}_{\rm t}(t))$, and the location of sensor $i$, $\theta_i = (x_i, y_i)$, the FC can compute its nominal received signal as $\hat{a}_i(t) = [P_0/(\hat{d}_i(t))^2]^{1/2}$, and $(\hat{d}_i(t))^2 = (x_i - \hat{x}_{\rm t}(t))^2 + (y_i - \hat{y}_{\rm t}(t))^2$. Based on $\hat{a}_i(t)$, the nominal quantized level of sensor $i$, $\hat{u}_i(t)$, can be determined using (1). That is, $\hat{u}_i(t) = \psi(\hat{a}_i(t))$.

Here, we introduce a metric, the fitness of the quantized level, to represent the behavior of the sensor node. Let $\xi_i$ be the fitness of the quantized level for sensor $i$ over a time window $T$. Using $\boldsymbol{v}_i = (v_i(1), v_i(2), \ldots, v_i(T))$ and $\hat{\boldsymbol{u}}_i = (\hat{u}_i(1), \hat{u}_i(2), \ldots, \hat{u}_i(T))$, $\xi_i$ can be calculated as

$$\xi_i = \frac{1}{T}\sum_{t=1}^{T} \delta(v_i(t) - \hat{u}_i(t)), i = 1, 2, \ldots, N. \tag{14}$$

For a practical system, the FC calculates $\xi_i$ at time interval $t$ in a recursive form as

$$\xi_i(t) = \frac{(t-1)\xi_i(t-1) + \delta[v_i(t) - \hat{u}_i(t)]}{t}, \quad t = 1, 2, \ldots, T,\ i = 1, 2, \ldots, N. \tag{15}$$

Sensor $i$ can be declared honest or malicious using the rule as follows:

$$\xi_i \underset{\mathcal{TY}_i = \rm H}{\overset{\mathcal{TY}_i = \rm B}{\gtrless}} \gamma_i,\ i = 1, 2, \ldots, N, \tag{16}$$

where $\gamma_i$ is the threshold of the malicious node identification method, $\mathcal{TY}_i$ denotes the type of sensor $i$ to be declared using the malicious node identification method, and $\mathcal{TY}_i \in \{\rm H, B\}$.

The performance of the malicious node identification method for sensor $i$ is quantified by two conditional probabilities, the identification probability $\Pi_{{\rm d},i} \triangleq \Pr\{\xi_i \leq \gamma_i \mid TY_i = \rm B\}$ and the false identification probability $\Pi_{{\rm f},i} \triangleq \Pr\{\xi_i \leq \gamma_i | TY_i = \rm H\}$. Specifically, $\Pi_{{\rm d},i}$ denotes the probability that malicious node $i$ is identified correctly, and $\Pi_{{\rm f},i}$ denotes the probability that honest node $i$ is falsely declared as malicious.

From (16), the behavior of the proposed malicious node identification method depends strongly on the choice of $\gamma_i$. The value of $\gamma_i$ should be set in such a way that $\Pi_{{\rm d},i}$ is high enough, as well as $\Pi_{{\rm f},i}$ is low. However, a tradeoff between the identification probability and the false identification probability should be achieved.

*1) Threshold selection:* In order to find the optimal choice of $\gamma_i$ in (16), we use the Neyman-Pearson framework in the context of malicious node identification. The objective is to maximize $\Pi_{{\rm d},i}$ subject to the condition $\Pi_{{\rm f},i} \leq \zeta$, and $\zeta$ is the required false identification probability.

The optimal threshold selection problem is expressed as

$$\gamma_i^* = \arg\max_{\gamma_i} \Pi_{{\rm d},i},\ \text{s.t. } \Pi_{{\rm f},i} \leq \zeta,\ i = 1, 2, \ldots, N, \tag{P.2}$$

where $\gamma_i^*$ denotes the optimal threshold for sensor $i$ in the malicious node identification method.

Obviously, the closed-form expressions of $\Pi_{{\rm d},i}$ and $\Pi_{{\rm f},i}$ are needed to resolve the problem (P.2). In order to obtain $\Pi_{{\rm d},i}$ and $\Pi_{{\rm f},i}$, we need the closed-form expressions for conditional distributions of $\xi_i$, $P(\xi_i \mid TY_i = \rm H)$ and $P(\xi_i \mid TY_i = \rm B)$. In practice, as $T$ is finite, it is intractable to determine the conditional distributions of $\xi_i$. Therefore, we give an asymptotic choice of $\gamma_i$ in (16) as $T$ is large enough.

We assume that the report process of the quantized level for each sensor is independent. As the value of $T$ is very large, the fitness of quantized level for sensor $i$ converges according to the *Central Limit Theorem* (CLT) [34]. Moreover, as $T$ is large enough, $\xi_i$ follows the normal distribution with mean and variance as follows:

$$\xi_i \sim \begin{cases} \mathcal{N}(\mu_i^{\rm H}, \frac{\mu_i^{\rm H}(1-\mu_i^{\rm H})}{T}), & \text{if} \quad TY_i = \rm H, \\ \mathcal{N}(\mu_i^{\rm B}, \frac{\mu_i^{\rm B}(1-\mu_i^{\rm B})}{T}), & \text{if} \quad TY_i = \rm B, \end{cases} \tag{17}$$

where $\mu_i^{\rm H}$ is the behavior feature of sensor $i$ as it is honest, $\mu_i^{\rm B}$ is the behavior feature of sensor $i$ as it is malicious.

If sensor $i$ is honest, the behavior feature can be calculated by

$$\begin{aligned} \mu_i^{\rm H} &= \Pr(\delta(v_i - \psi(a_i)) = 1 \mid \theta, TY_i = \rm H) \\ &= Q\left(\frac{\eta_{\psi(a_i)} - a_i}{\sigma_n}\right) - Q\left(\frac{\eta_{\psi(a_i)+1} - a_i}{\sigma_n}\right). \end{aligned} \tag{18}$$

Otherwise, if sensor $i$ is malicious, the behavior feature can

be calculated by

$$\mu_i^{\mathrm{B}} = \Pr(\delta(v_i - \psi(a_i)) = 1 \mid \theta, TY_i = \mathrm{B}) = (1-\beta)\mu_i^{\mathrm{H}} + \frac{\beta}{M-1}(1-\mu_i^{\mathrm{H}}). \quad (19)$$

According to (16)-(19), the identification probability and the false identification probability of the proposed malicious node identification method can be calculated by

$$\Pi_{\mathrm{d},i} = \Pr\{\xi_i \le \gamma_i \mid TY_i = \mathrm{B}\} = \Phi\left(\frac{\gamma_i - \mu_i^{\mathrm{B}}}{\sqrt{\frac{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}{T}}}\right) \quad (20)$$

and

$$\Pi_{\mathrm{f},i} = \Pr\{\xi_i \le \gamma_i \mid TY_i = \mathrm{H}\} = \Phi\left(\frac{\gamma_i - \mu_i^{\mathrm{H}}}{\sqrt{\frac{\mu_i^{\mathrm{H}}(1-\mu_i^{\mathrm{H}})}{T}}}\right), \quad (21)$$

respectively, and $\Phi(x) = \int_{-\infty}^{x} \exp(-t^2/2)dt/\sqrt{2\pi}$.

For the proposed malicious node identification method, we maximize $\Pi_{\mathrm{d},i}$ subject to $\Pi_{\mathrm{f},i} \le \zeta$. Since $\Phi(x)$ is monotonically increasing, $\Pi_{\mathrm{f},i}$ and $\Pi_{\mathrm{d},i}$ are increasing with $\gamma_i$. Let $\gamma_i'$ be the threshold satisfying $\Pi_{\mathrm{f},i}' = \Phi\left(\frac{\sqrt{T}(\gamma_i' - \mu_i^{\mathrm{H}})}{\sqrt{\mu_i^{\mathrm{H}}(1-\mu_i^{\mathrm{H}})}}\right) = \zeta$ with given $T$ and $\mu_i^{\mathrm{H}}$. Any other threshold $\gamma_i''$, $\gamma_i' > \gamma_i''$, satisfies $\Pi_{\mathrm{f},i}'' < \zeta$ and $\Pi_{\mathrm{d},i}' > \Pi_{\mathrm{d},j}''$ with the same $T$, $\mu_i^{\mathrm{H}}$ and $\mu_i^{\mathrm{B}}$, where $\Pi_{\mathrm{f},i}'' = \Phi\left(\frac{\sqrt{T}(\gamma_i'' - \mu_i^{\mathrm{H}})}{\sqrt{\mu_i^{\mathrm{H}}(1-\mu_i^{\mathrm{H}})}}\right)$, $\Pi_{\mathrm{d},i}' = \Phi\left(\frac{\sqrt{T}(\gamma_i' - \mu_i^{\mathrm{B}})}{\sqrt{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}}\right)$ and $\Pi_{\mathrm{d},i}'' = \Phi\left(\frac{\sqrt{T}(\gamma_i'' - \mu_i^{\mathrm{B}})}{\sqrt{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}}\right)$. Hence, $\Pi_{\mathrm{d},i}$ is maximized only if $\Pi_{\mathrm{f},i} = \zeta$ holds.

By considering $\Pi_{\mathrm{f},i} = \zeta$, the optimal threshold, $\gamma_i^*$, is calculated using (21), and

$$\gamma_i^* = \Phi^{-1}(\zeta)\sqrt{\frac{\mu_i^{\mathrm{H}}(1-\mu_i^{\mathrm{H}})}{T}} + \mu_i^{\mathrm{H}}. \quad (22)$$

Substituting $\gamma_i^*$ into (20), we obtain the identification probability, $\Pi_{\mathrm{d},i} = \Phi\left(\frac{\sqrt{T}(\gamma_i^* - \mu_i^{\mathrm{B}})}{\sqrt{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}}\right)$.

Therefore, the malicious node identification method is summarized in Algorithm 1 as follows.

**Algorithm 1 : Malicious Node Identification Method.**

**Input and Parameter Initialization:**

Input $T$, $\{\boldsymbol{v}(t); t = 1, 2, \ldots, T\}$, $\{\theta_i; i = 1, 2, \ldots, N\}$, $\varpi_\theta$, $\{\eta_m; m = 1, 2, \ldots, M+1\}$,$\zeta$.

**Node Identification Procedure:**

**for** time interval $t$ **do**
  Estimate the location of the target, $\hat{\theta}(t)$, using $\boldsymbol{v}(t)$ with (8).
  **for** sensor $i$ **do**
    Compute the nominal received signal with $\hat{\theta}(t)$ and $\theta_i$ as $\hat{a}_i(t) = \sqrt{\frac{P_0}{(x_i - \hat{x}_{\mathrm{t}}(t))^2 + (y_i - \hat{y}_{\mathrm{t}}(t))^2}}$.
    Compute the nominal quantized level as $\hat{u}_i(t) = \psi(\hat{a}_i(t))$.
    Estimate the fitness of the quantized level, $\xi_i(t)$, with (15).
  **end for**
**end for**
**for** sensor $i$ **do**
  Compute the received signal with $\varpi_\theta$ and $\theta_i$ as $a_i = \sqrt{\frac{P_0}{(x_i - x_{\mathrm{t}})^2 + (y_i - y_{\mathrm{t}})^2}}$.
  Compute the behavior feature $\mu_i^{\mathrm{H}}$ with (18) as $TY_i = \mathrm{H}$.
  Compute the optimal threshold $\gamma_i^*$ in (22).
  If $\xi_i(T) \le \gamma_i^*$ , sensor $i$ is declared as malicious, $\mathcal{TY}_i = \mathrm{B}$; otherwise, sensor $i$ is declared as honest, $\mathcal{TY}_i = \mathrm{H}$.
**end for**

**Output:**

Output $\{\mathcal{TY}_i; i = 1, 2, \ldots, N\}$.

*2) Performance analysis:* We analyze the performance of the proposed malicious node identification method.

*a) Detection performance:* The identification probability and the false identification probability are analyzed in above subsection. The closed-form expressions of $\Pi_{\mathrm{d},i}$ and $\Pi_{\mathrm{f},i}$ are given in (20) and (21), respectively.

*b) Detectability:* As mentioned above, if sensor $i$ is honest, $\xi_i \to \mu_i^{\mathrm{H}}$ almost surely as the value of $T$ is large enough according to the CLT; otherwise, $\xi_i \to \mu_i^{\mathrm{B}}$. Obviously, if $\mu_i^{\mathrm{B}} \ne \mu_i^{\mathrm{H}}$, the malicious node can be detected with probability 1 when the value of $T$ is large enough if the threshold is properly selected .

*Theorem 3:* (Detectability) The malicious node is always detectable using the proposed malicious node identification method.

*Proof:* We proof this theorem using the contradiction method. The malicious node is non-detectable when $\mu_i^{\mathrm{B}} = \mu_i^{\mathrm{H}}$. That is, $\mu_i^{\mathrm{H}} = (1-\beta)\mu_i^{\mathrm{H}} + \frac{\beta}{M-1}(1-\mu_i^{\mathrm{H}})$. So, we have $\frac{\beta}{M-1}(1 - M\mu_i^{\mathrm{H}}) = 0$. Hence, there are two selections to make $\mu_i^{\mathrm{B}} = \mu_i^{\mathrm{H}}$ hold.

One selection is to make $\beta = 0$, which means that sensor $i$ does not launch the Byzantine data attack at all. Obviously, this condition does not satisfy the definition of the malicious node.

The other selection is to make $\mu_i^{\mathrm{H}} = \frac{1}{M}$ as $\beta \ne 0$. Since $M$ is the number of quantization levels, $M \ge 2$, and then $\mu_i^{\mathrm{H}} \le 0.5$. Moreover, $\mu_i^{\mathrm{H}}$ is the behavior feature of sensor $i$ as $TY_i = \mathrm{H}$. Thus, $\mu_i^{\mathrm{H}} > 0.5$. Obviously, the contradiction occurs. Hence, when $\beta \ne 0$, it is impossible to make $\mu_i^{\mathrm{H}} = \frac{1}{M}$.

Therefore, the malicious node is always detectable. ■

*c) Impact of $\zeta$:* We consider the impact of the required false identification probability on the identification probability as $T$ is large enough.

*Proposition 1:* If the attack probability keeps unchanged, the identification probability of the proposed malicious node identification method defined in (20) increases as the required false identification probability increases.

*Proof:* As $T$ is large enough, $\xi_i \to \mu_i^{\mathrm{B}}$ if $TY_i = \mathrm{B}$.

Given the required false identification probability as $\Pi_{\mathrm{f},i} = \zeta$, the optimal threshold can be calculated as $\gamma_i^* = \Phi^{-1}(\zeta)\sqrt{\frac{\mu_i^{\mathrm{H}}(1-\mu_i^{\mathrm{H}})}{T}} + \mu_i^{\mathrm{H}}$. Since $\Phi^{-1}(x)$ is monotonically increasing, $\gamma_i^*$ increases along with the increase of $\zeta$.

With (20), the identification probability can be calculated as $\Pi_{\mathrm{d},i} = \Phi\left(\frac{\gamma_i^* - \mu_i^{\mathrm{B}}}{\sqrt{\frac{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}{T}}}\right)$. Since $\Phi(x)$ is monotonically increasing, $\Phi\left(\frac{\gamma_i^* - \mu_i^{\mathrm{B}}}{\sqrt{\frac{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}{T}}}\right)$ increases as $\gamma_i^*$ increases.

Therefore, as the required $\Pi_{\mathrm{f},i}$ increases, $\Pi_{\mathrm{d},i}$ increases. That is, the number of identified malicious nodes increases as the required false identification probability increases. ■

*d) Impact of the attack probability:* We consider the impact of the attack probability on the identification probability as $T$ is large enough.

*Proposition 2:* If the required false identification probability keeps unchanged, the identification probability defined in (20) increases when the attack probability increases.

*Proof:* As $T$ is large enough, $\xi_i \to \mu_i^{\mathrm{B}}$ if $TY_i = \mathrm{B}$. If $TY_i = \mathrm{B}$, the behavior feature of sensor $i$ is $\mu_i^{\mathrm{B}} = (1-\beta)\mu_i^{\mathrm{H}} + \frac{\beta}{M-1}(1-\mu_i^{\mathrm{H}}) = \frac{M+\beta[1-(M+1)\mu_i^{\mathrm{H}}]}{M-1}$. Since $M$ is the number of quantization levels, $M \geq 2$. Moreover, since $\mu_i^{\mathrm{H}}$ is the behavior feature of sensor $i$ as $TY_i = \mathrm{H}$, $\mu_i^{\mathrm{H}} > 0.5$. Thus, $1-(M+1)\mu_i^{\mathrm{H}} < 0$. Therefore, $\mu_i^{\mathrm{B}}$ decreases as the attack probability increases.

Considering $\Pi_{\mathrm{f},i} = \zeta$, the optimal threshold can be calculated as $\gamma_i^* = \Phi^{-1}(\zeta)\sqrt{\frac{\mu_i^{\mathrm{H}}(1-\mu_i^{\mathrm{H}})}{T}} + \mu_i^{\mathrm{H}}$. With (20), the identification probability can be calculated as $\Pi_{\mathrm{d},i} = \Phi\left(\frac{\gamma_i^* - \mu_i^{\mathrm{B}}}{\sqrt{\frac{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}{T}}}\right)$.

For two attack probabilities, $\beta$ and $\beta'$, and $\beta < \beta'$, the corresponding behavior features, $\mu_i^{\mathrm{B}}$ and $\mu_i'^{\mathrm{B}}$, satisfy $\mu_i^{\mathrm{B}} > \mu_i'^{\mathrm{B}}$. $\frac{\gamma_i^* - \mu_i^{\mathrm{B}}}{\sqrt{\frac{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}{T}}} - \frac{\gamma_i^* - \mu_i'^{\mathrm{B}}}{\sqrt{\frac{\mu_i'^{\mathrm{B}}(1-\mu_i'^{\mathrm{B}})}{T}}} = \frac{\sqrt{T}}{\sqrt{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}\sqrt{\mu_i'^{\mathrm{B}}(1-\mu_i'^{\mathrm{B}})}}$
$\Big[\gamma_i^*(\sqrt{\mu_i'^{\mathrm{B}}(1-\mu_i'^{\mathrm{B}})} - \sqrt{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}) +$
$\mu_i^{\mathrm{B}}\mu_i'^{\mathrm{B}}(\sqrt{\frac{1}{\mu_i^{\mathrm{B}}}-1} - \sqrt{\frac{1}{\mu_i'^{\mathrm{B}}}-1})\Big] < 0$. Since $\Phi(x)$ is monotonically increasing, $\Phi\left(\frac{\gamma_i^* - \mu_i^{\mathrm{B}}}{\sqrt{\frac{\mu_i^{\mathrm{B}}(1-\mu_i^{\mathrm{B}})}{T}}}\right)$ increases as the attack probability increases.

Therefore, as the attack probability increases, $\Pi_{\mathrm{d},i}$ increases. That is, the number of identified malicious nodes increases as the attack probability increases. ■

### B. Reliable Target Location Estimation Approach

Using the malicious node identification method described in Subsection IV.A, it is possible to resolve the Byzantine data attack problem by isolating malicious sensor(s) from the target location estimation process at the FC. After identifying and isolating malicious senor(s), the FC performs the target location estimation process with M-ary quantized data from the residual sensor nodes.

Let $\mathcal{S}$ be the set of all the sensor nodes in a WSN. Let $\mathcal{B}(t)$ be the set of the identified malicious sensor(s) at time interval $t$.

At time interval $t$, the FC collects the reported quantized data from the network, $\boldsymbol{v}(t)$. The FC identifies the malicious sensor(s) using the proposed malicious node identification method, and adds the identified malicious sensor(s) into $\mathcal{B}(t)$.

Then, isolating the received quantized data from sensor nodes belonging to $\mathcal{B}(t)$, the log-likelihood function defined in (7) at time interval $t$ can be rewritten as

$$\ln P(\mathbf{v} \mid \theta)(t) = \sum_{i \in \mathcal{S}\setminus\mathcal{B}(t)} \sum_{k=1}^{M} \delta(v_i(t)-k) \ln P(v_i(t)=k \mid \theta). \tag{23}$$

Hence, after collecting $\mathbf{v}(t)$, the FC estimates the location of the target at time interval $t$ by

$$\hat{\theta}(t) = \arg\max_{\theta} \sum_{i \in \mathcal{S}\setminus\mathcal{B}(t)} \sum_{k=1}^{M} \delta(v_i(t)-k) \ln P(v_i(t)=k \mid \theta). \tag{24}$$

## V. Performance Valuations

In this section, we validate the attack/defense analysis and demonstrate the performance of the proposed distributed target localization with M-ary quantized data under Byzantine data attacks by computer simulations.

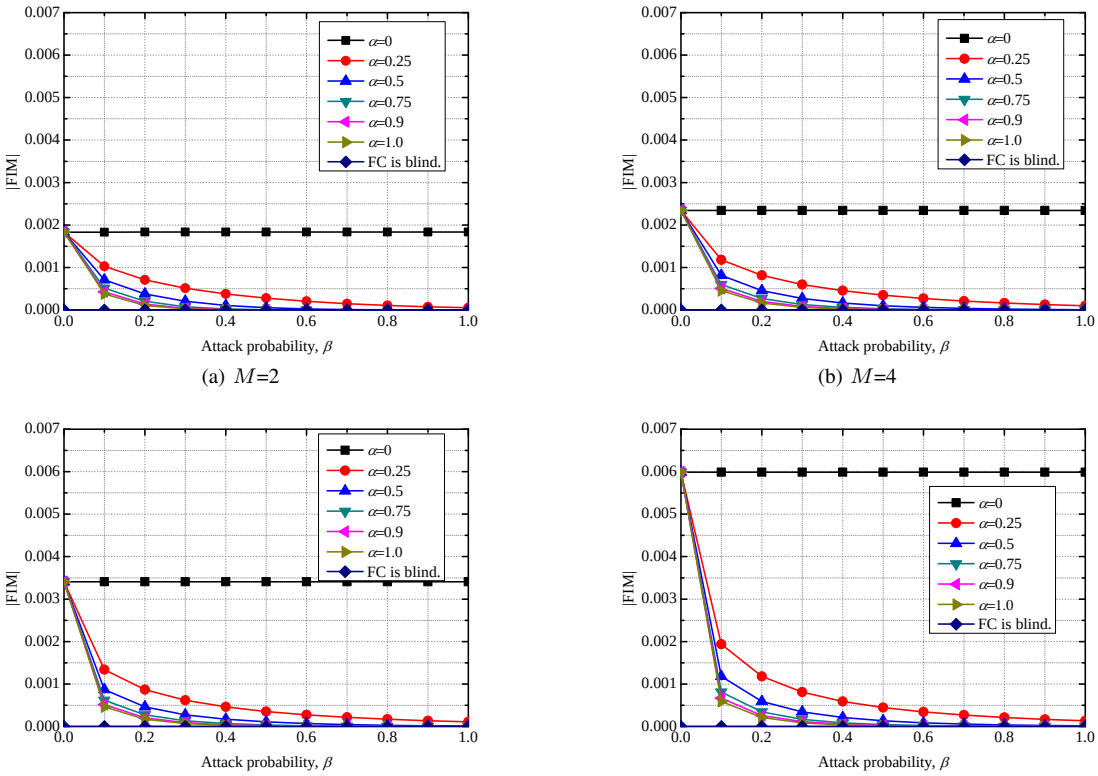
We consider a WSN with $N$=100 sensor nodes uniformly deployed in a 200m×200m area. Each sensor measures $s_i$ is the signal amplitude $a_i$ corrupted by AGWN with zero-mean and $\sigma_n$=0.275. The power at the reference distance $d_0$ is $P_0$=25000. The target location is a normal distribution, i.e., $\theta \sim \mathcal{N}(\varpi_\theta, \sigma_\theta^2\mathbf{I})$, where $\varpi_\theta$ is the center of ROI, and $\sigma_\theta$=38.8218 such that its 99% confidence region covers the entire ROI. The malicious nodes and honest nodes use the same quantization threshold set, since the attacker has no knowledge about the quantization thresholds.

It is assumed that the malicious nodes launch the Byzantine data attack according to the attack strategy derived in Subsection III-B. Moreover, the malicious nodes are distributed in the ROI uniformly.

### A. Probabilistic Byzantine data attack

Fig. 3 shows the impact of probabilistic Byzantine data attack on the performance of distributed target localization in terms of the determinant of FIM, $|\mathrm{FIM}|$, where the number of the quantization levels are set as 2, 4, 8 and 16 in Figs. 3(a), 3(b), 3(c) and 3(d), respectively. In these figures, the maximum value of $|\mathrm{FIM}|$ corresponds to the performance of distributed target localization when all the sensor nodes in the network are honest, i.e., $\alpha$=0. The minimum value of $|\mathrm{FIM}|$ corresponds to the performance of distributed target localization when the FC only uses the prior distribution information of the target location to estimate the location of the target, which means that the FC is made 'blind' completely.

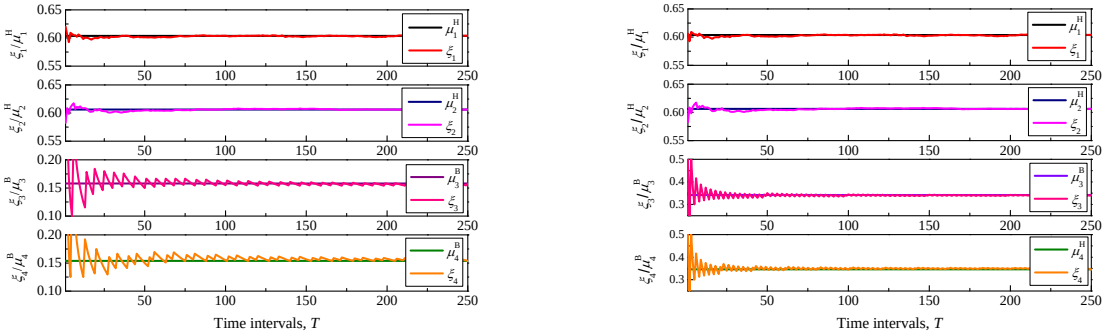
From Figs. 3(a)-3(d), we observe that the determinant of FIM decreases as the attack probability of malicious nodes, $\beta$, and the fraction of malicious nodes, $\alpha$, increase, which means that the performance of distributed target localization degrades, and the damage to the network introduced by malicious nodes increases. From the view of the attacker, malicious nodes would attack the network with a large attack probability to make the maximum damage. However, as the




(a) $M$=2 (b) $M$=4

(c) $M$=8 (d) $M$=16

Fig. 3. The impact of probabilistic Byzantine data attack on the performance of distributed target localization in terms of the determinant of FIM, |FIM|.




(a) $\beta$=1.0 (b) $\beta$=0.5

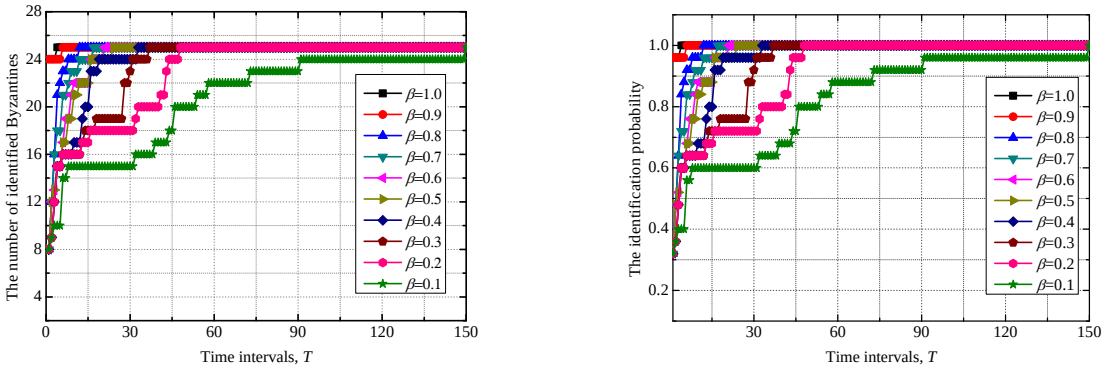
Fig. 4. The estimate of the fitness of the quantized level over time.

attack probability increases, the probability of malicious nodes to be identified will increase. Hence, the attacker faces a tradeoff between the performance damage and the risk to be identified.

Moreover, in Figs. 3(a)-3(d), we observe that when the number of quantization levels, $M$, increases, the fraction of malicious nodes and/or the attack probability should increase in order to make the FC blind. When $\beta$=1 and $M$=4, the attacker needs to compromise at least 75% of sensor nodes to blind the FC. When $\beta$=1 and $M$=8, the attacker needs to compromise at least 87.5% of sensor nodes to blind the FC. Similarly, when $\alpha$=0.9 and $M$=4, the attacker probability should be 0.83 to blind the FC. When $\alpha$=0.9 and $M$=8, the attacker probability should be 0.97. Obviously, this security performance improvement is at the cost of the communication overhead. Hence, the network designer faces a tradeoff between the security guarantee and the communication cost.

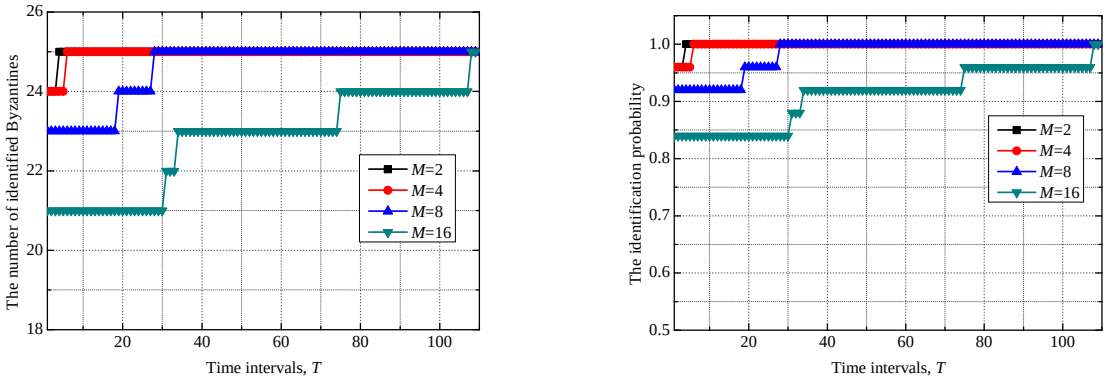
In addition, comparing Figs. 3(a)-3(d), the performance of distributed target localization improves as the number of quantization levels increases. In practical, as $M$ increases, the communication overhead of the quantized data transmission increases. Therefore, the defender should face with a tradeoff between the performance improvement and the communication overhead.

Fig. 4 shows the estimate of the fitness of the quantized level of four sensor nodes over time, where the target is located at (0, 0), sensor 1 located at (56m, 50m) and sensor 2 located at (90m, −50m) are honest, sensor 3 located at (−10m,




(a) The number of identified malicious nodes (b) The identification probability

Fig. 5. The identification performance vs. the number of time intervals and the attack probability.




(a) The number of identified malicious nodes (b) The identification probability

Fig. 6. The identification performance vs. the number of time intervals and the number of quantization levels.

−90m) and sensor 4 located at (−55m, −10m) are malicious, $M$=4 ($\boldsymbol{\eta} = [-\infty, 1.61, 2.03, 2.82, +\infty]$). Fig. 4(a) and 4(b) correspond to $\beta$=1.0 and $\beta$=0.5, respectively.

From Fig. 4, we observe that the sensor's behavior feature is related to the sensor's type (honest or malicious), the sensor's location, and the attack probability for malicious sensor. When $\beta$=1.0, the behavior features of four sensors are 0.6038, 0.6064, 0.1538, and 0.1578, respectively. When $\beta$=0.5, the behavior features of four sensors are 0.6038, 0.6064, 0.3419, and 0.3468, respectively. In general, the behavior feature of honest node is much larger than that of the malicious node. Hence, the type of sensor nodes can be identified according to their behavior features.

Moreover, as the number of time intervals increases, the fitness of the quantized level of four sensor nodes converges to their behavior feature. The convergence rate of the fitness of the quantized level is related to the sensor's location. For malicious sensor nodes, the convergence rate is also related to the attack probability. The convergence rate of the fitness of quantized level decreases along with the increase of the attack probability. Hence, it is applicable to adopt the fitness of the quantized level as a metric to identify the type of sensor nodes. However, the required number of time intervals is different in different scenarios.

### *B. Malicious Node Identification Method*

Fig. 5 shows the impact of the time intervals ($T$) and the attack probability ($\beta$) on the identification performance of the proposed method, in terms of the number of identified malicious nodes in Fig. 5(a) and the identification probability in Fig. 5(b), where the number of malicious nodes is 25, $M$ =4 ($\boldsymbol{\eta} = [-\infty, 1.61, 2.03, 2.82, +\infty]$), and $\zeta$ =0.01.

From Fig. 5, we observe that as the number of time intervals increases, the performance of the malicious node identification method improves. However, the performance degrades as the attack probability decreases. Specifically, malicious nodes are identified successfully at $T$ = 5, 7, 12, 17, 21, 24, 33, 37, 48, and 150 when $\beta$ = 1.0, 0.9, 0.8, 0.7, 0.6, 0.5, 0.4, 0.3, 0.2 and 0.1, respectively. The reason is that the required number of local observations for estimating the fitness of the quantized level precisely increases as the attack probability decreases. This result is also found from Fig. 4. For a practical distributed target localization system, the larger the required number of time intervals for successful identification, the longer the effect of the malicious nodes on the estimation performance. Hence, to identify all the malicious nodes in a short span time is essential for a malicious node identification method.

Fig. 6 shows the impact of the number of time intervals ($T$) and the number of quantization levels ($M$) on the identification performance of the proposed method, in terms of the number of identified malicious nodes in Fig. 6(a) and

the identification probability in Fig. 6(b), where the number of malicious nodes is 25, $\beta$ =1.0, and $\zeta$ =0.01. From Fig. 6, we observe that as the number of time intervals increases, the performance of the proposed malicious node identification method improves. However, the identification performance degrades as the number of quantization levels increases. Specifically, malicious nodes are identified successfully at $T$ = 4, 5, 28, and 108 for $M$ = 2, 4, 8 and 16, respectively. The reason for this phenomenon is that the required observation time window for estimating the fitness of the quantized level precisely increases as the number of quantization levels increases. From the view of malicious node identification, the number of quantization levels should be set a smaller value. However, from the view of estimation performance, the number of quantization levels should be set a larger value based on the results in Fig. 3. Hence, the network designer should face with a tradeoff among the estimation performance, the security and the communication overhead. Fig. 7 shows the ROC curves of the proposed malicious node identification method, where the number of malicious nodes is 25, $M$ =4 ($\boldsymbol{\eta} = [-\infty, 1.61, 2.03, 2.82, +\infty]$), and $T$ =24.

From Fig. 7, we observe that as the required false identification probability increase, the identification probability of the proposed method increases. Moreover, as the attack probability increases, the identification probability of the proposed method increases. When $\beta \geq$0.5, all the malicious nodes are identified successfully. This result can also be found in Fig. 5. When $T$=24, all the malicious nodes are identified successfully for $\beta \geq$0.5. Hence, in the proposed malicious node identification method, it is necessary to set different thresholds for malicious nodes with different attack behaviors.

### *C. Distributed target localization scheme with M-ary quantized data under Byzantine attacks*

Fig. 8 shows the estimation performance, in terms of the root mean square error (RMSE) value of the estimator, where the number of malicious nodes is 25, $M$ =4 ($\boldsymbol{\eta} = [-\infty, 1.61, 2.03, 2.82, +\infty]$), and $\zeta$ =0.01. Fig. 8(a) shows the impact of the attack probability on the estimation performance, where $T$ =23. Fig. 8(b) shows the impact of the number of time intervals on the estimation performance, where $\beta$ =0.8.

From Fig. 8(a), we observe that for the distributed target localization scheme with Byzantines (that is, the FC cannot identify and exclude the malicious nodes), the estimation error increases sharply as the attack probability increases. Specifically, the values of the RMSE are about 3.6870m, 6.1297m and 9.1329m for $\beta$ = 0.3, 0.5 and 0.8, respectively. Using the proposed malicious node identification method and the malicious node identification method proposed in [20], all the malicious nodes are identified successfully for $T$ =23 when $\beta \geq$0.5. The estimation performance of the distributed target localization scheme with Byzantines using proposed identification method and the identification method proposed in [20] is close to that of the distributed target localization scheme without Byzantines. Specifically, the values of the RMSE are about 0.1523m, 0.1608m and 0.1607m for the distributed target localization scheme without Byzantines, the

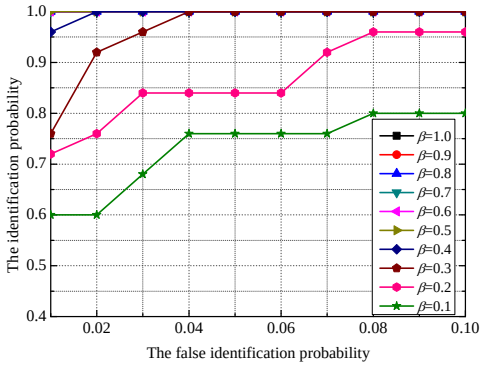
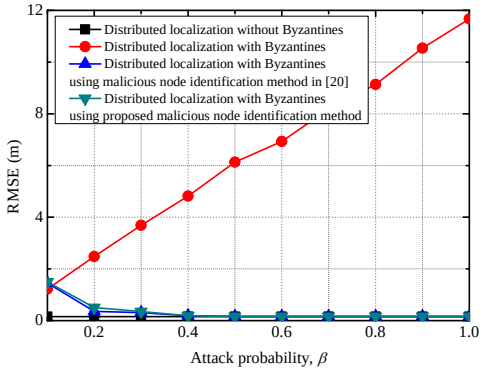
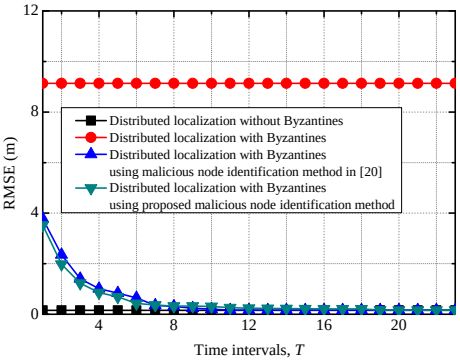



Fig. 7. ROC curves of the proposed malicious node identification method.




(a) $\beta$




(b) $T$

Fig. 8. The estimation performance.

distributed target localization scheme with Byzantines using proposed identification method, and, the distributed target localization scheme with Byzantines using the identification method proposed in [20], respectively. For the distributed target localization scheme with Byzantines using proposed identification method and the identification method proposed in [20], the estimation error increases as the attack probability decreases when $\beta <$ 0.5. The reason for this phenomenon is that not all of the malicious nodes are identified at $T$ = 23 when $\beta <$0.5. From Fig. 8(b), we observe that as the number of time intervals increases, the estimation error reduces for the distributed target localization scheme with Byzantines using proposed identification method and the identification method proposed in [20]. The reason is that the number of identification malicious nodes increases as the number of time

intervals increases. The results shown in Fig. 5 that all of the malicious nodes are identified successfully at $T$ =12 for the proposed malicious node identification method.

In addition, from Figs. 8(a) and 8(b), we observe that the performance of the distributed localization with the proposed malicious node identification method and the identification method proposed in [20] is nearly the same. However, for the malicious node identification method proposed in [20], the FC calculates the deviation of each sensor between the real amplitude and the inverse of the quantizer. Due to the inverse of the quantization process, the computational complexity of the malicious node identification method proposed in [20] is higher than that of the proposed malicious node identification method in this paper.

Therefore, using the proposed malicious node identification method, the distributed target localization scheme with M-ary quantized data is robust against Byzantine data attacks.

## VI. Conclusion

In this paper, we studied the problem of distributed target localization with M-ary quantized data in WSNs under Byzantine data attacks. We have significantly extended the research results obtained in [20] by considering a probabilistic Byzantine attack model and a more practical Byzantine attack defense method in the distributed target localization with M-ary quantized data. We introduced a probabilistic Byzantine data attack model for the distributed target localization with M-ary quantized data, where the compromised sensor node modifies its quantized measurement to the other quantized levels independently and probabilistically. The negative effect of defined probabilistic Byzantine data attack model on the distributed target localization with M-ary quantized data is characterized. We derived the condition that makes the FC completely incapable of estimating the target location using collected quantized data from the network. We also found an optimal strategy of the resource-limited Byzantine data attacks, which maximally degrades the estimation performance of the network. Moreover, in the perspective of the defender, we proposed a malicious node identification method and a reliable target location estimation approach to defend against Byzantine data attack on the distributed target localization. In the proposed malicious node identification method, the FC identifies the malicious sensor(s) by using the report history and the location of each sensor node, the knowledge of the quantization scheme and the estimated target location. The performance of the malicious node identification method is analytically evaluated. After identifying all the malicious sensor(s) in the network with the proposed malicious node identification method and excluding them from the distributed estimation process, the FC estimates the location of the target with M-ary quantized data from the residual sensor nodes. The numerical results demonstrate that the proposed malicious node identification method can successfully identify all the malicious sensor(s) in a limited time span, and the proposed location estimation approach is robust against Byzantine data attacks.

## Acknowledgment

This work was partly supported by National Natural Science Foundation of China (No. 61471318, No. 61571410, No. 61071127).

## Appendix A
## Proof for Theorem 2

The data's contribution to the posterior Fisher Information is given by

$$\begin{aligned}\mathbf{F}_{\mathrm{D}} &= -\mathbf{E}\left[\frac{\partial^2}{\partial\theta^2}\ln P(\mathbf{v}\mid\theta)\right]\\ &= \sum_{m=1}^{M} P(v_i=m\mid\theta)\left(\frac{\partial \ln P(v_i=m\mid\theta)}{\partial\theta}\right)^2\\ &= (1-\alpha Mp)^2\sum_{m=1}^{M}\frac{1}{P(v_i=m\mid\theta)}\,( \qquad (25)\\ &\left(\frac{\partial P(u_i=m\mid\theta)}{\partial\theta}\right)^2. \qquad (26)\end{aligned}$$

On partially differentiating $\mathbf{F}_{\mathrm{D}}$ with respect to $p$, we have

$$\begin{aligned}&\frac{\partial \mathbf{F}_{\mathrm{D}}}{\partial p}\\ &= 2(1-\alpha Mp)(-\alpha M)\sum_{m=1}^{M}\frac{1}{P(v_i=m\mid\theta)}\left(\frac{\partial P(u_i=m\mid\theta)}{\partial\theta}\right)^2\\ &+(1-\alpha Mp)^2\sum_{m=1}^{M}\\ &\frac{-1}{[P(v_i=m\mid\theta)]^2}[\alpha-\alpha M P(u_i=m\mid\theta)]\left(\frac{\partial P(u_i=m\mid\theta)}{\partial\theta}\right)^2\\ &= 2(1-\alpha Mp)(-\alpha M)\sum_{m=1}^{M}\Bigg\{[\alpha p+(1-\alpha Mp)P(u_i=m\mid\theta)]\\ &\left[\frac{1}{P(v_i=m\mid\theta)}\frac{\partial P(u_i=m\mid\theta)}{\partial\theta}\right]^2\Bigg\}\\ &+(1-\alpha Mp)^2\sum_{m=1}^{M}\\ &\frac{-1}{[P(v_i=m\mid\theta)]^2}[\alpha-\alpha M P(u_i=m\mid\theta)]\left[\frac{\partial P(u_i=m\mid\theta)}{\partial\theta}\right]^2\\ &= -(1-\alpha Mp)\alpha\Bigg\{(1+\alpha Mp)\\ &\sum_{m=1}^{M}\left[\frac{1}{P(v_i=m\mid\theta)}\frac{\partial P(u_i=m\mid\theta)}{\partial\theta}\right]^2\\ &+(1-\alpha Mp)M\\ &\sum_{m=1}^{M}P(u_i=m\mid\theta)\left[\frac{1}{P(v_i=m\mid\theta)}\frac{\partial P(u_i=m\mid\theta)}{\partial\theta}\right]^2\Bigg\}.\end{aligned} \qquad (27)$$

According to the discussion of the blind condition, it is clear that two cases exist, namely $\frac{M-1}{M\beta}<1$ and $\frac{M-1}{M\beta}>1$. We analyze each case in detail as follows.

Case 1: $\frac{M-1}{M\beta}<1$

When $\frac{M-1}{M\beta} < 1$ , the fraction of malicious sensor nodes for blinding the FC completely is $\alpha_{\text{blind}} = \frac{M-1}{M\beta}$ according to Theorem 1.

Now, we focus on the optimal Byzantine data attack when the FC is not made blind by the Byzantine attacker. Thus, the fraction of malicious sensor nodes in the WSN satisfies $\alpha < \frac{M-1}{M\beta}$. Since $0 \leq p \leq \frac{\beta}{M-1}$, we have $1 - \alpha M p > 0$. Hence, we have $\frac{\partial \mathbf{F}_{\text{D}}}{\partial p} < 0$, which means $\mathbf{F}_{\text{D}}$ is a decreasing function of $p$. The minimum value of $\mathbf{F}_{\text{D}}$ is achieved at the maximum value of $p$, i.e. $p^* = \frac{\beta}{M-1}$.

Case 2: $\frac{M-1}{M\beta} > 1$

When $\frac{M-1}{M\beta} > 1$, the fraction of malicious sensor nodes for blinding FC completely is $\alpha_{\text{blind}} = 1$ according to Theorem 1. Hence, when the FC is not made blind, $\alpha < 1$.

As $\frac{M-1}{M\beta} > 1$ , we have $\frac{\beta}{M-1} < \frac{1}{M}$. Moreover, we have $\frac{1}{M} < \frac{1}{\alpha M}$ since $\alpha < 1$. Thus, $\frac{\beta}{M-1} < \frac{1}{\alpha M}$.

When $0 \leq p \leq \frac{\beta}{M-1}$, we have $1 - \alpha M p > 0$. Hence, we have $\frac{\partial \mathbf{F}_{\text{D}}}{\partial p} < 0$ , which means $\mathbf{F}_{\text{D}}$ is a decreasing function of $p$. The minimum value of $\mathbf{F}_{\text{D}}$ is achieved at the maximum value of $p$ , i.e. $p^* = \frac{\beta}{M-1}$.

Therefore, the optimal solution to the problem (P.1) is given as $p_{lk} = \begin{cases} \frac{\beta}{M-1} & ; \quad \text{if } l \neq k. \\ 1-\beta & ; \quad \text{if } l = k. \end{cases}$

## REFERENCES


[1] C. W. Reed, R. Hudson, and K. Yao, "Direct joint source localization and propagation speed estimation", *Proc. of IEEE ICASSP 1999*, Phoenix, Arizona, USA, pp. 1169-1172, Mar. 1999.

[2] A. Yassin, Y. Nasser, M. Awad, A. Al-Dubai, R. Liu, C. Yuen, R. Raulefs, and E. Aboutanios, "Recent advances in indoor localisation: A survey on theoretical approaches and applications," *IEEE Communications Surveys & Tutorials*, 2016.

[3] L. M. Kaplan, L. Qiang, and N. Molnar, "Maximum likelihood methods for bearing-only target localization," *Proc. of IEEE ICASSP 2001*, Salt Lake City, UT, USA, pp. 3001-3004, May 2001.

[4] J. Chen, R. Hudson, and K. Yao, "Maximum likelihood Parametric Approach to Source Localization," *Proc. of IEEE ICASSP 2001*, Salt Lake City, UT, USA, pp. 3013-3016, May 2001.

[5] S. Marano, V. Matta, P. Willett, and L. Tong, "Support-based and ML approaches to DOA estimation in a dumb sensor network," *IEEE Trans. on Signal Processing*, vol. 54, no. 4, pp. 1563-1567, Apr. 2006.

[6] D. Li and Y. Hu, "Energy-based collaborative source localization using acoustic micro-sensor array," *EURASIP Journal on Applied Signal Processing*, vol. 2003, no. 4, pp. 321-337, Apr. 2003.

[7] X. Sheng and Y. Hu, "Maximum likelihood multiple-source localization using acoustic energy measurements with wireless sensor networks," *IEEE Trans. on Signal Processing*, vol. 53, no. 1, pp. 44-53, Jan. 2005.

[8] N. Patwari and A. Hero, "Using proximity and quantized RSS for sensor localization in wireless networks," *Proc. of the 2nd Int. ACM Workshop Wireless Sensor Network Applicaitons*, San Diego, CA, USA, pp. 20-29, Sep. 2003.

[9] R. Niu and P. K. Varshney, "Target localization estimation in sensor networks with quantized data," *IEEE Trans. on Signal Processing*, vol. 54, no. 12, pp. 4519-4528, Dec. 2006.

[10] A. Noroozi and M. A. Sebt, "Weighted least squares target location estimation in multi-transmitter multi-receiver passive radar using bistatic range measurements," *IET Radar Sonar and Navigation*, vol. 10, no. 6, pp. 1088-1097, June 2016.

[11] H. Ma, Y. Yang, Y. Chen, K. J. R. Liu, and Q. Wang, "Distributed state estimation with dimension reduction preprocessing," *IEEE Trans. on Signal Processing*, vol. 62, no. 12, pp. 3098-3110, Dec. 2014.

[12] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM - Wireless sensor networks*, vol. 47, no. 6, pp. 53-57, June 2004.

[13] A. Boukerche, H.A.B. Oliveira, E.F. Nakamura, and A.A.F. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Communications Magazines*, vol. 46, no. 4, pp. 96-101, Apr. 2008.

[14] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. on Programming Languages and Systems*, vol. 4, no. 3, pp. 382-401, July 1982.

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

[16] K. Agrawal, A. Vempaty, H. Chen, and P. K. Varshney, "Target localization in wireless sensor networks with quantized data in the presence of Byzantine attacks," *Proc. of the 45th Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Pacific Grove, CA, USA, pp. 1669-1673, Nov. 2011.

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

[18] H. Chen, L. Xie, and C. Shen, "Optimal Byzantine attack strategy for distributed localisation with M-ary quantised data," *Electronics Letters*, Vol. 51, no. 25, pp. 2158-2160, Dec. 2015.

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

[20] V. S. S. Nadendla, Y. S. Han, and P. K. Varshney, "Distributed inference with M-ary quantized data in the presence of Byzantine attacks," *IEEE Trans. on Signal Processing*, vol. 62, no. 10, pp. 2681C2695, Oct. 2014.

[21] P. Chen, Y. S. Han, H. Lin, and P. K. Varshney, "Optimal Byzantine attack for distributed inference with M-ary quantized data," *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, pp. 2474-2478, July 2016.

[22] A. Basel, J. Zhang, and R. S. Blum, "Attacks on sensor network parameter estimation with quantization: Performance and asymptotically optimum processing," *IEEE Trans. on Signal Processing*, vol. 63, no. 24, pp. 6659-6672, Dec. 2015.

[23] A.Vempaty, Y. S. Han, and P. K. Varshney, "Target localization in wireless sensor networks using error correcting codes," *IEEE Trans. on Information Theory*, vol. 60, no. 1, pp. 697-712, Jan. 2014.

[24] A. Vempaty, Y. S. Han, and P. K. Varshney, "Byzantine tolerant target localization in wireless sensor networks over non-ideal channels," *Proc. of 13th International Symposium on Communications and Information Technologies (ISCIT)*, Ko Samui, Thailand, pp. 407-411, Sep. 2013.

[25] C. Wilson, and V. Veeravalli, "MMSE estimation in a sensor network in the presence of an adversary," *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, pp. 2479-2483, July 2016.

[26] A. Vempaty, K. Agrawal, P. K. Varshney, and H. Chen, "Adaptive learning of Byzantines' behavior in cooperative spectrum sensing," *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, Quintana-Roo, Mexico, pp. 1310-1315, Mar. 2011.

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

[28] L. Zhang, G. Ding, Q. Wu, and F. Song, "Defending against Byzantine attack in cooperative spectrum sensing: Defense reference and performance analysis," *IEEE Access*, vol. 4, no. 8, pp. 4011-4024, Aug. 2016.

[29] J. Y. Koh, J. C. M. Teo, and W. Wong, "Mitigating byzantine attacks in data fusion process for wireless sensor networks using witnesses," *Proc. of IEEE International Conference on Communication Systems (ICCS)*, Macau, China, pp. 263-267, Nov. 2014.

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

[31] H. Li, and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Trans. on Wireless Communications*, vol. 9, no. 11, pp. 3554-3565, Nov. 2010.

[32] J. Luo, and Z. Cao, "Distributed detection in wireless sensor networks under Byzantine attacks," *International Journal of Distributed Sensor Networks*, vol. 2015, no. 222, pp. 1-18, Jan. 2015.

[33] D. Messerschmitt, "Quantizing for maximum output entropy," *IEEE Trans. on Information Theory*, vol. 17, no. 5, pp. 612-612, Sep. 1971.

[34] B. V. Gendenko and A.N. Kolmogorov, *Limit Distributions for Sums of Independent Random Variables*. New York: Addison-Wesley Press, 1954.

[35] A. W. van der Vaart and J. A. Wellner, *Glivenko-Cantelli Theorems*. Australia: Springer Press, 1996.