International Journal Of
Industrial Electronics Control and Optimization
Print ISSN: 3517-2645
Online ISSN: 3568-2645
Homepage: https://ieco.usb.ac.ir/

RSS Localization in the Presence of Byzantine Attacks using MAP Estimation

Mahdiye Mohammadi [1] | Hadi Zayyani [2] | Mehdi Bekrani [3]

Department of Electrical and Computer Engineering, Qom University of Technology, Qom, Iran [1,2,3]
Corresponding author's email: bekrani@qut.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 21-February-2025
Received in revised form: 13-April-2025
Accepted: 10-May-2025
Published online: 22-June-2026

Keywords:
Anchor node
Fusion center (FC),
MAP estimator,
Target node.

ABSTRACT

Target localization in wireless sensor networks (WSNs) is essential for various applications. This study investigates received signal strength (RSS)-based localization in the presence of malicious anchor nodes that intentionally alter signal power levels to mislead the fusion center (FC) and degrade positioning accuracy. To address this challenge, we adopt a Maximum a Posteriori (MAP) estimator, which estimates the target location even when the path loss exponent is unknown. We show that the MAP estimation method can estimate the WSN unknown parameters, including the path loss exponent, the distance between the target node and anchor nodes, and the received signal strength. Simulation results demonstrate that the MAP method achieves lower localization errors than other competing approaches when the Signal-to-Noise Ratio (SNR) exceeds 10 dB, although it entails higher computational complexity in terms of simulation run time. The proposed approach is particularly efficient in applications in transportation, military operations, security, smart industries, and mapping.

I. Introductions

Wireless sensor networks (WSNs) have diverse applications, including tracking goods in supply chains, monitoring air quality, observing farm animal behavior, detecting landslides, and providing navigation assistance in environments like shopping malls and airports.

A WSN is composed of multiple sensor nodes that communicate and collaborate to achieve a common objective. Sensor nodes collect data and transmit it to a fusion center (FC) for further analysis. Radio frequency (RF)-based target localization is particularly valuable in military and industrial applications. Target localization can be achieved using various methods, including angle of arrival (AOA) [1], time of arrival (TOA) [2], and time difference of arrival (TDOA) [3]. However, among these techniques, the received signal strength (RSS) method is more cost-effective and does not require synchronization [4]. Moreover, some studies have explored hybrid localization techniques that combine methods such as RSS and AOA, as presented in [5] and [6].

Significant advancements have been made in RSS-based localization due to extensive research. Most studies assume that anchor nodes function reliably, but this may not always be the case, particularly in the presence of malicious attacks. During such attacks, compromised anchor nodes transmit incorrect measurements to the FC, thereby disrupting localization accuracy. As a result, the FC may fail to determine the precise location of the target node. Anchor nodes that intentionally provide false data and interfere with the localization process are referred to as Byzantine nodes. The presence of these nodes introduces significant challenges to accurate localization.

Several methods have been explored in the literature to enhance localization accuracy in the presence of malicious anchor nodes. One approach involves iterative gradient descent, as discussed in [7]. Triangulation and RF-based fingerprinting methods have also been investigated in [8], where an adaptive least squares (LS) technique and Least Median of Squares (LMdS) were proposed for triangulation, while a median-based distance metric was employed for RF fingerprinting. In [8] and [9], techniques were introduced to detect and eliminate malicious nodes, thereby mitigating their impact on the localization process. The study in [10] analyzed uncoordinated attacks, where malicious anchor

nodes manipulate their transmission power following a Gaussian distribution to disrupt localization. Conversely, [11] assumed a uniform distribution for the transmission power, making the uncoordinated attack model more realistic.

Additionally, [11] examined both coordinated and uncoordinated attacks and proposed three localization techniques— Weighted LS (WLS), Secure WLS, and $l_1 - norm$ based (LN_1) localization—capable of identifying and mitigating the influence of malicious anchor nodes in the network. Localization in WSNs with unknown sensor positions has been explored in [12] and [13], offering a cost-effective solution that eliminates the need for time synchronization and extensive local processing.

Several approaches based on RSS have been proposed to address synchronization and computational challenges, utilizing LS or maximum likelihood (ML)-based source localization methods [14], [15]. Due to energy and bandwidth constraints, anchor nodes often rely on binary or multi-bit quantized data for communication. The problem of target node localization using quantized data has been investigated in various studies [16], [17]. In [18], an adversary is assumed to take control of certain sensors, compelling them to transmit false data to the FC.

A Byzantine identification scheme was introduced in [19] for distributed detection, where malicious nodes are adaptively identified, and their information is leveraged to enhance detection performance. The Byzantine problem has also been studied in the context of network coding and information theory [20], [21]. In [22], the ML estimation was employed for target localization in a WSN using binary quantized data, analyzing the impact of Byzantine attacks. In such a scenario, the performance metric is the Fisher information [23]. The work in [24] proposed an ML-based localization approach along with a Byzantine detection method and a dynamic non-uniform threshold design to mitigate malicious interference. Meanwhile, [25] examined target localization in the presence of malicious sensors using a Monte Carlo-based approach. This study assumed a random target location and evaluated the performance of the minimum mean square error (MMSE) estimator. The presence of malicious anchor nodes made performance evaluation more complex, with posterior Fisher information and the posterior Cramér-Rao lower bound (CRLB) serving as key performance measures.

In recent studies, one research effort reformulates the localization problem as a Generalized Trust Region Subproblem (GTRS) by applying specific approximations to enhance tractability [26]. However, these approximations can reduce the overall performance of the method. Additionally, the more recent work in RSS-based localization [27] proposes a cooperative localization approach in wireless sensor networks (WSNs) using biased RSS measurements, addressing a scenario with the presence of Byzantine nodes. This study employs semidefinite programming (SDP) with l_1 and l_2 norms to address the non-convexity of the maximum likelihood (ML) estimator, which is a notable advantage. Nonetheless, a key drawback of this method is its requirement to estimate both the biases and the distances/locations, which increases the computational complexity and may compromise localization accuracy.

In this study, we estimate the location of the target node using the Maximum A Posteriori (MAP) estimation method, which differs from the approach in [25] that employs the Minimum Mean Square Error (MMSE) estimator for the localization problem. In addition to the target node's location, denoted as Z, other unknown parameters include the Path Loss Exponent (PLE) (β), the distance between anchor nodes and the target node (d), and RSS. Each of these parameters is estimated using the MAP approach. We conduct a comprehensive analysis of the MAP method, detailing the estimation process for the path loss exponent, distances between non-malicious anchor nodes and the target node, RSS values, and the target node's location. The main contributions of this paper are as follows: (1) It computes the MAP estimator for all unknown variables, unlike other approaches such as the ML estimator, which does not consider prior distributions, and the MMSE estimator, which requires complex expectations and integral computations. (2) It employs an alternating maximization approach for estimating unknown variables, which simplifies the optimization process by updating one variable at a time instead of optimizing all variables jointly. (3) The study addresses RSS-based localization under Byzantine attacks in the case where the path loss exponent is also unknown, and estimates the PLE as part of the overall algorithm. Furthermore, we compare the MAP method with other state-of-the-art approaches to evaluate its performance. In the experimental results section, we present a detailed analysis of our MATLAB-based simulations, accurately reporting the estimation outcomes for all unknown parameters.

II. System model

We consider a network consisting of N anchor nodes with known locations and a single target node with an unknown location. It is assumed that all anchor nodes are within the communication range of the target node and transmit at a predefined power level. The target node extracts the RSS from packets transmitted by the anchor nodes and estimates its distance from each of them. Using these estimated distances and the known anchor node locations, a localization technique is applied to determine the target node's position.

The signal power loss is primarily influenced by the path loss exponent, which is modeled using the log-distance path loss model as follows:

$$P^r = P_0 - 10\beta \log_{10}(d) + \eta \quad (1)$$

where P^r represents the received power at the target, P_0 is the received power when the single anchor node is one meter away from the target node, β is the path loss exponent, d denotes the distance between the anchor node and the target node, and η is additive noise, assumed to be zero-mean, independently, and identically distributed (i.i.d) Gaussian.

The received power can be expressed as follows:

$$X_{i.j} = (p_i{}^r)_j = \begin{cases} P_0 - 10\beta \log_{10}(d_i) + \eta_{i.j}\,, i \text{ is non} - \text{malicious} \\ P_{0i} - 10\beta \log_{10}(d_i) + \eta_{i.j}, \;\; i \text{ is malicious} \end{cases} \quad (2)$$

where $(p_i{}^r)_j$ represents the received power from the i^{th} anchor node during the j^{th} observation, and P_{0i} represents the transmit power of the i^{th} malicious anchor node, while β is the path loss exponent, which follows a normal distribution with mean β_0 and variance σ_β^2. The power P_0 follows a normal distribution with mean $\overline{p_0}$ and variance $\sigma_{\varepsilon_P}^2$. Similarly, P_{0i} follows a normal distribution with mean $\overline{p_{0i}}$ and variance $\sigma_{a,i}^2$. The additive noise $\eta_{i.j}$ is assumed to be normally distributed with zero mean and variance $\sigma_{\eta_i}^2$. The target node is located at $\mathrm{Z} = [x_t\,.y_t]^T$. The distance between the target node and the i^{th} anchor node is given by:

$$d_i = \sqrt{(x_i - x_t)^2 + (y_i - y_t)^2} \quad (3)$$

The distance vector for all anchor nodes is:

$$d = [d_1.d_2 \ldots d_N]^T \quad (4)$$

The number of observations or snapshots is P, where j ranges from 1 to P. The observation vector for the i^{th} anchor node is:

$$\boldsymbol{X}_i = [X_{i.1}.X_{i.2} \ldots X_{i.P}]^T \quad (5)$$

where $X_{i.j} = (p_i{}^r)_j$. The total observation matrix is:

$$\mathrm{X} = [X_1.X_2 \ldots X_N]_{P\times N} \quad (6)$$

The vector of unknown parameters is:

$$\theta = [\beta, d, P_0^{'}, Z] \quad (7)$$

where

$$P_{0i}^{'} = \begin{cases} P_0 & i \text{ is non} - \text{malicious} \\ P_{0i} & i \text{ is malicious} \end{cases} \quad (8)$$

III. Estimation of the target location

Figure 1 illustrates the typical placement of sensors in the network. In this figure, the target node, located at [20,10], is represented by a green circle. The anchor nodes are positioned at [−50,−50], [−50,50], [50,−50], [50,50], [−30,−30], [−30,30], [30,−30], and [30,30].

Among these anchor nodes, we assume that the nodes at [−50,−50] and [50,50] are Byzantine, meaning they introduce false information to disrupt the localization process. In Figure 1, non-malicious anchor nodes are depicted in blue, while malicious anchor nodes are shown in red.

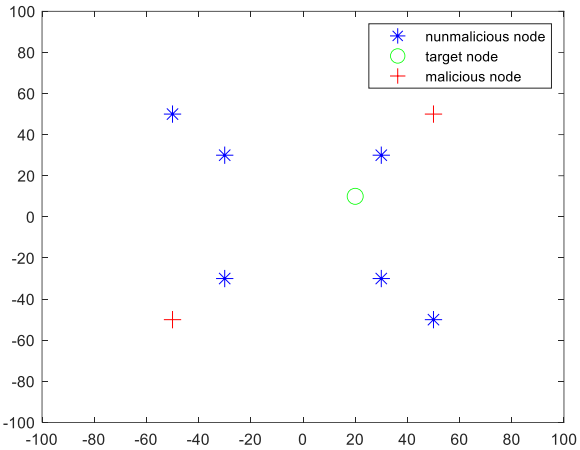


Fig. 1. Location of sensors in the network.

For target localization, the known locations of the sensors in the network are used to estimate the target's position based on RSS from these sensors. To achieve this, we employ the LS, WLS, and the proposed MAP methods. We then compare the performance of the MAP method against the LS and WLS methods to evaluate its effectiveness in target localization.

A. Estimating the location of the target node using the Linear LS (LLS) method

In [28], the LLS method is proposed for target node localization. In this approach, the target location is estimated using LLS estimation based on the received signal power from surrounding anchor nodes. To implement the LLS method, we first need to define a range variable that converts the RSS measurements into a linear model for estimating the target location.

Let the i^{th} anchor node be located at $[x_i.y_i]^T$. The range variable, R, is defined as follows:

$$R = x^2 + y^2 \quad (9)$$

The distance d_i between the target node and the i^{th} anchor node is given by:

$$d_i = \sqrt{(x_t - x_i)^2 + (y_t - y_i)^2} \quad (10)$$

Squaring both sides of equation (50) yields:

$$-2x_ix_t - 2y_iy_t + R = {d_i}^2 - {x_i}^2 - {y_i}^2 \quad (11)$$

To express this problem in matrix form, we get the following system:

$$A\lambda = b \quad (12)$$

where λ represents the unknowns to be estimated. The matrix A is:

$$A = \begin{bmatrix} -2x_1 & -2y_1 & 1 \\ -2x_2 & -2y_2 & 1 \\ \vdots & \vdots & \vdots \\ -2x_N & -2y_N & 1 \end{bmatrix} \quad (13)$$

The vector λ is:

$$\lambda = [x\ y\ R]^2 \quad (14)$$

and the observation vector b is:

$$b = \begin{bmatrix} {d_1}^2 - {x_1}^2 - {y_1}^2 \\ {d_2}^2 - {x_2}^2 - {y_2}^2 \\ \vdots \\ {d_N}^2 - {x_N}^2 - {y_N}^2 \end{bmatrix} \quad (15)$$

In this formulation, A is a known matrix, λ is the parameter vector to be estimated, and b is the observation vector.

The solution to the LLS optimization problem is given by:

$$\hat{\lambda} = (A^T A)^{-1} A^T b \quad (16)$$

B. Estimating the target location using the WLS method

The WLS method for localization is introduced in [11]. This method assigns weights to anchor nodes based on their distance from the target node. The target node receives P packets from anchor nodes and computes the mean received power. Using this power measurement, the target node estimates its distance from each anchor node. The WLS model is a refined version of the LS method.

The measurement model can be expressed as:

$$b = A\theta + w \quad (17)$$

where w is the noise vector, b is the measurement vector, A is the coefficient matrix, and θ is the vector of unknown parameters.

Without assuming a specific probability distribution for w, the target node's estimated location can be obtained by solving the WLS problem. The WLS estimate minimizes the weighted error:

$$\hat{\theta} = \underset{\theta}{\operatorname{argmin}} (b - A\theta)^T W (b - A\theta) \quad (18)$$

where W is a weight matrix that accounts for variations in measurement confidence, typically set as the inverse of the noise covariance matrix. In [11], a weighted diagonal matrix is considered whose elements are the inverse of the variance $\sigma_{\hat{d}_i}^2$ of the estimated distance between the i^{th} anchor node and the actual target node as follows:

$$W = \operatorname{diag}\left\{\frac{1}{\sigma_{\hat{d}_1}^2}, \cdots, \frac{1}{\sigma_{\hat{d}_N}^2}\right\} \quad (19)$$

The solution to this optimization problem is given by:

$$\hat{\theta} = (A^T W A)^{-1} A^T W b \quad (20)$$

where A and b are as defined in (13) and (15), respectively. This approach refines the target location estimate by reducing the influence of measurements with higher uncertainty.

In the WLS method, greater weight is assigned to anchor nodes that are closer to the target node, and specific weights are applied to the received signal strength based on the distance between each sensor and the target node. Since RSS-based localization methods also estimate the distances, these estimated distances are used to determine which anchor nodes are closer to the target, allowing greater weights to be assigned accordingly. While this approach improves accuracy, it increases the cost function, leading to longer computation times to determine the exact location of the target node, causing delays in reaching the goal in comparison to the LS method. However, due to its weighting of the received signal strength, the WLS method can localize the target node with lower error, making it more accurate in estimating the target's position despite the higher computational cost in comparison to the LS method.

IV. The proposed target localization

In this paper, we employ the MAP estimation method to determine the location of the target node [29]. In the MAP method, the target node location is estimated by maximizing the posterior distribution $P(\theta|X)$ [29], where θ represents the vector of unknown parameters, which includes the target location $Z = [x_t, y_t]^T$, the path loss parameter β, the received signal strength d, and a model parameter P_0. The posterior distribution is typically expressed as:

$$\max P(\theta|X) = \max\{\log P(\theta) + \log P(X|\theta)\} \quad (21)$$

The prior distribution $P(\theta)$ is defined as:

$$\log P(\theta) = \log\{P(Z)P(\beta|Z)P(d|\beta,Z)P\left(P_0^{'}\middle|d,\beta,Z\right)\} \quad (22)$$

This can be expanded as:

$$\log P(\theta) = \log P(\beta) + \log P\left(P_0^{'}\right) + \log P(d|\beta,Z) = -\frac{(\beta-\beta_0)^2}{2\sigma_\beta^2} + \sum_{i=1}^{N} \log P\left(P_{0.i}^{'}\right) + \sum_{i=1}^{N} \log P(d_i|\beta,Z) \quad (23)$$

We assume that $P(z)$ has a uniform distribution, while $P(d_i|\beta,z)$ is normally distributed with mean $\overline{d_i}$ and variance $\sigma_{\varepsilon_d}^2$. We note that

$$\mathrm{P}(P_{0.i}^{'}) = P_a \mathcal{N}\left(\overline{p_{0i}}, \sigma_{a,i}^2\right) + (1 - P_a)\mathcal{N}\left(\overline{p_0}, \sigma_{\varepsilon_P}^2\right) \quad (24)$$

where P_a is the probability that i^{th} sensor is malicious and $(1 - P_a)$ probability that i^{th} sensor is non-malicious.

The likelihood of the observed measurements $x_{i.j}$ is given by:

$$x_{i.j} = P_{0.i}^{'} - 10\beta \log(d_i) + \eta_{i.j} \tag{25}$$

where $\eta_{i.j}$ is the noise term. To compute (32), we note that the likelihood function is:

$$\begin{aligned} &\log\{P(X|\theta)\} = \sum_{i=1}^{N}\sum_{j=1}^{P} \log P\left(x_{i.j}|\theta\right) \\ &= c + \sum_{i=1}^{N}\sum_{j=1}^{P} \frac{-\left(x_{i.j} - P_{0i}^{'} - 10\beta \log d_i\right)^2}{2\sigma_{\eta_i}^2} \end{aligned} \tag{26}$$

Thus, the objective function to maximize for the MAP estimation is:

$$\begin{aligned} &J_{MAP}(\theta) \\ &= -\frac{(\beta - \beta_0)^2}{2\sigma_\beta^2} \\ &+ \sum_{i=1}^{N}\sum_{j=1}^{P} \frac{-\left(x_{i.j} - P_{0i}^{'} - 10\beta \log d_i\right)^2}{2\sigma_{\eta_i}^2} \\ &+ \sum_{i=1}^{N} \log\left(P_a \frac{1}{\sigma_{a,i}\sqrt{2\pi}} e^{\frac{-\left(P_{0i}^{'} - \overline{p_{0i}}\right)^2}{2\sigma_{a,i}^2}} \right. \\ &\left. + (1 - P_a)\frac{1}{\sigma_{\varepsilon_P}\sqrt{2\pi}} e^{\frac{-\left(P_{0i}^{'} - \overline{p_0}\right)^2}{2\sigma_{\varepsilon_P}^2}} \right) \\ &+ \sum_{i=1}^{N} \frac{-(d_i - \sqrt{(x_i - x_t)^2 + (y_i - y_t)^2})^2}{2\sigma_{\varepsilon_d}^2} \end{aligned} \tag{27}$$

Next, to estimate the unknown parameters θ, we maximize the function $J_{MAP}(\theta)$. Given that there are $2N + 1$ unknowns and PN known parameters, the estimation procedure proceeds by calculating the unknown parameters one by one, assuming the others are known.

For the first step, we solve for β by considering the values of d, $P_0^{'}$, and Z as known, and we maximize $J_1(\beta)$, which is given by:

$$J_1(\beta) = \frac{-1}{2\sigma_\beta^2}(\beta - \beta_0)^2 + \sum_{i=1}^{N}\sum_{j=1}^{P} -a_i\left(k_{ij} - \beta r_i\right)^2 \tag{28}$$

Expanding and simplifying, we get:

$$\begin{aligned} J_1(\beta) &= \frac{-1}{2\sigma_\beta^2}\beta^2 + \frac{\beta_0}{\sigma_\beta^2}\beta - \frac{{\beta_0}^2}{2\sigma_\beta^2} \\ &+ \sum_{i=1}^{N}\sum_{j=1}^{P} -a_i\left({k_{ij}}^2 + \beta^2 {r_i}^2 - 2k_{ij}\beta r_i\right) \\ &= \beta^2\left[\frac{-1}{2\sigma_\beta^2} - \sum_{i=1}^{N}\sum_{j=1}^{P} a_i {r_i}^2\right] \\ &+ \beta\left[\frac{\beta_0}{\sigma_\beta^2} + 2\sum_{i=1}^{N}\sum_{j=1}^{P} a_i r_i\, k_{ij}\right] \\ &- \frac{{\beta_0}^2}{2\sigma_\beta^2} - \sum_{i=1}^{N}\sum_{j=1}^{P} a_i {k_{ij}}^2 \end{aligned} \tag{29}$$

where $a_i \triangleq \frac{1}{2\sigma_{\eta_i}^2}$, $k_{ij} \triangleq x_{i.j} - P_{0i}^{'}$, and $r_i \triangleq 10\log d_i$. This leads to a quadratic equation in β, and solving for β gives:

$$\frac{\partial J_1(\beta)}{\partial \beta} = 0 \to \beta = \frac{\frac{\beta_0}{\sigma_\beta^2} + 2\sum_{i=1}^{N}\sum_{j=1}^{P} a_i r_i\, k_{ij}}{\frac{1}{\sigma_\beta^2} + 2\sum_{i=1}^{N}\sum_{j=1}^{P} a_i {r_i}^2} \tag{30}$$

This equation provides the MAP estimate for β. The process can be repeated to estimate the other unknowns, including d, $P_0^{'}$, and Z.

For the second step, we calculate $P_0^{'}$ by assuming the values of d, β, and Z are known and then maximizing the function $J_2\left(P_0^{'}\right)$, which is given by:

$$\begin{aligned} &J_2\left(P_0^{'}\right) \\ &= \sum_{i=1}^{N}\sum_{j=1}^{P} \frac{-1}{2\sigma_{\eta_i}^2}\left(x_{i.j} - P_{0i}^{'} - 10\beta \log d_i\right)^2 \\ &+ \sum_{i=1}^{N} \log\left(P_a \frac{1}{\sigma_{a,i}\sqrt{2\pi}} e^{\frac{-\left(P_{0i}^{'} - \overline{p_{0i}}\right)^2}{2\sigma_{a,i}^2}} \right. \\ &\left. + (1 - P_a)\frac{1}{\sigma_{\varepsilon_P}\sqrt{2\pi}} e^{\frac{-\left(P_{0i}^{'} - \overline{p_0}\right)^2}{2\sigma_{\varepsilon_P}^2}} \right) \end{aligned} \tag{31}$$

Using the steepest ascent (SA) method, we update $P_0^{'}$ as:

$$\begin{aligned} &P_0^{'} \\ &\leftarrow P_0^{'} + \mu_P \sum_{j=1}^{P} \frac{1}{\sigma_{\eta_i}^2}\left(x_{kj} - P_{0k}^{'} - 10\beta \log d_k\right) \\ &+ \mu_P \frac{\frac{-\left(P_{0k}^{'} - \overline{p_{0i}}\right)}{\sigma_{a,i}^2} \cdot P_a \frac{1}{\sigma_{a,i}\sqrt{2\pi}} e^{\frac{-\left(P_{0k}^{'} - \overline{p_{0i}}\right)^2}{2\sigma_{a,i}^2}}}{C} \\ &- \frac{\frac{\left(P_{0k}^{'} - \overline{p_0}\right)}{\sigma_{\varepsilon_P}^2} \frac{1 - P_a}{\sigma_{\varepsilon_P}\sqrt{2\pi}} e^{\frac{-\left(P_{0k}^{'} - \overline{p_0}\right)^2}{2\sigma_{\varepsilon_P}^2}}}{C} \end{aligned} \tag{32}$$

where μ_P is the step-size that control the convergence of $P_0^{'}$ and

TABLE 1: Localization error with respect to variance of biases of two Byzantine nodes in the network in SNR equal to 20 dB.

Methods	$\sigma_a^2 = 0.2$	$\sigma_a^2 = 0.5$	$\sigma_a^2 = 1$	$\sigma_a^2 = 5$
LS	7.0	8.4	9.5	12.2
WLS	2.6	3.3	4.0	7.2
SDP	2.9	3.7	4.2	6.9
BFLA	2.0	2.9	3.3	5.7
Proposed MAP	1.3	1.9	2.4	4.6

$$C = \frac{P_a}{\sigma_{a,i}\sqrt{2\pi}} e^{\frac{-\left(P_{0k}^{'} - \overline{P_{0i}}\right)^2}{2\sigma_{a,i}^2}} + \frac{1-P_a}{\sigma_{\varepsilon_P}\sqrt{2\pi}} e^{\frac{-\left(P_{0k}^{'} - \overline{P_0}\right)^2}{2\sigma_{\varepsilon_P}^2}} \quad (33)$$

For the third step, we solve for d by assuming $P_0^{'}$, β, and Z are known, and maximizing $J_2(d)$, which is:

$$J_3(d) = \sum_{i=1}^{N}\sum_{j=1}^{P} \frac{-1}{2\sigma_{\eta_i}^2}\left(x_{i.j} - P_{0i}^{'} - 10\beta \log d_i\right)^2 + \sum_{i=1}^{N} \frac{-1}{2\sigma_{\varepsilon_d}^2}(d_i - \sqrt{(x_i - x_t)^2 + (y_i - y_t)^2})^2 \quad (34)$$

Using the SA method, we derive the following update rule for d:

$$d_k = d_k + \mu_d \sum_{j=1}^{P} \frac{-1}{2\sigma_{\eta_k}^2}\left(\frac{-10\beta}{d_k}\right) \times 2\left(x_{kj} - P_{0,k}^{'} - 10\beta \log d_k\right) + \mu_d\left(\frac{-1}{2\sigma_{\varepsilon_d}^2}\right)(2)(d_k - \sqrt{(x_k - x_t)^2 + (y_k - y_t)^2}) \quad (35)$$

where μ_d is the step-size that controls the convergence of SA method. This is further simplified to:

$$d_k = d_k + \frac{10\beta\mu_d}{d_k\sigma_{\eta_k}^2}\sum_{j=1}^{P}\left(x_{kj} - P_{0.k}^{'} - 10\beta \log d_k\right) - \left(\frac{\mu_d}{\sigma_{\varepsilon_d}^2}\right)\left(d_k - \sqrt{(x_k - x_t)^2 + (y_k - y_t)^2}\right) \quad (36)$$

Finally, for the Z value, we solve by assuming $P_0^{'}$, β, and d are known and maximizing $J_4(Z)$, which is:

$$J_4(Z) = \sum_{i=1}^{N}\sum_{j=1}^{P} \frac{-\left(x_{i.j} - P_{0i}^{'} - 10\beta \log d_i\right)^2}{2\sigma_{\eta_i}^2} + \sum_{i=1}^{N} \frac{-1}{2\sigma_{\varepsilon_d}^2}(d_i - \sqrt{(x_i - x_t)^2 + (y_i - y_t)^2})^2 \quad (37)$$

We consider two strategies for solving this, as follows:

A. Strategy 1: SA method

$$x_t \leftarrow x_t + \mu_x \frac{\partial J_4}{\partial x_t} \quad (38)$$

$$y_t \leftarrow y_t + \mu_y \frac{\partial J_4}{\partial y_t} \quad (39)$$

where μ_x and μ_y are step-sizes that control the convergence of Z to its final value. We then derive:

$$x_t \leftarrow x_t + \mu_x \sum_{i=1}^{N}\sum_{j=1}^{P} \frac{-\left(x_{i.j} - P_{0i}^{'} - 10\beta \log d_i\right)\left[-10\beta \frac{\partial}{\partial x_t}\log d_i\right]}{\sigma_{\eta_i}^2} + \mu_x \sum_{i=1}^{N} \frac{-1}{\sigma_{\varepsilon_d}^2}(d_i - \sqrt{(x_i - x_t)^2 + (y_i - y_t)^2})^2 \cdot \frac{-2x_i - x_t}{2\sqrt{(x_i - x_t)^2 + (y_i - y_t)^2}}$$

$$= x_t + \mu_x \sum_{i=1}^{N}\sum_{j=1}^{P} \frac{10\beta\left(x_{i.j} - P_{0i}^{'} - 10\beta \log d_i\right)}{\sigma_{\eta_i}^2} \frac{\frac{\partial d_{i_1}}{\partial x_t}}{d_i} - \mu_x \sum_{i=1}^{N} \frac{1}{\sigma_{\varepsilon_d}^2}\left(d_i - d_{i_1}\right)\frac{\partial d_{i_1}}{\partial x_t} = \frac{-(x_i - x_t)}{\sqrt{(x_i - x_t)^2 + (y_i - y_t)^2}} \quad (40)$$

$$y_t \leftarrow y_t + \mu_y \sum_{i=1}^{N}\sum_{j=1}^{P} \frac{10\beta\left(x_{i.j} - P_{0i}^{'} - 10\beta \log d_i\right)}{\sigma_{\eta_i}^2}\frac{\partial d_{i_1}}{\partial y_t} + \mu_y \sum_{i=1}^{N} \frac{1}{\sigma_{\varepsilon_d}^2}\left(d_i - d_{i_1}\right)\frac{\partial d_{i_1}}{\partial y_t} = \frac{-(y_i - y_t)}{\sqrt{(x_i - x_t)^2 + (y_i - y_t)^2}} \quad (41)$$

B. Strategy 2: LS method

Assuming that d_i is known, we can write:

$$d_i{}^2 = (x_i - x_t)^2 + (y_i - y_t)^2 \quad (42)$$

Then, we derive

$$d_i{}^2 - x_i{}^2 - y_i{}^2 = -2x_i x_t - 2y_i y_t + x_t{}^2 + y_t{}^2 \quad (43)$$

$$R_t{}^2 = x_t{}^2 + y_t{}^2 \quad (44)$$

In the matrix form, we have:

$$\underline{b} = \begin{bmatrix} d_1{}^2 - x_1{}^2 - y_1{}^2 \\ \vdots \end{bmatrix} = \begin{bmatrix} -2x_1 & -2y_1 & 1 \\ -2x_2 & -2y_2 & 1 \\ \vdots & \vdots & \vdots \end{bmatrix}\begin{bmatrix} x_t \\ y_t \\ R_t \end{bmatrix} \quad (45)$$

$$A = \begin{bmatrix} -2x_1 & -2y_1 & 1 \\ -2x_2 & -2y_2 & 1 \\ \vdots & \vdots & \vdots \end{bmatrix} \quad (46)$$

$$\theta^{'} = \begin{bmatrix} x_t \\ y_t \\ R_t \end{bmatrix} \quad (47)$$

$$\widehat{\theta^{'}} = A^{\dagger} b \quad (48)$$

The first two elements of $\widehat{\theta^{'}}$ gives the estimated values of x_t and y_t.

V. Simulation Results

This section presents the simulation results demonstrating the enhanced system performance achieved using the proposed MAP method. We assume the true location of the target is $x = 20$, $y = 10$, with $P_0 = 10$ for eight sensors randomly distributed across the network in a 100 x 100

square region. The actual path loss exponent (β) is 3, with $\sigma_\beta = 0.2$, $\sigma_{\varepsilon_P}^2 = 0.01$, $\sigma_{a,i}^2 = \sigma_a^2 = 1$, and the signal-to-noise ratio (SNR) is 20 dB. Based on this setup, the results from the MATLAB simulation are provided below.

Figure 2 shows the actual value of PLE (β) and the estimated β using the MAP method after 30 iterations. The initial value of PLE is set to 2. The figure demonstrates the convergence of the estimated PLE, with the final estimation error of 5.2%.

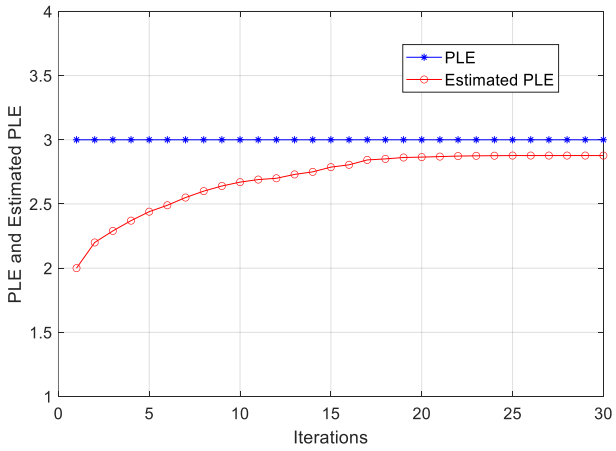


Fig. 2. Estimated β by MAP method with 30 iterations.

Figure 3 displays the estimated distances between the anchor nodes and the target node. The distance estimation is a close approximation to the actual values, with an average error of 16.05%.

Figure 4 shows the actual values of power $P_0^{'} = 10$ for each anchor node along with their estimated values of $P_0^{'}$ using the MAP method. As observed, the estimates converge well, with a final estimation error of approximately 2%.

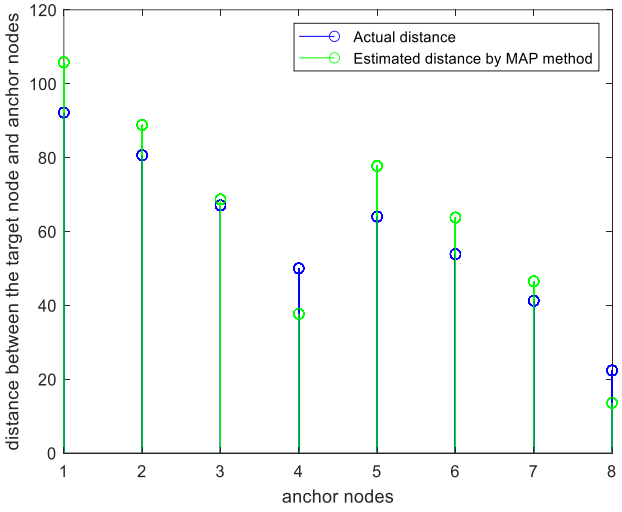


Fig. 3. Estimated distance between the target node and anchor nodes by MAP method

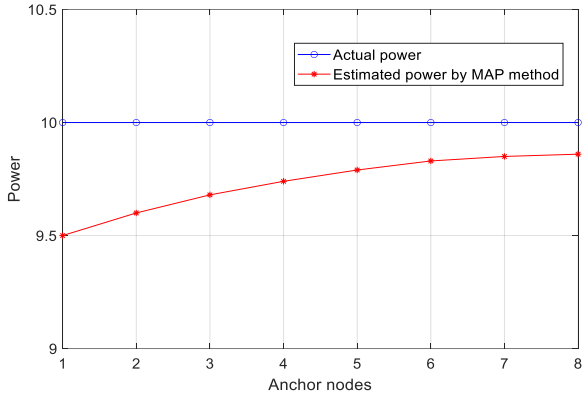


Fig. 4. Estimated power by MAP method

For comparison of the proposed MAP estimation method with the LS, WLS, Semidefinite Programming (SDP) method [27], and the Byzantine Fault-Tolerant Localization Algorithm (BFLA) [26], Figure 5 presents the target localization error as a function of SNR, along with the Cramér-Rao Bound (CRB) calculated in [25]. The graph shows that as the SNR increases, the error decreases. As shown, in the LS method graph, the error decreases slightly with increasing SNR, and it does not achieve optimal efficiency. The WLS method estimates the target location with considerably greater precision. Our proposed MAP estimation method effectively minimizes the impact of malicious anchor nodes, regardless of their number.

Moreover, the figure indicates that the proposed MAP method outperforms other methods when the SNR exceeds 10 dB, while for SNR values below 10 dB, its performance is comparable to that of the BFLA method. Additionally, as the SNR increases, the localization accuracy of both the WLS and the proposed MAP method approaches the CRB.

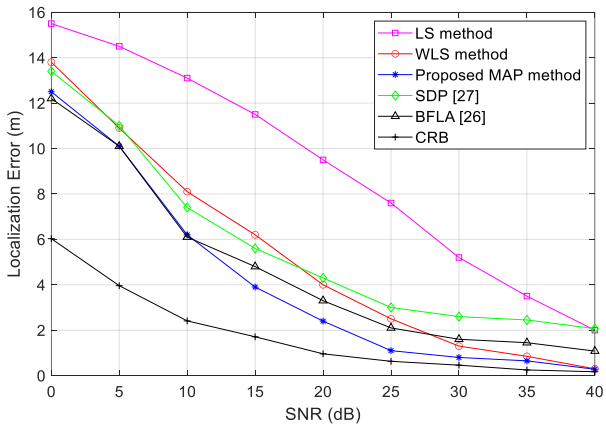


Fig. 5. Localization error in term of SNR for LS, WLS, SDP, BFLA and MAP methods in addition to CRB.

To investigate the effect of bias variance, denoted as σ_a^2 (where $\sigma_{a,i}^2 = \sigma_a^2$), we present Table 1 that illustrates the localization error as a function of σ_a^2 under an SNR of 20 dB. The results show that as the variance of biases introduced by Byzantine nodes increases, the localization error also

increases. Among the evaluated methods, the proposed MAP algorithm consistently achieves the lowest localization error, demonstrating its robustness to bias variance.

To evaluate the computational complexity of the methods, we calculated the average simulation run time over 200 Monte Carlo runs. Table 2 presents the simulation run times for all algorithms, indicating that the proposed MAP method exhibits the highest computational complexity in terms of average run time.

TABLE 2: Average Simulation run times of various algorithms in SNR equal to 20dB.

Methods	Simulation run time (s)
LS	0.06
WLS	0.51
Proposed MAP	2.12
SDP	0.89
BFLA	1.56

Referring to the target location in Figure 2, the WLS method is capable of accurately estimating the target location in certain scenarios. However, its accuracy is dependent on the target's position within the network. For instance, if the target is located at the edge of the network or far from the anchor nodes, the likelihood of error increases. However, as previously noted, the WLS method has higher computational complexity and is less time-efficient compared to the LS and MAP methods, which are more efficient.

VI. Conclusion

In this paper, we addressed the localization problem in the presence of malicious anchor nodes and proposed the use of the MAP method to overcome this challenge. We examined scenarios where the path loss exponent, the distance between the target node and anchor nodes, received signal strength, and the target node location were all unknown. This approach enables the fusion center to estimate the target node's location with minimal error. Simulations were carried out in MATLAB, and the corresponding graphs were generated. The MAP method effectively estimates unknown parameters, such as the path loss exponent, the distance between the target node and anchor nodes, and received signal strength. Simulations demonstrated that the MAP method effectively estimates all unknown parameters and achieves the lowest localization error among the evaluated methods. However, this improved accuracy comes at the cost of increased computational complexity due to the iterative calculation of complex likelihoods and gradients. It is also worth noting that all prior distributions were assumed to be Gaussian, which is a simplifying assumption. Future work could explore the use of non-Gaussian priors, such as impulsive noise models or non-Gaussian biases, to enhance robustness in more challenging environments.

References

[1] Q. Yan, H. M. Wang, Y. Chen, and C. Gao, "Robust 3-D AOA Localization Against Malicious Attacks in Non-Gaussian Noise," IEEE Sens. J., vol. 24, no. 9, pp. 14573-14585, 2024.

[2] C. Si, R. Fan, Y. Yang, and Y. Sun, "Improved TOA Localization Using Modified Polar Representation," IEEE Commun. Lett., vol. 28, no. 9, pp. 2051-2055, 2024.

[3] Y. Liu, C. Chen, Y. Wang, and C. Liu, "Range-Independent TDOA Localization Using Stepwise Accuracy Enhancement Under Speed Uncertainty," IEEE Signal Process. Lett., vol. 30, pp. 1372-1376, 2023.

[4] R. Sari and H. Zayyani, "RSS Localization Using Unknown Statistical Path Loss Exponent Model," IEEE Commun. Lett., vol. 22, no. 9, pp. 1830-1833, 2018.

[5] S. Haidari, H. Moradi, and S. M. M. Dehghan, "RF Source Localization Using Obstacles Map and Reflections," International Journal of Industrial Electronics, Control and Optimization, vol. 4, no. 2, pp. 181-190, 2021.

[6] M. H. Arabsorkhi, H. Zayyani, and M. Korki, "3-D Hybrid RSS-AoA Passive Source Localization with Unknown Path Loss Exponent," IEEE Sens. Lett., vol. 7, no. 6, pp. 1372-1376, 2023.

[7] R. Garg, A. L. Varna, and M. Wu, "An Efficient Gradient Descent Approach to Secure Localization in Resource Constrained Wireless Sensor Networks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 717-730, 2012.

[8] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," in Fourth Int. Symposium Inf. Process. Sensor Netw, pp. 91-98, 2005.

[9] J. Won and E. Bertino, "Robust Sensor Localization Against Known Sensor Position Attacks," IEEE Trans, Mobile Comput, vol. 18, no. 12, pp. 2954-2967, 2019.

[10] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, "Robust Range-Based Secure Localization in Wireless Sensor Networks," in IEEE Global Commun. Conf. (GLOBECOM), pp. 1-6, 2018.

[11] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, "RSS-Based Localization in the Presence of Malicious Nodes in Sensor Networks," IEEE Trans. Instrum. Meas., vol. 70, pp. 1-16, 2021.

[12] S. Marano, V. Matta, P. Willett, and L. Tong, "DOA Estimation Via a Network of Dump Sensors Under the SENMA Parading," IEEE Signal Process. Lett., vol. 12, no. 10, pp. 709-712, 2005.

[13] S. Marano, V. Matta, P. Willett, and L. Tong, "Support-Based and ML Approaches to DOA Estimation in a Dumb Sensor Network," IEEE Trans. Signal Process., vol. 54, no. 4. pp. 1563-1567, 2006.

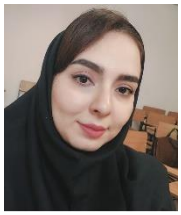
[14] D. Li and Y. H. Hu, "Energy-Based Collaborative Source Localization Using Acoustic Micro-Sensor Array," EURASIP J. Appl. Signal Process, pp. 321-337, 2003.

[15] X. Sheng and Y. H. Hu, "Maximum Likelihood Multiple-Source Localization Using Acoustic Energy Measurements with Wireless Sensor Networks," IEEE Trans. Signal Process., vol. 53, no. 1. pp. 44-53, 2005.

[16] N. Patwari and A. Hero, "Using Proximity and Quantized RSS For Sensor Localization in Wireless Networks," in Proc. 2nd Int. ACM Workshop Wireless Sens. Netw. Appl., San Diego, CA, USA, pp. 20-29, 2003.

[17] 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, 2006.

[18] S. Marano, V. Matta, and L. Tong, "Distributed Detection in the Presence of Byzantine Attacks," IEEE Trans. Signal Process., vol. 7, no. 1, pp. 16-29, 2009.
[19] A. Vempaty, K. Agrawal, H. Chen, and P. K. Varshney, "Adaptive Learning of Byzantines Behavior in Cooperative Spectrum Sensing," in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Cancun, Mexico, pp. 1310-1315, 2011.
[20] O. Kosut and L. Tong, "Distributed Source Coding in the Presence of Byzantine Sensors," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2550-2565, 2008.
[21] O. Kosut, L. Tong, and D. Tse, "Nonlinear Network Coding is Necessary to Combat General Byzantine Attacks," in Proc. 47th Ann. Allerton Conj. Commun. Contr. Comput., Urbana, IL, USA, pp. 593-599, 2009,.
[22] K. Agrawal, A. Vempaty, H. Chen, and P. K. Varshney, "Target Localization in Sensor Networks with Quantized Data in the Presence of Byzantine Attacks," in Proc. Asilomar Conf. Signals, Syst. Comp., Pacific Grove, CA, USA, pp. 1669-1673, 2011.
[23] H. L. V. Trees and K. L. Bell, Bayesian Bounds for Parameter Estimation and Nonlinear Filtering/Tracking, Wiley IEEE press, Hoboken, NJ, USA, 2007.
[24] A. Vempaty, O. Ozdemir, and P. Varshney, "Mitigation of Byzantine Attacks for Target Location Estimation in Wireless Sensor Networks," in Proc. 46th Ann. Conf. on Inf. Sci. Syst. (CISS), Princeton, NJ, USA, 2012.
[25] 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, 2013.
[26] X. Mei, H. Wu, J. Xian, and B. Chen, "RSS-Based Byzantine Fault-Tolerant Localization Algorithm Under NLOS Environment," IEEE Commun. Lett., vol. 25, no. 2, pp. 474-478, 2021.
[27] Q. Wang, Z. Duan, and F. Li, "Semidefinite Programming for Wireless Cooperative Localization Using Biased RSS Measurements," IEEE Commun. Lett., vol. 26, no. 6, pp. 1278-1282, 2022.
[28] H. C. So and L. Lin, "Linear Least Squares Approach for Accurate Received Signal Strength Based Source Localization," IEEE Trans. Signal Process., vol. 59, no. 8, pp. 4035-4040, 2011.
[29] S. Kay, Fundamentals of Statistical Signal Processing: Estimation Theory, Prentice Hall, 1993.



Mahdiye Mohammadi was born in Qom, Iran. She received her B.Sc. degree in Telecommunication Engineering from Qom University, Qom, Iran, in 2022. She is currently pursuing her M.Sc. degree in Telecommunication Systems Engineering at Qom University of Technology, Qom, Iran. Her current research interests include localization in wireless sensor networks and pattern recognition.

Hadi Zayyani received his B.Sc., M.Sc., and Ph.D. degrees in Electrical Engineering, all with a focus on communications, from Sharif University of Technology. Since 2012, he has been a faculty member at Qom University of Technology, where he was promoted to full professor in 2024. He was recognized among the top 2% of scientists worldwide by Stanford University in 2021, 2022, and 2023. Dr. Zayyani has published over 70 journal papers and 35 conference papers, with approximately half appearing in IEEE venues. He serves as an editor for the Iranian Journal of Science and Technology and as a reviewer for several high-impact journals published by IEEE and Elsevier. His research interests include statistical and sparse signal processing, adaptive filtering, radar signal processing, graph signal processing, and distributed signal processing.

Mehdi Bekrani received his B.Sc. degree in Electrical Engineering from Ferdowsi University of Mashhad, Iran, in 2002, and earned his M.Sc. and Ph.D. degrees in Electrical Engineering from Tarbiat Modares University, Tehran, Iran, in 2004 and 2010, respectively. From 2010 to 2012, he was a Research Fellow at Nanyang Technological University, Singapore. He joined the Department of Electrical and Computer Engineering at Qom University of Technology, Qom, Iran, in 2012, and is currently an Associate Professor at the same university. His research interests include acoustic and ultrasonic signal processing, with a focus on source localization, beamforming, channel equalization, and noise cancellation.