RSS-Based Localization in the Presence of Malicious Nodes in Sensor Networks

Bodhibrata Mukhopadhyay, *Graduate Student Member, IEEE*, Seshan Srirangarajan, *Member, IEEE*, and Subrat Kar, *Senior Member, IEEE*

***Abstract*—The ability of a sensor node to determine its location in a sensor network is important in many applications. We address the scenario, where malicious anchor node(s) attempt to disrupt, in an uncoordinated or coordinated manner, the localization process of a target node. We propose four localization techniques: weighted least square (WLS), secure WLS (SWLS), and ℓ_1-norm-based techniques LN-1 and LN-1E. WLS and SWLS techniques are shown to offer a significant advantage in uncoordinated attacks over existing techniques by detecting the malicious nodes and eliminating their measurements from the localization process and assigning larger weights to the measurements corresponding to anchor nodes that are closer to the target node. In a coordinated attack, the localization problem can be posed as a plane fitting problem, where the measurements from nonmalicious and malicious anchor nodes lie on two different planes. The LN-1E technique estimates the two planes and prevents disruption of the localization process. LN-1E can also determine the location where the malicious anchor nodes intend to make the target node appear to be located. The Cramer–Rao lower bound for the position estimate is also derived. We present simulation and experimental results, which demonstrate that the proposed techniques provide better localization accuracy than existing algorithms.**

***Index Terms*—Coordinated attack, Cramer–Rao lower bound (CRLB), least square (LS), localization, received signal strength (RSS), uncoordinated attack.**

I. Introduction

Rapid developments in the field of microelectronics, integrated circuit fabrication, and embedded software have increased the computational power, lifetime, and sensing capabilities of wireless sensor nodes. A wireless sensor network (WSN) is formed by a collection of authenticated sensor nodes that communicate among themselves and cooperate for a common purpose. The nodes sense and transmit the data to a base station for further processing. WSNs are used in applications, such as air quality monitoring [1], tracking goods in a supply chain [2], monitoring activities of farm animals [3], landslide detection [4], and navigation tools in places, such as shopping malls and airports. In these applications, data from the sensor nodes are useful only when it is associated with the sensor's location information. For example, in an air quality monitoring system, the location of the sensor node reporting a poor air quality index is essential for taking the required action. As the monitoring area becomes large, the number of sensor nodes in the network increases and it becomes difficult to keep track of the sensor nodes manually. Thus, it is necessary to employ localization techniques for estimating locations of the sensor nodes [5]–[8].

Localization techniques broadly fall into two categories: range-based techniques [9] and range-free techniques [10]. For determining the location of a target node, range-based techniques use the distance between the target node (node whose location is not known at the time of deployment) and the anchor nodes (nodes whose locations are known at the time of deployment), whereas range-free techniques only use connectivity information between the nodes.

Location-based services are open to security threats, where attackers can gain unauthorized access to the infrastructure responsible for carrying out the localization and/or modify the code on the sensor nodes turning them into malicious nodes (noncryptographic attacks). Thus, a malicious node may not provide the correct information required for the localization of the target node. These attacks can result in erroneous location estimation of the target nodes. A nonmalicious node can also seem to behave like a malicious node if the wireless link between this node and the target node is affected. This can happen if the direct path between the anchor and target node is obstructed, or the transmit antenna is damaged resulting in unusual variation in received signal strength (RSS) values.

In this article, we consider the scenario where a target node attempts to localize itself using RSS values from its neighboring anchor nodes. It is assumed that the anchor nodes transmit at a fixed predefined power level. However, some of the anchor nodes either individually (uncoordinated attack) or collaboratively (coordinated attack) change their transmit power without informing the target node in order to disrupt the localization process. The main contributions of this work are summarized in the following.

1) We propose four localization techniques: weighted least square (WLS), secure WLS (SWLS), and ℓ_1-norm-based localization techniques LN-1 and LN-1E for estimating

Manuscript received April 5, 2021; revised July 4, 2021; accepted July 26, 2021. Date of publication August 12, 2021; date of current version August 31, 2021. The work of Bodhibrata Mukhopadhyay was supported by the Visvesvaraya Ph.D. Scheme, MeitY, Government of India, under Grant MEITY-PHD-556. The Associate Editor coordinating the review process was V. R. Singh. *(Corresponding author: Seshan Srirangarajan.)*

Bodhibrata Mukhopadhyay is with the Department of Electrical Engineering, IIT Delhi, New Delhi 110016, India (e-mail: bodhibrata@gmail.com).

Seshan Srirangarajan and Subrat Kar are with the Department of Electrical Engineering, IIT Delhi, New Delhi 110016, India, and also with the Bharti School of Telecommunication Technology & Management, IIT Delhi, New Delhi 110016, India (e-mail: seshan@ee.iitd.ac.in; subrat@ee.iitd.ac.in).

This article has supplementary downloadable material available at https://doi.org/10.1109/TIM.2021.3104385, provided by the authors.

Digital Object Identifier 10.1109/TIM.2021.3104385

the target node location in the presence of malicious anchor nodes.

2) SWLS and LN-1E are capable of identifying the malicious anchor nodes in uncoordinated and coordinated attacks, respectively.
3) We present extensive performance evaluation of the proposed techniques and comparison with three existing localization methods inside-attack filtering minimum MSE (IAF-MMSE) [11], Grad-Desc [12], and LMdS [13].
4) We discuss the performance of LN-1E in estimating the location where the malicious nodes intend to make the target node appear in a coordinated attack.
5) We also present experimental results to validate the performance of the proposed localization techniques in indoor and outdoor environments.
6) We derive the Cramer–Rao lower bound (CRLB) on the root-mean-square error (RMSE) of the location estimate under uncoordinated and coordinated attacks.

The rest of this article is organized as follows. Section II discusses prior work in the area of secure localization techniques in WSN. Section III presents the system model and problem formulation. Section IV describes the proposed localization techniques. The CRLB for uncoordinated and coordinated attack is derived in Section V. Sections VI and VII present the performance evaluation of the proposed localization techniques via simulations and experiments, respectively. Section VIII concludes this article.

II. Related Work

The target node can estimate its location based on information, such as RSS, time of arrival, time difference of arrival, or connectivity, from its neighboring nodes. Attackers can try to falsify this information in order to disrupt the localization process. Various types of attacks on localization techniques have been studied in the literature [14], such as impersonation (malicious node masquerading as a nonmalicious node), distance fraud (malicious node reporting information resulting in incorrect distance estimation), time fraud (malicious nodes inserting incorrect timestamp into packets sent to the target node), and Sybil attack (malicious node claiming multiple identities/locations representing multiple nodes).

Won and Bertino [11] considered two attack strategies, aligned beacon position (ABP) attack and inside attack, assuming the malicious nodes are aware of the target node location. The ABP attack exploits the fact that anchor nodes usually lie along a straight line, such as a hallway or passage in indoor localization. The inside attack disrupts the degree of consistency (DOC) algorithm by introducing malicious anchor nodes into the network. The ABP attack is prevented using a novel anchor node deployment strategy. The inside attack is defended against by filtering the malicious anchor nodes based on their intersection points. A secure localization algorithm was proposed for cases where the network contains a greater number of nonmalicious anchor nodes than malicious anchor nodes.

Garg *et al.* [12] proposed an iterative gradient descent technique with inconsistent measurement pruning to achieve accurate localization in the presence of malicious nodes in a WSN. They consider mobile sensor networks where the nodes are mobile and some of them may be compromised and thus transmit false information. Assuming the measurement noise to be Gaussian distributed, the likelihood of the measurements is maximized. To account for the possibility of malicious nodes, the cost function is updated at each iteration by eliminating the anchor nodes with large residues from the localization process.

Li *et al.* [13] considered two robust localization techniques, namely, triangulation and RF-based fingerprinting. For triangulation, they proposed an adaptive LS and least median of squares (LMdS)-based location estimation, and for RF fingerprinting, they used a median-based distance metric. In the LMdS method, anchors are divided into many subsets of identical sizes with each subset estimating the target node location using LSs. The final target node location is given by the LSs location estimate of the subset with the smallest median residue. It was observed that this subset is least likely to contain malicious nodes. However, it was assumed that the number of malicious nodes is less than 50% of the total number of anchor nodes.

The techniques proposed in [11]–[13] attempt to detect the malicious nodes and eliminate them from the localization process. In [12], 50% of the anchor nodes are eliminated irrespective of the network size or strength of the attack. However, measurements from malicious nodes can also contain useful information. In the proposed WLS and LN-1 techniques, we consider RSS measurements from both malicious and nonmalicious anchor nodes in the localization process. The method in [11] requires some knowledge of the channel parameters and does not detect malicious anchor nodes accurately if the anchor nodes have the same DOC [15] and a similar number of intersection points [11]. The computational complexity of LN-1 and LN-1E increases linearly with the number of anchor nodes. In addition, LN-1E has the ability to estimate the location, where the malicious anchor nodes intend to make the target node appear.

This work is an extension of the proceedings article [16] which considered only uncoordinated attacks and proposed the WLS localization scheme. In this article, we consider both uncoordinated and coordinated attacks and propose three new localization techniques. In [16], the uncertainty introduced by the malicious anchor nodes in their transmit power levels to disrupt the localization process of the uncoordinated attack was assumed to follow a Gaussian distribution. In this work, we assume it to follow the uniform distribution which makes the uncoordinated attack model more realistic and challenging to tackle [12]. In addition, the proposed SWLS and LN-1E techniques can detect malicious nodes in the network.

III. System Model

Consider a network with N anchor nodes whose locations are known and one target node whose location is to be determined. It is assumed that all the anchor nodes are within the communication range of the target node. The nodes are assumed to transmit at a predefined power level. The target

TABLE I
ACRONYMS AND MATHEMATICAL NOTATIONS

Acronyms	Description
RSS	Received Signal Strength
WSN	Wireless Sensor Network
ML	Maximum Likelihood
PDF	Probability Density Function
LMdS	Least Median of Square
WLS	Weighted Least Square
SWLS	Secure Weighted Least Square
RMS	Root Mean Square
FIM	Fisher Information Matrix
CRLB	Cramer-Rao lower bound

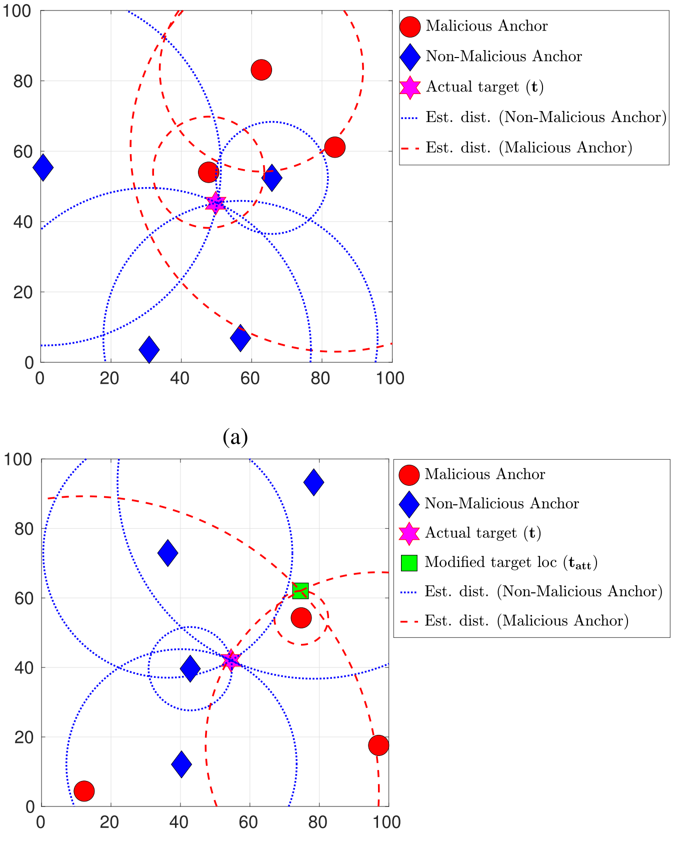
Notations	Description
$\mathbf{A}$	Matrices: uppercase bold letters
$\mathbf{a}$	Vectors: lowercase bold letters
$\mathrm{diag}(\cdot)$	Diagonal matrix
$\lVert\cdot\rVert_1$, $\lVert\cdot\rVert_2$	ℓ_1-norm, ℓ_2-norm
$\lvert\mathcal{A}\rvert$	Cardinality of set $\mathcal{A}$
$\mathbf{1}_N$	Column vector of size N with all its elements being 1
SVar $(x_1,\cdots,x_n)$	Sample variance of the $x_1,x_2,\cdots,x_n$
N	Number of anchor nodes
P	Number of packets
$\mathbf{t}$	Location coordinates of the target node: $[t^x,t^y]^T$
$\mathbf{a}_i$	Location coordinates of the i^{th} anchor node: $\left[a_i^x,a_i^y\right]^T$
p_i^r	RSS value of a packet received from the i^{th} anchor node (assuming $P=1$)
p_{ij}^r	RSS value of the j^{th} packet received from the i^{th} anchor node (for scenarios with multiple packets)
$\overline{p_i^r}$	Mean received power
$\mathbf{P}^r$	Matrix containing RSS values of P packets received by the target node from each of the N anchor nodes
p_0	Predefined transmit power of anchor nodes (assuming all anchor nodes transmit at the same power level)
p_{0_i}	Transmit power of the i^{th} anchor node in uncoordinated attack
$p_{0_i}^c$	Transmit power of the i^{th} anchor node in coordinated attack
d_i	Euclidean distance between $\mathbf{t}$ and $\mathbf{a}_i$
$\overline{d_i}$	Mean distance between $\mathbf{t}$ and $\mathbf{a}_i$
$f_{\overline{d_i}}(\cdot)$	Probability density function (PDF) of $\overline{d_i}$
n	Path loss exponent
η	Measurement noise
κ	Uncertainty introduced by the malicious anchor nodes in their transmit power in uncoordinated attack
δ_{k+}^p or δ_{k-}^p	Variation in the received power
δ_{k+}^d or δ_{k-}^d	Variation in the distance estimate
$\mathbf{F}_{\text{uc}}$ $(\mathbf{F}_{\text{c}})$	FIM for uncoordinated (coordinated) attack
$f_V(\cdot)$	PDF of $V=\eta+\kappa$
$p\left(\mathbf{P}^r;\mathbf{t}\right)$	PDF of the RSS measurements

node measures the RSS values of the packets received from the anchor nodes and estimates their distance from each of the anchor nodes. Localization techniques allow the target node to estimate its location using the estimated distances and the known locations of the anchor nodes. The key acronyms and notations used in this article are listed in Table I.

Assuming the signal power loss is dominated by path loss which can be modeled using the log-distance model [17], [18]

$$p^r = p_0 - 10n\log_{10}(d) + \eta \tag{1}$$

where p^r is the received power at the target node, and p_0 is the received power at the target node when the distance between the anchor node and target node is 1 m. Thus, p_0 depends on the transmit power of the anchor node[1] [19], n is the path loss exponent, d is the distance between the target and the anchor node, and η is the additive noise which is assumed to be zero mean and i.i.d. Gaussian.



(a)

(b)

Fig. 1. Attack strategies by malicious anchor nodes in a WSN. The dashed circles represent the estimated distance between the target and malicious anchor nodes, and the dotted circles represent the estimated distance between the target and nonmalicious anchor nodes in the absence of measurement noise. (a) Uncoordinated attack. (b) Coordinated attack.

Let the location coordinates of the target node and N anchor nodes be represented by $\mathbf{t} = [t^x, t^y]^T$ and $\mathbf{a}_i = [a_i^x, a_i^y]^T$, where $i = 1,\ldots,N$, respectively. The anchor nodes are assumed to broadcast packets at regular intervals. Let p_{ij}^r represent the RSS value of the j^{th} packet received from the i^{th} anchor node. Using (1) and p_{ij}^r, the target node computes its distance from the i^{th} anchor node as $d_{ij} = 10^{\frac{\left(p_0 - p_{ij}^r\right)}{10n}}$. Next, consider that some of the anchor nodes are malicious and attempt to disrupt the localization process. Two types of localization attacks are considered: uncoordinated and coordinated attacks. In an uncoordinated attack, the malicious node(s) act independently and attempt to disrupt the localization process of the target node, whereas in a coordinated attack, the malicious nodes coordinate among themselves in order to make the target node appear to be located at a location different from its actual location. These attacks are shown in Fig. 1 and can be modeled as described next.

1) Uncoordinated Attack: We consider noncryptographic attacks, where the malicious nodes deviate from their expected operation [20] and change their transmit power levels arbitrarily, and do not report it to the target node.

[1] In this work, we will refer to p_0 as the transmit power of the anchor node.

This type of attack can be modeled as

$$p_i^r = \begin{cases} p_0 - 10n\log_{10}(d_i) + \eta & \text{if node i is nonmalicious} \\ p_{0_i} - 10n\log_{10}(d_i) + \eta & \text{if node i is malicious} \end{cases} \tag{2}$$

where p_i^r is the received power at the target node from the i^{th} anchor node, p_0 is the predefined transmit power of the anchor nodes, p_{0_i} is the transmit power of the i^{th} malicious anchor node, $d_i = \|\mathbf{t} - \mathbf{a}_i\|_2$ is the distance between the i^{th} anchor node located at $\mathbf{a}_i$ and the actual target node located at $\mathbf{t}$, and $\eta \sim \mathcal{N}(0, \sigma^2)$ is a Gaussian random variable representing measurement noise. Let $p_{0_i} = p_0 + \kappa$, where κ represents the uncertainty introduced by the malicious anchor nodes in their transmit power levels to disrupt the localization process. κ is assumed to be a random variable that can follow any distribution; however, in this work, we assume $\kappa \sim \mathcal{U}(-\epsilon_{\text{att}}, \epsilon_{\text{att}})$ to be a uniform random variable [12] with probability density function (PDF) $f_\kappa(x)$

$$f_\kappa(x) = \begin{cases} \dfrac{1}{2\epsilon_{\text{att}}} & -\epsilon_{\text{att}} \le x \le \epsilon_{\text{att}} \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Similar attacks have been discussed in [12], [21], and [22]. Fig. 1(a) shows an uncoordinated attack, where a target node attempts to localize itself using information from seven anchor nodes of which three are malicious. The malicious anchor nodes change their transmit power levels dynamically and since the target node is not aware of their true transmit power (p_{0_i}), it incorrectly estimates its distance from the malicious anchor nodes resulting in a large error in its estimated location.

2) Coordinated Attack: In coordinated attacks, the malicious nodes communicate among themselves with the aim to make the target node appear to be located at a location different from its actual location. This type of attack is stronger than the uncoordinated attack. Similar to [11] and [23], we model the coordinated attack as

$$p_i^r = \begin{cases} p_0 - 10n\log_{10}(d_i) + \eta & \text{if node i is nonmalicious} \\ p_{0_i}^c - 10n\log_{10}(d_i) + \eta & \\ = p_0 - 10n\log_{10}(\|\mathbf{t}_{\text{att}} - \mathbf{a}_i\|_2) + \eta & \text{if node } i \text{ is malicious} \end{cases} \tag{4}$$

where $d_i = \|\mathbf{t} - \mathbf{a}_i\|_2$ and $p_{0_i}^c = p_0 - 10n\log_{10}(\chi_i)$ with $\chi_i = \frac{\|\mathbf{t}_{\text{att}} - \mathbf{a}_i\|_2}{\|\mathbf{t} - \mathbf{a}_i\|_2}$. $\mathbf{t}_{\text{att}}$ is the location where the malicious anchor nodes are trying to make the target node appear to be located, and $p_{0_i}^c$ is the transmit power of the i^{th} malicious anchor node. Thus, χ_i is the factor by which the malicious anchor nodes scale the actual distance between themselves and the target node.

A coordinated attack is shown in Fig. 1(b), where three malicious anchor nodes attempt to make the target node appear to be located at $\mathbf{t}_{\text{att}}$ instead of its actual location $\mathbf{t}$. It is seen that the dashed circles, with radius equal to the erroneous distance between the malicious anchor nodes and the target node, intersect at $\mathbf{t}_{\text{att}}$, whereas the dotted circles with radius equal to the actual distance between the nonmalicious anchor nodes and the target node intersect at $\mathbf{t}$.

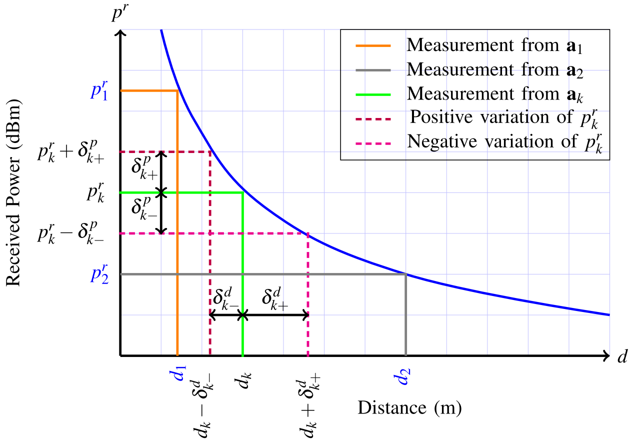


Fig. 2. Effect of variations in the received power on the distance estimate.

IV. Proposed Localization Techniques

The received power (p^r) as a function of the distance (d) between the anchor and target node is shown in Fig. 2. From (1)

$$d = 10^{\left(\frac{p_0 - p^r}{10n}\right)} \Rightarrow d = c\ 10^{\frac{-p^r}{10n}} \tag{5}$$

where $c = 10^{\frac{p_0}{10n}}$. As the relationship between p^r and d is nonlinear, variations in the received power affect the estimated distance in a nonlinear manner. From Fig. 2, it is seen that the distance estimates are more robust to variations in the received power when the anchor nodes are closer to the target node than when the anchor nodes are farther. Thus, anchor nodes closer to the target node should be given a larger weight in the localization process than anchor nodes that are farther.

In Fig. 2, a target node that receives a packet with power p_k^r from the k^{th} anchor node is estimated to be at a distance d_k from it. Positive and negative variations in the received power (p_k^r) are represented by δ_{k+}^p and δ_{k-}^p, and the corresponding variation in the distance estimates are represented by δ_{k-}^d and δ_{k+}^d. Lemma 4.1 quantifies the variation in the estimated distance corresponding to a variation in the received power.

Lemma 4.1: Relationship between the variation in received power and the corresponding variation in distance estimate is given by $\delta_{k-}^d = g(\delta_{k+}^p)10^{-\frac{p_k^r}{10n}}$ and $\delta_{k+}^d = -g(-\delta_{k-}^p)10^{-\frac{p_k^r}{10n}}$, where $g(x) = c\left(1 - 10^{\frac{-x}{10n}}\right)$, and $\delta_{k+}^p, \delta_{k-}^p > 0$.

Proof: From Fig. 2 and (5), we obtain $d_k - \delta_{k-}^d = c10^{-\frac{p_k^r + \delta_{k+}^p}{10n}}$. Thus, $\delta_{k-}^d = c10^{\frac{-p_k^r}{10n}} - c10^{-\frac{p_k^r + \delta_{k+}^p}{10n}} = 10^{-\frac{p_k^r}{10n}} c\left(1 - 10^{\frac{-\delta_{k+}^p}{10n}}\right) = 10^{-\frac{p_k^r}{10n}} g(\delta_{k+}^p)$. Similarly, it can be shown that $d_k + \delta_{k+}^d = c10^{-\frac{p_k^r - \delta_{k-}^p}{10n}} \Rightarrow \delta_{k+}^d = -10^{-\frac{p_k^r}{10n}} g(-\delta_{k-}^p)$. ■

Lemma 4.2: For the same amount of variation (δ_k^p) in the received power p_k^r, the received power with negative deviation ($p_k^r - \delta_k^p$) will result in a larger variation in the distance estimate than the received power with positive deviation ($p_k^r + \delta_k^p$), i.e., if $\delta_{k+}^p = \delta_{k-}^p = \delta_k^p$, then $\delta_{k+}^d > \delta_{k-}^d$.

Proof: Using Lemma 4.1, it can be shown that

$$\begin{aligned} g(x) + g(-x) &= c\left(2 - 10^{\frac{-x}{10n}} - 10^{\frac{x}{10n}}\right) \\ &= -\underbrace{\left(c10^{\frac{-x}{10n}}\right)}_{a(\geq 0)}\underbrace{\left(10^{\frac{x}{10n}} - 1\right)^2}_{b(\geq 0)} \leq 0. \end{aligned} \tag{6}$$

The variation in the distance estimates corresponding to a negative and positive variation in the received power p_k^r are given by $d_k + \delta_{k+}^d$ and $d_k - \delta_{k-}^d$, respectively. From Lemma 4.1

$$\delta_{k+}^d = -g\left(-\delta_k^p\right)10^{\frac{p_k^r}{10n}} \text{ and } \delta_{k-}^d = g\left(\delta_k^p\right)10^{\frac{p_k^r}{10n}}. \tag{7}$$

Using (6) and (7), it is seen that $\delta_{k+}^d \geq \delta_{k-}^d$ when $\delta_{k+}^p = \delta_{k-}^p = \delta_k^p$ [refer Fig. 2]. ■

Lemma 4.3 states that the distance estimation using RSS measurements from anchor nodes that are farther from the target node is less robust to variation in the received power.

Lemma 4.3: For the same amount of variation at two different received power levels, the lower received power level will result in larger variation in the distance estimate than the higher received power level, i.e., if $p_1^r > p_2^r$ and $\delta_1^p = \delta_2^p$, then $\delta_2^d > \delta_1^d$.

Proof: If variation in the received power levels is positive, i.e., $p_1^r + \delta_1^p$ and $p_2^r + \delta_2^p$, where $\delta_1^p = \delta_2^p > 0$, then the relationship between the corresponding variations in distance estimates is $\delta_2^d > \delta_1^d$. Using Lemma 4.1

$$p_1^r > p_2^r \Rightarrow g\left(\delta_2^p\right)10^{\frac{-p_2^r}{10n}} > g\left(\delta_1^p\right)10^{\frac{-p_1^r}{10n}} \Rightarrow \delta_2^d > \delta_1^d. \tag{8}$$

This relationship also holds if the variation in the received power levels is negative. ■

From Lemma 4.3, we can say that the malicious nodes that are closer to the target node can have a greater impact on disrupting the localization process than nodes that are farther. To reduce the effect of the malicious anchor nodes, we next propose secure localization techniques.

A. Weighted Least Square

We propose a localization technique based on the WLS algorithm [16]. This is a modified version of the LSs [24], where the anchor nodes are assigned weights based on their distance from the target node. The target node receives P packets from the i^{th} anchor node and computes the mean received power as $\overline{p_i^r} = \frac{1}{P}\sum_{j=1}^{P} p_{ij}^r$.

Using $\overline{p_i^r}$, the target node estimates its distance from the i^{th} anchor node as $\overline{d_i}$. Given $\mathbf{a}_i$ and $\overline{d_i}$ for $i = 1, \ldots, N$, the target node location estimation can be formulated as a WLSs problem, where each of the distance estimates is weighted by the variance of $\overline{d_i}^2$. Assuming $\overline{d_i}$ to be a random variable, its cumulative distribution function (CDF) $P(\overline{d_i} \leq \gamma)$ can be derived using (1) as

$$P\left(\log_{10}\left(\overline{d_i}\right) \leq \log_{10}(\gamma)\right) = P\left(\frac{\eta}{\sigma} \leq \frac{\overline{p_i^r} - p_0 + 10n\log_{10}(\gamma)}{\sigma}\right). \tag{9}$$

Let $\log_{10}(\omega_i) \triangleq \frac{\overline{p_i^r} - p_0}{-10n}$, and thus, (9) can be expressed as

$$\begin{aligned} P\left(\overline{d_i} \leq \gamma\right) &= P\left(\frac{\eta}{\sigma} \leq \frac{10n}{\sigma}\log_{10}\left(\frac{\gamma}{\omega_i}\right)\right) = P(Z \leq f(\gamma)) \\ &= \Phi(f(\gamma)) = \frac{1}{2}\left[1 + \operatorname{erf}\left(\frac{f(\gamma)}{\sqrt{2}}\right)\right] \end{aligned} \tag{10}$$

where $f(\gamma) = \frac{10n}{\sigma}\log_{10}\left(\frac{\gamma}{\omega_i}\right)$, $Z = \frac{\eta}{\sigma} \sim \mathcal{N}(0, 1)$, $\Phi(\cdot)$ is CDF of the standard normal distribution, and $\operatorname{erf}(\cdot)$ is the error function. The PDF of $\overline{d_i}$ is given by

$$\begin{aligned} f_{(\overline{d_i})}(\gamma) &= \frac{\mathrm{d}}{\mathrm{d}\gamma}P\left(\overline{d_i} \leq \gamma\right) = \frac{f'(\gamma)\exp\left(-\frac{f(\gamma)^2}{2}\right)}{\sqrt{2\pi}} \\ &= \frac{5n}{\gamma\,\sigma\ln(10)}\sqrt{\frac{2}{\pi}}\exp\left(-\frac{50n^2\ln^2\left(\frac{\gamma}{\omega_i}\right)}{\sigma^2\ln^2(10)}\right). \end{aligned} \tag{11}$$

Using (11), the variance of $\overline{d_i}$ and $\overline{d_i}^2$ can be shown to be [refer Appendix A for the derivation]

$$\operatorname{Var}\left(\overline{d_i}; \omega_i, \sigma\right) = \omega_i^2\exp\left(\frac{\sigma^2}{18.86n^2}\right)\left[\exp\left(\frac{\sigma^2}{18.86n^2}\right) - 1\right] \tag{12}$$

$$\operatorname{Var}\left(\overline{d_i}^2; \omega_i, \sigma\right) = \omega_i^4\exp\left(\frac{\sigma^2}{4.715n^2}\right)\left[\exp\left(\frac{\sigma^2}{4.715n^2}\right) - 1\right]. \tag{13}$$

The measurement matrix $\mathbf{P}^{\mathrm{r}} = [p_{ij}^r]$, where $i = 1, \ldots, N$ and $j = 1, \ldots, P$, consists of the RSS values of the P packets received by the target node from each of the N anchor nodes (both malicious and nonmalicious nodes). Consider a diagonal weight matrix $\mathbf{W}$ whose elements are reciprocal of the variance of $\overline{d_i}^2$

$$\mathbf{W} = \operatorname{diag}\left(\frac{1}{\operatorname{Var}\left(\overline{d_1}^2; \omega_1, \sigma\right)}, \ldots, \frac{1}{\operatorname{Var}\left(\overline{d_N}^2; \omega_N, \sigma\right)}\right). \tag{14}$$

The measurement model can be expressed as $\mathbf{b} = \mathbf{A}\boldsymbol{\theta} + \mathbf{w}$, where $\mathbf{w}$ is the noise vector. Without any assumption on the PDF of the noise term $\mathbf{w}$, the target node location estimation can be formulated as a WLSs problem [24]. The estimated target node location can be obtained as

$$\boldsymbol{\theta} = \left[t^x, t^y, \left(t^x\right)^2 + \left(t^y\right)^2\right]^T = \left(\mathbf{A}^T\mathbf{W}\mathbf{A}\right)^{-1}\mathbf{A}^T\mathbf{W}\mathbf{b} \tag{15}$$

where $\mathbf{A}$ and $\mathbf{b}$ are given in terms of $\mathbf{a}_i$ and $\overline{d_i}$ as

$$\mathbf{A} = \begin{pmatrix} -2a_1^x & -2a_1^y & 1 \\ -2a_2^x & -2a_2^y & 1 \\ \vdots & \vdots & \vdots \\ -2a_N^x & -2a_N^y & 1 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} \overline{d_1}^2 - \left(a_1^x\right)^2 - \left(a_1^y\right)^2 \\ \overline{d_2}^2 - \left(a_2^x\right)^2 - \left(a_2^y\right)^2 \\ \vdots \\ \overline{d_N}^2 - \left(a_N^x\right)^2 - \left(a_N^y\right)^2 \end{pmatrix}. \tag{16}$$

A flowchart of the WLS localization technique is shown in Fig. 3 and the detailed algorithm is given in the Supplementary Material.

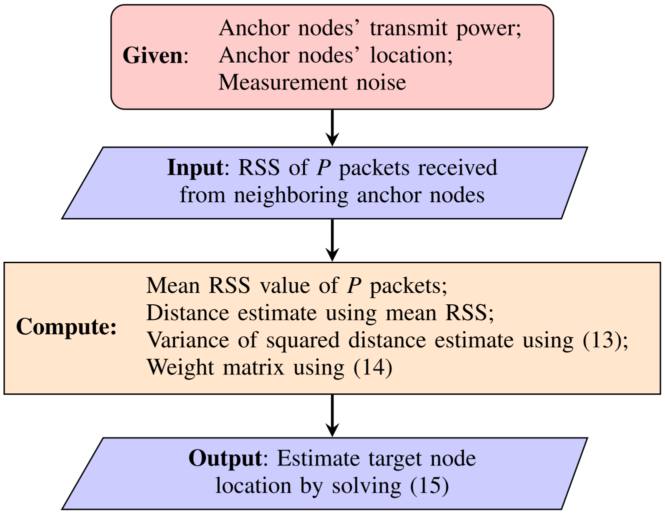

Given: Anchor nodes' transmit power;
Anchor nodes' location;
Measurement noise
Input: RSS of P packets received from neighboring anchor nodes
Compute: Mean RSS value of P packets;
Distance estimate using mean RSS;
Variance of squared distance estimate using (13);
Weight matrix using (14)
Output: Estimate target node location by solving (15)

Fig. 3. Flowchart of the WLS localization technique.

B. Secure Weighted Least Square

Consider an uncoordinated attack, where the malicious anchor nodes change their transmit powers arbitrarily without communicating this to the target node [refer Section III-1]. The received power (p_i^r) from a malicious anchor node can be expressed using (2) as

$$p_i^r = p_0 - 10n\log_{10}(d_i) + \eta + \kappa. \tag{17}$$

SWLS attempts to identify the malicious anchor nodes by observing the RSS values and eliminates them from the localization process. A flowchart of the SWLS localization technique is shown in Fig. 4 and the detailed algorithm is included in the Supplementary Material.

Let $\mathbf{D}$ be the $P \times N$ matrix of distance estimates from the target node to each of the anchor nodes, i.e., $\mathbf{D} = [d_{ij}]$, where $i = 1, \ldots, N$ and $j = 1, \ldots, P$, computed using (5). The average distance ($\overline{d_i}$) between the target node and an anchor node is calculated using $\overline{p^r}$ obtained from the RSS values of P packets and not as a column average of the matrix $\mathbf{D}$. This is due to the fact that the estimated distances (d_{ij}) do not follow a Gaussian distribution [refer (11)].

The variance of the distance estimates is computed using each of the P packets and (12), for different values of the noise standard deviation. An estimate of the noise standard deviation (σ_{est}) is obtained for each of the anchor nodes by solving

$$\begin{aligned}\hat{\sigma}_{\text{est}} &= \underset{\sigma_{\text{est}}\geq 0}{\arg\min}\ \left|\text{SVar}(d_{i1}, d_{i2}, \ldots, d_{iP}) - \text{Var}\left(\overline{d_i}; \omega_i, \sigma_{\text{est}}\right)\right| \\ &= \left[18.86n^2\ln\left(0.5 + 0.5\sqrt{1+\frac{4\text{SVar}(d_{i1}, d_{i2}, \ldots, d_{iP})}{\overline{d_i}^2}}\right)\right]^{\frac{1}{2}}\end{aligned} \tag{18}$$

where $\text{SVar}(d_{i1}, d_{i2}, \ldots, d_{iP})$ represents the sample variance of the distance estimates from each of the P packets. Refer Appendix B for the detailed derivation of $\hat{\sigma}_{\text{est}}$. The malicious nodes are identified by comparing $\hat{\sigma}_{\text{est}}$ with a threshold $\zeta\sigma$, where $\zeta > 0$ is a hyperparameter and an optimal value for ζ is determined empirically for a given network. If ζ is chosen to be too small, then SWLS will fail to identify malicious anchor nodes, and if ζ takes a large value, then SWLS will tag some of the nonmalicious anchor nodes as malicious. Finally, the WLS is applied to estimate the target node location by using information only from anchor nodes identified as nonmalicious

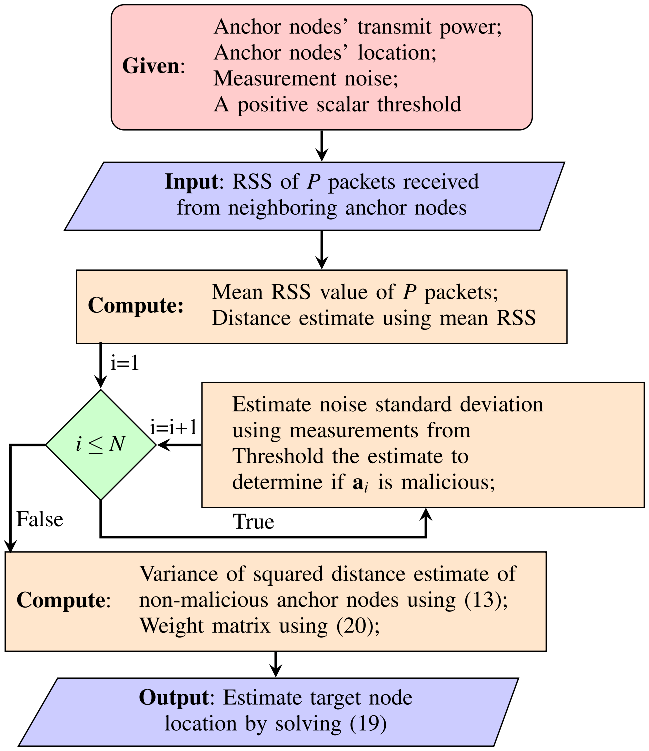

Given: Anchor nodes' transmit power;
Anchor nodes' location;
Measurement noise;
A positive scalar threshold
Input: RSS of P packets received from neighboring anchor nodes
Compute: Mean RSS value of P packets;
Distance estimate using mean RSS
i=1
$i \leq N$
i=i+1
Estimate noise standard deviation using measurements from
Threshold the estimate to determine if $\mathbf{a}_i$ is malicious;
True
False
Compute: Variance of squared distance estimate of non-malicious anchor nodes using (13);
Weight matrix using (20);
Output: Estimate target node location by solving (19)

Fig. 4. Flowchart of the SWLS localization technique.

$$\boldsymbol{\theta} = \left[t^x; t^y; \left(t^x\right)^2 + \left(t^y\right)^2\right] = \left(\hat{\mathbf{A}}^T\hat{\mathbf{W}}\hat{\mathbf{A}}\right)^{-1}\hat{\mathbf{A}}^T\hat{\mathbf{W}}\hat{\mathbf{b}} \tag{19}$$

where $\hat{\mathbf{A}} = \mathbf{A}(j, :)$, $\hat{\mathbf{b}} = \mathbf{b}(j, :)$, $j \in \mathcal{M}$ with $\mathcal{M}$ being the set of identified nonmalicious anchor nodes, and

$$\hat{\mathbf{W}} = \text{diag}\left(\frac{1}{\text{Var}\left(\overline{d_j}^2; \omega_j, \sigma\right)}\right), \quad j \in \mathcal{M}. \tag{20}$$

This technique relies on the variance in the RSS values, and in the case of a coordinated attack, the variance remains the same for malicious and nonmalicious anchor nodes [refer (4)]. Thus, this technique is not robust to coordinated attacks on the localization process.

C. Localization Using ℓ_1-Norm Optimization

The localization problem can be posed as a 3-D plane fitting problem $z = f(x, y)$, where z represents $\mathbf{b}$, and x and y represent the first two columns of $\mathbf{A}$ [refer (16)]. The objective is to find a plane $z = \alpha x + \beta y + \mu$, where $\alpha = t^x$, $\beta = t^y$, and $\mu = (t^x)^2 + (t^y)^2$, that fits the measurements (or data points)

$$\langle -2a_i^x, -2a_i^y, \overline{d_i}^2 - \left(a_i^x\right)^2 - \left(a_i^y\right)^2\rangle, \quad i = 1, \ldots, N. \tag{21}$$

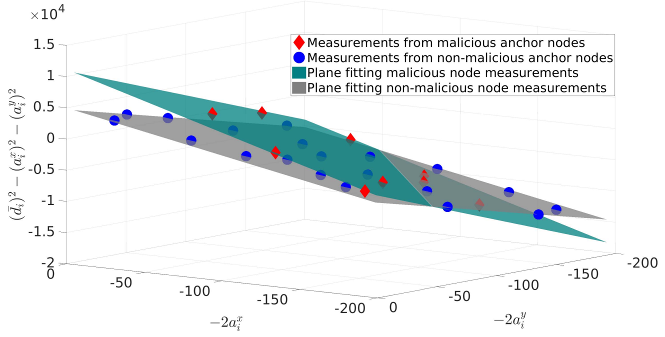


Fig. 5. Planes containing measurements corresponding to the malicious and nonmalicious anchor nodes. Anchor nodes are randomly distributed with 31% of the anchor nodes being malicious, $\sigma = 0$ dB, and $\|\mathbf{t} - \mathbf{t}_{\text{att}}\|_2 = 35.35$ m.

The values of α, β, and μ can be obtained by minimizing the ℓ_2-norm-based distance metric

$$\begin{aligned} &\min_{\mathbf{u}} \ \|\mathbf{r}\|_2^2 \\ &\text{subject to } \mathbf{r} = \mathbf{A}\mathbf{u} - \mathbf{b} \end{aligned} \tag{22}$$

where $\mathbf{u} = [\alpha, \beta, \mu]^T$. The closed-form solution of (22) is $\mathbf{u} = \mathbf{A}^{\dagger}\mathbf{b}$ [25], where $\dagger$ represents the pseudo inverse.

In an uncoordinated attack (2), the measurements representing points in three dimensions can be divided into two categories based on the variance of the RSS values. Measurements from nonmalicious anchor nodes would display less variance than those from malicious anchor nodes. However, in a coordinated attack (4), measurements from all the anchor nodes display similar variance since the malicious anchor nodes do not vary their transmit power randomly. The transmit power of the malicious anchor nodes is assumed to be different from those of the nonmalicious anchor nodes and depends on the value of χ_i [refer (4)]. Fig. 5 shows a coordinated attack visualized as a plane fitting problem. Each RSS measurement corresponds to a data point in this 3-D space. The data points corresponding to the measurements from nonmalicious anchor nodes (represented by blue circles) lie on the gray plane and measurements from malicious anchor nodes (represented by red diamonds) lie on the green plane. For $\sigma = 0$ dB, the data points will lie exactly on either of the two planes. Thus, the planes are parameterized by the location of the target node ($\mathbf{t}$) and the location where the malicious anchor nodes intend to make the target node appear ($\mathbf{t}_{\text{att}}$). Therefore, determining these planes will enable us to estimate $\mathbf{t}$ and $\mathbf{t}_{\text{att}}$. As $\|\mathbf{t} - \mathbf{t}_{\text{att}}\|_2$ increases, measurements corresponding to the malicious anchor nodes move farther from the plane that fits the measurements from the nonmalicious anchor nodes. This allows measurements from the malicious anchor nodes to be treated as outliers.

In both uncoordinated and coordinated attacks, (22) can be reformulated as a robust plane fitting problem by replacing ℓ_2-norm with ℓ_1-norm which is less sensitive to outliers [25]

$$\begin{aligned} &\min_{\mathbf{u}} \ \|\mathbf{r}\|_1 \\ &\text{subject to } \mathbf{r} = \mathbf{A}\mathbf{u} - \mathbf{b}. \end{aligned} \tag{23}$$

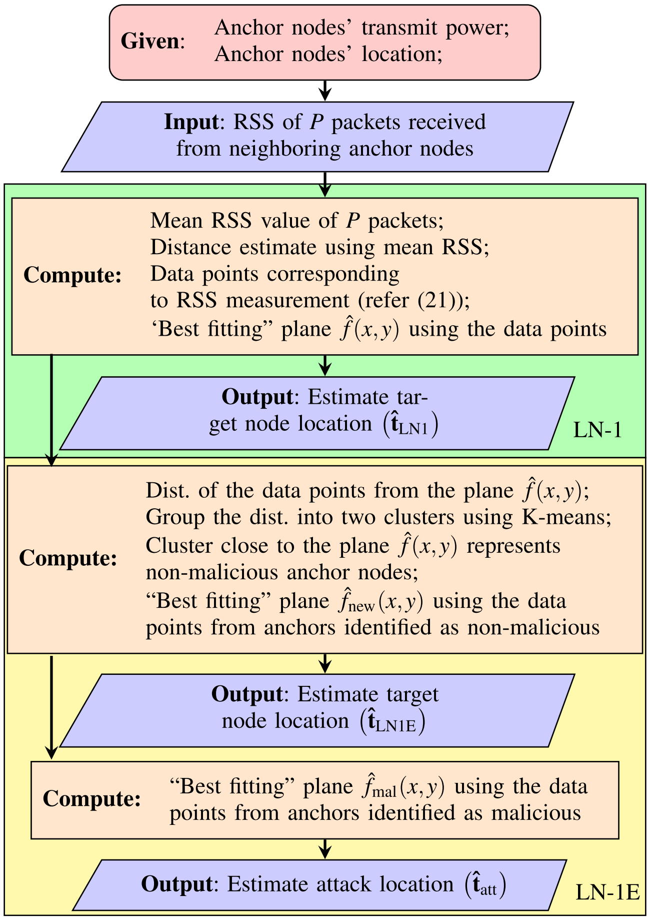

Given: Anchor nodes' transmit power;
Anchor nodes' location;
Input: RSS of P packets received from neighboring anchor nodes
Compute: Mean RSS value of P packets;
Distance estimate using mean RSS;
Data points corresponding to RSS measurement (refer (21));
'Best fitting" plane $\hat{f}(x,y)$ using the data points
Output: Estimate target node location $(\hat{\mathbf{t}}_{\text{LN1}})$
LN-1
Compute: Dist. of the data points from the plane $\hat{f}(x,y)$;
Group the dist. into two clusters using K-means;
Cluster close to the plane $\hat{f}(x,y)$ represents non-malicious anchor nodes;
"Best fitting" plane $\hat{f}_{\text{new}}(x,y)$ using the data points from anchors identified as non-malicious
Output: Estimate target node location $(\hat{\mathbf{t}}_{\text{LN1E}})$
Compute: "Best fitting" plane $\hat{f}_{\text{mal}}(x,y)$ using the data points from anchors identified as malicious
Output: Estimate attack location $(\hat{\mathbf{t}}_{\text{att}})$
LN-1E

Fig. 6. Flowchart of LN-1 and LN-1E localization techniques.

Assuming a majority of the anchor nodes are nonmalicious [11], [23], the malicious anchor nodes are expected to lie away from the plane obtained by solving (23). We can solve (23) efficiently using alternating direction method of multipliers (ADMM) by reformulating it as [26]

$$\begin{aligned} &\min_{\mathbf{u},\mathbf{z}} \ \|\mathbf{z}\|_1 \\ &\text{subject to } \mathbf{A}\mathbf{u} - \mathbf{z} = \mathbf{b}. \end{aligned} \tag{24}$$

Using standard ADMM steps, (24) can be solved iteratively

$$\mathbf{u}^{k+1} = \mathbf{G}\mathbf{A}^T\left(\mathbf{b} + \mathbf{z}^k - \frac{\mathbf{y}^k}{\rho}\right) \tag{24a}$$

$$\mathbf{z}^{k+1} = S_{\frac{1}{\rho}}\left(\mathbf{A}\mathbf{u}^{k+1} - \mathbf{b}^k + \frac{\mathbf{y}^k}{\rho}\right) \tag{24b}$$

$$\mathbf{y}^{k+1} = \mathbf{y}^k + \rho\left(\mathbf{A}\mathbf{u}^{k+1} - \mathbf{z}^{k+1} - \mathbf{b}\right) \tag{24c}$$

where $\mathbf{G} = (\mathbf{A}^T\mathbf{A})^{-1}$, $\mathbf{y}$ is the dual variable (Lagrange multiplier), and $\rho (>0)$ is the penalty parameter for violation of the linear constraint [27]. $S_{\frac{1}{\rho}}(x) = \{\max(|x| - \frac{1}{\rho}, 0).\text{sign}(x)\}$ is the proximal operator of ℓ_1-norm [28]. The convergence criterion is $|\|\mathbf{z}^{k+1}\|_1 - \|\mathbf{z}^k\|_1| \leq Conv_{\text{ADMM}}$, where $Conv_{\text{ADMM}} > 0$.

We propose two localization techniques LN-1 and LN-1E. LN-1 attempts to solve (24) in order to localize the target node in both uncoordinated and coordinated attack scenarios. LN-1E is an improvement over LN-1 to handle only coordinated attacks. LN-1E identifies the malicious anchor nodes by first executing LN-1 and then recomputes the plane after eliminating measurements from the anchor nodes identified as malicious. In LN-1, we determine the "best fitting" plane for measurements from all the anchor nodes $\hat{f}(x,y) = \widehat{\alpha}x + \widehat{\beta}y + \widehat{\mu}$. The data points corresponding to the nonmalicious anchor nodes are expected to lie closer to this plane than those corresponding to the malicious anchor nodes. Any standard clustering technique [29] can be used to partition the anchor nodes into two clusters based on their distance from this plane. In this article, we have used K-means clustering for partitioning the anchor nodes. The flowchart for LN-1 and LN-1E techniques is shown in Fig. 6 and the detailed algorithms are given in the Supplementary Material. The centroid of the cluster containing the malicious anchor nodes will be farther from the plane than the centroid of the other cluster. After identifying the two clusters, we recompute the "best fitting" plane $\hat{f}_{\text{new}}(x,y)$ using measurements only from the nonmalicious anchor nodes. We can also estimate the plane $\hat{f}_{\text{mal}}(x,y)$ corresponding to measurements only from the malicious anchor nodes and use it to estimate the location $\mathbf{t}_{\text{att}}$, where the malicious anchor nodes want to make the target node appear to be located.

V. Cramer–Rao Lower Bound

CRLB provides a lower bound on the variance of an unbiased estimator and can be used as a benchmark for other estimators [24], [30]. The MSE of an unbiased estimator $(\hat{\mathbf{t}})$ of the target node position $(\mathbf{t})$ can be bounded using the CRLB as

$$\begin{aligned}\text{MSE}(\hat{\mathbf{t}}) &= \mathbb{E}\left[\left(\hat{t^x} - t^x\right)^2\right] + \mathbb{E}\left[\left(\hat{t^y} - t^y\right)^2\right]\\ &= \text{SVar}(\hat{t^x}) + \text{SVar}(\hat{t^y}) \geq \left[\mathbf{F}^{-1}\right]_{11} + \left[\mathbf{F}^{-1}\right]_{22}\\ &= \text{tr}\left(\mathbf{F}^{-1}\right)\end{aligned} \tag{25}$$

where $\mathbf{F}$ is the Fisher information matrix (FIM). RMSE of an unbiased estimator satisfies $\text{RMSE}(\hat{\mathbf{t}}) \geq \sqrt{\text{tr}(\mathbf{F}^{-1})}$. Thus, CRLB provides a lower bound on the RMSE of unbiased estimators for the target node position. We define $\mathcal{A}_{\text{nm}}$ and $\mathcal{A}_{\text{m}}$ as sets containing the indices of nonmalicious and malicious anchor nodes, respectively.

A. CRLB for Uncoordinated Attack

Since the uncertainty introduced by the malicious anchor nodes and the measurement noise [refer (2)] is the sum of independent uniform and Gaussian random variables $(V = \eta + \kappa)$, the PDF of V is given by

$$\begin{aligned}f_V(x) = \left(f_\eta * f_\kappa\right)(x) &= \int_{-\epsilon_{\text{att}}}^{\epsilon_{\text{att}}} \frac{1}{2\sqrt{2\pi}\,\sigma\,\epsilon_{\text{att}}} \exp\left(\frac{-(x-k)^2}{2\sigma^2}\right) dk\\ &= \frac{1}{4\epsilon_{\text{att}}}\left(\text{erf}\left(\frac{x+\epsilon_{\text{att}}}{\sqrt{2}\sigma}\right) - \text{erf}\left(\frac{x-\epsilon_{\text{att}}}{\sqrt{2}\sigma}\right)\right)\end{aligned} \tag{26}$$

where $f_\eta(\cdot)$ is the PDF of measurement noise η. The standard deviation of the net perturbation in the measurements is $V_{\text{std}} = \sqrt{\sigma^2 + \frac{\epsilon_{\text{att}}^2}{3}}$. Therefore, PDF of the RSS values at the target node in an uncoordinated attack is given by

$$\begin{aligned}&p(\mathbf{P}^{\text{r}}; \mathbf{t})\\ &\quad= \prod_{j=1}^{P}\left[\prod_{i\in\mathcal{A}_{\text{nm}}} p\left(p_{ij}^r; \mathbf{t}\right) \times \prod_{k\in\mathcal{A}_{\text{m}}} p\left(p_{kj}^r; \mathbf{t}\right)\right]\\ &\quad= \prod_{j=1}^{P}\left[\prod_{i\in\mathcal{A}_{\text{nm}}} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\frac{-\left(p_{ij}^r - p_0 + 10n\log_{10}(d_i)\right)^2}{2\sigma^2}\right.\\ &\qquad\left.\times \prod_{k\in\mathcal{A}_{\text{m}}} \frac{1}{4\epsilon_{\text{att}}}\left(\text{erf}\left(\frac{p_{kj}^r - \Delta_1^k}{\sqrt{2}\sigma}\right) - \text{erf}\left(\frac{p_{kj}^r - \Delta_2^k}{\sqrt{2}\sigma}\right)\right)\right]\end{aligned} \tag{27}$$

where $\Delta_1^k = p_0 - 10n\log_{10}(d_k) - \epsilon_{\text{att}}$ and $\Delta_2^k = p_0 - 10n\log_{10}(d_k) + \epsilon_{\text{att}}$. The PDF $p(\mathbf{P}^{\text{r}}; \mathbf{t})$ satisfies the regularity conditions $\mathbb{E}\left[\frac{\partial \ln(p(\mathbf{P}^{\text{r}};\mathbf{t}))}{\partial t^x}\right] = 0$ and $\mathbb{E}\left[\frac{\partial \ln(p(\mathbf{P}^{\text{r}};\mathbf{t}))}{\partial t^y}\right] = 0$, and therefore, the CRLB for uncoordinated attack is given by $t_{\text{CRLB}}^{\text{uc}} = \sqrt{\text{tr}(\mathbf{F}_{\text{uc}}^{-1})}$, where the FIM is given by $\mathbf{F}_{\text{uc}} = [f_{xx}^{\text{uc}}\ f_{xy}^{\text{uc}};\ f_{yx}^{\text{uc}}\ f_{yy}^{\text{uc}}]$ with

$$\begin{aligned}f_{xx}^{\text{uc}} = \frac{100\ Pn^2}{\ln^2(10)}&\left[\frac{1}{\sigma^2}\sum_{i\in\mathcal{A}_{\text{nm}}} \frac{\left(a_i^x - t^x\right)^2}{\|\mathbf{a}_i - \mathbf{t}\|_2^4}\right.\\ &\left.+ \frac{I}{2\pi\sigma^2\epsilon_{\text{att}}}\sum_{k\in\mathcal{A}_{\text{m}}} \frac{\left(a_k^x - t^x\right)^2}{\|\mathbf{a}_k - \mathbf{t}\|_2^4}\right]\end{aligned} \tag{28a}$$

$$\begin{aligned}f_{yy}^{\text{uc}} = \frac{100\ Pn^2}{\ln^2(10)}&\left[\frac{1}{\sigma^2}\sum_{i\in\mathcal{A}_{\text{nm}}} \frac{\left(a_i^y - t^y\right)^2}{\|\mathbf{a}_i - \mathbf{t}\|_2^4}\right.\\ &\left.+ \frac{I}{2\pi\sigma^2\epsilon_{\text{att}}}\sum_{k\in\mathcal{A}_{\text{m}}} \frac{\left(a_k^y - t^y\right)^2}{\|\mathbf{a}_k - \mathbf{t}\|_2^4}\right]\end{aligned} \tag{28b}$$

$$\begin{aligned}f_{xy}^{\text{uc}} = \frac{100\ Pn^2}{\ln^2(10)}&\left[\frac{1}{\sigma^2}\sum_{i\in\mathcal{A}_{\text{nm}}} \frac{\left(a_i^x - t^x\right)\left(a_i^y - t^y\right)}{\|\mathbf{a}_i - \mathbf{t}\|_2^4}\right.\\ &\left.+ \frac{I}{2\pi\sigma^2\epsilon_{\text{att}}}\sum_{k\in\mathcal{A}_{\text{m}}} \frac{\left(a_k^x - t^x\right)\left(a_k^y - t^y\right)}{\|\mathbf{a}_k - \mathbf{t}\|_2^4}\right]\end{aligned} \tag{28c}$$

where

$$I = \int_{-\infty}^{\infty} \frac{\left[\exp\left(\frac{-\left(p_{ij}^r - \Delta_1^k\right)^2}{2\sigma^2}\right) - \exp\left(\frac{-\left(p_{ij}^r - \Delta_2^k\right)^2}{2\sigma^2}\right)\right]^2}{\text{erf}\left(\frac{p_{ij}^r - \Delta_1^k}{\sqrt{2}\sigma}\right) - \text{erf}\left(\frac{p_{ij}^r - \Delta_2^k}{\sqrt{2}\sigma}\right)} dp_{ij}^r \tag{29}$$

and can be calculated using numerical integration. I is independent of d_k, as Δ_1^k and Δ_2^k only shift the integrand on the p_{ij}^r axis. The detailed derivation of the regularity condition and CRLB are given in Appendixes C and D.

B. CRLB for Coordinated Attack

The PDF of the measurement matrix $\mathbf{P}^{\rm r}$ in the coordinated attack scenario can be expressed as

$$p(\mathbf{P}^{\rm r};\mathbf{t}) = \frac{1}{\sqrt{2\pi\sigma^2}}\prod_{j=1}^{P}\Bigg[\prod_{i\in\mathcal{A}_{\rm nm}}\exp\frac{-\left(p^r_{ij}-p_0+10n\log_{10}(d_i)\right)^2}{2\sigma^2} \times \prod_{k\in\mathcal{A}_{\rm m}}\exp\frac{-\left(p^r_{kj}-p_0+10n\log_{10}(d'_k)\right)^2}{2\sigma^2}\Bigg] \tag{30}$$

where $d'_k = \|\mathbf{a}_k - \mathbf{t}_{\rm att}\|_2$. The PDF $p(\mathbf{P}^{\rm r};\mathbf{t})$ satisfies the regularity conditions $\mathbb{E}\big[\frac{\partial \ln(p(\mathbf{P}^{\rm r};\mathbf{t}))}{\partial t^x}\big] = 0$ and $\mathbb{E}\big[\frac{\partial \ln(p(\mathbf{P}^{\rm r};\mathbf{t}))}{\partial t^y}\big] = 0$, and therefore, the CRLB for coordinated attack is $t^c_{\rm CRLB} = \sqrt{\mathrm{tr}(\mathbf{F}_{\rm c}^{-1})}$. The FIM for coordinated attack is given by $\mathbf{F}_{\rm c} = [f^{\rm c}_{xx}\ \ f^{\rm c}_{xy};\ f^{\rm c}_{yx}\ \ f^{\rm c}_{yy}]$ where

$$f^{\rm c}_{xx} = \frac{100\ Pn^2}{\sigma^2\ln^2(10)}\left[\sum_{i\in\mathcal{A}_{\rm nm}}\frac{\left(a^x_i - t^x\right)^2}{\|\mathbf{a}_i-\mathbf{t}\|_2^4}\right] \tag{31a}$$

$$f^{\rm c}_{yy} = \frac{100\ Pn^2}{\sigma^2\ln^2(10)}\left[\sum_{i\in\mathcal{A}_{\rm nm}}\frac{\left(a^y_i - t^y\right)^2}{\|\mathbf{a}_i-\mathbf{t}\|_2^4}\right] \tag{31b}$$

$$f^{\rm c}_{xy} = \frac{100\ Pn^2}{\sigma^2\ln^2(10)}\left[\sum_{i\in\mathcal{A}_{\rm nm}}\frac{\left(a^x_i - t^x\right)\left(a^y_i - t^y\right)}{\|\mathbf{a}_i-\mathbf{t}\|_2^4}\right]. \tag{31c}$$

CRLB is used as a benchmark as it represents the minimum RMSE that can be achieved by an unbiased estimator.

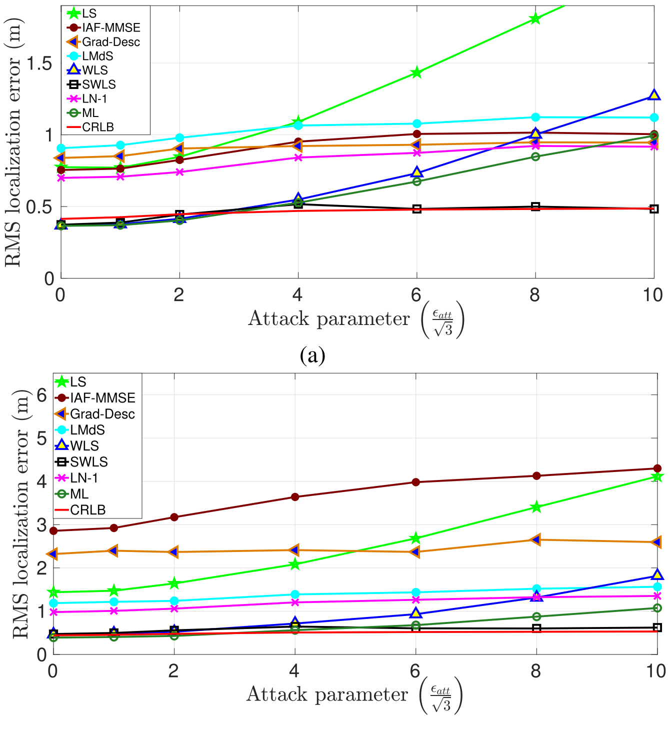
VI. Performance Evaluation Using Simulations

In this section, we present performance evaluation of the proposed secure localization techniques and compare it with existing techniques from the literature, namely, LSs [24], IAF-MMSE [11], LMdS [13], gradient descent (Grad-Desc) [12], [23], and maximum likelihood (ML) [24] methods. Consider a network spread across 100 m × 100 m area with 29 anchor nodes and one target node. We assume the anchor nodes have $p_0 = -10$ dBm, and the path loss exponent $n = 4$ representing a suburban environment [31]. The value of p^r_{ij} is calculated using (2) or (4) depending on the type of attack.

The LS method solves for the target node location as $\hat{\mathbf{t}} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}$. ML estimate for the target node location is obtained by solving the nonconvex optimization problem

$$\hat{\mathbf{t}} = \underset{\mathbf{t}}{\operatorname{argmin}}\sum_{j=1}^{P}\sum_{i=1}^{N}\left(p^r_{ij} - p_0 + 10n\log_{10}(d_i)\right)^2. \tag{32}$$

We solve (32) using the fminunc function in MATLAB, which is based on the quasi-Newton method [32]. ML is initialized with the true location of the target node. For IAF-MMSE, the hyperparameters θ and α (refer [11, Algorithms 2 and 3]) are set to σ^2 and 0, respectively. For Grad-Desc, the maximum number of iterations is 200 and a constant step size of 0.4 is chosen. Variable step size is not considered as its performance is reported to be similar to that with a constant step size [12]. The threshold for the anchor selection or pruning step in Grad-Desc is empirically set to a value that gives the best performance [23]. For LMdS, we consider 20 (intersecting) subsets with each subset consisting of four anchor nodes. In SWLS, ζ is empirically set to 1.5. LN-1 and LN-1E use ADMM to solve (24), and $Conv_{\rm ADMM}$ and ρ are empirically set to 10^{-6} and 0.2, respectively. The maximum number of iterations allowed for ADMM to converge is set to 5000. The simulation parameters are chosen similar to those in [12] and [23]. We consider a randomly deployed network with 29 anchor nodes and one target node. Of these, a certain percentage of anchor nodes are malicious and attempt to disrupt the target node's localization process. All results reported in this article are based on 5000 Monte Carlo simulations. Table II lists the various localization techniques considered in this article.



(a)

(b)

Fig. 7. Performance of localization techniques under uncoordinated attack ($P = 10$ and percentage of malicious nodes is 28%). RMS localization error as a function of $\epsilon_{\rm att}$ with $\sigma = 2$ dB and the target node at (a) (49, 49) m and (b) (10, 60) m.

A. Uncoordinated Attack

Fig. 7(a) and (b) shows the performance of the various secure localization techniques in terms of the RMS localization error and as a function of $\epsilon_{\rm att}$. The target node estimates its location by executing the localization process after receiving ten packets from each of the anchor nodes. In the Monte Carlo simulations, the topology and percentage of malicious anchor nodes are kept fixed, while the malicious anchor nodes are chosen randomly from the 29 anchor nodes for each simulation run. Simulations are also carried out to study the performance of the algorithms as the target node moves close to the edge of the network [refer Fig. 7(b)].

SWLS and WLS techniques assign large weights to the anchor nodes located closer to the target node, and thus,

TABLE II
LOCALIZATION TECHNIQUES BEING COMPARED

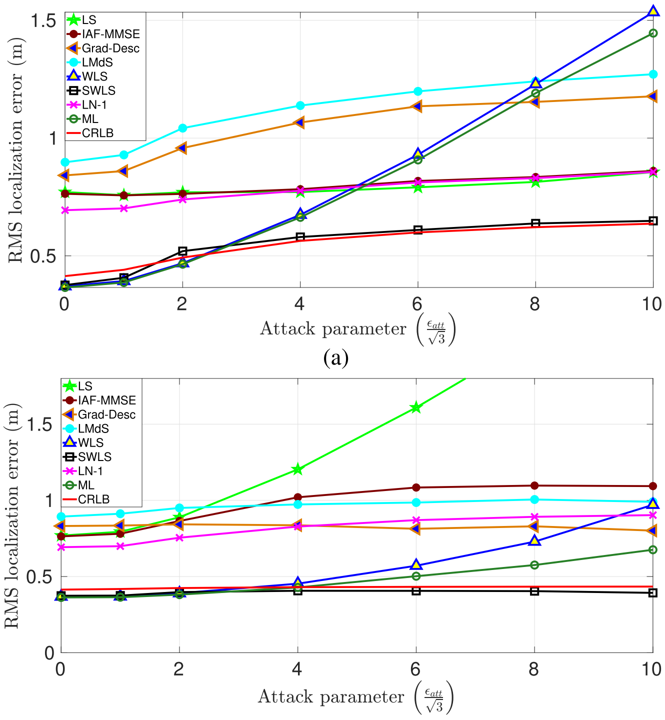
Algorithm	Description	Uncoordinated	Coordinated	Hyperparameters	Estimate of σ
LS	Least square-based localization [33]	✓	✗	–	Not required
IAF-MMSE	Inside-attack filtering minimum mean square error [11]	✓	✓	θ, α	Required
Grad-Desc	Iterative gradient descent with selective pruning [12]	✓	✓	Step size, threshold	Not required
LMdS	Least median of squares [13]	✓	✓	Number of subsets, number of anchors/subset	Not required
WLS	Weighted LS	✓	✓	–	Required
SWLS	Secure weighted LS	✓	✗	ζ	Required
LN-1	ℓ_1-norm based	✓	✓	$Conv_{\text{ADMM}}$, ρ	Not required
LN-1E	ℓ_1-norm based with malicious anchor node elimination	✗	✓	$Conv_{\text{ADMM}}$, ρ	Not required

reduce the effect of the larger distance estimation errors from the farther anchor nodes in the localization process. The performance of SWLS and WLS are similar as long as ϵ_{att} is not significantly larger than the measurement noise (σ). However, WLS performance deteriorates as $\frac{\epsilon_{\text{att}}}{\sqrt{3}}$ becomes larger than σ with WLS assigning larger weight to the malicious anchor nodes close to the target node. On the other hand, SWLS outperforms the other techniques as it attempts to eliminate the malicious anchor nodes from the localization process. SWLS is the only estimator whose RMS localization error is close to the CRLB in most scenarios. CRLB is almost constant even as ϵ_{att} increases since only 28% of the anchor nodes are malicious. From (28), it can be seen that the CRLB will be significantly affected when the percentage of malicious anchor nodes is higher and $\frac{\epsilon_{\text{att}}}{\sqrt{3}} > \sigma$. When the target node is moved close to the edge of the network [refer Fig. 7(b)], the performance of Grad-Desc degrades significantly as it appears to get stuck in local minima. A similar degradation in performance is observed for IAF-MMSE also. The relative performance of the other techniques is similar to the case when the target node is located at the center of the network.

Next, we study the performance of the localization techniques when the malicious anchor nodes are located near the edge of the network or close to the target node [refer Fig. 8]. It is seen that LS and IAF-MMSE are significantly affected by the location of the malicious anchor nodes and their performance deteriorates as the malicious anchor nodes move toward the edge of the network. In Fig. 8(a), when the malicious anchor nodes are located close to the target, LS and IAF-MMSE outperform LMdS and Grad-Desc. LS assigns equal weight to measurements from all anchor nodes, and from Lemma 4.3, we know that distance estimates for anchor nodes located farther from the target node tend to have larger errors.

In Fig. 8(a), the localization performance of LMdS and Grad-Desc deteriorates gradually with increase in ϵ_{att}. However, as the malicious anchor nodes move away from the target node and toward the edge of the network, these two techniques display robustness to the attack [refer Fig. 8(b)]. LMdS and Grad-Desc pick four and $\frac{N}{2}$ (or 15) anchor nodes, respectively. When the malicious anchor nodes are close to the target node, the residuals of the subset in LMdS or their gradients in Grad-Desc are lower than when the malicious anchor nodes are farther from the target nodes resulting in some malicious anchor nodes being chosen. In contrast to LS, WLS is more robust to locations of the malicious anchor nodes (located at the edge of the network) as it assigns larger weight to anchor nodes that are located closer to the target node. In Fig. 8(a), the localization error using SWLS increases abruptly as $\frac{\epsilon_{\text{att}}}{\sqrt{3}}$ becomes greater than σ. For $\frac{\epsilon_{\text{att}}}{\sqrt{3}} < \sigma$, V_{std} [refer Section V-A] is not significantly larger than σ, and thus, the localization accuracy is not significantly affected. When $\frac{\epsilon_{\text{att}}}{\sqrt{3}} > \sigma$, SWLS can identify the malicious anchor nodes and eliminate them. Similar behavior can be expected in Fig. 8(b) except now the malicious anchor nodes are farther from the target node and are assigned lower weight. Thus, the localization performance does not deteriorate, as shown in Fig. 8(a). ML outperforms WLS for higher values of ϵ_{att}, otherwise exhibits similar trend as WLS. In Fig. 8, the SWLS performance is close to the CRLB and outperforms the other estimators.

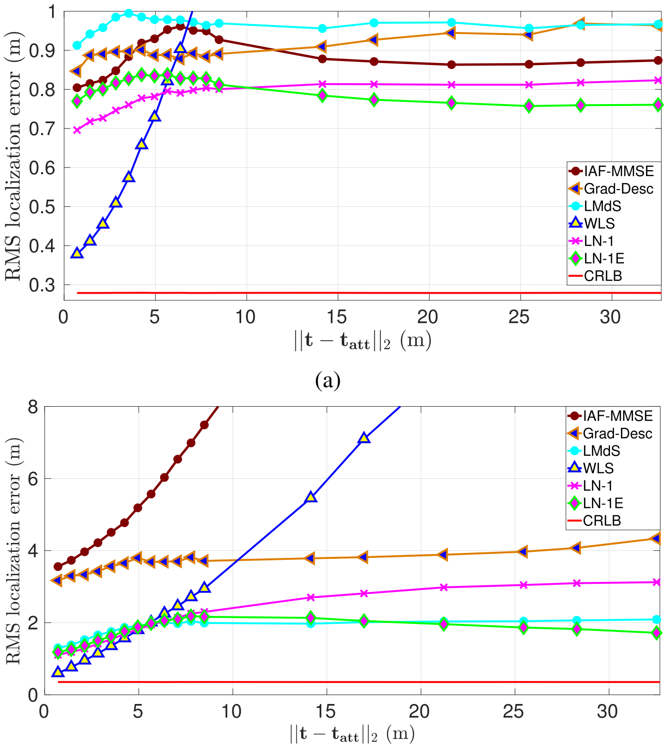
The localization performance of LN-1 is not affected by the location of the malicious anchor nodes with a similar



(a)

(b)

Fig. 8. Performance of localization techniques under uncoordinated attack [$\sigma = 2$ dB, $P = 10$, target node at (49, 49) m, and percentage of malicious anchor nodes is 28%]. (a) RMS localization error when the malicious anchor nodes are close to the target node (within 32 m). (b) RMS localization error when the malicious anchor nodes are located at the edge of the network.



(a)

(b)

Fig. 9. Performance of secure localization techniques under coordinated attack as a function of the strength of the attack ($\sigma = 2$ dB and $P = 10$). (a) RMS localization error with 10% of the anchor nodes being malicious and target node at $(49, 49)$ m. (b) RMS localization error with 28% of the anchor nodes being malicious and target node at $(5, 50)$ m.

performance in the cases considered in Figs. 7(a) and 8. LN-1 does not weigh measurements from anchor nodes differently depending on their location nor does it eliminate anchor nodes from the localization process. It only reduces the weight of those measurements that exhibit higher variance (outliers). Additional results considering the effect of the number of packets and the percentage of malicious anchor nodes on the localization performance are provided in Section II of the Supplementary Material.

B. Coordinated Attack

For coordinated attack, we consider the following localization techniques: WLS, IAF-MMSE, Grad-Desc, LMdS, LN-1, and LN-1E. The other techniques are not considered as their performance is poor under coordinated attack. Fig. 9 presents the localization performance under coordinated attack as the strength of the attack is increased by increasing the distance between $\mathbf{t}$ and $\mathbf{t}_{\text{att}}$. In Fig. 9(a), with 10% of the anchor nodes being malicious, WLS significantly outperforms the other techniques when the coordinated attack is mild. However, as the attack becomes stronger, the WLS performance deteriorates rapidly. LN-1 and LN-1E have a similar performance with both outperforming IAF-MMSE, Grad-Desc, and LMdS. The performance of LMdS and Grad-Desc suffers due to the elimination of some of the anchor nodes from the localization process. When the percentage of malicious anchor nodes is low and $\mathbf{t}_{\text{att}}$ is close to $\mathbf{t}$, eliminating the malicious anchor nodes does not improve the localization accuracy as the measurement noise tends to determine the localization performance.

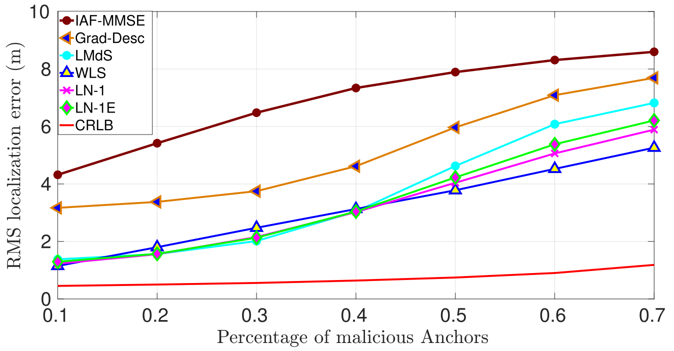
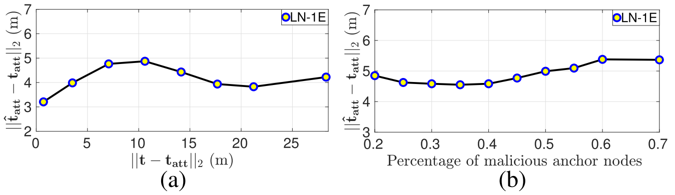


Fig. 10. Performance of localization techniques under coordinated attack as a function of the percentage of malicious anchor nodes [$\sigma = 2$ dB, $P = 10$, $\mathbf{t}_{\text{att}} = [t^x + 5, t^y + 5]^T$, $\|\mathbf{t} - \mathbf{t}_{\text{att}}\|_2 = 7.07$ m, and target node at $(5, 50)$ m].



(a)

(b)

Fig. 11. Performance of LN-1E in estimating $\mathbf{t}_{\text{att}}$ under coordinated attack [$\sigma = 2$ dB, $P = 10$, and target node at $(49, 49)$ m]. (a) Percentage of malicious anchor nodes is 28%. (b) Strength of the attack is $\mathbf{t}_{\text{att}} = [t^x + 4, t^y + 4]^T$.

In Fig. 9(b), we show the performance of the localization techniques when the target node is located close to the edge of the network. The performance of IAF-MMSE and Grad-Desc degrades significantly, while LN-1, LN-1E, and LMdS have a similar performance and degrade to a lesser extent. From (31), we note that the FIM $\mathbf{F}_{\text{c}}$ does not depend on $\|\mathbf{t} - \mathbf{t}_{\text{att}}\|_2$, and thus, the CRLB in Fig. 9 is constant.

Fig. 10 shows the localization performance as a function of the percentage of malicious anchor nodes. The malicious anchor nodes attempt to make the target node appear at $[t^x+5, t^y+5]^T$ instead of its true location $[t^x, t^y]^T$. The performance of Grad-Desc and IAF-MMSE is consistently inferior to the other techniques when the target node is located near the edge of the network. When the percentage of malicious anchor nodes is less than 50%, WLS, LMdS, LN-1, and LN-1E have a similar performance. However, as the percentage of malicious anchor nodes exceeds 50%, LMdS performance deteriorates as it is unable to consistently find a subset containing only nonmalicious anchor nodes. WLS outperforms the other techniques and is followed by LN-1 and LN-1E.

Fig. 11(a) shows the performance of LN-1E in estimating $\mathbf{t}_{\text{att}}$ as the strength of the attack ($\|\mathbf{t} - \mathbf{t}_{\text{att}}\|_2$) increases. When the attack is weak, LN-1E may not be able to cluster the malicious and nonmalicious anchor nodes. As the attack becomes stronger, LN-1E is able to cluster the anchor nodes resulting in improved performance. Fig. 11(b) shows the performance of LN-1E in estimating $\mathbf{t}_{\text{att}}$ as the percentage of malicious anchor nodes increases. The estimation error does not vary significantly when the percentage of malicious anchor nodes is less than 50%. However, when more than 50% of the anchor nodes are malicious, LN-1E is unable to cluster the anchor nodes accurately resulting in a deterioration in its performance. Further error analysis of the localization performance is presented in Section III of the supplementary material.

C. Security Performance

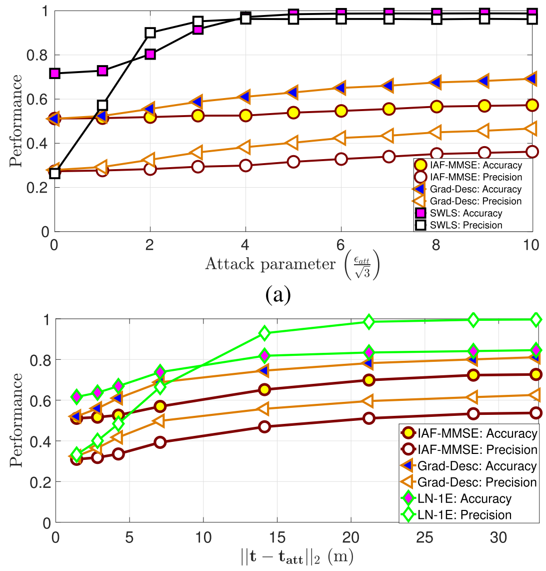
We next study the security performance of the proposed localization techniques in terms of their ability to identify the malicious anchor nodes. We consider the following two performance parameters:

$$\text{accuracy} = \frac{TP + TN}{TP + TN + FP + FN},$$
$$\text{precision} = \frac{TP}{TP + FP}$$

where TP is the number of correctly identified malicious anchor nodes, TN is the number of correctly identified nonmalicious anchor nodes, FP is the number of nonmalicious anchor nodes identified as malicious, and FN is the number of malicious anchor nodes identified as nonmalicious. Fig. 12(a) shows the security performance of IAF-MMSE, Grad-Desc, and SWLS under uncoordinated attack, and Fig. 12(b) shows the performance of IAF-MMSE, Grad-Desc, and LN-1E under coordinated attack, as a function of the strength of the attack. SWLS in uncoordinated attack and LN-1E in coordinated attack outperform the other techniques, and their accuracy and precision improve as the strength of the attack increases. In an uncoordinated attack, as the strength of the attack increases, V_{std} increases, and SWLS is able to identify the malicious anchor nodes better. Similarly, in a coordinated attack as the strength of the attack increases, LN-1E is able to cluster the malicious anchor nodes with improved accuracy. Grad-Desc does not perform well since it retains 50% of the anchor nodes as nonmalicious irrespective of the percentage of malicious anchor nodes and strength of the attack.

D. Computational Complexity

We next present a comparison of the computational complexity of the different localization techniques. Table III shows the asymptotic complexities of the localization techniques considered in this work. For WLS, the WLS (15) is the dominant computational step. Computing $\hat{\boldsymbol{\theta}}$ requires five matrix multiplications and one matrix inversion. Therefore, the computational complexity of WLS is $\mathcal{O}(3N^2 + 9N + 3N + 3^3 + 3^2 + N^2) \simeq \mathcal{O}(N^2)$. Similarly, the computational complexity of LS is $\mathcal{O}(N^2)$, and SWLS is $\mathcal{O}(|\mathcal{M}|^2)$, where $\mathcal{M}$ is the set of nonmalicious anchor nodes identified by SWLS. LN-1 executes (24a)–(24c) in an iterative manner until convergence is achieved. Assuming ADMM requires k_{ADMM} iterations on average to converge, and the computational complexity of (24a) is $\mathcal{O}(N)$ and the computational complexity for the ADMM steps is $\mathcal{O}(k_{\text{ADMM}}N)$. Thus, the computational complexity of LN-1 is $\mathcal{O}(\max(k_{\text{ADMM}}N, N^2)) \simeq \mathcal{O}(k_{\text{ADMM}}N)$, as in general $k_{\text{ADMM}} > N$. In addition to the steps in LN-1, LN-1E involves K-means clustering which has a complexity of $\mathcal{O}(NTk_{\text{K-means}})$ [34], where $k_{\text{K-means}}$ is the average number of iterations and T is the complexity for calculating the distance between two data. The computational complexity of LN-1E is $\mathcal{O}(\max(NTk_{\text{K-means}}, k_{\text{ADMM}}N))$. LMdS involves two main operations: (1) dividing the RSS measurements into M_{LMdS} subsets with each subset containing N_{LMdS} anchor nodes, and the target location is estimated for each subset using LS technique, and (2) computing median of the residue of the results obtained from each of the subsets. The computational complexity of the first operation is $\mathcal{O}(M_{\text{LMdS}}N_{\text{LMdS}}^2)$ and the second operation is $\mathcal{O}(M_{\text{LMdS}}N^2)$. Since in general $N > N_{\text{LMdS}}$, LMdS has a computational complexity of $\mathcal{O}(M_{\text{LMdS}}N^2)$. The computational complexity of Grad-Desc is $\mathcal{O}(k_{\text{GD}}N)$, where k_{GD} is the total number of iterations. IAF-MMSE has a computational complexity of $\mathcal{O}(k_{\text{IAF}}N^2)$, where k_{IAF} is the total number of iterations required to achieve an MMSE less than θ (refer [11, Algorithm 3]). Thus, the computational complexity of LN-1, LN-1E, and Grad-Desc varies linearly with the number of anchor nodes in the network [refer Table III].



(a)

(b)

Fig. 12. Security performance of localization techniques under uncoordinated and coordinated attack [$\sigma = 2$ dB, $P = 10$, and target node at $(49, 49)$ m] (a) Security performance under uncoordinated attack with 25% of the anchor nodes being malicious. (b) Security performance under coordinated attack with 30% of the anchor nodes being malicious.

VII. Experimental Results

We conduct experiments in both indoor and outdoor environments to validate the performance of the proposed localization techniques under uncoordinated and coordinated attacks. We use the ATOM matrix [35], which is based on the ESP32-PICO-D4 controller, as the hardware platform for the wireless sensor nodes.

First, we experimentally estimate the path loss exponent (n), transmit power of the anchor nodes (p_0), and the noise standard deviation (σ) for the RSSI measurements in indoor

TABLE III

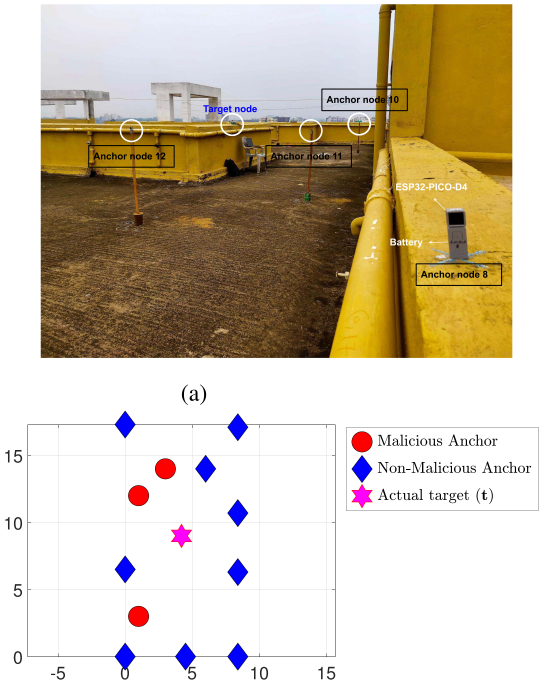
COMPUTATIONAL COMPLEXITY OF THE LOCALIZATION TECHNIQUES

LS	WLS	SWLS	LN-1	LN-1E	IAF-MMSE	Grad-Desc	LMdS
$\mathcal{O}\left(N^2\right)$		$\mathcal{O}\left(\lvert\mathcal{M}\rvert^2\right)$	$\mathcal{O}\left(k_{\text{ADMM}}N\right)$	$\mathcal{O}\left(\max\left(NTk_{\text{K-means}},k_{\text{ADMM}}N\right)\right)$	$\mathcal{O}\left(k_{\text{IAF}}N^2\right)$	$\mathcal{O}\left(k_{\text{GD}}N\right)$	$\mathcal{O}\left(M_{\text{LMdS}}N^2\right)$

TABLE IV

EXPERIMENTAL RESULTS IN TERMS OF THE AVERAGE RMS LOCALIZATION ERROR (IN m)

Technique	Uncoordinated attack								Coordinated attack							
	Indoor				Outdoor				Indoor				Outdoor			
	Attack strength: $\frac{\varepsilon_{\text{att}}}{\sqrt{3}}$ (dB)								Attack strength: $\lVert\mathbf{t}-\mathbf{t}_{\text{att}}\rVert_2$ (m)							
	0	4	10	12	0	4	10	12	0.28	0.85	1.46	2.02	2.00	4.00	5.39	8.25
LS	0.57	0.58	0.58	0.59	1.06	1.04	1.04	1.17	-							
IAF-MMSE	0.57	0.57	0.57	0.58	0.60	0.52	0.52	0.62	0.53	0.58	0.57	0.58	0.50	0.43	0.86	0.43
Grad-Desc	0.85	0.85	0.86	0.93	3.46	2.97	2.71	2.98	0.80	0.94	1.33	2.39	0.39	0.43	3.25	0.39
LMdS	0.98	0.81	0.96	0.89	*0.51*	*0.51*	*0.48*	0.61	0.56	0.55	1.55	2.05	0.46	0.41	*0.60*	0.48
WLS	**0.50**	**0.52**	0.52	*0.52*	0.64	0.65	0.70	0.85	0.60	0.49	0.52	0.50	1.09	2.00	0.99	*0.31*
SWLS	0.58	0.59	**0.42**	**0.43**	0.64	**0.38**	**0.19**	**0.21**	-							
LN-1	*0.55*	*0.54*	*0.51*	0.54	**0.46**	0.58	0.64	*0.59*	*0.31*	*0.47*	*0.33*	*0.30*	*0.35*	*0.34*	*0.60*	0.52
LN-1E	-								**0.28**	**0.37**	**0.29**	**0.27**	**0.34**	**0.43**	**0.43**	**0.29**



(a)

(b)

Fig. 13. Experimental setup and network topology. (a) Photograph of the outdoor experimental setup. (b) Network topology for the outdoor experiments.

and outdoor environments (refer to Table SIII of the Supplementary Material). A photograph of the outdoor experimental setup and the network topology are shown in Fig. 13. The hyperparameter values for all the techniques except SWLS are the same as mentioned in Section VI. The hyperparameter ζ in SWLS is empirically set to 3 and 6 for the indoor and outdoor network, respectively.

We repeat each experiment 50 times and the averaged results are presented in Table IV. In each experiment, the target node scans the network 10 times, i.e., $P = 10$. In Table IV, the best and the second-best results are shown in bold and italic, respectively. In terms of localization error, SWLS (for uncoordinated attack) and LN-1E (for coordinated attack) outperform the other techniques. In both attack types, their performance is closely followed by that of LN-1. In an uncoordinated attack, the performance of IAF-MMSE is close to that of LN-1 but it requires additional information in the form of σ and is computationally more expensive than LN-1. Further details about the experimental setup and performance analysis are provided in Section IV of the Supplementary Material.

VIII. CONCLUSION

We have presented four localization techniques, WLS, SWLS, LN-1, and LN-1E, that are robust in the presence of malicious anchor nodes in the network. Two types of attacks were considered: uncoordinated and coordinated. The proposed techniques were compared with the existing techniques IAF-MMSE, Grad-Desc, and LMdS. It was observed that SWLS outperformed the other techniques in uncoordinated attack scenarios with performance close to the CRLB in most cases. On the other hand, LN-1 is neither affected by an increase in the strength of the attack nor by the locations of the malicious anchor nodes. SWLS and LN-1E have better security performance compared with the other techniques under uncoordinated and coordinated attacks, respectively. Finally, LN-1 and LN-1E have computational complexity that varies linearly with the number of anchor nodes in the network.

APPENDIX A
DERIVATION OF VAR$(\overline{d_i};\omega_i,\sigma)$ AND VAR$(\overline{d_i}^2;\omega_i,\sigma)$

From (11), the probability density function of $\overline{d_i}$ is $f_{\overline{\mathrm{d}}_i}(x) \triangleq \frac{\lambda}{\sqrt{\pi}x}\exp\left(-\lambda^2\ln^2\left(\frac{x}{\omega_i}\right)\right)$ where

$\lambda = \frac{5\sqrt{2}n}{\ln(10)\sigma}$

$$\begin{aligned}\mathbb{E}\left[\overline{d_i}^h\right] &= \int_{-\infty}^{\infty} x^h f_{\mathrm{d}_i}(x)dx\\ &= \frac{\lambda}{\sqrt{\pi}}\int_{0^+}^{\infty} x^{h-1}\exp\left(-\lambda^2\ln^2\left(\frac{x}{\omega_i}\right)\right)dx. \end{aligned} \quad (33)$$

Substituting $p = \frac{x}{\omega_i}$ and $q = \ln(p)$ into (33), we get

$$\mathbb{E}\left[\overline{d_i}^h\right] = \frac{\lambda\omega_i^h}{\sqrt{\pi}}\exp\left(\frac{h^2}{4\lambda^2}\right)\int_{-\infty}^{+\infty}\exp\left(-\left(\lambda q - \frac{h}{2\lambda}\right)^2\right)dq. \quad (34)$$

Next, substituting $r = \lambda q - \frac{h}{2\lambda}$ into (34) gives

$$\mathbb{E}\left[\overline{d_i}^h\right] = \frac{\omega_i^h}{\sqrt{\pi}}\exp\left(\frac{h^2}{4\lambda^2}\right)\int_{-\infty}^{+\infty} e^{-r^2}dr = \omega_i^h\exp\left(\frac{h^2}{4\lambda^2}\right). \quad (35)$$

Using $\mathrm{Var}(\overline{d_i};\omega_i,\sigma) = \mathbb{E}[\overline{d_i}^2] - (\mathbb{E}[\overline{d_i}])^2$ and $\mathrm{Var}(\overline{d_i}^2;\omega_i,\sigma) = \mathbb{E}[\overline{d_i}^4] - (\mathbb{E}[\overline{d_i}^2])^2$, the expressions given in (12) and (13) can be obtained.

Appendix B
Closed-Form Expression for $\hat{\sigma}_{\mathrm{EST}}$

Let $l(\sigma_{\mathrm{est}}) \triangleq \upsilon - \mathrm{Var}(\overline{d_i};\omega_i,\sigma_{\mathrm{est}})$, where $\upsilon = \mathrm{SVar}(d_{i1}, d_{i2}, \ldots, d_{iP})$. It can be shown that

$$\frac{\partial^2\mathrm{Var}\left(\overline{d_i};\omega_i,\sigma_{\mathrm{est}}\right)}{\partial\sigma_{\mathrm{est}}^2} = \underbrace{\frac{2\overline{d_i}^2}{18.86n^2}\exp\left(\frac{\sigma_{\mathrm{est}}^2}{18.86n^2}\right)}_{k_1} \times\left[\underbrace{2\exp\left(\frac{\sigma_{\mathrm{est}}^2}{18.86n^2}\right)}_{k_2}\underbrace{\left(1+\frac{4\sigma_{\mathrm{est}}^2}{18.86n^2}\right)}_{k_3} - \underbrace{\left(1+\frac{2\sigma_{\mathrm{est}}^2}{18.86n^2}\right)}_{k_4}\right] \quad (36)$$

where $(k_2k_3 - k_4)$ is positive because $k_3 \geq k_4$ and $k_2 \geq 2$. Therefore, $\frac{\partial^2\mathrm{Var}(\overline{d_i};\omega_i,\sigma_{\mathrm{est}})}{\partial\sigma_{\mathrm{est}}^2} \geq 0$ and $\mathrm{Var}(\overline{d_i};\omega_i,\sigma_{\mathrm{est}})$ is a convex function. Therefore, $l(\sigma_{\mathrm{est}})$ is a concave function.

Remark 1: If function $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}$ is even, concave, $f(x = 0) \geq 0$, and $\exists\xi(\geq 0)$ such that $f(x) \leq \xi$, then $x^* = \underset{x\geq 0}{\arg\min}|f(x)| \implies f(x^*) = 0$.

Using the above-mentioned remark, optimal value ($\hat{\sigma}_{\mathrm{est}}$) can be obtained by solving $l(\hat{\sigma}_{\mathrm{est}}) = 0$ as $l(\sigma_{\mathrm{est}})$ is concave, even function with $l(\sigma_{\mathrm{est}} = 0) = \upsilon$ as $\mathrm{Var}(\overline{d_i};\omega_i,\sigma_{\mathrm{est}} = 0) = 0$ and is upper bounded by a nonnegative constant ($l(\sigma_{\mathrm{est}}) \leq \upsilon$, as $\mathrm{Var}(\overline{d_i};\omega_i,\sigma_{\mathrm{est}}) \geq 0$). The objective function of the optimization problem under consideration, i.e., $|l(\sigma_{\mathrm{est}})|$ is neither convex nor concave when $\sigma_{\mathrm{est}} \geq 0$, $|l(\sigma_{\mathrm{est}})|$ is concave when $\sigma_{\mathrm{est}} \in [0, \hat{\sigma}_{\mathrm{est}}]$, and convex when $\sigma_{\mathrm{est}} \in [\hat{\sigma}_{\mathrm{est}}, \infty)$.

Appendix C
Regularity Condition of $p(\mathbf{P}^{\mathrm{R}};\mathbf{t})$ for Uncoordinated Attack

From (27), the log-likelihood of $p(\mathbf{P}^{\mathrm{r}};\mathbf{t})$ is given as

$$\begin{aligned}&\ln(p(\mathbf{P}^{\mathrm{r}};\mathbf{t}))\\ &= -\frac{P|\mathcal{A}_{\mathrm{nm}}|\ln\left(2\pi\sigma^2\right)}{2} - P|\mathcal{A}_{\mathrm{m}}|\ln(4\epsilon_{\mathrm{att}})\\ &\quad - \sum_{j=1}^{P}\sum_{i\in\mathcal{A}_{\mathrm{nm}}}\frac{\left(p_{ij}^r - p_0 + 10n\log_{10}(d_i)\right)^2}{2\sigma^2}\\ &\quad + \sum_{j=1}^{P}\sum_{k\in\mathcal{A}_{\mathrm{m}}}\ln\left[\mathrm{erf}\left(\frac{p_{kj}^r - \Delta_1^k}{\sqrt{2}\sigma}\right) - \mathrm{erf}\left(\frac{p_{kj}^r - \Delta_2^k}{\sqrt{2}\sigma}\right)\right]. \end{aligned} \quad (37)$$

Differentiating (37) with respect to t^x, we get (38), as shown at the top of the next page.

Remark 2: $\mathbb{E}[p_{ij}^r] = p_0 - 10n\log_{10}(d_i)$, $i \in \mathcal{A}_{\mathrm{nm}}$ [refer (2)].

Remark 3: For $k \in \mathcal{A}_{\mathrm{m}}$, we have

$$\int_{-\infty}^{\infty}\left[\exp\left[\frac{-\left(p_{kj}^r - \Delta_1^k\right)^2}{2\sigma^2}\right] - \exp\left[\frac{-\left(p_{kj}^r - \Delta_2^k\right)^2}{2\sigma^2}\right]\right]dp_{kj}^r = 0. \quad (39)$$

Using (38), Remark 2, and Remark 3, we obtain the regularity condition of $p(\mathbf{P}^{\mathrm{r}};\mathbf{t})$ for all values of t^x

$$\begin{aligned}&\mathbb{E}\left[\frac{\partial\ln(p(\mathbf{P}^{\mathrm{r}};\mathbf{t}))}{\partial t^x}\right]\\ &= \sum_{j=1}^{P}\left[\sum_{i\in\mathcal{A}_{\mathrm{nm}}}\int_{-\infty}^{\infty}\frac{\partial\ln\left(p\left(P_{ij}^r;\mathbf{t}\right)\right)}{\partial t^x}p\left(P_{ij}^r;\mathbf{t}\right)dP_{ij}^r\right.\\ &\quad\left. + \sum_{k\in\mathcal{A}_{\mathrm{m}}}\int_{-\infty}^{\infty}\frac{\partial\ln\left(p\left(P_{kj}^r;\mathbf{t}\right)\right)}{\partial t^x}p\left(P_{kj}^r;\mathbf{t}\right)dP_{kj}^r\right] = 0. \end{aligned} \quad (40)$$

Similarly, we can obtain the regularity condition of $p(\mathbf{P}^{\mathrm{r}};\mathbf{t})$ for all values of t^y.

Appendix D
Derivation of FIM for Uncoordinated Attack

Individual elements of the Fisher information matrix for uncoordinated attack (28a) are expressed as $f_{xx}^{\mathrm{uc}} = -\mathbb{E}\left[\frac{\partial^2\ln(p(\mathbf{P}^{\mathrm{r}};\mathbf{t}))}{\partial t^{x^2}}\right]$, $f_{yy}^{\mathrm{uc}} = -\mathbb{E}\left[\frac{\partial^2\ln(p(\mathbf{P}^{\mathrm{r}};\mathbf{t}))}{\partial t^{y^2}}\right]$, and $f_{yx}^{\mathrm{uc}} = f_{xy}^{\mathrm{uc}} = -\mathbb{E}\left[\frac{\partial^2\ln(p(\mathbf{P}^{\mathrm{r}};\mathbf{t}))}{\partial t^x t^y}\right]$.

Remark 4: For $k \in \mathcal{A}_{\mathrm{m}}$, we have

$$\int_{-\infty}^{\infty}\left[\left(p_{kj}^r - \Delta_1^k\right)\exp\left(\frac{-\left(p_{kj}^r - \Delta_1^k\right)^2}{2\sigma^2}\right) - \left(p_{kj}^r - \Delta_2^k\right)\exp\left(\frac{-\left(p_{kj}^r - \Delta_2^k\right)^2}{2\sigma^2}\right)\right]dp_{kj}^r = 0. \quad (42)$$

$$\frac{\partial \ln(p(\mathbf{P}^{\mathrm{r}};\mathbf{t}))}{\partial t^x} = \frac{-10n}{\ln(10)} \sum_{j=1}^{P} \left[\sum_{i\in\mathcal{A}_{\mathrm{nm}}} \frac{\left(t^x - a_i^x\right)\left(p_{ij}^r - p_0 + 10n\log_{10}(d_i)\right)}{d_i^2\sigma^2} - \frac{\sqrt{2}}{\sqrt{\pi}\sigma} \sum_{k\in\mathcal{A}_{\mathrm{m}}} \frac{\left(a_k^x - t^x\right)\left[\exp\left[\frac{-\left(p_{kj}^r-\Delta_1^k\right)^2}{2\sigma^2}\right] - \exp\left[\frac{-\left(p_{kj}^r-\Delta_2^k\right)^2}{2\sigma^2}\right]\right]}{d_k^2\left[\operatorname{erf}\left(\frac{p_{kj}^r-\Delta_1^k}{\sqrt{2}\sigma}\right) - \operatorname{erf}\left(\frac{p_{kj}^r-\Delta_2^k}{\sqrt{2}\sigma}\right)\right]} \right]. \tag{38}$$

$$\begin{aligned} \frac{\partial^2 \ln(p(\mathbf{P}^{\mathrm{r}};\mathbf{t}))}{\partial t^{x2}} = {} & \frac{-10n}{\ln(10)\sigma^2} \sum_{j=1}^{P} \sum_{i\in\mathcal{A}_{\mathrm{nm}}} \left[\frac{\left(p_{ij}^r - p_0 + 10\log_{10}(d_i)\right)}{d_i^2} + \frac{10n\left(t^x - a_i^x\right)^2}{\ln(10)d_i^4} \right] \\ & - \frac{10\sqrt{2}n}{\sqrt{\pi}\ln(10)\sigma} \sum_{j=1}^{P} \sum_{k\in\mathcal{A}_{\mathrm{m}}} \Bigg[\frac{2\left(t^x - a_k^x\right)^2 - d_k^2}{d_k^4} \frac{\exp\left(\frac{-\left(p_{kj}^r-\Delta_1^k\right)^2}{2\sigma^2}\right) - \exp\left(\frac{-\left(p_{kj}^r-\Delta_2^k\right)^2}{2\sigma^2}\right)}{\operatorname{erf}\left(\frac{p_{kj}^r-\Delta_1^k}{\sqrt{2}\sigma}\right) - \operatorname{erf}\left(\frac{p_{kj}^r-\Delta_2^k}{\sqrt{2}\sigma}\right)} \\ & + \frac{10n\left(t^x - a_k^x\right)^2}{\ln(10)\sigma^2 d_k^4} \times \frac{\left(p_{kj}^r - \Delta_1^k\right)\exp\left(\frac{-\left(p_{kj}^r-\Delta_1^k\right)^2}{2\sigma^2}\right) - \left(p_{kj}^r - \Delta_2^k\right)\exp\left(\frac{-\left(p_{kj}^r-\Delta_2^k\right)^2}{2\sigma^2}\right)}{\operatorname{erf}\left(\frac{p_{kj}^r-\Delta_1^k}{\sqrt{2}\sigma}\right) - \operatorname{erf}\left(\frac{p_{kj}^r-\Delta_2^k}{\sqrt{2}\sigma}\right)} \\ & + \frac{10\sqrt{2}n\left(t^x - a_k^x\right)^2}{\sqrt{\pi}\ln(10)\sigma d_k^4} \left(\frac{\exp\left(\frac{-\left(p_{kj}^r-\Delta_1^k\right)^2}{2\sigma^2}\right) - \exp\left(\frac{-\left(p_{kj}^r-\Delta_2^k\right)^2}{2\sigma^2}\right)}{\operatorname{erf}\left(\frac{p_{kj}^r-\Delta_1^k}{\sqrt{2}\sigma}\right) - \operatorname{erf}\left(\frac{p_{kj}^r-\Delta_2^k}{\sqrt{2}\sigma}\right)} \right)^2 \Bigg]. \end{aligned} \tag{41}$$

f_{xx}^{uc} is calculated using (41), as shown at the top of the page and Remarks 2–4. In a similar manner, f_{yy}^{uc} and f_{xy}^{uc} can be obtained.

ACKNOWLEDGMENT

The authors would like to thank Mr. Kartick Patar for his help with the experimental setup which enabled us to experimentally validate the proposed algorithms.

REFERENCES

[1] Y.-C. Wang and G.-W. Chen, "Efficient data gathering and estimation for metropolitan air quality monitoring by using vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7234–7248, Aug. 2017.

[2] C. Costa, F. Antonucci, F. Pallottino, J. Aguzzi, D. Sarriá, and P. Menesatti, "A review on agri-food supply chain traceability by means of RFID technology," *Food Bioprocess Technol.*, vol. 6, no. 2, pp. 353–366, Feb. 2013.

[3] P. Sikka, P. Corke, P. Valencia, C. Crossman, D. Swain, and G. Bishop-Hurley, "Wireless ad hoc sensor and actuator networks on the farm," in *Proc. 5th Int. Conf. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2006, pp. 492–499.

[4] Y. Wang, Z. Liu, D. Wang, Y. Li, and J. Yan, "Anomaly detection and visual perception for landslide monitoring based on a heterogeneous sensor network," *IEEE Sensors J.*, vol. 17, no. 13, pp. 4248–4257, Jul. 2017.

[5] Z. Gao, Y. Gao, S. Wang, D. Li, and Y. Xu, "CRISLoc: Reconstructable CSI fingerprinting for indoor smartphone localization," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3422–3437, Mar. 2021.

[6] S. Srirangarajan and D. Pesch, "Source localization using graph-based optimization technique," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 1127–1132.

[7] J. Jiang, G. Wang, and K. C. Ho, "Sensor network-based rigid body localization via semi-definite relaxation using arrival time and Doppler measurements," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1011–1025, Feb. 2019.

[8] E. Schmidt, M. A. Mohammed, and D. Akopian, "A performance study of a fast-rate WLAN fingerprint measurement collection method," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 10, pp. 2273–2281, Oct. 2018.

[9] S. Srirangarajan, A. H. Tewfik, and Z. Q. Luo, "Distributed sensor network localization using SOCP relaxation," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4886–4895, Dec. 2008.

[10] R. Stoleru, T. He, and J. A. Stankovic, "Range-free localization," in *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*. Boston, MA, USA: Springer, 2007, pp. 3–31.

[11] J. Won and E. Bertino, "Robust sensor localization against known sensor position attacks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 12, pp. 2954–2967, Dec. 2019.

[12] 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, Apr. 2012.

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

[14] A. I. G.-T. Ferreres, B. R. Alvarez, and A. R. Garnacho, "Guaranteeing the authenticity of location information," *IEEE Pervas. Comput.*, vol. 7, no. 3, pp. 72–80, Jul. 2008.

[15] D. Liu, P. Ning, A. Liu, C. Wang, and W. K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 4, pp. 22:1–22:39, Jul. 2008.

[16] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, "Robust range-based secure localization in wireless sensor networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[17] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.

[18] V. Bianchi, P. Ciampolini, and I. De Munari, "RSSI-based indoor localization and identification for ZigBee wireless sensor networks in smart homes," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 2, pp. 566–575, Feb. 2019.

[19] R. M. Vaghefi, M. R. Gholami, R. M. Buehrer, and E. G. Ström, "Cooperative received signal strength-based sensor localization with unknown transmit powers," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1389–1403, Mar. 2013.

[20] 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, Feb. 2021.

[21] X. Mei, H. Wu, J. Xian, B. Chen, H. Zhang, and X. Liu, "A robust, non-cooperative localization algorithm in the presence of outlier measurements in ocean sensor networks," *Sensors*, vol. 19, no. 12, p. 2708, Jun. 2019.

[22] S. Jha, S. Tripakis, S. A. Seshia, and K. Chatterjee, "Game theoretic secure localization in wireless sensor networks," in *Proc. Int. Conf. Internet Things (IOT)*, Oct. 2014, pp. 85–90.

[23] R. Garg, A. L. Varna, and M. Wu, "Gradient descent approach for secure localization in resource constrained wireless sensor networks," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2010, pp. 1854–1857.

[24] S. M. Kay, *Fundamentals of Statistical Signal Processing*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[25] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[26] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Found. Trends Mach. Learn.*, vol. 3, no. 1, pp. 1–122, Jan. 2011.

[27] D. Han and X. Yuan, "A note on the alternating direction method of multipliers," *J. Optim. Theory Appl.*, vol. 155, no. 1, pp. 227–238, Oct. 2012.

[28] N. Parikh and S. Boyd, "Proximal algorithms," *Found. Trends Optim.*, vol. 1, no. 3, pp. 127–239, Jan. 2014.

[29] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer-Verlag, 2006.

[30] S. Cao, X. Chen, X. Zhang, and X. Chen, "Combined weighted method for TDOA-based localization," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 5, pp. 1962–1971, May 2020.

[31] X. Zhang and J. G. Andrews, "Downlink cellular network analysis with multi-slope path loss models," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1881–1894, May 2015.

[32] C. Broyden and W. Murray, "Quasi-Newton methods," in *Numerical Methods for Unconstrained Optimization*, vol. 972, W. Murray, Ed. New York, NY, USA: Academic, 1970.

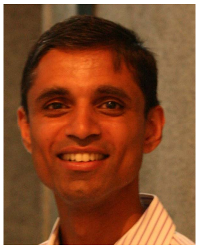
[33] K. Yu and Y. J. Guo, "NLOS error mitigation for mobile location estimation in wireless networks," in *Proc. IEEE 65th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2007, pp. 1071–1075.

[34] P. I. Dalatu, "Time complexity of k-means and k-medians clustering algorithms in outliers detection," *Global J. Pure Appl. Math.*, vol. 12, no. 5, pp. 4405–4418, 2016.

[35] *ATOM Matrix ESP32 Development Kit*. Accessed: May 30, 2021. [Online]. Available: https://shop.m5stack.com/products/atom-matrix-esp32-development-kit

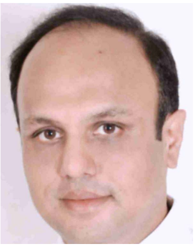
Bodhibrata Mukhopadhyay (Graduate Student Member, IEEE) received the M.S. (Research) degree in communication from IIT Delhi, New Delhi, India, in 2015, where he is currently pursuing the Ph.D. degree with the Department of Electrical Engineering.

Since 2017, he has been the Director of Suxma Systems, New Delhi—an IIT Delhi incubated startup, which is involved in developing intelligent IoT-based cyber-physical systems. He is involved in the area of cooperative and noncooperative localization techniques using nonlinear programming. His research interests include designing intelligent embedded systems and broad areas of signal processing and wireless communications, with a focus on sensor localization.



Seshan Srirangarajan (Member, IEEE) received the B.E. degree from the University of Mumbai, Mumbai, India, in 2001, and the M.S. and Ph.D. degrees from the University of Minnesota, Minneapolis, MN, USA, in 2005 and 2008, respectively, all in electrical engineering.

From 2005 to 2006, he was an Intern with the Wireless Technologies Group, Honeywell Technology Center, Minneapolis, MN, USA. From 2008 to 2011, he was a Research Fellow with the Intelligent Systems Center, Nanyang Technological University, Singapore. From 2011 to 2014, he was an IRCSET/Intel Post-Doctoral Fellow with the Nimbus Centre for Embedded Systems Research, Cork Institute of Technology, Cork, Ireland. He is currently an Assistant Professor with the Department of Electrical Engineering, IIT Delhi, New Delhi, India. His research interests span the broad areas of signal processing and wireless communications with a focus on positioning in wireless networks, sensor networks, compressed sensing, and array signal processing.



Subrat Kar (Senior Member, IEEE) received the B.E. degree (Hons.) in electrical and electronics engineering from the Birla Institute of Technology and Science, Pilani, Pilani, India, in 1987, and the Ph.D. degree in electrical communication engineering from the Indian Institute of Science, Bengaluru, India, in 1991.

He was a Post-Doctoral Fellow with the International Center for Theoretical Physics, Trieste, Italy, from 1991 to 1994. In 1994, he joined IIT Delhi, New Delhi, India, where he is currently a Professor with the Department of Electrical Engineering, and holds the Ram and Sita Sabnani Chair Professorship. He is one of the co-founders of Suxma Systems, New Delhi—a startup, which is involved in developing intelligent IoT-based cyber-physical systems. His research areas are in optical communication, switching, access technologies, telecom protocols, embedded systems, and high-speed networks.