



OPEN ACCESS

EDITED BY

Carlos Cambra,
University of Burgos, Spain

REVIEWED BY

Ahmad Bazzi,
New York University Abu Dhabi, United Arab
Emirates

Mohamed Saban,
University of Burgos, Spain

*CORRESPONDENCE

Slavisa Tomic,
✉ slavisa.tomic@ulusofona.pt

RECEIVED 22 October 2025

REVISED 24 December 2025

ACCEPTED 05 January 2026

PUBLISHED 28 January 2026

CITATION

Tomic S, Beko M, Vukobratovic D and Krco S
(2026) Voting mechanism for trustworthy
localization in wireless sensor networks.
Front. Sens. 7:1730414.
doi: 10.3389/fsens.2026.1730414

COPYRIGHT

© 2026 Tomic, Beko, Vukobratovic and Krco.
This is an open-access article distributed under
the terms of the [Creative Commons Attribution
License \(CC BY\)](https://creativecommons.org/licenses/by/4.0/). The use, distribution or
reproduction in other forums is permitted,
provided the original author(s) and the copyright
owner(s) are credited and that the original
publication in this journal is cited, in accordance
with accepted academic practice. No use,
distribution or reproduction is permitted which
does not comply with these terms.

Voting mechanism for trustworthy localization in wireless sensor networks

Slavisa Tomic^{1,2*}, Marko Beko^{1,3}, Dejan Vukobratovic⁴ and Srdjan Krco⁵

¹COPELABS, ECATI, Lusófona University, Lisbon, Portugal, ²UNINOVA-CTS - Center of Technology and Systems, NOVA School of Science and Technology, Caparica, Portugal, ³Instituto de Telecomunicações, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal, ⁴Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia, ⁵DunavNET, Novi Sad, Serbia

This work aspires to provide a trustworthy solution for target localization in adverse environments, where malicious nodes, capable of manipulating distance measurements (i.e., performing spoofing attacks), are present, thus hindering accurate localization. Besides localization, its other goal is to identify (detect) which of the nodes participating in the process are malicious. This problem becomes extremely important with the forthcoming expansion of IoT and smart cities applications, that depend on accurate localization, and the presence of malicious attackers can represent serious security threats if not taken into consideration. This is the case with most existing localization systems which makes them highly vulnerable to spoofing attacks. In addition, existing methods that are intended for adversarial settings consider very specific settings or require additional knowledge about the system model, making them only partially secure. Therefore, this work proposes a novel voting scheme based on clustering and weighted central mass to securely solve the localization problem and detect attackers. The proposed solution has two main phases: 1) Choosing a cluster of suitable points of interest by taking advantage of the problem geometry to assigning votes in order to localize the target, and 2) Attacker detection by exploiting the location estimate and basic statistics. The proposed method is assessed in terms of localization accuracy, success in attacker detection, and computational complexity in different settings. Computer simulations and real-world experiments corroborate the effectiveness of the proposed scheme compared to state-of-the-art methods, showing that it can accomplish an error reduction of 30% and is capable of achieving almost perfect attacker detection rate when the ratio between attacker intensity and noise standard deviation is significant.

KEYWORDS

clustering, received signal strength (RSS), secure localization, spoofing attacks, voting scheme (VS), weighted central mass (WCM)

1 Introduction

Recently, wireless sensor networks (WSNs) have attracted much interest of the scientific community, partially due to their ability to work in harsh environments, ease and low costs of implementation (Tomic et al., 2018; Matos-Carvalho et al., 2021), and wide variety of applications (Oigbochie et al., 2021; Qiang, 2014). From the localization perspective, generally, WSNs are composed of two distinct types of nodes: 1) anchor nodes, whose

locations are known and serve as reference points in the localization process and 2) target nodes, whose locations are unknown and one desires to determine them. Naturally, it is expected that nodes are capable to communicate with each other in order to execute the localization task. In this work, a non-cooperative network, where targets are only allowed to communicate with anchors, is considered.

In most applications, data acquired by sensors are only useful if they can be associated with the respective physical location (Bazzi et al., 2016a, Shi, 2024). However, most existing localization systems overlook possible security threats (Tomic and Beko, 2020; Coluccia and Fascista, 2018, Bazzi et al., 2016b, Bazzi et al., 2018). Therefore, if these systems are exposed to malicious attacks, they can result in catastrophic outcomes (e.g., failure in a self-driving car collision system, change in drone trajectory, etc.). Mainly for this reason, localization systems should be developed for potentially adversarial environments, where a malicious (or damaged) sensor can produce false distance measurements (spoofing attacks) to manipulate the localization process.

Perhaps the easiest and most common way of localization is to equip sensors with global positioning system (GPS) receivers. However, this solution has several undesirable consequences, such as increased implementation costs and infeasibility in some environments (e.g., indoor, urban areas, forests, etc.). In addition, from the security point of view, GPS is considered a civilian localization system (e.g., uses unencrypted signals); thus, it is not very difficult to manipulate (spoof) it. Although there are different types of attacks in WSNs nowadays, this work focuses its attention on spoofing attacks specifically due to their close relationship with distance measurements (proximity). These attacks include forging distance measurements (either by reducing or enlarging them) that can be performed in various non-cryptographic ways, meaning that no infraction of upper-layer security protocols for carrying out these attacks is at risk (for instance, an attacker can add a physical obstacle between two nodes or change node's transmit power without informing its neighbours). Moreover, these attacks (including GPS spoofing) come at a relatively low cost, but can cause severe problems in many systems (Kugler, 2017). Since spoofing attacks are closely related with distance they have real-world impact and are used in car thefts, executions of unauthorized payments and manipulation of navigation (Singh et al., 2019).

1.1 Related work

Secure localization in WSNs has attracted interest in the scientific literature (Li et al., 2005; Liu et al., 2007; Garg et al., 2012; Liu et al., 2019; Li et al., 2021; Beko and Tomic, 2021; Tomic and Beko, 2022; Mukhopadhyay et al., 2021; Tomic and Beko, 2024a; Tomic and Beko, 2024b). Still, there is no uniquely accepted solution and there is room for improvement in all aspects (localization accuracy, detection rates and complexity).

In Li et al. (2005), two secure localization solutions were explored: least median of squares (LMS) and radio frequency (RF) fingerprinting. LMS selects the subset of anchors with the least median residues, while RF fingerprinting employs a median-based distance metric. The work in Liu et al. (2007) introduced attack-resistant minimum mean square estimation

(ARMMSE) and a voting scheme (VS). ARMMSE detects and removes malicious anchors based on inconsistencies, whereas VS assigns votes to grid cells based on distance measurements, identifying the target's likely location. An iterative algorithm using gradient descent was proposed in Garg et al. (2012) for both uncoordinated and coordinated attacks. Malicious anchors were identified by their higher residues and excluded from the localization process. In Liu et al. (2019), a density-based spatial clustering method classified location points as normal or abnormal, followed by a sequential probability ratio test to authenticate anchors using received signal strength (RSS) and time of arrival (TOA) data. The study in Li et al. (2021) addressed secure localization and velocity estimation in mobile WSNs with malicious anchors, using a maximum *a posteriori* (MAP) estimator solved via variational message passing. In Beko and Tomic (2021), an initial location estimate was obtained via weighted central mass (WCM), followed by distance-based filtering and a generalized trust region sub-problem (GTRS) solved using a bisection method. This was extended in Tomic and Beko (2022) to a general range-based scenario using a generalized likelihood ratio test (GLRT) and law of cosines (LC). The work in Mukhopadhyay et al. (2021) proposed secure weighted least squares (SWLS) for uncoordinated spoofing attacks and l_1 -norm (LN-1E) for coordinated attacks. SWLS filters malicious nodes based on estimated noise standard deviation, while LN-1E uses 3D plane fitting and K-means clustering to separate malicious anchors. In Tomic and Beko (2024a), a robust min-max approach was formulated as a second-order cone programming (R-SOCP) problem and a robust GTRS (R-GTRS). Lastly, Tomic and Beko (2024b) introduced an alternating direction method of multipliers (ADMM) approach, applying a weighted least squares criterion within a decomposition-coordination iterative scheme.

Even though the methods in Li et al. (2005), Tomic and Beko (2024b) work well in the settings under scrutiny in the respective works, they either require additional knowledge on certain parameters, such as noise power or the maximum magnitude of an attack (e.g., Liu et al., 2007, Liu et al., 2019, Li et al., 2021, Mukhopadhyay et al., 2021, Tomic and Beko, 2024a) and/or convex relaxations/approximations that expand the set of possible solution leading to higher error (e.g., Li et al., 2005, Li et al., 2021, Tomic and Beko, 2024a) or are executed iteratively (e.g., Garg et al., 2012, Tomic and Beko, 2024b), leaving room for improvement in all aspects (localization accuracy, detection rates and complexity). These limitations could severely deteriorate their performance in scenarios where the required parameters are unknown or imperfectly known, i.e., where problem assumptions do not hold, resulting in the applied relaxations/approximations not being sufficiently tight or lead to burdensome computations that might even raise convergence issues. Furthermore, the majority of the existing works assume knowledge about the type of spoofing attacks (uncoordinated or coordinated) under which the network is beforehand and develop a solution for that specific type of attack. However, it is not possible to acquire such knowledge in practice. Therefore, there are still some challenges to address and room for improvement in all main aspects of the considered problem.

1.2 Main contributions of the current work

This work presents a geometric approach to compute intersection points between pairs of anchors and obtain an estimate of the target's location through a VS and WCM, which is then exploited to detect attackers based on confidence intervals (CIs). Unlike (Liu et al. (2007), Garg et al. (2012), Beko and Tomic (2021), Tomic and Beko (2022), Mukhopadhyay et al. (2021)), the proposed algorithm does not make hard (binary) detection decisions, but assigns beliefs (votes) to each intersection point, leveraging information from malicious anchors when attack intensity is low. Besides, mistakenly removing a genuine anchor can severely degrade the localization accuracy, leading to severe and potentially lethal consequences in real life, such as collisions of autonomous vehicles with obstacles, another vehicles or infrastructure, tardy arrival at the desired location in the case of an emergency event, like wildfire and organ transplantation and similar. The highest-voted points are converted into probabilities and used as WCM weights for location estimation. Attack intensities are assessed per link using a maximum likelihood (ML) criterion, with attacker detection based on CIs at a predefined level. Due to its geometric nature, the method is adaptable to any range-based measurement. The primary goal is to advance secure localization beyond traditional systems, ensuring reliable malicious node detection and accurate target positioning. The main contributions of this work are threefold and are summarized in the following.

- Design of a novel solution for target localization in randomly deployed sensor network in the presence of (uncoordinated and coordinated) spoofing attacks based on a new VS. The proposed localization estimator is a single-iteration scheme based on simple geometry, where points of interest extracted from the system model are clustered together and appraised by assigning votes to reach a set of the most trustworthy points. This set of points is then used to get an estimate on the target's location through WCM.
- Unlike the existing methods that make a *hard* binary decision, the current work converts votes into probabilities and makes a *soft* detection decision, i.e., it makes use of all anchors and gradually builds its confidence regarding which anchors might be malicious and which not, not excluding any anchor in the process.
- Proposal of a novel attacker detection scheme based on CIs. By exploiting the location estimate, estimates of the attack intensities and the genuine (non-malicious) measurement values are acquired and used to evaluate if a reported measurement falls outside a CI of one (estimated) standard deviation from its *genuine* doublet.
- The proposed solution not only matches, but outperforms more complex state-of-the-art solutions for high attack intensities. Thus, the proposed method sets the best achievable results reported in the literature thus far, both in terms of localization and detection performance.
- Lastly, both computer simulations and real-world experimental measurements are employed to validate the performance of the proposed solution.

Throughout the work, uppercase bold type, lowercase bold type, and regular type of fonts are used to denote matrices,

vectors, and scalars, respectively. \mathbb{R}^n denotes the n -dimensional real Euclidean space. Symbol $(\bullet)^T$ represent the transpose operator, while $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ and $proj_S(\mathbf{p})$ denote the binomial coefficients and the projection of the point \mathbf{p} onto the set S , respectively. The normal (Gaussian) distribution with mean μ and variance σ^2 is denoted by $\mathcal{N}(\mu, \sigma^2)$. The N -dimensional identity matrix is denoted by I_N and the $M \times N$ matrix of all zeros by $\mathbf{0}_{M \times N}$ (if no ambiguity can occur, subscripts are omitted). $\|\mathbf{x}\|$ denotes the vector norm defined by $\|\mathbf{x}\| = \sqrt{\mathbf{x}^T \mathbf{x}}$, where $\mathbf{x} \in \mathbb{R}^n$ is a column vector. The i -th column of the matrix \mathbf{M} is denoted by \mathbf{M}_i and an estimate of a parameter \mathbf{x} with $\hat{\mathbf{x}}$.

The rest of this paper is structured as follows: Section 2 defines the problem, while Section 3 details the proposed solution. Section 4 presents performance comparisons, and Section 5 summarizes the key findings.

2 Problem formulation

Let us consider a 2-dimensional, non-cooperative and static WSN, where a single target, whose true location is unknown and denoted by \mathbf{x} , is located at a time by the help of a set of anchors whose true locations are known and denoted by \mathbf{a}_i , $i = 1, \dots, N$. Some of the anchors are assumed malicious and try to disrupt the location process by manipulating their distance measurements (spoofing attacks). The target receives radio signals (from which it measures the RSS values) from the anchors. Note that in this work the measurement acquisition is assumed practically instantaneous; thus, ambient conditions do not change significantly during the measurement process, having very little to no impact on the deviation of the RSS measurements. This work considers two types of spoofing attacks: coordinated and uncoordinated.

2.1 Uncoordinated attack

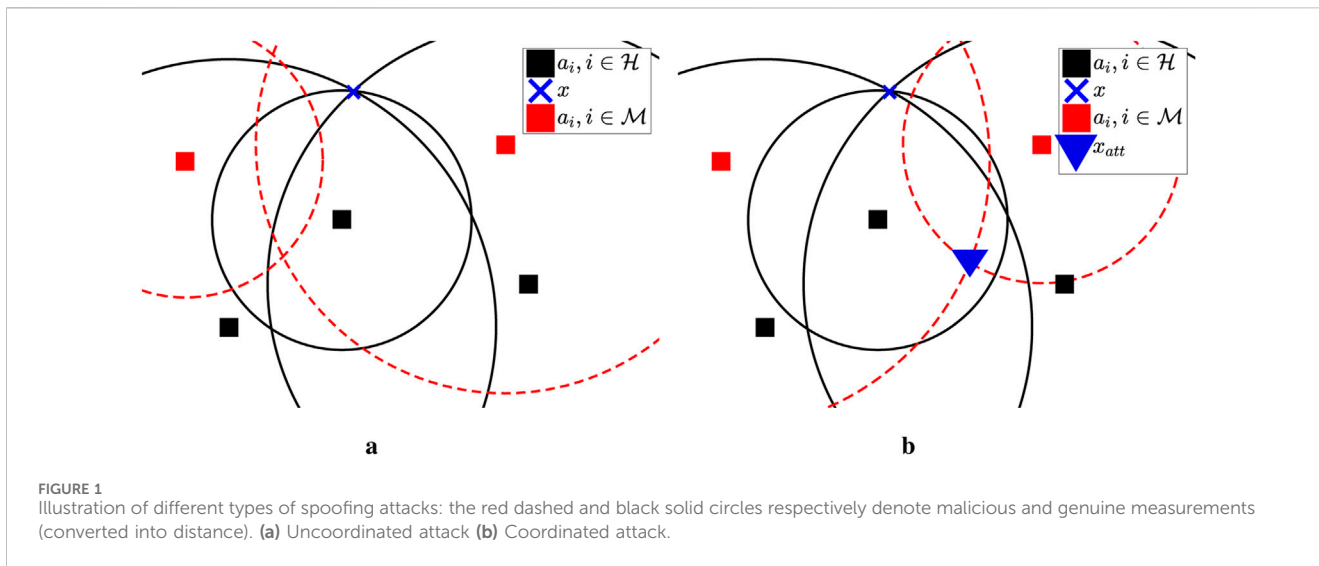
In this setting, the genuine anchors have a predefined transmitted power, while the malicious anchors change the transmitted power arbitrarily without notifying the network. The k -th RSS measurement sample ($k = 1, \dots, K$) between the target and the i -th anchor can be modeled as

$$P_{i,k} = P_0 - 10\gamma \log_{10} \frac{\|\mathbf{x} - \mathbf{a}_i\|}{d_0} + \delta_i + n_{i,k} \quad (1)$$

where

$$\delta_i = \begin{cases} 0, & i \in \mathcal{H} \\ \delta, & i \in \mathcal{M} \end{cases}$$

and \mathcal{M} and \mathcal{H} are, respectively, the set of malicious and honest nodes, P_0 is the RSS at a short reference distance d_0 (for simplicity referred to as the transmitted power), γ is the path loss exponent (PLE) representing the decay of the signal strength with distance, $n_{i,k}$ is the noise term modeled as $n_{i,k} \sim \mathcal{N}(0, \sigma_{i,k}^2)$, and $\delta_i \in \mathbb{R}$ is the intensity of the spoofing attack of the i -th anchor. Note that in this work the measurement acquisition is assumed practically instantaneous; thus, ambient conditions do not change significantly during the measurement process, having very little to no impact on the deviation of the RSS measurements.



Note that, in contrast to Beko and Tomic (2021), where malicious anchors could only enlarge their distance measurements, in this work it is assumed that the attackers can either reduce or enlarge distance measurements. For simplicity, it is assumed that the variance of all measurements is equal (for every link and sample), i.e., for $\sigma_{i,k}^2 = \sigma^2$, $i = 1, \dots, N$ and $k = 1, \dots, K$. Moreover, to easier combat outliers and also for the sake of notation simplicity and without loss of generality, the median of all K RSS measurements in (Equation 1) from the i -th anchor (P_i) is used in the following derivations.

Figure 1a shows an uncoordinated attack, where two (represented by red squares) of the five anchors are malicious and report, independently, false distance measurements, aggravating the localization process. In the concrete case, both malicious anchors reduced their measurements independently from each other, resulting in two intersection points of the red dashed circles to be relatively remote from the main cluster of the intersection points and thus, from the true target location.

2.2 Coordinated attack

In coordinated attacks the malicious anchors communicate with each other to agree on a (false) location for the target. The idea is to make the network believe that the target is at a different location than it actually is. Similar to Mukhopadhyay et al. (2021), the coordinated attack can be modeled as

$$P_{i,k} = \begin{cases} P_0 - 10\gamma \log_{10} \left(\frac{\|\mathbf{x} - \mathbf{a}_i\|}{d_0} \right) + n_{i,k} & i \in \mathcal{H} \\ P_0 - 10\gamma \log_{10} \left(\frac{\|\mathbf{x}_{att} - \mathbf{a}_i\|}{d_0} \right) + n_{i,k} & i \in \mathcal{M}, \end{cases} \quad (2)$$

where \mathbf{x}_{att} is the false location that the attackers agree upon.

Figure 1b shows an example of a coordinated attack, where two malicious anchors (represented by a red square) attempt to make the network think that the location of the target is the one represented

by a blue triangle (\mathbf{x}_{att}) instead of the real target position represented by a blue cross (\mathbf{x}).

Note that (Equation 2) is a special case of (Equation 1), having $\delta_i = 10\gamma \log_{10} \frac{\|\mathbf{x} - \mathbf{a}_i\|}{\|\mathbf{x}_{att} - \mathbf{a}_i\|}$. Hence, this work adopts (Equation 1) as the general model for both types of spoofing attacks. From it, the probability density function of \mathbf{x} parametrized by the median RSS observation at the i -th anchor P_i is given by

$$f(\mathbf{x}; P_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp \left\{ -\frac{\left(P_i - P_0 + 10\gamma \log_{10} \left(\frac{\|\mathbf{x} - \mathbf{a}_i\|}{d_0} \right) - \delta_i \right)^2}{2\sigma^2} \right\}, \quad (3)$$

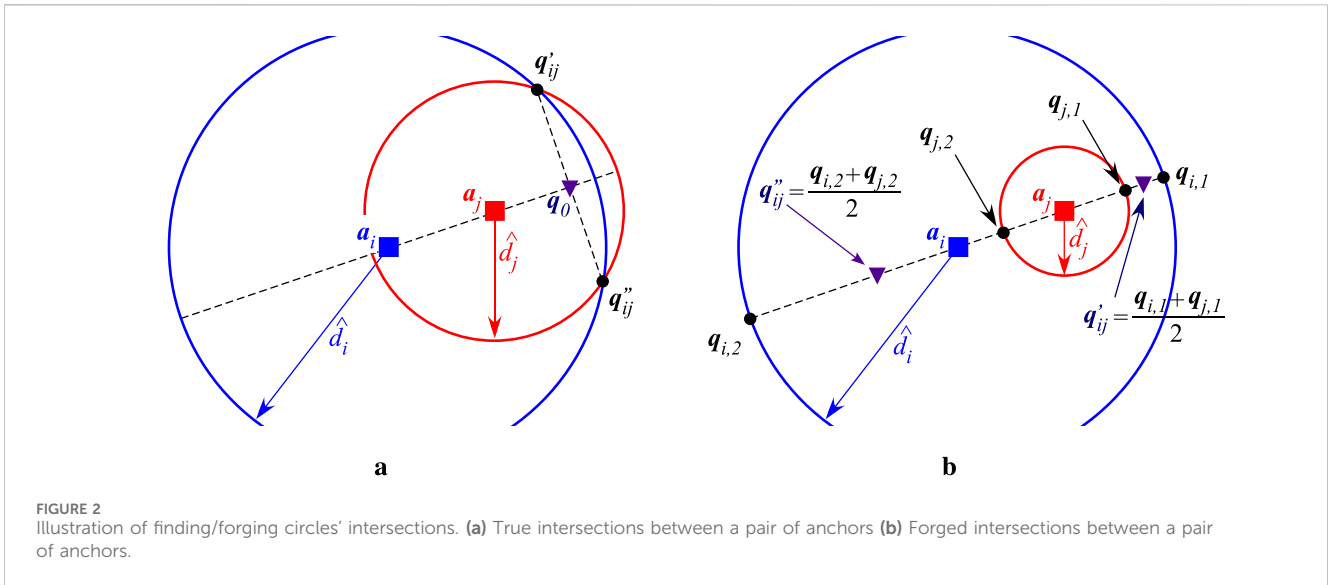
where $\exp\{\bullet\}$ denotes the exponential function. Minimizing (Equation 3) leads to the ML estimator Kay (1993). However, the ML estimator is non-convex and therefore difficult to tackle directly. In this work, a VS algorithm is introduced to estimate the target's location instead.

3 The proposed approach for the secure localization problem

This section describes the derivation of the proposed algorithm for secure localization. It is organized into three parts: 1) a preliminary part, where points of interest are determined, and two main parts in which 2) the proposed localization estimator is described in detail, and 3) the proposed detection procedure to identify attackers is introduced.

3.1 Determining points of interest

At the beginning, all anchors are treated as honest. Hence, the set of malicious nodes is initialized as $\mathcal{M} = \emptyset$, whereas the set of honest nodes is $\mathcal{H} = \{i: 1 \leq i \leq N\}$. Afterwards, one can construct circles, c_i , centered at the known locations of the anchors and radii equivalent to the distance estimate, $\hat{d}_i = d_0 10^{\frac{P_0 - P_i}{10\gamma}}$, obtained from (Equation 1), of the respective anchor (the reader is referred to Figure 2a). The intersection points between all pairs of circles are used as points of



interest for the voting scheme. The intersection points between a pair of circles (given that they exist) can be calculated Tomic and Beko (2022) as follows

$$q'_{ij} = q_0 + t \text{ and } q''_{ij} = q_0 - t, \text{ for } i = 1, \dots, N - 1, j = i + 1, \dots, N, \tag{4}$$

where

$$q_0 = (a_j - a_i) \frac{\hat{d}_i^2 - \hat{d}_j^2}{2\|a_j - a_i\|^2} + \frac{a_i + a_j}{2},$$

$$t = \frac{\sqrt{u}}{2\|a_j - a_i\|^2} T(a_j - a_i), T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

with

$$u = \left((\hat{d}_i + \hat{d}_j)^2 - \|a_j - a_i\|^2 \right) \left(\|a_j - a_i\|^2 - (\hat{d}_j - \hat{d}_i)^2 \right),$$

according to Figure 2a. However, due to the presence of noise and possibly malicious/faulty nodes, a pair of circles might not intersect (the reader is referred to Figure 2b). In this case, the tuple set of anchors without intersection is defined as $\mathcal{C} = \{(i, j): c_i \cap c_j = \emptyset\}$, where the notation $c_i \cap c_j = \emptyset$ is used to denote that the circles corresponding to the i -th and j -th anchors do not intersect. In that case, one can draw a line that passes through the respective pair of anchors, and compute the intersections between the circles and the drawn line as follows.

$$q_{i,1} = a_0 + \left[(a_i - a_0)^T \hat{b} + \sqrt{\left[(a_i - a_0)^T \hat{b} \right]^2 - (a_0^T a_0 + a_i^T a_i - d_i - 2a_0^T a_i)} \right],$$

$$q_{i,2} = a_0 + \left[(a_i - a_0)^T \hat{b} - \sqrt{\left[(a_i - a_0)^T \hat{b} \right]^2 - (a_0^T a_0 + a_i^T a_i - d_i - 2a_0^T a_i)} \right],$$

$$q_{j,1} = a_0 + \left[(a_j - a_0)^T \hat{b} + \sqrt{\left[(a_j - a_0)^T \hat{b} \right]^2 - (a_0^T a_0 + a_j^T a_j - d_j - 2a_0^T a_j)} \right],$$

$$q_{j,2} = a_0 + \left[(a_j - a_0)^T \hat{b} - \sqrt{\left[(a_j - a_0)^T \hat{b} \right]^2 - (a_0^T a_0 + a_j^T a_j - d_j - 2a_0^T a_j)} \right],$$

where $a_0 = \frac{a_i + a_j}{2}$ is the position vector of the line, and $\hat{b} = \frac{a_i - a_j}{\|a_i - a_j\|}$ is the unit vector that describes the line's direction. Afterwards, the intersection points to be used in the voting-scheme, q'_{ij}, q''_{ij} , are

obtained as the middle of the intersection points between the line and the circles at both ends, according to

$$q'_{ij} = \frac{q_{i,1} + q_{j,1}}{2}, \quad q''_{ij} = \frac{q_{i,2} + q_{j,2}}{2} \tag{5}$$

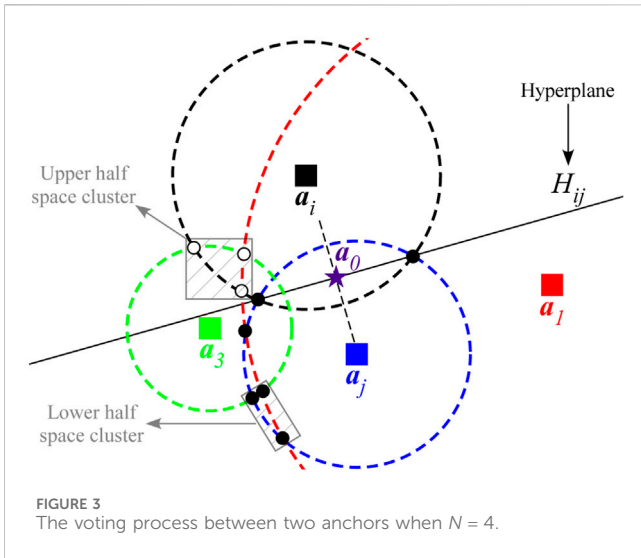
The forged intersection points are required for the proposed algorithm in scenarios where the number of anchors is scarce and/or the genuine intersection points are in insufficient number. This idea has already been implemented in Tomic and Beko (2022), and the reasoning behind it is that when a pair of anchors is genuine, the intersection points would lay in the vicinity of the drawn line, making these forged intersection points a reasonable approximation of the real ones.

3.2 The proposed voting-based scheme for target localization

The voting scheme is a process to cluster and assign votes to the intersection points based on some criterion (for instance, their physical proximity). The main idea is to assign a value (vote) to each intersection point in order to find the most trustworthy ones. It is important to highlight that the localization process is done for a specific instant in time, therefore, past information of the network is not used to aid the voting-scheme. For the sake of simplicity, let us define the matrix $Q = [q'_{ij} \ q''_{ij}] \in \mathbb{R}^{2 \times \binom{N}{2}}$ containing all intersection points, and the vector $Q_g \in \mathbb{R}^2$ as the g -th column of Q . This process iterates all pairs of anchors, and for each pair a hyperplane is computed as

$$H_{ij} = \left\{ g: \hat{b}^T Q_g = \hat{b}^T a_0 \right\}, \tag{6}$$

which divides the problem space into two-half spaces. The intersection points are assigned to the upper half space, $H_{ij}^{(u)} = \{g: \hat{b}^T Q_g > \hat{b}^T a_0\}$, or to the lower half space, $H_{ij}^{(l)} = \{g: \hat{b}^T Q_g < \hat{b}^T a_0\}$, according to their physical location with respect to the hyperplane. Next, clusters composed of $N - 1$ elements that are physically the closest to each other in each half



space are built: $C_{ij}^{(u)} \subseteq H_{ij}^{(u)}$ as the upper cluster and $C_{ij}^{(l)} \subseteq H_{ij}^{(l)}$ as the lower cluster. Lastly, votes, v_g , are assigned to the points that belong to a cluster (if these exist), based on their distance to the hyperplane, see Figure 3. Vote for the g -th intersection point is calculated as

$$v_g = \sum_{i=1}^{N-1} \sum_{j=i+1}^N w_g \frac{\text{proj}_{H_{ij}}(\mathbf{Q}_g)}{\sum_{g: g \in C_{ij}^{(u)}} \text{proj}_{H_{ij}}(\mathbf{Q}_g)} + w_g \frac{\text{proj}_{H_{ij}}(\mathbf{Q}_g)}{\sum_{g: g \in C_{ij}^{(l)}} \text{proj}_{H_{ij}}(\mathbf{Q}_g)}, \quad g \in C_{ij}^{(u)} \cup C_{ij}^{(l)} \quad (7)$$

where

$$w_g = \begin{cases} \frac{\hat{d}_j}{\hat{d}_i + \hat{d}_j}, & \text{if } g \in H_{ij}^{(u)} \\ \frac{\hat{d}_i}{\hat{d}_i + \hat{d}_j}, & \text{if } g \in H_{ij}^{(l)} \end{cases}, \quad (8)$$

$$\text{proj}_{H_{ij}}(\mathbf{Q}_g) = \|\mathbf{Q}_g - (\mathbf{e}\mathbf{e}^T \mathbf{Q}_g + (\mathbf{I}_2 - \mathbf{e}\mathbf{e}^T) \mathbf{a}_0)\| \quad (9)$$

with $\mathbf{e} = \mathbf{T}\hat{\mathbf{b}}$, \mathbf{I}_2 is the identity matrix of order two, $\text{proj}_{H_{ij}}(\mathbf{Q}_g)$ denotes the distance of an intersection point, \mathbf{Q}_g , to its respective projection on the hyperplane, and w_g is a weight based on the distances \hat{d}_i and \hat{d}_j which takes into account the anchor and the point \mathbf{Q}_g .

The procedure to compute the votes defined in (Equation 7) is explained in the following. For every point of interest \mathbf{Q}_g , with $g = 1, \dots, \binom{N}{2}$, one considers all combinations of pairs of anchors (i, j) , where $i = 1, \dots, N$ and $j = i + 1, \dots, N$, and calculates the respective hyperplanes H_{ij} according to (Equation 6). Then, each weight w_g divides a single vote according to the proximity of H_{ij} to \mathbf{a}_i and \mathbf{a}_j , such that more weight is assigned to the half space containing the anchor closer to the hyperplane (Equation 8). A cluster of $N - 1$ points physically closest to one another, $C_{ij}^{(u)}$ and $C_{ij}^{(l)}$, are formed in each half space. If $g \in C_{ij}^{(u)}$ or $g \in C_{ij}^{(l)}$, distances of the cluster points to H_{ij} are calculated (Equation 9) and converted into weights by dividing the individual distances with the sum of all distances of the points in the cluster to the hyperplane; otherwise, sum zero and move on to the next anchor pair. Lastly, these weights

are further weighted with w_g and summed up to form a vote for the g -th point of interest. Hence, the intuition behind the votes defined in (Equation 7) is that it assigns greater weights (belief) to points closer to the hyperplane, since the correct cluster of (genuine) points should lie in its vicinity.

An estimate of the target's location can be obtained by re-ordering the vote vector in a descending fashion, $\tilde{\mathbf{v}} = [\tilde{v}_h]$, such that $\tilde{v}_1 \geq \tilde{v}_2 \geq \dots \geq \tilde{v}_{\binom{N}{2}}$. The first $N - 1$ votes correspond to the most trustworthy points; hence, the estimate is obtained by applying the WCM principle for the $N - 1$ (normalized) vote values as

$$\hat{\mathbf{x}} = \sum_{h=1}^{N-1} \tilde{w}_h \mathbf{Q}_h, \quad \text{with } \tilde{w}_h = \frac{\tilde{v}_h}{\sum_{h=1}^{N-1} \tilde{v}_h}. \quad (10)$$

3.3 Attack detection

Considering (Equation 3), in the case of a malicious anchor, it is intuitive that the attack would shift the probability distribution according to the attack intensity. This shift of the distribution could cause the mean to fall outside of a CI. In other words, one could take advantage of it to detect attackers. However, as the attack intensity is unknown, it can be estimated by exploiting the estimated target location in (Equation 10) based on the ML principle. Similar can be done for the noise standard deviation and the expected (genuine) RSS value as

$$\hat{\delta}_i = \frac{\sum_{k=1}^K P_0 - P_{i,k} - 10\gamma \log_{10} \|\hat{\mathbf{x}} - \mathbf{a}_i\|}{K}, \quad (11)$$

$$\hat{\sigma} = \frac{1}{N} \sum_{i=1}^N \sqrt{\frac{1}{(K-1)} \sum_{k=1}^K (\alpha_i - \hat{\delta}_i)^2}, \quad (12)$$

$$\hat{P}_i = P_0 - 10\gamma \log_{10} \|\hat{\mathbf{x}} - \mathbf{a}_i\|, \quad (13)$$

with $\alpha_{i,k} = P_{i,k} - P_0 + 10\gamma \log_{10} \|\hat{\mathbf{x}} - \mathbf{a}_i\|$.

It is well known that 68% of the mass of a normal distribution falls within one standard deviation of the mean. Thus, if the measured RSS in (Equation 1) lays outside of the CI $[\hat{P}_i - \hat{\sigma}, \hat{P}_i + \hat{\sigma}]$, the respective anchor is classified as malicious, and the set of malicious nodes becomes $\mathcal{M} = \{i: P_i < \hat{P}_i - \hat{\sigma} \vee P_i > \hat{P}_i + \hat{\sigma}\}$. Notice that the symmetric band $[\hat{P}_i - \hat{\sigma}, \hat{P}_i + \hat{\sigma}]$ used to flag an anchor as malicious might not be the optimal one, especially for anchors at very different ranges. Still, it effectively serves its intended purpose and achieves strong performance in practice; thus, its further enhancement is left for future work.

Note that, in contrast to Beko and Tomic (2021), Mukhopadhyay et al. (2021), the malicious node is possibly exploited in the localization process. This can be advantageous when the $|\delta_i|$ is not high compared to noise power, and quantity of anchors prevails over quality.

The proposed algorithm is summarized in Algorithm 1. It should be noted that the proposed algorithm operates entirely locally at the target using a single network snapshot in time. While the inferred corruption status of the anchors could be reused by the same target over time (e.g., in tracking or navigation problems) or shared with other targets in a cooperative setting, such mechanisms fall outside the scope of

this work; thus, no inter-target cooperation or information exchange is assumed or required by the algorithm.

```

Require:  $N$ : Number of anchors in the network
Require:  $\mathbf{a}_i$ : True anchor locations  $i = 1, \dots, N$ 
Require:  $K$ : Number of measurement samples
Require:  $\gamma$ : Path loss exponent
Require:  $d_0$ : References distance
Require:  $P_0$ : Transmit power
Require:  $P_{i,k}$ :  $k$ -th RSS measurement sample at  $i$ -th anchor

1: Initialization: Set  $\mathcal{M} = \emptyset$  and  $\mathcal{H} = \{i: 1 \leq i \leq N\}$ 
2: Form circles centered at  $\mathbf{a}_i$  with radius  $d_i$  for  $i = 1, \dots, N$ 
3: for  $i = 1, \dots, N-1$  do
4:   for  $j = i+1, \dots, N$  do
5:     if  $C_i \cap C_j \neq \emptyset$  then
6:        $q'_{ij}, q''_{ij} \leftarrow$  (Equation 4) // Find circle intersection points
7:     else
8:        $q'_{ij}, q''_{ij} \leftarrow$  (Equation 5) // Forge intersection points
9:     end if
10:     $H_{ij} \leftarrow$  (Equation 6) // Compute hyperplanes
11:     $C_{ij}^{(l)} \subseteq H_{ij}^{(l)}$  and  $C_{ij}^{(u)} \subseteq H_{ij}^{(u)}$  // Cluster in half spaces
12:    end for
13:  end for
14:  $v_g \leftarrow$  (Equation 7) // Compute votes for cluster points
15:  $\hat{\mathbf{x}} \leftarrow$  (Equation 10) // Estimate target's location
16:  $\hat{\delta}_i \leftarrow$  (Equation 11) // Estimate attack intensity
17:  $\hat{\sigma} \leftarrow$  (Equation 12) // Estimate noise STD
18:  $\hat{p}_i \leftarrow$  (Equation 13) // Estimate expected genuine RSS value
19: for  $i = 1, \dots, N$  do
20:   if  $P_i \in [\hat{p}_i - \hat{\sigma}, \hat{p}_i + \hat{\sigma}]$  then
21:      $\mathcal{M} \leftarrow \mathcal{M} \cup \{i\}$  // Label anchor  $i$  as malicious
22:      $\mathcal{H} \leftarrow \mathcal{H} \setminus \{i\}$  // Remove anchor  $i$  from honest ones
23:   end if
24: end for
25: Return:  $\hat{\mathbf{x}}$  and  $\mathcal{M}$ 

```

Algorithm 1. Pseudo-code for the proposed VS algorithm.

4 Performance analysis

This section presents a series of numerical results in order to assess the performance of the proposed solution. It presents analysis based on computational complexity, localization accuracy and success in detecting malicious attackers, as well as a discussion on the limitations of the proposed scheme. It is thus organized correspondingly.

4.1 Complexity analysis

The complexity analysis is highly relevant for the applicability of the algorithm, especially in real-time scenarios. Given that B_{\max} and

B_{ADMM} are respectively the maximum number of iterations for the GTRS-based and for the ADMM-based algorithms, Table 1 summarizes the worst-case computational complexity together with the average running time of the considered methods. The latter evaluation was performed with 100 Monte Carlo (MC) runs, for $N = 6$, $\sigma = 1$ dB, $\delta = 10$ dB, on a machine with the following characteristics: CPU: Intel(R) Core(TM) i5-1135G7 CPU @ 2.40 GHz, RAM: 16 GB, OS: Windows 11 Home, running MATLAB R2016b.

Essentially, all considered methods involve matrix addition, multiplication and transpose operations, and the LC-GTRS in Tomic and Beko (2022) and SWLS in Mukhopadhyay et al. (2021) require matrix inversion. These operations come with certain computational costs associated with them (e.g., $\mathcal{O}(m^3)$ is the cost of matrix inversion, where m stands for the size of the square matrix). Nevertheless, one can note from the table that all considered algorithms have linear complexity in the dominant term, N . Regarding the complexity of the proposed VS method, its most expensive operation is the calculation of the votes in (Equation 7), where a series of matrix additions and multiplications is required in order to compute the projection of points of interest onto the hyperplane. However, dimensions of the matrices and vectors involved in these computations are fixed to $y \times y$ and y respectively, with y denoting the dimension of the space of interest (2-D or 3-D). Hence, although the operations in VS are computationally the least demanding, the proposed algorithm requires repeated actions (for each pair of anchors), which results in somewhat higher average running time than SWLS and R-GTRS. However, note that these actions could be done in parallel, so that the running time of VS is reduced significantly. Moreover, the GTRS-based and ADMM-based approaches require repeated actions, while LC-GTRS and LN-1E require two phases to obtain the final location estimation.

4.2 Performance analysis via simulations

This section validates the performance of the considered algorithms in terms of localization accuracy and success of attacker detection through numerical simulations. All simulations disclose the results for N randomly deployed anchors and a single target (at a time), within a two-dimensional area of 25×25 m² with two malicious anchors. Moreover, anchors are randomly deployed $N_D = 1000$ times and, for each localization setting, two randomly chosen anchors are considered malicious $N_A = 50$ times.

The RSS measurements¹ were obtained through (Equation 1), where the transmit power at the target node is set to $P_0 = 15$ dBm, the PLE is set at $\gamma = 3$, which corresponds to propagation in an urban area, and $K = 10$ observation were considered. The main metric used to assess the localization performance is the root mean squared error (RMSE), $\text{RMSE} = \sqrt{\frac{\sum_{i=1}^{MC} \|x_i - \hat{x}_i\|^2}{MC}}$ (m), where x_i and \hat{x}_i

1 Note that this work considers PLE and the transmit power known *a priori*. This might not be the case in practice, so these parameters might not be (perfectly) known beforehand. Considering these parameters not known might be an interesting direction for future work.

TABLE 1 Brief summary of the considered algorithms.

Algorithm	Complexity	Running time (ms)	Type of attack	Additional requirements
VS in Section 3	$(\frac{N}{2}) \times \mathcal{O}(N)$	7	UC and C	No
LC-GTRS in Tomic and Beko (2022)	$2 \times \mathcal{O}(B_{\max} \times N)$	5	UC and C	No
SWLS in Mukhopadhyay et al. (2021)	$\mathcal{O}(N)$	1	UC	Knowledge about σ
LN-1E in Mukhopadhyay et al. (2021)	$2 \times \mathcal{O}(B_{\text{ADMM}} \times N)$	18	C	No
R-GTRS in Tomic and Beko (2024a)	$\mathcal{O}(B_{\max} \times N)$	1	UC and C	Knowledge about $\max\{ \delta_i \}$
WADMM in Tomic and Beko (2024b)	$\mathcal{O}(B_{\text{ADMM}} \times N)$	20	UC and C	No

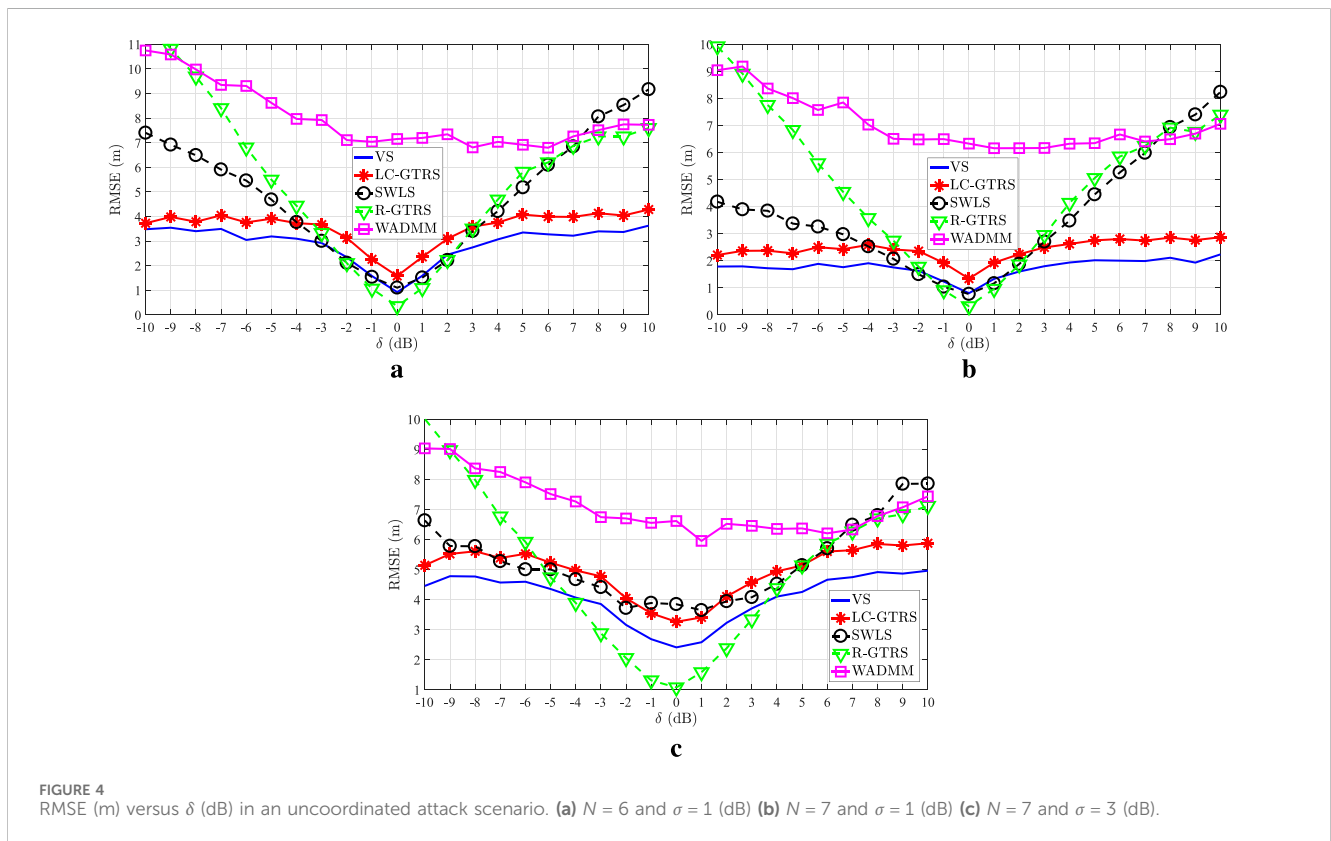


FIGURE 4 RMSE (m) versus δ (dB) in an uncoordinated attack scenario. (a) $N = 6$ and $\sigma = 1$ (dB) (b) $N = 7$ and $\sigma = 1$ (dB) (c) $N = 7$ and $\sigma = 3$ (dB).

are, respectively, the true and the estimated target location in the i -th Monte Carlo run, i.e., $MC = N_D \times N_A$.

It is worth mentioning here that SWLS in Mukhopadhyay et al. (2021) requires tuning the detection threshold by studying an empirical parameter, ζ . By fine-tuning the empirical threshold in the considered settings, it was concluded that the best localization results for SWLS were obtained for $\zeta = 1.5$; thus, this value is adopted for SWLS in all presented simulations. Furthermore, R-GTRS in Tomic and Beko (2024a) requires knowledge on the magnitude of the attack intensity, i.e., $|\delta_i|$ in (Equation 1). The true value δ_i is given to R-GTRS in all presented simulations.

4.2.1 Uncoordinated attacks

In a non-coordinated attack, the attack intensity in (Equation 1) is chosen according to

$$\delta_i = \begin{cases} 0, & i \in \mathcal{H} \\ \delta, & i \in \mathcal{M} \end{cases}$$

where δ (dB) is defined below for each scenario.

Figure 4 illustrates RMSE (m) versus δ (dB) comparison of the considered approaches in an uncoordinated attack scenario with two malicious anchors for different values of N and σ (dB). As expected, the figure clearly shows that the performance of all methods degrades with the increase of $|\delta|$ (dB). Likewise, it shows a trend that all methods benefit from the increase of N and suffer from the increase of σ (dB). From Figure 4, one can see that the proposed solution outperforms the existing ones for medium-to-high $|\delta|$ (dB), whereas R-GTRS exhibits superior performance for low $|\delta|$ (dB). Nevertheless, R-GTRS suffers significant performance degradation for high $|\delta|$ (dB), making it

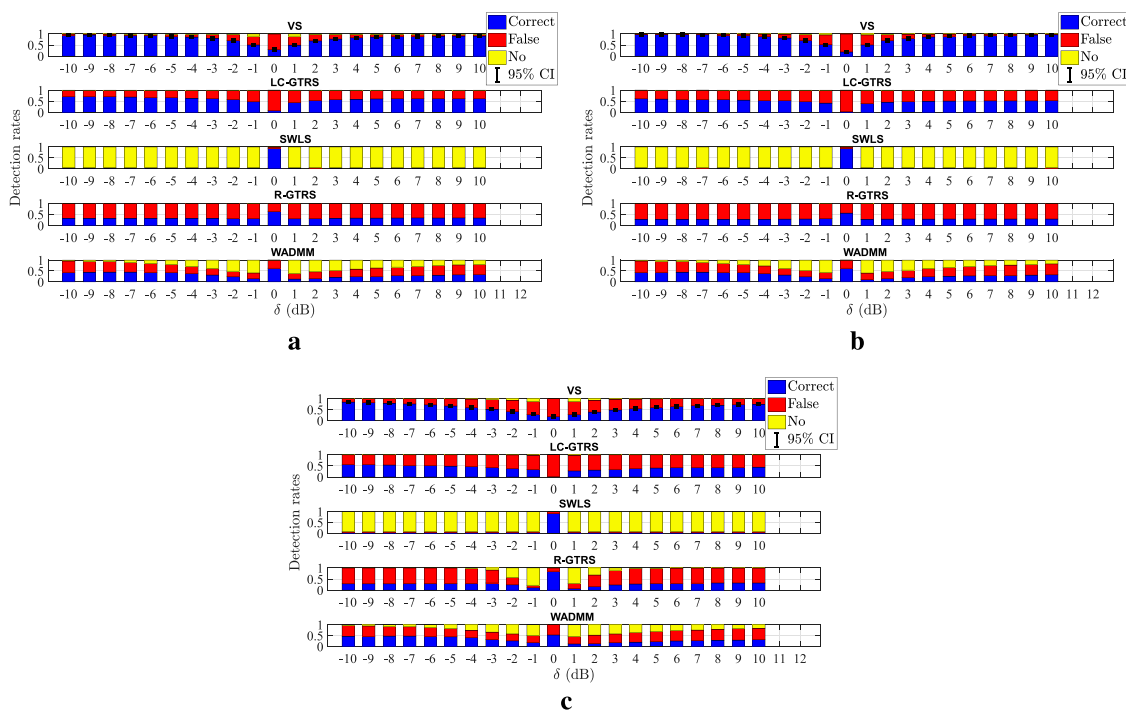


FIGURE 5 Detection rates versus δ (dB) in an uncoordinated attack scenario. (a) $N = 6$ and $\sigma = 1$ (dB) (b) $N = 7$ and $\sigma = 1$ (dB) (c) $N = 7$ and $\sigma = 3$ (dB).

unusable in these settings. This behavior most likely occurs due to a high dis-balance between the number of genuine and malicious anchors in the considered scenario, causing R-GTRS to erroneously penalize the genuine anchors instead of the malicious ones. This is particularly noticeable when $|\delta|$ is relatively high, causing significant difference in malicious and genuine measurements and tricking R-GTRS to mistakenly penalize more the genuine anchors, thus favoring the malicious ones and resulting in higher performance loss. Hence, although it is a robust min-max approach that is conceived for the worst-case scenario (it assumes that all anchors malicious initially), R-GTRS method experiences difficulties in *lighter and milder* settings.

Figure 5 illustrates different detection rates versus δ (dB) comparison of the considered approaches in an uncoordinated attack scenario with two malicious anchors for different values of N and σ (dB). In order to show the stability of the detection results, 95% Wilson binomial CI Wilson (1927) is employed to provide accurate coverage for finite sample sizes. In this way, each detection outcome is a Bernoulli process, with the correct detection corresponding to success, and all other outcomes (false and no detection) are treated as failure. The CI is calculated as

$$CI = \left[\frac{P_{CD} + \frac{z^2}{2MC|\mathcal{M}|} - z \sqrt{\frac{P_{CD}(1-P_{CD})}{MC|\mathcal{M}|} + \frac{z^2}{4(MC|\mathcal{M}|)^2}}}{1 + \frac{z^2}{MC|\mathcal{M}|}}, \frac{P_{CD} + \frac{z^2}{2MC|\mathcal{M}|} + z \sqrt{\frac{P_{CD}(1-P_{CD})}{MC|\mathcal{M}|} + \frac{z^2}{4(MC|\mathcal{M}|)^2}}}{1 + \frac{z^2}{MC|\mathcal{M}|}} \right], \quad (14)$$

with P_{CD} denoting the empirical correct detection rate, MC and $|\mathcal{M}|$ respectively being the number of Monte Carlo runs and the

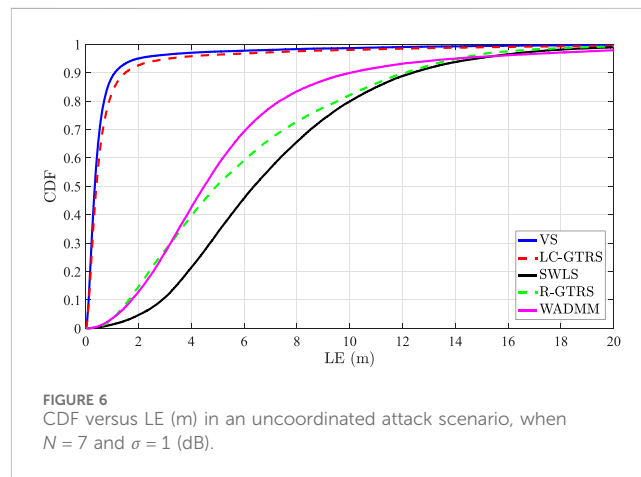


FIGURE 6 CDF versus LE (m) in an uncoordinated attack scenario, when $N = 7$ and $\sigma = 1$ (dB).

number of attackers, and z representing the standard normal quantile ($z = 1.96$ for 95% confidence interval). Figure 5 corroborates the effectiveness of the proposed detection scheme and confirms the superiority of the proposed approach for high $|\delta|$ (dB). The latter claim can be explained by the robustness of the proposed approach to high $|\delta|$ (dB) in terms of localization performance, since the location estimate of VS is exploited for detection, and having better localization estimate can naturally lead better detection performance (if used in a correct manner). Finally, it is worth mentioning that the detection of SWLS is poor in general, which suggest that its hyper-parameter ζ might need more fine-tuning (even though $\zeta = 1.5$ resulted in the best localization performance).

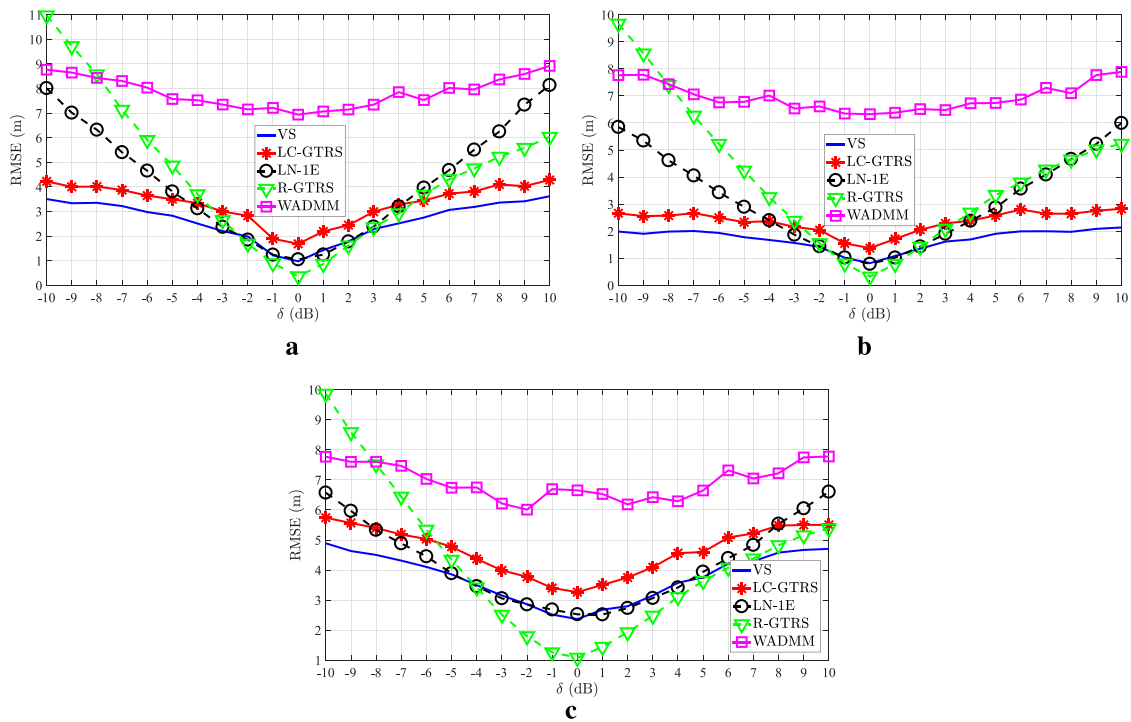


FIGURE 7 RMSE (m) versus δ (dB) in a coordinated attack scenario. (a) $N = 6$ and $\sigma = 1$ (dB) (b) $N = 7$ and $\sigma = 1$ (dB) (c) $N = 7$ and $\sigma = 3$ (dB).

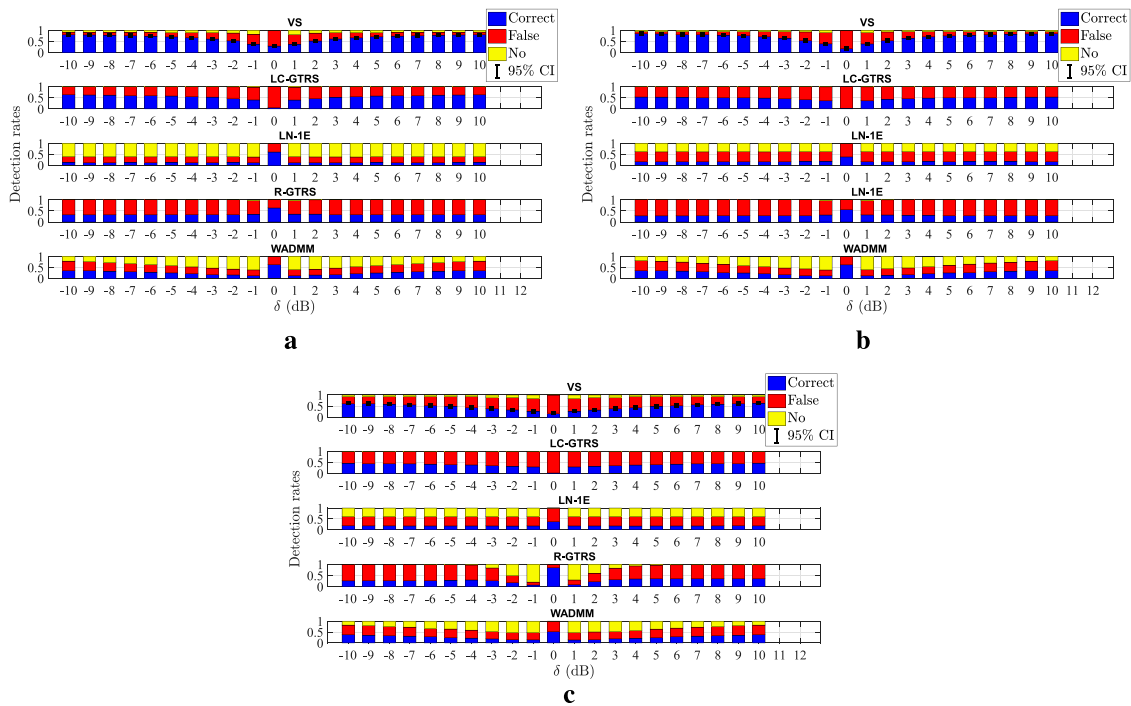


FIGURE 8 Detection rates versus δ (dB) in a coordinated attack scenario. (a) $N = 6$ and $\sigma = 1$ (dB) (b) $N = 7$ and $\sigma = 1$ (dB) (c) $N = 7$ and $\sigma = 3$ (dB).

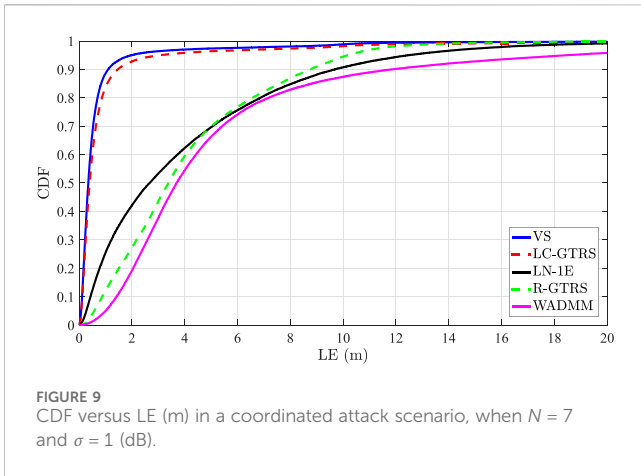


FIGURE 9 CDF versus LE (m) in a coordinated attack scenario, when $N = 7$ and $\sigma = 1$ (dB).

Figure 6 illustrates the cumulative distribution function (CDF) versus localization error (LE) in the considered uncoordinated scenario, when $N = 7$, $\delta = 7$ (dB) and $\sigma = 1$ (dB). The LE in the i -th MC run is defined as $LE_i = \|\mathbf{x}_i - \hat{\mathbf{x}}_i\|$. The figure shows that the proposed scheme and LC-GTRS exhibit similar performance which is clearly superior over the remaining existing ones. For instance, the former two solutions have a median of $LE \approx 0.4$ (m), whereas the best of the remaining ones exhibits a median of $LE \approx 4.5$ (m).

4.2.2 Coordinated attacks

In a coordinated attack, \mathbf{x}_{att} in (Equation 2) is obtained by choosing a random point on a circle centered at the true target's location with

radius δ , i.e., $\mathbf{x}_{att} = \mathbf{x} + \delta[\cos \theta, \sin \theta]^T$, where θ is a random angle chosen from a uniform distribution from the interval $[0, 2\pi]$.

Figure 7 illustrates RMSE (m) versus δ (dB) comparison of the considered approaches in a coordinated attack scenario with two malicious anchors for different values of N and σ (dB). Similar as in the uncoordinated scenario, Figure 7 exhibits superior performance of the proposed solution for medium-to-high $|\delta|$ (dB), being R-GTRS and LN-1E its only competitors for low $|\delta|$ (dB). This result suggests that these two methods might be somewhat more robust to noise, since low $|\delta|$ (dB) can be seen as noise corruption. Still, the gain that the new method achieves for high $|\delta|$ (dB) clearly compensates this behavior.

Figure 8 illustrates different detection rates versus δ (dB) comparison of the considered approaches in a coordinated attack scenario with two malicious anchors for different values of N and σ (dB). As foreseen, (correct) detection performance of all methods degrades with the increase of σ (dB). This is explained by the fact that higher noise power gives attackers more room to disguise their malicious deeds within the noise, aggravating the detection process. This is particularly discernible for all methods in the interval $0 < \frac{|\delta|}{\sigma} \leq 2$. Nonetheless, the proposed scheme significantly outperforms the existing ones in terms of attacker detection in general.

Figure 9 illustrates the cumulative distribution function (CDF) versus localization error (LE) in the considered coordinated scenario, when $N = 7$, $\delta = 7$ (dB) and $\sigma = 1$ (dB). Figure 9 shows that the proposed scheme and LC-GTRS have almost identical performance which is clearly superior over the remaining existing ones. For instance, the former two solutions have a median of $LE \approx 0.4$ (m), whereas the best of the remaining ones exhibits a median of $LE \approx 3$ (m).

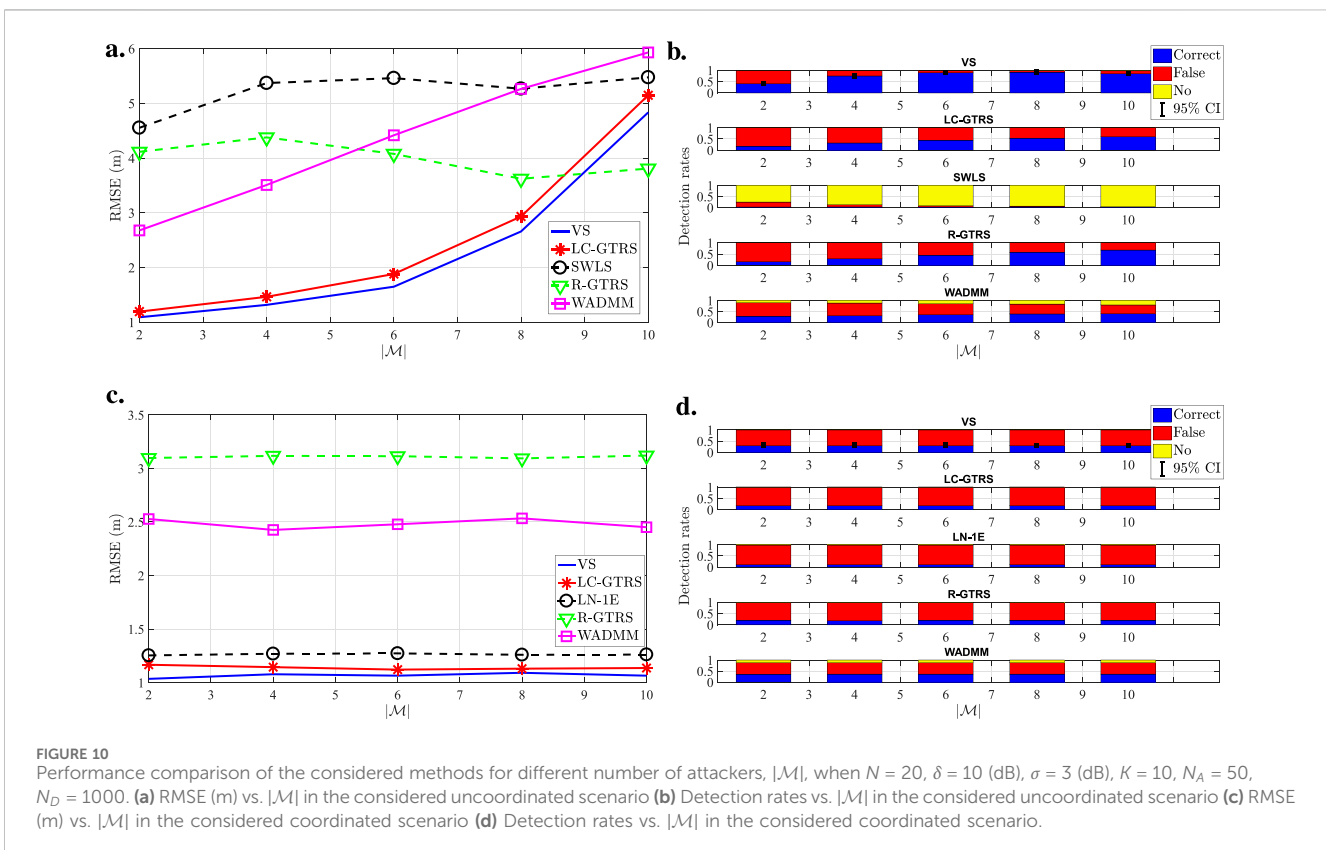


FIGURE 10 Performance comparison of the considered methods for different number of attackers, $|\mathcal{M}|$, when $N = 20$, $\delta = 10$ (dB), $\sigma = 3$ (dB), $K = 10$, $N_A = 50$, $N_D = 1000$. (a) RMSE (m) vs. $|\mathcal{M}|$ in the considered uncoordinated scenario (b) Detection rates vs. $|\mathcal{M}|$ in the considered uncoordinated scenario (c) RMSE (m) vs. $|\mathcal{M}|$ in the considered coordinated scenario (d) Detection rates vs. $|\mathcal{M}|$ in the considered coordinated scenario.

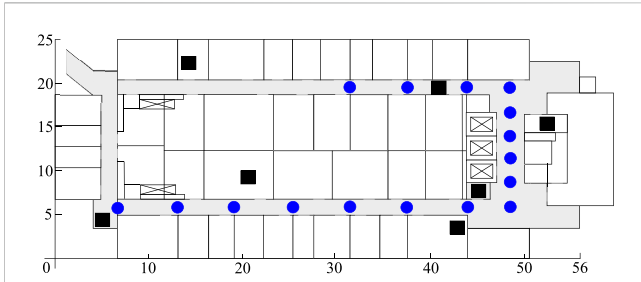


FIGURE 11 Real-world experimental set up under consideration: blue circles and black squares respectively denote the true target and anchor locations. The data set is a courtesy of our colleagues from Computer Science department at Rutgers University [Niculescu and Nath \(2004\)](#).

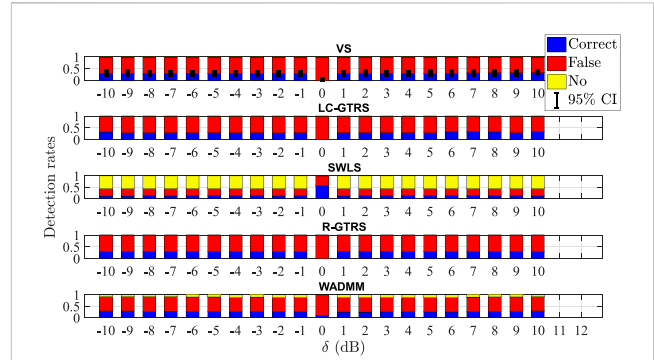


FIGURE 13 Detection rates versus δ (dB) in the considered experimental uncoordinated attack scenario, for $N_A = 100$.

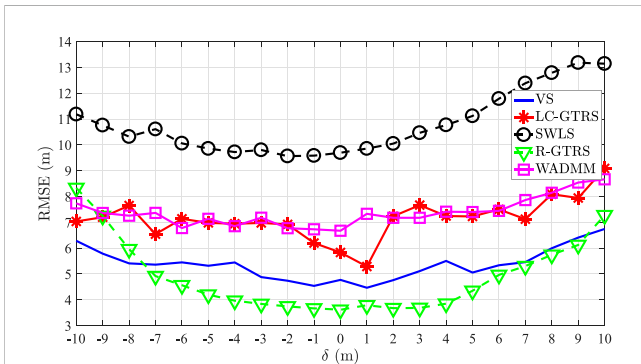


FIGURE 12 RMSE (m) versus δ (dB) in the considered experimental uncoordinated attack scenario, for $N_A = 100$.

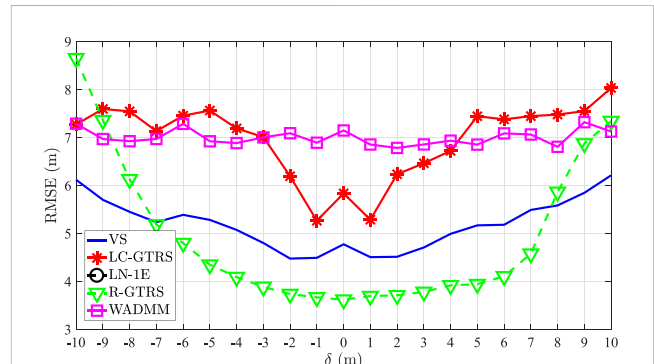


FIGURE 14 RMSE (m) versus δ (dB) in the considered experimental coordinated attack scenario, for $N_A = 100$.

To finish off the analysis via computer simulations, [Figure 10](#) illustrates the performance comparison in the considered uncoordinated and coordinated attack scenarios, when $N = 20$, $\delta = 10$ (dB), $\sigma = 3$ (dB), $K = 10$, where $|\mathcal{M}|$ attackers were randomly chosen $N_A = 50$ times in each of $N_D = 1000$ random deployments of all nodes. The figure illustrates general superiority of the proposed VS in both uncoordinated and coordinated attack scenarios. Only R-GTRS manages to provide better results in uncoordinated attack scenario when half of the anchors are malicious. This is not surprising, since the R-GTRS method is a robust min-max approach that is conceived for the worst-case scenario, but experiences difficulties in *lighter* and *milder* settings. Similarly, the proposed detection scheme outperforms the existing ones in both scenarios in general, achieving around 90% of correct attacker detection in the considered uncoordinated attack scenarios when at least 30% of anchors are malicious.

4.3 Performance analysis via experimental measurements

This section validates the performance of the considered algorithms in terms of localization accuracy and success of

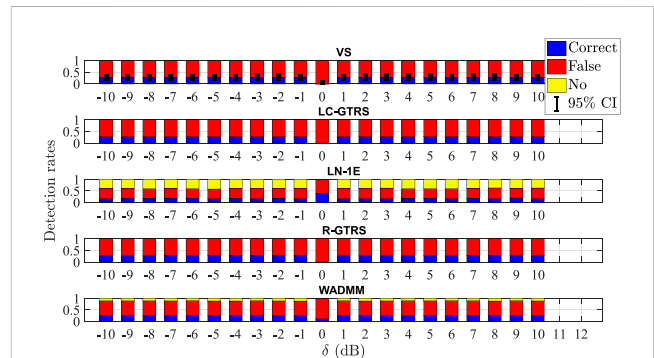
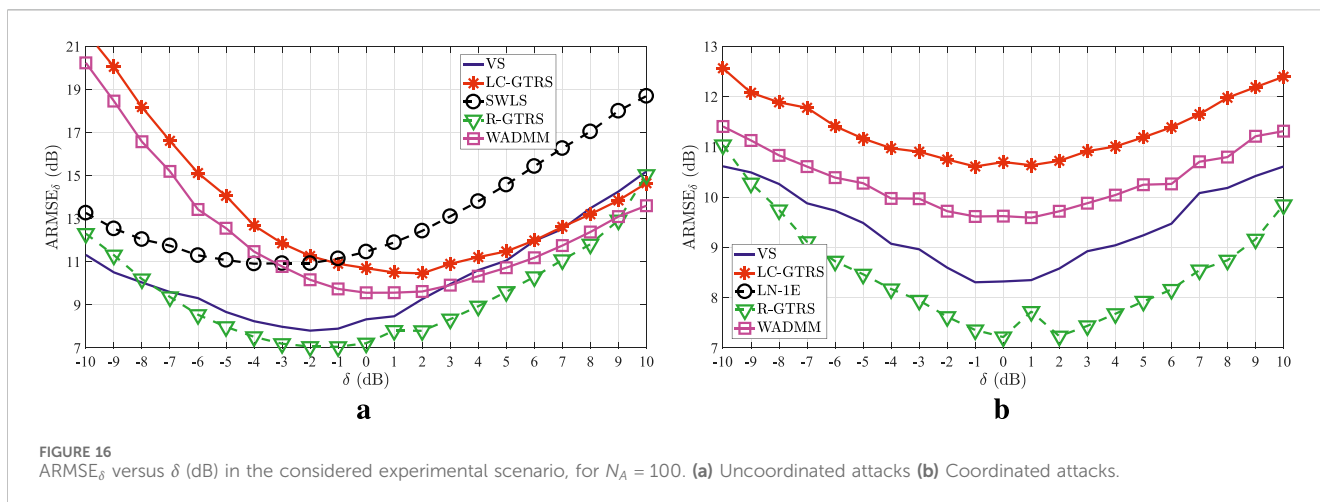


FIGURE 15 Detection rates versus δ (dB) in the considered experimental coordinated attack scenario, for $N_A = 100$.

attacker detection through experimental measurements. The considered experimental configuration is illustrated in [Figure 11](#). In all experiments, $K = 50$ was considered to localize a single target at a time, in the presence of two malicious anchors. Moreover, two randomly chosen anchors in each run out of $N_A = 100$ runs are



considered malicious, and their spoofing attacks were generated by simply injecting a value into the acquired experimental measurements.

4.3.1 Uncoordinated attacks

Figure 12 illustrates RMSE (m) versus δ (dB) comparison of the considered approaches in the experimental uncoordinated attack scenario with two malicious anchors. The figure exhibits that only R-GTRS performs better than the proposed scheme for low-to-medium δ (dB), whereas for high attack intensities (e.g., $|\delta| \geq 7$), both methods exhibit similar performance. Nevertheless, it is worth remembering that R-GTRS requires additional knowledge about the maximum attack intensity, which is unlikely to be perfectly available beforehand in practice.

Figure 13 illustrates detection rates versus δ (dB) comparison of the considered approaches in the experimental uncoordinated attack scenario with two malicious anchors. Figure 13 shows that the achieved detection rates are significantly lower than the ones from the simulations, but this is expected given various obstacles, anisotropies and other phenomena that were not considered in simulations. Even so, the results indicate that the proposed detection scheme works well in practice, which is corroborated by the fact that its results match the best existing ones, LC-GTRS in this case, and go up to $\approx 34\%$.

4.3.2 Coordinated attacks

Figure 14 illustrates RMSE (m) versus δ (dB) comparison of the considered approaches in the experimental coordinated attack scenario with two malicious anchors. Similar as in the uncoordinated case, only R-GTRS performs better than the proposed scheme for low-to-medium δ (dB), whereas for high attack intensities (e.g., $|\delta| \geq 7$), the proposed approach exhibits the best performance.

Figure 15 illustrates detection rates versus δ (dB) comparison of the considered approaches in the experimental coordinated attack scenario with two malicious anchors. Naturally, the figure shows a drop in the detection rates when compared with the ones in the simulations. Again, the proposed detection scheme is corroborated in practice, matching the performance of the best existing one, and goes up to $\approx 30\%$.

4.4 Discussion

While the proposed solution outperforms existing methods in localization and detection for medium-to-high attack intensity, some limitations and parameter choices are worth discussing. Certain parameters are fixed, such as the number of points of interest set to $N - 1$ for localization and the confidence interval for attacker detection set within one estimated noise standard deviation. The rationale for using $N - 1$ points is that not all N intersection points are necessary, as some may be affected by attacks or excessive noise. For smaller N , trimming unnecessary points improves accuracy. The confidence interval choice balances false detection (if too narrow) and missed detection (if too wide), with one standard deviation offering a reasonable trade-off. Although these parameters could be fine-tuned for different scenarios, numerical results indicate that the chosen values work well within the considered settings.

The proposed approach assigns beliefs (votes) to each intersection point, but under high noise or unfavorable attack coordination, it may mistakenly remove a genuine point, potentially impacting localization accuracy. However, numerical results confirm that such occurrences are infrequent and do not significantly degrade performance. While the final detection output is a binary decision (genuine or malicious anchor), this classification is solely for detection purposes and does not influence localization refinement. Like existing methods, the approach requires at least 50% of anchors to be non-compromised, particularly in coordinated attacks, as a malicious majority would easily manipulate localization. A unique aspect of the method is its ability to generate points of interest even when anchor circles do not intersect. In extreme cases, all points might need to be fabricated, leading to inaccurate clusters. However, this scenario poses a challenge for all existing methods, as they inherently rely on intersection points for localization.

Although not all considered methods estimate the attack intensity directly in their detection procedure, one can obtain this estimate as explained here in (Equation 11). Hence, Figure 16 illustrates the average RMSE of $\delta = [\delta_i]^T$ (ARMSE_δ) in (dB) versus δ (dB) in the considered experimental uncoordinated attack scenario, Figure 16a, and the considered experimental coordinated attack scenario, Figure 16b, for $N_A = 100$. The figure shows that none of the

considered approaches accomplishes an error below 7 (dB), which is due to the complexity of the scenario. Still, the proposed scheme exhibits a fairly good, but in general not the best, estimation performance, indicating that this estimation is not a prerequisite for high detection rate, which is somewhat intuitive. Finally, it is worth mentioning that the results of LN-IE are around 22 dBs in the considered setting, and are thus cut off for a better overview.

5 Conclusion

This work advances target localization in randomly deployed WSNs under both uncoordinated and coordinated spoofing attacks by introducing a novel geometric approach for accurate localization and attacker detection. The method estimates the target's location using intersection points of anchor pairs, applying a VS and WCM, followed by attacker detection via confidence intervals. Unlike traditional methods, it employs soft detection decisions, assigning beliefs (votes) instead of binary classifications. These votes are converted into probabilities and used as WCM weights for refined localization. Potential attack intensities are estimated using an ML criterion, with final detection based on confidence intervals. Performance evaluation in terms of localization accuracy, detection rate, and computational complexity shows that the method achieves near-perfect detection when the attack intensity-to-noise ratio is sufficiently high. Although detection rate decreases as this ratio lowers, the proposed approach consistently outperforms existing methods in both detection performance and localization accuracy, reducing localization error by at least 30 % across various scenarios. Additionally, the VS-based solution operates efficiently, with a runtime of just a few milliseconds.

Data availability statement

The data analyzed in this study is subject to the following licenses/restrictions: The datasets will be share upon request. Requests to access these datasets should be directed to slavisa.tomic@ulusofona.pt.

Author contributions

ST: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. MB: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. DV:

Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. SK: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing.

Funding

The author(s) declared that financial support was received for this work and/or its publication. This research was partially funded by the European Union's Horizon Europe Research and Innovation Programme under the Marie Skłodowska-Curie grant agreement No. 101086387, by the Science Fund of the Republic of Serbia, Grant No. 221, *Agile Drone Swarm Control based on Federated Reinforcement Learning and Optimization - ASCENT*, by the Fundação para a Ciência e a Tecnologia under Projects UIDB/50008/2020 (<https://doi.org/10.54499/UIDB/50008/2020>) and 2021.04180.CEECIND.

Conflict of interest

Author SK was employed by DunavNET.

The remaining author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Bazzi, A., Slock, D. T. M., and Meilhac, L. (2016a). JADED-RIP: Joint angle and delay estimator and detector via rotational invariance properties, *IEEE international symposium on signal processing and information technology (ISSPIT)*, Limassol, Cyprus, 160–165. doi:10.1109/ISSPIT.2016.7886027

Bazzi, A., Slock, D. T. M., and Meilhac, L. (2016b). Sparse recovery using an iterative variational bayes algorithm and application to AoA estimation, *IEEE international symposium on signal processing and information technology (ISSPIT)*, Limassol, Cyprus, 197–202. doi:10.1109/ISSPIT.2016.7886034

- Bazzi, A., Slock, D. T. M., and Meilhac, L. (2018). On Maximum Likelihood Angle of Arrival Estimation Using Orthogonal Projection, 2018 *IEEE international conference on acoustics, speech and signal processing (ICASSP)*, Calgary, AB, Canada, 3241–3245. doi:10.1109/ICASSP.2018.8462437
- Beko, M., and Tomic, S. (2021). Toward secure localization in randomly deployed wireless networks. *IEEE Internet Things J.* 8, 17436–17448. doi:10.1109/jiot.2021.3078216
- Coluccia, A., and Fascista, A. (2018). On the hybrid toa/rss range estimation in wireless sensor networks. *IEEE Trans. Wirel. Commun.* 17, 361–371. doi:10.1109/twc.2017.2766628
- Garg, R., Varna, A. L., and Wu, M. (2012). An efficient gradient descent approach to secure localization in resource constrained wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* 7, 717–730. doi:10.1109/tifs.2012.2184094
- Kay, S. M. (1993). *Fundamentals of statistical signal processing: estimation theory*. Prentice-Hall, Inc.
- Kugler, L. (2017). Why gps spoofing is a threat to companies, countries. *Commun. ACM* 6, 18–19. doi:10.1145/3121436
- Li, Z., Trappe, W., Zhang, Y., and Nath, B. (2005). “Robust statistical methods for securing wireless localization in sensor networks,” in *IPSN 2005. Fourth international symposium on information processing in sensor networks*, 91–98.
- Li, Y., Ma, S., Yang, G., and Wong, K.-K. (2021). Secure localization and velocity estimation in mobile iot networks with malicious attacks. *IEEE Internet Things J.* 8, 6878–6892. doi:10.1109/jiot.2020.3036849
- Liu, D., Ning, P., Liu, A., Wang, C., and Du, W. (2007). Attack-resistant location estimation in wireless sensor networks. *Electr. Eng. Comput. Sci.* 11, 1–36. doi:10.1145/1380564.1380570
- Liu, X., Su, S., Han, F., Liu, Y., and Pan, Z. (2019). A range-based secure localization algorithm for wireless sensor networks. *IEEE Sensors J.* 19, 785–796. doi:10.1109/jsen.2018.2877306
- Matos-Carvalho, J. P., Santos, R., Tomic, S., and Beko, M. (2021). Gtrs-based algorithm for uav navigation in indoor environments employing range measurements and odometry. *IEEE Access* 9, 89120–89132. doi:10.1109/access.2021.3089900
- Mukhopadhyay, B., Srirangarajan, S., and Kar, S. (2021). Rss-based localization in the presence of malicious nodes in sensor networks. *IEEE Trans. Instrum. Meas.* 70, 1–16. doi:10.1109/tim.2021.3104385
- Niculescu, D., and Nath, B. (2004). “Vor base stations for indoor 802.11 positioning,” in *MobiCom’04*, 58–69.
- Oigbochie, A., Odigie, E., and Adejumo, B. (2021). Importance of drones in healthcare delivery amid a pandemic: current and generation next application. *Open J. Med. Res.* 2, 1–13. doi:10.52417/ojmr.v2i1.187
- Qiang, C. (2014). A forest early fire detection algorithm based on wireless sensor networks. *Sensors and Transducers* 166, 89–96.
- Shi, Y., and Yang, G. H. (2024). Secure bearing-based target localization for multi-agent networks against malicious agents. *IEEE Trans. Automation Sci. Eng.* 21, 5812–5825. doi:10.1109/tase.2023.3319334
- Singh, M., Leu, P., Abdou, A. R., and Čapkun, S. (2019). “Uwb-ed: distance enlargement attack detection in ultra-wideband,” in *28th USENIX security symposium*, 73–88.
- Tomic, S., and Beko, M. (2020). A geometric approach for distributed multi-hop target localization in cooperative networks. *IEEE Trans. Veh. Technol.* 69, 914–919. doi:10.1109/tvt.2019.2952715
- Tomic, S., and Beko, M. (2022). Detecting distance-spoofing attacks in arbitrarily-deployed wireless networks. *IEEE Trans. Veh. Technol.* 71, 4383–4395. doi:10.1109/tvt.2022.3148199
- Tomic, S., and Beko, M. (2024a). A min-max optimization-based approach for secure localization in wireless networks. *IEEE Trans. Veh. Technol.* 73, 4151–4161. doi:10.1109/tvt.2023.3325063
- Tomic, S., and Beko, M. (2024b). Trustworthy target localization via admm in the presence of malicious nodes. *IEEE Trans. Veh. Technol.* 73, 7250–7261. doi:10.1109/tvt.2023.3346476
- Tomic, S., Beko, M., Dinis, R., and Bernardo, L. (2018). On target localization using combined rss and aoa measurements. *Sensors* 18, 1–25. doi:10.3390/s18041266
- Wilson, E. B. (1927). Probable inference, the law of succession, and statistical inference. *J. Am. Stat. Assoc.* 22, 209–212. doi:10.1080/01621459.1927.10502953