



Please cite the Published Version

Tomic, Slavisa , Beko, Marko , Tsado, Yakubu , Adebisi, Bamidele  and Oladipo, Abiola (2025) Reinforcing Localization Credibility Through Convex Optimization. IEEE Signal Processing Letters, 32. pp. 3445-3449. ISSN 1070-9908

DOI: <https://doi.org/10.1109/LSP.2025.3601835>

Publisher: IEEE

Version: Published Version

Downloaded from: <https://e-space.mmu.ac.uk/641880/>

Usage rights:  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

Additional Information: This is an Open Access article published in IEEE Signal Processing Letters by IEEE.

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

Reinforcing Localization Credibility Through Convex Optimization

Slavisa Tomic , Marko Beko , Yakubu Tsado, Bamidele Adebisi , and Abiola Oladipo

Abstract—This work proposes a novel approach to reinforce localization security in wireless networks in the presence of malicious nodes that are able to manipulate (spoof) radio measurements. It substitutes the original measurement model by another one containing an auxiliary variance dilation parameter that disguises corrupted radio links into ones with large noise variances. This allows for relaxing the non-convex maximum likelihood estimator (MLE) into a semidefinite programming (SDP) problem by applying convex-concave programming (CCP) procedure. The proposed SDP solution simultaneously outputs target location and attacker detection estimates, eliminating the need for further application of sophisticated detectors. Numerical results corroborate excellent performance of the proposed method in terms of localization accuracy and show that its detection rates are highly competitive with the state of the art.

Index Terms—Attacker detection, convex-concave programming (CCP), measurement-spoofing, secure localization, semidefinite programming (SDP).

I. INTRODUCTION

RELIABLY determining locations of devices in wireless networks has always been a challenging task and will play an essential role in the forthcoming 6 G wireless systems, where manipulated (spoofed) location information can lead to catastrophic repercussions. Even though secure non-satellite based localization problem has been attracting interest in recent years [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], there

is no uniquely accepted solution and there is still potential for improvement in all relevant aspects (localization accuracy, detection rates and complexity).

Several studies have explored secure localization techniques to mitigate the impact of malicious anchors. Early approaches include least median of squares (LMS) and radio frequency (RF) fingerprinting, as investigated in [1]. The LMS method selects the best localization estimate based on median residues, while RF fingerprinting employs a median-based distance metric. Attack-resistant methods such as attack-resistant minimum mean square estimation (ARMMSE) and voting scheme (VS) were proposed in [2] to detect and exclude malicious anchors by analyzing inconsistencies or leveraging grid-based voting mechanisms. An iterative gradient descent approach for handling spoofing attacks was introduced in [3], where residues from malicious anchors tend to be higher and can thus be filtered out to enhance location estimation. More recent approaches employ weighted least squares (WLS) estimator [8] and density-based spatial clustering to distinguish normal from contaminated location points, as seen in [4], combined with sequential probability ratio tests for anchor authentication. Probabilistic models such as maximum a posteriori (MAP) estimators, solved using variational message passing, have been applied for secure localization in mobile wireless sensor networks in [5]. Other methods, such as the weighted central mass (WCM) approach in [6], exploit geometric properties to obtain initial estimates and iteratively refine them using trust region sub-problems (GTRS). A generalization of this method was presented in [7], where a generalized likelihood ratio test (GLRT) was used for detection, and the law of cosines (LC) was applied to reformulate the problem into a GTRS. Recent advancements include robust optimization techniques such as secure weighted least squares (SWLS) and l_1 -norm-based approaches, introduced in [9], which use statistical deviation thresholds and clustering methods to detect malicious nodes. Additionally, robust formulations using min-max optimization, second-order cone programming (SOCP), and robust GTRS (R-GTRS) were proposed in [10] to enhance localization security by treating attacks as nuisance parameters. Another approach, based on the alternating direction method of multipliers (ADMM) that employs least squares criterion together with a decomposition-coordination iterative scheme to refine localization estimates was presented in [11]. A VS based on the distance to hyperplanes formed by pairs of anchors was introduced in [12], with attacker classification being performed by confidence intervals.

In huge contrast to the existing solutions, this work takes a radically different approach and proposes a substitution of the original measurement model by a different one that accounts for noise variance dilation in order to capture corrupted measurements as ones with large noise variances. This is achieved by

Received 20 May 2025; accepted 18 August 2025. Date of publication 22 August 2025; date of current version 10 September 2025. This work was supported in part by the European Union's Horizon Europe Research and Innovation Programme through Marie Skłodowska-Curie under Grant 101086387; in part by the Science Fund of the Republic of Serbia under Grant No. 221, *Agile Drone Swarm Control based on Federated Reinforcement Learning and Optimization - ASCENT*; in part by the Fundação para a Ciência e a Tecnologia under Project UIDB/50008/2020 (10.54499/UIDB/50008/2020) and Project 2021.04180.CEECIND; and in part by the U.K. Engineering and Physical Sciences Research Council (EPSRC) and Horizon Europe Guarantee under Grant EP/X039021/1- REMARKABLE. The associate editor coordinating the review of this article and approving it for publication was Dr. Chen He. (*Corresponding author: Slavisa Tomic.*)

Slavisa Tomic is with COPELABS, ECATI, Lusófona University, 1749-024 Lisbon, Portugal, and also with the UNINOVA-CTS - Center of Technology and Systems, NOVA School of Science and Technology, 2829-516 Caparica, Portugal (e-mail: slavisa.tomic@ulusofona.pt).

Marko Beko is with Instituto de Telecomunicações, Instituto Superior Técnico, Universidade de Lisboa, 1049-001 Lisbon, Portugal, and also with COPELABS, ECATI, Lusófona University, 1749-024 Lisbon, Portugal (e-mail: marko.beko@tecnico.ulisboa.pt).

Yakubu Tsado and Bamidele Adebisi are with the Department of Engineering, Manchester Metropolitan University, M15 6BH Manchester, U.K. (e-mail: Y.Tsado@mmu.ac.uk; B.Adebisi@mmu.ac.uk).

Abiola Oladipo is with Tiwakiki Consulting Limited, M40 3LE Manchester, U.K. (e-mail: abiola.oladipo@tiwakikiconsulting.com).

Digital Object Identifier 10.1109/LSP.2025.3601835

defining an auxiliary variance amplification parameter which allows for transformation of the non-convex maximum likelihood estimator (MLE) into a convex semidefinite programming (SDP) problem by applying a simple convex-concave programming (CCP) procedure. The proposed SDP solution not only sets a new achievable lower bound on localization accuracy, but also holds within attacker detection estimation, depriving the need for refined detectors.

II. PROBLEM FORMULATION

Consider a q -dimensional ($q = 2$ or $q = 3$) wireless network, composed of two types of nodes: targets (nodes whose locations one desires to determine) and anchors (nodes whose locations are known and are exploited as reference points for localization purposes). Targets communicate with anchors that estimate distance information from the received signal (e.g., via time of arrival or received signal strength), which is then exploited for localization process of a single target at a time. The true location of a target is denoted by \mathbf{x} , while the true locations of anchors are denoted by $\mathbf{a}_i, i = 1, \dots, N$. Finally, a fraction of the anchors is considered corrupted and attempts to hinder the localization process by modifying its distance measurements, i.e., by performing spoofing attacks.

One can formulate secure range-based localization problem as a system of non-linear equations, where each equation corresponds to measured distance between an anchor and a target, corrupted with noise and potentially by a spoofing attack [7]. Hence, the k -th distance measurement sample, with $1 \leq k \leq K$, between the target and the i -th anchor (in meters) can be modelled [13], [14] as

$$d_{i,k} = \|\mathbf{x} - \mathbf{a}_i\| + \delta_i + n_{i,k}, \quad (1)$$

where $n_{i,k}$ stands for the measurement noise, modelled as a zero-mean Gaussian random variable with variance $\sigma_{i,k}^2$, i.e., $n_{i,k} \sim \mathcal{N}(0, \sigma_{i,k}^2)$, and $\delta_i \in \mathbb{R}$ represents the (unknown) intensity of the spoofing attack. It is clear that when $\delta_i = 0$ the i -th anchor is genuine (i.e., $i \in \mathcal{G}$), while $\delta_i \neq 0$ corresponds to the i -th anchor being corrupted (i.e., $i \in \mathcal{C}$).

For simplicity and with no loss of generality in the following derivations, the median of the K range measurements, d_i , is employed as the observation at the i -th anchor; thus, the subscript k is omitted. Likewise, the noise variances are assumed equal for all links (and samples), i.e., $\sigma_1^2 = \dots = \sigma_N^2 = \sigma^2$.

From (1) and following maximum likelihood principle [15], one can formulate the localization problem as an optimization problem with \mathbf{x} and δ_i as variables [11]. Nevertheless, such a problem is non-convex [16], since the argument of the square factor $(\|\mathbf{x} - \mathbf{a}_i\| + \delta_i - d_i)^2$ has a negative region when $\|\mathbf{x} - \mathbf{a}_i\| + \delta_i < d_i$, and is under-determined ($N + q$ unknowns with N equations). Hence, this work circumvents the presence of spoofed measurements by dilating noise variance, as illustrated in Fig. 1. To do so, the model in (1) is rewritten as

$$d_i = \|\mathbf{x} - \mathbf{a}_i\| + \epsilon_i, \quad (2)$$

where $\epsilon_i \sim \mathcal{N}(0, \rho_i \sigma^2)$, with $\rho_i = \begin{cases} 1, & \text{if } i \in \mathcal{G} \\ R_i \gg 1, & \text{if } i \in \mathcal{C} \end{cases}$ and R_i being the variance dilation parameter.

Note that the model in (2) is adopted to allow for the following derivations; the actual observations still come from (1).

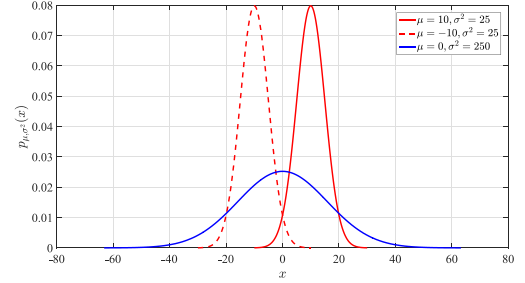


Fig. 1. Dilating noise variance to circumvent spoofing.

In what follows, this approximation is justified by showing that the Cramér-Rao lower bound (CRLB) of an estimator resulting from (2) is approximately equal to the one from (1). Let $\boldsymbol{\theta} = [\mathbf{x}^T, \nu_1, \dots, \nu_N]^T$ denote the $N + q$ vector of all unknown parameters, i.e., $\nu_i = \delta_i$ for (1) and $\nu_i = \rho_i$ for (2), $i = 1, \dots, N$. According to [15], the variance of any unbiased estimator is lower bounded by $\text{var}(\hat{\boldsymbol{\theta}}_i) \geq [\mathbf{F}^{-1}(\boldsymbol{\theta})]_{ii}$, with $\mathbf{F}(\boldsymbol{\theta})$ being the $(N + q) \times (N + q)$ Fisher information matrix, whose elements are defined as $[\mathbf{F}(\boldsymbol{\theta})]_{ij} = -\mathbb{E}[\frac{\partial^2 L(\mathbf{d}; \boldsymbol{\theta})}{\partial \theta_i \partial \theta_j}]$, where $i, j = 1, \dots, N + q$ and $L(\mathbf{d}; \boldsymbol{\theta})$ is the log-likelihood of $\mathbf{d} = [d_1, \dots, d_N]$ parametrized by $\boldsymbol{\theta}$. One can partition $\mathbf{F}(\boldsymbol{\theta})$ as

$$\mathbf{F}(\boldsymbol{\theta}) = \begin{bmatrix} \mathbf{A}(\boldsymbol{\theta}) \in \mathbb{R}^{q \times q} & \mathbf{B}(\boldsymbol{\theta}) \in \mathbb{R}^{q \times N} \\ \mathbf{B}^T(\boldsymbol{\theta}) \in \mathbb{R}^{N \times q} & \mathbf{C}(\boldsymbol{\theta}) \in \mathbb{R}^{N \times N} \end{bmatrix},$$

such that $\mathbf{A}(\boldsymbol{\theta}) = \frac{1}{\sigma^2} \sum_{i=1}^N \frac{(\mathbf{x} - \mathbf{a}_i)(\mathbf{x} - \mathbf{a}_i)^T}{\|\mathbf{x} - \mathbf{a}_i\|^2}$, $\mathbf{B}(\boldsymbol{\theta}) = \frac{1}{\sigma^2} [\frac{(\mathbf{x} - \mathbf{a}_1)}{\|\mathbf{x} - \mathbf{a}_1\|}, \dots, \frac{(\mathbf{x} - \mathbf{a}_N)}{\|\mathbf{x} - \mathbf{a}_N\|}]$, $\mathbf{C}(\boldsymbol{\theta}) = \frac{1}{\sigma^2} \mathbf{I}_N$ for (1), and $\mathbf{A}(\boldsymbol{\theta}) = \frac{1}{\sigma^2} \sum_{i=1}^N \frac{(\mathbf{x} - \mathbf{a}_i)(\mathbf{x} - \mathbf{a}_i)^T}{\rho_i \|\mathbf{x} - \mathbf{a}_i\|^2}$, $\mathbf{B}(\boldsymbol{\theta}) = \mathbf{0}_{2 \times N}$, $\mathbf{C}(\boldsymbol{\theta}) = \text{diag}([\frac{1}{2\rho_1^2}, \dots, \frac{1}{2\rho_N^2}])$ for (2). The CRLB for \mathbf{x} can then be derived as $\text{var}(\hat{\mathbf{x}}) \geq \text{trace}(\mathbf{F}_x^{-1}(\boldsymbol{\theta}))$, by computing the Schur complement of $\mathbf{C}(\boldsymbol{\theta})$, i.e.,

$$\mathbf{F}_x(\boldsymbol{\theta}) = \mathbf{A}(\boldsymbol{\theta}) - \mathbf{B}(\boldsymbol{\theta})\mathbf{C}^{-1}(\boldsymbol{\theta})\mathbf{B}^T(\boldsymbol{\theta}).$$

Recall that $\delta_i = 0$ and $\rho_i = 1$ when $i \in \mathcal{G}$; thus, it is clear that $\mathbf{F}_x = \frac{1}{\sigma^2} \sum_{i=1}^N \frac{(\mathbf{x} - \mathbf{a}_i)(\mathbf{x} - \mathbf{a}_i)^T}{\|\mathbf{x} - \mathbf{a}_i\|^2}$ for the two models, while when $i \in \mathcal{C}$, the CRLBs are approximately equal for $\rho_i \gg 1$.

According to (2), one can cast the localization problem as

$$(\hat{\mathbf{x}}, \hat{\boldsymbol{\rho}}) = \arg \max_{\mathbf{x}, \boldsymbol{\rho}} L(\mathbf{x}, \boldsymbol{\rho}) \quad (3)$$

where $\boldsymbol{\rho} = [\rho_1, \dots, \rho_N]^T$ and $L(\mathbf{x}, \boldsymbol{\rho}) = -\sum_{i=1}^N \ln \left\{ \frac{1}{\sqrt{2\pi\rho_i\sigma^2}} \exp\left\{-\frac{(d_i - \|\mathbf{x} - \mathbf{a}_i\|)^2}{2\rho_i\sigma^2}\right\} \right\}$ is the log-likelihood function. Then, since

$$L(\mathbf{x}, \boldsymbol{\rho}) \propto \sum_{i=1}^N \frac{(d_i - \|\mathbf{x} - \mathbf{a}_i\|)^2}{\rho_i} + \sum_{i=1}^N \ln(\rho_i)$$

and by relaxing the binary variable ρ_i into a continuous variable in the range $[1, \infty)$, yields

$$\underset{\mathbf{x}, \boldsymbol{\rho}}{\text{minimize}} \sum_{i=1}^N \frac{(d_i - \|\mathbf{x} - \mathbf{a}_i\|)^2}{\rho_i} + \sum_{i=1}^N \ln(\rho_i) \quad (4a)$$

$$\text{subject to } \rho_i \geq 1, i = 1, \dots, N. \quad (4b)$$

The problem in (4) involves an objective function that is a sum of non-convex and concave terms and is thus difficult to tackle directly. Nevertheless, the following section shows how this problem can be converted into a convex, SDP, problem.

III. THE PROPOSED SDP ESTIMATOR

Current section offers details on the derivation of the proposed algorithm for credible localization. Start by defining auxiliary variables $y_i = d_i - \|\mathbf{x} - \mathbf{a}_i\|$, $\mathbf{Y} = \mathbf{y}\mathbf{y}^T$ and $\mathbf{X} = \mathbf{x}\mathbf{x}^T$, where $\mathbf{y} = [y_1, \dots, y_N]^T$. Then, it follows that

$$(y_i - d_i)^2 = \|\mathbf{x} - \mathbf{a}_i\|^2 \Leftrightarrow Y_{ii} - 2d_i y_i + d_i^2 = \text{tr}(\mathbf{X}) - 2\mathbf{a}_i^T \mathbf{x} + \|\mathbf{a}_i\|^2$$

and consequently

$$(y_i - d_i)(y_j - d_j) = \|\mathbf{x} - \mathbf{a}_i\| \|\mathbf{x} - \mathbf{a}_j\|,$$

which, by applying the Cauchy–Schwarz inequality, yields

$$Y_{ij} \geq |\text{tr}(\mathbf{X}) - \mathbf{a}_j^T \mathbf{x} - \mathbf{a}_i^T \mathbf{x} + \mathbf{a}_j^T \mathbf{a}_i| + d_j y_i + d_i y_j - d_i d_j.$$

Moreover, introduce $e_i = \frac{(d_i - \|\mathbf{x} - \mathbf{a}_i\|)^2}{\rho_i} = \frac{(y_i)^2}{\rho_i} = \frac{Y_{ii}}{\rho_i}$ as an epigraph variable. This substitution, together with $\rho_i \geq 1$ results in

$$e_i \geq 0, \text{ and } Y_{ii} \geq e_i.$$

It also allows to deal with the second (concave term) summation of (4a) efficiently through an iterative CCP [17] as follows. Note first that $\ln(\rho_i) = \underbrace{\ln(Y_{ii})}_{\text{concave}} - \underbrace{\ln(e_i)}_{\text{convex}}$. Thus, for a feasible initial

point, $\hat{Y}_{ii}^{(0)}$, the concave terms are *convexified* in iteration t by an affine approximation (gradient evaluation) around that point, i.e.,

$$\ln(Y_{ii}; \hat{Y}_{ii}^{(t)}) = \ln(\hat{Y}_{ii}^{(t)}) + \frac{(Y_{ii} - \hat{Y}_{ii}^{(t)})}{\hat{Y}_{ii}^{(t)}},$$

for $t = 0, \dots, T$, with T being the maximum number of steps.

Therefore, by joining all described steps together, one arrives at the proposed SDP as

$$\underset{\mathbf{x}, \mathbf{y}, \mathbf{X}, \mathbf{Y}, \mathbf{e}}{\text{minimize}} \quad \sum_{i=1}^N e_i - \sum_{i=1}^N \ln(e_i) + \sum_{i=1}^N \frac{Y_{ii}}{\hat{Y}_{ii}^{(t)}} \quad (5a)$$

$$\text{subject to } e_i \geq 0, \quad i = 1, \dots, N, \quad (5b)$$

$$Y_{ii} \geq e_i, \quad i = 1, \dots, N, \quad (5c)$$

$$Y_{ii} = \text{tr}(\mathbf{X}) - 2\mathbf{a}_i^T \mathbf{x} + \|\mathbf{a}_i\|^2 + 2d_i y_i - d_i^2, \quad i = 1, \dots, N, \quad (5d)$$

$$Y_{ij} \geq |\text{tr}(\mathbf{X}) - \mathbf{a}_j^T \mathbf{x} - \mathbf{a}_i^T \mathbf{x} + \mathbf{a}_j^T \mathbf{a}_i| + d_j y_i + d_i y_j - d_i d_j, \\ i = 1, \dots, N, \quad j = 1, \dots, N, \quad (5e)$$

$$\begin{bmatrix} \mathbf{Y} & \mathbf{y} \\ \mathbf{y}^T & 1 \end{bmatrix} \succeq \mathbf{0}_{N+1}, \quad \begin{bmatrix} \mathbf{X} & \mathbf{x} \\ \mathbf{x}^T & 1 \end{bmatrix} \succeq \mathbf{0}_{q+1}, \quad (5f)$$

where all terms having no influence on minimization are omitted, the constraints $\mathbf{Y} = \mathbf{y}\mathbf{y}^T$ and $\mathbf{X} = \mathbf{x}\mathbf{x}^T$ are relaxed and written as semidefinite cone (SDC) constraints by applying the Schur complement, whereas the respective rank-1 constraints are dropped. The problem in (5) is an SDP and can be readily solved by CVX [18].

Algorithm 1: Pseudo-code for the Proposed SDP 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: $d_{i,k}$: k -th distance measurement sample at i -th anchor

Require: T : Maximum number of iterations

Require: τ : Threshold for stopping criterion

1: **Set:** $\hat{\mathbf{Y}}^{(0)} = 0.1 \times \mathbf{I}_N$, $\hat{\mathbf{x}}^{(0)} = 10^6 \times \mathbf{1}_{q \times 1}$,

$\hat{\mathbf{x}}^{(1)} = \mathbf{0}_{q \times 1}$, $\hat{\mathcal{M}} = \emptyset$ and $t = 1$

2: **while** $t \leq T$ and $\|\hat{\mathbf{x}}^{(t)} - \hat{\mathbf{x}}^{(t-1)}\| > \tau$ **do**

3: **Solve:** (5)

4: **Update:** $\hat{\mathbf{Y}}^{(t)} := \hat{\mathbf{Y}}$

5: **Update:** $\hat{\mathbf{x}}^{(t)} := \hat{\mathbf{x}}$

6: **Update:** $t := t + 1$

7: **end while**

8: **for** $i = 1, \dots, N$ **do**

9: **if** $\frac{\hat{y}_i^2}{e_i} > 1$ **then**

10: **Detect attacker:** $\hat{\mathcal{M}} := \hat{\mathcal{M}} \cup \{i\}$

11: **end if**

12: **end for**

13: **Return:** $\hat{\mathbf{x}}$ and $\hat{\mathcal{M}}$

The proposed solution for secure localization is summarized as a pseudo-code in Algorithm 1. It is worth mentioning that the initial $\hat{\mathbf{Y}}^{(0)}$ is chosen assuming that all measurements are genuine. Given this, and since $Y_{ii} = (d_i - \|\mathbf{x} - \mathbf{a}_i\|)^2$ by construction, $\hat{Y}_{ii}^{(0)}$ is initially set to a relatively low value.

IV. PERFORMANCE ANALYSIS

In this section, the performance of the proposed solution is validated from various perspectives, including computational complexity, localization accuracy and detection rates.

A. Complexity Analysis

The worst case computational complexity of an SDP is calculated [19] as

$$\mathcal{O} \left(C \left(m \sum_{i=1}^{N_{sd}} (n_i^{sd})^3 + m^2 \sum_{i=1}^{N_{sd}} (n_i^{sd})^2 + m^3 \right) \right),$$

where C is the iteration complexity, m denotes the number of equality constraint, n_i^{sd} is the dimension of the i -th SDC and N_{sd} is the number of SDC constraints.

Assuming that B_{\max} and B_{ADMM} stand for the maximum number of iterations for the GTRS-based and for the ADMM-based algorithms respectively, the worst-case computational complexity of the considered algorithms is summarized in Table I. The table shows that the proposed solution is computationally the most burdensome, but this is compensated in accuracy, as will be seen in the following subsection.

B. Localization and Detection Assessment

The following figures disclose numerical results where N anchors and a single target (at a time) were randomly deployed

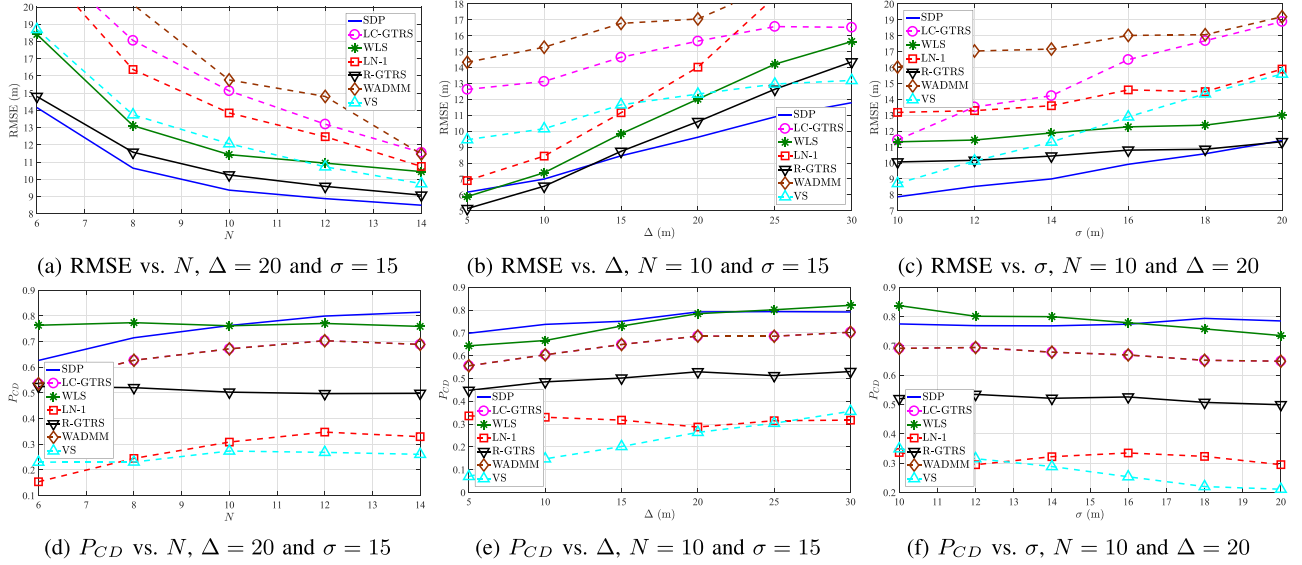


Fig. 2. Localization and detection performance comparisons in different scenarios.

TABLE I
SUMMARY OF THE CONSIDERED ALGORITHMS

Algorithm	Complexity
SDP in Section III	$\mathcal{O}(T \times N^{4.5})$
LC-GTRS in [7]	$2 \times \mathcal{O}(B_{\max} \times N)$
WLS in [8]	$\mathcal{O}(N)$
LN-1 in [9]	$\mathcal{O}(B_{\text{ADMM}} \times N)$
R-GTRS in [10]	$\mathcal{O}(B_{\max} \times N)$
WADMM in [11]	$\mathcal{O}(B_{\text{ADMM}} \times N)$

within a two-dimensional area of $B \times B \text{ m}^2$, with $B = 100$. Moreover, at most $N/2$ anchors were randomly chosen as corrupted, and this selection process was repeated $N_C = 20$ times for each node deployment, considering $N_D = 1000$ node deployments in total. All measurements were generated according to (1), where $K = 10$ measurement samples were considered and attacks were modelled through an exponential distribution whose rate was drawn from a uniform distribution on the interval $[0, \Delta]$ (m), i.e., $\delta_i \sim \pm \mathcal{E}(\mathcal{U}[0, \Delta])$, $\forall i$, where \pm represents a random sign attribution to δ_i . Results of the proposed SDP were achieved in maximum $T = 3$ iterations with the threshold set at $\tau = B/200$ m. Note that the results could be further improved by fine-tuning T and τ , but our experiments have shown that its performance for the adopted values is sufficient. Lastly, all methods were tested against exactly the same noise and attack realizations to guarantee a fair comparison.

The main performance metric for localization is the root mean square error (RMSE), defined as $\text{RMSE} = \sqrt{\sum_{m=1}^{M_C} \frac{\|\mathbf{x}_m - \hat{\mathbf{x}}_m\|^2}{M_C}}$, where $\hat{\mathbf{x}}_m$ is the estimate of the true target location, \mathbf{x}_m , in the m -th Monte Carlo, $M_C = N_D \times N_C$, run, while detection is validated through the probability of correct detection, P_{CD} . It is worth noting that this work considers that the event space is composed of two possible events: a malicious anchor is correctly detected (CD) or not detected (ND); thus, $P_{CD} = \frac{N_{CD}}{N_{CD} + N_{ND}}$, where N_{CD} , and N_{ND} denote respectively the number of CD and ND corrupted anchors.

Fig. 2 validates the performance of the considered algorithms in different scenarios. In terms of localization accuracy, Fig. 2 shows that the proposed SDP algorithm outperforms the existing ones in general, being R-GTRS the only true competitor in some cases. However, note that R-GTRS in [10] requires additional knowledge about model parameters, namely on the magnitude of the attack intensity, $|\delta_i|$ in (1); thus, the true value of $|\delta_i|$ is given to R-GTRS in all presented simulations. Obviously, perfect knowledge about this parameter can hardly be possible in practice beforehand, and R-GTRS could exhibit significant performance impairments in more practical settings. Still, the proposed SDP gains almost 20% in terms of accuracy over R-GTRS when $\Delta = 30$, $\sigma = 15$ and $N = 10$. In terms of detection rates, the figure corroborates the effectiveness of the proposed approach, classifying it among the most superior ones in all considered scenarios. This goes to show that competitive attacker detection can be accomplished even without resorting to sophisticated detection procedures.

V. CONCLUSION

This work introduced a novel approach to reinforce localization credibility in wireless networks in the presence of corrupted/malfunctioning nodes. It proposed neutralizing malicious attacks by considering a surrogate measurement model with dilated noise variance to eliminate malicious attacks by disguising corrupted radio links into ones with large noise variances. In this way, one is able to transform the non-convex MLE into an SDP via a simple CCP procedure. Overall, the proposed method is straightforward to implement and represents a good trade off between localization accuracy and computational complexity, carrying higher computational burden than the existing solutions, but compensating for that by improved localization accuracy. The proposed solution is aimed towards mission-critical applications that require accurate and trustworthy location information and have abundant computational resources available. It also serves to show that the current lower bound on the achievable localization performance can still be brought down.

REFERENCES

- [1] 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.*, 2005, pp. 91–98.
- [2] D. Liu, P. Ning, A. Liu, C. Wang, and W. Du, "Attack-resistant location estimation in wireless sensor networks," *Elect. Eng. Comput. Sci.*, vol. 11, no. 20, pp. 1–36, 2007.
- [3] 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 Secur.*, vol. 7, no. 2, pp. 717–730, Apr. 2012.
- [4] X. Liu, S. Su, F. Han, Y. Liu, and Z. Pan, "A range-based secure localization algorithm for wireless sensor networks," *IEEE Sensors J.*, vol. 19, no. 2, pp. 785–796, Jan. 2019.
- [5] Y. Li, S. Ma, G. Yang, and K.-K. Wong, "Secure localization and velocity estimation in mobile IoT networks with malicious attacks," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6878–6892, Apr. 2021.
- [6] M. Beko and S. Tomic, "Toward secure localization in randomly deployed wireless networks," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17436–17448, Dec. 2021.
- [7] S. Tomic and M. Beko, "Detecting distance-spoofing attacks in arbitrarily-deployed wireless networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4383–4395, Apr. 2022.
- [8] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, "Robust range-based secure localization in wireless sensor networks," in *Proc. IEEE Glob. Commun. Conf.*, 2018, pp. 1–6.
- [9] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, "RSS-based localization in the presence of malicious nodes in sensor networks," *IEEE Trans. Instrum. Meas.*, vol. 70, 2021, Art. no. 5503716.
- [10] S. Tomic and M. Beko, "A min-max optimization-based approach for secure localization in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 73, no. 3, pp. 4151–4161, Mar. 2024.
- [11] S. Tomic and M. Beko, "Trustworthy target localization via ADMM in the presence of malicious nodes," *IEEE Trans. Veh. Technol.*, vol. 73, no. 5, pp. 7250–7261, May 2024.
- [12] S. Tomic, M. Beko, D. Vukobratovic, and S. Krco, "Voting scheme to strengthen localization security in randomly-deployed wireless networks," 2025, *arXiv.2502.20218*.
- [13] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, 2011, pp. 75–86.
- [14] S. H. Seo, G. I. Jee, and B. H. Lee, "Spoofing signal generation based on manipulation of code delay and Doppler frequency of authentic GPS signal," *Int. J. Control, Automat. Syst.*, vol. 19, no. 2, pp. 1026–1040, 2021.
- [15] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.
- [16] C. Soares, F. Valdeira, and J. Gomes, "Range and bearing data fusion for precise convex network localization," *IEEE Signal Process. Lett.*, vol. 27, pp. 670–674, 2020.
- [17] X. Shen, S. Diamond, Y. Gu, and S. Boyd, "Disciplined convex-concave programming," in *Proc. IEEE Conf. Decis. Control*, 2016, pp. 1009–1014.
- [18] M. Grant and S. Boyd, "CVX: MatLab software for disciplined convex programming," 2010. Accessed: Apr. 23, 2024. [Online]. Available: <http://cvxr.com/cvx>
- [19] I. Pólik and T. Terlaky, "Interior point methods for nonlinear optimization," in *Nonlinear Optimization*, G. D. Pillo and F. Schoen, Eds., Berlin, Germany: Springer, 2010, pp. 215–276.